3. Abstract Boolean Algebras

3.1. Abstract Boolean Algebra.

Definition 3.1.1. *An* **abstract Boolean algebra** *is defined as a set* $\mathcal{B}$ *containing two distinct elements* 0 *and* 1, *together with binary operations* $+, \cdot$, *and a unary operation* $^-$, *having the following properties:*

$x + 0 = x$ $x \cdot 1 = x$	*Identity Laws*
$x + \overline{x} = 1$ $x \cdot \overline{x} = 0$	*Compliments Laws*
$(x + y) + z = x + (y + z)$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$	*Associative Laws*
$x + y = y + x$ $x \cdot y = y \cdot x$	*Commutative Laws*
$x + (y \cdot z) = (x + y) \cdot (x + z)$ $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	*Distributive Laws*

Discussion

The definition of an abstract Boolean algebra gives the **axioms** for an abstract Boolean algebra. The unary operation $^-$ is called **complementation**. Named after the English mathematician George Boole (1815-1864), Boolean algebras are especially important in computer science because of their applications to switching theory and design of digital computers.

3.2. Examples of Boolean Algebras. Examples.

1. $B = \{0, 1\}$ together with the operations $+, \cdot, ^-$ described in *Boolean Functions* is a Boolean Algebra.
2. B^k together with the operations
   (a) $(x_1, x_2, x_3, \ldots, x_k) + (y_1, y_2, y_3, \ldots, y_k) = (x_1 + y_1, x_2 + y_2, x_3 + y_3, \ldots, x_k + y_k)$
   (b) $(x_1, x_2, x_3, \ldots, x_k) \cdot (y_1, y_2, y_3, \ldots, y_k) = (x_1 \cdot y_1, x_2 \cdot y_2, x_3 \cdot y_3, \ldots, x_k \cdot y_k)$
   (c) $\overline{(x_1, x_2, x_3, \ldots, x_k)} = (\overline{x_1}, \overline{x_2}, \overline{x_3}, \ldots, \overline{x_k})$

   is a Boolean Algebra.

   We can find the element of B^k that is considered the "one element" by asking which element of B^k will satisfy the properties: $x \cdot$ "one" $= x$ and $x + \overline{x} =$ "one" for all $x \in B^k$? In other words, using the definition of the operations in B^k we need to find the element of B^k so that for all $(x_1, x_2, x_3, \ldots, x_k) \in B^k$ we have

$(x_1, x_2, x_3, \ldots, x_k)\cdot$"one" $= (x_1, x_2, x_3, \ldots, x_k)$ and $(x_1 \cdot \overline{x_1}, x_2 \cdot \overline{x_2}, x_3 \cdot \overline{x_3}, \ldots, x_k \cdot \overline{x_k})$. Notice that the ordered k-tuple of all 1's satisfies these properties, so the "one" element is $(1, 1, 1, \ldots, 1)$.

3. $BOOL(k)$ defined to be the set of all Boolean functions of degree k together with the operations
   (a) $F + G$ (or $F \vee G$) defined by $(F + G)(u) = F(u) + G(u)$ for any $u \in B^k$,
   (b) $F \cdot G$ (or $F \wedge G$) defined by $(F \cdot G)(u) = F(u) \cdot G(u)$ for any $u \in B^k$,
   (c) and $\overline{F}$ defined by $\overline{F}(u) = \overline{F(u)}$ for any $u \in B^k$.
   is a Boolean Algebra.
4. Let S be a set and let $FUN(S, \{0, 1\})$ be the set of all functions with domain S and codomain $\{0, 1\}$. Define the Boolean operations on $FUN(S, \{0, 1\})$ as follows: Let $F, G \in FUN(S, \{0, 1\})$, then
   (a) $F + G : S \to \{0, 1\}$ is the function defined by $(F + G)(x) = F(x) + G(x)$ for all $x \in S$,
   (b) $F \cdot G : S \to \{0, 1\}$ is the function defined by $(F \cdot G)(x) = F(x) \cdot G(x)$ for all $x \in S$,
   (c) $\overline{F} : S \to \{0, 1\}$ is the function defined by $\overline{F}(x) = \overline{F(x)}$ for all $x \in S$,
   $FUN(S, \{0, 1\})$ together with these operations is a Boolean Algebra.
5. Let S be a set. The power set $P(S)$ together with the operations
   (a) $A + B = A \cup B$ for all $A, B \in P(S)$
   (b) $A \cdot B = A \cap B$ for all $A, B \in P(S)$
   (c) $\overline{A}$ is the complement of A for all $A \in P(S)$
   is a Boolean Algebra.

