Algebraic Aspects of Propositional Logic

Nicholas Leisegang

Dissertation Presented for the degree of Master of Science in the Department of Mathematics and Applied Mathematics, University of Cape Town

Supervisor: Dr Tamar Janelidze-Gray

Co-supervisor: Professor George Janelidze

January 2024

Abstract

In this dissertation, we seek to examine the connection between abstract algebra and propositional logic. We start by considering the category **Bool** of Boolean algebras, the algebraic counterpart of classical propositional logic. We provide an algebraic definition of theories and models of classical logic and provide algebraic algorithms to determine whether a chosen formula is a theorem of a given theory of classical logic. In order to generalize this approach, we then describe varieties of universal algebra and some of their properties. Using this framework, we show in a general setting how a formal theory of propositional logic induces a variety of universal algebra in which logical connectives become algebraic operations and logical formulae are considered equal when they are logically equivalent. We then discuss algebraic varieties corresponding to various non-classical propositional logics. In particular, we consider the variety of Heyting algebras **Heyt** which corresponds to intuitionistic logic, and certain subvarieties of **Heyt** which correspond to intermediate logics. We then describe several algebraic varieties which correspond to theories of normal modal logic. Moreover, by considering free algebras and completeness in **Heyt**, we establish that we are unable to use the same methods used in **Bool** to construct algorithms to determine theorems of intuitionistic logic. Lastly, we construct an adjunction between **Heyt** and the category of topological Boolean algebras, and through this show that we again cannot construct similar algebraic algorithms to determine theorems in the modal logic **S4**.

Acknowledgements

I would first like to thank my supervisors, Dr Tamar Janelidze-Gray and Professor George Janelidze, whose guidance, expertise and dedication made this dissertation possible.

I would like to thank the Skye Foundation, the EDTP-SETA bursary and the Myer Levinson Scholarship for their financial support during my masters studies.

I would also like to thank the Erasmus+ Programme for providing me with the opportunity to complete a two month academic traineeship at the Université Catholique de Louvain (UCLouvain). I would also like to express my gratitude to the administrators and academics in the UCLouvain mathematics department for making me feel welcome during my stay; especially to Professor Marino Gran and Professor Tim Van Der Linden for their supervision during this time.

I would like to thank the postgraduate students who I have engaged with at the University of Cape Town and UCLouvain mathematics departments, whose insightful conversations and friendships have maintained my motivation.

Finally, I would like to thank my parents, my sister and my partner, for their constant love and support throughout my masters studies.

Contents

1 Introduction

1.1 Introduction

The algebra of propositional logic begins by converting propositions in a formal theory of classical logic (such as in [15]) into elements of a Boolean algebra. In this dissertation, we aim to examine the connection between propositional logics and algebraic varieties in a more general setting. In doing so, we aim to describe the algebraic structures which correspond to various propositional logics, both classical and non-classical. Moreover, we aim to investigate certain properties of these algebraic varieties which give us insight into both the algebraic structures and their corresponding logics.

We begin in Chapter 2 by examining various properties of the category of Boolean algebras, which corresponds to classical propositional logic. In particular, we provide a construction of the free Boolean ring, or equivalently the free Boolean algebra over a set X. Furthermore, we conclude that finitely generated Boolean algebras are finite, and that the category of finite Boolean algebras is dual to the category of finite sets. Using these facts, we define a theory of classical propositional logic as a pair (X, A) where X is a set of variables, logical formulae are represented by the elements of the free Boolean algebra over X, denoted $F_{\mathbf{Bool}}(X)$, and $A \subseteq F_{\mathbf{Bool}}(X)$ is a set of axioms. We then define the models (also called $\{0,1\}$-valued models) of a theory (X, A) as any Boolean homomorphism $m \in \hom(F_{\mathbf{Bool}}(X), \{0,1\})$ such that $m(a) = 1$ for all $a \in A$. This allows us to provide algebraic proofs of the completeness and soundness of classical propositional logic, as well as construct two algorithms which can determine whether a given formula $p \in F_{\mathbf{Bool}}(X)$ is a theorem in a given theory of classical logic (X, A).

In Chapter 3, we provide a definition of varieties of universal algebra, and discuss certain properties of such varieties. This allows us to generalize our previous approach to non-classical logics and to formally consider "terms" which are equal to 1 in all Boolean algebras, and hence theorems in any theory of classical logic. In particular, we define a term algebra for a given signature of algebraic operations, and define a variety as a class of algebras with the same signature where each algebra satisfies a set of identities, expressed as pairs of elements in the term algebra. We consider subalgebras, product algebras, congruences, quotient algebras and free algebras in a general variety, and provide a proof of Birkhoff's Theorem. Lastly, we describe completeness in a general variety $\mathbb{V}$ with respect to L-valued models for some $L \in \mathbb{V}$, which generalizes the concept of completeness discussed in Chapter 2.

In Chapter 4, we discuss the connection between formal theories and algebraic varieties. Specifically, we introduce the definition of a formal propositional theory $\mathscr{T}$ and show how the formulae of such a theory $\mathrm{Frm}(\mathscr{T})$ can be considered an algebra where its logical connectives are considered as a signature of algebraic operations, denoted Ω. Moreover, we show that the resulting algebra is isomorphic to the term algebra over Ω. Furthermore, we consider a set of algebraic identities on $\mathrm{Frm}(\mathscr{T})$ which for a theory $\mathscr{T}$ induces a congruence on $\mathrm{Frm}(\mathscr{T})$ such that a pair (p, q) is an element of this congruence when p and q are logically equivalent in $\mathscr{T}$. From this we obtain a free algebra and a corresponding variety of algebras which characterizes our theory $\mathscr{T}$. We show how this construction can be applied by showing the correspondence between **Bool** and the formal theory of classical propositional logic as described in [15].

In our final chapter (Chapter 5), we consider some algebraic varieties corresponding to certain well-known non-classical propositional logics. We first consider the variety of Heyting algebras **Heyt** and some of its subvarieties, which correspond to intuitionistic logic and various superintuitionistic logics respectively. In particular, we show that finitely generated Heyting algebras are not, in general, finite, and that **Heyt** is not complete with respect to its L-valued models for any finite $L \in \mathbf{Heyt}$. Thus, we conclude that the methods used to construct the algorithms for determining theorems for classical logic cannot be used in the case of intuitionistic logic. However, we show that such an algorithm does exist in the case of Gödel–Dummett algebras, a subvariety of **Heyt**. We then consider certain varieties of algebras induced by various normal modal logics, whose objects are Boolean algebras equipped with an additional unary operator. Lastly, we construct an adjunction between **Heyt** and the variety of topological Boolean algebras **TopBool** which corresponds to the modal logic **S4**. Through this adjunction we show that finitely generated topological Boolean algebras are not finite in general, and thus the methods used to construct our algorithms in Chapter 2 cannot be used in the context of the modal logic **S4**.

This dissertation assumes some knowledge of basic order theory, lattice theory and category theory. We recall here some preliminary definitions and results (without proof) from these fields.

1.2 Adjoint Functors

Theorem 1.2.1. [13]**.** *Let $\mathbb{C}$ and $\mathbb{D}$ be categories. Then, the following conditions are equivalent,*

1. *There exist functors $F : \mathbb{C} \to \mathbb{D}$ and $G : \mathbb{D} \to \mathbb{C}$, such that for all objects $C \in \mathbb{C}$ and $D \in \mathbb{D}$ there is a bijection,*

$$hom(F(C), D) \cong hom(C, G(D))$$

which is natural in both C and D.

2. *There exist functors $F : \mathbb{C} \to \mathbb{D}$ and $G : \mathbb{D} \to \mathbb{C}$ and a natural transformation $\eta : 1_{\mathbb{C}} \to GF$ such that each $\eta_C : C \to GF(C)$ is a universal arrow from C to G.*

3. *There exists a functor $G : \mathbb{D} \to \mathbb{C}$ and object $F(C) \in \mathbb{D}$ for each object $C \in \mathbb{C}$ such that for each C, there exists a morphism $\eta_C : C \to GF(C)$ in $\mathbb{C}$ which is a universal arrow from C to G.*

4. *There exist functors $F : \mathbb{C} \to \mathbb{D}$ and $G : \mathbb{D} \to \mathbb{C}$ and a natural transformation $\epsilon : FG \to 1_{\mathbb{D}}$ such that each $\epsilon_D : FG(D) \to D$ is a universal arrow from F to D.*

5. *There exists a functor $F : \mathbb{C} \to \mathbb{D}$ and object $G(D) \in \mathbb{C}$ for each object $D \in \mathbb{D}$ such that for each D, there exists a morphism $\epsilon_D : FG(D) \to D$ in $\mathbb{D}$ which is a universal arrow from F to D.*

Definition 1.2.2. If any of the above hold we say there is an **adjunction** from $\mathbb{C}$ to $\mathbb{D}$. We also denote this by $F \dashv G$ and call the functors F and G the **left** and **right adjoints**, respectively. The natural transformations η and ϵ are called the **unit** and **counit** of our adjunction, respectively.

There are other equivalent conditions which define an adjunction. However, in this dissertation, we only make use of those above, referring most commonly to condition c. Thus, we typically construct an adjunction through the condition that there exists a functor $G : \mathbb{D} \to \mathbb{C}$, and for each object $C \in \mathbb{C}$, there exists an object $F(C) \in \mathbb{D}$, and a morphism $\eta_C : C \to GF(C)$ in $\mathbb{D}$, such that, for any object $D \in \mathbb{D}$ and any morphism $\alpha : C \to G(D)$ in $\mathbb{C}$, there exits a unique morphism $\phi : F(C) \to D$ in $\mathbb{D}$ such that the diagram

$$\begin{array}{ccc} C & \xrightarrow{\eta_C} & GF(C) \\ & \searrow^{\alpha} & \downarrow{\scriptstyle G(\Phi)} \\ & & G(D) \end{array}$$

commutes.

We also make use of the following results for adjunctions, all of which can be found in Mac Lane [13].

Lemma 1.2.3. *The following results hold,*

a. *If $F \dashv G$ is an adjunction from $\mathbb{C}$ to $\mathbb{D}$, and $F' \dashv G'$ is an adjunction from $\mathbb{D}$ to $\mathbb{E}$, then $F'F \dashv GG'$ is an adjunction from $\mathbb{C}$ to $\mathbb{E}$. That is, adjunctions compose.*

b. *If $F \dashv G$ and $F' \dashv G$, then F and F' are isomorphic functors. Similarly, if $F \dashv G$ and $F \dashv G'$ then G and G' are isomorphic functors. That is, adjunctions are unique up to isomorphism.*

c. *Right adjoints preserve limits. In particular, they preserve products and terminal objects.*

d. Left adjoints preserve colimits. In particular, they preserve coproducts and initial objects.

e. $\eta_C : C \to GF(C)$ *is an isomorphism for each object* $C \in \mathbb{C}$ *if and only if* F *is fully faithful.*

f. $\epsilon_D : FG(D) \to D$ *is an isomorphism for each object* $D \in \mathbb{D}$ *if and only if* G *is fully faithful.*

It is worth noting that although the general form of the result in 3. and 4. is given, in this dissertation we will typically refer to the result applied to products, coproducts, initial objects and terminal objects.

1.3 Lattices as Categories

We recall here certain order-theoretic structures and in particular, how they can be interpreted categorically.

Lemma 1.3.1. [13]. *A preordered set* $(P, \leq)$ *can be considered a category where the objects are the elements of* P *and for* $x, y \in P$*, there is a unique morphism* $x \to y$ *if and only if* $x \leq y$*.*

In particular, an ordered set $(P, \leq)$ is a category as above where the existence of morphisms $x \to y$ and $y \to x$ implies that $x = y$. We then characterize an adjunction between preordered sets.

Lemma 1.3.2. *A functor* f *from a preordered set* $(P, \leq)$ *to a preordered set* $(Q, \leq)$ *is equivalent to an order-preserving map* $f : P \to Q$*. Hence, an adjunction from a preordered set* $(P, \leq)$ *to a preordered set* $(Q, \leq)$ *is a pair of order preserving maps* $f : P \to Q$ *and* $g : Q \to P$ *such that* $f(x) \leq y$ *if and only if* $x \leq g(y)$ *for all* $x \in P$ *and* $y \in Q$*.*

Lemma 1.3.3. *In an ordered set* $(P, \leq)$*, considered as a category, the following holds,*

a. The product of x *and* y*, if it exists, is given by the infimum or meet,* $x \wedge y$*. Dually, the coproduct is given by* $x \vee y$*.*

b. The terminal object of P*, if it exists, is the greatest element of* P*. Dually, the initial object of* P *is the least element of* P*.*

We then recall the following definitions.

Definition 1.3.4.

- A **semilattice** $S = (S, \wedge, 1)$ is a set S equipped with an associative, commutative and idempotent binary operation $\wedge$ such that 1 is the identity for $\wedge$.
- A **lattice** $L = (L, \wedge, 1, \vee, 0)$ is a 5-tuple such that $(L, \wedge, 1)$ and $(L, \vee, 0)$ are semilattices, and for all $x, y \in L$, $(x \vee y) \wedge x = x$ and $(x \wedge y) \vee x = x$. These are called the absorption laws.
- A **distributive lattice** is a lattice L which satisfies the distributive laws $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$ and $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$ for all $x, y, z \in L$. Moreover, if a lattice satisfies one of the above laws it follows that it satisfies both laws.

- A **Boolean algebra** $B = (B, \wedge, 1, \vee, 0, \neg)$ is a 6-tuple such that $(B, \wedge, 1, \vee, 0)$ is a distributive lattice and $\neg$ is a unary operation such that $\neg x \vee x = 1$ and $\neg x \wedge x = 0$ for all $x \in B$. The element $\neg x$ is referred to as the complement of x and is the unique element of B with this property.

It is worth noting that we define lattices such that they have a greatest and least element. Some authors (such as in Davey and Priestley [9]) do not require this, and refer to lattices with greatest and least elements as *bounded* lattices. We also recall that any lattice L can be equipped with a partial order $\leq$ defined by $x \leq y$ if and only if $x \wedge y = x$ (or equivalently $x \vee y = y$) for all $x, y \in L$. A lattice L is called *complete* when any subset $A \subseteq L$ has a supremum and an infimum, with respect to the order $\leq$ as previously defined.

Thus, we can characterize a lattice $(L, \leq)$ as a preorder with finite products and coproducts, and an initial and terminal object. A complete lattice is a lattice with arbitrary products and coproducts.

Corollary 1.3.5. *If an order preserving map between lattices $f : L \to M$ is a left adjoint, it preserves $\vee$ and 1. If it is a right adjoint, it preserves $\wedge$ and 0.*

Lastly, we recall order-theoretic notions of closure and interior operators, which are utilized throughout the dissertation.

Definition 1.3.6. If $(P, \leq)$ is an ordered set, a **closure operator** is an order preserving map $c : P \to P$ such that $x \leq c(x)$ and $c(x) = cc(x)$ for all $x \in P$. If P has binary joins, then c is a **topological** closure operator if $c(x \vee y) = c(x) \vee c(y)$.

Dually, an **interior operator** is an order preserving map $i : P \to P$ such that $i(x) \leq x$ and $i(x) = ii(x)$ for all $x \in P$. If P has binary meets, then i is a **topological** interior operator if $i(x \wedge y) = i(x) \wedge i(y)$.

2 Boolean Algebras

In this chapter, we consider the category of Boolean algebras **Bool** which is the algebraic counterpart of classical logic. In particular, we introduce Boolean rings and show that the category of Boolean rings is isomorphic to **Bool**. We then construct a free Boolean ring, and thus prove that a finitely generated Boolean algebra is finite. Then, we show that the categories of finite Boolean algebras and finite sets, written $\mathbf{Bool_{Fin}}$ and $\mathbf{Set_{Fin}}$, are dual. Furthermore, we provide an algebraic definition for theories and models of classical propositional logic, and prove the soundness and completeness of classical propositional logic algebraically. Moreover, we introduce a Galois connection between models and theories, which, along with the duality of $\mathbf{Bool_{Fin}}$ and $\mathbf{Set_{Fin}}$, will be used to construct two algorithms which can determine whether a chosen formula is a theorem of a given theory of classical propositional logic.

2.1 Boolean Rings

In this section, we show that the category of Boolean algebras is isomorphic to the category of Boolean rings, such that each Boolean algebra induces a Boolean ring structure on its underlying set. This will allow us to treat Boolean rings and algebras as equivalent structures in further sections.

Definition 2.1.1. A **Boolean ring** $B = (B, +, -, 0, \cdot, 1)$ is a ring such that multiplication is commutative and idempotent. The category **BoolRing** has Boolean rings as its objects and ring homomorphisms as its morphisms.

Lemma 2.1.2. *In a Boolean ring B, $-x = x$ for all $x \in B$.*

Proof. First note that $(x + x)(x + x) = x + x$, since $\cdot$ is idempotent. Then using distributive laws we have,

$$x + x = (x + x)(x + x) = xx + xx + xx + xx = x + x + x + x$$

and thus, $-x = x + x - x - x - x = x + x + x + x - x - x - x = x$. □

Note 2.1.3. Since $-x = x$ in a Boolean ring, we may remove the $-$ when we denote it, and simply write $B = (B, +, 0, \cdot, 1)$.

Theorem 2.1.4. [17]**.** *The categories **Bool** and **BoolRing** are isomorphic. In particular, any Boolean algebra $B = (B, 0, \wedge, 1, \vee, \neg)$ can be considered a Boolean ring, where the ring operations on B are defined in terms of its Boolean algebra operations, and any Boolean ring $B = (B, +, 0, \cdot, 1)$ can be considered a Boolean algebra with the algebra operations defined in terms of its ring operations.*

Proof. In order to show that these categories are isomorphic, we construct functors $F : \mathbf{Bool} \to \mathbf{BoolRing}$ and $G : \mathbf{BoolRing} \to \mathbf{Bool}$ such that $GF = 1_{\mathbf{Bool}}$ and $FG = 1_{\mathbf{BoolRing}}$. That is, we

1. Construct F and show that it is a well-defined functor.

2. Construct G and show that it is a well-defined functor.

3. Prove that $GF = 1_{\mathbf{Bool}}$ and $FG = 1_{\mathbf{BoolRing}}$.

1.: For each object $(B, 0, \wedge, 1, \vee, \neg)$, we let $F((B, 0, \wedge, 1, \vee, \neg)) = (B, +, -, 0, \cdot, 1)$ where B is the same underlying set, 0 and 1 are the same elements in the ring and the Boolean algebra and,

- $x + y = (x \wedge \neg y) \vee (y \wedge \neg x)$
- $x \cdot y = x \wedge y$

for all $x, y \in B$. Then for any morphism $f : A \to B$ in **Bool** we define $F(f)$ as the same underlying function f, considered as a ring homomorphism.

Let $x, y, z \in B$. Note that,
$x + y = (x \wedge \neg y) \vee (y \wedge \neg x) = (y \wedge \neg x) \vee (x \wedge \neg y) = y + x$. Thus, $+$ is commutative.
Moreover,

$$\begin{aligned}
x + (y + z) &= (x \wedge \neg((y \wedge \neg z) \vee (z \wedge \neg y))) \vee (((y \wedge \neg z) \vee (z \wedge \neg y)) \wedge \neg x) \\
&= (x \wedge \neg(y \wedge \neg z) \wedge \neg(z \wedge \neg y)) \vee (y \wedge \neg z \wedge \neg x) \vee (z \wedge \neg y \wedge \neg x) \\
&= (x \wedge (\neg y \vee z) \wedge (\neg z \vee y)) \vee (y \wedge \neg z \wedge \neg x) \vee (z \wedge \neg y \wedge \neg x) \\
&= (((x \wedge \neg y) \vee (x \wedge z)) \wedge (\neg z \vee y)) \vee (y \wedge \neg z \wedge \neg x) \vee (z \wedge \neg y \wedge \neg x) \\
&= (x \wedge \neg y \wedge \neg z) \vee (x \wedge z \wedge y) \vee (y \wedge \neg z \wedge \neg x) \vee (z \wedge \neg y \wedge \neg x) \\
&= (x \wedge y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge z).
\end{aligned}$$

Similarly,

$$\begin{aligned}
(x + y) + z &= (((x \wedge \neg y) \vee (y \wedge \neg x)) \wedge \neg z) \vee (z \wedge \neg((x \wedge \neg y) \vee (y \wedge \neg x)) \\
&= (x \wedge \neg y \wedge \neg z) \vee (y \wedge \neg x \wedge \neg z) \vee (z \wedge (\neg(x \wedge \neg y) \wedge \neg(y \wedge \neg x))) \\
&= (x \wedge \neg y \wedge \neg z) \vee (y \wedge \neg x \wedge \neg z) \vee (z \wedge (\neg x \vee y) \wedge (\neg y \vee x)) \\
&= (x \wedge \neg y \wedge \neg z) \vee (y \wedge \neg x \wedge \neg z) \vee (z \wedge \neg x \wedge \neg y) \vee (z \wedge y \wedge x) \\
&= (x \wedge y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge z)
\end{aligned}$$

and hence, $+$ is associative.

Furthermore, note that, $x+0 = (x \wedge \neg 0) \vee (0 \wedge \neg x) = (x \wedge 1) \vee 0 = x \wedge 1 = x$. Thus, 0 is the identity for $+$.

Then, $x + x = (x \wedge \neg x) \vee (x \wedge \neg x) = x \wedge \neg x = 0$, and it follows that $x = -x$.

Furthermore, since $\cdot$ is the same operation as $\wedge$, $\cdot$ must be idempotent associative and commutative by definition of $\wedge$. We have that 1 is the identity of $\cdot$ since, $x \cdot 1 = x \wedge 1 = x$.

We then only need to show the distributivity axiom for rings holds in $(B, +, 0, \cdot, 1)$. Note that,

$$\begin{aligned} x(y+z) &= x \wedge ((y \wedge \neg z) \vee (z \wedge \neg y)) \\ &= (x \wedge y \wedge \neg z) \vee (x \wedge z \wedge \neg y). \end{aligned}$$

And,

$$\begin{aligned} xy + xz &= ((x \wedge y) \wedge \neg(x \wedge z)) \vee ((x \wedge z) \wedge \neg(x \wedge y)) \\ &= (x \wedge y \wedge (\neg x \vee \neg z)) \vee (x \wedge z \wedge (\neg x \vee \neg y)) \\ &= (x \wedge y \wedge \neg x) \vee (x \wedge y \wedge \neg z) \vee (x \wedge z \wedge \neg x) \vee (x \wedge z \wedge \neg y) \\ &= (0 \wedge y) \vee (x \wedge y \wedge \neg z) \vee (0 \wedge z) \vee (x \wedge z \wedge \neg y) \\ &= 0 \vee (x \wedge y \wedge \neg z) \vee 0 \vee (x \wedge z \wedge \neg y) \\ &= (x \wedge y \wedge \neg z) \vee (x \wedge z \wedge \neg y). \end{aligned}$$

Hence, the distributivity axiom holds and $(B, +, 0, \cdot, 1)$ is a Boolean ring.

If $f : A \to B$ is a morphism in **Bool**, it must preserve the ring operations on $(B, +, 0, \cdot, 1)$, since each ring operation is defined in terms of Boolean algebra operations. Hence, each Boolean algebra homomorphism $f : A \to B$ is a Boolean ring homomorphism $f : F(A) \to F(B)$. Trivially, F preserves identities and function composition, and thus F is a well-defined functor.

2.: For each object $(B, +, 0, \cdot, 1)$ in **BoolRing** we let $G((B, +, -, 0, \cdot, 1)) = (B, 0, \wedge, 1, \vee, \neg)$ where B is the same underlying set, 0 and 1 are the same elements in the Boolean ring and Boolean algebra and,

- $x \vee y = x + y + xy$.

- $x \wedge y = xy$.
- $\neg x = 1 + x$.

for all $x, y \in B$. For any morphism $f : A \to B$ in **BoolRing** we similarly define $G(f)$ as the same underlying function, f, considered as a Boolean algebra homomorphism. We first show that $G((B, +, 0, \cdot, 1)) = (B, 0, \wedge, 1, \vee, \neg)$ is a Boolean algebra. Consider, $x, y, z \in B$. Then,
$x \vee y = x + y + xy = y + x + yx = y \vee x$, and so $\vee$ is commutative.

Furthermore,

$$\begin{aligned}(x \vee y) \vee z &= (x + y + xy) + z + (x + y + xy)z \\ &= x + y + xy + z + zx + zy + zxy \\ &= x + y + z + xy + xz + yz + xyz.\end{aligned}$$

And,

$$\begin{aligned}x \vee (y \vee z) &= x + (y + z + yz) + x(y + z + yz) \\ &= x + y + z + yz + xy + xz + xyz \\ &= x + y + z + xy + xz + yz + xyz \\ &= (x \vee y) \vee z.\end{aligned}$$

Therefore, $\vee$ is associative.

Moreover, we observe that $x \vee x = x + x + xx = x + x + x = x$, and thus $\vee$ is idempotent. Then, since $x \vee 0 = x + 0 + x \cdot 0 = x + 0 + 0 = 0$, we have that 0 is the identity of $\vee$.

The commutativity, associativity, and idempotency of $\wedge$ follows directly from the fact that $\cdot$ is defined to be commutative, associative and idempotent. Furthermore, 1 is the identity of the $\wedge$ operation since it is the identity of our ring multiplication.

We then observe that

$$
\begin{aligned}
x \vee \neg x &= x + (1+x) + x(1+x) \\
&= x + 1 + x + x + xx \\
&= x + x + x + x + 1 \\
&= 0 + 1 = 1.
\end{aligned}
$$

Moreover,

$$
\begin{aligned}
x \wedge \neg x &= x(1+x) \\
&= x + xx \\
&= x + x = 0.
\end{aligned}
$$

Hence $\neg$, as defined above, satisfies the axioms of $\neg$ in a Boolean algebra.

Finally, we show that the absorption and distributivity laws hold for $(B, 0, \wedge, 1, \vee, \neg)$. Note that,

$$
\begin{aligned}
x \wedge (x \vee y) &= x(x + y + xy) \\
&= xx + xy + xxy \\
&= x + xy + xy \\
&= x.
\end{aligned}
$$

Then $x \vee (x \wedge y) = x + xy + xxy = x + xy + xy = x$, and so the absorption law holds.

Furthermore, $x \vee (y \wedge z) = x + yz + xyz$.
And lastly,

$$
\begin{aligned}
(x \vee y) \wedge (x \vee z) &= (x + y + xy)(x + z + xz) \\
&= xx + xz + xxz + xy + yz + yxz + xxy + xyz + xxyz \\
&= x + xz + xz + xy + xy + yz + xyz + xyz + xyz \\
&= x + yz + xyz \\
&= x \vee (y \wedge z).
\end{aligned}
$$

And,

$$\begin{aligned} x \wedge (y \vee z) &= x(y + z + yz) \\ &= xy + xz + xyz \\ &= xy + xz + (xx)yz \\ &= xy + xz + (xy)(xz) \\ &= (x \wedge y) \vee (x \wedge z). \end{aligned}$$

Hence, distributivity laws hold for $\vee$ and $\wedge$. Therefore $G((B, +, 0, \cdot, 1)) = (B, 0, \wedge, 1, \vee, \neg)$ is a Boolean algebra.

Using a similar argument to what was used in the case of F, we see that any morphism $f : A \to B$ in **BoolRing** is a morphism $f : G(A) \to G(B)$ in **Bool**. Again, G preserves identity morphisms and composition and so G is a well-defined functor.

3.: We first note that trivially FG and GF are the identity maps on the morphisms of **Bool** and **BoolRing** respectively. Thus, it is sufficient to show they are the identities for the objects of our categories.

For every object $(B, 0, \vee, 1, \wedge, \neg)$ let us write $(B, +, 0, \cdot, 1)$ for $F((B, 0, \vee, 1, \wedge, \neg))$ and $(B, 0, \vee', 1, \wedge', \neg')$ for $G((B, +, -, 0, \cdot, 1))$. We show that $(B, 0, \vee, 1, \wedge, \neg) = (B, 0, \vee', 1, \wedge', \neg')$.

Note that for all $x, y \in B$
$x \wedge' y = x \cdot y = x \wedge y$.
Hence, $\wedge' = \wedge$.

It follows then that the order on B induced by $\wedge'$ is the same as the order $\leq$ induced by $\wedge$. That is, $x \leq y$ if and only if $x \wedge y = x$. Furthermore, this order induces the same joins and complements in $(B, 0, \vee', 1, \wedge', \neg')$ and $(B, 0, \vee, 1, \wedge, \neg)$. Therefore, $(B, 0, \vee, 1, \wedge, \neg) = (B, 0, \vee', 1, \wedge', \neg')$.

From this we conclude that $GF((B, 0, \vee, 1, \wedge, \neg)) = (B, 0, \vee, 1, \wedge, \neg)$ and so $GF = 1_{\mathbf{Bool}}$.

On the other hand, for every object $(B, +, 0, \cdot, 1)$ in **BoolRing**, let $(B, 0, \vee, 1, \wedge, \neg)$ denote $G((B, +, -, 0, \cdot, 1))$ and let $(B, +', 0, \cdot', 1)$ denote $F((B, 0, \vee, 1, \wedge, \neg))$. We show $(B, +, -, 0, \cdot, 1) = (B, +', -', 0, \cdot', 1)$.

Let $x, y \in B$. Firstly, we have that $x \cdot' y = x \wedge y = x \cdot y$.

Moreover,

$$
\begin{aligned}
x +' y &= (x \wedge \neg y) \vee (y \wedge \neg x) \\
&= (x(1+y)) + (y(1+x)) + (x(1+y))(y(1+x)) \\
&= x + xy + y + yx + (x+xy)(y+yx) \\
&= x + xy + y + yx + xy + xyy + xyx + xyyx \\
&= x + y + xy + xy + xy + xy + xy + xy \\
&= x + y.
\end{aligned}
$$

Thus, $+' = +$.

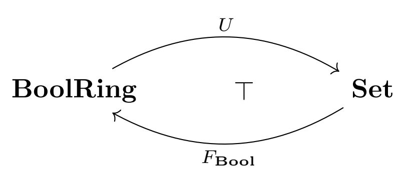
Therefore $(B, +, 0, \cdot, 1) = (B, +', 0, \cdot', 1)$ and it follows that $FG = 1_{\mathbf{BoolRing}}$ and our categories are isomorphic. □

Therefore, we are able to refer to Boolean algebras and rings interchangeably, since each Boolean ring induces a Boolean algebra structure on its underlying set, and each Boolean algebra induces a ring structure on its underlying set.

2.2 Free Boolean Rings

In this section we provide a construction of free Boolean rings, and using this construction, conclude that finitely generated Boolean rings are finite.

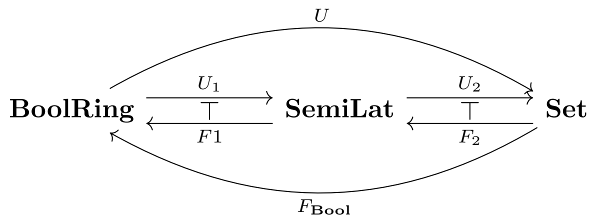
Definition 2.2.1. Consider the adjunction



where U is the forgetful functor. For each set X, we call $F_{\mathbf{Bool}}(X)$ the **free Boolean ring** (equivalently, the **free Boolean algebra**) on X. The functor $F_{\mathbf{Bool}}$ is called the **free functor**.

Lemma 2.2.2. *The adjunction defined above, between* ***BoolRing*** *and* ***Set****, exists.*

Proof. Consider the following,



where **SemiLat** is the category of semilattices. The functor U_2 is the forgetful functor. That is, for each semilattice, $(M, \cdot, 1)$ (where $\cdot$ is our binary operation) $U_2((M, \cdot, 1)) = M$, and $U_2(f) = f$ for any morphism f. Hence, the functor maps each semilattice to its underlying set, and each semilattice homomorphism to itself (but only considered as a function). U_1 is defined by, $U_1((B, +, 0, \cdot, 1)) = (B, \cdot, 1)$ and again $U_1(f) = f$ for any morphism in **BoolRing**. That is, U_1 removes the additive structure of the Boolean ring. We have that $U_2U_1((B, +, 0, \cdot, 1)) = U_2((B, \cdot, 1)) = B$, and $U_2U_1(f) = f$. Hence, $U_2U_1 = U$ is the forgetful functor defined as above.

Then, if we can construct functors F_1 and F_2 as above where $F_1 \dashv U_1$ and $F_2 \dashv U_2$, by the fact that adjunctions compose, we can construct the free functor $F_{\mathbf{Bool}} = F_1F_2 \dashv U_2U_1 = U$, which defines the free Boolean ring over any set X.

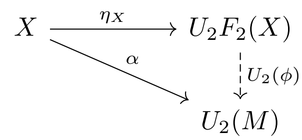
Constructing F_2:

For each set X, we define $F_2(X)$ as the set of finite subsets of X. That is,

$$F_2(X) = \{A \in P(X) \mid A \text{ is finite}\}$$

where our semilattice multiplication is the union of sets. Clearly, $F_2(X)$ is a semilattice with respect to union of sets. From the definition of a powerset as a Boolean algebra, we know $\cup$ is idempotent, associative and commutative. We also have that $\emptyset$ is a finite set and so $\emptyset \in F_2(X)$ for any set X, and since $A \cup \emptyset = A$ for any $A \in P(X)$, our operation $\cup$ has an identity in $F_2(X)$.

Now we show that for each $F_2(X)$ there exists a function $\eta_X : X \to U_2F_2(X)$, such that for each function $\alpha : X \to U_2(M)$ (where M is a semilattice), we have a unique semilattice homomorphism $\phi : F_2(X) \to M$ such that the diagram



commutes. We defined η_X by $\eta_X(x) = \{x\}$ for all $x \in X$. We then define ϕ by $\phi(A) = \alpha(a_1) \cdot \alpha(a_2) \cdot ... \cdot \alpha(a_n)$ for any $A = \{a_1, ..., a_n\} \in F_2(X)$. We write A in this form since it is finite by assumption.

It is clear that ϕ makes the diagram commute since for any $x \in X$, we have $\phi\eta_X(x) = \phi(\{x\}) = \alpha(x)$. Then, note that for $A, B \in F_2(X)$ we have $\phi(A \cup B) = \alpha(x_1)\alpha(x_2)...\alpha(x_k)$ where $\{x_1, ..., x_k\} = A \cup B$. Moreover, $\phi(A) \cdot \phi(B) = \alpha(a_1)...\alpha(a_n)\alpha(b_1)...\alpha(b_m)$ where $A = \{a_1, ..., a_n\}$ and $B = \{b_1, ..., b_m\}$. However, each a_i or b_i is equal to some $x_i \in A \cup B$. Therefore, since multiplication is idempotent, if $a_i = b_j$ for any of the above values, we have that $\alpha(a_i)\alpha(b_j) = \alpha(a_i)$ and thus, if there are "repeated occurrences" of any $\alpha(a_i)$ in the expression $\alpha(a_1)...\alpha(a_n)\alpha(b_1)...\alpha(b_m)$ it has the same value as the same expression without "repeated occurrences". Therefore $\alpha(a_1)...\alpha(a_n)\alpha(b_1)...\alpha(b_m) = \alpha(x_1)...\alpha(x_k)$. Thus, ϕ is a homomorphism.

Lastly, in order to see ϕ is the unique morphism such that the diagram commutes, assume there exists some $\varphi : F_2(X) \to M$ with $\alpha = \varphi\eta_X$. Note that it is sufficient to show that ϕ and φ agree on all singleton sets, since each $A \in F_2(X)$ is a finite union of singleton sets and our homomorphisms preserve finite union. Then, for each singleton subset $\{x\} \in F_2(X)$, we have $\varphi(\{x\}) = \alpha(x) = \phi(\{x\})$ by the assumption that the diagram commutes. Therefore, $\varphi = \phi$ and so ϕ is unique. Hence, $F_2 \dashv U_2$.

Constructing F1:

We define $F_1(M)$, for any semilattice M, as the set of finite subsets of M. That is,

$$F_1(M) = \{A \in P(M) \mid A \text{ is finite}\}$$

where we define addition by $A + B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$. We know that this addition is commutative, associative and that each set is its own inverse, since this definition for addition corresponds with the definition of addition given in 2.1.4 where we define $+$ in terms of the Boolean algebra operations of the usual Boolean powerset algebra.

We then define multiplication as follows. For $A, B \in F_1(M)$, we have that

$$AB = \sum_{a \in A, b \in B} \{a \cdot b\}$$

where $\cdot$ is the semilattice multiplication for M. That is, $AB = \{a_1 \cdot b_1\} + \{a_1 \cdot b_2\} + ... + \{a_1 \cdot b_m\} + \{a_2 \cdot b_1\} + ... + \{a_n \cdot b_m\}$, where $A = \{a_1, ..., a_n\}$ and $B = \{b_1, ..., b_m\}$.

Note here that the commutativity, and associativity of multiplication for $F_1(M)$ follow directly from the fact that our semilattice multiplication is commutative and associative. We also have multiplicative idempotency since,

$$\begin{aligned} AA =& \{a_1a_1\} + \{a_1a_2\} + ... + \{a_1a_n\} + \{a_2a_1\} + ... + \{a_na_n\} \\ &= \{a_1a_1\} + \{a_2a_2\} + ... + \{a_na_n\} + \{a_1a_2\} + \{a_2a_1\} + ... + \{a_{n-1}a_n\} + \{a_na_{n-1}\} \\ &= \{a_1\} + \{a_2\} + ... + \{a_n\} \\ &= \{a_1, ..., a_n\} = A. \end{aligned}$$

Here, our third equality is derived from the fact that multiplication in M is idempotent and commutative and that each $A \in F_1(M)$ is its own additive inverse. We also use the assumption that each a_i is distinct, from our definition of A, in our fourth equality.

The unit for multiplication in this case is the singleton set $\{1_M\}$ where 1_M is the semilattice multiplicative identity for M. Observe that $A\{1_M\} = \sum_{a \in A} \{a \cdot 1_M\} = \sum_{a \in A} \{a\} = A$ for all $A \in F_1(M)$.

Lastly, we show that $F_1(M)$ obeys the distributive properties of Boolean rings. Observe that,

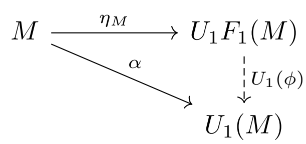
$$AB + AC = \sum_{a \in A, b \in B} \{a \cdot b\} + \sum_{a \in A, c \in C} \{a \cdot c\}$$

for all $A, B, C \in F_1(M)$. However, note that in the above sum, for any $y \in B \cap C$, the term $\{a \cdot y\}$ will appear twice in the above sum for each $a \in A$. Therefore, since each term is its own additive inverse, these terms will cancel, and thus,

$$\sum_{a\in A,b\in B}\{a\cdot b\}+\sum_{a\in A,c\in C}\{a\cdot c\}=\sum_{a\in A,x\in(B\cup C)-(B\cap C)}\{a\cdot x\}$$
$$=\sum_{a\in A,x\in B+C}\{a\cdot x\}=A(B+C).$$

Therefore, $F_1(M)$ is a well-defined Boolean ring.

We then show that, for every semilattice M, there exists a semilattice morphism $\eta_M : M \to U_1F_1(M)$ such that for any semilattice morphism $\alpha : M \to U_1(B)$ where B is a Boolean ring, there exists a unique Boolean ring morphism $\phi : F_1(M) \to B$ such that the diagram



commutes. We define η_M by $\eta_M(x) = \{x\}$ for all $x \in M$. Note that η_M is a semilattice homomorphism, since $\eta_M(xy) = \{xy\} = \{x\}\cdot\{y\} = \eta_M(x)\eta_M(y)$.

We define $\phi : F_1(M) \to B$ as $\phi(A) = \alpha(a_1) + \alpha(a_2) + ... + \alpha(a_n)$ where $A = \{a_1, ..., a_n\}$. It is clear this makes the diagram commute since $\phi\eta_M(x) = \phi(\{x\}) = \alpha(x)$.

In order to see that ϕ is a morphism in **Bool**, consider elements $A, B \in F_1(M)$. Then $\phi(A)+\phi(B) = \alpha(a_1) + ... + \alpha(a_n) + \alpha(b_1) + ...\alpha(b_m)$. But then, if $a_i = b_j$ for any $a_i \in A$ and $b_j \in B$, we obtain that $\alpha(a_i) + \alpha(b_j) = 0_B$. Thus, in the sum $\alpha(a_1) + ... + \alpha(a_n) + \alpha(b_1) + ... + \alpha(b_m)$, our terms cancel whenever any a_i or b_j is in $A \cap B$. And so, $\alpha(a_1) + ... + \alpha(a_n) + \alpha(b_1) + ... + \alpha(b_m) = \alpha(a'_1)+...+\alpha(a'_{n'})+\alpha(b'_1)+...+\alpha(b'_{m'})$ where $\{a'_1, ..., a'_{n'}\} = A-B$ and $\{b'_1, ..., b'_{m'}\} = B-A$. Hence, $\phi(A) + \phi(B) = \alpha(x_1) + ... + \alpha(x_k)$ where $\{x_1, ..., x_k\} = (A \cap -B) \cup (B \cap -A) = A + B$, and thus $\phi(A) + \phi(B) = \phi(A + B)$.

Furthermore, note that
$\phi(A)\phi(B) = (\alpha(a_1) + ... + \alpha(a_n))(\alpha(b_1) + ... + \alpha(b_m))$.

Thus, by the distributive properties of B and the fact that α is a semilattice homomorphism,

$$\begin{aligned}
&(\alpha(a_1) + ... + \alpha(a_n))(\alpha(b_1) + ... + \alpha(b_m)) \\
&= \alpha(a_1b_1) + \alpha(a_1b_2) + ... + \alpha(a_1b_m) + \alpha(a_2b_1) + ... + \alpha(a_nb_m) \\
&= \phi(\{a_1b_1\}) + \phi(\{a_1b_2\}) + ... + \phi(\{a_1b_m\}) + \phi(\{a_2b_1\}) + ... + \phi(\{a_nb_m\}) \\
&= \phi(\{a_1b_1\} + ... + \{a_nb_m\}) \\
&= \phi(\sum_{a\in A, b\in B} \{ab\}) = \phi(AB).
\end{aligned}$$

Therefore ϕ is a Boolean ring morphism.

Lastly, we show that ϕ is the unique morphism that makes the above diagram commute. Assume $\varphi : F_1(M) \to B$ is a Boolean ring morphism such that $\alpha = \varphi\eta_M$. Then, as in the previous case, we need only to prove that ϕ and φ agree on all singleton subsets of M. However, by assumption $\varphi(\{m\}) = \varphi\eta_M(m) = \alpha(m) = \phi(\{m\})$. Therefore $\phi = \varphi$ and $F_1 \dashv U_1$.

Thus, $F_1F_2 \dashv U_2U_1$. Moreover, our free Boolean ring $F_{\mathbf{Bool}}(X)$ is the set of all finite subsets of finite subsets of X. Then, for any $S = \{A_1, ..., A_n\}$ and $T = \{B_1, ..., B_m\}$ in $F_{\mathbf{Bool}}(X)$ our operations are defined by $S \cdot T = \{A_1 \cup B_1\} + \{A_1 \cup B_2\} + ... + \{A_1 \cup B_m\} + \{A_2 \cup B_1\} + ... + \{A_n \cup B_m\}$ and $S + T = (S \cup T) - (S \cap T)$. Moreover, $0 = \emptyset$ and $1 = \{\emptyset\}$ in $F_{\mathbf{Bool}}(X)$. Therefore, we have a well-defined free Boolean ring over any set X. □

Note 2.2.3.

- Note that what we are intuitively doing in the previous proof is taking a set X of "variables" and then constructing all our possible monomials by multiplying variables together, while respecting the idempotency of multiplication. Each finite subset of X represents one of these monomials by telling us which variables "appear" in the monomial. For example, if $X = \{x, y, z\}$ then the monomial "xy" is represented by $\{x, y\}$ in $F_2(X)$.
- Similarly, applying F_1 to the set of our monomials $F_2(X)$ corresponds to constructing every finite sum of these monomials. A set of finite subsets of X then represents a polynomial where each subset is a "term" of the polynomial. Considering $X = \{x, y, z\}$, the sets $\{x, y\}$ and $\{z\}$ represent the monomials "xy" and "z" in $F_2(X)$. Then the set of these sets $\{\{x, y\}, \{z\}\}$ represents the polynomial "$xy + z$" in $F_1F_2(X)$.
- If X is finite, it is clear that the requirement that $A \subseteq X$ is finite is trivially satisfied, and $F_2(X) = P(X)$ and $F_1F_2(X) = PP(X)$.

- The free Boolean ring $F_{\mathbf{Bool}}(X)$ can be considered a Boolean algebra with its operations defined as in Theorem 2.1.4. However, these Boolean algebra operations are not the usual operations for a powerset algebra. For example, $1 = \{\emptyset\}$ in $F_{\mathbf{Bool}}(X)$, which is not the greatest element with respect to the usual subset ordering $\subseteq$.

Corollary 2.2.4. *If X is finite with n elements, then $F(X)$ has 2^{2^n} elements.* □

We say that the free algebra $F_{\mathbf{Bool}}(X)$ is **finitely generated** if X is a finite set. Hence, finitely generated free Boolean algebras are finite.

