Algebra 30710 Final Project

Henry Jochaniewicz

December 2024

1 Introduction.

This final project is a discussion and analysis of *Boolean rings* and *Boolean algebras*, which are structures which have broad applications, especially in computer science. Each Boolean algebra is in fact a Boolean ring, and vice versa. They are also both intensely related to the power set. We will explore all these ideas in this short paper.

2 Buildup: Lattices, Lattice Properties, and the Power Set.

To explain this, we will use the power set as an example to frame some more complicated ideas throughout this paper.

Definition 2.1 (Power set)**.** For a set X, we define $\mathcal{P}(X)$, the *power set of* X, as the set of all subsets of X. Formally,

$$\mathcal{P}(X) \coloneqq \{x : x \subseteq X\}.$$

One of the axioms of ZFC Set Theory indicates that for every set X, $\mathcal{P}(X)$ exists.

The power set has a lot of interesting aspects to it, and related to algebra, we will eventually impose a ring structure on it. But first, we will examine why the power set has a special structure called a Boolean algebra.

To get to that point, we need to recall a partial order.

Definition 2.2 (Partial Order)**.** A relation $R \subseteq X \times X$ on a set X is called a *partial order* if and only if it satisfies the following:

1. **Reflexivity.** $\forall x \in X, (x, x) \in R$.
2. **Antisymmetry.** $\forall x, y \in X$, if $(x, y), (y, x) \in R$, then $x = y$.
3. **Transitivity.** $\forall x, y, z \in X$, if $(x, y), (y, z) \in R$, then $(x, z) \in R$.

We shall let the symbol $\preceq$ indicate an arbitrary partial order, i.e. $a \preceq b \iff (a, b) \in R$.

We will refer to a set with a partial order as a partially ordered set, or **poset**. For the example of the power set, we can define a partial order with $\subseteq$.

To define a Boolean algebra, we must define the following:

Definition 2.3 (Upper/lower bound, supremum/infimum)**.** For a set X with a partial order $\preceq$, consider $W \subseteq X$. We call $a \in X$ an *upper bound* of W if $\forall w \in W$, $w \preceq a$. We similarly call $b \in X$ a *lower bound* of W if $\forall w \in W$, $b \preceq w$. The least upper bound of W is called the *supremum* of W, and the greatest lower bound of W is called the *infimum* of W. By being the least upper bound and greatest lower bound, it's clear that the supremum and infimum are unique.

Now, it's possible that a subset of a poset has no infimum or supremum. But when this is the case, we call it a lattice.

Definition 2.4 (Lattice)**.** For a poset X with partial order $\preceq$, we call X a *lattice* if and only if $\forall a, b \in X$, a, b has an infimum and supremum.[1] We denote the supremum as $a \vee b$, called the *join*, and similarly the infimum as $a \wedge b$, called the meet.

[1] Technically, $\{a, b\}$ would have an infimum and supremum, but this distinction is unimportant.

The power set is actually a lattice. We can show this now:

Proof. Consider the poset $(\mathcal{P}(X), \subseteq)$ on a set X.

Let $A, B \in \mathcal{P}(X)$. It's clear that $A, B \subseteq A \cup B$, and $A \cap B \subseteq A, B$, so $A \cup B$ is an upper bound and $A \cap B$ is a lower bound. We will show they are the join and meet of A, B.

Let u be an upper bound of A, B, so $A, B \subseteq u$. Let $a \in A \cup B$. Then $a \in A$ or $a \in B$. In both cases, $a \in u$. Thus $A \cup B \subseteq u$. So, $A \cup B$ is the supremum, and thus $A \cup B = A \vee B$.

Let v be a lower bound of A, B, so $v \subseteq A, B$. Let $b \in V$. Then $b \in A, B$. So, $b \in A \cap B \implies v \subseteq A \cap B$. So, $A \cap B$ is the supremum, and thus $A \cap B = A \wedge B$.

A, B were arbitrary, so every pair of elements has a join and meet. Thus, $\mathcal{P}(X)$ is a lattice.

Q.E.D.

There are a few properties of lattices we summarize here but shall not prove (because they are fairly straightforward, and there's cooler stuff to get to). They will be useful to have, though.