   We can find the element of $P(S)$ that is the "one" element by asking which element of $P(S)$ will satisfy the identity and compliments properties of a Boolean algebra. Interpreting this in terms of the way the operations are defined on this set we see the set S is the element in $P(S)$ that satisfies the properties since $A \cup \overline{A} = S$ and $A \cap S = A$ for any set A in $P(S)$.
6. The set $D_6 = \{1, 2, 3, 6\}$ along with the operations
   (a) $a + b = lcm(a, b)$ for all $a, b \in D_6$
   (b) $a \cdot b = gcd(a, b)$ for all $a, b \in D_6$
   (c) $\overline{a} = 6/a$ for all $a \in D_6$
   is a Boolean algrebra.

   The element 1 of D_6 is the "zero" element of D_6 since it satisfies the identity and compliments properties for this Boolean algebra. That is "zero" $= a \cdot \overline{a} = gcd(a, 6/a) = 1$ and $a +$ "zero" $= a + 1 = lcm(a, 1) = a$ for all $a \in D_6$.

Discussion

The set $B = \{0, 1\}$, together with the Boolean operations defined earlier, is the simplest example of a Boolean algebra, but there are many others, some of which do not involve Boolean operations on the set $\{0, 1\}$, at least overtly. The examples above exhibits six examples of abstract Boolean algebras, including $\{0, 1\}$ and the Boolean algebra of Boolean functions discussed in the lectures on Boolean Functions and their Representations.

Let us examine example 3 a bit closer. The set $BOOL(2)$ is the set of all Boolean functions of degree 2. In the lecture notes *Boolean Functions* we determined there were 16 different Boolean functions of degree 2. In fact, in an exercise following this observation you created a table representing all 16 Boolean functions of degree 2. Notice $BOOL(2)$ is the set of the 16 functions represented by this table.

EXERCISE 3.2.1. *Write a table representing all the elements of $BOOL(2)$ and name the elements (functions) $F_1, F_2, F_3, \ldots, F_{16}$.*

(a) Find $F_3 + F_4$, $F_3 \cdot F_4$, and $\overline{F_3}$ (your answers will depend on how you labeled your functions).
(b) Which of the functions is the 0 element of the abstract Boolean algebra?
(c) Which of the functions is the 1 element of the abstract Boolean algebra?

The following table gives some of the identity elements, 0 and 1, of the Boolean algebras given in the previous examples of abstract Boolean algebras.

EXERCISE 3.2.2. *Fill in the rest of the information in the table.*

Boolean Algebra	*0 element*	*1 element*	*an element that is neither 0 nor 1*
B	*0*	*1*	*none*
B^5	*?*	$(1,1,1,1,1)$	$(1,0,0,0,0)$
$FUN(\{a,b,c\},\{0,1\})$	$\chi_\emptyset$	*?*	$f:\{a,b,c\}\to B$ *defined by* $f(a)=0, f(b)=1, f(c)=1$
$P(S)$	*?*	S	*?*
D_6	*1*	*?*	*?*

The function $\chi_A : S \to B$, where A a subset of S is called the *characteristic function of* A and is defined by $\chi_A(x) = 1$ if $x \in A$, and $\chi_A(x) = 0$ if $x \in S - A$. (χ is the lower case Greek letter "chi".)

Here is another important example that we discussed in some detail in MAD 2104.

EXAMPLE 3.2.7. *Let $\mathcal{B}$ be a nonempty set of propositions satisfying the conditions:*

(1) if p is in $\mathcal{B}$, then so is $\neg p$, and
(2) if p and q are in $\mathcal{B}$, then so are $p \vee q$ and $p \wedge q$.

Then $\mathcal{B}$ together with the operations $\vee$ (for $+$), $\wedge$ (for $\cdot$), and $\neg$ (for $^-$) is a Boolean algebra.

PROOF. Since $\mathcal{B} \neq \emptyset$, $\mathcal{B}$ contains a proposition p. By (1), $\neg p$ is also in $\mathcal{B}$. By (2), $\mathcal{B}$ contains the tautology $p \vee \neg p = \mathbf{1}$ and the contradiction $p \wedge \neg p = \mathbf{0}$. The remaining properties were established in the materials covered in MAD 2104. □

As these examples illustrate, the names for addition and multiplication in a particular Boolean algebra may be idiomatic to that example. Addition may be called *sum*, *union*, *join*, or *disjunction*; whereas, multiplication may be called *product*, *intersection*, *meet*, or *conjunction*. Because the addition and multiplication operations in a Boolean algebra behave so differently from addition and multiplication in the more familiar algebraic systems, such as the integers or real numbers, alternative notation, such as $\vee$ for $+$ and $\wedge$ for $\cdot$, are often used instead. At the risk of creating confusion we shall use $+$ and $\cdot$ when working in an abstract Boolean algebra, but, when working with a particular example, such as the one above, we will use conventional notation associated with that example.