2.3 Duality of Finite Boolean Algebras and Finite Sets

In this section we show that the category of finite Boolean algebras is dual to the category of finite sets. That is, we show that there exists an equivalence of categories between $\mathbf{Bool_{Fin}}$ and $\mathbf{Set_{Fin}^{Op}}$. In addition to this, we define ultrafilters, and atomic elements of a Boolean algebra, and show how these structures have a one to one correspondence in the case of finite Boolean algebras. We will use this to construct the quasi-inverse of our duality.

Lemma 2.3.1. *There exists a well-defined functor*

$$\mathbf{Set_{Fin}} \xrightarrow{\quad P \quad} \mathbf{Bool_{Fin}^{Op}}$$

Where for any finite set X, $P(X)$ is the powerset of X and is defined as a Boolean algebra with the usual set theoretic operations $(P(X), \cup, \emptyset, \cap, X, -)$, and for any morphism $f : X \to Y$ in $\mathbf{Set_{Fin}}$ we have that $P(f) : P(Y) \to P(X)$ is a morphism in $\mathbf{Bool_{Fin}}$ where $P(f)(S) = f^{-1}(S) = \{x \in X \mid f(x) \in S\}$ for any $S \in P(Y)$.

Proof. For any set X, the powerset algebra $(P(X), \cup, \emptyset, \cap, X, -)$ is a well-known example of a Boolean algebra (for example, see [17] or [9]). Moreover, if X is finite so is $P(X)$. To show that $P(f)$ as above is a Boolean morphism, note that for subsets $U, S \in P(Y)$,

$$\begin{aligned} f^{-1}(U \cup S) &= \{x \in X \mid f(x) \in U \cup S\} = \{x \in X \mid f(x) \in U \text{ or } f(x) \in S\} \\ &= \{x \in X \mid f(x) \in U\} \cup \{x \in X \mid f(x) \in S\} = f^{-1}(U) \cup f^{-1}(S). \end{aligned}$$

And,

$$\begin{aligned} f^{-1}(U \cap S) &= \{x \in X \mid f(x) \in U \cap S\} = \{x \in X \mid f(x) \in U \text{ and } f(x) \in S\} \\ &= \{x \in X \mid f(x) \in U\} \cap \{x \in X \mid f(x) \in S\} = f^{-1}(U) \cap f^{-1}(S). \end{aligned}$$

Moreover, $f^{-1}(\emptyset) = \emptyset$ and $f^{-1}(Y) = X$. Lastly,
$f^{-1}(-S) = \{x \in X \mid f(x) \in -S\} = \{x \in X \mid f(x) \notin S\} = X - f^{-1}(S)$. Hence, $P(f)$ is a Boolean morphism.

Then, note that $1_X^{-1}(S) = \{x \in X \mid 1_X(x) \in S\} = \{x \in X \mid x \in S\} = S$ and if $f : X \to Y$ and $g : Y \to Z$ are morphisms in $\mathbf{Set_{Fin}}$ then, for any $S \in P(Z)$, $P(fg)(S) = (gf)^{-1}(S) = \{x \in X \mid gf(x) \in S\}$ and $P(f)P(g)(S) = f^{-1}(g^{-1}(S)) = \{x \in X \mid f(x) \in g^{-1}(S)\}$. But $f(x) \in g^{-1}(S)$ if and only if $gf(x) \in S$ and so $P(f)P(g)(S) = \{x \in X \mid gf(x) \in S\} = P(fg)(S)$. Therefore, P is a well-defined functor. □

Corollary 2.3.2. *Let $f : X \to Y$ be a bijective function between finite sets. Then there exists an isomorphism of Boolean algebras between $P(X)$ and $P(Y)$, where this isomorphism is the map $\hat{f} : P(X) \to P(Y)$ defined by $\hat{f}(S) = \{f(x) \mid x \in S\}$.*

Proof. If $f : X \to Y$ is a bijection it is an isomorphism in $\mathbf{Set_{Fin}}$ and has an inverse $f^{-1} : Y \to X$. Then by the construction in Lemma 2.3.1, $P(f^{-1}) : P(X) \to P(Y)$ is an isomorphism of Boolean algebras. Note that

$$\begin{aligned} P(f^{-1})(S) &= (f^{-1})^{-1}(S) \\ &= \{y \in Y \mid f^{-1}(y) = x \in S\} \\ &= \{y \in Y \mid y = f(x) \text{ for some } x \in S\} \\ &= \{f(x) \mid x \in S\} = \hat{f}(S). \end{aligned}$$

Therefore $\hat{f} = P(f^{-1})$. □

Before we construct our duality, we need a preliminary definition.

Definition 2.3.3. Let L be a lattice. Then $a \in L$ is called an **atom** of L if $a \neq 0$ and, for any $x \in L$, $x \leq a$ implies that $x = a$ or $x = 0$. The set of atoms on L is denoted $\mathrm{At}(L)$.

Lemma 2.3.4. [9]. *Each finite Boolean algebra B is isomorphic to the powerset $P(At(B))$.*

Proof. We claim that the map $\mu_B : B \to P(\mathrm{At}(B))$ defined by $\mu_B(x) = \{a \in \mathrm{At}(B) \mid a \leq x\}$ is an isomorphism.

We first show that μ_B is surjective. We have that $\mu_B(0) = \{a \in \mathcal{A}(B) \mid a \leq 0\} = \emptyset$. Further, let $S = \{a_1, a_2, \ldots, a_k\}$ be a non-empty subset of $\mathrm{At}(B)$. Then we claim that if $x = \bigvee S$, then $\mu_B(x) = S$.

Clearly $S \subseteq \mu_B(x)$, since $a_i \leq x = \bigvee S$ for all $i \in \{1, \ldots, k\}$. Then, if a is an element of $\mu_B(x)$, we have that $a \leq x = a_1 \vee a_2 \vee \cdots \vee a_k$. Hence, for each a_i, we have that $0 \leq a \wedge a_i \leq a$. Since a is an atom, then either $a \wedge a_i = 0$ for all i, or there exists some j such that $a \wedge a_j = a$. In the first case, we have that $a = a \wedge x = a \wedge (a_1 \vee a_2 \vee \cdots \vee a_k) = (a \wedge a_1) \vee \cdots \vee (a \wedge a_k) = 0$. However, since a is an atom, $a \neq 0$ which is a contradiction. Therefore, there exists some j such that $a \wedge a_j = a$, implying that $a \leq a_j$. Then $a = a_j \in S$ since a_j is an atom. Thus we have $\mu_B(x) \subseteq S$ and so $\mu_B(x) = S$ and μ_B is surjective.

We then note that, for $x, y \in B$, since x is an upper bound of $\mu_B(x)$, $\bigvee \mu_B(x) \leq x$. Now let $b \in B$ be an upper bound of $\mu_B(x)$, and suppose that $x \nleq b$.

Note that for any $x, b \in B$, $x \wedge \neg b = 0$ implies $x \wedge b = (x \wedge b) \vee 0 = (x \wedge b) \vee (x \wedge \neg b) = x \wedge (b \vee \neg b) = x$ which implies $x \leq b$.

Then $x \nleq b$ implies $0 \neq x \wedge \neg b$. Hence, we can choose $a \in \mathrm{At}(B)$ with $a \leq x \wedge \neg b \leq \neg b$ and $a \leq b$, since b is an upper bound of $\mu_B(x)$. But then $a \leq b \wedge \neg b = 0$, which is a contradiction. Therefore, $x \leq b$ and $x = \bigvee \mu_B(x)$. Thus, we have that $\mu_B(x) \subseteq \mu_B(y)$ implies $x = \bigvee \mu_B(x) \leq \bigvee \mu_B(y) = y$. We obtain that $x \leq y$ implies $\mu_B(x) \subseteq \mu_B(y)$, since every element $a \in \mu_B(x)$ is an atom $a \leq x$ and so a is an atom such that $a \leq y$. Hence $a \in \mu_B(y)$, and μ_B is an order isomorphism.

Injectivity follows from the fact that $\mu_B(x) = \mu_B(y)$ if and only if $\mu_B(x) \subseteq \mu_B(y)$ and $\mu_B(y) \subseteq \mu_B(x)$. This is true if and only if $x \leq y$ and $y \leq x$ which is equivalent to $x = y$. ◻

We are now able to construct our duality.

Theorem 2.3.5. *The category $\boldsymbol{Bool_{Fin}}$ is dual to $\boldsymbol{Set_{Fin}}$, with the functor*

$$\boldsymbol{Set_{Fin}} \xrightarrow{\ P\ } \boldsymbol{Bool^{Op}_{Fin}}$$

inducing the desired equivalence.

Proof. It is sufficient to show that P is fully faithful and essentially surjective on objects. We have, directly from Lemma 2.3.4, that each finite Boolean algebra, B, is isomorphic to $P(\mathrm{At}(B))$. Therefore, P is essentially surjective on objects.

Then, consider a Boolean morphism $h : P(Y) \to P(X)$, where X and Y are finite sets. Then, for any subset $S \subseteq Y$, we have,

$$h(S) = h(\bigcup_{s \in S} \{s\}) = \bigcup_{s \in S} h(\{s\})$$

where the second equality follows from the fact that h preserves finite joins. Then, we define $f : X \to Y$ by $f(x) = s$ if and only if $x \in h(\{s\})$. We know that this value is defined for each $x \in X$ since $h(Y) = \bigcup_{y \in Y} h(\{y\}) = X$, as h preserves the greatest element of our algebra. Hence, for any $x \in X$, we have that $x \in h(\{y\})$ for some $y \in Y$. Furthermore, if $f(x) = s$ and $f(x) = s'$ then $x \in h(\{s\}) \cap h(\{s'\}) = h(\{s\} \cap \{s'\})$. For this to be true it is required that $\{s\} \cap \{s'\} \neq \emptyset$ which holds if and only if $s = s'$. Therefore f is a well-defined function.

Moreover, for any $S \in P(Y)$,

$$P(f)(S) = \bigcup_{s \in S} P(f)(\{s\}) = \bigcup_{s \in S} \{x \in X \mid f(x) = s\}.$$

Then, since $f(x) = s$ if and only if $x \in h(\{s\})$, we have $\{x \in X \mid f(x) = s\} = h(\{s\})$ and,

$$\bigcup_{s \in S} \{x \in X \mid f(x) = s\} = \bigcup_{s \in S} h(\{s\}) = h(S).$$

Thus, $P(f) = h$ as desired, and so P is full.

To show that P is faithful, we consider functions g and f

$$X \underset{g}{\overset{f}{\rightrightarrows}} Y$$

such that X and Y are finite and $P(f) = P(g)$. Then, for any $y \in Y$,

$$P(f)(\{y\}) = \{x \in X \mid f(x) = y\} = \{x \in X \mid g(x) = y\} = P(g)(\{y\})$$

and therefore, $f(x) = y$ if and only if $g(x) = y$. That is, for any $x \in X$ where $f(x) = y$, we have that $g(x) = y$. Therefore $f(x) = g(x)$ for each $x \in X$, implying that P is faithful. $\square$

Therefore, the categories $\mathbf{Set_{Fin}}$ and $\mathbf{Bool_{Fin}}$ are dual. We consider the following to construct the quasi-inverse of P.

Definition 2.3.6. [17]**.** Let L be a lattice. A **filter** is a non-empty subset $X \subseteq L$ such that

- If $a \in X$ and $b \in X$, then $a \wedge b \in X$.
- If $b \in X$ then, whenever $b \leq a$, we have $a \in X$.

Lemma 2.3.7. *If L is a lattice and $A \subseteq L$, then the smallest filter containing A is the set $F_A = \{x \in L \mid a_1 \wedge ... \wedge a_n \leq x$ for some $a_1, ..., a_n \in A\}$.*

Proof. If $x \in F_A$ and $x \leq y$, then $a_1 \wedge ... \wedge a_n \leq x \leq y$ for some $a_1, ..., a_n \in A$. If $x, y \in A$, then $a_1 \wedge ... \wedge a_n \leq x$ and $a'_1 \wedge ...a'_m \leq y$ and so $a_1 \wedge ...a_n \wedge a'_1 \wedge ... \wedge a'_m \leq x \wedge y$. Hence $x \wedge y \in F_A$ and F_A is a filter. Then, if F is a filter containing A, we must have that $a_1 \wedge ... \wedge a_n \in F$ for all $a_1, ..., a_n \in A$, and if $a_1 \wedge ... \wedge a_n \leq x$, then $x \in F$. Hence $F_A \subseteq F$. □

In particular, the smallest filter containing $\emptyset$ is equal to $\{1\}$, since it only contains the empty meet $\bigwedge \emptyset = 1$.

Corollary 2.3.8. [16]**.** *Let L be a lattice, F be a filter on L and consider $y \in L$. Then, the smallest filter containing $F \cup \{y\}$ is $F' = \{x \in L \mid a \wedge y \leq x$ for some $a \in F\}$.*

Proof. Clearly, if $x \in F'$ and $x \leq x'$ then $x' \in F'$. Then if $x, x' \in F$ we have that, for $a, a' \in F$, $a \wedge y \leq x$ and $a' \wedge y \leq x'$ and therefore $(a \wedge a') \wedge y \leq x \wedge x'$. Since $a \wedge a' \in F$, then $x \wedge x' \in F'$. Thus F' is a filter and so $\{x \in L \mid a_1 \wedge ... \wedge a_n \leq x$ for some $a_1, ..., a_n \in F \cup \{y\}\} \subseteq F'$ by our previous lemma. Then if $x \in F'$ we have that $y \wedge a \leq x$ for some $a \in F$, and clearly $x \in \{x \in L \mid a_1 \wedge ... \wedge a_n \leq x$ for some $a_1, ..., a_n \in F \cup \{y\}\}$. Thus $F' = \{x \in L \mid a_1 \wedge ... \wedge a_n \leq x$ for some $a_1, ..., a_n \in F \cup \{y\}\}$. □

Definition 2.3.9. Let B be a Boolean algebra. Then the binary operations $\Rightarrow$ and $\Leftrightarrow$ are defined on B by

$$x \Rightarrow y = \neg x \vee y \text{ and } x \Leftrightarrow y = (x \Rightarrow y) \wedge (y \Rightarrow x)$$

Lemma 2.3.10. *Let B be a Boolean algebra and F be a subset of B. Then the following conditions are equivalent,*

a. F is a filter.

b. The set $E = \{(x, y) \in B \times B \mid x \Leftrightarrow y \in F\}$ is a congruence. That is, E is a subalgebra of $B \times B$.

c. There exists a Boolean algebra homomorphism $f : B \to C$ to some Boolean algebra C such that $F = \{x \in B \mid f(x) = 1\}$.

Proof. *a.⇒b.:*

We first show that E defined above is an equivalence relation. We have that $x \Leftrightarrow x = 1$ and $1 \in F$, for any filter F. Hence, $(x, x) \in E$ and so E is reflexive. Then note that $x \Leftrightarrow y = y \Leftrightarrow x$ for all $x, y \in B$. Hence, if $x \Leftrightarrow y \in F$, then $y \Leftrightarrow x \in F$. Thus E is symmetric. Then suppose that $(x, y), (y, z) \in E$. Then $x \Leftrightarrow y, y \Leftrightarrow z \in F$ and for $x, y \in B$ we have,

$$x \Leftrightarrow y = (\neg x \vee y) \wedge (\neg y \vee x) = (\neg x \wedge \neg y) \vee (\neg x \wedge x) \vee (y \wedge x) \vee (\neg y \wedge y) = (\neg x \wedge \neg y) \vee (x \wedge y).$$

Then, if $x \Leftrightarrow y, y \Leftrightarrow z \in F$, we have that $(x \Leftrightarrow y) \wedge (y \Leftrightarrow z) \in F$. Note,

$$\begin{aligned}(x \Leftrightarrow y) \wedge (y \Leftrightarrow z) &= ((\neg x \wedge \neg y) \vee (x \wedge y)) \wedge ((\neg y \wedge \neg z) \vee (y \wedge z)) \\ &= (\neg x \wedge \neg y \wedge \neg y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge y \wedge z) \vee (x \wedge y \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge y \wedge z) \\ &= (\neg x \wedge \neg y \wedge \neg z) \vee 0 \vee 0 \vee (x \wedge y \wedge z) = (\neg x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge z) \\ &\leq (\neg x \wedge \neg z) \vee (x \wedge z) = x \Leftrightarrow z.\end{aligned}$$

And since F is up-closed, it follows that $x \Leftrightarrow z \in F$ and E is transitive.

Now we show that E is closed under Boolean algebra operations for $B \times B$. That is, we must show that if $x \Leftrightarrow y \in F$ and $p \Leftrightarrow q \in F$, then $(x \wedge p) \Leftrightarrow (y \wedge q), (x \vee p) \Leftrightarrow (y \vee q), \neg x \Leftrightarrow \neg y \in F$.

Note that, if $x \Leftrightarrow y = (\neg x \vee y) \wedge (\neg y \vee x)$ and $p \Leftrightarrow q = (\neg p \vee q) \wedge (\neg q \vee p)$ are in F, then $(\neg x \vee y), (\neg y \vee x)(\neg p \vee q), (\neg q \vee p) \in F$, since F is up-closed. Moreover,

$$\begin{aligned}(x \wedge p) \Leftrightarrow (y \wedge q) &= (\neg(x \wedge p) \vee (y \wedge q)) \wedge (\neg(y \wedge q) \vee (x \wedge p)) \\ &= (\neg x \vee \neg p \vee (y \wedge q)) \wedge (\neg y \vee \neg q \vee (x \wedge p)) \\ &= (\neg x \vee \neg p \vee y) \wedge (\neg x \vee \neg p \vee q) \wedge (\neg y \vee \neg q \vee x) \wedge (\neg y \vee \neg p \vee q).\end{aligned}$$

We also have that $(\neg x \vee y) \leq (\neg x \vee \neg p \vee y)$, $(\neg p \vee q) \leq (\neg x \vee \neg p \vee q)$, $(\neg y \vee x) \leq (\neg y \vee \neg q \vee x)$ and $(\neg p \vee q) \leq (\neg y \vee \neg p \vee q)$. It follows from the definition of F that $(\neg x \vee \neg p \vee y), (\neg x \vee \neg p \vee q), (\neg y \vee \neg q \vee x), (\neg y \vee \neg p \vee q) \in F$. Then, since F is closed under $\wedge$, we have $(x \wedge p) \Leftrightarrow (y \wedge q) = (\neg x \vee \neg p \vee y) \wedge (\neg x \vee \neg p \vee q) \wedge (\neg y \vee \neg q \vee x) \wedge (\neg y \vee \neg p \vee q) \in F$.

Using similar methods, we are able to show that,

$$(x \vee p) \Leftrightarrow (y \vee q) = (x \vee p \vee \neg y) \wedge (x \vee p \vee \neg q) \wedge (\neg x \vee y \vee q) \wedge (\neg p \vee y \vee q).$$

Then, using the same methods as for the previous expression we can show that, if $(x \Leftrightarrow y), (p \Leftrightarrow q) \in F$, then the above formula is an element of F.

Lastly, we have $\neg x \Leftrightarrow \neg y = (\neg\neg x \vee \neg y) \wedge (\neg\neg y \vee \neg x) = (x \vee \neg y) \wedge (y \vee \neg x) = x \Leftrightarrow y$ and so $\neg x \Leftrightarrow \neg y \in F$.

b.⇒c.:
Since E is a congruence we consider $f : B \to B/E$ where $f(x) = [x] = \{y \in B \mid (x, y) \in E\}$ for all $x \in B$. Then $f(x) = [1]$, if and only if $(1, x) \in E$. This is true if and only if $1 \Leftrightarrow x \in F$. But we can see that $1 \Leftrightarrow x = (0 \vee x) \wedge (\neg x \vee 1) = x \wedge 1 = x$. Combining the above, we get that $f(x) = [1]$ if and only if $x \in F$ and so $F = \{x \in B \mid f(x) = [1]\}$.

c.⇒a.:
If such a morphism $f : B \to C$ exists then, when $x, y \in F$, we obtain $f(x \wedge y) = f(x) \wedge f(y) = 1 \wedge 1 = 1$. Therefore $x \wedge y \in F$. Moreover, if $x \in F$ and $x \leq y$ then $1 = f(x) \leq f(y)$ and so $f(y) = 1$. Thus, $y \in F$ and it follows that F is a filter. □

Definition 2.3.11. Let L be a lattice. $X \subseteq L$ is an **ultrafilter** of L if X is a maximal non-trivial filter. That is, X is a filter of L such that $X \neq L$ and for any other filter $X' \neq L$ we have that $X \subseteq X'$ implies that $X = X'$.

Note 2.3.12. No proper filter of L contains 0, since if $0 \in U$, then $0 \leq x$ for every $x \in L$ and thus $U = L$.

Definition 2.3.13. A **principal filter** is a filter of the form $F_a = \{x \in L \mid a \leq x\}$. If a principal filter is maximal it is called a **principal ultrafilter**.

Note 2.3.14. We can see that any such subset is a filter since:

- If $x \in F_a$ and $x \leq y$, then $a \leq x \leq y$ so $y \in F_a$.
- If $x, y \in F_a$, we have that $a \leq x \wedge y$ by the order-theoretic definition of $\wedge$ and so $x \wedge y \in F_a$.

Lemma 2.3.15. *In a lattice L, a principal filter F_x is an ultrafilter if and only if x is an atom.*

Proof. Suppose F_x is an ultrafilter. Then, $x \neq 0$ since F_x is a proper filter. Then suppose $a \in L$ such that $0 < a \leq x$. Since $a \leq x \leq y$ for every $y \in F_x$, we must have that $F_x \subseteq F_a$. Moreover, F_a is a proper filter, and thus by assumption $F_x = F_a$. Therefore, $x \leq a$, implying that $a = x$. Hence, x is an atom.

Conversely, assume that x is an atom. Then F_x is a proper filter, since $x \neq 0$. Now assume $F_x \subseteq U$ for some filter U of L, such that there is some $u \in U$ with $u \notin F_x$. Then $u \neq x$ and we must have $0 \leq u \wedge x \leq x$. But in this case, since x is an atom, either $u \wedge x = x$ or $u \wedge x = 0$. If $u \wedge x = x$, then $x \leq u$ which contradicts the assumption that $u \notin F_x$. Therefore $u \wedge x = 0$ and so $0 \in U$, and it follows that U is not a proper filter. Hence, F_x is a maximal proper filter. □

Lemma 2.3.16. *In a finite lattice L, each ultrafilter U contains exactly one atom of L.*

Proof. We first prove that if U is an ultrafilter, then it cannot contain more than one distinct atom. If $x, y \in U$ are atoms, then $x \wedge y \in U$ by the fact that U is a filter. But then $0 \leq x \wedge y \leq x$. But since x is an atom either $x = x \wedge y$ or $x \wedge y = 0$. By our assumption U is a proper filter, and so $0 \notin U$, and $x \wedge y = x$. By a similar argument, $x \wedge y = y$ and therefore $x = x \wedge y = y$. Hence, any two atoms in U are equal.

Now we show that if a filter contains no atoms, it cannot be maximal. Suppose U has no atoms. Since L is finite, then U is also finite and $\bigwedge U \in U$ is a well-defined element. But, by assumption, $\bigwedge U$ is not an atom. Thus, there exists some $x \neq \bigwedge U$ such that $0 < x \leq \bigwedge U$. But then, for any $u \in U$, we have that $x \leq \bigwedge U \leq u$. Therefore $U \subseteq F_x$ and $x \notin U$. But since F_x is a filter, then U is not maximal. Then if U is maximal, it must contain an atom. Therefore, each ultrafilter of L must contain exactly one atom of L. □

Corollary 2.3.17. *For a finite lattice L, let $At(L)$ be the set of atoms of L, and $UFil(L)$ be the set of ultrafilters on L. Then:*

a. *Every $U \in UFil(L)$ is of the form $U = F_x$ for some $x \in At(L)$.*

b. *There exists a bijection between $At(L)$ and $UFil(L)$.*

Proof.

a. If U is an ultrafilter of L, by Lemma 2.3.16, U contains a unique atom a. By Lemma 2.3.15, F_a is an ultrafilter. Then, since U is up-closed, if $x \in F_a$, then $a \leq x$ and $x \in U$. Thus $F_a \subseteq U$, and since F_a is maximal, $F_a = U$.

b. We define $\gamma_L : \mathrm{UFil}(L) \to \mathrm{At}(L)$ by $\gamma_L(F_a) = a$. By part 1 of this proof, this defines γ_L for each $U \in \mathrm{UFil}(L)$. Clearly γ_L is surjective since $F_{a'}$ exists for each $a' \in \mathrm{At}(L)$. γ_L is also injective, since if U and V are ultrafilters such that $\gamma_L(U) = a$ and $\gamma_L(V) = a$, then $U = F_a = V$.

□

This allows us to characterize ultrafilters in a finite lattice, and show that each ultrafilter is uniquely determined by an atomic element of the lattice. Another result, which we use later in this chapter concerns the fact that any filter of a lattice is contained in some ultrafilter. It is worth noting that the proof of this lemma relies on Zorn's Lemma.

Lemma 2.3.18. [9]. *Let L be a lattice. Then, if F is a proper filter of L, it is contained in some ultrafilter of L.*

Proof. Consider the ordered set $(\mathrm{Fil}(L), \subseteq)$, where $\mathrm{Fil}(L)$ is the set of all filters on L. This ordered set is clearly bounded above since $L \in \mathrm{Fil}(L)$ contains every filter on L.

Now for a proper filter F, consider the set $\mathcal{G} = \{G \in \mathrm{Fil}(L) \mid F \subseteq G \text{ and } G \neq L\}$. This set is non-empty since $F \in \mathcal{G}$. Consider a non-empty chain $\mathcal{C}$ such that $\mathcal{C} \subseteq \mathcal{G}$. We note that if $C = \bigcup_{C_i \in \mathscr{C}} \{C_i\}$ then, since $F \subseteq C_i$ for each C_i, we have $F \subseteq C$. Note that $C \neq L$ since if $C = L$ we must have $0 \in C$, and so $0 \in C_i$ for some $C_i \in \mathcal{C}$. Thus, since each C_i is a proper filter, no C_i contains 0, and therefore $0 \notin C$. Moreover, if $x \in C$ and $x \leq y$, we must have $x \in C_i$. Since C_i is up-closed then $y \in C_i$ and so $y \in C$. If $x, y \in C$ we must have that $x \in C_i$ and $y \in C_j$ where $C_i, C_j \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, we can then assume that $C_i \subseteq C_j$ without loss of generality. Therefore $x, y \in C_j$ and so $x \wedge y \in C_j$ which gives us that $x \wedge y \in C$ and thus C is a filter. This allows us to conclude that C is an element of $\mathcal{G}$ for any non-empty chain $\mathcal{C}$ of $\mathcal{G}$.

Therefore, we can apply Zorn's Lemma to $\mathcal{G}$, which states that $\mathcal{G}$ contains a maximal element U. Then U is a maximal proper filter which contains F. □

Corollary 2.3.19. *Let L be a lattice. Then for every $x \in L$ there exists an ultrafilter such that $x \in L$.*

Proof. Simply apply Lemma 2.3.18 to the principal filter F_x. □

Lemma 2.3.20. [17]. *A subset X of a Boolean Algebra B is an ultrafilter if and only if it contains exactly one element of the set $\{a, \neg a\}$ for any $a \in B$.*

Proof. Suppose $X \subseteq B$ is an ultrafilter. Then $0 \notin X$, and since $0 = a \wedge \neg a$, we cannot have both $a \in X$ and $\neg a \in X$, since X is closed under $\wedge$. So at most X contains one element of $\{a, \neg a\}$.

Suppose $X \cap \{a, \neg a\} = \emptyset$. Then $X \cup \{a\}$ is a proper subset of B. Furthermore, we can consider the filter $X' = \{c \mid a \wedge x \leq c \text{ for some } x \in X\}$ by Corollary 2.3.8. However, note that then X is not maximal since $X \subset X'$, $X \neq X'$ and $X' \neq B$, since $\neg a \notin X'$. Therefore, in order for X to be maximal, it must contain one element of $\{a, \neg a\}$.

Conversely, suppose that X contains one element of each set of the form $\{a, \neg a\}$ in B. Clearly, X is a proper subset of B. Moreover, if $x \in X$ and $x \leq y$, then $\neg y \leq \neg x$. Then since $\neg x \notin X$, it follows that $\neg y \notin X$ and thus $y \in X$. Moreover, if $x, y \in X$, and $\neg(x \wedge y) \in X$, then $x \wedge \neg y = x \wedge (\neg x \vee \neg y) = \neg(x \wedge y) \in X$. This implies that $\neg y \in X$ which is a contradiction. Therefore, if $x, y \in X$ then $x \wedge y \in X$ and so X is a filter. Suppose $X \subseteq X'$ for some filter X', then either $X' = X$ or $\neg a \in X'$ for some $a \in X$. In the second case, since X' is a filter, we get $0 = a \wedge \neg a \in X'$ and so $X' = B$. Hence, X is a maximal proper filter on B. □

Lemma 2.3.21. *For a Boolean algebra B let UFil(B) be the set of ultrafilters of B. Then the set UFil(B) is isomorphic to hom$(B, \{0,1\})$, the set of morphisms from B to $\{0,1\}$ in **Bool**.*

Proof. We define isomorphisms between our sets,

$$\mathrm{UFil}(B) \underset{\psi_B}{\overset{\phi_B}{\rightleftarrows}} \mathrm{hom}(B, \{0,1\})$$

as follows. For each ultrafilter $X \subseteq B$ we define $\phi_B(X)$ as the map such that $\phi_B(X)(b) = 1$ if $b \in X$ and $\phi_B(X)(b) = 0$ otherwise. To see this is a well-defined homomorphism note the following.

$\phi_B(X)(0) = 0$ since 0 is not an element of any ultrafilter.
$\phi_B(X)(1) = 1$ since X is up-closed and non-empty.
$\phi_B(X)(a \wedge b) = 1$ if and only if $a \wedge b$ is in X, which is true if and only if $a, b \in X$. That is, $\phi_B(X)(a \wedge b) = 1$ if and only if $\phi_B(X)(a) = 1$ and $\phi(X)(a) = 1$.
$\phi_B(X)(a \vee b) = 0$ if and only if $a \vee b$ is not in X, which is true if and only if neither a or b is in X. That is, $\phi_B(X)(a \vee b) = 0$ if and only if $\phi_B(X)(a) = 0$ and $\phi_B(X)(a) = 0$. Thus $\phi_B(X)(a \vee b) = \phi_B(X)(a) \vee \phi_B(X)(b)$.
Lastly, $\phi_B(X)(b) = 1$ if and only if $b \in X$ which is true if and only if $\phi_B(X)(\neg b) = 0$ by Lemma 2.3.20. Hence $\phi_B(X)(\neg b) = \neg\phi_B(X)(b)$ and ϕ is a homomorphism.

We then define $\psi(f)$, for each $f \in \mathrm{hom}(B, \{0,1\})$, by $\psi_B(f) = f^{-1}(\{1\}) = \{b \in B \mid f(b) = 1\}$. This is well-defined, since for each set $\{a, \neg a\}$ we must either have $f(a) = 1$ and $f(\neg a) = \neg f(a) = 0$ or $f(a) = 0$ and $f(\neg a) = \neg f(a) = 1$. Thus $\psi(f)$ contains exactly one element of each set $\{a, \neg a\}$, and so $\psi_B(f)$ is an ultrafilter.

In order to see these are isomorphisms note that for each ultrafilter X, we have that $\psi_B\phi_B(X) = \{b \in B \mid \phi(X)(b) = 1\} = \{b \in B \mid b \in X\} = X$. On the other hand, $\phi_B\psi_B(f)(b) = 1$ if and only if b is in

$\psi_B(f)$. But b is in $\psi_B(f)$ if and only if $f(b) = 1$ and so $\phi_B\psi_B(f)(b) = 1$ is equivalent to $f(b) = 1$. Hence, $f = \phi_B\psi_B(f)$ and our constructed maps are isomorphisms. □

Corollary 2.3.22. *In a finite Boolean algebra B, the sets $At(B)$, $UFil(B)$ and $hom(B, \{0, 1\})$ are bijective.* □

Using our previous results, and the fact that $P : \mathbf{Set} \to \mathbf{Bool}^{Op}$ is a functor, we obtain the following result.

Corollary 2.3.23. *For a finite Boolean algebra B, the following holds (where "≅" denotes isomorphic).*

$$B \cong P(At(B)) \cong P(UFil(B)) \cong P(hom(B, \{0, 1\}))$$

Proof. By Lemma 2.3.4 $\mu_B : B \to P(\mathrm{At}(B))$ is an isomorphism. By Corollary 2.3.22 we have that $\mathrm{At}(B)$, UFil(B) and $\mathrm{hom}(B, \{0, 1\})$ are all bijective. Then by Corollary 2.3.2 we know that the powersets of all three of these sets are isomorphic to each other, and by the transitive property of isomorphisms, all three are isomorphic to B. □

Note 2.3.24. To compute the above isomorphisms, note that $\phi_B\gamma_B^{-1} : \mathrm{At}(B) \to \mathrm{hom}(B, \{0, 1\})$ is the desired map (using the maps in Lemmas 2.3.16 and 2.3.22), and then if we let $\tau_B = \phi_B\gamma_B^{-1}$, using the notation from Corollary 2.3.2, $\hat{\tau}_B$ is the isomorphism between the powersets of $\mathrm{At}(B)$ and $\mathrm{hom}(B, \{0, 1\})$. That is, for $b \in B$, we have that $\hat{\tau}_B\mu_B(b)$ is the set of homomorphisms f such that each f corresponds to an ultrafilter F_a, where a is an atom of B which is smaller than b. And so, if $f \in \hat{\tau}_B\mu_B(b)$ then $f(x) = 1$ for every $x \in F_a$ for some atom a with $a \leq b$. But then for every $f \in \hat{\tau}_B\mu_B(b)$, we have $f(b) = 1$.

On the other hand, if $f : B \to \{0, 1\}$ is a homomorphism such that $f(b) = 1$ it corresponds to an ultrafilter U such that b is an element of U. But then $U = F_a$ for an atom $a \in B$, and so b is an element of F_a, such that $a \leq b$. And so, f corresponds to such an F_a and is hence in $\hat{\tau}_B\mu_B(b)$. Explicitly, this gives us:

$$\hat{\tau}_B\mu_B(b) = \{f \in \mathrm{hom}(B, \{0, 1\}) \mid f(b) = 1\}$$

We also compute the inverse as follows. If $M \subseteq \mathrm{hom}(B, \{0, 1\})$ then $\hat{\tau}_B^{-1}(M) = \{a \in \mathrm{At}(B) \mid f(a) = 1 \text{ for some } f \in M\}$. Moreover, for $A \subseteq \mathrm{At}(B)$, $\mu_B^{-1}(A) = \bigvee A$. Hence,

$$\mu_B^{-1}\hat{\tau}_B^{-1}(M) = \bigvee\{a \in \mathrm{At}(B) \mid f(a) = 1 \text{ for some } f \in M\}$$

for all $M \subseteq \hom(B, \{0,1\})$. Using this construction, we can describe the quasi-inverse to our duality.

Theorem 2.3.25. *The quasi-inverse to P in Theorem 2.3.5 is the hom-functor*

$$hom(-, \{0,1\}) : \boldsymbol{Bool_{Fin}} \to \boldsymbol{Set_{Fin}^{Op}}$$

Proof. Following the method in [13], we can define the quasi-inverse to P, called G, on objects to P by considering $G(B)$ to be equal to some object in **Set** such that $PG(B) \cong B$. We choose $\hom(B, \{0,1\})$, since the image of $\hom(B, \{0,1\})$ under P is isomorphic to B. Then our natural transformation is induced by the isomorphism $\alpha_B : B \to P(\hom(B, \{0,1\}))$ defined by $\alpha_B = \hat{\tau}_B \mu_B$ as in Corollary 2.3.23. Lastly, for a Boolean morphism $f : B \to B'$ we define $G(f) : \hom(B', \{0,1\}) \to \hom(B, \{0,1\})$ as the unique morphism such that $PG(f) = \alpha_{B'} f \alpha_B^{-1}$. We then only need to show the mapping $G(f) = \hom(f, \{0,1\})$ defined by $m \mapsto mf$ satisfies the above equality.

Recall that for $M \subseteq \hom(B, \{0,1\})$

$$\alpha_B^{-1}(M) = \bigvee \{a \in \text{At}(B) \mid m(a) = 1 \text{ for some } m \in M\} = a_1 \vee a_2 \vee ... \vee a_n$$

Where for each a_i there is a unique $m \in M$ such that $m(a_i) = 1$. Then,

$$\alpha_{B'} f(a_1 \vee ... \vee a_n) = \{m' \in \hom(B', \{0,1\}) \mid m' f(a_1 \vee ... \vee a_n) = 1\}$$

Note that $m'f(a_1 \vee ... \vee a_n) = m'f(a_1) \vee ... \vee m'f(a_n) = 1$ if and only if $m'f(a_i) = 1$ for some $i \in \{1, ..., n\}$. But then, since such a morphism is unique for each a_i, then $m'f(a_i) = 1$ is equivalent to saying that $m'f = m$ for the morphism $m \in M$ such that $m(a_i) = 1$. Hence, $m'f(a_1 \vee ... \vee a_n) = 1$ if and only if $m'f \in M$. However, on the other hand we have that,

$$P(\hom(f, \{0,1\}))(M) = \{m' \in \hom(B', \{0,1\}) \mid m'f \in M\}$$

and so $P(\hom(f, \{0,1\})) = \alpha_{B'} f \alpha_B^{-1}$ and we are done. □

Corollary 2.3.26. *We can induce isomorphic functors to hom$(-, \{0,1\})$, called UFil$(-)$ and At$(-)$ which map each finite Boolean algebra to the set of its ultrafilters and atomic elements respectively. In particular, the map UFil$(-)$ maps each $f : B \to C$ to the preimage map $f^{-1}(-) :$ UFil$(C) \to$ UFil(B).*

Proof. We first construct the natural isomorphism $\psi : \hom(-, \{0,1\}) \cong \text{UFil}(-)$. Note here that in order to do this we must have that for each $f : B \to C$, UFil(f) is the unique function such that the diagram

$$\begin{array}{ccc}
\mathrm{UFil}(C) & \overset{\mathrm{UFil}(f)}{\dashrightarrow} & \mathrm{UFil}(B) \\
\big\downarrow \phi_C & & \psi_B \big\uparrow \\
\hom(C, \{0,1\}) & \xrightarrow{\hom(f,\{0,1\})} & \hom(B, \{0,1\})
\end{array}$$

commutes. That is, for $U \in \mathrm{UFil}(C)$, we have that $\mathrm{UFil}(f)(U) = \psi_B \hom(f, \{0,1\}\phi_C(U) = (m_U f)^{-1}(\{1\})$, where $m_U : C \to \{0,1\}$ is defined by $m_U(y) = 1$ if and only if $y \in U$. Then,

$$(m_U f)^{-1}(\{1\}) = \{x \in B \mid m_U f(x) = 1\} = \{x \in B \mid f(x) \in U\}$$

and therefore $\mathrm{UFil}(f)(U) = f^{-1}(U)$.

Applying the same method to obtain $\gamma : \mathrm{UFil}(-) \cong \mathrm{At}(-)$ we have that the bijection $\gamma_C : \mathrm{UFil}(C) \to \mathrm{At}(C)$ is given by $\gamma(U) = \bigwedge U$, and that its inverse is defined by $\gamma_C^{-1}(a) = F_a$. Then, in order to make the diagram

$$\begin{array}{ccc}
\mathrm{At}(C) & \overset{\mathrm{At}(f)}{\dashrightarrow} & \mathrm{At}(B) \\
\big\downarrow \gamma_C^{-1} & & \gamma_B \big\uparrow \\
\mathrm{UFil}(C) & \xrightarrow{\mathrm{UFil}(f)} & \mathrm{UFil}(B)
\end{array}$$

commute, for each $f : B \to C$ in $\mathbf{Bool_{Fin}}$ we define $\mathrm{At}(f)(a) = \gamma_B \mathrm{UFil}(U)\gamma_C^{-1}(a) = \bigwedge f^{-1}(F_a)$a, and thus we compute

$$\bigwedge f^{-1}(F_a) = \bigwedge\{x \in B \mid f(x) \in F_a\} = \bigwedge\{x \in B \mid a \leq f(x)\}.$$

This allows us to construct three isomorphic quasi-inverses to $P : \mathbf{Set_{Fin}} \to \mathbf{Bool_{Fin}^{\mathit{Op}}}$, given by $\hom(-, \{0,1\}) \cong \mathrm{UFil}(-) \cong \mathrm{At}(-)$. □

In this chapter, we use this duality to construct algorithms that decide whether a logical formula is a theorem or not in a given theory of classical propositional logic. However, we first consider some preliminary results on Galois connections.

2.4 Galois Connections

Definition 2.4.1. [13]**.** Let $(P, \leq)$ and $(Q, \leq)$ be sets equipped with partial orders. Then a **Galois connection** is a pair of functions,

$$P \rightleftarrows Q$$

both written $x \mapsto x^*$ for an element x of P or Q, such that when $x, y \in P$ or $x, y \in Q$ we have

1. $x \leq y$ implies that $y^* \leq x^*$
2. $x \leq x^{**}$

Lemma 2.4.2. *The maps in a Galois connection between $(P, \leq)$ and $(Q, \leq)$ can be viewed as an adjunction between $(P, \leq)$ and $(Q, \leq)^{Op}$ where our posets are considered as categories.*

Proof. Recall that an adjunction between two ordered sets P and Q is a pair of functors $(F : P \to Q, U : Q \to P)$ such that $x \leq U(y)$ if and only if $F(x) \leq y$. In our case, since the order in Q is reversed, this becomes a pair of order reversing maps from P to Q and Q to P such that $x \leq y^*$ if and only if $y \leq x^*$ where either $x \in P$ and $y \in Q$, or $y \in P$ and $x \in Q$.

We already have from 1. in our definition that each map in the Galois connection is a contravariant functor, since they are both order-reversing. Now note that $x \leq y^*$ implies that $y^{**} \leq x^*$ from 1. and $y \leq y^{**}$ by 2. Hence $y \leq x^*$. We can also prove $y \leq x^*$ implies $x \leq y^*$ using the same method. □

Lemma 2.4.3. *For a Galois connection between $(P, \leq)$ and $(Q, \leq)$ we have that $x^{***} = x^*$, and therefore $x \mapsto x^{**}$ is a closure operation when considered on P or Q.*

Proof. We have that $x^* \leq x^{***}$ by 2., where we substitute x^* for x. By 2. once more, we obtain $x \leq x^{**}$, which by 1. implies that $x^{***} \leq x^*$. Hence, $x^* = x^{***}$. We then have that $x \mapsto x^{**}$ is a closure operator since:

a. $x \leq x^{**}$ by 2.

b. $x \leq y$ implies $y^* \leq x^*$, which implies $x^{**} \leq y^{**}$ by applying 1. twice.

c. $x^{****} = (x^*)^{***} = (x^*)^* = x^{**}$ from our result above.

□

Lemma 2.4.4. *For a Galois connection between $(P, \leq)$ and $(Q, \leq)$, where P or Q have binary meets and joins, we have that $(x \vee y)^* = x^* \wedge y^*$.*

Proof. Since $x \leq x \vee y$ and $y \leq x \vee y$ we obtain $(x \vee y)^* \leq x^*$ and $(x \vee y)^* \leq y^*$ by applying Galois connection property 1.. Consider an element c such that $c \leq x^*$ and $c \leq y^*$. Then, $x \leq x^{**} \leq c^*$ and $y \leq y^{**} \leq c^*$ from properties 1. and 2. and it follows that $x \vee y \leq c^*$. Lastly, by applying 1. and 2. once again, $c \leq c^{**} \leq (x \vee y)^*$. That is, $(x \vee y)^*$ is the greatest lower bound of $\{x^*, y^*\}$, and so $(x \vee y)^* = x^* \wedge y^*$. □

Lemma 2.4.5. *A Galois connection between a lattice P and an ordered set Q induces a lattice on $P^{**} = \{x^{**} \mid x \in P\}$ ordered by the same order as P, where we define the meet $\curlywedge$ and join $\curlyvee$ operations on P^{**} by*

$$x^{**} \curlyvee y^{**} = (x \vee y)^{**} \text{ and } x^{**} \curlywedge y^{**} = x^{**} \wedge y^{**}$$

where $\vee$ and $\wedge$ are the lattice operations on P. The least and greatest elements of P^{**} are given by 0^{**} and 1 respectively.

Proof. First we note that since $x, y \leq x \vee y$ then $x^{**}, y^{**} \leq (x \vee y)^{**}$. Now note that since $x \leq x^{**}, y \leq y^{**}$, we get that $x \vee y \leq x^{**} \vee y^{**}$. Then if $x^{**}, y^{**} \leq a^{**}$ for some $a \in P$, we get that $x \vee y \leq x^{**} \vee y^{**} \leq a^{**}$ and so $(x \vee y)^{**} \leq a^{****} = a^{**}$, hence $x^{**} \curlyvee y^{**}$ is the supremum of x^{**} and y^{**} in P^{**}.