Theorem 1. *The following are true for elements a, b, c of a lattice L:*

1. ***Commutativity.*** $a \vee b = b \vee a$ *and* $a \wedge b = b \wedge a$.
2. ***Associativity.*** $a \vee (b \vee c) = (a \vee b) \vee c$ *and* $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.
3. ***Idempotency.*** $a \vee a = a \wedge a = a$.
4. ***Absorption.*** $a \vee (a \wedge b) = a \wedge (a \vee b) = a$.

Any set with binary operations with these properties is also a lattice. This will be used later.

Theorem 2. *Let L be a nonempty set with binary operations $\wedge, \vee$ that satisfy the above laws in Theorem 1. Then, for $a, b \in L$, we define partial order $a \preceq b$ if $a \vee b = b$ and $a \wedge b = a$. If we define the supremum and infimum of a, b as $a \vee b, a \wedge b$ respectively, then L is a lattice with respect to $\preceq$.*

Proof. We must first show $\preceq$ is a valid partial order. Let $a, b, c \in L$.

Observe $a \vee a = a = a \wedge a$ by idempotency, so $\preceq$ is reflexive.

Observe $a \preceq b, b \preceq a \implies a \vee b = b, b \vee a = a \implies b = a \vee b = b \vee a = a$ by commutativity. Similarly, $a \preceq b, b \preceq a \implies a \wedge b = a, b \wedge a = b \implies b = b \wedge a = a \wedge b = a$. So, $\preceq$ is antisymmetric.

Lastly, $a \preceq b, b \preceq c \implies a \vee b = b, b \vee c = c \implies a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$, and $a \preceq b, b \preceq c \implies a \wedge b = a, b \wedge c = b \implies a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$. Taken together, we conclude $a \preceq c$. Thus, $\preceq$ is transitive.

So, $\preceq$ is a partial order. We now show that each pair of elements in L has a supremum and infimum. Let $a, b \in L$.

Because by absorption and commutativity $a = (a \wedge b) \vee a$, $b = (a \wedge b) \vee b$, we conclude $a \wedge b \preceq a, b \implies a \wedge b$ is a lower bound. Let t be some other lower bound. So, $t \preceq a, b \implies t \wedge a = t, t \wedge b = t$. But $t \wedge (a \wedge b) = (t \wedge a) \wedge b = t \wedge b = t \implies t \preceq a \wedge b$.

Similarly, $a = a \wedge (a \vee b)$, $b = b \wedge (a \vee b)$ tells us that $a, b \preceq a \vee b \implies a \vee b$ is an upper bound. Let u be some other upper bound, so $a, b \preceq u \implies a \vee u = u$ and $b \vee u = u$. But $(a \vee b) \vee u = a \vee (b \vee u) = a \vee u = u \implies a \vee b \preceq u$.

Thus, $a \vee b$ is the supremum and $a \wedge b$ is the infimum. So L is a lattice.

Q.E.D.

Now, it's possible for a lattice to have a 'greatest' and 'least' element. We quickly define this now as it is relevant to define a Boolean algebra.

Definition 2.5. For a lattice L, an element $I \in L$ is called a greatest element if $\forall a \in L$, $a \preceq I$. Similarly, $O \in L$ is a least element if $\forall a \in L$, $O \preceq a$. Thus, $a \vee I = I$, $a \wedge O = O$, $a \wedge I = a$, $a \vee O = a$.

We will refer to the smallest element as O and the largest as I in order to not confuse with $0, 1$ of a ring structure.

If we look to $\mathcal{P}(X)$, it's clear the greatest and least element are $X, \varnothing$ respectively.

Quickly, let us recall set difference. For sets A, B, we define $A - B$ as the following:

$$A - B := \{z : z \in A \text{ and } z \notin B\}.$$

This is relevant to explore an interesting property of the power set with its greatest and least elements (X and $\varnothing$). For some element $A \in \mathcal{P}(X)$, $(X - A) \cap A = \varnothing$, $(X - A) \cup A = X$. We call $X - A$ the **complement** of A, denoted A'. We can abstract this to all lattices.

Definition 2.6 (Complemented)**.** A lattice L with a greatest element I and smallest O is *complemented* if and only if $\forall x \in L, \exists x' \in L$ such that $x \vee x' = I$, $x \wedge x' = O$.

The power set is clearly complemented, as shown above. There's one more property that the power set fulfills, though:

Definition 2.7 (Distributive)**.** A lattice L is called distributive if and only if $\forall a, b, c \in L$,

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

It can be easily be shown that this above law holds if and only if the following holds:[2]

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

This holds for the power set, since $\forall A, B, C \in \mathcal{P}(X)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, and the same holds if we swap $\cup, \cap$.