3.3. Duality.

DEFINITION 3.3.1 (**Duality**). *Notice how the axioms of an abstract Boolean algebra in the definition of a Boolean algebra have been grouped in pairs. It is possible to get either axiom in a pair from the other by interchanging the operations* $+$ *and* $\cdot$ *, and interchanging the elements* 0 *and* 1*. This is called the* **principle of duality***. As a consequence, any property of a Boolean algebra has a dual property (which is also true) obtained by performing these interchanges.*

3.4. More Properties of a Boolean Algebra.

THEOREM 3.4.1 (Properties). *Let* $\mathcal{B}$ *be an abstract Boolean algebra. Then for any* $x, y \in \mathcal{B}$...

(1) *Idempotent Laws:* $x + x = x$ *and* $x \cdot x = x$
(2) *Domination Laws:* $x + 1 = 1$ *and* $x \cdot 0 = 0$
(3) *Absorption Laws:* $(x \cdot y) + x = x$ *and* $(x + y) \cdot x = x$
(4) $x + y = 1$ *and* $x \cdot y = 0$ *if and only if* $y = \overline{x}$
(5) *Double Complements Law:* $\overline{\overline{x}} = x$
(6) *DeMorgan's Laws:* $\overline{x \cdot y} = \overline{x} + \overline{y}$ *and* $\overline{x + y} = \overline{x} \cdot \overline{y}$

Discussion

The properties in Theorem 3.4.1 are all consequences of the axioms of a Boolean algebra. When proving any property of an abstract Boolean algebra, we may only use the axioms and previously proven results. In particular, we may *not* assume we are working in any one particular example of a Boolean algebra, such as the Boolean algebra $\{0, 1\}$. In the following examples and exercises, $x, y, z, ...$ represent elements of an arbitrary Boolean algebra $\mathcal{B}$. Notice that these arbitrary elements may or *may not* be the zero or one elements of the Boolean algebra.

EXAMPLE 3.4.1. *For any x in $\mathcal{B}$, $0 + x = x$ and $1 \cdot x = x$.*

PROOF. These follow directly from the Identity Laws and the Commutative Laws. Notice that the second property is the dual of the first. $\square$

3.5. Proof of Idempotent Laws.

PROOF OF FIRST IDEMPOTENT LAW. Let $\mathcal{B}$ be a Boolean algebra and let $x \in \mathcal{B}$.

$$
\begin{array}{lll}
x + x & = (x + x) \cdot 1 & \text{Identity Law} \\
 & = (x + x) \cdot (x + \overline{x}) & \text{Compliments Law} \\
 & = x + (x \cdot \overline{x}) & \text{Distributive Law} \\
 & = x + 0 & \text{Compliments Law} \\
 & = x & \text{Identity Law}
\end{array}
$$

$\square$

Discussion

EXERCISE 3.5.1. *Interpret the Idempotent Laws for the Boolean algebra $P(S)$ of subsets of a set S (Example 5).*

EXERCISE 3.5.2. *Prove the other Idempotent Law, for any x in $\mathcal{B}$, $x \cdot x = x$, in two ways: (a) using the principle of duality, and (b) directly (without invoking the duality principle).*

3.6. Proof of Dominance Laws.

PROOF OF THE THE DOMINANCE LAW $x + 1 = 1$. Let $\mathcal{B}$ be a Boolean algebra and let $x \in \mathcal{B}$.

$$
\begin{array}{lll}
x + 1 & = (x + 1) \cdot 1 & \text{Identity Law} \\
 & = (x + 1) \cdot (x + \overline{x}) & \text{Compliments Law} \\
 & = x + 1 \cdot \overline{x} & \text{Distributive Law} \\
 & = x + \overline{x} & \text{Identity Law} \\
 & = 1 & \text{Compliments Law}
\end{array}
$$

$\square$

Discussion

One of the Dominance Laws, Property 2 of Theorem 3.4.1, is proved above. This "Dominance Law" may look a little peculiar, since there is no counterpart in the algebra of the integers or real numbers. It is, however, a familiar property of the Boolean algebra $P(S)$ of subsets of a set S. It merely says that $A \cup S = S$ for every subset A of S.