It is clear that if $x^{**} \wedge y^{**}$ is in P^{**}, it is the infimum of x^{**} and y^{**}. Then note that $x^{**} \wedge y^{**} \leq (x^{**} \wedge y^{**})^{**}$ but then, since $x^{**} \wedge y^{**} \leq x^{**}, y^{**}$ we have that $(x^{**} \wedge y^{**})^{**} \leq x^{****} = x^{**}$ and $(x^{**} \wedge y^{**})^{**} \leq y^{****} = y^{**}$. Hence $(x^{**} \wedge y^{**})^{**} \leq x^{**} \wedge y^{**}$ and so $(x^{**} \wedge y^{**})^{**} = x^{**} \wedge y^{**}$, meaning $x^{**} \wedge y^{**} \in P^{**}$.

Clearly if $x^{**} \in P$, then $0 \leq x$ implies $0^{**} \leq x^{**}$, and $x^{**} \leq 1 = 1^{**}$. □

We now consider some results specific to the Galois connections on powersets. That is, Galois connections of the form

$$P(A) \rightleftarrows P(B)$$

Where A and B are sets, and our powersets are ordered by $\subseteq$. Specifically we want to show that Galois connections of this form are closely linked to relations between A and B.

Theorem 2.4.6. [13]**.** *For every Galois connection between $P(A)$ and $P(B)$ there is a unique relation $R \subseteq A \times B$ defined by $R = \{(a, b) \in A \times B \mid \{a\} \subseteq \{b\}^*\} = \{(a, b) \in A \times B \mid \{b\} \subseteq \{a\}^*\}$.*

Moreover, each relation $R \subseteq A \times B$ induces a Galois connection where for any subset S of A, $S^* = \{b \in B \mid (a, b) \in R \text{ for all } a \in S\}$ and for every subset T of B, $T^* = \{a \in A \mid (a, b) \in R \text{ for all } b \in T\}$.

Proof. For the first part of the theorem, it is easy to see that given a Galois connection, such a relation R exists. Moreover, by Lemma 2.4.2 we have that $\{a\} \subseteq \{b\}^*$ if and only if $\{b\} \subseteq \{a\}^*$, and so we can see the two sets described above are equal.

For the second part of the theorem, we show that, given $R \subseteq A \times B$, the maps defined above form a Galois connection between $P(A)$ and $P(B)$. Consider subsets $S, T \subseteq A$. If $S \subseteq T$ then we consider an element $b \in T^*$. If $b \in T^*$ then $(a, b) \in R$ for all $a \in T$. Then since $a \in S$, we obtain $(a, b) \in R$ for all $a \in S$, and therefore $T^* \subseteq S^*$. Consider that,

$$S^{**} = \{a \in A \mid (a, b) \in R \text{ for all } b \in S^*\}$$

Then, if $a \in S$, for any $b \in S^*$, we have that $(a, b) \in R$, by definition. Hence, $a \in S^{**}$, and $S \subseteq S^{**}$. Note that a similar proof can be applied if $S, T \subseteq B$, and thus our induced maps form a Galois connection. □

2.5 Theories and Models of Classical Propositional Logic

In this section we provide an algebraic definition for a theory and a model of propositional logic. We also show how we can define a Galois connection derived from a relation between the formulae in a theory of propositional logic and its models, and thus define the theorems of a given theory, and provide an algebraic proof of the completeness and soundness of classical logic.

Definition 2.5.1. A **theory of classical propositional logic** is a pair (X, A) where X is a set and A is a subset of $F_{\mathbf{Bool}}(X)$, where $F_{\mathbf{Bool}}(X)$ is the free Boolean algebra (or equivalently free Boolean ring) as described in Lemma 2.2.2.

Note 2.5.2. Intuitively this corresponds to a "typical" definition of a theory of classical propositional logic as follows:

- The elements of our set X are called the *variables* in our propositional logic.
- For a set X of variables, the elements of $F_{\mathbf{Bool}}(X)$ are the *formulae* of our propositional theory.
- A is a subset of $F_{\mathbf{Bool}}(X)$, called the *axioms* of (X, A), where in our theory we treat each formula $a \in A$ as assumed "true" or "satisfied" in our theory.

The correspondence between this algebraic definition of a theory of classical logic, and theories of classical logic given in a non-algebraic setting (such as in [15]) will be discussed in greater detail in Chapter 4.

Lemma 2.5.3. *In any Boolean algebra, B and its corresponding Boolean ring, the following are equivalent,*

a. $x = y$

b. $x + y = 0$

c. $x \Leftrightarrow y = 1$

for any $x, y \in B$.

Proof. *a.*$\Leftrightarrow$ *b.:*
Notice that $x + y = 0$ if and only if $x + y + x = 0 + x$. But since x is its own additive inverse this is equivalent to $y = x$. Hence, a. and b. are equivalent.
a.$\Leftrightarrow$ *c.:*
$x \Leftrightarrow y = 1$ if and only if $(x \Rightarrow y) \wedge (y \Rightarrow x) = 1$, if and only if $x \Rightarrow y = 1$ and $y \Rightarrow x = 1$. This is equivalent to $x \leq y$ and $y \leq x$. That is, $x = y$, and so a. and c. are equivalent conditions. □

Definition 2.5.4. If X is our set of variables in a theory as above, a **model** of classical logic is a Boolean algebra homomorphism $m : F_{\mathbf{Bool}}(X) \to \{0, 1\}$. That is, the set of models is the set $\hom(F_{\mathbf{Bool}}(X), \{0, 1\})$. In particular, a model of a theory (X, A) is a Boolean algebra homomorphism $m : F_{\mathbf{Bool}}(X) \to \{0, 1\}$ such that $m(p) = 1$ whenever $p \in A$.

Note 2.5.5. Again, the intuition we use to construct this definition is as follows,

- A map $F_{\mathbf{Bool}}(X) \to \{0, 1\}$ corresponds to selecting a "truth value" for each formula in our logic where 0 is "false" and 1 is "true".

- The way we define a model of a theory (X, A) can also be seen a truth value map which always assigns the axioms in A the value of "true".

Definition 2.5.6. The above definition of a model of A, gives us a relation, sometimes called an **entailment** relation, $\vDash \subseteq \hom(F_{\mathbf{Bool}}(X), \{0, 1\}) \times F_{\mathbf{Bool}}(X)$. This is defined as follows:

$$\vDash = \{(m, p) \in \hom(F_{\mathbf{Bool}}(X), \{0, 1\}) \times F_{\mathbf{Bool}}(X) \mid m(p) = 1\}$$

We write $m \vDash p$ in this case and say that m **satisfies, entails** or **is a model of** p.

As we have seen in Theorem 2.4.6, this relation induces a Galois connection,

$$P(F_{\mathbf{Bool}}(X)) \rightleftarrows P(\hom(F_{\mathbf{Bool}}(X), \{0, 1\}))$$

which is defined for each $S \subseteq F_{\mathbf{Bool}}(X)$ and $M \subseteq \hom(F_{\mathbf{Bool}}(X), \{0, 1\})$ by,

$$S^* = \{m \in \hom(F_{\mathbf{Bool}}(X), \{0, 1\}) \mid m \vDash p \text{ for all } p \in S\}$$

and,

$$M^* = \{p \in F_{\mathbf{Bool}}(X) \mid m \vDash p \text{ for all } m \in M\}.$$

We recall that this Galois connection induces a closure operation given by $(-)^{**}$ on both $P(F_{\mathbf{Bool}}(X))$ and $P(\hom(F_{\mathbf{Bool}}(X), \{0,1\}))$. The first closure operator on the relations on $F_{\mathbf{Bool}}(X)$ can be described as follows.

Lemma 2.5.7. *For any set $A \subseteq F_{\mathbf{Bool}}(X)$ the set A^{**} is the smallest filter on $F_{\mathbf{Bool}}(X)$ containing A.*

Proof. First, note that

$$A^{**} = \{p \in F_{\mathbf{Bool}}(X) \mid m \vDash p \text{ for all } m \in A^*\} = \{p \in F_{\mathbf{Bool}}(X) \mid m \vDash p \text{ whenever } m \vDash a \text{ for all } a \in A\}$$

Thus, if $p, q \in A^{**}$, then $m(p \wedge q) = m(p) \wedge m(q) = 1 \wedge 1 = 1$ for any $m \in A^*$. Hence $p \wedge q \in A^{**}$. Moreover, we have that if $p \in A^{**}$ and $p \leq q$, then $m(p) \leq m(q)$ for any $m \in A^*$. Then $1 = m(p) \leq m(q)$ and so $m(q) = 1$. Thus $q \in A^{**}$, and so A^{**} is a filter.

We now need to show that A^{**} is the *smallest* filter containing A. Consider then a filter $F \subseteq F_{\mathbf{Bool}}(X)$ such that $A \subseteq F$. Then, by Lemma 2.3.10, there exists some Boolean homomorphism $f : F_{\mathbf{Bool}}(X) \to B$ such that $F = \{x \in F_{\mathbf{Bool}}(X) \mid f(x) = 1\}$. Then, since $A \subseteq F$, we have that $f(a) = 1$ for any $a \in A$. Hence $mf(a) = 1$ for all $m \in \hom(B, \{0,1\})$, and so $mf \in A^*$. It follows that, $\hom(B, \{0,1\}) = \{m \in \hom(B, \{0,1\}) \mid mf(a) = 1 \text{ for all } a \in A\}$.

Thus, if $p \in A^{**}$ it is sufficient to show that $f(p) = 1$ in order to conclude that $p \in F$. Note that $mf(p) = 1$ for all $m \in \hom(B, \{0,1\})$ since $mf \in A^*$. Now assume that $f(p) \neq 1$. It follows then that $\neg f(p) \neq 0$. Then there is an ultrafilter U on B containing $\neg f(p)$, by Lemma 2.3.18, but then by Lemma 2.3.20 we have $f(p) \notin U$. This means that there must exist $m : B \to \{0,1\}$ such that $mf(p) = 0$ which contradicts the fact that $mf(p) = 1$ for every $m \in \hom(B, \{0,1\})$. Hence, $f(p) = 1$, and thus $p \in F$. □

Corollary 2.5.8. *Let E_A be the congruence corresponding to the filter A^{**}. Then E_A is the smallest congruence on $F_{\mathbf{Bool}}(X)$ containing $A \times \{1\}$. Equivalently, it is the smallest congruence such that $A \subseteq [1]$ in $F_{\mathbf{Bool}}(X)/E_A$.*

Proof. Note that if E is a congruence containing $A \times \{1\}$, then by Lemma 2.3.10 there exists some filter F such that $(p, q) \in E$ if and only if $p \Leftrightarrow q \in F$. Therefore, $a = a \Leftrightarrow 1 \in F$ for all $a \in A$. Thus

F is a filter containing A and by our previous lemma, $A^{**} \subseteq F$. Then if $(p, q) \in E_A$, we have that $p \Leftrightarrow q \in A^{**} \subseteq F$ and therefore $(p, q) \in E$. Hence, $E_A \subseteq E$. $\square$

These results allow us to consider the quotient algebra $F_{\mathbf{Bool}}(X)/E_A$. Recall explicitly that the elements of this quotient algebra are the equivalence classes $[p]$ where $p \in F(X)$ and $[p] = \{q \in F(X) \mid p \Leftrightarrow q \in A^{**}\}$. Moreover, since A^{**} is the smallest filter containing A, we can consider A^{**} to be the *closure of A under "logical consequence"*. That is, if we consider elements of A to be axioms, then A^{**} includes A and other formulae that necessarily become equivalent to 1 in a Boolean algebra once we treat the members of A as being equal to 1. We then define a theorem of (X, A) as follows.

Definition 2.5.9. A **theorem** of (X, A) is an element $p \in F_{\mathbf{Bool}}(X)$ such that $[p] = [1]$ in $F_{\mathbf{Bool}}(X)/A^{**}$, or equivalently $p \in A^{**}$.

Theorem 2.5.10. *If (X, A) is a theory of classical propositional logic, then p is a theorem of (X, A) if and only if $m \vDash p$ for every model m of A.*

Note 2.5.11. This result is often called the *completeness* and *soundness* properties of classical logic. In particular, the "if" statement is completeness and the "only if" statement is soundness.

Proof. Suppose p is a theorem of (X, A). Then by definition $p \in A^{**}$ and so $m(p) = 1$ for each $m \in A^*$. Since A^* is the set of all models of A then we can say $m \vDash p$ for every model of A.

Conversely, consider p such that $m \vDash p$ whenever m is a model of A. That is, is $m(a) = 1$ for any $a \in A$. Then by definition of A^{**} we obtain that $p \in A^{**}$ and so we have that p is a theorem of (X, A). $\square$

This completeness and soundness result shows us that the theorems of (X, A) are exactly those propositions which are entailed by every model of A.

2.6 Determining Theorems of (X, A)

In this section, we find several different equivalent conditions for an element p of $F_{\mathbf{Bool}}(X)$ to be a theorem of a given theory (X, A). We then determine two algorithms which, given $p \in F_{\mathbf{Bool}}(X)$ and a theory (X, A), decides whether p is a theorem or not, as long as A is finite.

Lemma 2.6.1. *Let (X, A) be a theory of classical propositional logic, and let p be an element of $F_{\mathbf{Bool}}(X)$. Then the following conditions are equivalent:*

a. $[p] = [1]$ *in* $F_{\textbf{\textit{Bool}}}(X)/A^{**}$.

b. p *is an element of* A^{**}.

c. $\{p\}^{**} \subseteq A^{**}$.

d. $A^* \subseteq \{p\}^*$.

That is, if p *satisfies any of the above conditions, then it is a theorem of* (X, A).

Proof. *a.⇔b.:* By the definition of our equivalence classes in $F_{\mathbf{Bool}}(X)/A^{**}$, we have $[p] = [1]$ is true if and only if $p \in A^{**}$.

b.⇔c.: Note that if $p \in A^{**}$, then A^{**} is a filter of $F_{\mathbf{Bool}}(X)$ that contains $\{p\}$. Then since $\{p\}^{**}$ is the smallest filter containing $\{p\}$ we must have that $\{p\}^{**} \subseteq A^{**}$. Clearly the converse holds since $p \in \{p\}^{**} \subseteq A^{**}$ so $p \in A^{**}$.

a.⇔d.: $A^* \subseteq \{p\}^*$ states that if m is a model of A, then $m \vDash p$. Therefore, by our Theorem 2.5.10 it follows that this is true if and only if p is a theorem of (X, R). □

We now come to the construction of our algorithms which can determine whether or not an element of $F_{\mathbf{Bool}}(X)$ is a theorem. We first consider the case for finite X.

Theorem 2.6.2. *Given a theory of classical propositional logic* (X, A) *where* X *is a finite set, and an element* p *of* $F_{\textbf{\textit{Bool}}}(X)$*, we can construct two algorithms to determine whether or not* p *is a theorem of* (X, A)*, which can be computed in finitely many steps.*

Proof. In this proof, we use the shorthand $F(X)$ to denote $F_{\mathbf{Bool}}(X)$.

First algorithm:

Consider from the above Lemma 2.6.1 that p is a theorem if and only if $A^* \subseteq \{p\}^*$. Then, since X is finite we can consider the diagram below

$$P(F(X)) \underset{(-)^*}{\overset{(-)^*}{\rightleftarrows}} P(\hom(F(X), \{0,1\})) \underset{\alpha_{F(X)}}{\overset{\alpha^{-1}_{F(X)}}{\rightleftarrows}} F(X)$$

where the rightmost arrows are the isomorphisms constructed in Theorem 2.3.5. Then it follows that $A^* \subseteq \{p\}^*$ if and only if $\alpha^{-1}_{F(X)}(A^*) \leq \alpha^{-1}_{F(X)}(\{p\}^*)$. In particular, notice that $\{p\}^* = \{m \in \hom(F(X), \{0,1\}) \mid m(p) = 1\} = \alpha_{F(X)}(p)$. And so $\alpha^{-1}_{F(X)}(\{p\}^*) = p$.

We can also note that if A is finite then $A = \bigcup_{x \in A} \{x\}$ which represents a finite join of elements in $P(F(X))$. Hence, by Lemma 2.4.4 we have that $A^* = (\bigcup_{x \in A} \{x\})^* = \bigcap_{x \in A} (\{x\}^*)$. We then have for each $a \in A$ that $\alpha^{-1}_{F(X)}(\{a\}^*) = a$, and since $\alpha^{-1}_{F(X)}$ is an order isomorphism we can compute the image of A^* under $\alpha^{-1}_{F(X)}$ as,

$$\alpha^{-1}_{F(X)}(A^*) = \alpha^{-1}_{F(X)}(\bigcap_{x \in A} (\{x\}^*)) = \bigwedge_{a \in A} \{a\}.$$

This is computable since A is finite. In order to determine whether p is a theorem, we then only need to check if,

$$\bigwedge_{a \in A} \{a\} \leq p.$$

Alternatively, we can convert our expressions into polynomials in a Boolean ring, and the following condition is equivalent:

$$\prod_{a \in A} a \leq p.$$

Or if we take the meet with $\neg p$ to each side of the inequality, which corresponds to multiplying by $1 + p$ we equivalently have:

$$(\prod_{a \in A} a)(1 + p) = 0.$$

It is clear that this involves finitely many operations while X is finite. Furthermore, if we consider $F(X)$ as being equal to $PP(X)$ with the Boolean ring operations defined as in Theorem 2.2.2 then this corresponds to performing finitely many set operations on the elements of $PP(X)$. We can then perform the above computation on our sets, and if our answer is $\emptyset$ then p is a theorem of (X, A), and if the answer is non-empty, then p is not a theorem.

Second algorithm:

Using the same result in Theorem 2.6.1, we can also apply the fact that p is a theorem if and only if $A^* \subseteq \{p\}^*$. That is, if and only if for any homomorphism $m \in \hom(F(X), \{0, 1\})$, $m \vDash a$ for all $a \in A$ implies that $m \vDash p$.

Also note that since $F(X)$ is a free algebra, each $m \in \hom(F(X), \{0, 1\})$ is uniquely determined by the map $m' : X \to \{0,1\}$ where $m'(x) = m(x)$.

Then, in order to determine whether p is a theorem, we take each function $m' : X \to \{0,1\}$ and consider the unique morphism $m : F(X) \to \{0,1\}$ such that $\eta_X m = m'$. Then we compute $m(a)$ for each $a \in A$. If $m(a) = 0$ for any $a \in A$ then it is not in A^* and so we do not need to check if it is a member of $\{p\}^*$. If $m(a) = 1$ for all $a \in A$, then we check if $m(p) = 1$. If $m(p) = 0$ for any such m then we can conclude that p is not a theorem of (X, A). If $m(p) = 1$ for every m such that $m(a) = 1$ for every $a \in A$, then p is a theorem of (X, A). Also note that since X is finite, there are only $2^{|X|}$ functions from X to $\{0,1\}$ and we are also given that the number of axioms in A are finite. Therefore this algorithm only involves finitely many steps. □

Note 2.6.3. In the case where X is non-finite, we note that A is finite, and each element of A only contains finite elements in X. Moreover, each formulae $p \in F_{\mathbf{Bool}}(X)$ which we are applying our algorithm to only contains finite members of X. Therefore we consider a finite subset of X, consisting of the elements of X which appear in A and the formula p, and denote it $V_{(A,p)} \subseteq X$. Then, it is clear that p is a theorem of (X, A) if and only if it is a theorem of $(V_{(A,p)}, A)$. Therefore, we are able to use our algorithms in the case where X is infinite, by restricting the variables we consider to those that occur in A and p.

To conclude the chapter, we show how these algorithms can decide, given axioms, whether or not certain results are theorems.

Example 2.6.4. Suppose the following statements are axioms:

a. $a \Rightarrow b$.

b. $c \Rightarrow \neg b$.

And we want to determine whether the following are theorems,

c. $c \Rightarrow \neg a$.

d. $a \Rightarrow c$.

We apply our first algorithm in the case of c. and our second algorithm in the case of d. Note here that our variables are $\{a, b, c\}$.

To determine whether c. is a theorem, we convert the terms into ring operations and calculate

$(a \Rightarrow b) \wedge (c \Rightarrow \neg b) = (1+a+ab)(1+bc) = 1+a+ab+bc+abc+abc = 1+a+ab+bc$. Then we multiply this by $\neg(c \Rightarrow \neg a) = ac$. Thus, we obtain,

$$(1+a+ab+bc)(ac) = ac+ac+abc+abc = 0$$

and therefore, by our first algorithm, $c \Rightarrow \neg a$ is a theorem.

Using our second algorithm to determine whether d. is a theorem, first note that each morphism $F(\{a,b,c\}) \to \{0,1\}$ is determined entirely by its values on $\{a,b,c\}$. Then, we consider the map $f : F(\{a,b,c\}) \to \{0,1\}$ determined by $f(a) = 0$, $f(b) = 0$ and $f(c) = 1$. We notice that $f(a \Rightarrow b) = 0 \Rightarrow 0 = 1$, $f(c \Rightarrow \neg b) = 1 \Rightarrow \neg 0 = 1$ and $f(a \Rightarrow c) = 0 \Rightarrow 1 = 0$. By the first two equalities, we have that $f \in A^*$, but by the third inequality $f \notin \{a \Rightarrow c\}^*$. Thus d. is not a theorem.

This shows us how we can use our two algorithms to determine whether an element $p \in F_{\mathbf{Bool}}(X)$ is a theorem of (X, A) for some finite set $A \subseteq F_{\mathbf{Bool}}(X)$. It also worth noting that these algorithms rely on results proved earlier in the chapter, such as the duality between finite sets and finite Boolean algebras, and the fact that each finitely generated Boolean algebra is finite.

Of particular interest is the theory $(X, \emptyset)$, which we will see corresponds to what is called the *formal theory of classical propositional logic* in Chapter 4. In this theory the set of theorems is $\emptyset^{**} = \{1\}$. That is, its theorems consist of just those "terms" which are equal to 1 in the free Boolean algebra. However, in order to formally describe what we mean by a "term" in $F_{\mathbf{Bool}}(X)$, we consider a universal approach to categories of algebras, including **Bool**, which is given in the following chapter.

3 Varieties of Universal Algebra

In this chapter, we introduce varieties of universal algebra, which describes many well-known categories of algebras, such as **Bool**. In order to do this, we introduce an algebraic theory, and define a variety of universal algebras as the category whose objects are the models of this theory. Furthermore, we describe internal structures of a variety of universal algebras, such as subalgebras, quotient algebras, product algebras and free algebras, and provide a proof of Birkhoff's Theorem [2], which shows that a class of algebras with the same signature is a variety if and only if it is closed under subalgebras, products and quotients. We discuss subvarieties of a given variety of algebras, and show how these form a lattice in which meets and joins can be expressed both as an operation on the classes of objects in our subvarieties, and as an operation on the axioms of the algebraic theories which determine these varieties. Lastly, we generalize the concept of completeness of **Bool** in our previous chapter to consider completeness with respect to L-valued models in a general variety.

3.1 Ω-Algebras

In this subsection, we define a category of Ω-algebras, and construct a free Ω-algebra, also called a term algebra or an absolutely free algebra, over a set X.

Definition 3.1.1. Let $\Omega = (\Omega, l_\Omega)$ be a pair such that Ω is a set and $l_\Omega : \Omega \to \mathbb{N}$ is a function where $\mathbb{N} = \{0, 1, 2, ...\}$. The set Ω is referred to as the **signature**.
An Ω**-algebra** is a pair $A = (A, v)$ where A is a set, called the underlying set of (A, v) and

$$v : \Omega \to \bigcup_{n \in \mathbb{N}} A^{A^n}$$

is a map such that for each $\omega \in \Omega$, $v(\omega)$ is a function $v(\omega) : A^{l_\Omega(\omega)} \to A$.

Note 3.1.2. Together with the above definition, we introduce some additional notation and terminology.

1. For each $\omega \in \Omega$, the value $l_\Omega(\omega)$ is called the **arity** of ω.
2. We refer to each ω as an **operation symbol** or **operator**. If $l_\Omega(\omega) = n$ we say that ω is an n**-ary operation**.
3. For an Ω-algebra (A, v), we call $v(\omega)$ the **valuation** or **interpretation** of ω for (A, v).
4. In an Ω-algebra (A, v), we will often write $\omega(a_1, ..., a_n)$ instead of $v(\omega)(a_1, ..., a_n)$ where $\omega \in \Omega$ is an n-ary operation and $a_1, .., a_n \in A$.

5. When ω is a 0-ary, 1-ary and 2-ary operation, we will call it a nullary, unary or binary operation respectively. In the above cases we also write ω, ωa_1 and $a_1 \omega a_2$ for $\omega()$, $\omega(a_1)$ and $\omega(a_1, a_2)$ respectively.

6. When $\Omega = \{\omega_1, \omega_2, ..., \omega_m\}$ is a finite set, we may denote an Ω-algebra (A, v) as an $m+1$-tuple, $(A, \omega_1, \omega_2, ..., \omega_m)$.

7. In particular we note that when ω is a nullary operation, this corresponds to a map $v(\omega) : A^0 \to A$ where A^0 is a one element set, $\{*\}$. This corresponds with picking a certain element of A, the element $v(\omega)(*)$. As mentioned before, we will simply refer to $v(\omega)(*)$ as ω, and so $\omega \in A$ is a selected element of A for each nullary operation $\omega \in \Omega$.

8. We can also denote Ω as a union of disjoint sets $\Omega_0 \cup \Omega_1 \cup \Omega_2 \cup ...$, where for each $n \in \mathbb{N}$, we define $\Omega_n = l_\Omega^{-1}(\{n\})$. That is, Ω_n is the set of all n-ary operations in Ω.

Definition 3.1.3. A **homomorphism of Ω-algebras** $f : (A, v) \to (B, w)$ is a function $f : A \to B$ such that the diagram

$$\begin{array}{ccc} A^n & \xrightarrow{f^n} & B^n \\ \downarrow{\scriptstyle v(\omega)} & & \downarrow{\scriptstyle w(\omega)} \\ A & \xrightarrow{f} & B \end{array}$$

commutes for each $\omega \in \Omega$, where f^n is defined by $f^n(a_1, ..., a_n) = (f(a_1), ..., f(a_n))$ for $(a_1, ..., a_n) \in A^n$. That is, using the notation in Note 3.1.2, we require f to be a function $f : A \to B$ such that $f(\omega(a_1, ..., a_n)) = \omega(f(a_1), ..., f(a_n))$ for every $\omega \in \Omega$.

Definition 3.1.4. The category of Ω-algebras, denoted $\mathbf{Alg}(\Omega)$, is a category where the objects are Ω-algebras and the morphisms are Ω-algebra homomorphisms.

Note 3.1.5. It is easy to see how this is a well-defined category since trivially each identity map $1_A : A \to A$ preserves operations in Ω. Furthermore if $f : A \to B$ and $g : B \to C$ are morphisms in $\mathbf{Alg}(\Omega)$ then $gf(\omega(a_1, ..., a_n)) = g(\omega(f(a_1), ..., f(a_n))) = \omega(gf(a_1, ..., gf(a_n)))$ and so gf is a morphism.

Example 3.1.6.

a. $\mathbf{Alg}(\emptyset)$ is the category **Set** since if there are no operations in Ω the map v for each (A, v) is empty.

b. Let Ω_2 be a one element set, and $\Omega_n = \emptyset$ for all $n \in \mathbb{N} - \{2\}$. Then $\mathbf{Alg}(\Omega)$ is the category of magmas, **Magma**. That is, each object of $\mathbf{Alg}(\Omega)$ is a set closed under a single binary operation, usually written $\cdot$. If A is the underlying set of the magma we will often write it $(A, \cdot)$.

In our examples above, the categories we have described are closed under the specified operations in Ω. However, the algebraic structure of the objects in these categories is fairly simple, since the specified operations are not defined in such a way that they satisfy any properties, or *identities*, which are often used to describe other well-known algebras. For example, a semigroup $(S, \cdot)$, is an associative magma. That is, a magma such that,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

for all $x, y, z \in S$. The structure of an Ω-algebra provides us a systematic way to define the operations of an algebraic structure and their arities, but it does not provide a systematic way to describe identities, such as the associativity property of $\cdot$ above. In order to incorporate these, we must first describe a free Ω-algebra over X, also called the term algebra, or the absolutely free algebra.

Definition 3.1.7. Consider the adjunction

$$\mathbf{Alg}(\Omega) \underset{F_\Omega}{\overset{U}{\rightleftarrows}} \mathbf{Set} \quad (\top)$$

where U is the forgetful functor. Then we call F_Ω the **free functor** to $\mathbf{Alg}(\Omega)$ and for any set X, we call $F_\Omega(X)$ the **free Ω-algebra over** X.

For the rest of this section, we will be constructing and proving the existence of the free functor for $\mathbf{Alg}(\Omega)$ for an arbitrary Ω. In particular, we will show that for any set X, the underlying set of $F_\Omega(X)$ is a subset of the free monoid over $X \cup \Omega$. The free monoid is defined similarly.

Definition 3.1.8. Consider the adjunction,

$$\mathbf{Mon} \underset{F_{\mathbf{Mon}}}{\overset{U}{\rightleftarrows}} \mathbf{Set} \quad (\top)$$

where U is the forgetful functor. Then we call $F_{\mathbf{Mon}}$ the **free functor** to **Mon** and for any set X, we call $F_{\mathbf{Mon}}(X)$ the **free monoid over** X.

Lemma 3.1.9. *The free monoid over any set X is given by*

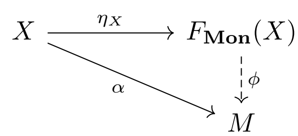
$$F_{\boldsymbol{Mon}}(X) = \bigcup_{n \in \mathbb{N}} X^n,$$

where our monoid multiplication is defined by $(x_1, ..., x_n) \cdot (y_1, ..., y_m) = (x_1, ..., x_n, y_1, ..., y_m)$ *for all* $x_i, y_j \in X$*, and our identity* 1 *is the unique element contained in the one element set* X^0*, which we write as the empty brackets* $()$.

Proof. It is clear to see that $F_{\mathbf{Mon}}(X)$ is a monoid. We have that $()(x_1, ..., x_n) = (x_1, ..., x_n) = (x_1, ..., x_n)()$, and

$$\begin{aligned}((x_1, ..., x_n) \cdot (y_1, ..., y_m)) \cdot (z_1, ..., z_k) &= (x_1, ..., x_n, y_1, ..., y_m) \cdot (z_1, ..., z_k)\\ &= (x_1, ..., x_n, y_1, ..., y_m, z_1, ..., z_k)\\ &= (x_1, ..., x_n) \cdot (y_1, ..., y_m, z_1, ..., z_k)\\ &= (x_1, ..., x_n) \cdot ((y_1, ..., y_m) \cdot (z_1, ..., z_k)).\end{aligned}$$

In order to see it is in fact the free monoid over X, we must find a function $\eta_X : X \to F(X)$ such that for any monoid M, and any function $\alpha : X \to M$, there is a unique monoid homomorphism ϕ such that the diagram



commutes in **Set**. We define η_X by $\eta_X(x) = x$, where $x \in X$ is considered a 1-tuple in $\bigcup_{n\in\mathbb{N}} X^n$. We claim then that $\phi((x_1, ..., x_n)) = \alpha(x_1)\alpha(x_2)...\alpha(x_n)$ is the unique homomorphism such that the diagram commutes. Clearly $\phi\eta_X(x) = \phi(x) = \alpha(x)$, and so the diagram commutes. Secondly, note that

$$\begin{aligned}\phi((x_1, ..., x_n)(y_1, ..., y_m)) &= \phi((x_1, ..., x_n, y_1, ...y_m))\\ &= \alpha(x_1)...\alpha(x_n)\alpha(y_1)...\alpha(y_m)\\ &= (\alpha(x_1)...\alpha(x_n))(\alpha(y_1)...\alpha(y_m))\\ &= \phi((x_1, ..., x_n))\phi((y_1, ..., y_m))\end{aligned}$$

for any $(x_1, ..., x_n), (y_1, ..., y_m) \in F_{\mathbf{Mon}}(X)$ and so ϕ is a monoid homomorphism.

Lastly, we need to note that for any homomorphism $\varphi : F_{\mathbf{Mon}}(X) \to M$, we get $\varphi((x_1, ..., x_n)) = \varphi(x_1)\varphi(x_2)...\varphi(x_n)$ and so the value of $\varphi((x_1, ..., x_n))$ for any $(x_1, ..., x_n) \in F_{\mathbf{Mon}}(X)$ is determined entirely by the image of φ on the 1-tuples $x_1, .., x_n \in X$. Therefore, if $\varphi : F_{\mathbf{Mon}}(X) \to M$ is a homomorphism such that $\varphi\eta_X = \alpha = \phi\eta_X$ then $\varphi(x) = \alpha(x) = \phi(x)$ for all $x \in X$. Then since ϕ is uniquely determined by its values on X, we can conclude that $\phi = \varphi$, and so ϕ is unique. □

We can now consider $F_{\mathbf{Mon}}(X \cup \Omega)$ where an element is an m-tuple (for any $m \in \mathbb{N}$), $(a_1, ..., a_m)$ such that each a_i is an element of either X or Ω. Specifically, we consider the case when X and Ω are disjoint. In this instance, we call the elements of $X \cup \Omega$ **letters** and the elements of $F_{\mathbf{Mon}}(X \cup \Omega)$ **words**. In our next result, we show that we can describe a free Ω-algebra over X by selecting a subset of the words in $F_{\mathbf{Mon}}(X \cup \Omega)$. In particular we want to define the elements of $F_\Omega(X)$ in such a way that it contains the elements of X. Moreover, in order to ensure $F_\Omega(X)$ is closed under its operations, we want to have that, for any $\omega \in \Omega_n$ we have that the image of any m-tuple in $F_\Omega(X)$ under ω is still contained in the set $F_\Omega(X)$. That is, we require elements of $F_\Omega(X)$ to be constructed in the following way.

i. If $x \in X$, then $x \in F_\Omega(X)$, where x is considered a 1-tuple in $F_{\mathbf{Mon}}(X \cup \Omega)$.

ii. If $\omega_0 \in \Omega_0$, then $\omega_0 \in F_\Omega(X)$.

iii. If $t_1, ..., t_n$ are elements of $F_\Omega(X)$, and ω is an element of Ω_n, then $(\omega, t_1, ..., t_n) \in F_\Omega(X)$.

A more formal approach to this can be used to define the free Ω-algebra over X, as seen below.

Lemma 3.1.10. *Let X and Ω be distinct sets, and consider the subset of $F_{\mathbf{Mon}}(X \cup \Omega)$ defined by $\bigcup_{i \in \mathbb{N}} X_i$, where each X_i is defined inductively as:*

$$X_0 = X$$

$$X_{i+1} = X_i \cup \left(\bigcup_{n \in \mathbb{N}} \left\{ (\omega, t_1, ..., t_n) \mid \omega \in \Omega_n \text{ and } t_1, ..., t_n \in X_i \right\} \right)$$

Then $\bigcup_{i \in \mathbb{N}} X_i$ is an Ω-algebra where for each m-ary operation $\omega \in \Omega$, we define ω as an operation by $\omega(t_1, ..., t_m) = (\omega, t_1, ..., t_m)$ for all $t_1, ..., t_m \in \bigcup_{i \in \mathbb{N}} X_i$.

Proof. First note that by construction $X_i \subseteq X_{i+1}$ for each $i \in \mathbb{N}$. Now we want to show that $F_\Omega(X)$ is closed under each $\omega \in \Omega$. If ω is an m-ary operation, then we consider $t_1, ..., t_m \in F_\Omega(X)$. We know for each of these elements that $t_1 \in X_{i_1}$,$t_1 \in X_{i_1}$,...,$t_n \in X_{i_n}$ for some $i_1, ..., i_n \in \mathbb{N}$. We choose $k = \max\{i_1, ..., i_n\}$, and hence we have that $t_1, ..., t_n$ are all elements of X_k. Therefore by definition $\omega(t_1, .., t_m) = (\omega, t_1, ..., t_m)$ is an element of X_{k+1} and so $\omega(t_1, .., t_m) \in \bigcup_{i \in \mathbb{N}} X_i$. In particular, each nullary operation ω_0 is an element of X_1, since it is a member of $\{(\omega_0) \mid \omega_0 \in \Omega_0\}$ which is part of our union of sets forming X_1. Therefore $F_\Omega(X)$ is closed under every operation $\omega \in \Omega$ and so is an Ω-algebra. □

Definition 3.1.11. Using notation as above, we refer to the elements of $X \cup \omega$ as **letters**, the elements of $F_{\mathbf{Mon}}(X \cup \Omega)$ as **words** and the elements of $\bigcup_{i \in \mathbb{N}} X_i$ as **terms**. Then we denote the **length** of a word by $|w|$ for all w in $F_{\mathbf{Mon}}(X \cup \Omega)$ and define it by $|w| = m$ when $w \in (X \cup \Omega)^m$.

Note 3.1.12. It is clear that the following holds:

- For any words w and v, we get $|wv| = |w| + |v|$.
- $|w| = 0$ if and only if $w = 1$.
- If $x_1, ..., x_n, x'_1, ..., x'_{n'}$ are letters, then $x_1 x_2 ... x_n = x'_1 ... x'_{n'}$ if and only if $n = n'$ and each $x_i = x'_i$. This principle is often called the uniqueness of product presentation.

Lemma 3.1.13. *For a given X and Ω, if t is a term, and tw is a term then $w = 1$.*

Proof. Let z be the smallest positive integer such there exist terms t and tw where $|t| = z$. Then, if $t \in X$, then by definition of $\bigcup_{i \in \mathbb{N}} X_i$, the only terms with their first entry in X are those in X_0. Hence, in this case if tw is a term then $t = tw$.

If $t \notin X$ then we can write t and tw in the form $t = \omega t_1 t_2 ... t_n$ and $tw = \omega' t'_1, ..., t'_{n'}$ for $\omega \in \Omega_n$ and $\omega' \in \Omega_{n'}$. But then, from the uniqueness of product presentation, the first letter of t is unique and hence $\omega = \omega'$, which also gives us that $n = n'$.

Thus, we are able to compare the next letter of t and tw. That is, we compare the first letter of terms t_1 and t'_1, and since these both occur in t they must be equal. In the case that $t_1 = x_1 \in X$, then t_1 is a letter, by uniqueness of product presentation, we must have $t_1 = x_1 = t'_1$. In the other case, we obtain $t_1 = \omega_1 v_1 ... v_k$ and $t'_1 = \omega'_1 v'_1 .... v'_{k'}$. Again, using uniqueness of product presentation, we get $\omega_1 = \omega'_1$ and thus $k = k'$. Repeating this argument, we obtain that t_1 and t'_1 contain the same number of letters in $(X \cup \Omega)$ and that each of these letters are the same.

This allows us then to compare t_2 and t'_2. Repeating the same argument, we then get that $t_2 = t'_2$. Furthermore, this can be repeated n times to obtain that $t_i = t'_i$ for $i \in \{1, .., n\}$. Finally, this gives us

$$|t| = 1 + \sum_{i=1}^{n} |t_i| = 1 + \sum_{i=1}^{n} |t'_i| = |tw| = |t| + |w|$$

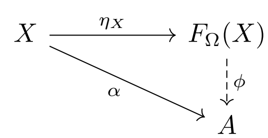
and therefore $|w| = 0$ which tells us $w = 1$.

Note here that if z was not minimal we could have that $t = uv$ for some term u and word v, and so we would need to show that $tw = uvw$ implies that vw is empty. Again, we could apply the same proof as above to u and uvw under the assumption that u is minimal. That is, if we have proved the above for minimal length k, then the same holds for terms of non-minimal length. $\square$

Corollary 3.1.14. *If* $\omega t_1...t_n = \omega' t'_1...t'_{n'}$ *in* $\bigcup_{i\in\mathbb{N}} X_i$*, where* $\omega, \omega' \in \Omega$ *and* $t_1, ..., t_n, t'_1, ..., t'_{n'} \in \bigcup_{i\in\mathbb{N}} X_i$ *then* $\omega = \omega'$*,* $n = n'$ *and* $t_i = t'_i$ *for all* $i \in \{1, ..., n\}$*.* $\square$

Lemma 3.1.15. *For any set* X *which is distinct from* Ω*, the free* Ω*-algebra,* $F_\Omega(X)$ *is the algebra* $\bigcup_{i\in\mathbb{N}} X_i$ *as described in Lemma 3.1.10.*

Proof. We claim the inclusion $\eta_X : X \to F_\Omega(X)$ defined by $\eta_X(x) = x$ for all $x \in X$ is the desired function so that for every $\alpha : X \to A$ there is a unique Ω-algebra homomorphism $\phi : F_\Omega(X) \to A$ such that the diagram



commutes, where A is some Ω-algebra. We claim that the unique morphism ϕ can be defined inductively by,

$$\phi(t) = \begin{cases} \alpha(t) & \text{if } t \in X_0 \\ \omega(\phi(t_1), ...\phi(t_n)) & \text{if } t = (\omega, t_1, ..., t_n) \in X_{i+1} - X_i \text{ for some } i \in \mathbb{N} \end{cases}$$

where in the second case ω is an n-ary operation for some arbitrary $n \in \mathbb{N}$ and $t_1, ..., t_n \in X_i$.

It is clear that the diagram commutes since for $x \in X$ $\phi\eta_X(x) = \phi(x) = \alpha(x)$ by definition. In order to see that ϕ is a homomorphism note that for any n-ary operation ω and any $t_1, ..., t_n \in F_\Omega(X)$ we have $\omega(t_1, ..., t_n) = (\omega, t_1, ..., t_n)$. We also have that there exists some smallest $k \in \mathbb{N}$ such that $t_1, ..., t_n \in X_k$, and hence $(\omega, t_1, ..., t_n) \in X_{k+1} - X_k$. Therefore $\phi(\omega(t_1, ..., t_n)) = \phi((\omega, t_1, ...t_n)) = \omega(\phi(t_1), ..., \phi(t_n))$ and so ϕ is a homomorphism.

Lastly, we must prove that if ψ is a morphism such that $\psi\eta_X = \alpha$ then $\psi = \phi$. We do this by induction. First notice that for $x \in X_0$ we must have $x \in X$ and so $\psi(x) = \psi\eta_X(x) = \alpha(x) = \phi(x)$. Now we assume that $\phi(x) = \psi(x)$ for all $x \in X_i$ and show that $\phi(t) = \psi(t)$ for all $t \in X_{i+1}$. The only non-trivial cases we need to consider are those where $t \in X_{i+1} - X_i$, and $t = \omega(t_1, ..., t_n)$ for some $\omega \in \Omega_n$ and some $t_1, ..., t_n \in X_i$. Then

$$\psi(\omega(t_1, .., t_n)) = \omega(\psi(t_1), ..., \psi(t_n)) = \omega(\phi(t_1), ..., \phi(t_n)) = \phi(\omega(t_1, ..., t_n)).$$

Thus $\psi(t) = \phi(t)$ for all $t \in X_{i+1}$ and so by induction, $\phi(t) = \psi(t)$ for $t \in \bigcup_{i \in \mathbb{N}} X_i = F_\Omega(X)$. Therefore, $F_\Omega(X)$ is the free Ω-algebra over X. □

Note 3.1.16. It is worth noting some details of the structures defined in the above proofs:

- The process we use in order to construct $F_\Omega(X)$ in Lemma 3.1.10 can be seen intuitively as follows. Our free monoid $F_{\mathbf{Mon}}(X \cup \Omega)$ corresponds to the set of any finite list of symbols in X and Ω. Then, in order to derive the free Ω-algebra over X, we want to take every list of symbols in $F_{\mathbf{Mon}}(X \cup \Omega)$ which is "well-defined" in an Ω-algebra, by ensuring that for any set of m terms in $F_\Omega(X)$ that their image under an m-ary operation in Ω is still contained in $F_\Omega(X)$. Therefore, for each X_{i+1}, we include all the terms in our previous set X_i and "add" every image of the terms in X_i under the operations in Ω. By doing this for every X_n with $n \in \mathbb{N}$, we ensure that $F_\Omega(X)$ is, in fact, closed under its operations.
- In the above proof, the inductive definition of ϕ can be seen as follows. If $x \in X_0$, then $x \in X$ and we simply define $\phi(x)$ to be $\alpha(x)$. Then if $t \in X_1$, then either t is an element of X or $t = (\omega, x_1, ..., x_n)$ for some $\omega \in \Omega_n$ and some $x_1, .., x_n \in X$. In the first case, $\phi(t) = \alpha(t)$ and in the second case $\phi(\omega, x_1, ..., x_n) = \omega(\phi(x_1), ..., \phi(x_n)) = \omega(\alpha(x_1), ..., \alpha(x_n))$ and so this value is well-defined. For $t \in X_2$ then either $t \in X_1$ or $t = (\omega', t_1, ..., t_m)$ for some $\omega' \in \Omega_m$ and some $t_1, .., t_m \in X_1$. In the first case, we have seen how this value is well-defined. In the second case $\phi(\omega', t_1, ..., t_m) = \omega'(\phi(t_1), ..., \phi(t_m))$ and since we know the value of each $\phi(t_j)$ for $j \in \{1, ..., m\}$ then the value for $\phi(t)$ is well-defined. Repeating this process, we can see how the inductive definition for ϕ in Lemma 3.1.15 does give us a well-defined function.

