Section 8.1: Boolean Algebra Structure

April 13, 2021

Abstract

First of all, note that we're only reading 8.1 through p. 626 (up to Isomorphic Boolean Algebras).

A Boolean algebra (named after George Boole[1]) is a generalization of both the propositional logic and the set theory we studied earlier this term. We are going to focus on using it to understand the basic elements of (computer) logic, however, which is based on a binary (0,1) alphabet.

In this first section we are introduced to the fundamental concepts of Boolean algebra.

1 Definition and Terminology

Definition: a **Boolean Algebra** is a set B on which are defined two binary operations $+$ and $\cdot$, and one unary operation $'$, and in which there are two distinct elements 0 and 1 such that the following properties hold for all $x, y, z \in B$:

$1a.\ x + y = y + x$	$1b.\ x \cdot y = y \cdot x$	commutative property
$2a.\ (x + y) + z = x + (y + z)$	$2b.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$	associative property
$3a.\ x + (y \cdot z) = (x + y) \cdot (x + z)$	$3b.\ x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	distributive property
$4a.\ x + 0 = x$	$4b.\ x \cdot 1 = x$	identity property
$5a.\ x + x' = 1$	$5b.\ x \cdot x' = 0$	complement property

The element x' is called the **complement** of x. The algebra may be denoted $[B, +, \cdot, ', 0, 1]$.

Of these properties, certainly the distributive property 3a. may seem the strangest, since it obviously doesn't hold for the usual suspects $+$ and $\cdot$. However these aren't the usual suspects!

Notice the beautiful **symmetry** (or **duality**) in this definition: the roles of $+$ and $\cdot$ are exactly reversed, as are the special elements 0 and 1.

Question: how are these reflected in the properties of propositional logic that we studied earlier this term?

$+ \to \cup \to \vee$

$\cdot \to \cap \to \wedge$

$S, \emptyset \quad T, F$

A change in notation: Speaking of propositional logic, as we move forward one change that I'll want you to make is to switch to thinking of truth *functions*, instead of wffs:

output - T or F

$$f : \underbrace{\{T, F\}^n}_{n\text{-tuple}} \to \{T, F\},$$

which take elements of the Cartisian product $\{T, F\}^n$ into the set $\{T, F\}$. We're doing algebra, afterall, so it seems reasonable that we'll want to operate on variables with functions.

So we'll want to think of implication, for example, as a function of two variables (wffs) of the form $f : \{T, F\}^2 \to \{T, F\}$. If we wrote out the truth table, there would be four rows for the domain (all ordered pairs of T, F), and the range values would be in the right column.

A	B	$A \longrightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

$f(T,T) = T$

$f(T,F) = F$

$\vdots$

Furthermore, we'll often want to replace "T" and "F" with 1 and 0 from now on.

There's an advantage to the function notation: we can speak of two functions being equal (=), to mean that their corresponding wffs are equivalent ($\iff$). Equality is a little easier to throw around....

In Example 2, p. 621, which illustrates the world's simplest Boolean Algebra, the set $B = \{0, 1\}$ consists of **only** two elements (so they must be our distinguished elements), and the binary operations of $+$ and $\cdot$ are given by $x + y = max(x, y)$ and by $x \cdot y = min(x, y)$. Complements are given by $0' = 1$ and $1' = 0$.

Example: Practice 1, p. 621 : Verify property 4b for the Boolean algebra of Example 2.

$x \cdot 1 = x$

Check 0: $0 \cdot 1 = min(0,1) = 0$ ✓

Check 1: $1 \cdot 1 = min(1,1) = 1$ ✓

Proof by exhaustion!

1.1 Idempotence

Curiously enough, $x + x = x$ in a Boolean algebra (this is the **idempotent property**. You'll want to remember that one, for any proofs!) And since $x + x = x$, we must have $x \cdot x = x$ by the beautiful symmetry of the operations. This symmetry, which you have already encountered as **duality**, means that we only have to do half the work most of the time (or that we oftentimes get something for free!).

You may have bumped into the notion of idempotence in linear algebra: for example, projection matrices are idempotent, such as

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

A very special case! Not at all true in general for matrices

This matrix projects three-dimensional space onto the first and second dimensions; and projecting onto those dimensions a second time doesn't change anything (i.e., $A \cdot A = A$). However, in a Boolean algebra, this property is true **for every element**!

Example: Practice 2, p. 624

a. What does the idempotent property of Example 3 become in the context of propositional logic? $x \wedge x = x \quad x \vee x = x$

b. What does it become in the context of set theory? $A \cap A = A$ & $A \cup A = A$

c. Let's prove the dual property $x \cdot x = x$. We get it for free by duality (but we can prove it, of course, using one of my favorite tricks in the book).

$$\begin{aligned} x \cdot x &= x \cdot x + 0 && (4a) \\ &= x \cdot x + x \cdot x' && (5b) \\ &= x \cdot (x + x') && (3b) \\ &= x \cdot (1) && (5a) \\ &= x && (4b) \end{aligned}$$

Example: Practice 3, p. 624

a. Prove that the property $x + 1 = 1$ holds in any Boolean algebra. Give a reason for each step.

b. What is the dual property?

$$\begin{aligned} x + 1 &= x + (x + x') && (5a) \\ &= (x + x) + x' && (2a) \\ &= x + x' && \text{idempotence} \\ &= 1 && (5a) \end{aligned}$$

$x \cdot 0 =$

$= 0$

Proof of Practice 3

1.2 Complements are Unique

Given an element x of the set B of a Boolean algebra, the complement x' is the **unique** element of B with the property that

$$\boxed{x + x' = 1 \text{ and } x \cdot x' = 0}$$

Furthermore, if you ever find an element a such that

$$x + a = 1 \text{ and } x \cdot a = 0$$

then $a = x'$. (The proof is on p. 625.)