We can finally lift the veil on what the power set is.

3 Boolean Algebras.

The power set, in fulfilling all of these properties given in the above section, has a special structure: a *Boolean algebra.*

Definition 3.1 (Boolean Algebra)**.** A lattice L with O and I that is both complemented and distributive is called a Boolean algebra.

After defining all that whatnot with infimums, supremums, and partial orders, we can actually abstract out all of these to just two binary operations $\vee, \wedge$, and define a binary algebra as such.

Theorem 3. *A set B is a Boolean algebra if and only if there exist two binary operations $\vee, \wedge$ such that the following holds for $a, b, c \in B$:*

1. $a \vee b = b \vee a$ *and* $a \wedge b = b \wedge a$.
2. $a \vee (b \vee c) = (a \vee b) \vee c$ *and* $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.
3. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ *and* $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.
4. $(\exists I, O \in B)(a \vee O = a$ *and* $a \wedge I = a)$.
5. $(\forall a \in B)(\exists a' \in B)(a \vee a' = I, a \wedge a' = O)$.

Proof. The forward direction is immediate via definitions and previous theorems. We prove the reverse.

Let B be a set with binary operations $\vee, \wedge$ satisfying (1)-(5) above.

We must satisfy the commutativity, associativity, idempotence, and absorption laws of a lattice. But commutativity, associativity is given, so we only need show idempotency and absorption.

Let $a, b \in B$. Then we know:

$$\begin{aligned} a &= a \vee O \\ &= a \vee (a \wedge a') \\ &= (a \vee a) \wedge (a \vee a') \\ &= (a \vee a) \wedge I \\ &= a \vee a. \end{aligned}$$

[2] See Judson's *Abstract Algebra: Theory and Applications*, Theorem 19.15, for a proof.

The other idempotent law is proved the same, but by replacing $\vee, O$ with $\wedge, I$ at each instance. Also,

$$\begin{aligned} a \vee (a \wedge b) &= (a \wedge I) \vee (a \wedge b) \\ &= a \wedge (I \vee b) \\ &= a \wedge ((b' \vee b) \vee b) \\ &= a \wedge (b' \vee (b \vee b)) \\ &= a \wedge (b' \vee b) \\ &= (a \wedge I) = a. \end{aligned}$$

The other absorption law is proven the same, but by transposing $\vee, \wedge$ each time, and I with O.

Thus, B is a lattice. By Theorem 2, this means B is a poset with partial order $\preceq$ given by $a \preceq b$ if $a \vee b = b$ and $a \wedge b = a$.

It is given to us, then, that O is the least element of B because $O \vee a = a \implies O \preceq a$. We must now show I is the largest element of B. But $a \vee I = (a \wedge I) \vee I = I$ by absorption. So $a \preceq I$.

Thus, we conclude B is a Boolean algebra. Q.E.D.

By the above theorem, we know that $\mathcal{P}(X)$ is a Boolean algebra for a set X with largest element X and smallest element $\varnothing$.

We know some more about the power set, though; for example, $\forall A \in \mathcal{P}(X), A \cup X = X$ and $A \cap \varnothing = \varnothing$. We will show these properties now for all Boolean algebras, since we will need them for our conclusion in Section 5.

Theorem 4 (Uniqueness of Complements)**.** *For Boolean algebra B, let $a, b \in B$. Then $a \wedge b = O$ and $a \vee b = I \implies b = a'$.*

Theorem 5 (Domination)**.** *For Boolean algebra B with $\vee, \wedge$, $(\forall a \in B)(a \vee I = I, b \vee O = b)$.*

This is proven immediately via definition of I, O.

Theorem 6 (Complement of O, I)**.** *For Boolean algebra B, $I' = O$ and $O' = I$.*

Proof. Observe that $I \vee O = O \vee I = I$ and $I \wedge O = O \wedge I = O$ by definition. Q.E.D.