3.2 (Ω, Φ)-Algebras

In this section we define a relation $\models$ between the objects in $\mathbf{Alg}(\Omega)$ and the product $F_\Omega(X) \times F_\Omega(X)$ where X is a countably infinite set. Then, we consider the Galois connection induced by this relation, and use this connection to define a variety of universal algebras.

Definition 3.2.1. [1]**.** Let X be a countably infinite set, and let $\mathbf{Alg}(\Omega)_0$ be the class of objects in the category $\mathbf{Alg}(\Omega)$. Then we define the relation $\models \subseteq \mathbf{Alg}(\Omega)_0 \times (F_\Omega(X) \times F_\Omega(X))$ by $A \models (t, t')$ if and only if $m(t) = m(t')$ for every $m \in \hom(F_\Omega(X), A)$.
If $A \models (t, t')$ we say that A **satisfies** (t, t') or that (t, t') **holds in** A. We often denote this by saying $t = t'$ in A.

We now consider the Galois connection between the subsets of $\mathbf{Alg}(\Omega)_0$ and $(F_\Omega(X) \times F_\Omega(X))$ induced by $\models$. Consider a set $\Phi \subseteq F(X) \times F(X)$ and a class of Ω-algebras $\mathcal{A} \subseteq \mathbf{Alg}(\Omega)_0$. Then taking their images under the Galois connection we have that,

$$\Phi^* = \{A \in \mathbf{Alg}(\Omega)_0 \mid A \vDash (t,t') \text{ for all } (t,t') \in \Phi\}$$

$$\mathcal{A}^* = \{(t,t') \in F_\Omega(X) \times F_\Omega(X) \mid A \vDash (t,t') \text{ for all } A \in \mathcal{A}\}$$

That is, Φ^* consists of every Ω-algebra A such that every identity in Φ holds in A, and $\mathcal{A}^*$ consists of all the pairs of terms which can be considered equal in every $A \in \mathcal{A}$. We call Φ^* the class of **models** of Φ, and the set $\mathcal{A}^*$ the **algebraic theory** of $\mathcal{A}$. We can also consider the closures of Φ and $\mathcal{A}$ induced by the given Galois connection, which are described by,

$$\Phi^{**} = \{(t,t') \in F_\Omega(X) \times F_\Omega(X) \mid A \vDash (t,t') \text{ for any } A \in \mathbf{Alg}(\Omega)_0 \text{ such that } A \vDash (a,a') \text{ for all } (a,a') \in \Phi\}$$

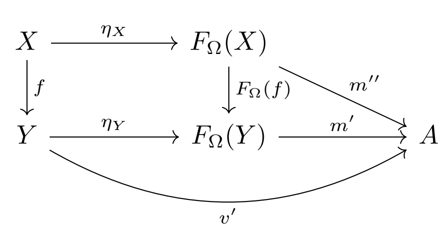
$$\mathcal{A}^{**} = \{B \in \mathbf{Alg}(\Omega)_0 \mid B \vDash (t,t') \text{ for any } (t,t') \in F_\Omega(X) \times F_\Omega(X) \text{ such that } A \vDash (t,t') \text{ for every } A \in \mathcal{A}\}$$

The set Φ^{**} then describes the full set of identities which hold in every model of Φ, and $\mathcal{A}^{**}$ describes the class of every algebra which is a model of the algebraic theory of $\mathcal{A}$. In general, we consider the pair (Ω, Φ) to be an **algebraic theory** in which the set Φ is called the **axioms** of the theory.

Lemma 3.2.2. [1]**.** *Let Ω be a signature, and let (t,t') be an element of $F_\Omega(X) \times F_\Omega(X)$ for a given set X. Then let $f : X \to Y$ be an injection and A be an Ω-algebra. Then $m(t) = m(t')$ for all $m \in hom(F_\Omega(X), A)$ if and only if $m'F_\Omega(f)(t) = m'F_\Omega(f)(t')$ for every $m' \in hom(F_\Omega(Y), A)$.*

Proof. For the first implication, let us assume that $m(t) = m(t')$ for all $m \in \hom(F_\Omega(X), A)$. Then, in particular, for any injection $f : X \to Y$, and any morphism $m' \in \hom(F_\Omega(Y), A)$, we have $m'F_\Omega(f) \in \hom(F_\Omega(X), A)$. Hence $m'F_\Omega(f)(t) = m'F_\Omega(f)(t')$.

In order to prove the converse, we assume that $m'F_\Omega(f)(t) = m'F_\Omega(f)(t')$ for all $m' \in \hom(F_\Omega(Y), A)$. Then consider $m \in \hom(F_\Omega(X), A)$. Note that m is uniquely determined by its restriction on X. That is, the map $v : X \to A$ such that $v\eta_X = m$. Moreover, any $m' \in \hom(F_\Omega(Y), A)$ is uniquely determined by the map $v' : Y \to A$ such that $v'\eta_Y = m'$. Consider the diagram



where m'' is the unique map such that $v'f = m''\eta_X$. We must have that $m'F_\Omega(f)\eta_X = m'\eta_Y f = v'f$ and so by uniqueness of m'' we get $m'F_\Omega(f) = m''$. Hence, if we show that each map $v : X \to A$ is equal to $v'f$ for some $v' : Y \to A$, we have that every morphism $m \in \hom(F_\Omega(X), A)$ is equal to $m'F_\Omega(f)$ for some $m' \in \hom(F_\Omega(Y), A)$. Then, for each v as above, we can define $v' : Y \to A$ such that for each $y \in f(X)$, $v'(y) = v(x)$ where $x \in f^{-1}(\{y\})$. Then, since f is injective, $f^{-1}(\{y\})$ is a singleton set for each $y \in f(X)$ and so this map is well defined and has the property $v = v'f$. Hence, any $m \in \hom(F_\Omega(X), A)$ is equal to $m'F_\Omega(f)$ for some $m' \in \hom(F_\Omega(Y), A)$, and so $m(t) = m'F_\Omega(f)(t) = m'F_\Omega(f)(t') = m(t')$ and we are done. □

Corollary 3.2.3. *If X is a countably infinite set and Y is any set, then an identity $(s, s') \in F_\Omega(Y) \times F_\Omega(Y)$ is equivalent to an identity $(t, t') \in F_\Omega(X) \times F_\Omega(X)$.*

Proof. Let (s, s') be an element in $F_\Omega(Y) \times F_\Omega(Y)$. Then since s, s' are members of $\bigcup_{n \in \mathbb{N}} (Y \cup \Omega)^n$, the entries of s, s' consist of a finite subset of $Y \cup \Omega$. Consider the elements of Y which are entries in s or s', and call this set Y_0. Since $Y_0 \subseteq Y$, we have $F_\Omega(Y_0) \subseteq F_\Omega(Y)$ and $s, s' \in F_\Omega(Y_0)$. Moreover, for each $m \in \hom(F_\Omega(Y), A)$, the values of $m(s)$ and $m(s')$ are determined by the restriction of m on $F_\Omega(Y_0)$. Hence, $m(s) = m(s')$ for all $m \in \hom(F_\Omega(Y), A)$ if and only if $m'(s) = m'(s')$ for all $m' \in \hom(F_\Omega(Y_0), A)$. Then, since Y_0 is finite and X is infinite there exists some injection $f : Y_0 \to X$, and by Lemma 3.2.2 we must have that $m'(s) = m'(s')$ for all $m' \in \hom(F_\Omega(Y_0), A)$ if and only if $m''F_\Omega(f)(s) = m''F_\Omega(f)(s')$ for all $m'' \in \hom(F_\Omega(X), A)$. Then, if we choose $t = F_\Omega(f)(s)$ and $t' = F_\Omega(f)(s')$, then (t, t') is an equivalent identity in A to (s, s'). □

Convention 3.2.4. *For the rest of this chapter we will treat X as a fixed countably infinite set, unless otherwise specified, and treat the relation $\vDash$ and its corresponding Galois connection as induced by this set X (or equivalently by any other countably infinite set X'). From Corollary 3.2.3 we know that we are able to express any desired identity in this way.*

Definition 3.2.5. Let Ω be an algebraic signature, and Φ be a set of formulas in $F_\Omega(X) \times F_\Omega(X)$. Then $A = (A, v)$ is an **(Ω, Φ)-algebra** if it is an Ω-algebra such that $A \in \Phi^*$. We write $A \in \mathbf{Alg}(\Omega, \Phi)$ to say that A is an object of $\mathbf{Alg}(\Omega, \Phi)$. The category $\mathbf{Alg}(\Omega, \Phi)$ of (Ω, Φ)-algebras is the full subcategory of $\mathbf{Alg}(\Omega)$ with its objects being the class of (Ω, Φ)-algebras. The category $\mathbf{Alg}(\Omega, \Phi)$ for some chosen Ω and Φ is also called a **variety of universal algebra**.

Corollary 3.2.6. *If $\mathcal{K}$ is a class of Ω-algebras, then $\mathcal{K}^{**}$ is the smallest variety containing $\mathcal{K}$.*

Proof. Clearly if $\mathcal{K} \subseteq \mathbb{V}$ then $\mathcal{K}^{**} \subseteq \mathbb{V}^{**} = \mathbb{V}$, since if $\mathbb{V}$ is a variety, it is the category of all $(\Omega, \mathbb{V}^*)$-algebras, and so it is equal to $\mathbb{V}^{**}$. □

Note 3.2.7. Our construction of (Ω, Φ)-algebras provides us with a structure on universal algebras which can provide not only a list of algebraic operations for the algebra, but also a set of equations which define how the operations behave. Types of (Ω, Φ)-algebras include many well-known algebraic structures as can be seen in the examples below.

Example 3.2.8. Recall that a semigroup $(S, \cdot)$ is a set S equipped with a binary operation $\cdot : S \times S \to S$, such that the operation is associative. That is, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for all $a, b, c \in S$. The category of semigroups, can be considered an (Ω, Φ)-algebra, where S is the underlying set and $\Omega = \{\cdot\}$ and $l_\Omega(\cdot) = 2$. Then $\Phi \subseteq F_\Omega(X) \times F_\Omega(X)$ is given by,

$$\Phi = \{((\cdot, x, \cdot, y, z), (\cdot, \cdot, x, y, z))\}$$

where $x, y, z \in X$. If S is an (Ω, Φ)-algebra, for any $a, b, c \in S$, we can choose a function $m' : X \to S$ such that $m'(x) = a$, $m'(y) = b$, $m'(z) = c$. Then, since m' uniquely extends to a morphism $m : F_\Omega(X) \to S$, we get that $m((x \cdot y) \cdot z) = m(x \cdot (y \cdot z))$ and therefore,

$$(a \cdot b) \cdot c = (m(x) \cdot m(y)) \cdot m(z) = m((x \cdot y) \cdot z) = m((x \cdot (y \cdot z)) = m(x) \cdot (m(y) \cdot m(z)) = a \cdot (b \cdot c)$$

for all $a, b, c \in S$.

Example 3.2.9. The category $\mathbf{Alg}(\Omega)$ for any Ω is equivalent to the category $\mathbf{Alg}(\Omega, \Phi)$ when $\Phi = \emptyset$.

Example 3.2.10. The category **Bool** can also be seen as a category of (Ω, Φ)-algebras. In this case $\Omega = \{0, 1, \neg, \vee, \wedge\}$ where 0 and 1 are nullary operations, $\neg$ is a unary operation and $\wedge$ and $\vee$ are binary operations. Each axiom of Boolean algebras corresponds to an element of $F_\Omega(X) \times F_\Omega(X)$ as follows, where $x, y, z \in X$.

- **Associativity** of $\wedge$ and $\vee$ corresponds to

  $$\phi_1 = ((\wedge, x, \wedge, y, z), (\wedge, \wedge, x, y, z)) \text{ and } \phi_2 = ((\vee, x, \vee, y, z), (\vee, \vee, x, y, z))$$

  respectively.

- **Commutativity** of $\wedge$ and $\vee$ corresponds to

  $$\phi_3 = ((\wedge, x, y), (\wedge, y, x)) \text{ and } \phi_4 = ((\vee, x, y), (\vee, y, x))$$

  respectively.

- **Idempotentcy** of $\wedge$ and $\vee$ corresponds to

$$\phi_5 = ((\wedge, x, x), x) \text{ and } \phi_6 = ((\vee, x, x), x)$$

respectively

- The **absorption** properties are represented by,

$$\phi_7 = ((\wedge, x, \vee, x, y), x) \text{ and } \phi_8 = ((\vee, x, \wedge, x, y), x)$$

- The fact that 0 and 1 are **identities** can be given by

$$\phi_9 = ((\wedge, x, 1), x) \text{ and } \phi_{10} = ((\vee, x, 0), x)$$

- The **distributivity** properties can be given by

$$\phi_{11} = ((\wedge x, \vee, y, z), (\vee, \wedge, x, y, \wedge, x, z)) \text{ and } \phi_{12} = ((\vee x, \wedge, y, z), (\wedge, \vee, x, y, \vee, x, z))$$

- The definition of the **complement** is given by

$$\phi_{13} = ((\wedge, x, \neg, x), 0) \text{ and } \phi_{14} = ((\vee, x, \neg, x), 1)$$

Then taking $\Phi = \{\phi_i \mid i \in \{1, ..., 14\}\}$, we obtain that B is a Boolean algebra if and only if it is an (Ω, Φ)-algebra for the chosen values of Ω and Φ.

Example 3.2.11. It is also worth noting that for each Ω, the **trivial** variety of Ω-algebras is the variety $\mathbb{V} = \mathrm{Alg}(\Omega, \Phi)$ where there is an element (x, y) in Φ such that $x, y \in X$ and $x \neq y$. In this case, any object $A \in \mathbb{V}$ has at most one-element. Since we have that $m(x) = m(y)$ for every $m \in \hom(F_\Omega, X)$, for any $a, b \in A$, we can find $f : X \to A$ such that $f(x) = a$ and $f(y) = b$. The function f can then be extended uniquely to a morphism $f' : F_\Omega(X) \to A$ such that $f'(x) = f(x) = f(y) = f'(y)$ and so $a = b$. That is, any two elements of A are equal and so any non-empty $A \in \mathbb{V}$ has only one element.

We now show how certain types of morphisms can be characterized in a variety.

Lemma 3.2.12. *Let $f : A \to B$ be a morphism in a variety $\mathbb{V}$. Then the following holds:*

a. If f is an injection, then it is a monomorphism *b. If f is a surjection, then it is an epimorphism.*

c. f is an isomorphism if and only if it is a bijection.

Proof. a. Assume f is an injection and consider $u, v : C \to A$ such that $fu = fv$. Then, $fu(x) = fv(x)$ for all $x \in C$, and so by the injectivity of f, then $u(x) = v(x)$ for all $x \in C$. Hence $u = v$.

b. Assume f is a surjection and consider $u, v : A \to C$ such that $uf = vf$. Then $uf(a) = vf(a)$ for all $a \in A$. But since f is surjective, for all $b \in B$ there exists some $a \in A$ such that $b = f(a)$, and so $u(b) = v(b)$ for all $b \in B$ and so $u = v$.

c. Assume that f is bijective and then define the morphism $f^{-1} : B \to A$ by $f^{-1}(b) = a$ where a is the unique element of A such that $f(a) = b$. Note that such an a exists for each b since by the surjectivity of f we have for all $b \in B$, that there exists a $a \in A$ such that $f(a) = b$. Moreover, since f is injective, if $f(a) = f(a') = b$ then $a = a'$ and so, a is unique. Clearly it is an inverse function to f. Moreover, f^{-1} is a homomorphism since for $\omega \in \Omega$ we have,

$$f^{-1}(\omega(b_1, ..., b_n)) = f^{-1}\omega(f(a_1), ..., f(a_n)) = f^{-1}f(\omega(a_1, ..., a_n)) = \omega(a_1, ..., a_n) = \omega(f^{-1}(b_1), ..., f^{-1}(b_n)).$$

Conversely, if f is an isomorphism then it is injective since whenever $f(a) = f(b)$, $a = f^{-1}f(a) = f^{-1}f(b) = b$. It is surjective since for each $b \in B$ the element $f^{-1}(b) \in A$ is such that $ff^{-1}(b) = b$.

□

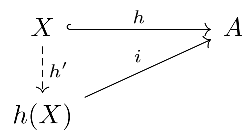
Note 3.2.13. In part b. of the above lemma note that the converse implication does not hold. For a counterexample consider the inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Q}$ in the category (or variety) **Rng** of rings [13]. Consider, $u, v : \mathbb{Q} \to R$ are ring homomorphisms such that $u(z) = v(z)$ for all $z \in \mathbb{Z}$. Note that the corestriction of u (or v) onto its image preserves multiplicative, inverses since $u(q)u(q^{-1}) = u(q \cdot q^{-1}) = u(1)$, and therefore $u(q^{-1}) = u(q)^{-1}$, and similarly $v(q^{-1}) = v(q)^{-1}$. Then, each $q \in \mathbb{Q}$ is equal to $\frac{x}{y}$ for $x, y \in \mathbb{Z}$. Hence $u(q) = u(x)u(y^{-1})$. Then, since $u(y) = v(y)$ we have that $u(y^{-1})v(y) = u(1) = v(1)$, and therefore $v(y)^{-1} = u(y^{-1})$, where $v(y)^{-1}$ is the inverse of $v(y)$ in the image of v. Thus, $u(q) = v(x)v(y)^{-1} = v(x)v(y^{-1}) = v(x \cdot y^{-1}) = v(q)$ and so $u = v$. Hence, the inclusion is an epimorphism, but is clearly not surjective. The converse to part a. of the above will be proved later in this chapter in Corollary 3.5.7.

3.3 Subalgebras

Definition 3.3.1. Let A be an Ω-algebra. Then a **subalgebra** of A is an Ω-algebra B such that the underlying set B is a subset of A. That is, $B \subseteq A$ such that, for any n-ary operation $\omega \in \Omega$ and for all $b_1, ..., b_n \in B$, we have $\omega(b_1, ..., b_n) \in B$.

Lemma 3.3.2. *Let X and A be Ω-algebras. If $h : X \to A$ is an injective homomorphism then $X \cong B$ for a subalgebra of A.*

Proof. Consider the diagram



where $h(X) = \{h(x) \mid x \in X\}$, the morphism h' is defined by $h'(x) = h(x)$ and i is the inclusion morphism.

First we note that since h is a morphism then $h(\omega(x_1, ..., x_n)) = \omega(h(x_1), ..., h(x_n))$ for each n-ary operation $\omega \in \Omega$ and all $x_1, ..., x_n \in X$. Therefore $h(X)$ is closed under each $\omega \in \Omega$ and is closed under a subalgebra of A.

Next notice that since h is injective, h' is also injective. Furthermore, by definition h' is surjective since for any $h(x) \in h(X)$ we have $h'(x) = h(x)$. □

Convention 3.3.3. *We can then see that each injective morphism into A can be identified up to isomorphism with a subalgebra of A. This is a specific instance of the more general idea of a subobject of A in a general category $\mathbb{C}$ as is given by Mac Lane [13]. We will also adopt the convention of referring to a subalgebra of A up to isomorphism as an Ω-algebra S equipped with an injection $f : S \to A$. Then, if $\mathcal{K}$ is a class of Ω-algebras. We say that $\mathcal{K}$ is **closed under subalgebras** if for any $A \in \mathcal{K}$ and any injection $f : S \to A$ we have that $S \in \mathcal{K}$.*

Lemma 3.3.4. *Any variety of Ω-algebras is closed under subalgebras.*

Proof. Let $\mathbf{Alg}(\Omega, \Phi)$ be a variety and let A be an object of $\mathbf{Alg}(\Omega, \Phi)$. Now suppose $f : S \to A$ is an injective morphism in $\mathbf{Alg}(\Omega)$. We want to show that S is an (Ω, Φ)-algebra.

Let (t, t') be an element of Φ and consider any Ω-algebra morphism $m : F_\Omega(X) \to S$. Then since $A \in \mathbf{Alg}(\Omega, \Phi)$, we have that $fm(t) = fm(t')$. But then since f is an injection $m(t) = m(t')$ and so $S \vDash (t, t')$ for all $(t, t') \in \Phi$. □

Corollary 3.3.5. *Any variety $\mathbb{V}$ is closed under isomorphism.* □

3.4 Product Algebras

Definition 3.4.1. Let $(A_i)_{i \in I}$ be a family of Ω-algebras. Then the **product** algebra of the family $(A_i)_{i \in I}$, denoted $\prod_{i \in I} A_i$, is the product of the underlying sets of each A_i equipped with the following algebraic structure. For any n-ary operation $\omega \in \Omega$ and for all $(a_{i1})_{i\in I}, ..., (a_{in})_{i\in I} \in \prod_{i\in I} A_i$,

$$\omega((a_{1i})_{i\in I}, ..., (a_{ni})_{i\in I}) = (\omega(a_{1i}, ..., a_{ni}))_{i\in I}.$$

In a finitary case, we have that the product of $A_1, ..., A_n$ has the underlying set $A_1 \times ... \times A_n$ and each n-ary operation ω is defined by $\omega(a_1, ..., a_n) = (\omega(a_1), ..., \omega(a_n))$ for any $(a_1, ..., a_n) \in A_1 \times ... \times A_n$.

Note 3.4.2. Recall the definition of a product of a family of objects $(A_i)_{i\in I}$ in a general category $\mathbb{C}$ is given by the pair $(\prod_{i\in I} A_i, \pi_i)$ where $\prod_{i\in I} A_i$ is an object of $\mathbb{C}$ and $\pi_i : \prod_{i\in I} A_i \to A_i$ is a family of morphisms such that, for any family of morphisms $f_i : Y \to A_i$ in $\mathbb{C}$, there exists a unique morphism $f : Y \to \prod_{i\in I} A_i$ such that the diagram

$$\begin{array}{ccc} & & \prod_{i\in I} A_i \\ & \overset{f}{\dashrightarrow} & \downarrow \pi_i \\ Y & \xrightarrow{\quad f_i \quad} & X_i \end{array}$$

commutes for each $i \in I$. [13]

This definition corresponds with definition 3.4.1 above, where we define $\pi_j : (a_i)_{i\in I} \mapsto a_j$ for each $j \in I$ and $f : y \mapsto (f_i(y))_{i\in I}$. Thus, the product of a family of Ω-algebras is a specific instance of a general product of objects in a category.

Lemma 3.4.3. *If $\mathbb{V} = \boldsymbol{Alg}(\Omega, \Phi)$ is a variety and $A_i \in \mathbb{V}$ for all $i \in I$, then $\prod_{i\in I} A_i \in \mathbb{V}$. That is, varieties are closed under products.*

Proof. Consider the diagram

$$F_\Omega \xrightarrow{\quad m \quad} \prod_{i\in I} A_i \xrightarrow{\quad \pi_i \quad} A_i$$

where each π_i is defined as above and m is any Ω-algebra morphism. Since each $A_i \models (t, t')$ for $(t, t') \in \Phi$, we have that $\pi_i m(t) = \pi_i m(t')$ for every $i \in I$. But then by the definition of π_i, this means that each entry in $m(t)$ and $m(t')$ are equal, and so $m(t) = m(t')$, and hence $\prod_{i\in I} A_i \models (t, t')$. $\square$

3.5 Congruences and Quotient Algebras

Definition 3.5.1. If A is an Ω-algebra, then $E \subseteq A \times A$ is a congruence on A if it is a subalgebra of $A \times A$ such that it is an equivalence relation.

Corollary 3.5.2. *If $A \in \mathbb{V}$ for some variety $\mathbb{V} = \boldsymbol{Alg}(\Omega, \Phi)$ then any congruence of A is in $\mathbb{V}$.*

Proof. This follows from Lemma 3.3.4 and Lemma 3.4.3, since any congruence of A is a subalgebra of a product of A. $\square$

Lemma 3.5.3. [2]**.** *Let $Con(A)$ be the set of congruences on A. Then $Con(A)$ is a complete lattice ordered by $\subseteq$.*

Proof. Let $\{E_i\}_{i\in I}$ be a family of congruences on A. We define the meet of $\{E_i\}_{i\in I}$ as the intersection $\bigcap_{i\in I} E_i$. This intersection is reflexive since $(a,a) \in E_i$ for all $i \in I$. Moreover if $(a,b) \in \bigcap_{i\in I} E_i$ then (a,b) and (b,a) are both elements of each E_i and so $(b,a) \in \bigcap_{i\in I} E_i$. Lastly, if $(a,b),(b,c) \in \bigcap_{i\in I} E_i$ then $(a,b),(b,c) \in E_i$ which implies $(a,c) \in E_i$ for all $i \in I$, hence $(a,c) \in \bigcap_{i\in I} E_i$.

We also have that if $(a_1,a_1'),...,(a_n,a_n') \in \bigcap_{i\in I} E_i$, for any n-ary operation $\omega \in \Omega$, it follows that $\omega((a_1,a_1'),...,(a_n,a_n')) \in E_i$ for all $i \in I$ $\omega((a_1,a_1'),...,(a_n,a_n')) \in \bigcap_{i\in I} E_i$.

We define the join $\bigvee_{i\in I} E_i$ as $\bigcap_{j\in J} E_j$ where each $\{E_j\}_{j\in J}$ is the family of congruences such that for each $j \in J$, $E_i \subseteq E_j$ for each $i \in I$. Clearly, by the previous paragraph $\bigvee_{i\in I} E_i$ is a congruence. Moreover, it is clear that $E_i \subseteq \bigvee_{i\in I} E_i$ for all $i \in I$, and if $E_i \subseteq E$ for all $i \in I$, we have by definition that $E = E_j$ for some $j \in J$, and $\bigvee_{i\in I} E_i = \bigcap_{j\in J} E_j \leq E$. Therefore $\bigvee_{i\in I} E_i$ is the join of $\{E_i\}_{i\in I}$. $\square$

Definition 3.5.4. Let A be an Ω-algebra and let E be a congruence on A. Then the **quotient algebra** A/E is the set of equivalence classes,

$$A/E = \{[a]_E \mid a \in A\} \text{where for each } a \in A,\ [a]_E = \{b \in A \mid (a,b) \in E\}.$$

and each n-ary operation $\omega \in \Omega$ is defined on A/E by

$$\omega([a_1]_E,...,[a_n]_E) = [\omega(a_1,...,a_n)]_E.$$

We will write $[a]_E$ as $[a]$ when it is clear which congruence is generating the equivalence classes.

Note 3.5.5. If $[a_1]_E = [a_1']_E, ...[a_n]_E = [a_n']_E$, then $(a_1,a_1'),...,(a_n,a_n') \in E$, and since E is a congruence $\omega((a_1,a_1'),...,a_n,a_n') = (\omega(a_1,...,a_n),\omega(a_1',...,a_n')) \in E$. Therefore $[\omega(a_1,...,a_n)]_E = [\omega(a_1',...,a_n')]_E$. Hence, the definition of ω given above is well-defined.

Lemma 3.5.6. *An equivalence class E on an Ω-algebra A is a congruence if and only if there exists some Ω-algebra homomorphism $f : A \to B$ such that $E = \{(a,b) \mid f(a) = f(b)\}$.*

Proof. If E is a congruence, consider the canonical map $q : A \to A/E$ defined by $a \mapsto [a]$. This map is clearly a homomorphism and furthermore has the desired property. Specifically, $q(a) = q(b)$ if and only if $[a] = [b]$ if and only if $(a, b) \in E$.

For the converse implication, assume $f : A \to B$ is a homomorphism and consider the relation $E_f = \{(a, b) \mid f(a) = f(b)\}$. Then it is clear that $f(a) = f(a)$, $f(a) = f(b)$ implies $f(b) = f(a)$ and $f(a) = f(b), f(b) = f(c)$ implies that $f(a) = f(c)$. Therefore, E_f is an equivalence relation.

Now consider $(a_1, a_1'), ..., (a_n, a_n') \in E_f$ and an n-ary operation $\omega \in \Omega$. Note that since $f(a_1) = f(a_1')$,...,$f(a_n) = f(a_n')$ we get that $\omega(f(a_1), ..., f(a_n)) = \omega(f(a_1'), ..., f(a_n'))$ which is equivalent to $f(\omega(a_1, ..., a_n)) = f(\omega(a_1', ..., a_n'))$ and so $(\omega(a_1, ..., a_n), \omega(a_1', ..., a_n')) \in E_f$ and so E_f is a congruence. □

This result allows us to prove the converse of part a. of Lemma 3.2.12.

Corollary 3.5.7. *Every monomorphism in a variety* $\mathbb{V}$ *is injective.*

Proof. Let $f : A \to B$ be a monomorphism and consider

$$E_f \xrightarrow{\quad i \quad} A \times A \underset{\pi_2}{\overset{\pi_1}{\rightrightarrows}} A$$

where E_f is the congruence such that $(x, y) \in E_f$ if and only if $f(x) = f(y)$, i is the inclusion and π_1 and π_2 are the projection morphisms. Then clearly $f\pi_1 i = f\pi_2 i$ and hence $\pi_1 i = \pi_2 i$ and so whenever $f(a) = f(b)$ then $(a, b) \in E_f$, and so $a = \pi_1 i((a, b)) = \pi_2 i((a, b)) = b$. Thus f is injective. □

As in the construction of subalgebras, we can show that a surjective homomorphism $A \to B$ induces an isomorphism between B and a quotient algebra of A.

Lemma 3.5.8. *If* $h : A \to B$ *is a surjective* Ω*-algebra homomorphism, then* B *is isomorphic to a quotient algebra of* A.

Proof. We consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{\quad q \quad} & A/E_h \\ & \searrow^{h} & \downarrow g \\ & & B \end{array}$$

where q is the canonical map, E_h is defined as in Lemma 3.5.6 and we define g by $g([a]) = h(a)$ for each $[a] \in A/E_h$. Clearly g is a well-defined homomorphism since h is a homomorphism and if $[a] = [a']$ by definition $h(a) = h(a')$ and so $g([a]) = h(a) = h(a') = g([a'])$.

Then since h is surjective, g is also surjective, and lastly if $g([a]) = g([a'])$ then $h(a) = h(a')$ and so $[a] = [a']$ which gives us that g is injective. □

Convention 3.5.9. *Similar to the case for subalgebras, we will refer to quotient algebras of A up to isomorphism as an Ω-algebra B equipped with a surjective morphism $A \to B$.*

Corollary 3.5.10. *For any Ω-algebra morphism $f : A \to B$, the corestriction of f to its image, $f' : A \to f(A)$ defined by $f'(a) = f(a)$ for all $a \in A$ is a quotient algebra up to isomorphism.*

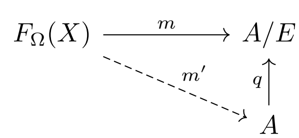
Proof. It is clear that the map f' is surjective by definition. Moreover, since f is a homomorphism, then for any selection of elements $f(a_1), ..., f(a_n) \in f(A)$ and any n-ary operation $\omega \in \Omega$ we have that $\omega(f(a_1), ..., f(a_n)) = f(\omega(a_1, .., a_n)) \in f(A)$ and so $f(A)$ is an Ω-algebra equipped with a surjection, and so is a quotient algebra of A, up to isomorphism. In fact, $f(A)$ is isomorphic to the quotient algebra A/E_f, since $(a, b) \in E_f$ if and only if $f'(a) = f(a) = f(b) = f'(b)$. □

Due to the above result, in some literature, quotient algebras are referred to as homomorphic images.

Definition 3.5.11. Let $\mathcal{K}$ be a class of Ω-algebras. We say that $\mathcal{K}$ is **closed under quotients** if for any $A \in \mathcal{K}$ and any surjection $f : A \to B$ we have that $B \in \mathcal{K}$.

Lemma 3.5.12. *Any variety of Ω-algebras is closed under quotients.*

Proof. If $f : A \to B$ is a surjective Ω-algebra homomorphism and $A \in \mathbb{V}$ for some variety $\mathbb{V}$, then B is isomorphic to A/E for some congruence E on A. It therefore suffices to prove that A/E is in $\mathbb{V}$ for each $E \in \mathrm{Con}(A)$. Consider the diagram



where m is any Ω-algebra homomorphism, q is the canonical morphism, and we define $m' : F_\Omega(X) \to A$ inductively by $m'(x) = a$ for some $a \in m(\{x\})$, whenever $x \in X$, and $m'(t) = m'(\omega(t_1, ..., t_n)) = \omega(m'(t_1), ..., m'(t_n))$ for $\omega(t_1, ..., t_n) \in F_\Omega(X) - X$. This map is well-defined since an element $a \in m(\{x\})$ exists for all $x \in X$, and is clearly a Ω-algebra homomorphism. Moreover, it makes the diagram commute since, if $x \in X$ then $qm'(x) = q(a) = [a] = m(x)$, since $a \in m(x)$. Then, using the notation in Lemma 3.1.10 we assume that for $t \in X_k$ that $qm'(t) = m(t)$. Now let $u \in X_{k+1}$, then either $u \in X_k$ or $u = \omega(t_1, ..., t_n)$ for $t_1, ..., t_n \in X_k$ and some n-ary operation $\omega \in \Omega$. In the first case, by assumption $qm'(u) = m(u)$, in the second case $qm'(\omega(t_1, ..., t_n)) = \omega(qm'(t_1), ..., qm'(t_n)) = \omega(m(t_1), .., m(t_n)) = m(\omega(t_1, ..., t_n))$ $qm'(u) = m(u)$ for all $u \in X_{k+1}$. Therefore, by induction we have that $qm' = m$ and so the diagram above commutes.

Then, if $A \vDash (t, t')$ we have that $m'(t) = m'(t')$, and so $m(t) = qm'(t) = qm'(t') = m(t')$, and so $A/E \vDash (t, t')$. In particular, if A is in a variety $\mathbf{Alg}(\Omega, \Phi)$ with a set of axioms Φ, then $A/E \vDash (t, t')$ for all $(t, t') \in \Phi$. □

The last result that we will prove is often referred to as the Second Isomorphism Theorem. The formulation of the result here is the same as that in Burris and Sankappanavar [7].

Theorem 3.5.13. *Let A be an (Ω, Φ)-algebra and let E and D be congruences on A such that $D \subseteq E$. Then the set*

$$E/D = \{([a]_D, [b]_D) \in A/D \times A/D \mid (a, b) \in E\}$$

is a congruence and $(A/D)\big/(E/D) \cong A/E$.

Proof. First let us show that E/D is a congruence. Note that if $[a]_D = [a']_D$, $[b]_D = [b']_D$ and $([a]_D, [b]_D) \in E/D$, then $(a, b) \in E$. Then, since $E \subseteq D$, we have $(a', b') \in E$ and so $([a']_D, [b']_D) \in E/D$. That is, the relation E/D is independent of the representatives of the equivalence classes in D.

In order to see E/D is an equivalence, consider that $(a, a) \in E$ for all $a \in A$ and so each $([a]_D, [a]_D) \in E/D$. Then if $([a]_D, [b]_D) \in E/D$ then $(a, b) \in E$ and so $(b, a) \in E$, hence $([b]_D, [a]_D) \in E/D$. Using a similar method, if $([a]_D, [b]_D), ([b]_D, [c]_D) \in E/D$, by the transitivity of E, we get that $([a]_D, [c]_D) \in E/D$.

To see that it is a congruence, note that if $\omega \in \Omega$ is some n-ary operation, then for $([a_1]_D, [b_1]_D), ..., ([a_n]_D, [b_n]_D) \in E/D$ we have that $(a_1, b_1), ..., (a_n, b_n) \in E$ and so $(\omega(a_1, ..., a_n), \omega(b_1, ..., b_n)) \in E$ which gives us that $(\omega([a_1]_D, ..., [a_n]_D), \omega([b_1]_D, ..., [b_n]_D) = ([\omega(a_1, ..., a_n)]_D, [\omega(b_1, ..., b_n)]_D) \in E/D$. Thus E/D is a congruence.

Then in order to see that $(A/D)\big/(E/D) \cong A/E$, consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{\quad f_D \quad} & A/D \\ \downarrow{\scriptstyle f_E} & & \downarrow{\scriptstyle f_{E/D}} \\ A/E & \xrightarrow{\quad g \quad} & (A/E)/(E/D) \end{array}$$

where f_E, f_D and $f_{E/D}$ are the canonical morphisms. From Lemma 3.5.6, f_E has the property that $f_E(a) = f_E(b)$ if and only if $(a, b) \in E$, and the other morphisms have the same property with respect to the congruence they are defined by. We define g as $g([a]_E) = [a]_{E/D}$. Note that g is a well-defined function since $(a,b) \in E$ implies that $([a]_D, [b]_D) \in E/D$. It is a homomorphism since

$$\begin{aligned} g(\omega([a_1]_E, ..., [a_n]_E)) &= g([\omega(a_1, ..., a_n)]_E) \\ &= [\omega(a_1, ..., a_n)]_{E/D} \\ &= \omega([a_1]_{E/D}, ..., [a_n]_{E/D}) = \omega(g([a_1]_E), .., g([a_n]_E)) \end{aligned}$$

for all $[a_1]_E, ..., [a_n]_E \in A/E$ and $\omega \in \Omega$. Moreover, the square commutes by this definition of g.

Observe that $g([a]_E) = g([b]_E)$ implies $[a]_{E/D} = [b]_{E/D}$ which is true if and only if $([a]_D, [b]_D) \in E/D$. But then $(a,b) \in E$ and so $[a]_E = [b]_E$ which shows that g is injective. Then clearly for each $[a]_{E/D} \in (A/E)/(E/D)$ we have that $g([a]_E) = [a]_{E/D}$ and so g is surjective. Hence g is an isomorphism. □

Corollary 3.5.14. *Let A be an (Ω, Φ)-algebra and let E and D be congruences on A such that $D \subseteq E$. Then A/E is a quotient (up to isomorphism) of A/D.* □

Lemma 3.5.15. *Let A be an algebra in a variety, $\mathbb{V}$. Then, if E and E' are congruences on A, $A/E \cap E'$ is a subalgebra of $A/E \times A/E'$.*

Proof. We claim the map,

$$h : A/E \cap E' \to A/E \times A/E'$$

defined by $h([a]_{E\cap E'}) = ([a]_E, [a]_{E'})$ is an injective homomorphism. Note that if $[a]_{E\cap E'} = [a']_{E\cap E'}$ then $(a, a') \in E$ and $(a, a') \in E'$ so h is a well-defined function. Moreover,

$$\begin{aligned} h(\omega([a_1]_{E\cap E'}, ..., [a_n]_{E\cap E'})) &= h([\omega(a_1, ..., a_n)]_{E\cap E'}) \\ &= ([\omega(a_1, .., a_n)]_E, [\omega(a_1, .., a_n)]_{E'}) \\ &= (\omega([a_1]_E, ..., [a_n]_E), \omega([a_1]_{E'}, ..., [a_n]_{E'})) \\ &= \omega(([a_1]_E, [a_1]_{E'}), ...([a_n]_E, [a_n]_{E'})) = \omega(h([a_1]_{E\cap E'}), ..., h([a_n]_{E\cap E'})). \end{aligned}$$

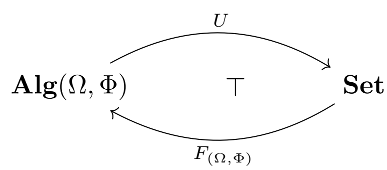
Thus, h is a homomorphism.

Lastly, if $h([a]_{E\cap E'}) = h([a']_{E\cap E'})$ then $([a]_E, [a]_{E'}) = ([a']_E, [a']_{E'})$ and therefore $(a, a') \in E$ and $(a, a') \in E'$. Hence $[a]_{E\cap E'} = [a']_{E\cap E'}$. Therefore h is injective and so $A/E \cap E'$ is a subalgebra of $A/E \times A/E'$. □

3.6 Free Algebras

In previous chapters we have constructed free algebras in the categories **Alg**(Ω), **Bool**, and **Mon**. We now define a free algebra over a set in a category of general (Ω, Φ)-algebras, and show how this can be represented as a quotient of the free Ω-algebra over the same set.

Definition 3.6.1. Consider the adjunction,



where U is the forgetful functor. The left adjoint of U, denoted $F_{(\Omega,\Phi)}$, is called the **free functor** to **Alg**(Ω, Φ). For any set X, the algebra $F_{(\Omega,\Phi)}(X)$ is called the **free** (Ω, Φ)**-algebra** over X.

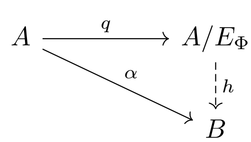
Lemma 3.6.2. [1]**.** *For any $\Phi \subseteq F_\Omega(X) \times F_\Omega(X)$, **Alg**$(\Omega, \Phi)$ is a reflective subcategory of **Alg**(Ω).*

Proof. We want to show that the inclusion functor $K : \mathbf{Alg}(\Omega, \Phi) \to \mathbf{Alg}(\Omega)$ has a left adjoint $F_\Phi : \mathbf{Alg}(\Omega) \to \mathbf{Alg}(\Omega, \Phi)$. We claim that we can define $F_\Phi(A)$ by $F_\Phi(A) = A/E_\Phi$, where $E_\Phi = \bigcap \mathcal{E}$, where $\mathcal{E}$ is the set of all congruences on A containing the set,

$$I_\Phi = \{(f(t), f(t')) \mid (t, t') \in \Phi \text{ and } f \in \hom(F_\Omega(X), A)\} \subseteq A \times A.$$

Note that for any morphism $m : F_\Omega(X) \to A/E_\Phi$, by the proof in Lemma 3.5.12 we know $m = qm'$ for some $m' : F_\Omega(X) \to A$. Therefore, for any $(t, t') \in \Phi$ we have $(m'(t), m'(t')) \in I_\Phi$, and so $m(t) = [m'(t)] = [m'(t')] = m(t')$. Hence, $A/E_\Phi \in \mathbf{Alg}(\Omega, \Phi)$.

Then note that if E is a congruence such that $A/E \in \mathbf{Alg}(\Omega, \Phi)$ then for any $f : F_\Omega(X) \to A$ we have that $[f(t)] = [f(t')]$ in A/E for any $(t, t') \in F_\Omega(X)$ (by composing f with the quotient map) and so $(f(t), f(t')) \in E$. Hence $E_\Phi \subseteq E$. Then in order to see that A/E_Φ is the free algebra over A, for any $\alpha : A \to B$ with $B \in \mathbf{Alg}(\Omega, \Phi)$ consider the diagram



where q is the canonical quotient homomorphism. Note that if a homomorphism h exists such that the diagram commutes it must be defined uniquely by $h([a]) = \alpha(a)$ for all $a \in A$, and so it is sufficient to prove that if $[a] = [a']$ in A/E_Φ, then $\alpha(a) = \alpha(a')$. Consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \downarrow{\scriptstyle q_\alpha} & & \uparrow{\scriptstyle i} \\ A/E_\alpha & \xrightarrow{\alpha'} & \alpha(A) \end{array}$$

where E_α is the congruence induced by α, α' is the isomorphism defined by $\alpha'([a]) = \alpha(a)$, and i is the inclusion. Then since A/E_α is a subalgebra of B, by Lemma 3.3.4 it is an (Ω, Φ)-algebra. But then, since E_Φ is the smallest congruence such that A/E_Φ is an (Ω, Φ)-algebra then $E_\Phi \subseteq E_\alpha$ and so $[a] = [a']$ in A/E_Φ implies that $\alpha(a) = \alpha(a')$. Hence, h exists and so F_Φ is the left adjoint to $K : \mathbf{Alg}(\Omega, \Phi) \to \mathbf{Alg}(\Omega)$. □

Corollary 3.6.3. *The free functor $F_{(\Omega,\Phi)} : \boldsymbol{Set} \to \boldsymbol{Alg}(\Omega, \Phi)$ exists.*

Proof. In order to see this we simply compose the adjunctions

$$\mathbf{Set} \underset{U}{\overset{F_\Omega}{\rightleftarrows}} \mathbf{Alg}(\Omega) \underset{K}{\overset{F_\Phi}{\rightleftarrows}} \mathbf{Alg}(\Omega, \Phi)$$

Then clearly $UK : \mathbf{Alg}(\Omega, \Phi) \to \mathbf{Set}$ is the free functor from $\mathbf{Alg}(\Omega, \Phi)$ to $\mathbf{Set}$ and so the composition $F_\Phi F_\Omega$ is the left adjoint to UK, and so $F_\Phi F_\Omega = F_{(\Omega,\Phi)}$. □

We now consider the case of the free (Ω, Φ)-algebra over the countably infinite set X.

