Boolean Algebras

Harini Desikan

May 2020

1 Introduction

This paper explains the elementary theory of Boolean Algebras in detail. It develops all of the important machinery and concludes with a short section on more advanced and exciting things one can do with these structures.

2 Boolean Rings

A ring is a set which forms an abelian group under addition, and has an associative multiplication operation. The distributive property is required to hold, but the multiplication operation need not be commutative or have an identity. When the multiplication operation is commutative, we call the ring a commutative ring. When a ring has a multiplicative identity, we call it a ring with unit.

A ring has characteristic 2 if every element is its own inverse, and it is idempotent if every element is its own square. A Boolean ring is an idempotent ring with unit.

Boolean rings always have characteristic 2, and they are also always commutative.

Proof: For any two elements p and q, we have $p + q = (p + q)^2 = p^2 + pq + qp + q^2 = p + pq + qp + q$, so $0 = pq + qp$.

So if $p = q$, we have $0 = p \cdot p + p \cdot p = p + p$, so $p = -p$. Thus the ring has characteristic 2. This means that for any two elements p and q, $pq = -qp = qp$, and the ring is also commutative.

Example: the ring consisting of just two elements, 0 and 1, with addition mod 2 and multiplication as usual, is a boolean ring.

Example: Take the Klein Four Group and set that group operation to be addition. Define multiplication such that the ring is idempotent. This is a Boolean ring.

Example: the set 2^X, or the set of functions from X to 2, is a Boolean ring. Addition of two such functions is defined as $(p+q)x = p(x)+q(x)$ (with addition mod 2, as usual), and multiplication is defined as $(pq)(x) = p(x)q(x)$. Proving this is a little bit more technically complicated but intuitively the same.

3 Boolean Algebras

A Boolean Algebra is a nonempty set A, together with two binary operations $\wedge$ and $\vee$, one unary operation $'$, and two special elements 0 and 1, satisfying the following axioms:

1. $0' = 1$ and $1' = 0$
2. $p \wedge 0 = 0$ and $p \vee 1 = 1$
3. $p \wedge 1 = p$ and $p \vee 0 = p$
4. $p \wedge p' = 0$ and $p \vee p' = 1$
5. $(p')' = p$
6. $p \wedge p = p$ and $p \vee p = p$
7. $(p \wedge q)' = p' \vee q'$ and $(p \vee q)' = p' \wedge q'$
8. $p \wedge q = q \wedge p$ and $p \vee q = q \vee p$
9. $p \wedge (q \wedge r) = (p \wedge q) \wedge r$ and $p \vee (q \vee r) = (p \vee q) \vee r$
10. $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ and $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$

Example: if $A = P(X)$, then 1 would represent the whole space X while 0 would represent the empty set. $\wedge$ would represent intersection, $\vee$ would represent union, and $'$ would represent complementation.

Example: The set A need not even be the whole power set of X. Let X be the set of natural numbers, and let A be the set of all finite subsets and cofinite subsets of X. (Cofinite subsets include all but finitely many elements.) Then A is still a Boolean algebra under the operations of intersection, union, and complementation, since it is closed under all three. We call this the finite-cofinite Boolean algebra.

4 Boolean Algebras vs Rings

Boolean algebras and Boolean rings look awfully similar. Given an arbitrary Boolean algebra, can we turn it into a Boolean ring, and vice versa?

This is, in fact, something we can do. Let's see how to prove it.

First we will take an arbitrary Boolean algebra A and turn it into a Boolean ring. Take a boolean algebra A. Let $p + q$ be defined as $(p \wedge q') \vee (q \wedge p')$, and let $p \cdot q$ be defined as $p \wedge q$.

We want to show that A, with these operations of $+$ and $\cdot$, is a Boolean ring.

Commutativity and associativity of addition and and associativity of multiplication are both trivial. To show that every element is its own additive inverse, take an element p. Then $p + p = (p \wedge p') \vee (p \wedge p') = 0 \vee 0 = 0$.

To show that every element is its own square, take an element p. Then $p \cdot p = p \wedge p = p$.

Next, we show that the distributive property holds. We have that

$$\begin{aligned} p \cdot (q + r) &= p \wedge ((q \wedge r') \vee (r \wedge q')) \\ &= (p \wedge (q \wedge r')) \vee (p \wedge (r \wedge q')) \\ &= ((p \wedge q) \wedge r') \vee ((p \wedge r) \wedge q') \end{aligned}$$

We can simply verify that this is equal to

$$\begin{aligned} &= ((p \wedge q) \wedge (p' \vee r')) \vee ((p \wedge r) \wedge (p' \vee q')) \\ &= ((p \wedge q) \wedge (p \wedge r)') \vee ((p \wedge r) \wedge (p \wedge q)') \\ &= (p \wedge q) + (p \wedge r) \\ &= pq + pr \end{aligned}$$

.