We use these to prove the final important theorem we need:

Theorem 7 (De Morgan's Laws)**.** *For Boolean algebra B, let $a, b \in B$. Then*

$$(a \wedge b)' = (a' \vee b') \text{ and } (a \vee b)' = (a' \wedge b').$$

Proof. We show $a \wedge b$ acts as the complement of $a' \vee b'$.

$$\begin{aligned} (a \wedge b) \wedge (a' \vee b') &= a \wedge ((b \wedge a') \vee (b \wedge b')) \\ &= a \wedge ((b \wedge a') \vee O) \\ &= a \wedge b \wedge a' \\ &= a \wedge a' \wedge b \\ &= O \wedge b \\ &= O \end{aligned}$$

Also,

$$\begin{aligned} (a \wedge b) \vee (a' \vee b') &= ((a \vee a') \wedge (b \vee a')) \vee b' \\ &= (I \wedge (b \vee a')) \vee b' \\ &= b \vee a' \vee b' \\ &= a' \vee I \\ &= I \end{aligned}$$

Thus, $(a \wedge b)' = (a' \vee b')$ by Theorem 4. It's nearly identical to show $a \wedge b$ acts as the complement of $a' \vee b'$ and similarly conclude $(a \vee b)' = a' \wedge b'$. Q.E.D.

As the power set is a Boolean algebra, it clearly has these properties as well. We will now turn from Boolean algebras to something intimately related: Boolean rings.

4 Boolean Rings.

Remember the power set? We can impose a ring structure on it. We won't actually *prove* it is a ring in this section because we wil prove more generally that *all* Boolean algebras are rings in Section 5.

To do so, we need to define an 'addition' and 'multiplication' on the power set.

We let addition over the power set be the symmetric difference.

Definition 4.1 (Symmetric Difference)**.** For sets A, B, the *symmetric difference* of A, B is denoted $A \oplus B$ and is defined as follows:

$$A \oplus B \coloneqq (A - B) \cup (B - A).$$

Now that we've found an addition through $\oplus$ on the power set, we now must define some sort of 'multiplication.' We shall use the intersection $\cap$ of two sets to do so. This allows us to fully impose the ring structure on the power set.

Theorem 8. *For a set X, $(\mathcal{P}(X), \oplus, \cap)$ is a commutative ring with unity.*

For now, take my word for this. It will be proved in a more general fashion in Section 5.

When looking at the power set, it has a special property that $\forall a \in \mathcal{P}(X)$, $a \cdot a = a \cap a = a$. This property is called *idempotency.* This makes the power set a special kind of ring called a *Boolean ring.*

Definition 4.2 (Boolean Ring)**.** A ring R is a *Boolean ring* such that $a \cdot a = a$ for all $a \in R$.

There are two properties nice about Boolean rings we will prove now:

Theorem 9. *For a Boolean ring R, $(\forall r \in R)(r + r = e = 0)$.*

Proof. Let R be a Boolean ring. Let $a \in R$.

We know that $(a + a) - (a + a) = 0$. But, $(a + a)(a + a) = a + a$, so

$$\begin{aligned} 0 &= (a + a)(a + a) - (a + a) \\ &= a \cdot a + a \cdot a + a \cdot a + a \cdot a - (a + a) \\ &= a + a + a + a - a - a \\ &= a + a. \end{aligned}$$

Thus, $a + a = 0$. Q.E.D.

Theorem 10. *Every Boolean ring is commutative.*

Proof. Let $(R, +, \cdot)$ be a Boolean ring. Let $a, b \in R$. Consider the following:

$$\begin{aligned} a + b &= (a + b)(a + b) \\ &= a \cdot a + b \cdot a + a \cdot b + b \cdot b \\ &= a + ba + ab + b \end{aligned}$$

So, $a + b = a + ba + ab + b \implies ba + ab = 0$. However, $ab + ab = 0$, since $ab \in R$. Thus,

$$ab + ba = ab + ab \implies ab = ba.$$

Thus, R is commutative.

Q.E.D.

It's quite interesting that the power set is both a Boolean algebra and a Boolean ring. The names are meant to be indicative of a greater connection which we now explore.

5 Boolean Algebrings.

Notice that the power set is a *Boolean algebra* under the operations $\cup, \cap$, and that the power set is a *Boolean ring* under the operations $\oplus, \cap$, and in fact, $\oplus$ is defined using $\cap, \cup$.

We can actually turn every Boolean algebra into a Boolean ring through a similar transformation.

Theorem 11 (Boolean Algebrings)**.** *A Boolean algebra B with operations $\vee, \wedge$ is a Boolean ring with multiplication $\wedge$ and addition defined as $x + y := (x' \wedge y) \vee (y' \wedge x)$.*

Proof. We will first show that $(B, +)$ is an abelian group.