Lemma 3.6.4. *For any $\Phi \subseteq F_\Omega(X) \times F_\Omega(X)$ we have that Φ^{**} is a congruence on $F_\Omega(X)$ where $(-)^*$ is the Galois connection defined in Definition 3.2.1.*

Proof. Suppose A is an arbitrary (Ω, Φ)-algebra.
First we show that Φ^{**} is an equivalence. Since $m(t) = m(t)$ for all $t \in F_\Omega(X)$ and any function $m : F_\Omega(X) \to A$, in particular $m(t) = m(t)$ for any Ω-algebra homomorphism $m : F_\Omega(X) \to A$. Therefore, since this is true for any $A \in \mathbf{Alg}(\Omega, \Phi)$, we have $(t, t) \in \Phi^{**}$ and so Φ^{**} is reflexive.
Then, if $(t, t') \in \Phi^{**}$ we have that $m(t) = m(t')$ for all $m \in \hom(F_\Omega(X), A)$ for any $A \in \mathbf{Alg}(\Omega, \Phi)$. But this is the same as $m(t') = m(t)$ and so $(t', t) \in \Phi^{**}$.
Lastly, if $(t, t'), (t', t'') \in \Phi^{**}$ we have $m(t) = m(t')$, $m(t') = m(t'')$, and therefore $m(t) = m(t'')$ for all $m \in \hom(F_\Omega(X), A)$ for each $A \in \mathbf{Alg}(\Omega, \Phi)$. Therefore $(t, t'') \in \Phi^{**}$.

In order to see that Φ^{**} is a congruence consider an n-ary operation $\omega \in \Omega$. Then if $(t_1, t'_1), ..., (t_n, t'_n) \in \Phi^{**}$ we have that $m(t_1) = m(t'_1), m(t_2) = m(t'_2), ..., m(t_n) = m(t'_n)$ for all $m \in \hom(F_\Omega(X), A)$ and all $A \in \mathbf{Alg}(\Omega, \Phi)$. Therefore $\omega(m(t_1), ..., m(t_n)) = \omega(m(t'_1), ..., m(t'_n))$ and so $m(\omega(t_1, ..., t_n)) = m(\omega(t'_1, ..., t'_n))$ and so $(\omega(t_1, ..., t_n), \omega(t'_1, ..., t'_n)) \in \Phi^{**}$ which proves that Φ^{**} is a congruence. □

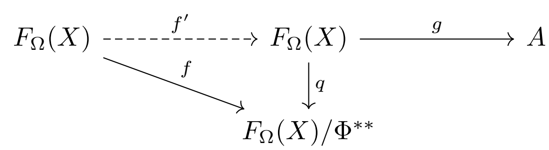
Lemma 3.6.5. *Using the same notation as above, if $\Phi \subseteq F_\Omega(X) \times F_\Omega(X)$, then Φ^{**} is the smallest congruence on $F_\Omega(X)$ such that $F_\Omega(X)/\Phi^{**}$ is an (Ω, Φ)-algebra.*

Proof. In order to prove the above statement we must prove two things:

a. $F_\Omega(X)/\Phi^{**}$ is an (Ω, Φ)-algebra.

b. If E is a congruence on$F_\Omega(X)$ such that $F_\Omega(X)/E$ is an (Ω, Φ)-algebra then $\Phi^{**} \subseteq E$.

a. In order to show that $F_\Omega(X)/\Phi^{**}$ is an (Ω, Φ)-algebra we need to show that for any homomorphism $f : F_\Omega(X) \to F_\Omega(X)/\Phi^{**}$ we have that $f(a) = f(a)$ for all $(a, a') \in \Phi$. Now for any $f \in \hom(F_\Omega(X), F_\Omega(X)/\Phi^{**})$ consider the diagram



in $\mathbf{Alg}(\Omega)$ where A is an (Ω, Φ)-algebra, q is the canonical morphism and $f' : F_\Omega(X) \to F_\Omega(X)$ is defined with respect to f in the same way that m' is defined in Lemma 3.5.12 with respect to m. Then, as in Lemma 3.5.12, the triangle commutes. Hence, we have that $f(t) = f(t')$ if and only if $[f'(t)] = [f'(t')]$ which is true if and only if $(f'(t), f'(t')) \in \Phi^{**}$.

Now note, since A is an (Ω, Φ)-algebra, then $A \vDash (a, a')$ for all $(a, a') \in \Phi$. Therefore $gf'(a) = gf'(a')$ for all $(a, a') \in \Phi$. Thus, $gf'(a) = gf'(a')$ for each $g \in \hom(F_\Omega(X), A)$. But since A is an arbitrary (Ω, Φ)-algebra, it follows that $A \vDash (f'(a), f'(a'))$ for all $A \in \Phi^*$, and so $(f'(a), f'(a')) \in \Phi^{**}$. From this we can conclude that $f(a) = f(a')$ for each $(a, a') \in \Phi$ and so $F_\Omega(X)/\Phi^{**}$ is an (Ω, Φ)-algebra.

b. Suppose E is a congruence such that $F_\Omega(X)/E$ is an (Ω, Φ)-algebra. Then for $(t, t') \in \Phi^{**}$ we have that $m(t) = m(t')$ for all $m \in \hom(F_\Omega(X), F_\Omega(X)/E)$. In particular, then for the canonical homomorphism $q : F_\Omega(X) \to F_\Omega(X)/E$ we have that $q(t) = q(t')$. Furthermore, this is true if and only if $(t, t') \in E$ and so $\Phi^{**} \subseteq E$. □

Corollary 3.6.6. *From the above, and the fact that both E_Φ and Φ^{**} have been shown to be the smallest congruence E such that $F_\Phi(X)/E$ is an (Ω, Φ)-algebra, we have that $F_\Phi(X)/\Phi^{**} = F_\Phi(X)/E_\Phi$ and so $F_\Phi(X)/\Phi^{**}$ is the free (Ω, Φ)-algebra over X.*

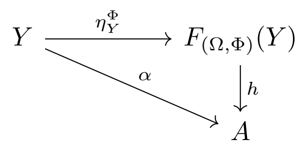
Corollary 3.6.7. *Given a signature Ω and a set of axioms Φ, the following are equivalent:*

a. $(t, t') \in \Phi^{**}$.

b. $[t] = [t']$ *in* $F_{(\Omega,\Phi)}(X)$.

Lemma 3.6.8. [2]**.** *Let* A *be an* (Ω, Φ)*-algebra and* Y *be a set. Then if* $|A| \leq |Y|$*, we have that* A *is a quotient of* $F_{(\Omega,\Phi)}(Y)$.

Proof. Since $|A| \leq |Y|$ there exists a surjection $\alpha : Y \to A$. Then, since $F_{(\Omega,\Phi)}(Y)$ is a free algebra, there exists a morphism $h : F_{(\Omega,\Phi)}(Y) \to A$ such that the diagram



commutes, where η_Y^Φ is the unit of our adjunction. Then, since $\alpha = h\eta_Y^\Phi$ is a surjection, h is a surjection. Therefore h is a surjective homomorphism and so A is a quotient of $F_{(\Omega,\Phi)}(Y)$. □

3.7 Birkhoff's Theorem

In our previous chapters we have seen that a variety $\mathbb{V}$ of (Ω, Φ)-algebras is closed under isomorphisms, subalgebras, products and quotients. However, in this section we show that the converse holds, and so a variety of (Ω, Φ)-algebras is equivalent to a class of Ω-algebras closed under subalgebras, products and quotients. This result was discovered by Birkhoff [2], although the original theorem's description of (Ω, Φ)-algebras was different to the one used in this chapter (a proof of the theorem using similar definitions can be found in [1]). This result is often referred to as Birkhoff's Theorem.

Theorem 3.7.1. ***Birkhoff's Theorem.*** [2]**.** *Let* $\mathcal{K}$ *be a class of algebras in* ***Alg***(Ω). *Then* $\mathcal{K}$ *is a variety if and only if* $\mathcal{K}$ *is closed under subalgebras, products and quotients.*

Proof. We have already proved that a variety is closed under subalgebras, products and quotients in Lemmas 3.3.4, 3.4.3 and 3.5.12.

In order to prove the converse, assume $\mathcal{K}$ is closed under subalgebras, products and quotients. Then we will show that $\mathcal{K} = \mathcal{K}^{**}$. That is, we will show that $\mathcal{K}$ is equal to the class of objects in $\mathbf{Alg}(\Omega, \mathcal{K}^*)$. It follows from the definition of a Galois connection that $\mathcal{K} \subseteq \mathcal{K}^{**}$. Moreover, recall that

$$\mathcal{K}^* = \{(t, t') \in F_\Omega(X) \times F_\Omega(X) \mid A \vDash (t, t') \text{ for all } A \in \mathcal{K}\}$$

Then, if we can show that $F_{(\Omega,\Phi)}(Y)$ is in $\mathcal{K}$ for any set Y, by Lemma 3.6.8 every $(\Omega, \mathcal{K})$-algebra is a quotient of $F_{(\Omega,\Phi)}(Y)$ for some Y. Then, since $\mathcal{K}$ is closed under quotients, if $F_\Omega(X)/\mathcal{K}^*$ is in $\mathcal{K}$, then every $(\Omega, \mathcal{K}^*)$-algebra is in $\mathcal{K}$.

In order to prove $F_{(\Omega,\Phi)}(Y)$ is in $\mathcal{K}$ we consider the set of congruences on $F_\Omega(Y)$,

$$\mathcal{E} = \{E \in \mathrm{Con}(F_\Omega(Y)) \mid F_\Omega(Y)/E \in \mathcal{K}\}$$

We then want to show that if $D = \bigcap \mathcal{E}$ we get that $F_\Omega(Y)/D \in \mathcal{K}$. It is clear from Lemma 3.5.3 that D is in fact a congruence. Define $f : F_\Omega(Y) \to \prod_{E\in\mathcal{E}} F_\Omega(Y)/E$, defined by $f(t) = ([t]_E)_{E\in\mathcal{E}}$. Consider the diagram

$$\begin{array}{ccc}
F_\Omega(Y) & \xrightarrow{\quad f \quad} & \prod_{E\in\mathcal{E}} F_\Omega(Y)/E \\
\downarrow{\scriptstyle q} & & {\scriptstyle i}\uparrow \\
F\Omega(Y)/E_f & \xrightarrow{\quad f' \quad} & f(F_\Omega(Y))
\end{array}$$

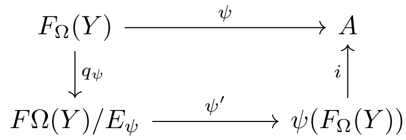
where q is the canonical homomorphism, i is the inclusion and $f'([t]) = f(t)$ for all $t \in F_\Omega(Y)$. By Corollary 3.5.10 we have that f' is an isomorphism, and it is clear that by definition the above diagram commutes. Then since $\mathcal{K}$ is closed under products, $\prod_{E\in\mathcal{E}} F_\Omega(Y)/E \in \mathcal{K}$, and since if' is an injection (an injection composed with an isomorphism) then $F_\Omega(Y)/E_f$ is a subalgebra (up to isomorphism) of $\prod_{E\in\mathcal{E}} F_\Omega(Y)/E$ and therefore $F_\Omega(Y)/E_f \in \mathcal{K}$.

However, note that $f(t) = f(t')$ if and only $(t, t') \in E$ for all $E \in \mathcal{E}$. Furthermore, this is true if and only if $(t, t') \in \bigcap \mathcal{E} = D$. That is, $(t, t') \in E_f$ if and only if $(t, t') \in D$ and so $E_f = D$.

Now since $F_\Omega(Y)/D \in \mathcal{K}$, note that, by definition, $F_\Omega(Y)/D$ is an $(\Omega, \mathcal{K}^*)$-algebra. Now for any function $\alpha : X \to A$ and any $A \in \mathcal{K}$ consider the diagram

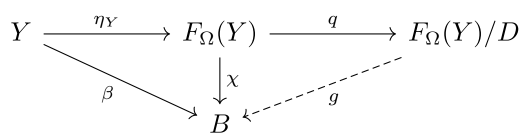
$$\begin{array}{ccccc}
Y & \xrightarrow{\quad \eta_Y \quad} & F_\Omega(Y) & \xrightarrow{\quad q \quad} & F_\Omega(Y)/D \\
& {\scriptstyle \alpha}\searrow & \downarrow{\scriptstyle \psi} & \swarrow{\scriptstyle h} & \\
& & A & &
\end{array}$$

where η_Y is the usual inclusion, q is the canonical morphism, and ψ is the unique morphism making the left triangle commute. We want to construct h such that h is the unique morphism such that $hq\eta_Y = \alpha = \psi\eta_Y$, but then since ψ is the unique morphism such that $\psi\eta_Y = \alpha$ the above equality is equivalent to $hq = \psi$. Then, if we choose $h([t]) = \psi(t)$ for all $t \in F_\Omega(Y)$ it is clear that the equality would be satisfied and that h would be unique (since ψ is unique). Since ψ is a homomorphism, it would also follow that h is a homomorphism. In order to show that this choice for h is well-defined, it is then sufficient to show that $(t, t') \in D$ implies that $\psi(t) = \psi(t')$. This can be shown if we take a similar factorization of ψ as of f in the diagram



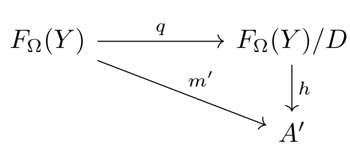
where q_ψ and i are again the canonical quotient homomorphism and the inclusion homomorphism respectively. As before, it is clear from this that $F\Omega(Y)/E_\psi$ is a subalgebra of A and is hence in $\mathcal{K}$. But then by the definition of D, we must have $D \subseteq E_\psi$ and so $(t, t') \in D$ implies that $\psi(t) = \psi(t')$. Therefore, h is well-defined and is the unique homomorphism making the previous diagram commute for a given α.

Now consider, some $B \in \mathcal{K}^{**}$, and for some function $\beta : Y \to B$ consider the diagram



defined similarly as done with respect to A. We want to show that a unique morphism g exists such that the right-hand triangle commutes. However, as before, if such a g exists it must be uniquely defined by $g([t]) = \chi(t)$ for all $t \in F_\Omega(Y)$. To show that such a map exists it is again sufficient to prove that $[t] = [t']$ in $F_\Omega(Y)/D$ implies that $\chi(t) = \chi(t')$.

Suppose to the contrary that $\chi(t) \neq \chi(t')$ for some $t, t' \in F_\Omega(Y)$ such that $[t] = [t']$ in $F_\Omega(Y)/D$. Then, by Lemma 3.2.2 we can find some $s, s' \in F_\Omega(X)$ such that for any Ω-algebra, B', we get that $m(t) = m(t')$ for all $m \in \hom(F_\Omega(X), B')$ if and only if $B' \vDash (s, s')$. Then, since $\chi(t) \neq \chi(t')$ we have that $B \nvDash (s, s')$. However, since $B \in \mathcal{K}^{**}$ then $B \vDash (u, u')$ for all $(u, u') \in \mathcal{K}^*$, and so $(s, s') \notin \mathcal{K}^*$. Then, by definition of $\mathcal{K}^*$ there must exist some $A' \in \mathcal{K}$ such that $A' \nvDash (s, s')$ and so there exists a morphism $m : F_\Omega(X) \to A'$ such that $m(s) \neq m(s')$. However, if this is the case, then there must exist some $m' : F_\Omega(Y) \to A'$ such that $m(t) \neq m(t')$ (by Lemma 3.2.2). But then, by the fact that $F_\Omega(Y)/D$ has is free over all $A' \in \mathcal{K}$, we must have a unique $h : F_\Omega(Y)/D \to A'$ such that the diagram



commutes. However, this is a contradiction, since $[t] = [t']$ and so $h([t]) = h([t'])$, which gives us $m'(t) = m'(t')$. Therefore, we can conclude that $[t] = [t']$ in $F_\Omega(Y)/D$ implies that $\chi(t) = \chi(t')$. Moreover, this tells us that $F_\Omega(Y)/D$ has the free mapping property over all $B \in \mathcal{K}^{**}$ and so (since the free $(\Omega, \mathcal{K}^*)$-algebra is unique up to isomorphism) $F_\Omega(Y)/D \cong F_{(\Omega,\mathcal{K}^*)}(Y)$. Therefore, for any set Y, we have that $F_{(\Omega,\mathcal{K}^*)}(Y) \in \mathcal{K}$ and so by Lemma 3.6.8 we have that every algebra in $\mathcal{K}^{**}$ is in $\mathcal{K}$ and therefore $\mathcal{K}^{**} = \mathcal{K}$. □

Definition 3.7.2. Let $\mathcal{K}$ be a class of Ω-algebras. Then we define

$$S(\mathcal{K}) = \{B \mid S \text{ is isomorphic to a subalgebra of some } A \in \mathcal{K}\}$$

$$P(\mathcal{K}) = \{B \mid P \text{ is isomorphic to a product of some family} (A_i)_{i \in I} \text{such that each } A_i \in \mathcal{K}\}$$

$$Q(\mathcal{K}) = \{B \mid S \text{ is isomorphic to a quotient of some } A \in \mathcal{K}\}$$

Corollary 3.7.3. *Let $\mathcal{K}$ be a class of Ω-algebras. Then $\mathcal{K}^{**} = QSP(\mathcal{K})$.*

Proof. Clearly, if $A \in QSP(\mathcal{K})$ then A is an element of any variety containing $\mathcal{K}$ and so $QSP(\mathcal{K}) \subseteq \mathcal{K}^{**}$. Then, if $A \in \mathcal{K}^{**}$, we have from Lemma 3.6.8 that A is a quotient of the free $(\Omega, \mathcal{K}^*)$-algebra over X for some X. Then, from the proof Theorem 3.7.1 we can see that $F_{(\Omega,\mathcal{K}^*)}(Y)$ is a subset of a product of algebras in $\mathcal{K}$. Then $A \in QSP(\mathcal{K})$, and so $\mathcal{K}^{**} \subseteq QSP(\mathcal{K})$. □

3.8 Subvarieties

In this section, we define subvarieties of a given variety of algebras, and show how varieties with the same signature form a lattice when we consider them ordered by inclusion of subvarieties.

Definition 3.8.1. Let $\mathbb{V} = \mathbf{Alg}(\Omega, \Phi)$ be a variety of algebras. A subvariety $\mathbb{V}'$ of $\mathbb{V}$ is a full subcategory of $\mathbb{V}$ such that $\mathbb{V}' = \mathbf{Alg}(\Omega, \Phi')$ for some $\Phi' \subset F_\Omega(X) \times F_\Omega(X)$. That is, $\mathbb{V}'$ is a subcategory of $\mathbb{V}$ such that it is a variety with respect to the same signature Ω. We will write $\mathbb{V}' \leq \mathbb{V}$ to denote that $\mathbb{V}'$ is a subvariety of $\mathbb{V}$.

Note 3.8.2. Let $\mathcal{K}$ be a class of Ω-algebras. By Birkhoff's Theorem, we have that $\mathcal{K}$ is a subvariety of $\mathbb{V}$ if every object $A \in \mathcal{K}$ is in $\mathbb{V}$, and $\mathcal{K}$ is closed under subalgebras, products and quotients.

Example 3.8.3. The category **Set**, which can be seen as $\mathbf{Alg}(\emptyset)$, has only itself and the trivial variety as its subvarieties. This is because $F_\emptyset(X) = X$, and so if we let Φ be a subset of $X \times X$, then if $(x, y) \in \Phi$ for $x \neq y$, then $\mathbf{Alg}(\emptyset, \Phi)$ is the trivial variety, as in the case of Example 3.2.11. On the other hand if Φ only contains elements of the form (x, x) for $x \in X$ then clearly $(t, t') \in \Phi^{**}$ if and only if $t = t'$ in X, and so any set is in $\mathbf{Alg}(\emptyset, \Phi)$.

Example 3.8.4. Consider the variety of monoids $\mathbf{Mon} = \mathbf{Alg}(\Omega, \Phi_M)$ where $\Omega = \{m, 1\}$, where m is a binary operation and 1 is a nullary operation. $\Phi_M = \{\phi_1, \phi_2, \phi_3\}$ where $\phi_1 = ((m, m, t, u, v), (m, t, m, u, v))$,

$\phi_2 = ((m,1,t),t)$ and $\phi_3 = ((m,t,1),t)$. In this case ϕ_1 gives us the associativity of m, and ϕ_2 and ϕ_3 gives us the fact that 1 is the identity for m.

It is easy to see that **SemiLat** is a subvariety of **Mon** since each semilattice is an idempotent commutative monoid, and so can be seen a monoid with extra axioms of commutativity and idempotency. Explicitly, these extra axioms are given by $\phi_4 = ((m,t,u),(m,u,t))$ and $\phi_5 = ((m,t,t),t)$.

Example 3.8.5. If we consider the category **Ring** of rings (with identity) we have that **BoolRing** is a subvariety of this category since both **Ring** and **BoolRing** have the same signature, $\Omega = \{+, 0, \cdot, 1, -\}$ where $+$ and $\cdot$ are binary, 0 and 1 are nullary and $-$ is unary. Although we will not explicitly list the axioms here, it is also clear to see that each object in **BoolRing** is a ring, and so can be considered an object of **Ring**. However, **BoolRing** has additional axioms which not every ring satisfies, namely that $\cdot$ is commutative and idempotent. It is also worth noting that since **Bool** and **BoolRing** are isomorphic, we can say that **Bool** is, up to isomorphism, a subvariety of **Ring**.

Our general definition and results for Galois connections (Lemmas 2.4.4 and 2.4.5) can be applied in order to obtain the following three results for subvarieties.

Lemma 3.8.6. *Let* $\boldsymbol{Alg}(\Omega,\Phi) = \mathbb{U}$ *and* $\boldsymbol{Alg}(\Omega,\Phi') = \mathbb{V}$ *be varieties of* Ω*-algebras, then* $\mathbb{U} \leq \mathbb{V}$ *if* $\Phi' \subseteq \Phi$*, and* $\Phi'^{**} \subseteq \Phi^{**}$ *if* $\mathbb{U} \leq \mathbb{V}$.

Lemma 3.8.7. *Let* $\mathbb{V}$ *be a variety of* Ω*-algebras, and let* $\mathrm{Sub}(\mathbb{V})$ *denote the class of subvarieties of* $\mathbb{V}$*. Then* $\mathrm{Sub}(\mathbb{V})$ *is a lattice ordered by* $\leq$ *defined as in 3.8.1, where for* $\mathbb{S}, \mathbb{U} \in \mathrm{Sub}(\mathbb{V})$, $\mathbb{S} \wedge \mathbb{U} = \mathbb{S} \cap \mathbb{U}$ *and* $\mathbb{S} \vee \mathbb{U} = (\mathbb{S} \vee \mathbb{U})^{**}$.

Lemma 3.8.8. *Let* $\boldsymbol{Alg}(\Omega,\Phi) = \mathbb{S}$ *and* $\mathbb{U} = \boldsymbol{Alg}(\Omega,\Phi')$ *be subvarieties of* $\mathbb{V}$*. Then* $\mathbb{S} \wedge \mathbb{U} = \boldsymbol{Alg}(\Omega, \Phi \cup \Phi')$ *and* $\mathbb{S} \vee \mathbb{U} = \boldsymbol{Alg}(\Omega, \Phi^{**} \cap \Phi^{**})$.

Example 3.8.9. Consider the subvarieties of $\mathbf{Alg}(\Omega)$ where $\Omega = \{m, 1\}$ where m is a binary operation and 1 is a nullary operation.

Then consider the varieties **ComMon** and **IdemMon** of commutative monoids and idempotent monoids respectively. Note that **ComMon** $= \mathbf{Alg}(\Omega, \Phi_{CM})$ such that in Φ_{CM} we have the axioms for each $M \in$ **ComMon**:

1. For each $x, y, z \in M$, $m(m(x,y),z) = m(x, m(y,z))$. This is called associativity and can be expressed as an element of Φ_{CM} by $\phi_1 = ((m,m,t,u,v),(m,t,m,u,v))$.

2. For each $x \in M$ we have $m(1,x) = x = m(x,1)$. This expresses that 1 is the identity for m and can be expressed as two element of Φ_{CM} by $\phi_2 = ((m,1,t),t)$ and $\phi_3 = ((m,t,1),t)$.

3. For all $x, y \in M$, $m(x,y) = m(y,x)$. This is called commutativity and can be expressed as an element of Φ_{CM} by $\phi_4 = ((m,t,u),(m,u,t))$.

And so $\Phi_{CM} = \{\phi_1, \phi_2, \phi_3, \phi_4\}$.

We can describe **IdemMon** $= \mathbf{Alg}(\Omega, \Phi_{IM})$ where $\Phi_{IM} = \{\phi_1, \phi_2, \phi_3, \phi_5\}$. In this case the first three elements are the same which tells us each member of **IdemMon** has the axioms 1 and 2 as above, and $\phi_5 = ((m,t,t),t)$ which expresses the idempotent property of m.

Then, we have that **ComMon** $\wedge$ **IdemMon** $= \mathbf{Alg}(\Omega, \Phi_{CM} \cup \Phi_{IM})$, which is equal to the category **SemiLat**, of semilattices.

Lemma 3.8.10. *If* $\mathbb{U}$ *is a subvariety of* $\mathbb{V}$*, then* $\mathbb{U}$ *is a reflective subcategory of* $\mathbb{V}$*.*

Proof. Consider the inclusion functor $I : \mathbb{U} \to \mathbb{V}$. We claim that the left adjoint to I is $F_U K_V$ where $K_V : \mathbb{V} \to \mathbf{Alg}(\Omega)$ is the inclusion and F_U is the left adjoint to the inclusion $K_U : \mathbb{U} \to \mathbf{Alg}(\Omega)$. It is clear to see that for any $A \in \mathbb{V}$ that the algebra $F_U K_V(A) = F_U(A)$ is a member of $\mathbb{U}$ and is free over all $B \in \mathbb{U}$, since in fact this is true of $F_U(A')$ for any $A' \in \mathbf{Alg}(\Omega)$ (by Corollary 3.6.3) and we are just considering the restriction of this functor to the Ω-algebras in $\mathbb{V}$. $\square$

Corollary 3.8.11. *If* $\mathbf{Alg}(\Omega, \Phi) \leq \mathbf{Alg}(\Omega, \Phi')$*, then* $F_\Phi K F_{(\Omega,\Phi')} \cong F_{(\Omega,\Phi)}$ *for any set* Y*, where* $K : \mathbf{Alg}(\Omega, \Phi) \to \mathbf{Alg}(\Omega, \Phi')$ *is the inclusion and* F_Φ*,* $F_{(\Omega,\Phi)}$ *and* $F_{\Phi'}$ *are as in the section on free algebras.*

Proof. We simply compose adjunctions

$$\mathbf{Set} \underset{U}{\overset{F_{(\Omega,\Phi')}}{\rightleftarrows}} \mathbf{Alg}(\Omega, \Phi') \underset{K'}{\overset{F_\Phi K}{\rightleftarrows}} \mathbf{Alg}(\Omega, \Phi)$$

where K' is the inclusion functor. Then UK' is the forgetful functor from $\mathbf{Alg}(\Omega, \Phi)$ to **Set** and so its left adjoint is unique up to isomorphism, hence since $F_\Phi K F_{(\Omega,\Phi')} \vdash UK'$ we have $F_\Phi K F_{(\Omega,\Phi')} \cong F_{(\Omega,\Phi)}$. $\square$

The structural elements of subvarieties above allow us to compare varieties with the same signature, as well as use the meet and join operations to construct new related varieties from given varieties. In the last section of this chapter, we consider conditions relating to completeness in a variety.

3.9 Completeness with Respect to L-valued Models

Example 3.9.1. In our previous chapter, we described a theory of classical logic as a pair (Y, A), where Y is a set of variables and A is a set of axioms. However, considering **Bool** as a variety, we can consider the free Boolean algebra over Y as being isomorphic to $F_\Omega(Y)/E_\Phi$, and in particular, if X is a countably infinite set $F_{\mathbf{Bool}}(X) \cong F_\Omega(X)/\Phi^{**}$, where Φ is the set of identities in Example 3.2.10. Then, we can consider the theory $(X, \emptyset)$ in which our theorems are in the smallest filter containing $\emptyset$. That is, every term $t \in F_\Omega(X)$ such that $[t] = [1]$ in $F_\Omega(X)/\Phi^{**}$, or equivalently, $(t, 1) \in \Phi^{**}$. Then our completeness theorem for classical logic can be formulated as:

$t \in F_\Omega(X)$ *is a theorem of* $(X, \emptyset)$ *if and only if* $m([t]) = 1$ *for all* $m \in$ *hom*$(F_{\boldsymbol{Bool}}(X), \{0, 1\})$.

Additionally, we also have that

- If t is a theorem of $(X, \emptyset)$, then $B \vDash (t, 1)$ for all $B \in \mathbf{Bool}$.
- $(t, t') \in \Phi^{**}$ if and only if $[t \Leftrightarrow t'] = [1]$ in $F_{\mathbf{Bool}}(X)$, and thus, $t \Leftrightarrow t'$ is a theorem of $(X, \emptyset)$.
- For all $B \in \mathbf{Bool}$, $x = y$ for $x, y \in B$ if and only if $m(x \Leftrightarrow y) = 1$, or equivalently $m(x) = m(y)$, for all $m \in \hom(B, \{0, 1\})$. This follows from Lemma 2.6.1, and the fact that any Boolean algebra is a quotient of a free Boolean algebra.
- The second algorithm given in Chapter 2 can be used to determine whether $t \in F_\Omega(X)$ is a theorem, by computing whether $f(t) = 1$ for all $f \in \hom(F_{\mathbf{Bool}}(V_t), \{0, 1\})$, where $V_t \subseteq X$ are the elements of X which occur in t.

Thus, the theory $(X, \emptyset)$ characterizes a property of **Bool** which states that each equality $x = y$ in a Boolean algebra holds if and only if it holds under the image of f for every $f \in \hom(B, \{0, 1\})$. We describe this by saying that **Bool** is *complete with respect to its* $\{0, 1\}$*-valued models*, or by saying that **Bool** is $\{0, 1\}$**-complete**.

In this section, we will characterize L-completeness for a general variety $\mathbb{V}$ and specify some conditions which are necessary for $\mathbb{V}$ to be L-complete.

Theorem 3.9.2. *In a variety* $\boldsymbol{Alg}(\Omega, \Phi)$*, the following are equivalent for some fixed object* $L \in \boldsymbol{Alg}(\Omega, \Phi)$*:*

1. *For any* $A \in \boldsymbol{Alg}(\Omega, \Phi)$ *and any elements* $a, b \in A$*, we have that* $f(a) = f(b)$ *for all* $f \in$ *hom*(A, L) *if and only if* $a = b$.
2. *Each* $A \in \boldsymbol{Alg}(\Omega, \Phi)$ *is a subalgebra of a product of* L.

Proof. *1.⇒2.:*

Note that if 1. holds for $L \in \mathbf{Alg}(\Omega, \Phi)$, then we claim that we can define an injective morphism

$$A \xrightarrow{\quad h \quad} \prod_{f \in \hom(A,L)} L$$

for each A defined by $h(a) = (f(a))_{f \in \hom(A,L)}$ (if A is empty then 2. trivially holds since if $\emptyset \in \mathbf{Alg}(\Omega, \Phi)$, it is a subalgebra of every algebra in the variety). h is a homomorphism, since

$$\begin{aligned} h(\omega(a_1, ..., a_n)) &= (f(\omega(a_1, ..., a_n)))_{f \in \hom(A,L)} \\ &= (\omega(f(a_1), ..., f(a_n)))_{f \in \hom(A,L)} \\ &= \omega((f(a_1))_{f \in \hom(A,L)}, ..., (f(a_n))_{f \in \hom(A,L)}) \\ &= \omega(h(a_1), ..., h(a_n)) \end{aligned}$$

for all $\omega \in \Omega$ and $a_1, ..., a_n \in A$. Moreover, h is an injection, since if $h(a) = h(b)$ then $f(a) = f(b)$ for all $f \in \hom(A, L)$ and by 1., $a = b$. Hence, A is a subalgebra of $\prod_{f \in \hom(A,L)} L$.

2.⇒1.:

Let A be an (Ω, Φ)-algebra. If A is empty then $\hom(A, L)$ is empty and 1. is trivially satisfied. Then, consider $a, b \in A$ and note that if $a = b$, we trivially have that $f(a) = f(b)$ for $f \in \hom(A, L)$. Then, in order to prove the converse, we note that by assumption, there is an injection $h : A \to \prod_{i \in I} L$ for some set I. Then, we note that $h(a) = (\hat{a}_i)_{i \in I}$ such that each $\hat{a}_i \in L$. Then, we define for every $i \in I$, the map $h_i : A \to L$ defined by $h_i(a) = \hat{a}_i$. Note each h_i is a homomorphism since $h(\omega(a_1, ..., a_n)) = \omega(h(a_1), ..., h(a_n))$ implies that $(h_i(\omega(a_1, ..., a_n)))_{i \in I} = (\omega(h_i(a_1), ..., h_i(a_n)))_{i \in I}$. That is, $h_i(\omega(a_1, ..., a_n)) = \omega(h_i(a_1), ..., h_i(a_n))$ for all $i \in I$.

Then, assume that $f(a) = f(b)$ for all $f \in \hom(A, L)$. Then $h_i(a) = h_i(b)$ for all $i \in I$, and therefore $h(a) = h(b)$. Since h is injective, this implies $a = b$ and therefore 1. holds. □

Definition 3.9.3. Let $\mathbb{V}$ be a variety of algebras. If $\mathbb{V}$ satisfies either of the above properties for some $L \in \mathbb{V}$, then we say that $\mathbb{V}$ is ***L*-complete**, or complete with respect to its L-valued models.

Lemma 3.9.4. *If* $\mathbf{Alg}(\Omega, \Phi)$ *is* L*-complete, then* $L \vDash (t, t')$ *if and only if* $(t, t') \in \Phi^{**}$.

Proof. It is clear that if $(t, t') \in \Phi^{**}$ then $L \vDash (t, t')$ Then, if $L \vDash (t, t')$ we have that $f(t) = f(t')$ for every $f \in \hom(F_\Omega(X), L)$. Then note that for each $f' \in \hom(F_\Omega(X)/\Phi^{**}, L)$, then $f : F_\Omega(X) \to L$ defined by $f(t) = f'([t])$ is a well-defined morphism, since if $[t] = [t']$ then $(t, t') \in \Phi^{**}$ and $f(t) = f(t')$.

Therefore, if $L \vDash (t, t')$, we have that $f'([t]) = f'([t'])$ for every $f' \in \mathrm{hom}(F_\Omega(X)/\Phi^{**}, L)$. But then since $F_\Omega(X)/\Phi^{**}$ is in $\mathbf{Alg}(\Omega, \Phi)$, by L-completeness we have that $[t] = [t']$ and so $(t, t') \in \Phi^{**}$. □

Corollary 3.9.5. *If $\boldsymbol{Alg}(\Omega, \Phi)$ is L-complete, then there is no proper subvariety, $\boldsymbol{Alg}(\Omega, \Phi')$, such that $L \in \boldsymbol{Alg}(\Omega, \Phi')$.*

Proof. If $\mathbf{Alg}(\Omega, \Phi') \leq \mathbf{Alg}(\Omega, \Phi)$ then $\Phi^{**} \subseteq \Phi'^{**}$, and since $\mathbf{Alg}(\Omega, \Phi')$ is a proper subvariety $\Phi^{**} \neq \Phi'^{**}$. Then by Lemma 3.9.4, if $L \vDash (t, t')$ then $(t, t') \in \Phi^{**}$ and so there is some $(s, s') \in \Phi'^{**} - \Phi^{**}$ such that $L \nvDash (s, s')$. Hence L is not an (Ω, Φ')-algebra. □

Lemma 3.9.6. *Let $\mathbb{V}$ be a variety. Then, if the free algebra $F_\mathbb{V}(Y)$ is non-finite for any finite set Y, then there is no finite algebra $L \in \mathbb{V}$ such that $\mathbb{V}$ is L-complete.*

Proof. Let L be a finite algebra in $\mathbb{V}$ with n elements, and let $|Y| = k$. Since each $m \in \mathrm{hom}(F_\mathbb{V}(Y), L)$ is uniquely determined by the restriction of m on Y, we have that $|\mathrm{hom}(F_\mathbb{V}(Y), L)| = n^k$, since there are only n^k distinct functions from Y to L.

Then, for each $m \in \mathrm{hom}(F_\mathbb{V}(Y), L)$, let E_m be the congruence induced on $F_\mathbb{V}(Y)$ by m, and let $\{m_1, ..., m_{n^k}\} = \mathrm{hom}(F_\mathbb{V}(Y), L)$. Then, if $\mathbb{V}$ is L-complete, we must have, for $y, z \in F_\mathbb{V}(Y)$, that $y = z$ if and only if $(y, z) \in \bigcap_{i=1}^{n^k} E_{m_i}$. That is, we have that $F_\mathbb{V}(Y) \cong F_\mathbb{V}(Y)/\bigcap_{i=1}^{n^k} E_{m_i}$. Then since L is finite, for each E_{m_i} we have that $F_\mathbb{V}(Y)/E_{m_i}$ is finite, since it is a subalgebra of L by Lemma 3.5.10. Then, $\prod_{i=1}^{n^k} F_\mathbb{V}(Y)/E_{m_i}$ is finite since it is a finite product of finite algebras. However, by Lemma 3.5.15 we have that $F_\mathbb{V}(Y)/\bigcap_{i=1}^{n^k} E_{m_i}$ is a subalgebra of $\prod_{i=1}^{n^k} F_\mathbb{V}(Y)/E_{m_i}$, and therefore is also finite. But then, since $F_\mathbb{V}(Y)$ is infinite it cannot be isomorphic to $F_\mathbb{V}(Y)/\bigcap_{i=1}^{n^k} E_{m_i}$ which is a contradiction. Thus, $\mathbb{V}$ is not L-complete. □

In our next chapters we will discuss how the framework of universal algebra can be applied generally to propositional logic, and describe varieties which correspond to some non-classical propositional logics.

4 Formal Theories and Varieties of Algebra

In this chapter, we consider formal propositional theories and their correspondence to varieties of universal algebra.

4.1 Formal Theories of Propositional Logic

In this section, we provide a definition of a formal language and a general formal theory, and describe proofs, theorems and consequences in a given theory. Using the theory of classical propositional logic as a motivating example, we then give a more specific definition of a propositional theory, which include the theories of many well-known propositional logics, including all those which we study in this thesis.

Definition 4.1.1. [15]. A formal **language** $\mathscr{L}$ is a a pair $\mathscr{L} = (S_{\mathscr{L}}, \text{Frm}(\mathscr{L}))$, where $S_{\mathscr{L}}$ is a countable set called the **symbols** of $\mathscr{L}$. A finite sequence of symbols of $\mathscr{L}$ is called an **expression** of $\mathscr{L}$. $\text{Frm}(\mathscr{L})$ is a subset of the expressions of $\mathscr{L}$ called the formulae of $\mathscr{L}$.

Note 4.1.2. For each expression $s_1 s_2 ... s_n$ of $\mathscr{L}$, it is clear to see that this finite sequence can be uniquely expressed as an n-tuple $(s_1, ..., s_n)$. Therefore, the set of expressions in $\mathscr{L}$ is bijective to the set $\bigcup_{n \in \mathbb{N}} (S_{\mathscr{L}})^n$ which is the underlying set of the free monoid $F_{\mathbf{Mon}}(S_{\mathscr{L}})$.

Definition 4.1.3. [15]. A **formal theory** $\mathscr{T}$ is a triple $\mathscr{T} = (\mathscr{L}, A, \mathscr{R})$, where $\mathscr{L}$ is a formal language A is a subset of $\text{Frm}(\mathscr{L})$ called the **axioms** of $\mathscr{T}$, and $\mathscr{R} = \{R_1, ..., R_j\}$ is a finite set called the **rules of inference**. Each R_i is a subset of $(\text{Frm}(\mathscr{L}))^n$ for some $n \in \mathbb{N}$, usually made up of an n-tuple of formulae of a certain form. If $(p_1, ..., p_n) \in R_i \subseteq (\text{Frm}(\mathscr{L}))^n$, we say that p_n is a **direct consequence** of $p_1, ..., p_{n-1}$ by R_i. We may also write $\text{Frm}(\mathscr{T})$ to denote the formulae in a language of a specified theory.

Definition 4.1.4. Given a formal theory $\mathscr{T}$ a **proof** in $\mathscr{T}$ is a finite sequence of formulae $p_1, ..., p_n$ such that every p_i is an axiom or p_i is a direct consequence of $p_{j_1}, ..., p_{j_m}$ by some rule of inference R, where $1 \leq j_k < i$ for each j_k. If $p \in \text{Frm}(\mathscr{T})$ belongs to some proof, we say that p is a **theorem** of $\mathscr{T}$.

Definition 4.1.5. [15]. Let Γ be a set of formulae in $\mathscr{T}$. Then we say that $p \in \text{Frm}(\mathscr{T})$ is a **consequence** of Γ if there exists a finite sequence $p_1, ..., p_k$ such that $p_k = p$ and for each p_i, we have that p_i is an axiom, p_i is a direct consequence of $p_{j_1}, ..., p_{j_m}$ where $p_{j_1}, ..., p_{j_m}$ occur previously in the sequence, or p_i is an element of Γ. If this is the case, we write $\Gamma \vdash_{\mathscr{T}} p$.

Note 4.1.6. We note some conventions and results of the above definition:

- If it is unambiguous what theory we are considering we write $\Gamma \vdash p$ instead of $\Gamma \vdash_{\mathscr{T}} p$.
- We write $\vdash_{\mathscr{T}} p$ to denote $\emptyset \vdash_{\mathscr{T}} p$. Moreover, $\vdash_{\mathscr{T}} p$ if and only if p is a theorem of $\mathscr{T}$.
- A corollary of the definition above is that $\Gamma \vdash_{\mathscr{T}} p$ if and only if $\vdash_{\mathscr{T}'} p$, where $\mathscr{T}'$ is the theory with the same rules of inference and language as $\mathscr{T}$ but with $\Gamma \cup A$ as its axioms (where A are the axioms of $\mathscr{T}$).

Example 4.1.7. The theory of classical logic $\mathscr{T}_{CL}$ is defined as follows,

1. The symbols of $\mathscr{T}_{CL}$ are given by a countably infinite set $X = \{x_1, x_2, ...\}$ called the set of *variables, statement letters* or *atomic formulae*, the brackets $($, $)$ and the logical connectives 1, $\wedge$, $\vee$, $\Rightarrow$ and $\neg$.
2. The formulae are defined inductively as follows
   i. Every $x \in X$ is a formula.
   ii. 1 is a formula.
   iii. If p and q are formulae then $p \wedge q$, $p \vee q$, $p \Rightarrow q$ and $\neg p$ are also formulae.
3. The axioms are the formulae,
   A1. $p \Rightarrow (q \Rightarrow p)$.
   A2. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$.
   A3. $(p \wedge q) \Rightarrow p$.
   A4. $(p \wedge q) \Rightarrow q$.
   A5. $p \Rightarrow (q \Rightarrow (p \wedge q))$.
   A6. $p \Rightarrow (p \vee q)$.
   A7. $q \Rightarrow (p \vee q)$.
   A8. $(p \Rightarrow q) \Rightarrow ((r \Rightarrow q) \Rightarrow ((p \vee r) \Rightarrow q))$.
   A9. $(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$.
   A10. $\neg p \Rightarrow (p \Rightarrow q)$
   A11. $\neg p \vee p$.
   A12. 1

   for any formulae p, q and r.

4. There is only one rule of inference called *modus ponens* given by the set,

$$MP = \{(p, p \Rightarrow q, q) \mid p, q \in \mathrm{Frm}(\mathscr{T}_{CL})\}.$$

Note 4.1.8.

- The definition above is given in Borceux [6] (with several different equivalent axiomatizations given in Mendelson [15] and Rasiowa and Sikorski [16]), with the added inclusion of the nullary connective 1 to represent "true/provable". We also define an additional nullary connective by $0 = \neg 1$ which represents "false/disprovable". Many authors do not include these in the construction of formal propositional theories, and in the cases of translating a theory into an algebra will use 1 as shorthand for some provable formula (for example, Borceux [6] uses the formula $p \Rightarrow p$). However, for our purposes we will include these nullary connectives in our theory.

- In other equivalent axiomatizations of $\mathscr{T}_{CL}$, the language does not include all the connectives in our above example. Instead, they include a subset of these connectives as part of the language and define the other connectives in terms of those given in the language. For example, an axiomatization of $\mathscr{T}_{CL}$ given in Mendelson [15] includes only $\Rightarrow$ and $\neg$ in its language, and has axioms A1. and A2. as in example 4.1.7, and an additional set of axioms of the form

  A3*.$((\neg q) \Rightarrow (\neg p)) \Rightarrow (((\neg q) \Rightarrow p) \Rightarrow q)$.

  for any formulae p and q. Then additional connectives are defined by,

  a. $p \vee q = \neg p \Rightarrow q$.

  b. $p \wedge q = \neg(p \Rightarrow \neg q)$.

  c. $p \Leftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$.

  We will use the same definition of $\Leftrightarrow$ in c. for the theory given in 4.1.7.

We now observe an example of a proof in $\mathscr{T}_{CL}$.

Theorem 4.1.9. *For any formula $p \in Frm(\mathscr{T}_{CL})$ we have that $\vdash p \Rightarrow p$.*

Proof. We provide a proof of the above for any formula p given by the following sequence:

1. $(p \Rightarrow ((p \Rightarrow p) \Rightarrow p)) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p))$, by A2.

2. $p \Rightarrow ((p \Rightarrow p) \Rightarrow p)$, by A1.

3. $(p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)$by MP applied to 1. and 2.

4. $p \Rightarrow (p \Rightarrow p)$ by A1.

5. $p \Rightarrow p$ by MP applied to 3. and 4.