Therefore, any Boolean Algebra can also be represented as a Boolean ring. The converse can also be done. Take an arbitrary Boolean ring R. Define

1. $p \vee q = p + q + pq$
2. $p \wedge q = pq$
3. $p' = p + 1$

We verify each of the Boolean algebra axioms, recalling that our original ring is idempotent, commutative and has characteristic 2:

1. $0' = 0 + 1 = 1$ and $1' = 1 + 1 = 0$
2. $p \wedge 0 = p \cdot 0 = 0$ and $p \vee 1 = p + 1 + p \cdot 1 = p + p + 1 = 1$
3. $p \wedge 1 = p \cdot 1 = p$ and $p \vee 0 = p + 0 + p \cdot 0 = p$
4. $p \wedge p' = p \cdot (p+1) = p^2 + p \cdot 1 = p + p = 0$ and $p \vee p' = p + p + 1 + p(p+1) = 1$
5. $(p')' = (p + 1) + 1 = p$
6. $p \wedge p = p \cdot p = p$ and $p \vee p = p + p + p \cdot p = p$
7. $(p \wedge q)' = pq + 1 = (p + 1) + (q + 1) + (p + 1)(q + 1) = p' \vee q'$ and $(p \vee q)' = p + q + pq + 1 = (p + 1)(q + 1) = p' \wedge q'$
8. $p \wedge q = pq = qp = q \wedge p$ and $p \vee q = pq + p + q = qp + q + p = q \vee p$
9. $$p \wedge (q \wedge r) = p(qr) = (pq)r = (p \wedge q) \wedge r$$

   and

   $p \vee (q \vee r) = p \vee (qr + q + r) = p(qr + q + r) + p + qr + q + r = (pq + p + q)r + pq + p + q + r = (p \vee q) \vee r$

10.

$p \wedge (q \vee r) = p(qr+q+r) = pqr+pq+pr = (pq)(pr)+pq+pr = (p \wedge q) \vee (p \wedge r)$

and

$$p \vee (q \wedge r) = p+qr+pqr = (pq)(pr)+p^2r+pqr+p^2q+p^2+pq+pqr+pr+qr$$

$$= (pq+p+q)(pr+p+r) = (p \vee q) \wedge (p \vee r)$$

So clearly this is a Boolean algebra.

Example: Take the Boolean algebra of the powerset of X. When we map $P(X)$ to a ring, the algebra will map to 2^X. A subset E of X will map to its characteristic function, that is, the function on X defined to be 1 on all values in E, and 0 elsewhere.

5 A Partial Ordering

Lemma: $p \wedge q = p$ iff $p \vee q = q$.

Proof: If $p \wedge q = p$, then $p \vee q = (p \wedge q) \vee q = q$. Similarly, if $p \vee q = q$, then $p \wedge q = p \wedge (p \vee q) = p$.

We let $p \leq q$ if $p \wedge q = p$, or equivalently, if $p \vee q = q$. If $\leq$ is a partial order, it will have the properties that

1. Reflexive: $p \leq p$
2. Antisymmetric: If $p \leq q$ and $q \leq p$, then $p = q$.
3. Transitive: If $p \leq q$ and $q \leq r$, then $p \leq r$.

We wish to prove that $\leq$ satisfies all of these properties.

Reflexive: For any p, $p \wedge p = p$, so $\leq$ must be reflexive.

Antisymmetric: If $p \leq q$ and $q \leq p$, then $p \wedge q = p$ and $q \wedge p = q$, so $p = p \wedge q = q \wedge p = q$.

Transitive: If $p \leq q$ and $q \leq r$, then $p \wedge q = p$ and $q \wedge r = q$. So $p \wedge r = (p \wedge q) \wedge r = p \wedge (q \wedge r) = p \wedge q = p$, as desired.

Therefore, $\leq$ is a partial order.

The following three facts also trivially follow from our definition of $\leq$:

1. For all p, $0 \leq p$ and $p \leq 1$.
2. If $p \leq q$ and $r \leq s$, then $p \wedge r \leq q \wedge s$ and $p \vee r \leq q \vee s$.
3. If $p \leq q$, then $q' \leq p'$.

Take a subset of a Boolean algebra E. The supremum of E is defined to be the least element of A that is greater than every element of E, if such an element exists. The infimum of E is defined to be the greatest element of A that is less than every element of E, if such an element exists. A Boolean algebra is *complete* if every subset has a supremum and infimum.

6 Applications

Boolean algebras can be used to show the independence of the Axiom of Choice, amongst other things. One can take a model theoretic universe and assign every statement a value from a complete Boolean algebra. Then, using ultrafilters, one can create a new model in which certain other statements are "forced" to be true.

They are also abundantly used when studying computer science.