Since a Boolean algebra is a lattice, by definition we know that, for $a, b \in B$, that $a \wedge b \in B$ since $a \wedge b$ is the infimum of a, b and thus is in B. We also know that $a', b' \in B$ because a Boolean algebra is a complemented lattice. Thus, we conclude $a' \wedge b, b' \wedge a \in B \implies (a' \wedge b) \vee (b' \wedge a) \in B$ since $\vee$ is similarly a closed operation like $\wedge$. But $a + b = (a' \wedge b) \vee (b' \wedge a) \in B$ by definition, so $a + b \in B$.

We now show, tediously, that $x + (y + z) = (x + y) + z$ for $x, y, z \in B$. Consider the following:

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

The right half of the above equation can be expanded as follows:

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

Thus,

$$(x+y)+z = (x' \wedge y \wedge z') \vee (x \wedge y' \wedge z') \vee (x' \wedge y' \wedge z) \vee (x \wedge y \wedge z).$$

If one has the patience, it is similarly tedious to show that $x + (y + z)$ evaluates to the same expression. Thus, $(x + y) + z = x + (y + z)$. This means that $+$ is associative.

Before we look to the identity and inverse, we show that B is abelian. For $x, y \in B$,

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

Because B is abelian, it simplifies the following calculations a bit.

We now show the identity element is O for arbitrary $a \in B$.

$$\begin{aligned}a + O = O + a &= (O' \wedge a) \vee (O \wedge a') \\ &= (I \wedge a) \vee O \\ &= a \vee O = a.\end{aligned}$$

So O is e_B. We now let $z \in B$. It turns out z is its own inverse:

$$\begin{aligned}z + z = z + z &= (z' \wedge z) \vee (z \wedge z') \\ &= O \vee O \\ &= O && \text{by idempotency.}\end{aligned}$$

The above suffices to show that $(B, +)$ is an abelian group.

We now show that $(B, +, \cdot)$ is a commutative ring with unity.

From above, we showed that $\wedge$ is a closed binary operation on B. Therefore, for $x, y \in B$, $x \cdot y = x \wedge y \in B$ is a closed operation. Similarly, $\wedge$ is an associative and commutative operation by Theorem 1, so $\cdot$ is similarly associative and commutative.

We now prove one of the distributivity laws, making heavy use of distribution of $\vee$ andi $\wedge$, commutativity, complement, domination, and DeMorgan's Laws:

$$\begin{aligned}
a \cdot (b + c) &= a \cdot ((b' \wedge c) \vee (c' \wedge b)) \\
&= a \wedge ((b' \wedge c) \vee (c' \wedge b)) \\
&= (a \wedge (b' \wedge c)) \vee (a \wedge (c' \wedge b)) \\
&= ((O \vee (a \wedge b')) \wedge c)) \vee ((O \vee (a \wedge c')) \wedge b)) \\
&= (((a \wedge a') \vee (a \wedge b')) \wedge c) \vee (((a \wedge a') \vee (a \wedge c')) \wedge b) \\
&= (a \wedge (a' \vee b') \wedge c) \vee (a \wedge (a' \vee c') \wedge b) \\
&= ((a \wedge b)' \wedge (a \wedge c)) \vee ((a \wedge c)' \wedge (a \wedge b)) \\
&= ((a \cdot b)' \wedge (a \cdot c)) \vee ((a \cdot c)' \wedge (a \cdot b)) \\
&= (a \cdot b) + (a \cdot c)
\end{aligned}$$

Knowing this distribution law, we easily prove the other using commutativity of multiplication:

$$\begin{aligned}
(a + b) \cdot c &= c \cdot (a + b) \\
&= c \cdot a + c \cdot b \\
&= a \cdot c + b \cdot c
\end{aligned}$$

The unity element of B is I, since $a \cdot I = I \cdot a = I \wedge a = a$.

Thus, B is a commutative ring with unity.

Lastly, B is a Boolean ring: $a \cdot a = a \wedge a = a$ by idempotency.

Thus, any Boolean algebra is a Boolean ring. Q.E.D.

Because the power set is a Boolean algebra, this theorem directly proves Theorem 8, since for $A, B \in \mathcal{P}(X)$,

$$A + B = (A' \wedge B) \vee (B' \wedge A) = ((X - A) \cap B) \cup ((X - B) \cap A) = (B - A) \cup (A - B) = A \oplus B.$$

Since every Boolean algebra is a Boolean ring, it would be nice if the reverse were true. Good thing it is!