□

Definition 4.1.4 provides a general description of a theory which can be applied to many areas of mathematics. In order to construct the connection between formal theories of propositional logic and varieties of algebra, we restrict the theories we consider to **propositional theories**, which are those whose formulae are made up of variables connected by "logical connectives" in a specified way. Examples of propositional theories includes many known systems of propositional logic, and can be applied to each theory of logic which we consider in this thesis. We define these theories as in [16], but generalize to allow logical connectives with an arity greater than 2.

Definition 4.1.10. A **propositional theory** $\mathscr{T}$ is a formal theory such that the following holds.

1. If $\mathscr{L}$ is the language of $\mathscr{T}$, then $\mathrm{Sym}(\mathscr{L}) = X \cup \Omega \cup \{(,)\}$ where X, Ω, and $\{(,)\}$ are all disjoint sets, and X is countably infinite. The elements of X are called **variables** and elements of Ω are called **logical connectives**.

2. The set Ω is equipped with a map $l : \Omega \to \mathbb{N}$ such that for each $\omega \in \Omega$, $l(\omega)$ is called the **arity** of ω. We call ω an n-ary connective if $l(\omega) = n$.

3. The formulae $\mathrm{Frm}(\mathscr{L})$ are defined inductively as follows:

   i. Each $x \in X$ is a formula.

   ii. For each $\omega \in \Omega$, we have that $(\omega p_1 p_2 p_3 ... p_{l(\omega)})$ is a formula where $p_1, ..., p_{l(\omega)} \in \mathrm{Frm}(\mathscr{L})$. In the special case that $l(\omega) = 2$, we may write $(p_1 \omega p_2)$ instead of $(\omega p_1 p_2)$.

   iii. In the case where $l(\omega) = 0$, we have that ω is a formula of $\mathscr{L}$. In this case we call ω a nullary connective, or a **constant**.

4.2 Constructing a Free Algebra from a Propositional Theory

In this section we show how a propositional theory corresponds to a free algebra, in which terms of the algebra are equal when they are logically equivalent. Specifically, we will show that the set of formulae of a propositional language corresponds to the free term algebra over the set of variables in the language, where the set of algebraic operations of the algebra is equal to the set of logical connectives in the language. Furthermore, we construct a set of identities Φ induced by the axioms of our theory, and therefore construct a free (Ω, Φ)-algebra whose elements are equivalence classes of the formulae in our theory. We start by considering the term algebra induced by a propositional language.

Lemma 4.2.1. *If $\mathscr{L}$ is a propositional language, then Frm($\mathscr{L}$) is an Ω-algebra where Ω is the set of logical connectives in $\mathscr{L}$, where the arity of each ω considered as an operation is the same as the arity of ω considered as a logical connective. Then for any $\omega \in \Omega$, let $l(\omega) = n$. Then, we define the n-ary operation $\omega : Frm(\mathscr{L})^n \to Frm(\mathscr{L})$ by,*

$$\omega(p_1, ..., p_n) = (\omega p_1 ... p_n)$$

for any $p_1, ..., p_n \in Frm(\mathscr{L})$. Moreover, Frm($\mathscr{L}$) is isomorphic to $F_\Omega(X)$ where X is the set of variables in $\mathscr{L}$.

Proof. Clearly, for each $\omega \in \Omega$, the map $\omega : \mathrm{Frm}(\mathscr{L})^{l(\omega)} \to \mathrm{Frm}(\mathscr{L})$ is well-defined and therefore Frm($\mathscr{L}$) is an Ω-algebra. Moreover, it is clear from definition 4.1.10 that Frm($\mathscr{L}$) can be written as a union of sets $\bigcup_{n\in\mathbb{N}} \mathscr{X}_n$, where

$$\mathscr{X}_0 = X$$

and

$$\mathscr{X}_{k+1} = \mathscr{X}_k \cup (\bigcup_{\omega\in\Omega} \{(\omega p_1 ... p_{l(\omega)}) \mid p_1, ..., p_{l(\omega)} \in \mathscr{X}_k\})$$

Moreover, since each expression in Frm($\mathscr{L}$) is uniquely determined by the sequence of symbols which makes it up we have that $(\omega p_1 p_2 .. p_{l(\omega)}) = (\omega' p'_1 p'_2 ... p'_{l(\omega')})$ implies that $\omega = \omega'$ and $p_1 = p'_1, ..., p_{l(\omega)} = p'_{l(\omega')}$. The proof of this is similar to the proof of Lemma 3.1.13 where we define the length of $p \in \mathrm{Frm}(\mathscr{L})$ by taking the number of symbols in the sequence making up p and subtracting the number of times the brackets, (and), occur.

Let $\eta'_X : X \to \mathrm{Frm}(\mathscr{L})$ be the inclusion, and consider function $\alpha : X \to A$ for any Ω-algebra A. Then the diagram

$$\begin{array}{ccc} X & \xrightarrow{\eta'_X} & \mathrm{Frm}(\mathscr{L}) \\ & \searrow^{\alpha} & \downarrow \\ & & A \end{array}$$

commutes for a unique Ω-algebra homomorphism ψ, defined by

$$\psi(p) = \begin{cases} \alpha(p) & \text{if } p \in X \\ \omega(\psi(p_1), ..., \psi(p_{l(\omega)})) & \text{if } p = (\omega p_1 ... p_{l(\omega)}) \notin X \end{cases}$$

The proof of this follows the same method as the proof of Lemma 3.1.15. Hence Frm($\mathscr{L}$) is the free

Ω-algebra over X and is therefore isomorphic to $F_\Omega(X)$. □

Corollary 4.2.2. *The isomorphism $\psi : Frm(\mathscr{L}) \to F_\Omega(X)$ is defined by,*

$$\psi(p) = \begin{cases} p & \text{if } p \in X \\ (\omega, \psi(p_1), ..., \psi(p_{l(\omega)})) & \text{if } p = (\omega p_1 ... p_{l(\omega)}) \notin X \end{cases}$$

From the above, we are able to express formulae of a propositional language $\mathscr{L}$ in terms of universal algebra. However, in order to express a propositional theory algebraically, we need to include the axioms and rules of inference in the algebraic structure. Furthermore, we want to do it in such a way that formulae are considered equal when they are logically equivalent. For this to be the case, we will pick a subset $\Phi \subseteq F_\Omega(X) \times F_\Omega(X)$ which gives us the desired set of equalities in terms.

We consider formulae to be logically equivalent if p holds if and only if q holds, or q implies p and p implies q. We then consider three conditions below, which express this intuition in a formal manner:

i. $\vdash p \Rightarrow q$ and $\vdash q \Rightarrow p$

ii. $\vdash p \Leftrightarrow q$.

iii. $\{p\} \vdash q$ and $\{q\} \vdash p$.

Where $\Rightarrow$ is a connective signifying "implication", and $p \Leftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$ where $\wedge$ is a connective signifying "and" or conjunction.

Authors such as, Borceux [6] and Rasiowa and Sikorski [16] refer to condition i., while others, such as Hughes and Cresswell [8] and Mendelson [15] refer to condition ii. Condition iii., which reads "q is a consequence of p and p is a consequence of q" is less common but has the advantage of not assuming the existence of implication or conjunction in our propositional language. In many cases, i.–iii. are equivalent conditions in a given propositional theory. We now consider certain properties on a propositional theory $\mathscr{T}$ which entail that conditions i.–iii. are equivalent in $\mathscr{T}$.

Lemma 4.2.3. *In a propositional theory $\mathscr{T}$ with binary implication and conjunction connectives, we have that condition i. and ii. are equivalent if for every $a, b \in Frm(\mathscr{T})$, we have that $\vdash a$ and $\vdash b$, if and only if $\vdash a \wedge b$.*

Proof. Assume that for every $a, b \in \text{Frm}(\mathscr{T})$, $\vdash a$ and $\vdash b$, if and only if $\vdash a \wedge b$. Then $\vdash p \Rightarrow q$ and $\vdash q \Rightarrow p$ if and only if $\vdash (p \Rightarrow q) \wedge (q \Rightarrow p) = p \Leftrightarrow q$. That is, i. and ii. are equivalent. □

Definition 4.2.4. Let $\mathscr{T}$ be a propositional logic with an implication connective. Then we say that $\mathscr{T}$ satisfies the **deduction theorem** if the following condition holds for any formulae p and q:

$$\Gamma \vdash p \Rightarrow q \text{ if and only if } \Gamma \cup \{p\} \vdash q$$

Lemma 4.2.5. *If $\mathscr{T}$ satisfies the deduction theorem, then conditions i. and iii. are equivalent.*

Proof. It is clear that if $\mathscr{T}$ satisfies the deduction theorem then $\vdash p \Rightarrow q$ is equivalent to $\{p\} \vdash q$ and $\vdash q \Rightarrow p$ is equivalent to $\{q\} \vdash p$. Thus, i. and iii. are equivalent. □

In particular, in the theory of classical propositional logic $\mathscr{T}_{CL}$ satisfies both properties, as can be seen in the following two results.

Lemma 4.2.6. *If a propositional theory $\mathscr{T}$ with conjunction and implication operations has axioms of the form A3., A4. and A5. and MP as a rule of inference, then i. and ii. are equivalent.*

Proof. If $\vdash p$ and $\vdash q$ then there must be a proof in $\mathscr{T}$ containing p and q. Then, we can extend this proof as follows:

1. $p \Rightarrow (q \Rightarrow (p \wedge q))$ by A5.

2. $q \Rightarrow (p \wedge q)$ by assumption and MP.

3. $p \wedge q$ by assumption and MP.

On the other hand, if $\vdash p \wedge q$ then there is a proof in $\mathscr{T}$ containing $p \wedge q$. Then once again we can extend this proof with the following formulae:

1. $(p \wedge q) \Rightarrow p$ by A3.

2. p by assumption and MP.

3. $(p \wedge q) \Rightarrow q$ by A4.

4. q by assumption and MP.

and so by Lemma 4.2.3 we have that i. and ii. are equivalent in $\mathscr{T}$. □

The next theorem is given in Mendelson [15] as the deduction theorem for classical logic.

Theorem 4.2.7. *If a propositional theory $\mathscr{T}$ with an implication connective $\Rightarrow$ has axioms A1., A2. and the only rule of inference is MP, then $\mathscr{T}$ satisfies the deduction theorem.*

Proof. Let $p_1, p_2, ..., p_n$ be a proof of q from $\Gamma \cup \{p\}$, such that $p_n = q$. Then we prove inductively that for any $i \in \{1, ..., n\}$ that $\Gamma \vdash p \Rightarrow p_i$. First, suppose $i = 1$. Then either p_1 is an axiom, an element of Γ or $p_1 = p$. If p_1 is an axiom or an element of Γ, we have that, by A1., $p_1 \Rightarrow (p \Rightarrow p_1)$ is an axiom and so by MP and the fact that $p_1 \in \Gamma \cup A$ we have $\Gamma \vdash p \Rightarrow p_1$. If $p_1 = p$ then $\vdash p \Rightarrow p_1$ by Theorem 4.1.9, and therefore $\Gamma \vdash p \Rightarrow p_1$. Note that Theorem 4.1.9 holds in $\mathscr{T}$ since its proof relies only on A1., A2. and MP.

Then if we assume that $\Gamma \vdash p \Rightarrow p_j$ for all j such that $1 \leq j < k$, we want to show that $\Gamma \vdash p \Rightarrow p_k$. If $\Gamma \cup \{p\} \vdash p_k$ then either p_k is an axiom, an element of $\Gamma \cup \{p\}$, or p_k is a direct consequence of MP from p_{j_1} and p_{j_2} such that $j_1, j_2 < k$. In the first two cases, using the same argument as the previous paragraph $\Gamma \vdash p \rightarrow p_k$. In the third case, since we are applying MP, we can assume that $p_{j_2} = p_{j_1} \Rightarrow (p \Rightarrow p_k)$ without loss of generality. Then we have the following:

1. $\Gamma \vdash p \Rightarrow p_{j_1}$ by assumption.

2. $\Gamma \vdash p \Rightarrow (p_{j_1} \Rightarrow (p \Rightarrow p_k))$ by assumption.

3. $\Gamma \vdash (p \Rightarrow (p_{j_1} \Rightarrow (p \Rightarrow p_k))) \Rightarrow ((p \Rightarrow p_{j_1}) \Rightarrow (p \Rightarrow (p \Rightarrow p_k)))$ by A2.

4. $\Gamma \vdash (p \Rightarrow p_{j_1}) \Rightarrow (p \Rightarrow (p \Rightarrow p_k))$ by MP on 2. and 3.

5. $\Gamma \vdash p \Rightarrow (p \Rightarrow p_k)$ by MP on 1. and 4.

6. $\Gamma \vdash (p \Rightarrow (p \Rightarrow p_k)) \Rightarrow ((p \Rightarrow p) \Rightarrow (p \Rightarrow p_k))$ by A2.

7. $\Gamma \vdash (p \Rightarrow p) \Rightarrow (p \Rightarrow p_k)$ by MP applied to 5. and 6.

8. $\Gamma \vdash p \Rightarrow p$ by Theorem 4.1.9.

9. $\Gamma \vdash p \Rightarrow p_k$ by MP applied to 7. and 8.

Therefore, by induction $\Gamma \vdash p \Rightarrow p_k$ for all $k \in \{1, ..., n\}$ and in particular $\Gamma \vdash p \Rightarrow p_n$.

In order to prove the converse, simply note that if $\Gamma \vdash p \Rightarrow q$, then $\Gamma \cup \{p\} \vdash p \Rightarrow q$ and $\Gamma \cup \{p\} \vdash p$. Hence, by MP $\Gamma \cup \{p\} \vdash q$. □

Note that the proof above does not hold if there are rules of inference in $\mathscr{T}$ which are not MP, since in our inductive step we assume either $p_k \in A \cup \Gamma \cup \{p\}$ or p_k is a consequence of MP. If there were more rules we would have to consider cases where p_k is a consequence of these rules as well.

The above results shows that for $\mathscr{T}_{CL}$, as well as other theories which satisfy the specified conditions above, the conditions i., ii., and iii are equivalent when defining logical equivalence. In fact, in each propositional theory we consider in this dissertation, the conditions i. and ii. are equivalent. For the rest of the dissertation, we then consider the logical equivalence generated by condition i.

Definition 4.2.8. If $\mathscr{T}$ is a propositional theory with an implication binary connective $\Rightarrow$, then we define $\Psi \subseteq \mathrm{Frm}(\mathscr{T}) \times \mathrm{Frm}(\mathscr{T})$ as follows:

$$(p, q) \in \Psi \text{ if and only if } \vdash_{\mathscr{T}} p \Rightarrow q \text{ and } \vdash_{\mathscr{T}} q \Rightarrow p.$$

Note 4.2.9. In the above definition, since $\mathrm{Frm}(\mathscr{T}) \times \mathrm{Frm}(\mathscr{T}) \cong F_\Omega(X) \times F_\Omega(X)$, let us define Φ to be the image of Ψ under the isomorphism between the sets. Then we can consider the set Φ^{**}, the closure of Φ under algebraic consequence, and let Ψ^{**} denote the image of Φ^{**} under the isomorphism $F_\Omega(X) \times F_\Omega(X) \cong \mathrm{Frm}(\mathscr{T}) \times \mathrm{Frm}(\mathscr{T})$. Then, since Φ^{**} is a congruence, its image under isomorphism will also be a congruence, and we obtain an Ω-algebra, $\mathrm{Frm}(\mathscr{T})/\Psi^{**}$. In many cases Ψ is a congruence and in these cases $\Psi^{**} = \Psi$. We will see later in the chapter that this is the case for $\mathscr{T}_{CL}$.

Definition 4.2.10. For a propositional theory (with implication) $\mathscr{T}$ we call the algebra $\mathrm{Frm}(\mathscr{T})/\Psi^{**}$ the **Lindenbaum–Tarski algebra** for $\mathscr{T}$. Since $F_\Omega(X)/\Phi^{**}$ is isomorphic to $\mathrm{Frm}(\mathscr{T})/\Psi^{**}$, we will use this term to refer to both algebras interchangeably.

Note 4.2.11. Since X is a countably infinite set, $F_\Omega(X)$ is the term algebra over X, and moreover, by Lemma 3.6.6, the Lindenbaum–Tarski algebra for $\mathscr{T}$, $F_\Omega(X)/\Phi^{**}$ is the free (Ω, Φ)-algebra over X. Then our set Φ determines a variety of algebras $\mathbb{V} = \mathbf{Alg}(\Omega, \Phi)$ such that $A \vDash (t, t')$ for all $A \in \mathbb{V}$ if and only if $[t] = [t']$ in the Lindenbaum–Tarski algebra of $\mathscr{T}$. In this case, we say that $\mathbb{V}$ is the **variety of Ω-algebras determined by** $\mathscr{T}$, denote it by $\mathbb{V}(\mathscr{T})$.

Lemma 4.2.12. *Let $\mathscr{T}$ and $\mathscr{T}'$ be propositional theories with the same language. Define A and A' as the sets of axioms and $\mathscr{R}$ and $\mathscr{R}'$ as the sets of rules of inference for $\mathscr{T}$ and $\mathscr{T}'$ respectively. Then if $A \subseteq A'$ and $\mathscr{R} \subseteq \mathscr{R}'$, it follows that $\mathbb{V}(\mathscr{T}')$ is a subvariety of $\mathbb{V}(\mathscr{T})$.*

Proof. If $A \subseteq A'$ and $\mathscr{R} \subseteq \mathscr{R}'$, then it is clear that any sequence of formulae which are a proof in $\mathscr{T}$ can also be given as a proof in $\mathscr{T}'$. Therefore, if $\vdash_{\mathscr{T}} p \Rightarrow q$ and $\vdash_{\mathscr{T}} q \Rightarrow p$ then $\vdash_{\mathscr{T}'} p \Rightarrow q$ and $\vdash_{\mathscr{T}'} q \Rightarrow p$. Hence if $(p, q) \in \Psi$ then $(p, q) \in \Psi'$ where Ψ and Ψ' are the subsets of logically equivalent statements for $\mathscr{T}$ and $\mathscr{T}'$ respectively. Then if we consider the images of Ψ and Ψ' under the isomorphism $\mathrm{Frm}(\mathscr{T}) \times \mathrm{Frm}(\mathscr{T}) \cong F_\Omega(X) \times F_\Omega(X)$ and denote them Φ and Φ' respectively, we obtain that $\Phi \subseteq \Phi'$ and by Lemma 3.8.6 we have,

$$\mathbb{V}(\mathscr{T}') = \mathbf{Alg}(\Omega, \Phi') \leq \mathbf{Alg}(\Omega, \Phi) = \mathbb{V}(\mathscr{T}).$$

□

Note 4.2.13. In this section, we have constructed algebras from propositional theories through the use of implication connectives in the propositional language. However, we must also consider the case where a language has multiple implication connectives which are not always equivalent. For example, in the language of modal logic (which will be discussed in more detail in the next chapter) we have two implication connectives, where the symbol $\Rightarrow$ represents "usual" implication, and the symbol $\multimap$ represents strict implication [8]. In the case of languages with multiple implication operations $\Rightarrow_1, \Rightarrow_2, ... \Rightarrow_n$ it is worth noting that the algebraic variety obtained using Definition 4.2.8 may depend on which implication connective is used. In this situation, the choice of which implication should be used to induce our congruence depends on which implication best represents "logical equivalence" in a given theory. Thus, while we note that different implication operations may induce different algebraic structures, we will not discuss in this dissertation the problem of which implication ought to be used in a given theory.

4.3 The Algebraic Variety of $\mathscr{T}_{CL}$

In this section, we apply our previous work to the case of $\mathscr{T}_{CL}$, by constructing the Lindenbaum–Tarski algebra for the theory of classical logic, and conclude that $\mathbb{V}(\mathscr{T}_{CL}) = \mathbf{Bool}$. Moreover, many of the propositions given in order to construct our main result apply to different theories, which do not contain all the axioms of $\mathscr{T}_{CL}$. In particular, many results here apply to the theory of intuitionistic logic. Many of the results here can be found in Borceux [6] and Rasiowa and Sikorski [16].

Lemma 4.3.1. *Let $\mathscr{L}_{CL}$ be the language of $\mathscr{T}_{CL}$. If we consider $\Psi \subseteq Frm(\mathscr{L}_{CL}) \times Frm(\mathscr{L}_{CL})$ defined as in Definition 4.2.8, then we have that Ψ is an equivalence class for any theory such that A1. and A2. are axioms and MP is a rule of inference.*

Proof. By Lemma 4.1.9, $\vdash p \Rightarrow p$ for any formula p and so Ψ is reflexive. Clearly, if $(p, q) \in \Psi$ then $\vdash p \Rightarrow q$ and $\vdash q \Rightarrow p$ gives us that $(q, p) \in \Psi$. Hence Ψ is symmetric. Furthermore, if $\vdash p \Rightarrow q$ and $\vdash q \Rightarrow r$ we have:

1. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ by A2.

2. $q \Rightarrow r$ by assumption.

3. $(q \Rightarrow r) \Rightarrow (p \Rightarrow (q \Rightarrow r))$ by A1.

4. $(p \Rightarrow (q \Rightarrow r))$ by MP on 2. and 3.

5. $(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$ by MP on 1. and 4.

6. $p \Rightarrow q$ by assumption.

7. $p \Rightarrow r$ by MP on 5. and 6.

Using a similar argument, we can show $\vdash r \Rightarrow p$. Hence, Ψ is transitive. $\square$

Corollary 4.3.2. *The relation $\leq$ on Frm$(\mathscr{L}_{CL})/\Psi$, defined by $[p] \leq [q]$ if and only if $\vdash p \Rightarrow q$, is an order relation for any theory such that A1. and A2. are axioms and MP is a rule of inference.*

Proof. First note if $[p] = [p']$ and $[q] = [q']$ then $[p] \leq [q]$ if and only if $\vdash p \Rightarrow q$ then since $\vdash p' \Rightarrow p$ and $\vdash q \Rightarrow q'$ we have, by the proof of Lemma 4.3.1, that $\vdash p' \Rightarrow q'$. Then using a similar argument, if we assume $\vdash p' \Rightarrow q'$, we can show $\vdash p \Rightarrow q$. Hence the relation is well-defined. Moreover, from the proof of Lemma 4.3.1 we can see that $\leq$ is reflexive and transitive. Lastly, it is clear that if $[p] \leq [q]$ and $[q] \leq [p]$, by definition $(p, q) \in \Psi$. $\square$

From the above, we also obtain a preorder relation, $\preceq$ on Frm$(\mathscr{L}_{CL})$ given by $p \preceq q$ when $\vdash p \Rightarrow q$.

Lemma 4.3.3. *Let $\mathscr{T}$ be a theory with the language $\mathscr{L}_{CL}$, such that A1.–A8., and A12. are axioms and MP is a rule of inference. Then Frm$(\mathscr{L}_{CL})/\Psi$ has binary meets and joins with respect to the order in Corollary 4.3.2 where $[p] \wedge [q] = [p \wedge q]$ and $[p] \vee [q] = [p \vee q]$, and $[1]$ is the greatest element with respect to this order.*

Proof. In order to see that $[p \wedge q]$ is the infimum note that directly from A3. and A4. we get $[p \wedge q] \leq [p], [q]$. Then if $[a] \leq [p], [q]$ note that by A5. we have that $\vdash q \Rightarrow (p \Rightarrow (p \wedge q))$. Then since $[a] \leq [q]$ and $[q] \leq [(p \Rightarrow (p \wedge q))]$ by transitivity, $\vdash a \Rightarrow (p \Rightarrow (p \wedge q))$. Hence,

1. $a \Rightarrow (p \Rightarrow (p \wedge q))$ by above.

2. $(a \Rightarrow (p \Rightarrow (p \wedge q))) \Rightarrow ((a \Rightarrow p) \Rightarrow (a \Rightarrow (p \wedge q)))$ by A2.

3. $(a \Rightarrow p) \Rightarrow (a \Rightarrow (p \wedge q))$ by MP on 1. and 2.

4. $a \Rightarrow p$ by assumption.

5. $a \Rightarrow (p \wedge q)$ by MP on 3. and 4.

Then $[a] \leq [p \wedge q]$ so $[p \wedge q]$ is the infimum.

To calculate the supremum of $[p]$ and $[q]$, note that it follows directly from A6. and A7. that $[p], [q] \leq [p \vee q]$.Then if we assume $[p], [q] \leq [a]$ then we have the following proof

1. $(p \Rightarrow a) \Rightarrow ((q \Rightarrow a) \Rightarrow ((p \vee q) \Rightarrow a))$ from A6.

2. $p \Rightarrow a$ from assumption.

3. $q \Rightarrow a$ from assumption.

4. $(q \Rightarrow a) \Rightarrow ((p \vee q) \Rightarrow a)$ by MP on 1. and 2.

5. $(p \vee q) \Rightarrow a$ by MP on 3. and 4.

Hence $[p \vee q] \leq [a]$. Thus, $[p \vee q]$ is the supremum.

Since 1 is a theorem, for every formulae p we have $\vdash 1 \Rightarrow (p \Rightarrow 1)$ by A1. and by MP $\vdash p \Rightarrow 1$. Hence, $[p] \leq [1]$. □

Corollary 4.3.4. *Let $\mathscr{T}$ be a theory with language $\mathscr{L}_{CL}$ such that A1.–A8. and A12. are axioms and MP is a rule of inference. Then, for any theorem p, we have that $[p] = [1]$ in $Frm(\mathscr{L}_{CL})/\Psi$, and therefore $[1]$ is the set of all theorems of $\mathscr{T}$.*

Proof. If p is a theorem then $\vdash p$ and $\vdash p \Rightarrow (1 \Rightarrow p)$. Thus, $\vdash 1 \Rightarrow p$ and since $[1]$ is the greatest element $[p] = [1]$. □

Lemma 4.3.5. *Let $\mathscr{T}$ be a theory with language $\mathscr{L}_{CL}$ such that A1.–A8. are axioms and MP is the only rule of inference. Then the maps*

$$(- \wedge p), (p \Rightarrow -) : Frm(\mathscr{L}_{CL}) \to Frm(\mathscr{L}_{CL})$$

are order preserving with respect to $\preceq$ and $- \wedge p$ is the left adjoint of $p \Rightarrow -$, for any formula p.

Proof. The fact that $[q] \wedge [p] \leq [r] \wedge [p]$ for any formulae q and r with $[q] \leq [r]$ follows from a general result for infima, and so $q \wedge p \preceq r \wedge p$. Then if $q \preceq r$ we have $\vdash q \Rightarrow r$ and therefore $\vdash p \Rightarrow (q \Rightarrow r)$ for any formulae p. Then applying, A2. and MP, we obtain $\vdash (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$ and therefore $p \Rightarrow q \preceq p \Rightarrow r$.

In order to see that our adjunction holds, note that if $q \wedge p \preceq r$ for any formulae q and r, then

$$q \preceq p \Rightarrow (q \wedge p) \preceq p \Rightarrow r$$

where the first inequality is an application of A3. and the second follows from the fact that $p \Rightarrow -$ is order preserving. Conversely,

1. $((p \Rightarrow r) \wedge p) \Rightarrow p$ by A4.

2. $((p \Rightarrow r) \wedge p) \Rightarrow (p \Rightarrow r)$ by A3.

3. $(((p \Rightarrow r) \wedge p) \Rightarrow (p \Rightarrow r)) \Rightarrow ((((p \Rightarrow r) \wedge p) \Rightarrow p) \Rightarrow ((p \Rightarrow r) \wedge p) \Rightarrow r)$ by A2.

4. $(p \Rightarrow r) \wedge p) \Rightarrow r$ by applying MP twice on 3. with 2. and then 1.

Hence, if $q \preceq p \Rightarrow r$, then $q \wedge p \preceq (p \Rightarrow r) \wedge p \preceq r$. □

Corollary 4.3.6. *The map,*

$$(- \Rightarrow p) : Frm(\mathscr{L}_{CL}) \to Frm(\mathscr{L}_{CL})$$

is order reversing with respect to $\preceq$ for any formula p.

Proof. Assume $q \preceq r$. Then $(r \Rightarrow p) \wedge q \preceq (r \Rightarrow p) \wedge r \preceq p$ by A4 and the fact that $(r \Rightarrow p) \wedge -$ is order preserving. Then, by adjunction, $r \Rightarrow p \preceq q \Rightarrow p$ for any formula p. □

Lemma 4.3.7. *If $[p] = [p']$ and $[q] = [q']$ in $Frm(\mathscr{L}_{CL})/\Psi$ in a theory where A1.-A8. are axioms and MP is a rule of inference, then $[p \Rightarrow q] = [p' \Rightarrow q']$.*

Proof. If $[p] = [p']$ and $[q] = [q']$ then $q \preceq q'$, and we have that $p \Rightarrow q \preceq p \Rightarrow q'$. Then since $p' \preceq p$ we have $p \Rightarrow q' \preceq p' \Rightarrow q'$. That is $\vdash (p \Rightarrow q) \Rightarrow (p' \Rightarrow q')$. Using a similar argument we get $\vdash (p' \Rightarrow q') \Rightarrow (p \Rightarrow q)$ and so $[p \Rightarrow q] = [p' \Rightarrow q']$. □

We can then define the operation $\Rightarrow$ on $\text{Frm}(\mathscr{L}_{CL})/\Psi$ by $[p] \Rightarrow [q] = [p \Rightarrow q]$.

Corollary 4.3.8. *For any formula p, the maps*

$$(- \wedge [p]), ([p] \Rightarrow -) : Frm(\mathscr{L}_{CL})/\Psi \to Frm(\mathscr{L}_{CL})/\Psi$$

are order preserving with respect to $\leq$ and $(- \wedge [p])$ is the left adjoint of $([p] \Rightarrow -)$. Moreover the map $(- \Rightarrow [p]) : Frm(\mathscr{L}_{CL})/\Psi \to Frm(\mathscr{L}_{CL})/\Psi)$ is order reversing with respect to $\leq$. □

Lemma 4.3.9. *Let $\mathscr{T}$ be a theory with language $\mathscr{L}_{CL}$ such that A1.–A8. are axioms and MP is a rule of inference. Then $Frm(\mathscr{L}_{CL})/\Psi$ is a distributive lattice.*

Proof. Let $[p], [q], [r] \in \text{Frm}(\mathscr{L}_{CL})/\Psi$. Then since $- \wedge [r]$ is a left adjoint and $[p] \vee [q]$ is a coproduct in a preorder, it follows that $([p] \vee [q]) \wedge [r] = ([p] \wedge [r]) \vee ([q] \wedge [r])$ by the preliminary result that left adjoints preserve coproducts. Then since the distributive laws are equivalent to each other, we have that $\text{Frm}(\mathscr{L}_{CL})/\Psi$ is a distributive lattice. □

Lemma 4.3.10. *Let $\mathscr{T}$ be a theory with language $\mathscr{L}_{CL}$ such that A1.-A10. and A12. are axioms and MP is a rule of inference. Then in Frm($\mathscr{L}_{CL}$)/Ψ, the operation $\neg[p] = [\neg p]$ is well-defined and $[0]$ is the least element with respect to $\leq$.*

Proof. We show that under our assumptions, if $\vdash p \Rightarrow q$, then $\vdash \neg q \Rightarrow \neg p$.

1. $(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$ by A9.

2. $(p \Rightarrow q)$ by assumption.

3. $(p \Rightarrow \neg q) \Rightarrow \neg p$ by MP on 1. and 2.

4. $\neg q \Rightarrow (p \Rightarrow \neg q)$ by A1.

Therefore, since $\preceq$ is transitive, $\vdash \neg q \Rightarrow \neg p$. Then, if $[p] = [q]$ we get that $\vdash \neg q \Rightarrow \neg p$ and $\vdash \neg p \Rightarrow \neg q$. Hence, $[\neg p] = [\neg q]$, and therefore $\neg[p] = [\neg p]$ is a well-defined operation.

Moreover,

1. $\neg\neg 1 \Rightarrow (\neg 1 \Rightarrow p)$ by A10.

2. $(\neg 1 \Rightarrow 1) \Rightarrow ((\neg 1 \Rightarrow \neg 1) \Rightarrow \neg\neg 1)$ by A9.

3. $\neg 1 \Rightarrow 1$ since $[1]$ is the greatest element.

4. $\neg 1 \Rightarrow \neg 1$ by Lemma 4.1.9.

5. $\neg\neg 1$ by applying MP twice to 2 with 3 and 4.

6. $\neg 1 \Rightarrow p$ by MP on 1. and 5.

Hence $[\neg 1] \leq [p]$ and so $[0]$ is the least element. □

It follows that the Ψ is a congruence with respect to the operations in Ω.

Lemma 4.3.11. *Let $\mathscr{T}$ be a theory with language $\mathscr{L}_{CL}$ such that A1.–A10. and A12. are axioms and MP is a rule of inference. Then in Frm($\mathscr{L}_{CL}$)/Ψ we have that $[p \Rightarrow 0] = [\neg p]$ and $[\neg p \wedge p] = [0]$.*

Proof. First we note $\vdash \neg p \Rightarrow (p \Rightarrow 0)$ directly from A10. Then,

1. $(p \Rightarrow 1) \Rightarrow ((p \Rightarrow \neg 1) \Rightarrow \neg p)$ by A9.

2. $p \Rightarrow 1$ since $[1]$ is the greatest element.

3. $(p \Rightarrow 0) \Rightarrow \neg p$ by MP on 1. and 2., and $0 = \neg 1$.

Therefore $[p \Rightarrow 0] = [\neg p]$. Moreover, applying our adjunction to $[p] \Rightarrow [0] \leq [p] \Rightarrow [0]$, we obtain $([p] \Rightarrow [0]) \wedge p \leq [0]$. Hence, $[(p \Rightarrow 0) \wedge p] = [\neg p \wedge p] \leq [0]$ and since $[0]$ is the least element $[\neg p \wedge p] = [0]$. □

Our last result, as well as the fact that $[\neg p \vee p] = [1]$ in $\mathrm{Frm}(\mathscr{L})/\Psi$, for any formula p, by axiom A11., allows us to conclude the following theorem.

Theorem 4.3.12. *$Frm(\mathscr{T}_{CL})/\Psi$ is a Boolean algebra, and any Boolean algebra, B, satisfies the property that $p = q$ if and only if $p \Rightarrow q = 1$ and $q \Rightarrow p = 1$.*

Proof. The first part is proved from the above results. For the second part, we can see if $p = q$ then clearly $p \Rightarrow p = \neg p \vee p = 1$ and if $p \Rightarrow q = 1$ then $p \leq q$. Hence, if $q \Rightarrow p = 1$ then $p = q$. □

Corollary 4.3.13. *In $Frm(\mathscr{T}_{CL})/\Psi$, we have that $\neg[p] \vee [q] = [p] \Rightarrow [q]$ for all $p, q \in Frm(\mathscr{L}_{CL})$.*

Proof. Since adjoint are unique up to isomorphism, it is sufficient to prove that $[p] \wedge [q] \leq [r]$ if and only if $[p] \leq \neg[q] \vee [r]$. Note that if $[p] \wedge [q] \leq [r]$ then,

$$[p] \leq (\neg[q] \vee [p]) = (\neg[q] \vee [q]) \wedge (\neg[q] \vee [p]) = \neg[q] \vee ([q] \wedge [p]) \leq \neg[q] \vee [r].$$

On the other hand, if $[p] \leq \neg[q] \vee [r]$, then

$$[p] \wedge [q] \leq (\neg[q] \vee [r]) \wedge [q] = (\neg[q] \wedge [q]) \vee (\neg[q] \wedge [r]) = \neg[q] \wedge [r] \leq [r]$$

and we are done. □

Corollary 4.3.14. *Using the notation in Definition 4.2.10, $\Phi = \Phi^{**}$, and therefore*

a. $\Psi = \Psi^{**}$.

b. *$F_{\Omega}(X)/\Phi$, is the free Boolean algebra over the countably infinite set X.*

Proof. We have that $B \vDash (p, q)$ for all $(p, q) \in \Phi$, if and only if B is a Boolean algebra. Then, since Φ is a congruence such that $F_{\Omega}(X)/\Phi$ is a Boolean algebra, we must have that it is the smallest congruence containing Φ such that this holds, and so $\Phi^{**} = \Phi$. □

This allows to the conclude that the models of the Lindenbaum–Tarski algebra for classical logic is the variety of Boolean algebras. That is, $\mathbb{V}(\mathscr{T}_{CL}) = \mathbf{Bool}$.

Note 4.3.15. This correspondence between the formal theory of classical logic and the variety of Boolean algebras also shows us the following:

- The set of algebraic axioms for Boolean algebras given in our last chapter in Example 3.2.10 is a sufficient and much smaller set of algebraic axioms in order to induce the congruence Φ as given in the above result.
- In Chapter 2, we gave the Definition 2.5.1 of a theory of classical logic as a pair (Y, A) where Y is a set of variables and A is a set of elements in the free Boolean algebra over Y. in this case, we are considering the theory obtained from $\mathscr{T}_{CL}$ where we restrict (or change) the variables from a countably infinite set X to the set Y, and then consider terms in $F_\Omega(Y)$ rather than $F_\Omega(X)$. Then the axioms and rule of inferences in $\mathscr{T}_{CL}$ apply to all those terms in $F_\Omega(Y)$, while the axioms A in the pair (Y, A) are added to the original axioms of $\mathscr{T}_{CL}$, to obtain a stronger theory which includes all those theorems of $\mathscr{T}_{CL}$, when applied to the terms in $F_\Omega(Y)$.

We consider now the algebra induced by a "stronger" theory of classical logic (Y, A). One (previously considered) method is to consider the free Boolean algebra $F_{\mathbf{Bool}}(Y)$ and then incorporate the axioms in A by taking the smallest filter containing A and taking the quotient of $F_{\mathbf{Bool}}(Y)$ induced by this filter. However, in the next example we consider a different approach, using the methods introduced in this chapter.

Example 4.3.16. Suppose we add as an additional axiom to our theory $\mathscr{T}_{CL}$ the single identity $x \wedge y = z$ for variables x, y, z. That is, $x \wedge y$ is logically equivalent to z. It is important to note, that to calculate the resulting algebra, we cannot simply add $(x \wedge y, z)$ to the algebraic axioms for **Bool**, Φ, given in Example 3.2.10, since the variety induced by $\Phi \cup \{(x \wedge y, z)\}$ would be the trivial variety.

Therefore, in order to introduce our axiom into our algebraic identities, we define x, y and z as nullary operations for our algebra. Then, let $\Omega' = \Omega_{\mathbf{Bool}} \cup \{x, y, z\}$, and $\Phi = \Phi_{\mathbf{Bool}} \cup \{(x \wedge y, z)\}$, and the algebra $F_{\Omega'}(X - \{x, y, z\})/\Phi'$ is the algebra which corresponds to our theory, since it requires that $x \wedge y = z$ for the desired variables, but not that $p \wedge q = r$ for any $p, q, r \in F_\Omega(X)$. We also remove the variables which occur in the axiom from X in order for the signature and the algebraic variables to be disjoint sets.

This can be applied in general to $F_{(\Omega,\Phi)}(X)$ where $\mathbf{Alg}(\Omega, \Phi) = \mathbb{V}(\mathscr{T})$ for some theory $\mathscr{T}$. If we add a set of axioms A which only apply to certain variables of our theory, then we add the set of variables in these axioms, denoted V_A, to the set of nullary operations in Ω. Then we compute $F_{\Omega\cup V}(X - V)/(\Phi \cup A)^{**}$ to obtain the corresponding algebra.

In the case where a new set of axioms are given which apply to every variable, we do not need to change the signature for our free algebra, and only add the given identity to our axioms and calculate the corresponding congruence. For example, if we have an algebra $F_\Omega(X)/\Phi$ corresponding to some theory $\mathscr{T}$, and we introduce the set of axioms $A' = \{(\neg p \vee q, p \Rightarrow q) \mid p, q \in F_\Omega(X)\}$, the resulting algebra is given by $F_\Omega(X)/(\Phi \cup \{(\neg p \vee q, p \Rightarrow q)\})^{**}$.

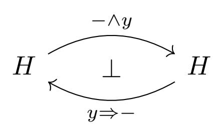
5 Algebraic Varieties for Non-Classical Logic

In this chapter, we consider some theories of non-classical logic and their corresponding algebraic varieties. Furthermore, we consider the completeness of certain varieties with regards to their L-valued models, and thus determine whether algorithms similar to those constructed for classical logic in Chapter 2 exist for these theories of non-classical logic.

5.1 Heyting Algebras

Definition 5.1.1. [6]. A **Heyting algebra** $H = (H, \wedge, 1, \vee, 0, \Rightarrow)$ is an algebra such that

1. $(H, \wedge, 1, \vee, 0)$ is a lattice.
2. The binary operation $\Rightarrow: H \times H \to H$, called *implication*, is defined such that there is an adjunction,



   for each $y \in H$.

That is, for $x, y, z \in H$, $x \wedge y \leq z$ if and only if $x \leq y \Rightarrow z$. We denote the category of Heyting algebras by **Heyt**.

Lemma 5.1.2. *In a Heyting algebra H, $x \Rightarrow y = \bigvee\{z \mid z \wedge x \leq y\}$ for all $x, y \in H$.*

Proof. By definition, if $z \in \{z \mid z \wedge x \leq y\}$ we have $z \leq x \Rightarrow y$ by adjunction. Moreover, since $x \Rightarrow y \leq x \Rightarrow y$, by our adjunction $(x \Rightarrow y) \wedge x \leq y$. Thus, $x \Rightarrow y$ is the greatest element of $\{z \mid z \wedge x \leq y\}$. □

Example 5.1.3. Let (X, τ) be a topological space, where τ denotes the set of open sets in the space. Then $(\tau, \cap, X, \cup, \emptyset, \Rightarrow)$ is a Heyting algebra, ordered by $\subseteq$, where $A \Rightarrow B = \bigcup\{C \in \tau \mid C \cap A \subseteq B\}$. Since τ is closed under arbitrary union, $A \Rightarrow B \in \tau$ for all $A, B \in \tau$. Moreover, by Lemma 5.1.2, $\Rightarrow$ satisfies the properties of implication in a Heyting algebra.

Example 5.1.4. Let $(C, \leq)$ be a chain with a top and bottom element, called 1 and 0 respectively. Then $(C, \wedge, 0, \vee, 1, \Rightarrow)$ is a Heyting algebra, where

$$x \Rightarrow y = \begin{cases} 1 \text{ if } x \leq y \\ y \text{ if } y \leq x \end{cases}$$

for all $x, y \in C$. Assume that $z \wedge x \leq y$. Then, if $x \leq y$, trivially $z \leq x \Rightarrow y = 1$. If $y \leq x$, since C is totally ordered, $z \wedge x \leq y \leq x$ implies $z \wedge x = z \leq y$ and thus $z \leq y = x \Rightarrow y$. Conversely, assume $z \leq x \Rightarrow y$. Then $x \leq y$ implies that $z \wedge x \leq x \leq y$ and $y \leq x$ implies $z \leq x \Rightarrow y = y$ and therefore $z \wedge x \leq z \leq y$. Hence, our operation $\Rightarrow$ satisfies the adjunction in Definition 5.1.1.

Definition 5.1.5. The **theory of intuitionistic propositional logic** $\mathscr{T}_{IL}$ is a formal theory where,

1. The language of $\mathscr{T}_{IL}$ is the same as the language of $\mathscr{T}_{CL}$.

2. The axioms of $\mathscr{T}_{IL}$ are all formulae of the form A1.-A10. and A12. as in Example 4.1.7.

3. The only rule of inference is *modus ponens* (MP).

That is, $\mathscr{T}_{IL}$ is the theory obtained by removing the axiom A11. from the theory of classical propositional logic. A11. is also known as the **law of excluded middle**.

It is a direct result of the results in Section 4.3. in our previous chapter, that the free algebra induced by $\mathscr{T}_{IL}$ is a Heyting algebra. Moreover, in order to see that equality between elements of a Heyting algebra can be induced by the same relation Ψ as in Lemma 4.3.1, we prove the following.

Lemma 5.1.6. *Let H be a Heyting algebra. Then for any $x, y \in H$, we have $x = y$ if and only if $x \Rightarrow y = 1$ and $y \Rightarrow x = 1$.*

Proof. If $1 \leq x \Rightarrow y$, then by adjunction this is equivalent to $x = 1 \wedge x \leq y$. □

Thus, we can conclude that the variety induced by the theory of intuitionistic propositional logic is the variety of Heyting algebras.

Theorem 5.1.7. $\mathbb{V}(\mathscr{T}_{IL}) =$ ***Heyt***. □

Furthermore, we obtain the following results directly from results in Chapter 4.

Corollary 5.1.8. *Let H be a Heyting algebra. Then,*

a. $\neg : H \to H$ *is a well-defined operation where* $\neg x = x \Rightarrow 0$.

b. H *is a distributive lattice.*

c. $- \Rightarrow x : H \to H$ *is an order reversing map.*

d. $x \Rightarrow x = 1$.

e. $\neg x \wedge x = 0$.

for any $x \in H$. □

Definition 5.1.9. For any element x of a Heyting algebra H the element $\neg x$ is called the **pseudocomplement** of x. Moreover, by Lemma 5.1.2, we can see that $x \Rightarrow 0$ is the greatest element of H such that $x \wedge \neg x = 0$.