2 Hints for proving Boolean Algebra Equalities (p. 624)

- Usually the best approach is to start with the more complicated expression and try to show that it reduces to the simpler expression via the axioms of the Boolean algebra.
- It may help to frame the argument in terms of either set theory or propositional logic, to give you a framework for understanding the thrust of the argument.
- Think of adding some form of 0 (like $x \cdot x'$) or multiplying by some form of 1 (like $x + x'$). [These are my among my favorite tricks in mathematics!]
- Don't forget property 3a, the distributive property of addition over multiplication (just because it seems weird).
- Remember the idempotent properties: $x + x = x$ and $x \cdot x = x$.
- Remember the uniqueness of complements.

3 Examples

Example: Exercise 8, p. 633 : Prove De Morgan's Laws for any Boolean algebra, e.g.

$$(x+y)' = x' \cdot y'$$

By uniqueness of complements:

Part I

$(x+y) + x' \cdot y'$
$= ((x+y)+x') \cdot ((x+y)+y')$ (3a)
$= ((y+x)+x') \cdot (x+(y+y'))$ (comm. & assoc.)
$= (y+(x+x')) \cdot (x+(y+y'))$ (assoc.)
$= (y+1) \cdot (x+1)$ (complements)
$= 1 \cdot 1$ (Practice 3)
$= 1$ (identity)

$(x+y) \cdot (x' \cdot y')$
$= ((x+y) \cdot x') \cdot y'$ (assoc.)
$= (x \cdot x' + y \cdot x') \cdot y'$ (dist.)
$= (0 + y \cdot x') \cdot y'$ (complements)
$= (y \cdot x') \cdot y'$ (identity)
$= (x' \cdot y) \cdot y'$ (comm.)
$= x' \cdot (y \cdot y')$ (assoc.)
$= x' \cdot 0$ (complements)
$= 0$ (Dual of Practice 3)

By uniqueness of complements, we must have $x' \cdot y' = (x+y)'$

$\therefore x' + y' = (x \cdot y)'$ by duality

Example: Exercise 14, p. 634 : Prove that in any Boolean algebra

$$x \cdot y' = 0 \iff x \cdot y = x$$

$\Rightarrow$: Assume $x \cdot y' = 0$
Consider
$x \cdot y = x \cdot y + 0$ (identity)
$= x \cdot y + x \cdot y'$ (hyp)
$= x \cdot (y + y')$ (dist.)
$= x \cdot 1$ (complements)
$= x$ (identity)

$\Leftarrow$: Assume $x \cdot y = x$
Consider
$x \cdot y' = (x \cdot y) \cdot y'$ (hyp)
$= x \cdot (y \cdot y')$ (assoc)
$= x \cdot 0$ (complements)
$= 0$ (Practice 3)

$A \cap B' = \emptyset \iff A \cap B = A$
(In set theory)

Example: Exercise 16a, p. 634 : Prove that in any Boolean algebra

$$x + y = 0 \to (x = 0 \wedge y = 0)$$

Let's prove that $x+y=0 \to x=0$; then by symmetry, we have $x+y=0 \to y=0$, & we'll have proven our theorem.

Assume $x+y=0$. Consider

$$\begin{aligned} x &= x+0 && \text{(identity)} \\ &= x+(x+y) && \text{(hyp)} \\ &= (x+x)+y && \text{(assoc.)} \\ &= x+y && \text{(idempotence)} \\ &= 0 && \text{(hyp)} \end{aligned}$$

$\therefore x=0$

$\therefore y=0$ by symmetry

$\therefore x=0 \wedge y=0$

4 One last cool thing...

This section ends "in the weeds" a bit, but the upshot is really interesting: the characterization of all finite Boolean algebras. It turns out that every **finite** Boolean algebra is of order (size) 2^n. **Can you think of a finite Boolean algebra with 2^n elements?**[2]

Then it turns out that every finite Boolean algebra is isomorphic to every other finite Boolean algebra of the same order. The power... of the Power set!

Consider a set A of n elements. Then $B = \mathcal{P}(A)$ has cardinality 2^n - All subsets of A. The binary operations on the power set are $\cap$, & $\cup$; the unary operation is set complement; the 1 is A; the 0 is $\emptyset$.

If you have a finite Boolean Algebra, you may as well think of it as this set theoretic Boolean Algebra - They're "isomorphic" to "power set" Boolean algebras.

[2]Subsets of a set S of order n, with intersection and union, and special elements S and $\emptyset$.