Theorem 12 (Boolean Ringebras)**.** *Let $(B, +, \cdot)$ be a Boolean ring with unity. Then B is a Boolean algebra with operations $\wedge$ defined as $\cdot$ and $\vee$ defined as $x \vee y := x + y + xy$ and $x' = 1 - x$.*

Proof. By Theorem 3, we need only show that B fulfills properties of commutativity, assocativity, distributivity, that B has a greatest and least element, and each element has a complement in B.

Commutativity.

Let $a, b \in B$. By Theorem 10, we know $a \cdot b = b \cdot a$. But this is by definition $a \wedge b = b \wedge a$. Thus, $\wedge$ is commutative. We now show that $\vee$ is commutative. Observe:

$$a \vee b = a + b + ab = b + a + ba = b \vee a.$$

Associativity.

Let $a, b, c \in B$. Because B is a ring, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. But this is by definition $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Similarly,

$$\begin{aligned} a \vee (b \vee c) &= a + b \vee c + a(b \vee c) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \\ &= (a + b + ab) + c + (ac + bc + abc) \\ &= (a \vee b) + c + (a + b + ab)c \\ &= (a \vee b) + c + (a \vee b)c \\ &= (a \vee b) \vee c \end{aligned}$$

So, both binary operations are associative.

Distributivity.

Let $a, b \in B$.

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &= (a + b + ab) \cdot (a + c + ac) \\ &= aa + ac + aac + ba + bc + bac + aba + abc + abac \\ &= a + ac + ac + ab + bc + abc + ab + abc + abc \\ &= a + (ac + ac) + (ab + ab) + (abc + abc) + bc + abc \\ &= a + 0 + 0 + 0 + bc + abc \\ &= a + bc + abc \\ &= a \vee bc \\ &= a \vee (b \wedge c) \end{aligned}$$

Similarly,

$$\begin{aligned} (a \wedge b) \vee (a \wedge c) = ab \vee ac &= ab + ac + abac \\ &= ab + ac + abc \\ &= a(b + c + bc) \\ &= a \wedge (b \vee c) \end{aligned}$$

Greatest and Least Element O, I.

The greatest element of B is unity element 1, and the smallest element is $0 = e_B$. Let $a \in B$. Then, $a \vee 0 = a + 0 + a \cdot 0 = a$, and $a \wedge 1 = a \cdot 1 = a$.

Complement.

Let $a \in B$. We define $a' := 1 - a$. We show this satisifes the complement properties of a Boolean algebra.

$$a \vee a' = a + a' + aa' = a + 1 - a + a(1 - a) = 1 + a - aa = 1 + a - a = 1.$$

Similarly,

$$a \wedge a' = a(1 - a) = a - aa = a - a = 0.$$

All these properties being satisfies means we know that B is a Boolean algebra by Theorem 3.

Q.E.D.

This proves that every Boolean ring is a Boolean algebra and vice versa.

The power set is actually the *quintessential* Boolean algebra and Boolean ring. We show this relationship more directly now.

6 Isomorphism to the Power Set.

We first define a **finite Boolean algebra**, which is just a Boolean algebra whose set cardinality is finite. We also define what an isomorphism is between Boolean algebras (it is quite similar to rings and groups).

Definition 6.1 (Boolean algebra isomorphism)**.** For Boolean algebras B, C, a bijection $\varphi : B \to C$ is an isomorphism of boolean algebras if, $\forall a, b \in B$,

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

$$\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b).$$

It turns out every finite Boolean algebra, and consequently every Boolean ring, is isomorphic to the power set for some finite set. We need a few more definitions and lemmas to get there, though.

Definition 6.2 (Atom)**.** For Boolean algebra B, an element $a \in B$ is an *atom* if $a \neq O$ and $\forall b \in B$, $a \wedge b = a$ or $a \wedge b = O$. Another way to say this is that, if for $b \in B$, $b \preceq a$, then $b = O$ or $b = a$. Essentially, there is nothing *between* a and O with respect to $\preceq$ (except a).

Sensibly, any non-atom in a Boolean algebra should have an atom "below" it.