Note 5.1.10. In $\mathscr{T}_{IL}$, we see that the law of excluded middle is a not an axiom of our theory. In fact, it is not a theorem since it does not hold for Heyting algebras in Examples 5.1.3 and 5.1.4. If we consider the real numbers $\mathbb{R}$ with its usual topology, and consider the open set $(-\infty, 0)$, we observe that the pseudocomplement of $(-\infty, 0)$ is the set $(0, \infty)$, and $(-\infty, 0) \cup (0, \infty) \neq \mathbb{R}$.
Furthermore, in the three element chain $\{0, 1, 2\}$ with its usual ordering, we have that $\neg 1 = 1 \Rightarrow 0 = 0$ and hence $1 \vee \neg 1 = 1 \vee 0 = 1$.

We are further able to find a set of equalities which are equivalent to the adjunction given in Definition 5.1.1. This characterization for Heyting algebras is given in Burris and Sankappanavar [7], and provides a finite set Φ of algebraic axioms which characterize the variety of Heyting algebras.

Lemma 5.1.11. $H = (H, \wedge, 1, \vee, 0, \Rightarrow)$ *is a Heyting algebra if and only if* $\Rightarrow$ *is a binary operation on* H *such that,*

a. $(H, \wedge, 1, \vee, 0)$ *is a distributive lattice.*

b. $x \Rightarrow x = 1$.

c. $(x \Rightarrow y) \wedge y = y$ *and* $x \wedge (x \Rightarrow y) = x \wedge y$.

d. $x \Rightarrow (y \wedge z) = (x \Rightarrow y) \wedge (x \Rightarrow z)$ *and* $(x \vee y) \Rightarrow z = (x \Rightarrow z) \wedge (y \Rightarrow z)$.

for all $x, y, z \in H$.

Proof. Let H be a Heyting algebra. Then by Corollary 5.1.8 we have that a. and b. hold. Then, note that $(x \Rightarrow y) \wedge y \leq y$, and since $y \wedge x \leq y$, by adjunction, $y \leq x \Rightarrow y$. Thus, $y \leq (x \Rightarrow y) \wedge y$. Furthermore, $x \Rightarrow y \leq x \Rightarrow y$ is equivalent to $x \wedge (x \Rightarrow y) \leq y$ and since $x \wedge (x \Rightarrow y) \leq x$, we have $x \wedge (x \Rightarrow y) \leq x \wedge y$. Then $x \wedge y = x \wedge y \wedge x \leq y$ implies $x \wedge y \leq x \Rightarrow y$. Moreover $x \wedge y \leq x$ implies $x \wedge y \leq (x \Rightarrow y) \wedge x$. Hence the equalities in c. hold.

In order to see that d. holds in H, observe that by c., $x \wedge (x \Rightarrow (y \wedge z)) = x \wedge y \wedge z \leq y$ and by adjunction we obtain $x \Rightarrow (y \wedge z) \leq x \Rightarrow y$. Similarly, $x \Rightarrow (y \wedge z) \leq x \Rightarrow z$ and so $x \Rightarrow (y \wedge z) \leq (x \Rightarrow y) \wedge (x \Rightarrow z)$. Then, from the inequality $x \wedge y \wedge z \leq y \wedge z$, applying c. twice gives us $x \wedge y \wedge z = x \wedge (x \Rightarrow y) \wedge (x \Rightarrow z) \leq y \wedge z$ and so by adjunction $(x \Rightarrow y) \wedge (x \Rightarrow z) \leq x \Rightarrow (y \wedge z)$, and the first equality in d. holds.

Then note that since $x \leq x \vee y$ and $- \Rightarrow z : H \to H$ is order-reversing, we have that $(x \vee y) \Rightarrow z \leq x \Rightarrow z$. Similarly $(x \vee y) \Rightarrow z \leq y \Rightarrow z$ and so $(x \vee y) \Rightarrow z \leq (x \Rightarrow z) \wedge (y \Rightarrow z)$. On the other hand, note that,

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

By adjunction, this implies $(x \Rightarrow y) \wedge (y \Rightarrow z) \leq (x \vee y) \Rightarrow z$, and so d. holds.

Conversely, suppose H satisfies a.–d. and let $x, y, z \in H$. Note that if $x \leq y$ then $(z \Rightarrow x) \wedge (z \Rightarrow y) = z \Rightarrow (x \wedge y) = z \Rightarrow x$ and so $z \Rightarrow x \leq z \Rightarrow y$. Hence, $z \Rightarrow - : H \to H$ is order preserving. Then, if $x \wedge y \leq z$, we have that $y \Rightarrow (x \wedge y) \leq y \Rightarrow z$ and by b. and d. $y \Rightarrow (x \wedge y) = (y \Rightarrow x) \wedge (y \Rightarrow y) = (y \Rightarrow x)$. Thus $x \wedge (y \Rightarrow x) = x$ by b., which gives us $x \leq y \Rightarrow x \leq y \Rightarrow z$. Lastly, if $x \leq y \Rightarrow z$ then $x \wedge y \leq (y \Rightarrow z) \wedge y = y \wedge z \leq z$ and so H is a Heyting algebra. □

Thus, **Heyt** $= \mathbf{Alg}(\Omega, \Phi)$ where $\Omega = \{0, 1, \vee, \wedge, \Rightarrow\}$ and Φ is given by the algebraic axioms of a distributive lattice with the equalities in b., c., and d. as above.

Lemma 5.1.12. [6]**.** *Any finite distributive lattice L is a Heyting algebra.*

Proof. Since L is finite, for any $A \subseteq L$ we have that $\bigvee A \in L$. In particular, for any elements $x, y \in L$, $x \Rightarrow y = \bigvee\{z \in L \mid z \wedge x \leq y\} \in L$. □

Lemma 5.1.13. *The mapping $\neg : H \to H$ induces a Galois connection*

$$H \underset{\neg}{\overset{\neg}{\rightleftarrows}} H$$

on any Heyting algebra H.

Proof. Since $\neg$ is an order reversing map, if $x \leq y$ in H, then $\neg y \leq \neg x$. Moreover, since $x \wedge \neg x \leq 0$, we have by adjunction that $x \leq \neg x \Rightarrow 0 = \neg\neg x$. □

Corollary 5.1.14. *From previous results for Galois connections, we then obtain the following results for any Heyting algebra H and any elements $x, y \in H$.*

a. $\neg\neg : H \to H$ *is a closure operator.*

b. $\neg\neg\neg x = \neg x$.

c. $\neg(x \vee y) = \neg x \wedge \neg y$.

d. $\neg\neg(x \wedge y) = \neg\neg x \wedge \neg\neg y$.

Lemma 5.1.15. *For any Heyting algebra H and any elements $x, y, z \in H$,*

a. $\neg x \vee y \leq x \Rightarrow y$

b. $\neg x \vee \neg y \leq \neg(x \wedge y)$

c. $(x \Rightarrow y) \wedge (y \Rightarrow z) \leq (x \Rightarrow z)$.

Proof. a. $(\neg x \vee y) \wedge x = (\neg x \wedge x) \vee (x \wedge y) = x \wedge y \leq y$ and hence, by adjunction $\neg x \vee y \leq x \Rightarrow y$.

b. $0 = (x \wedge \neg x) \vee (y \wedge \neg y) = (x \wedge \neg x \wedge y) \vee (y \wedge \neg y \wedge x) = (\neg x \vee \neg y) \wedge (x \wedge y)$. Again, by adjunction, $\neg x \vee \neg y \leq (x \wedge y) \Rightarrow 0 = \neg(x \wedge y)$.

c. Since, $x \wedge (x \Rightarrow y) \wedge (y \Rightarrow z) = x \wedge y \wedge (y \Rightarrow z) = x \wedge y \wedge z \leq z$, we obtain $(x \Rightarrow y) \wedge (y \Rightarrow z) \leq x \Rightarrow z$ by adjunction.

□

Lemma 5.1.16. *For any Heyting algebra H and any elements $x, y, z \in H$,*

a. $\neg\neg(x \Rightarrow y) = \neg\neg x \Rightarrow \neg\neg y$.

b. $(x \wedge y) \Rightarrow z = x \Rightarrow (y \Rightarrow z)$

c. $x \Rightarrow 1 = x$.

Proof. a. $\neg\neg x \wedge \neg\neg(x \Rightarrow y) = \neg\neg(x \wedge (x \Rightarrow y)) = \neg\neg(x \wedge y) = \neg\neg x \wedge \neg\neg y \leq \neg\neg y$. Then, by adjunction, $\neg\neg(x \Rightarrow y) \leq \neg\neg x \Rightarrow \neg\neg y$.

On the other hand, $(\neg\neg x \Rightarrow \neg\neg y) \wedge \neg\neg x = \neg\neg y \wedge \neg\neg x \leq \neg\neg y$. Therefore $(\neg\neg x \Rightarrow \neg\neg y) \wedge \neg\neg x \wedge \neg y = 0$. From this we further obtain $(\neg\neg x \Rightarrow \neg\neg y) \wedge \neg(x \Rightarrow y) \leq (\neg\neg x \Rightarrow \neg\neg y) \wedge \neg(\neg x \vee y) = 0$ by applying Corollary 5.1.14 and the fact that $\neg x \vee y \leq x \Rightarrow y$ and $\neg$ is order reversing. Therefore, $\neg\neg x \Rightarrow \neg\neg y \leq \neg(x \Rightarrow y) \Rightarrow 0 = \neg\neg(x \Rightarrow y)$.

b. $x \wedge y \wedge ((x \wedge y) \Rightarrow z) = x \wedge y \wedge z \leq z$. Applying the adjunction twice we get $(x \wedge y) \Rightarrow z \leq x \Rightarrow (y \Rightarrow z)$. On the other hand, $x \wedge y \wedge (x \Rightarrow (y \Rightarrow z)) = x \wedge y \wedge (y \Rightarrow z) = x \wedge y \wedge z \leq z$. Therefore, by adjunction $x \Rightarrow (y \Rightarrow z) \leq (x \wedge y) \Rightarrow z$.

c. Since $x \wedge 1 \leq x$, we have $x \leq 1 \Rightarrow x$ and since $1 \Rightarrow x \leq 1 \Rightarrow x$ then $1 \Rightarrow x = (1 \Rightarrow x) \wedge 1 \leq x$.

□

It is worth noting that the above results tell us certain equational properties that hold in all Heyting algebras, and hence, give us logical equivalences in $\mathscr{T}_{IL}$. We now consider a similar characterization of quotient Heyting algebras as was observed in the category **Bool**.

Lemma 5.1.17. [16]**.** *If H is a Heyting algebra, then a subset $F \subseteq H$ is a filter on H if and only if $E_F = \{(x, y) \mid x \Leftrightarrow y \in F\}$ is a congruence on H.*

Proof. Note that if F is a filter, then since $\Leftrightarrow$ is commutative, and $x \Rightarrow x = 1 \in F$ for all $x \in H$, we have that E_F is reflexive and symmetric. Moreover, if $x \Rightarrow y, y \Rightarrow z \in F$, then $(x \Rightarrow y) \wedge (y \Rightarrow z) \leq x \Rightarrow z$ and so $x \Rightarrow z \in F$. Similarly, $y \Rightarrow x, z \Rightarrow y \in F$ implies that $z \Rightarrow x \in F$, and so $x \Leftrightarrow y, y \Leftrightarrow z \in F$ implies that $x \Leftrightarrow z \in F$. Thus, E_F is an equivalence relation.

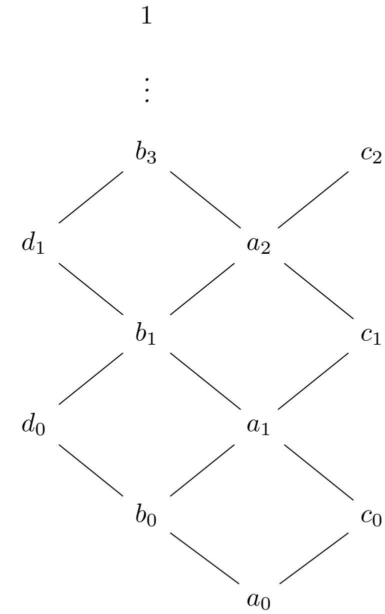
Note that from the above we also obtain a partial order on H/E_F defined by $[x] \leq [y]$ if $x \Rightarrow y \in F$. Then since $(x \wedge y) \Rightarrow x = 1 \in F$ for all $x, y \in H$, we have that $[x \wedge y] \leq [x], [y]$, and moreover, if $[z] \leq [x], [y]$, then $z \Rightarrow x, z \Rightarrow y \in F$, and so $(z \Rightarrow x) \wedge (z \Rightarrow y) = z \Rightarrow (x \wedge z) \in F$. Hence, $[z] \leq [x \wedge y]$, and so $[x \wedge y] = [x] \wedge [y]$. Using a similar proof, and the identity that $(x \Rightarrow z) \wedge (y \Rightarrow z) = (x \vee y) \Rightarrow z$ for all $x, y, z \in H$, we obtain $[x \vee y] = [x] \vee [y]$.

Now note that for all $x \in H$, $0 \Rightarrow x = 1 = x \Rightarrow 1$ and since $1 \in F$, $[0]$ and $[1]$ are the least and greatest elements of H/E_F. Then note that $[z \wedge x] \leq [y]$ if and only if, $(z \wedge x) \Rightarrow y \in F$ if and only if $z \Rightarrow (y \Rightarrow z) \in F$, if and only if $[z] \leq [x \Rightarrow y]$. Therefore H/E_F is a Heyting algebra where $[x] \Rightarrow [y] = [x \Rightarrow y]$. Hence, E_F is a congruence.

Then note that if E_F is a congruence, we have that $x \in F$ if and only if $x \Leftrightarrow 1 = x \in F$, and hence $[x] = [1]$ in H/E_F. Then, if $x \leq y$ and $x \in F$, $[y] = [x] \vee [y] = [1] \vee [y]$. Hence $[y] = [1]$ and $y \in F$. Then if $x, y \in F$, we have that $[x \wedge y] = [x] \wedge [y] = [1] \wedge [1] = [1]$, and therefore $x \wedge y \in F$. Hence, F is a filter. ☐

In Chapter 2, we observed that if we consider cases where we restrict our classical logic to have finite variables, we are able to construct an algorithm which determines whether or not a given term is a theorem. This algorithm relies on the fact the free Boolean algebra over any finite set is finite. In the case of intuitionistic logic, and the variety **Heyt**, we will see that similar results do not apply.

Theorem 5.1.18. [12]**.** *The free Heyting algebra over a singleton set $\{x\}$ is infinite, and is given by* *the lattice,*



denoted H_1. *Moreover, in* H_1, a_n, b_n c_n *and* d_n *are sequences defined by* $a_0 = 0$, $b_0 = x$, $c_n = b_n \Rightarrow a_n$, $d_n = c_n \Rightarrow b_n$, $a_{n+1} = b_n \vee c_n$ *and* $b_{n+1} = d_n \vee c_n$.

In order to prove this theorem, we consider a preliminary lemma.

Lemma 5.1.19. *The lattice* H_1*, as given above, is a Heyting algebra.*

Proof. It is clear to see that binary suprema and infima exist in the given lattice. Thus, it is sufficient to prove that $x \Rightarrow y$ can be defined for all $x, y \in H$. If $x \leq y$, then $x \Rightarrow y = 1$ and so we consider $x \Rightarrow y$ such that $x \not\leq y$. Note that if $x \Rightarrow y$ is defined it is equal to the supremum of the set $\{z \in H \mid z \wedge x \leq y\}$. Thus, to prove H is Heyting, it is sufficient to show that for each $x, y \in H$, with $x \not\leq y$ that the set $\{z \in H \mid z \wedge x \leq y\}$ is finite.

We first note that, for any $y \in H$, we have that there are only finitely many elements $z \in H$ such that $y \not\leq z$. Thus again, it is sufficient to show that the set $\{z \in H \mid z \wedge x \leq y \text{ and } y \leq z\}$ is finite. Then, note that if $y \leq x$ and $y \leq z$, then $y \leq z \wedge x$. Therefore $\{z \in H \mid z \wedge x \leq y \text{ and } y \leq z\} = \{y\}$ when $y \leq x$. Hence, we only need to consider the case where $x \not\leq y$ and $y \not\leq x$.

If $y = a_n$ for some $n \geq 1$, the only non-comparable element is $x = d_{n-1}$. Then we observe that the only choices of z such that $z \wedge d_{n-1} \leq a_n$ and $a_n \leq z$ are $z = c_n$ and $z = a_n$. If $y = b_n$ for $n \in \mathbb{N}$, then the only non-comparable value to y is $x = c_n$. Then we observe that if $z \wedge c_n \leq b_n$ and $b_n \leq z$ then $z = d_n$ or $z = b_n$. If $y = c_n$ then $x = b_n$, $x = d_n$ or $x = d_{n-1}$ where applicable. For each of these values of x we can observe that if $z \wedge x \leq c_n$ and $c_n \leq z$, we can only have $z = c_n$ (since any other choice of z which is greater than c_n gives us $d_{n-1} \leq z \wedge x$). Lastly, if $y = d_n$ then we consider $x = a_{n+1}$. $x = c_n$ and $x = c_{n+1}$. As in the previous case, we observe that for each of these values for x, the only value of z such that $z \wedge x \leq d_n$ and $d_n \leq z$ is $z = d_n$. Hence $\{z \in H \mid z \wedge x \leq y \text{ and } y \leq z\}$ is finite for each $x, y \in H$ with $x \nleq y$ and so $x \Rightarrow y$ is defined for all $x, y \in H$. □

We now prove that H_1 is, in fact, the free Heyting algebra over $\{x\}$.

Proof. Let H_1 be the lattice depicted above. It is clear that for each $k \geq 1$, we have $a_k = b_{k-1} \vee c_{k-1}$ and $b_k = d_{k-1} \vee c_{k-1}$. Then, for each $n \in \mathbb{N}$, we have that $b_n \Rightarrow a_n = \bigvee\{z \in H \mid z \wedge b_n \leq a_n\}$. Note that if $z \wedge b_n \leq a_n$ then $b_n \nleq z$, hence $z \leq c_n$. Moreover, $c_n \wedge b_n = a_n$. Hence, $\bigvee\{z \in H \mid z \wedge b_n \leq a_n\} = c_n$. Similarly, note that $d_n \wedge c_n = b_n$ and if $z \wedge c_n \leq b_n$, then $c_n \nleq z$, and thus $z \leq d_n$. Hence $d_n = \bigvee\{z \in H \mid z \wedge c_n \leq b_n\}$, and the sequences defined in the theorem correspond to the lattice H_1 depicted.

Let G be an arbitrary Heyting algebra. Then, let $\alpha : \{x\} \to G$ be a function and consider the diagram

$$\begin{array}{ccc} \{x\} & \xrightarrow{\eta} & H_1 \\ & \searrow^{\alpha} & \downarrow{\scriptstyle \phi} \\ & & G \end{array}$$

where η is the inclusion mapping and $\phi : H_1 \to G$ is a Heyting algebra homomorphism. Note that, in order for the diagram to commute, we only need to have that $\phi(x) = \alpha(x)$. In order to show that H is the free Heyting algebra, we then show that the image of any $y \in H_1$ under ϕ is determined by the value of $\alpha(x)$. Note that if ϕ is a homomorphism making the diagram commute, then $\phi(a_0) = \phi(0) = 0$, $\phi(b_0) = \phi(x) = \alpha(x)$, $\phi(c_0) = \phi(\neg x) = \neg\alpha(x)$, and $\phi(d_0) = \phi(\neg x \Rightarrow x) = \neg\alpha(x) \Rightarrow \alpha(x)$. Hence, the values of $\phi(a_0)$, $\phi(b_0)$, $\phi(c_0)$ and $\phi(d_0)$ are uniquely determined by the value of $\alpha(x)$. Then, if we assume that the values of $\phi(a_n)$, $\phi(b_n)$, $\phi(c_n)$ and $\phi(d_n)$ are fixed, then
$\phi(a_{n+1}) = \phi(b_n \vee c_n) = \phi(b_n) \vee \phi(c_n)$,
$\phi(b_{n+1}) = \phi(d_n \vee c_n) = \phi(d_n) \vee \phi(d_n)$,
$\phi(c_{n+1}) = \phi(b_{n+1} \Rightarrow a_{n+1}) = \phi(b_{n+1}) \Rightarrow \phi(a_{n+1})$,
and $\phi(d_{n+1}) = \phi(c_{n+1} \Rightarrow b_{n+1}) = \phi(c_{n+1}) \Rightarrow \phi(b_{n+1})$.
And so the values of $\phi(a_{n+1})$, $\phi(b_{n+1})$, $\phi(c_{n+1})$ and $\phi(d_{n+1})$ are determined by the values of $\phi(a_n)$, $\phi(b_n)$, $\phi(c_n)$ and $\phi(d_n)$. Therefore, by induction, the value of $\phi(y)$ is uniquely determined by the value of $\alpha(x)$ for any $y \in H$. Therefore, ϕ is the unique homomorphism such that the above diagram commutes, and so $H = F_{\mathbf{Heyt}}(\{x\})$. □

From this result and Lemma 3.9.6 we obtain the following corollary.

Corollary 5.1.20. ***Heyt*** *is not L-complete for any finite Heyting algebra L. In particular, there is no finite Heyting algebra L such that $f(t) = f(s)$ for all $f \in hom(F_{\textbf{Heyt}}(\{x\}), L)$ if and only if $s = t$.*

Note that the algorithms constructed to determine theorems of classical logic rely on the fact that finitely generated Boolean algebras are finite, and that **Bool** is $\{0, 1\}$-complete. Therefore, since **Heyt** does not satisfy similar properties, we cannot construct similar algorithms for intuitionistic logic which can be determined in finitely many steps.

5.2 Subvarieties of Heyting Algebras

In this section, we discuss subvarieties of **Heyt**. Each such subvariety corresponds to a propositional theory which satisfies each axiom and rule of inference of $\mathscr{T}_{IL}$ but are not necessarily equivalent to $\mathscr{T}_{CL}$. These are often called *intermediary*, or *superintuitionistic* logics. In particular, we consider the varieties of De Morgan Heyting algebras, and Gödel–Dummett algebras. But first, we consider **Bool** as a subvariety of **Heyt**.

Lemma 5.2.1. *In a Heyting algebra H the following identities are equivalent,*

a. $x \vee \neg x = 1$.

b. $\neg\neg x = x$.

c. $\neg x \vee y = x \Rightarrow y$.

where $x, y \in H$.

Proof. First we note that in any Heyting algebra we have that $x \leq \neg\neg x$ and $\neg x \vee y \leq x \Rightarrow y$ and so in order to show the equalities in b. and c. it is sufficient to show the other inequality holds.

a.⇒b.:
If $x \vee \neg x = 1$ then,
$(x \vee \neg x) \wedge \neg\neg x = 1 \wedge \neg\neg x = \neg\neg x$, and therefore
$(x \wedge \neg\neg x) \vee (\neg x \wedge \neg\neg x) = (x \wedge \neg\neg x) \vee 0 = x \wedge \neg\neg x = \neg\neg x$. Hence, $\neg\neg x \leq x$.

b.⇒a.:
$\neg(x \vee \neg x) = \neg x \wedge \neg\neg x = 0$. But then, by b., $x \vee \neg x = \neg\neg(x \vee \neg x) = \neg 0 = 1$.

a.⇒c.: Using the same method as in Corollary 4.3.13, we can prove that $z \wedge x \leq y$ if and only if $z \leq \neg x \vee y$ under the assumption that $\neg x \vee x = 1$.

c.⇒a.: If c. holds then $\neg x \vee x = x \Rightarrow x = 1$. □

Therefore, any Heyting algebra which satisfies any of these three identities is a Boolean algebra. Then, since any Boolean algebra satisfies these identities, we have that **Bool** is a subvariety of **Heyt** that can be obtained by adding one of these to the algebraic axioms Φ, which define the variety.

Corollary 5.2.2. *We can obtain a theory equivalent to $\mathscr{T}_{CL}$ by adding one of the following sets of axioms to $\mathscr{T}_{IL}$:*

A12. $p \vee \neg p$ for all $p \in Frm(\mathscr{L}_{CL})$.

A12′. $p \Rightarrow \neg\neg p$ for all $p \in Frm(\mathscr{L}_{CL})$.

A12″. $(p \Rightarrow q) \Rightarrow (\neg p \vee q)$ for all $p, q \in Frm(\mathscr{L}_{CL})$.

Definition 5.2.3. [16]**.** An element x of a Heyting algebra H is called **regular** if $\neg\neg x = x$. The regular elements of H are denoted $R(H)$.

Note 5.2.4. Each $x \in R(H)$ can be expressed as $\neg\neg x'$ for some $x' \in H$. Trivially, $x \in R(H)$ implies that $x = \neg\neg x$ for $x \in H$. Moreover $\neg\neg x' \in R(H)$ for all $x' \in H$. Therefore $R(H) = \{\neg\neg x' \mid x' \in H\}$.

Lemma 5.2.5. [16]**.** *$(R(H), \vee', 0, \wedge, 1, \Rightarrow)$ is a Boolean algebra where $\wedge$, $\Rightarrow$ 0 and 1 are the same as in H but $x \vee' y = \neg\neg(x \vee y)$.*

Proof. Since $\neg\neg 1 = 1$ and $\neg\neg 0 = 0$, we have that $0, 1 \in R(H)$. If $x, y \in R(H)$, then $\neg\neg(x \wedge y) = \neg\neg x \wedge \neg\neg y = x \wedge y$ and $\neg\neg(x \Rightarrow y) = \neg\neg x \Rightarrow \neg\neg y = x \Rightarrow y$ and so $x \wedge y, x \Rightarrow y \in R(H)$. Then note that $x \leq x \vee y \leq \neg\neg(x \vee y)$ and $y \leq \neg\neg(x \vee y)$. Moreover, if $z \in R(H)$ such that $x \leq z$, $y \leq z$ then $x \vee y \leq z$ and $\neg\neg(x \vee y) \leq \neg\neg z = z$. Therefore $x \vee' y$ is the supremum of $\{x, y\}$ in $R(H)$, and $R(H)$ is a Heyting algebra. Lastly, since $\neg\neg x = x$ for all $x \in R(H)$ by definition, we have that $R(H)$ is Boolean. □

Lemma 5.2.6. *For each $H \in$ **Heyt**, we have that $R(H)$ is the image of H under the left adjoint to the inclusion functor K : **Bool** $\to$ **Heyt**.*

Proof. Let B be a Boolean algebra, and for each $f : H \to B$ consider the diagram

$$\begin{array}{ccc} H & \xrightarrow{\neg\neg} & R(H) \\ & \searrow^{f} & \downarrow{\scriptstyle g} \\ & & B \end{array}$$

where $\neg\neg : H \to R(H)$ is defined by $\neg\neg(x) = \neg\neg x$. Note that this is a map onto $R(H)$ since for each $x \in H$, $\neg\neg\neg\neg x = \neg\neg x$ and so $\neg\neg x \in R(H)$. Moreover, $\neg\neg$ is a homomorphism since $\neg\neg : H \to H$

preserves $0, 1, \wedge$ and $\Rightarrow$, and $\neg\neg(x \vee y) = x \vee' y$. We then claim g can be defined by $g(\neg\neg x) = f(x)$ for each $x \in H$ (by Note 5.2.4 this defines g on all of $R(H)$). Clearly, g makes the diagram commute and is the unique map such that it commutes. In order to see that it is a well-defined morphism, we note that for all $x, y \in H$,

$$g(\neg\neg x \wedge \neg\neg y) = g(\neg\neg(x \wedge y)) = f(x \wedge y) = f(x) \wedge f(y) = g(\neg\neg x) \wedge g(\neg\neg y),$$

and similarly $g(\neg\neg x \Rightarrow \neg\neg y) = g(\neg\neg x) \Rightarrow g(\neg\neg y)$. Lastly,

$$g(\neg\neg x \vee' \neg\neg y) = g(\neg\neg(\neg\neg x \vee \neg\neg y)) = f(\neg\neg x \vee \neg\neg y) = \neg\neg f(x) \vee \neg\neg f(y) = f(x) \vee f(y) = g(\neg\neg x) \vee g(\neg\neg y),$$

where the assumption that B is Boolean provides the fourth equality. Hence, g is a well-defined morphism and thus is the unique morphism making the diagram commute. □

Lemma 5.2.7. ***Bool*** *is the smallest non-trivial subvariety of* ***Heyt***.

Proof. We have seen in previous chapters that **Bool** is $\{0, 1\}$-complete. Hence, by Lemma 3.9.2 each Boolean algebra B is a subalgebra of some product of $\{0, 1\}$. Then suppose $\mathbb{V}$ is a subvariety of **Heyt**, such that $0 = 1$ for all $A \in \mathbb{V}$. We then have that if $0 = 1$ then $x \vee 0 = x \vee 1 = 1 = 0$ and therefore $x \leq 0$, implying $x = 0 = 1$ for all $x \in A$. Therefore if $0 = 1$ in A, then A is the one-element algebra. Then, if $\mathbb{V}$ is a non-trivial subvariety, it must contain an algebra A such that $0 \neq 1$ in A. Then, $\{0, 1\}$ is a subalgebra of A, and so $\{0, 1\} \in \mathbb{V}$. However, then by Birkhoff's Theorem, $\mathbb{V}$ must contain each subalgebra of each product of $\{0, 1\}$. Hence, it must contain each Boolean algebra, and so **Bool** $\leq \mathbb{V}$. □

We now consider another subvariety of Heyting algebras induced by the identities in the following lemma.

Lemma 5.2.8. *If H is a Heyting algebra, then the following identities are equivalent,*

a. $\neg(x \wedge y) = \neg x \vee \neg y$.

b. $\neg x \vee \neg\neg x = 1$.

c. $\neg\neg(x \vee y) = \neg\neg x \vee \neg\neg y$.

for all $x, y \in H$.

Proof. a.⇒b.:
Note that since $x \wedge \neg x = 0$, if a. holds then $\neg x \vee \neg\neg x = \neg(x \wedge \neg x) = \neg 0 = 1$.

a.⇒c.:

$\neg\neg(x \vee y) = \neg(\neg x \wedge \neg y) = \neg\neg x \vee \neg\neg y$, with the first equality holding for all Heyting algebras and the second and application of a.

c.⇒a.:

$\neg(x \wedge y) = \neg\neg\neg(x \wedge y) = \neg(\neg\neg x \wedge \neg\neg y) = \neg\neg(\neg x \vee \neg y) = \neg\neg\neg x \vee \neg\neg\neg y = \neg x \vee \neg y$, where we apply c. in the fourth equality.

b.⇒c.:

$$\begin{aligned}
\neg\neg(x \vee y) &= \neg\neg(x \vee y) \wedge (\neg y \vee \neg\neg y) \\
&= (\neg\neg(x \vee y) \wedge \neg y) \vee (\neg\neg(x \vee y) \wedge \neg\neg y) \\
&= (\neg\neg(x \vee y) \wedge \neg\neg\neg y)) \vee (\neg\neg((x \vee y) \wedge y)) \\
&= \neg\neg((x \vee y) \wedge \neg y) \vee \neg\neg y \\
&= \neg\neg((x \wedge \neg y) \vee (y \wedge \neg y)) \vee \neg\neg y \\
&= \neg\neg(x \wedge \neg y) \vee \neg\neg y \\
&= (\neg\neg x \wedge \neg\neg\neg y) \vee \neg\neg y \\
&= (\neg\neg x \vee \neg\neg y) \wedge (\neg\neg\neg y \vee \neg\neg y) \\
&= (\neg\neg x \vee \neg\neg y) \wedge 1 = \neg\neg x \vee \neg\neg y.
\end{aligned}$$

□

Definition 5.2.9. A Heyting algebra D satisfying the above algebraic identities is called a **De Morgan Heyting Algebra**, or **DMH-algebra**. We denote the variety of De Morgan algebras by, **DMH-Alg** and the propositional theory corresponding to the variety of DMH-algebras by $\mathscr{T}_{DM}$.

The identity b. in the definition is called the **weak law of excluded middle**, and the condition c. along with Lemma 5.2.8 implies that **DMH-Alg** is the smallest subvariety of **Heyt** such that $\neg\neg : D \to D$ is an endomorphism for each $D \in$ **DMH-Alg**.

Example 5.2.10. Any totally ordered set $(C, \leq)$ is a De Morgan Heyting algebra with $\Rightarrow$ defined as in Example 5.1.4. Note that for all $x \in C$, $\neg x \vee \neg\neg x = (x \Rightarrow 0) \vee ((x \Rightarrow 0) \Rightarrow 0)$. Then if $x = 0$, we have that $(x \Rightarrow 0) \vee ((x \Rightarrow 0) \Rightarrow 0) = 1 \vee \neg 1 = 1$. If $x \neq 0$ then $(x \Rightarrow 0) \vee ((x \Rightarrow 0) \Rightarrow 0) = 0 \vee (0 \Rightarrow 0) = 0 \vee 1 = 1$, and so the weak law of excluded middle holds in every such lattice.

Example 5.2.11. The Heyting algebra of open sets in a topological space (X, τ) is a DMH-algebra if and only if for each $U \in \tau$, we have that $\neg U = \bigcup\{V \in \tau \mid V \cap U = \emptyset\}$ is clopen. This is due to the fact that if τ is a DMH-algebra, we must have $\neg U \cup \neg\neg U = X$, and so $\neg\neg U = X - (\neg U)$ and so the complement of $\neg U$ is open, making $\neg U$ closed. If each $\neg U$ is clopen, then $X - (\neg U)$ is an open set and hence is in τ, and so $\neg U \cup \neg\neg U = \neg U \cup (X - (\neg U)) = X$. A common example of such a space is the real numbers with the cofinite topology. That is, the space $(\mathbb{R}, \tau)$ where $\tau = \{U \subseteq \mathbb{R} \mid U = \emptyset \text{ or } \mathbb{R} - U \text{ is finite}\}$. If $U \in \tau$ then in the case where $U = \emptyset$, then $\neg U = \mathbb{R}$ which is trivially clopen. If $\mathbb{R} - U$ is finite then $\neg U = \emptyset$, which is trivially clopen.

Example 5.2.12. Clearly each Boolean algebra is a DMH-algebra since Boolean algebras satisfy De Morgan's laws.

The last subvariety of Heyting algebras we describe in this section is that which corresponds to the propositional theory below.

Definition 5.2.13. [10]**.** The theory of **Gödel–Dummett propositional logic**, denoted $\mathscr{T}_{GD}$, is given by adding to $\mathscr{T}_{IL}$ the axioms,

$$\text{GD. } (p \Rightarrow q) \vee (q \Rightarrow p) \text{ for all } p, q \in \mathrm{Frm}(\mathscr{T}_{GD}).$$

The resulting variety of algebras is defined as follows.

Definition 5.2.14. The category **GD-Alg** is the variety of algebras $\mathbb{V}(\mathscr{T}_{GD})$, whose objects are Heyting algebras, H such that for all $x, y \in H$,

$$(x \Rightarrow y) \vee (y \Rightarrow x) = 1.$$

such algebras are called **Gödel–Dummett (GD) algebras**, or **linear Heyting algebras**.

An equivalent axiomatization of $\mathscr{T}_{GD}$ is given by Dummett [10] and described algebraic terms in the lemma below.

Lemma 5.2.15. *If H is Heyting algebra, the following are equivalent,*

a. $(x \Rightarrow y) \vee (y \Rightarrow x) = 1$*.*

b. $x \Rightarrow (y \vee z) \leq (x \Rightarrow y) \vee (x \Rightarrow z)$*.*

for all $x, y, z \in H$.

Proof. If we assume a. holds then we have that $(y \Rightarrow z) \vee (z \Rightarrow y) = 1$. Then since $(y \vee z) \Rightarrow z =$

$(y \Rightarrow z) \wedge (z \Rightarrow z) = y \Rightarrow z$ for all $y, z \in H$, we have that $((y \vee z) \Rightarrow z) \vee ((y \vee z) \Rightarrow y) = 1$. Therefore,

$$\begin{aligned}(x \Rightarrow (y \vee z)) \wedge 1 &= (x \Rightarrow (y \vee z)) \wedge ((y \vee z) \Rightarrow y) \vee ((y \vee z) \Rightarrow z)\\ &= ((x \Rightarrow (y \vee z)) \wedge ((y \vee z) \Rightarrow y)) \vee ((x \Rightarrow (y \vee z)) \wedge ((y \vee z) \Rightarrow z))\\ &\leq (x \Rightarrow y) \vee (x \Rightarrow z)\end{aligned}$$

where the last inequality is an application of Lemma 5.1.15.c.

On the other hand, if b. holds, then,

$$\begin{aligned}1 &= (x \vee y) \Rightarrow (x \vee y)\\ &\leq ((x \vee y) \Rightarrow x) \vee ((x \vee y) \Rightarrow y)\\ &= ((x \Rightarrow y) \wedge (y \Rightarrow y)) \vee ((x \Rightarrow x) \wedge (y \Rightarrow x))\\ &= (x \Rightarrow y) \vee (y \Rightarrow x).\end{aligned}$$

□

This subvariety of Heyting algebras is of particular interest since it can be shown that we are able to construct an algorithm with finitely many steps that determines whether a formula is a theorem of $\mathscr{T}_{GD}$. However, to show this we need a preliminary result, given below.

Definition 5.2.16. Let L be a lattice, and F be a proper filter on L. Then F is a **prime filter** if $x \vee y \in F$ implies that $x \in F$ or $y \in F$ for all $x, y \in L$.

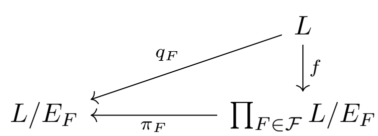
Note 5.2.17. In a Boolean algebra B, each prime filter is an ultrafilter, since for every filter F and every element $x \in B$, $x \vee \neg x \in F$, and so if F is prime either $x \in F$ or $\neg x \in F$.

Lemma 5.2.18. [16]. *If L is a distributive lattice, then for each $x, y \in L$ such that $x \not\leq y$ there is a prime filter F such that $x \in F$ and $y \notin F$.*

Proof. Consider the set $\mathcal{F}$ of filters such that $x \in F$ and $y \notin F$. Then, each chain of filters in $\mathcal{F}$ has an upper bound in $\mathcal{F}$ (the proof of this is similar to the proof in Lemma 2.3.18). Hence, by Zorn's Lemma, $\mathcal{F}$ contains a maximal element. We show that if $F' \in \mathcal{F}$ is not prime then it is not maximal. Assume, $x_1 \vee x_2 \in F'$ such that x_1 and x_2 are not in F'. Then, we consider the smallest filters containing $F' \cup \{x_1\}$ and $F' \cup \{x_2\}$, denoted F_1 and F_2 respectively. If $y \in F_1 \cap F_2$, by Corollary 2.3.8 we must have that $x_1 \wedge a_1 \leq y$ and $x_2 \wedge a_2 \leq y$ for some $a_1, a_2 \in F'$. Then, $(x_1 \vee x_2) \wedge a_1 \wedge a_2 \in F'$ and $(x_1 \vee x_2) \wedge a_1 \wedge a_2 = (x_1 \wedge a_1 \wedge a_2) \vee (x_2 \wedge a_1 \wedge a_2) \leq y$ implies that $y \in F'$, which contradicts our assumption. Hence, $y \notin F_1 \cap F_2$. If we assume $y \notin F_1$, we have that $F' \subseteq F_1$ by definition, $F_1 \in \mathcal{F}$ and $F' \neq F_1$ since $x_1 \notin F'$. Hence, F' is not maximal. Therefore, any maximal element of $\mathcal{F}$ is prime. □

Lemma 5.2.19. [11]**.** *Each GD algebra L is a subalgebra of a product of totally ordered lattices.*

Proof. Since $(x \Rightarrow y) \vee (y \Rightarrow x) = 1$ for all $x, y \in L$, then for each filter F of L we have that $(x \Rightarrow y) \vee (y \Rightarrow x) \in F$. Then if F is a prime filter, $x \Rightarrow y \in F$ or $y \Rightarrow x \in F$. Therefore in L/E_F, we have that $[x] \Rightarrow [y] = 1$ or $[y] \Rightarrow [x] = 1$ for all $x, y \in L$. Thus, L/E_F is a totally ordered lattice.
Let $\mathcal{F}$ be the set of all prime filters on L. We claim that $f : L \to \prod_{F \in \mathcal{F}} L/F$, defined by $x \mapsto ([x]_F)_{F \in \mathcal{F}}$ is injective. Clearly, it is a homomorphism, since it is the unique morphism such that the diagram



commutes for each $F \in \mathcal{F}$ where q_F is the quotient map for each $F \in \mathcal{F}$. Now note that if $x \neq y$ then either $x \not\leq y$ or $y \not\leq x$. If we assume the first case, then there is some prime filter $F \in \mathcal{F}$ such that $x \in F$ and $y \notin F$. But then $[x]_F \neq [1]_F = [y]_F$, and so $f(x) \neq f(y)$. Thus, f is injective and L is a subalgebra of $\prod_{F \in \mathcal{F}} L/F$. □

Corollary 5.2.20. ***GD-Alg*** *is a subvariety of* ***DMH-Alg****.* □

Proof. Any chain C is a DMH-algebra, and therefore, since every GD-algebra is a subalgebra of a product of chains, any GD-algebra is in **DMH-Alg**. □

Corollary 5.2.21. ***GD-Alg*** *is C^∞-complete for an infinite chain C^∞.*

Proof. Since each $L \in$ **GD-Alg** is a subalgebra of $\prod_{F \in \mathcal{F}} L/E_F$, we choose C^∞ to be a chain such that $|L/E_F| \leq |C^\infty|$ for all $L \in$ **GD-Alg** and every prime filter F of each GD-algebra L. Then each L/E_F is a subalgebra of C^∞ and so $\prod_{F \in \mathcal{F}} L/E_F$ is a subalgebra of $\prod_{F \in \mathcal{F}} C^\infty$ for every $L \in$ **GD-Alg**. □

Theorem 5.2.22. [11]**.** *Let F_{GD} :* ***Set*** *$\to$* ***GD-Alg*** *be the free functor, and let X be a countably infinite set and t be a term in $F_\Omega(X)$. Then the following are equivalent:*

1. *$F_{GD}(X) \vDash (t, 1)$.*

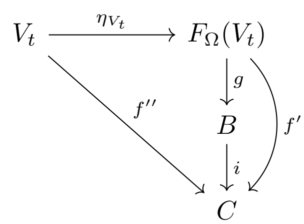
2. *$L \vDash (t, 1)$ for every GD-algebra L.*

3. *$C \vDash (t, 1)$ for every chain C.*

4. *$B \vDash (t, 1)$ for every chain B with at most $n + 2$ elements, where n is the number of variables in t.*

Proof. As we have seen in Corollary 3.6.7, $F_{GD}(X) \vDash (t, 1)$ if and only if 2. holds. Clearly, 2. implies 3. and 3. implies 4.

In order to show 4. implies 3. assume that 4. holds and $C \nvDash (t, 1)$ for some chain C. That is, there is some $f : F_\Omega(X) \to C$ such that $f(t) \neq 1$. Then, if $V_t = \{x_1, ..., x_n\} \subseteq X$ are the variables in t, we have that $B = \{0, 1, f(x_1), ..., f(x_n)\}$ is a subalgebra of C with $n + 2$ elements. Let $g : F_\Omega(V_t) \to B$ be a homomorphism such that $g(x_k) = f(x_k)$, for all $i \in \{1, ..., n\}$. Then consider the diagram



where η_{V_t} and i are inclusions, and f' and f'' are the restrictions of f to $F_\Omega(V_t)$ and V_t respectively. Then since $ig(x_k) = f'(x_k) = f(x_k)$ for each $k \in \{1, ..., n\}$ we have that $ig = f'$ by the universal property of $F_\Omega(V_t)$. Moreover, since $t \in F_\Omega(V_t)$ we have that $1 = g(t)$ by 4. Therefore $1 = ig(t) = f'(t) = f(t)$ which is a contradiction. Hence, if 4. holds then 3. holds.

Lastly, if 3. holds we have that $C \vDash (t, 1)$ for every chain C, and so $P \vDash (t, 1)$ for any product of chains, P. But by Lemma 5.2.19, each GD-algebra L is a subalgebra of a product of chains and so $L \vDash (t, 1)$ for each $L \in \textbf{GD-Alg}$. □

Corollary 5.2.23. *There exists an algorithm with finitely many steps to determine whether a formula t is a theorem of $\mathscr{T}_{GD}$.*

Proof. We have that t is a theorem if and only if $F_{GD}(X) \vDash (t, 1)$,. However, we have seen that this is equivalent to $B \vDash (t, 1)$ for every chain with at most $n + 2$ elements, where $n = |V_t|$, and $V_t \subseteq X$ is the set of variables in t. Then, it is sufficient to show that $f(t) = 1$ for every $f \in \hom(F_\Omega(V_t), B_{n+2})$, where B_{n+2} is an $(n + 2)$-element chain. Then, since each f is uniquely determined by some function $f' : V_t \to B_{n+2}$, there are only $(n + 2)^n$ such homomorphisms, and so $f(t)$ can be computed for every $f \in \hom(F_\Omega(V_t), B_{n+2})$ in finitely many steps. □

5.3 Varieties of Algebras for Modal Logic

In this section, we consider varieties of algebras which correspond to certain theories of propositional modal logic. In particular, we consider theories of *normal* modal logic, which correspond to theories which have all the theorems of **K**, the weakest theory of normal modal logic [3]. In particular, we will consider the corresponding varieties of the Modal systems known as **K, T, S4, B** and **S5**. We will discuss in the most detail the variety corresponding to **S4**, known as the variety of topological Boolean algebras.

Definition 5.3.1. [3]**.** The theory of propositional logic **K** also known as the theory of **basic normal modal logic**, is defined as follows:

1. The language includes the symbols and rules of $\mathscr{T}_{CL}$ but with an additional unary connective, denoted $\Box$. The formulae of **K** are all those in $\mathscr{T}_{CL}$ with the additional rule that if p is a formula then $\Box p$ is a formula. We will denote this language $\mathscr{L}_M$.

2. All of the axioms of $\mathscr{T}_{CL}$ are axioms of **K**. An additional set of axioms is given by,

$$K1.\ \Box(p \Rightarrow q) \Rightarrow (\Box p \Rightarrow \Box q) \text{ for all } p, q \in \mathrm{Frm}(\mathbf{K}).$$

3. MP is a rule of inference, and there is an additional rule of inference, called *generalization*, given by,

$$G = \{(p, \Box p) \mid p \in \mathrm{Frm}(\mathbf{K})\}.$$

Theorem 5.3.2. *The variety associated with* ***K*** *is given as follows.* $\mathbb{V}(\boldsymbol{K}) = \boldsymbol{Alg}(\Omega, \Phi)$*, where*

1. $\Omega = \{\wedge, 1, \vee, 0, \neg, \Box\}$*, where* $\Box$ *is a unary operation.*

2. Φ *consists of the algebraic axioms of a Boolean algebra (where* $\neg x$ *is defined as* $x \Rightarrow 0$*) and the identities* $(\Box 1, 1)$ *and* $(\Box(x \wedge y), \Box x \wedge \Box y)$*.*

That is, each object $A \in \mathbb{V}(\boldsymbol{K})$ *is a Boolean algebra with an additional unary operation* $\Box$ *such that* $\Box 1 = 1$ *and* $\Box(x \wedge y) = \Box x \wedge \Box y$ *for all* $x, y \in A$*.*

Proof. We already have that since A1.-A12. are axioms and MP is a rule of inference that each $(A, \wedge, 1, \vee, 0, \neg)$ is a Boolean algebra. We then only need to show that the algebraic axioms and the additional axioms and rules of inference in our propositional theory are equivalent.

First we note that in **K**, we trivially have $\vdash 1$ and so by G we have $\vdash \Box 1$. That is, in $\mathrm{Frm}(\mathbf{K})/\Psi$, we have that $[\Box 1] = [1]$, and so $A \vDash (\Box 1, 1)$ for all $A \in \mathbb{V}(\mathbf{K})$. Furthermore, we have that if $x \leq y$ in $A \in \mathbb{V}(\mathbf{K})$, then $x \Rightarrow y = 1$ and so $\Box(x \Rightarrow y) = \Box 1 = 1$. Hence, $1 = \Box(x \Rightarrow y) \leq \Box x \Rightarrow \Box y$ by K1., and therefore $\Box x \leq \Box y$.

Using the fact that $\Box$ is order-preserving, we see that $((x \wedge y) \Rightarrow x) = 1$ if and only if, $\Box((x \wedge y) \Rightarrow x) = 1$ and therefore, $\Box(x \wedge y) \Rightarrow \Box x = 1$. Similarly $\Box(x \wedge y) \Rightarrow \Box y = 1$. Hence, $\Box(x \wedge y) \leq \Box x \wedge \Box y$.

On the other hand, $x \wedge y \leq x \wedge y$ if and only if $x \leq y \Rightarrow (x \wedge y)$, by adjunction. But, since $\Box$ is order preserving, $\Box x \leq \Box(y \Rightarrow (x \wedge y)) \leq \Box y \Rightarrow \Box(x \wedge y)$. Then applying adjunction again we obtain $\Box x \wedge \Box y \leq \Box(x \wedge y)$. Thus, the axioms of **K** imply our algebraic axioms.

Conversely, if our algebraic axioms hold, in any $A \in \mathbb{V}(\mathbf{K})$, we have that if $x = 1$, then $\Box x = \Box 1 = 1$. This is equivalent to saying that if $\vdash p$, then $\vdash \Box p$ for any formula p, which shows that G holds in each $A \in \mathbb{V}(\mathbf{K})$. Then, note that $(x \Rightarrow y) \wedge x = y$, therefore

$$\Box(x \Rightarrow y) \wedge \Box y = \Box((x \Rightarrow y) \wedge x) = \Box y$$

and by adjunction we get $\Box(x \Rightarrow y) \leq \Box x \Rightarrow \Box y$. Therefore, $\mathbf{Alg}(\Omega, \Phi) = \mathbb{V}(\mathbf{K})$. $\Box$

Definition 5.3.3. We call each $A \in \mathbb{V}(\mathbf{K})$ a **modal algebra** or a **K-algebra**, and denote $\mathbb{V}(\mathbf{K})$ by **K-Alg**.

We introduce additional unary and binary connectives $\Diamond$ and $⥽$ to the formulae of **K** (and corresponding operations to **K-Alg** defined) by,

1. $\Diamond x = \neg \Box \neg x$.

2. $x ⥽ y = \Box(x \Rightarrow y)$.

We refer to the operations $\Box$,$\Diamond$ and $⥽$ as **necessity, possibility** and **strict implication**.

Note 5.3.4. Although $\vdash p$ implies that $\vdash \Box p$ in **K**, we do not have that $p \Rightarrow \Box p$ is a theorem of **K** for any formulae p. For example a K-algebra which provides a counterexample to this is given later in this section in Example 5.3.26. It follows from this fact that theories of normal modal logic do not, in general, satisfy the deduction theorem.

Lemma 5.3.5. *For all $A \in$ **K-Alg**,*

a. $\Box x = \neg \Diamond \neg x$,

b. $\Diamond : A \to A$ *is order preserving.*

c. $\Diamond(x \vee y) = \Diamond x \vee \Diamond y$.

d. $\Diamond(x \Rightarrow y) = \Box x \Rightarrow \Diamond y$.

e. $\Diamond 0 = 0$.

f. $\neg\Diamond x = \Box\neg x$ *and* $\neg\Box x = \Diamond\neg x$.

g. $\Box(x \Rightarrow y) \leq \Diamond x \Rightarrow \Diamond y$.

h. $\Box x \vee \Box y \leq \Box(x \vee y)$.

i. $\Diamond(x \wedge y) \leq \Diamond x \wedge \Diamond y$.

for all $x, y \in A$.

Proof. a. $\neg\Diamond\neg x = \neg\neg\Box\neg\neg x = \Box x$.

b. Since $\neg : A \to A$ is order-reversing and $\Box : A \to A$ is order-preserving the composition $\neg\Box\neg = \Diamond : A \to A$ is order-preserving.

c. $\Diamond(x \vee y) = \neg\Box\neg(x \vee y) = \neg\Box(\neg x \wedge \neg y) = \neg(\Box\neg x \wedge \Box\neg y) = \neg\Box\neg x \vee \neg\Box\neg y = \Diamond x \vee \Diamond y$.

d. $\Diamond(x \Rightarrow y) = \Diamond(\neg x \vee y) = \Diamond\neg x \vee \Diamond y = \neg\Box\neg\neg x \vee \Diamond y = \Box x \Rightarrow \Diamond y$.

e. $\Diamond 0 = \neg\Box\neg 0 = \neg\Box 1 = \neg 1 = 0$.

f. $\neg\Diamond x = \neg\neg\Box\neg x = \Box\neg x$. The other identity is similar.

g. $\Box(x \Rightarrow y) = \Box(\neg y \Rightarrow \neg x) \leq \Box\neg y \Rightarrow \Box\neg y = \neg\Box\neg x \Rightarrow \neg\Box\neg y = \Diamond x \Rightarrow \Diamond y$, where we use the contrapositive rule for Boolean algebras.

h. Since $\Box$ is order preserving, then $\Box x \leq \Box(x \vee y)$ and $\Box y \leq \Box(x \vee y)$. Hence, $\Box x \vee \Box y \leq \Box(x \vee y)$.

i. The proof is similar to h.

$\Box$

Note 5.3.6. We can equivalently describe the variety **K-Alg** by adding the operation $\Diamond$ and the axioms $(\Diamond 0, 0)$ and $(\Diamond(x \vee y), \Diamond x \vee \Diamond y)$ to the algebraic theory of Boolean algebras. Then, defining $\Box x = \neg\Diamond\neg x$, we can see that the axioms in Definition 5.3.3 hold, using a similar proof to those which prove c. and e. in the previous lemma.

Lemma 5.3.7. *For all* $A \in$ ***K-Alg****,*

a. $\Box y \leq x \dashv y$.

b. $\Box\neg x \leq x \dashv y$.

c. $(x \dashv y) \wedge (\neg x \dashv y) = \Box y$.

for all $x, y \in A$.

Proof. a. and b. follow from the fact that $\Box$ is order preserving and $y \leq x \Rightarrow y$ and $\neg x \leq x \Rightarrow y$ in any Boolean algebra. Then

$$\begin{aligned}(x \multimap y) \wedge (\neg x \multimap y) &= \Box(x \Rightarrow y) \wedge \Box(\neg x \Rightarrow y) \\ &= \Box((\neg x \vee y) \wedge (x \vee y)) \\ &= \Box((\neg x \wedge x) \vee (y \wedge x) \vee (\neg x \wedge y) \vee (y \wedge y)) \\ &= \Box(((\neg x \vee x) \wedge y) \vee y) = \Box y.\end{aligned}$$

$\Box$

Some authors, such as Hughes and Cresswell [8] consider a stronger set of logical axioms as a basis for modal logic.

Definition 5.3.8. The theory **T** (also referred to as **M**) is obtained by adding the axioms

$$T1.\ \Box p \Rightarrow p \text{ for all } p \in \mathrm{Frm}(\mathbf{T})$$

to **K**. The variety induced by **T** is denoted **T-Alg**. The objects of **T-Alg** are K-algebras who satisfy the identity $\Box x \Rightarrow x = 1$, for every element x. These are called **T-algebras**.

Lemma 5.3.9. *For* $p, q \in Frm(\mathscr{L}_M)$, *we have that* $\vdash_{\boldsymbol{T}} p \Rightarrow q$ *if and only if* $\vdash_{\boldsymbol{T}} p \multimap q$.

Proof. If $\vdash_{\mathbf{T}} p \Rightarrow q$ then by G we have $\vdash_{\mathbf{T}} p \multimap q$. If $\vdash_{\mathbf{T}} p \multimap q$, then by T1. $\vdash_{\mathbf{T}} \Box(p \Rightarrow q) \Rightarrow (p \Rightarrow q)$ and by MP $\vdash_{\mathbf{T}} p \Rightarrow q$. $\Box$

Corollary 5.3.10. *If* $\mathscr{T}$ *is a theory with the language* $\mathscr{L}_M$ *which satisfies the axioms of* ***T****, we have that the variety generated by the relations* $\Psi_{\Rightarrow}, \Psi_{\multimap} \subseteq Frm(\mathscr{L}_M) \times Frm(\mathscr{L}_M)$, *where* $\Psi_{\Rightarrow} = \{(p,q) \mid \vdash_{\mathscr{T}} p \Rightarrow q \text{ and } \vdash_{\mathscr{T}} q \Rightarrow p\}$, *and* $\Psi_{\multimap} = \{(p,q) \mid \vdash_{\mathscr{T}} p \multimap q \text{ and } \vdash_{\mathscr{T}} q \multimap p\}$, *are equivalent. However, in this section, we only refer to the relation* $\Psi_{\Rightarrow}$.

Lemma 5.3.11. *In a K-algebra* A *we have that* $\Box x \leq x$ *for each* $x \in A$ *if and only if* $y \leq \Diamond y$ *for each* $y \in A$.

Proof. If $\Box \neg x \leq \neg x$, then $x \vee \Diamond x = \neg\neg x \vee \neg \Box \neg x = \neg(\neg x \wedge \Box \neg x) = \neg\neg x = x$. Similarly, if $\neg x \leq \Diamond \neg x$ we have that $x \vee \Box x = \neg\neg x \vee \neg \Diamond \neg x = \neg(\neg x \wedge \Diamond \neg x) = \neg\neg x = x$. $\Box$

This shows us that as in the case of **K-Alg**, we are able to use equivalent axioms of $\Diamond$ in order to induce the category **T-Alg**. Note directly from T1. we also obtain that for $A \in$ **K-Alg**,

a. $\Box\Box x \leq \Box x$.

b. $\Box\Diamond x \leq \Diamond x$

for all $x, y \in A$.

Definition 5.3.12. [8]**.** The theories **S4** and **S5** are formed by adding the axioms

$$S4.\ \Box p \Rightarrow \Box\Box p \text{ for all } p \in \mathscr{L}_M.$$

or,

$$S5.\ \Diamond p \Rightarrow \Box\Diamond p \text{ for all } p \in \mathscr{L}_M$$

to **T**, respectively.

Clearly, since $\vdash_{\mathbf{T}} \Box\Box p \Rightarrow p$ and $\vdash_{\mathbf{T}} \Diamond p \Rightarrow \Box\Diamond p$ for all $p \in \mathrm{Frm}(\mathscr{L}_M)$, the varieties induced by theories **S4** and **S5** can be formed by adding the pairs $(\Box x, \Box\Box x)$ or $(\Diamond x, \Box\Diamond x)$ respectively to the algebraic axioms of **T-Alg**.

Definition 5.3.13. [16]**.** A **topological Boolean algebra** is an algebra $B = (B, \wedge, 1, \vee, 0, \neg, \Box)$, such that $(B, \wedge, 1, \vee, 0, \neg)$ is a Boolean algebra and $\Box : B \to B$ is a topological interior operator on B. That is, it is a unary operation such that

1. $\Box 1 = 1$.

2. $\Box x \leq x$.

3. $\Box\Box x = \Box x$.

4. $\Box(x \wedge y) = \Box x \wedge \Box y$.

for all $x, y \in B$. We denote the variety of Topological Boolean Algebras by **TopBool**.

It is clear that **TopBool** is formed by adding the axiom $(\Box x, \Box\Box x)$ to **T-Alg** and therefore it is the subvariety of **T-Alg** corresponding to **S4**. Topological Boolean algebras are also referred to as interior algebras (see [5]) or closure algebras (see [14]).

Lemma 5.3.14. *$A \in$ **T-Alg** satisfies $\Box\Box x = \Box x$ for every $x \in A$ if and only if $\Diamond\Diamond x = \Diamond x$ for each $x \in A$.*

Proof. Note that if $\Box\Box y = \Box y$ for every $y \in A$, then $\Box\Box\neg x = \Box\neg x$ for all $x \in A$ and so $\Diamond\Diamond x = \neg\Box\neg\neg\Box\neg x = \neg\Box\Box\neg x = \neg\Box\neg x = \Diamond x$. The proof of the converse is similar. $\Box$

Note 5.3.15. The previous lemma shows us that again, **TopBool** can be axiomatized by $\Diamond$, which forms a topological closure operator on each Boolean algebra B. That is, we can replace the axioms i.-iv. in our definition with equivalent axioms,

1′. $\Diamond 0 = 0$.

2′. $x \leq \Diamond x$.

3′. $\Diamond\Diamond x = \Diamond x$.

4′. $\Diamond(x \vee y) = \Diamond x \vee \Diamond y$.

for all $x, y \in B$.

A third axiomatization of **TopBool** is given as follows.

Lemma 5.3.16. [8]**.** *Let B be a Boolean algebra. Then B is a topological Boolean algebra if and only if there is a unary operation $\Box : B \to B$ such that 1. and 2. as in Definition 5.3.8 hold, and for all $x, y \in B$,*

$$\Box(x \Rightarrow y) \leq \Box(\Box x \Rightarrow \Box y).$$

Proof. In order to see that a Boolean algebra B satisfying this property is a topological Boolean algebra, first note that $\Box(x \Rightarrow y) \leq \Box(\Box x \Rightarrow \Box y) \leq \Box x \Rightarrow \Box y$ by 2. Then by Lemma 5.3.2 and 1., we obtain that $\Box(x \wedge y) = \Box x \wedge \Box y$. Then, we only need to show that $\Box x \leq \Box\Box x$. Observe that since $x \leq ((x \Rightarrow x) \Rightarrow x)$ we have that,

$$\Box x \leq \Box((x \Rightarrow x) \Rightarrow x) \leq \Box(\Box(x \Rightarrow x) \Rightarrow \Box x) \leq \Box\Box(x \Rightarrow x) \Rightarrow \Box\Box x,$$

and, applying A2. from $\mathscr{T}_{CL}$, we obtain $\Box x \Rightarrow \Box\Box(x \Rightarrow x) \leq \Box x \Rightarrow \Box\Box x$. But since $x \Rightarrow x = 1$ we have that $\Box x \Rightarrow \Box\Box(x \Rightarrow x) = \Box x \Rightarrow 1 = 1$. Hence $\Box x \Rightarrow \Box\Box x = 1$, which implies that $\Box\Box x = \Box x$.

To prove the converse we note that if B is a topological Boolean algebra, we have that $\Box(x \Rightarrow y) \leq \Box x \Rightarrow \Box y$, and therefore $\Box(x \Rightarrow y) = \Box\Box(x \Rightarrow y) \leq \Box(\Box x \Rightarrow \Box y)$. ☐

Lemma 5.3.17. *If $A \in$ **TopBool**, then $\Box x = \bigvee\{y \in A \mid y \leq x$ and $y = \Box y\}$ and $\Diamond x = \bigwedge\{y \in A \mid x \leq y$ and $y = \Diamond y\}$.*

Proof. Note that if $y = \Box y$, and $y \leq x$ then $y = \Box y \leq \Box x$. Moreover, $\Box x \leq x$ and $\Box\Box x = \Box x$. Hence, $\Box x$ is the greatest element of the set $\{y \in A \mid y \leq x$ and $y = \Box y\}$. We note that $\Diamond x = \bigwedge\{y \in A \mid x \leq y$ and $y = \Diamond y\}$ can be proved using a similar method. ☐

We see a similar definition for the algebraic variety corresponding to **S5** given below.

Definition 5.3.18. An S5-Algebra B is a T-algebra such that,

$$\Diamond x = \Box\Diamond x$$

for all $x \in B$. The variety of S5-algebras is denoted **S5-Alg**.

Lemma 5.3.19. *A T-algebra B is an S5-algebra if and only if $\Box x = \Diamond\Box x$ for all $x \in A$.*

Proof. If B is an S5-algebra then,

$$\begin{aligned}\Box x &= \neg\Diamond\neg x\\ &= \neg\Box\Diamond\neg x\\ &= \neg\Box\neg\neg\Diamond\neg x\\ &= \Diamond\Box x.\end{aligned}$$

The proof of the converse is similar. ☐

Lemma 5.3.20. ***S5-Alg*** *is a subvariety of* ***TopBool****.*

Proof. Let B be an S5-algebra. Then for any $x \in B$,

$$\Box\Box x = \Diamond\Box\Diamond\Box x = \Diamond\Diamond\Box x = \Diamond\Box x = \Box x$$

and so B is a topological Boolean algebra. ☐

Lemma 5.3.21. *If B is an S5 algebra, then for any $x \in B$,*

$$\#\#\#\#\#...\#\Box x = \Box x \text{ and } \#\#\#\#\#...\#\Diamond x = \Diamond x$$

where each $\#$ is either the operator $\Box$ or $\Diamond$.

Proof. We will prove the first equality inductively on the number of operations. Note that $\#\Box x = \Box x$ if $\# = \Box$ or $\# = \Diamond$. Then, assume there are n operators such that $\#'\#...\#\Box x = x$, where $\#'$ is the nth operator applied. If $\#' = \Diamond$ then $\Box\Diamond\#...\#\Box x = \Diamond\#...\#\Box x = \#'\#...\#\Box x = \Box x$, and $\Diamond\Diamond\#...\#\Box x = \Diamond\#...\#\Box x = \#'\#...\#\Box x = \Box x$. If $\#' = \Box$, then $\Box\Box\#...\#\Box x = \Box\#...\#\Box x = \#'\#...\#\Box x = \Box x$, and $\Diamond\Box\#...\#\Box x = \Box\#...\#\Box x = \#'\#...\#\Box x = \Box x$. Hence, if $\#...\#\Box x = x$ for n operators, then $\#...\#\Box x = x$ for $n+1$ operators. By induction $\#...\#\Box x = \Box x$ for any finite number of operators $\Diamond$ or $\Box$ applied to $\Box x$. The second equality is proved similarly. ☐

Lemma 5.3.22. *If B is a topological Boolean algebra such that,*

$$B.\ x \Rightarrow \Box\Diamond x = 1 \text{ for all } x \in B$$

then B is a S5-algebra.

Proof. If B. holds for all $x \in B$, then $x \leq \Box\Diamond x$ and therefore $\Box x \leq \Box\Box\Diamond x = \Box\Diamond x$ and so B is an S5-algebra. $\Box$

Moreover, the axiom B. above, when added to **T-Alg** induces a subvariety, which we denote **B-Alg** which corresponds to the following propositional theory of modal logic.

Definition 5.3.23. [8]**.** The propositional theory **B** is obtained by adding to **T** the additional axioms

$$B.\ p \Rightarrow \Box\Diamond p \text{ for all } p \in \mathrm{Frm}(\mathscr{L}_M).$$

Corollary 5.3.24. *In the lattice of subvarieties of **K-Alg**, we have that **S5-Alg** = **TopBool**∧**B-Alg**.* $\Box$

We now introduce various examples of objects in our varieties for modal algebra where our underlying Boolean algebra structure is a power set algebra.

Example 5.3.25. Let (X, τ) be a topological space. Then we claim that $(P(X)\cap, X, \cup, \emptyset, -, I)$ is a Topological Boolean algebra, where the necessity operator I maps each subset $A \subseteq X$ to its interior. That is, $I(A) = \bigcup\{U \in \tau \mid U \subseteq A\}$, or $I(A)$ is the largest open set contained in A. We can see that $I(X) = X$, since X is open. Observe that $I(A) \subseteq A$ by definition of interior and $II(A) = I(A)$ since $I(A) \in \tau$ by definition. Then note that if $A \subseteq B$, then clearly the largest open set contained in A is an open set contained in B and so $I(A) \subseteq I(B)$. Thus $I(A \cap B) \subseteq I(A)$ and $I(A \cap B) \subseteq I(B)$. Lastly, since the finite intersection of open sets is open $I(A) \cap I(B) \subseteq A \cap B$ yields $I(A) \cap I(B) \subseteq I(A \cap B)$. Therefore, $(P(X), \cap, X, \cup, \emptyset, -, I)$ is a topological Boolean algebra.

Note here that the derived operations have a similar topological equivalent. The possibility operator $-I(-A) = C(A)$ is the complement of the largest open set containing no elements of A. That is, it is the smallest closed set containing A. Secondly, strict implication is given, for any $A, B \in \tau$, by $I(-A \cup B) = \bigcup\{U \in \tau \mid U \subseteq -A \cup B\}$. However, $U \subseteq -A \cup B$ if and only if $U \cap A \subseteq B$. When A and B are open sets, this corresponds to Heyting implication on τ as in Example 5.1.3.

Note that numerous topological spaces provide an example of a topological Boolean algebra which is not an S5-algebra. For example, in $\mathbb{R}$ with the usual topology, for any singleton set $C(\{a\}) = \{a\}$ and $IC(\{a\}) = \emptyset$.

Example 5.3.26. An example of a K-algebra which does not belong to any other variety described in this chapter is the Boolean powerset algebra $P(\mathbb{N})$ on the natural numbers, with the operator $S(A) = A \cup \{n-1 \mid n \in A - \{0\}\}$. Then note that $S(\mathbb{N}) = \mathbb{N}$, and

$$\begin{aligned} S(A \cap B) &= (A \cap B) \cup \{n-1 \mid n \in (A \cap B) - \{0\}\} \\ &= (A \cap B) \cup (\{n-1 \mid n \in A - \{0\}\} \cap \{n-1 \mid n \in B - \{0\}\} \\ &= (A \cup \{n-1 \mid n \in A - \{0\}\}) \cap (B \cup \{n-1 \mid n \in B - \{0\}\}) = S(A) \cap S(B). \end{aligned}$$

Therefore, S satisfies the axioms for $\Box$ in **K-Alg**. However, clearly, $S(A) \nsubseteq A$ and so this algebra is not in **T-Alg**.

Example 5.3.27. An example of a T-algebra which is not a topological Boolean algebra or a B-algebra is given by $P(\mathbb{N})$ with the same operator S, but where we consider S to be the possibility, or $\Diamond$, operator. We have that $S(\emptyset) = \emptyset$, and $A \subseteq S(A)$ for each $A \subseteq \mathbb{N}$, and lastly since $\{n-1 \mid n \in (A \cap B) - \{0\}\} = \{n-1 \mid n \in A - \{0\}\} \cup \{n-1 \mid n \in B - \{0\}\}$ we have that $S(A \cup B) = S(A) \cup S(B)$ by using a similar method to the proof that S preserves intersections. Therefore $P(\mathbb{N})$ with the operator S considered as $\Diamond$ is a T-algebra.

Example 5.3.28. A topological space (X, τ) which induces a closure and interior operator which correspond to an S5-Algebra is any set with the trivial topology $\tau = \{X, \emptyset\}$ or the topology $\tau = P(X)$. In the first case $IC(A)$ is X if A is non-empty and $\emptyset$ if $A = \emptyset$. Hence, $A \subseteq IC(A)$ for all $A \in P(X)$. In the second case, since every set is clopen, trivially $A = IC(A)$ for all $A \in P(X)$.

This also shows us that the topology τ on a set X such that every subset of X is open induces a S5-Algebra such that $\Box A = A$ for all $A \subseteq X$. This result can be generalized as follows.

Lemma 5.3.29. ***Bool*** *is the smallest non-trivial variety of* ***K-Alg****.*

Proof. Every Boolean algebra B can be viewed as a **K-Alg** where $\Box$ is trivial (that is $\Box x = x$ for all $x \in B$). Hence, **Bool** is the subvariety of **K-Alg** obtained by adding $(\Box x, x)$ to its algebraic axioms. The proof that **Bool** is the *least* non-trivial subvariety is similar to the proof of Lemma 5.2.7. $\Box$

5.4 Relating Topological Boolean Algebras and Heyting Algebras

In this section, we define an adjunction between **TopBool** and **Heyt**, and using the adjunction conclude that the free algebra over one element in **TopBool** is infinite, and hence, **TopBool** is not complete with respect to its L-valued models for any finite $L \in$ **TopBool**.

Definition 5.4.1. Let B be a topological Boolean algebra. Then we define $O(B) = \{x \in B \mid \Box x = x\}$ to be the set of **open elements of** B.

Lemma 5.4.2. [14]**.** *For each $B \in$ **TopBool**, $(O(B), \wedge, 1, \vee, 0, \dashv)$ is a Heyting algebra. For every morphism $f : B \to C$ in **TopBool**, the map $O(f) : O(B) \to O(C)$ is a Heyting algebra homomorphism, where $O(f)$ is the restriction of f to $O(B)$.*

Proof. Note that if x, y are open then $x \vee y = \Box x \vee \Box y = \Box(\Box x \vee \Box y)$, since $\Box\Box x \vee \Box\Box y \leq \Box(\Box x \vee \Box y) \leq \Box x \vee \Box y$. Furthermore, $x \wedge y = \Box x \wedge \Box y = \Box(x \wedge y)$ and $x \dashv y = \Box(x \dashv y)$. Then since $\Box x \in O(B)$ for all $x \in B$, and $0, 1 \in O(B)$, we have that our operations are well-defined on $O(B)$. In order to show that $\dashv$ satisfies Heyting implication, note that for $x, y, z \in O(B)$, we have $x \leq y \dashv z$ implies,

$$x \wedge y \leq (y \dashv z) \wedge y = \Box(\neg y \vee z) \wedge \Box y = \Box((\neg y \vee z) \wedge y) = \Box(y \wedge z) \leq \Box z = z$$

and $x \wedge y \leq z$ implies $x = \Box x \leq \Box(y \Rightarrow z) = y \dashv z$. Therefore $O(B)$ is a Heyting algebra.

If $f : B \to C$ is a morphism in **TopBool**, then if $x \in O(B)$ we have that $f(x) = f(\Box x) = \Box f(x)$ and so $f(x) \in O(C)$. Then since f preserves the operations on B, it clearly preserves the Heyting operations on $O(B)$ and therefore $O(f) : O(B) \to O(C)$ is a Heyting algebra homomorphism. $\Box$

Corollary 5.4.3. [5]**.** *O : **TopBool** $\to$ **Heyt** is a functor which preserves injective and surjective homomorphisms.*

Proof. It is clear to see that $O(1_B) : O(B) \to O(B)$ is the identity, $1_{O(B)}$, and that for any composable morphisms g, f in **TopBool** we have $O(g)O(f)(x) = gf(x) = O(gf)(x)$ for each element x in the domain of $O(f)$.

If $f : B \to C$ is injective then in particular for $x, y \in O(B)$, we have that $f(x) = f(y)$ implies $x = y$ and so $O(f)$ is injective. If f is surjective, then for each $c \in O(C)$, there exists $x \in B$ such that $f(x) = c$. Then note that $f(\Box x) = \Box f(x) = \Box c = c$, and so there exists $\Box x \in O(B)$ such that $O(f)(\Box x) = c$. Therefore, O preserves injective and surjective morphisms. $\Box$

In order to construct the left adjoint to O, we first need two preliminary results.

Lemma 5.4.4. [16]**.** *Every distributive lattice is a subalgebra of a Boolean algebra.*

Proof. Let L be a distributive lattice. We claim that L is (up to isomorphism) a subalgebra of $P(\mathcal{F}(L))$, where $\mathcal{F}(L)$ is the set of prime filters on L. We define the map

$$h : L \to P(\mathcal{F}(L))$$

by $x \mapsto \{F \mid x \in F\}$.

Moreover, if $F \in h(x \vee y)$ then $x \vee y \in F$. Then since F is prime, we have that either $x \in F$ or $y \in F$. On the other hand, if either x or y is an element of F, then $x \vee y \in F$, and so $h(x) \cup h(y) = h(x \vee y)$. Conversely, if $F \in h(x \wedge y)$ then $x \in F$ and $y \in F$, and if $F \in h(x) \cap h(y)$ then $x, y \in F$ and so $x \wedge y \in F$. Hence, $h(x \wedge y) = h(x) \wedge h(y)$. Clearly $h(1) = P(\mathcal{F}(L))$ since 1 is an element of every filter. Similarly, since $\mathcal{F}(L)$ only contains proper filters, $h(0) = \emptyset$. Lastly, if $x \neq y$, by Lemma 5.2.18, there exists some $F \in \mathcal{F}(L)$ which does not contain both x and y. That is, $h(x) \neq h(y)$, and so h is injective. □

Lemma 5.4.5. [4]**.** *Let B be a Boolean algebra and L be a sublattice of B. Then there exists a topological interior operator $\Box : B \to B$ such that $L = O(B)$ if and only if $\bigvee(I_x \cap L)$ exists for each $x \in B$, where $I_x = \{b \in B \mid b \leq x\}$. In this case, $\Box x = \bigvee(I_x \cap L)$ for each $x \in B$.*

Proof. Assume that there is a topological interior operator $\Box : B \to B$ such that $L = O(B)$. Then, for each $x \in B$, we have that $\Box x = \bigvee\{y \in B \mid y \leq x \text{ and } \Box y = y\}$ by Lemma 5.3.17. Then note that $y \leq x$ if and only if $x \in I_x$, and $\Box y = y$ if and only if $y \in L$. Hence, $\{y \in B \mid y \leq x \text{ and } \Box y = y\} = I_x \cap L$, and so if $\Box : B \to B$ is defined as in our assumption, we must have $x = \bigvee(I_x \cap L)$ for each $x \in B$. Thus, $\bigvee(I_x \cap L)$ exists for each $x \in B$. Conversely, assume that $\Box x = \bigvee(I_x \cup L)$ for each $x \in B$. If $y \in O(B)$ then $y = \Box y = \bigvee(I_y \cap L)$, and since $y = \bigvee I_y$, then $y \in L$. If $y \in L$ we have that $y \in I_y \cap L$ and by definition $y = \bigvee I_y$. Hence, $\Box y = \bigvee(I_y \cap L) = y$, therefore $O(B) = L$. □

Theorem 5.4.6. [14]**.** *If H is a Heyting algebra, there exists some topological Boolean algebra B such that $O(B) = H$.*

Proof. Since H is a distributive lattice, we consider the Boolean algebra A such that H is a sublattice of A. We then consider the subset, $B \subseteq A$ which consists of all elements of the form,

$$\bigwedge_{i=1}^{n}(x_i \vee \neg y_i) \text{ such that } x_i, y_i \in H \text{ for each } i \in \{1, ..., n\}$$

and claim that this is a Boolean algebra with an interior operator which satisfies the desired property. For the rest of the proof we use $\to$ to denote the Heyting implication operation on H and $\neg$ to denote the Boolean complement of an element in A.

It is clear that B is closed under $\wedge$. Then note that,

$$\bigwedge_{i=1}^{n}(x_i \vee \neg y_i) \vee \bigwedge_{j=1}^{m}(z_j \vee \neg u_j) = \bigwedge_{j=1}^{j=m}\bigwedge_{i=1}^{i=n}((x_i \vee z_j) \vee \neg(y_i \wedge u_j))$$

and therefore, since $\wedge$ is associative, if $x_i, y_i, z_j, u_j \in H$, we have that $x_i \vee z_j, y_i \wedge u_j \in H$ and hence B is closed under $\vee$. Lastly,

$$\bigwedge_{i=1}^{n}(x_i \vee \neg y_i) \vee \bigwedge_{i=1}^{n}(\neg x_i \vee y_i) = \bigwedge_{i=1}^{n}(\neg x_i \vee x_i \vee y_i \vee \neg y_i) = \bigwedge_{i=1}^{n} 1 = 1$$

and therefore the complement of each $a \in B$ is also in B and so B is a Boolean subalgebra of A. Then, for each $a \in B$, we consider the set $\{z \in B \mid z \leq a \text{ and } z \in H\}$. Note that $z \leq a = \bigwedge_{i=1}^{n}(x_i \vee \neg y_i)$ if and only if $z \leq x \vee \neg y_i$ for all $i \in \{1, .., n\}$. Equivalently, for each $i \in \{1, .., n\}$, we have $z \wedge y_i \leq x_i$, which is true if and only if $z \leq y_i \dashv x_i$, since $z, x_i, y_i \in H$. That is, $z \in H \cap I_a$ if and only if $z \leq \bigwedge_{i=1}^{n}(y_i \dashv x_i)$. Then, since $(y_i \dashv x_i) \wedge y_i \leq x_i$, for each $i \in \{1, ..., n\}$ we have that $\bigwedge_{i=1}^{n}(y_i \dashv x_i) \in I_a$, and so $\bigwedge_{i=1}^{n}(y_i \dashv x_i) = \bigvee(I_a \cap H)$ for each $a \in B$. Hence, if we define $\Box a = \bigwedge_{i=1}^{n}(y_i \dashv x_i)$ for each $\bigwedge_{i=1}^{n}(x_i \vee \neg y_i) = a \in B$, by Lemma 5.4.5 we have a unique operator making B a topological Boolean algebra such that $O(B) = H$, treating $O(B)$ and H as sets. Moreover, by definition the Heyting implication induced on $O(B)$ is $\Box(\neg x \vee y)$ which is equal to $x \dashv y$ by definition. Therefore, considering $O(B)$ and H as Heyting algebras, we again obtain $O(B) = H$. $\Box$

For the rest of the chapter, for any $H \in$ **Heyt**, we use $T(H)$ to refer to the topological Boolean algebra B such that $O(B) = H$ as in the proof above.

Lemma 5.4.7. *If $f : H \to H'$ is a morphism in **Heyt**, then there is a unique topological Boolean algebra morphism extension of f, denoted $T(f) : T(H) \to T(H')$ such that $OT(f) = f$. Hence, T : **Heyt** $\to$ **TopBool** is a functor.*

Proof. Note that $T(f) : T(H) \to T(H')$ is a morphism in **TopBool** such that $OT(f) = f$ if and only if $T(f)(x) = f(x)$ for all $x \in H$. Assume $T(f)$ is defined thusly. Then for each $a \in T(H)$,

$$T(f)(a) = T(f)(\bigwedge_{i=1}^{n}(x_i \vee \neg y_i)) = \bigwedge_{i=1}^{n}(T(f)(x_i) \vee \neg T(f)(y_i)) = \bigwedge_{i=1}^{n}(f(x_i) \vee \neg f(y_i))$$

then clearly any map $h : T(H) \to T(H')$ such that $h(x) = f(x)$ for all $x \in H$ is defined similarly and so $T(f)$ is unique. Clearly $T(1_H) = 1_{T(H)}$ and for composable morphisms $f : H \to H'$ and $g : H' \to H''$ we have,

$$T(g)T(f)(a) = T(g)(\bigwedge_{i=1}^{n}(f(x_i) \vee \neg f(y_i))) = \bigwedge_{i=1}^{n}(gf(x_i) \vee \neg gf(y_i)) = T(gf)(a)$$

for all $a \in H$. Therefore, T : **Heyt** $\to$ **TopBool** is a functor. $\Box$

Theorem 5.4.8. [5]**.** *T : **Heyt** $\to$ **TopBool** is the left adjoint of O : **TopBool** $\to$ **Heyt**.*

Proof. By definition $OT(H) = H$. Therefore, for each $H \in$ **Heyt**, we claim the identity $1_H : H \to H = OT(H)$ is a map such that for any $B \in$ **TopBool** and any Heyting algebra morphism

$\alpha : H \to O(B)$, there is a unique morphism $h : T(H) \to B$, such that the diagram

$$\begin{array}{ccc} H & \xrightarrow{1_H} & H = OT(H) \\ & \searrow^{\alpha} & \downarrow{\scriptstyle O(h)} \\ & & O(B) \end{array}$$

commutes. By this definition we must have $O(h) = \alpha$. However, by Lemma 5.4.7 $T(\alpha) : T(H) \to B$ is the unique extension of α such that $OT(\alpha) = \alpha$. Hence, $h = T(\alpha)$ is unique and the adjunction is well-defined. $\square$

Corollary 5.4.9. *T : **Heyt** $\to$ **TopBool** is fully faithful, and preserves and reflects surjections and injections.*

Proof. Since the unit of our adjunction is given by the identity for each $H \in \mathbf{Heyt}$, it is clearly an isomorphism, and so T is fully faithful by our preliminary results for adjunctions. If $f : H \to H'$ in **Heyt** is surjective, consider an element $b \in T(H')$, then for some $u_1, ..., u_n, v_1, ..., v_n \in H'$ we have,

$$b = \bigwedge_{i=1}^{n} (u_i \vee \neg v_i) = \bigwedge_{i=1}^{n} (f(x_i) \vee \neg f(y_i)) = T(f)(\bigwedge_{i=1}^{n} (x_i \vee \neg y_i))$$

where $x_1, ..., x_n, y_1, ..., y_n \in H$, since f is surjective. Hence, $T(f)$ is surjective. Furthermore, for any $T(f) : T(H) \to T(H')$, then $OT(f) = f : H \to H'$, then since O preserves injections and surjections, T reflects injections and surjections. $\square$

Our next results discuss the size of free algebras and the completeness of **TopBool** with respect to finite models.

Theorem 5.4.10. *The free Topological Boolean algebra over the one element set $\{x\}$, which we denote $F_{TB}(\{x\})$, has infinitely many elements.*

Proof. For any Heyting algebra H, we have that H is a subset of $T(H)$. Therefore $TF_{\mathbf{Heyt}}(\{x\})$ is infinite since it contains an infinite subset. Then consider that any element $a \in TF_{\mathbf{Heyt}}(\{x\})$ can be expressed by,

$$a = \bigwedge_{i=1}^{n} (y_i \vee \neg z_i)$$

for $y_i, z_i \in F_{\mathbf{Heyt}}$. Furthermore, note that each $u \in F_{\mathbf{Heyt}}(\{x\})$ can be written in terms of x and the algebraic operations in the signature of **TopBool**, where Heyting implication, $\to$, of elements $u, w \in F_{\mathbf{Heyt}}(\{x\})$ can be expressed by $\square(\neg u \vee w)$. That is, each element of $TF_{\mathbf{Heyt}}(\{x\})$ is an equivalence class of terms in $F_\Omega(\{x\})$ where $\Omega = \{\wedge, \vee, \neg, \square, 0, 1\}$. Hence, there exists some surjective quotient map $f : F_\Omega(\{x\}) \to TF_{\mathbf{Heyt}}(\{x\})$. Therefore, since $TF_{\mathbf{Heyt}}(\{x\})$ is in **TopBool**, by the adjunction between $\mathbf{Alg}(\Omega)$ and **TopBool**, there exists a unique morphism $h : F_{TB}(\{x\}) \to TF_{\mathbf{Heyt}}(\{x\})$ such that the diagram (in $\mathbf{Alg}(\Omega)$),

$$\begin{array}{ccc} F_\Omega(\{x\}) & \xrightarrow{q} & F_{TB}(\{x\}) \\ & \searrow^{f} & \downarrow h \\ & & TF_{\mathbf{Heyt}}(\{x\}) \end{array}$$

commutes. However, since f is surjective and $hq = f$, then h is surjective. Therefore, since $TF_{\mathbf{Heyt}}(\{x\})$ is infinite, $F_{TB}(\{x\})$ has infinitely many elements. □

Further examples of infinite topological Boolean algebras generated by one element, which can be used to prove the above theorem in a similar manner, are discussed by Blok in [5]. We can again apply Lemma 3.9.6 to the above result and obtain the following corollary.

Corollary 5.4.11. *There is no finite topological Boolean algebra L such that **TopBool** is L-complete. In particular there is no finite $L \in$ **TopBool** such that $f(x) = f(y)$ for all $f \in hom(F_{TB}(\{x\}), L)$ if and only if $x = y$.*

It follows from this that the methods used to construct the algorithms to determine theorems in classical logic will be unable to be computed in finitely many steps when applied to topological Boolean algebras. Hence, as is the case for intuitionistic logic, the theorems of **S4** cannot be decidably determined through algebraic algorithms similar to those introduced in Chapter 2.

References

[1] Bergman, G. 2015. *An invitation to general algebra and universal constructions.* 2nd ed. Cham: Springer. 304–333.

[2] Birkhoff, G. 1935. On the Structure of Abstract Algebras. *Proceedings of the Cambridge Philosophical Society.* 31(4):433–454.

[3] Blackburn, P., Rijke, M. and Venema, Y. 2001. *Modal Logic.* Cambridge: Cambridge University Press. 33–41.

[4] Blok, W., and Dwinger, P. 1975. Equational Classes of Closure Algebras. *Indagationes Mathimaticae.* 78(3):189–198.

[5] Blok, W. 1976. Varieties of Interior Algebras. PhD Thesis. Universiteit van Amsterdam. 24-27, 30–34.

[6] Borceux, F. 1994. *Handbook of Categorical Algebra 3, Categories of Sheaves.* Cambridge: Cambridge University Press. 1–18.

[7] Burris, S. and Sankappanavar, H. 1981. *A Course in Universal Algebra.* New York: Springer-Verlag. 28, 51–53.

[8] Cresswell, M., and Hughes, G. 1968. *An Introduction to Modal Logic.* London: Methuen and Co Ltd. 22–61, 311–321.

[9] Davey, B. and Priestley, H. 2002. *Introduction to lattices and order.* 2nd. ed. New York: Cambridge University Press. 93–116.

[10] Dummett, M. 1959. A Propositional Calculus with a Denumerable Matrix. *The Journal of Symbolic Logic.* 24(2):97–106.

[11] Horn, A. 1969. Logic with Truth Values in a Linearly Ordered Heyting Algebra. *The Journal of Symbolic Logic.* 34(3):395–408.

[12] Johnstone, P. 1982. *Stone Spaces.* Cambridge: Cambridge University Press. 32–35.

[13] Mac Lane, S. 1971. *Categories for the Working Mathematician.* New York: Springer-Verlag. 1–27, 62–72, 79–105.

[14] McKinsey, J., and Tarski, A. 1946. On Closed Elements in Closure Algebras. *Annals of Mathematics.* 47(1):122–162.

[15] Mendelson, E. 1997. *Introduction to Mathematical Logic*. 4th ed. London: Chapman and Hall. 33–50.

[16] Rasiowa, H. and Sikorski, R. 1963. *The Mathematics of Metamathematics*. Warsawa: Polska Akademia Nauk, Monografie Matematyczne. 1–63, 93–100, 123–135, 376–397, 469–481.

[17] Sikorski, R. 1969. *Boolean Algebras*. 3rd Ed. Berlin: Springer-Verlag. 1–11, 27–29, 51–54.