Lemma 1. *Let B be a finite Boolean algebra. Then, if $b \in B - \{O\}$, then $\exists a \in B$ where a is an atom such that $a \preceq b$. (It is possible that $a = b$).*

Proof. If b is an atom we are done. Otherwise, let $b_0 \in B$ where $b_0 \neq O, b$ and $b_0 \preceq b$. We know such an element exists because b is not an atom. We repeat the same process with b_0: if b_0 is an atom, we are done. Otherwise, $\exists b_1 \in B$ where $b_1 \neq O, b_0$ and $b_1 \preceq b_0$. This process produces a chain $O \preceq ... \preceq b_1 \preceq b_0 \preceq b$. We cannot continue this chain infinitely because B is finite; thus one of b_k, $k \in \mathbb{Z}$, is an atom. Q.E.D.

Addtionally, any two atoms, as atoms, should not share a greater lower bound that is not the least element of the Boolean algebra; otherwise, one of them isn't actually an atom. We prove this now:

Lemma 2. *Let B be a Boolean algebra, and let $a, b \in B$ be atoms where $a \neq b$. Then $a \wedge b = O$.*

Proof. Suppose $a \wedge b \neq O$. By Definition 2.4 and Theorem 3, $a \wedge b \preceq a$ as $a \wedge b$ is the infimum of a, b. Because $a \wedge b \in B - O$, though, $a \preceq a \wedge b$ by definition of a being an atom. So, $a = a \wedge b \implies a \preceq b$, so b is not an atom. This is a contradiction, so $a \wedge b = O$. Q.E.D.

Here are a few more lemmas to prove our final result:

Lemma 3. *Let B be a Boolean algebra. The following are equivalent for $a, b \in B$:*

1. $a \preceq b$
2. $a \wedge b' = O$
3. $a' \vee b = I$.

Proof. For 1 to 2: suppose $a \preceq b$, so $a \vee b = b$. Then,

$$\begin{aligned} a \wedge b' &= a \wedge (a \vee b)' \\ &= a \wedge (a' \wedge b') \\ &= (a \wedge a') \wedge b' \\ &= O \wedge b' = O. \end{aligned}$$

For 2 to 3: suppose $a \wedge b' = O$. Then $(a \wedge b')' = O' = I$. But $(a \wedge b')' = a' \vee b$ by De Morgan's Laws.

For 3 to 1: suppose $a' \vee b = I$. Then,

$$\begin{aligned} a &= a \wedge I \\ &= a \wedge (a' \vee b) \\ &= (a \wedge a') \vee (a \wedge b) \\ &= O \vee (a \wedge b) = a \wedge b \\ &\implies a \preceq b. \end{aligned}$$

Q.E.D.

Lemma 4. *For a Boolean algebra B, let $b, c \in B$ such that $b \npreceq c$. Then $\exists a \in B$ such that a is an atom, $a \preceq b$ and $a \npreceq c$.*

Proof. By Lemma 3, $b \npreceq c \implies b \wedge c' \neq O$. Thus, there exists an atom a where $a \preceq b \wedge c'$. Therefore, $a \preceq b$ and $a \preceq c'$. Thus $a \wedge c = O$ by Lemma 3. But $a \neq O$ by definition of an atom; so, $a \wedge c \neq a$, so $a \npreceq c$. Q.E.D.

These crucially culminate in this defining idea:

Lemma 5 (Constituent Atoms)**.** *Let $b \in B$ and $a_0, ..., a_n \in B$ be the set of all atoms such that $a_i \preceq b$. Then $b = a_0 \vee ... \vee a_n$. We will call $a_0, ..., a_n$ the* ***constituent atoms*** *of b.*

Proof. Let $c = a_0 \vee ... \vee a_n$. It's clear $c \preceq b$, since for any pair a_i, a_j, $a_i \vee b = b$ and $a_j \vee b = b \implies a_i \vee b = a_j \vee b \implies a_j \vee a_i \vee b = a_j \vee a_j \vee b = a_j \vee b = b \implies a_i \vee a_j \preceq b$.

Suppose by contradiction that $b \npreceq c$. Then by Lemma 4, $\exists a \in B$ atom where $a \preceq b$ and $a \npreceq c$. But because $a \preceq b$, $a \in \{a_0, ..., a_n\}$, so $a \preceq c$, which is a contradiction. Thus, $b \preceq c$, so by antisymmetry, $b = c$. Q.E.D.

Now we reach our conclusion:

Theorem 13 (Isomorphism to the Power Set)**.** *Let B be a finite Boolean algebra. Then there exists a set X where $B \cong \mathcal{P}(X)$.*

Proof. Let $X := \{a \in B : a \text{ is an atom}\}$. The bijection we define will be from an element of B to its constituent atoms in X. Formally, let $a \in B$. By above lemma, $a = a_0 \vee ... \vee a_n$, where $a_0, ..., a_n \in X$. Define $\varphi : B \to \mathcal{P}(X)$ as

$$\varphi(a) := \{a_0, ..., a_n\}.$$

This is surjective: let $A = \{x_1, ..., x_k\} \subseteq X$. Then $\varphi(x_1 \vee ... \vee x_k) = A$.

This is also injective: let $a, b \in B$, $a = a_0 \vee ... \vee a_m$, $b = b_0 \vee ... \vee b_n$. Then $\varphi(a) = \varphi(b) \implies \{a_0, ..., a_m\} = \{b_0, ..., b_n\} \implies a = b$.

Now observe:

$$\varphi(a \vee b) = \varphi(a_0 \vee ... \vee a_m \vee b_0 \vee ... \vee b_n) = \{a_0, ..., a_m, b_0, ..., b_n\} = \{a_0, ..., a_m\} \cup \{b_0, ..., b_n\} = \varphi(a) \cup \varphi(b).$$

Recall that $\cup$ is the equivalent of $\vee$ for the power set as a Boolean algebra, so this satisifies the first part of φ being an isomorphism.

This is slightly harder to show for $\wedge$. Let $c = a \wedge b$. Then $c = (a_0 \vee ... \vee a_m) \wedge (b_0 \vee ... \vee b_n) = c_0 \vee ... \vee c_h$ for $c_0, ..., c_h \in X$. We will show $\{c_0, .., c_h\} = \{a_0, ..., a_m\} \cap \{b_0, ..., b_n\}$.

> Let $c_i \in \{c_0, ..., c_h\}$. Then, $c_i \preceq c \preceq a, b$, so $c_i \preceq a, b$. But c_i is an atom, so $c_i \in \{a_0, ..., a_m\}$ and $c_i \in \{b_0, ..., b_n\}$, which implies $c_i \in \{a_0, ..., a_m\} \cap \{b_0, ..., b_n\}$. Similarly, let $x \in \{a_0, ..., a_m\} \cap \{b_0, ..., b_n\}$. Then, x is a constituent atom of a and b, so $x \preceq a, b$. Thus, x is a lower bound of a, b, so by definition, $x \preceq a \wedge b = c$, so $x \in \{c_0, ..., c_h\}$ because x is an atom.

This lets us conclude the following:

$$\varphi(a \wedge b) = \varphi(c) = \varphi(c_0 \vee ... \vee c_h) = \{c_0, ..., c_h\} = \{a_0, ..., a_m\} \cap \{b_0, ..., b_n\} = \varphi(a) \cap \varphi(b).$$

Recall that $\cap$ is the equivalent of $\wedge$ for the power set. So, φ is a Boolean algebra isomorphism.

Thus, $B \cong \mathcal{P}(X)$. Q.E.D.

Because every Boolean ring is a Boolean algebra and vice versa, this means every finite Boolean ring is isomorphic to the power set of some set as a *Boolean algebra*. However, this *also* means that every Boolean ring is isomorphic to the power set of some set as a *ring*, because we define the ring structure on a Boolean algebra via the operations of that Boolean algebra. The only thing that remains to be shown is that unity element of a Boolean ring, which is the largest element of that set as a Boolean algebra, maps to the unity element of the power set via φ.

Corollary 1. *Let B be a finite Boolean ring. Then B is a finite Boolean algebra. The unity element $1 \in B$ is I when B is a Boolean algebra. Then, using φ defined in the above theorem, $\varphi(I) = X = 1_{\mathcal{P}(X)}$, where X is the set of all atoms of B (defined the same as in the above theorem).*

Proof. Let B be a finite Boolean ring. Then, $1_B = I$ is the greatest element of B as a Boolean algebra. Because $I \in B$, $I = a_0 \vee ... \vee a_k$ for atoms $a_0, ..., a_k \in X$. However, $(\forall x \in B)(x \preceq I)$, and since $(\forall y \in X)(y \in B)$, we conclude the constituent of I are all atoms in B, so $\{a_0, ..., a_k\} = X$. Thus, $\varphi(I) = \varphi(a_0 \vee ... \vee a_k) = \{a_0, ..., a_k\} = X = 1_{\mathcal{P}(X)}$. Q.E.D.

This makes the power set the quintessential Boolean algebra and Boolean ring, which concludes the goals for this project. I hope you enjoyed it (I enjoyed writing it). Thank you for reading!