Exercise 3.6.1. *Prove the other Dominance Law (Theorem 3.4.1 Property 2), $x \cdot 0 = 0$ for every x in $\mathcal{B}$, in two ways: (a) using the principle of duality, and (b) directly (without invoking the duality principle).*

Exercise 3.6.2. *Prove the Absorption Laws (Theorem 3.4.1 Property 3): $(x \cdot y) + x = x$ and $(x + y) \cdot x = x$ for all x, y in $\mathcal{B}$. [Hint: Use Property 2.]*

Exercise 3.6.3. *Interpret the Absorption Laws for the Boolean algebra $P(S)$ of subsets of a set S (Example 5).*

3.7. Proof of Theorem 3.4.1 Property 4.

3.7. Proof of Theorem 3.4.1 Property 4. Recall Theorem 3.4.1 Property 4: For all x and y in $\mathcal{B}$, $x + y = 1$ and $x \cdot y = 0$ if and only if $y = \overline{x}$.

Proof of Theorem 3.4.1 Property 4. Let $x, y \in \mathcal{B}$ and suppose that $x + y = 1$ and $x \cdot y = 0$. Then,

$$\begin{aligned}
y &= y \cdot 1 && \text{Identity Law} \\
&= y \cdot (x + \overline{x}) && \text{Compliments Law} \\
&= y \cdot x + y \cdot \overline{x} && \text{Distributive Law} \\
&= 0 + y \cdot \overline{x} && \text{Hypothesis} \\
&= y \cdot \overline{x} && \text{Identity Law}
\end{aligned}$$

On the other hand

$$\begin{aligned}
\overline{x} &= \overline{x} \cdot 1 && \text{Identity Law} \\
&= \overline{x} \cdot (x + y) && \text{Hypothesis} \\
&= \overline{x} \cdot x + \overline{x} \cdot y && \text{Distributive Law} \\
&= x \cdot \overline{x} + y \cdot \overline{x} && \text{Commutative Law} \\
&= 0 + y \cdot \overline{x} && \text{Compliments Law} \\
&= y \cdot \overline{x} && \text{Identity Law}
\end{aligned}$$

Thus, $y = y \cdot \overline{x} = \overline{x}$. □

Discussion

One direction of the "if and only if" statement of Property 4 Theorem 3.4.1 is just a restatement of the Compliments Laws; hence, we need only prove that if $u + v = 1$ and $u \cdot v = 0$, then $v = \overline{u}$. Since $u \cdot \overline{u} = 0$ and $u \cdot v = 0$, it is tempting to take the resulting equation $u \cdot \overline{u} = u \cdot v$ and simply "cancel" the u from each side to conclude that $\overline{u} = v$. However, **there is no cancellation law for multiplication**

(or addition) in a Boolean algebra as there is in the algebra of the integers or the real numbers. Thus, we must be a little more clever in constructing a proof.

EXERCISE 3.7.1. *Give an example of a Boolean algebra* $\mathcal{B}$ *and elements* x, y, z *in* $\mathcal{B}$ *such that* $x + z = y + z$*, but* $x \neq y$*.*

Property 4 shows that the complement of an element u in a Boolean algebra is the *unique* element that satisfies the Compliments Laws relative to u. Such uniqueness results can provide very powerful strategies for showing that two elements in a Boolean algebra are equal. Here is another example of uniqueness, this time of the additive identity element 0.

THEOREM 3.7.1. *Suppose* u *is an element of a Boolean algebra* $\mathcal{B}$ *such that* $x+u = x$ *for all* x *in* $\mathcal{B}$*. Then* $u = 0$*.*

PROOF. Since $x + u = x$ for all x in $\mathcal{B}$, $0 + u = 0$. But $0 + u = u + 0 = u$ by the Commutative and Identity Laws; hence, $u = 0$. ☐

EXERCISE 3.7.2. *Suppose* v *is an element of a Boolean algebra* $\mathcal{B}$ *such that* $x \cdot v = x$ *for all* x *in* $\mathcal{B}$*. Prove that* $v = 1$*.*

EXERCISE 3.7.3. *Prove that* $\overline{1} = 0$ *and* $\overline{0} = 1$*. [Hint: Use Theorem 3.4.1 Property 4 and duality.]*

EXERCISE 3.7.4. *Prove the Double Complements Law:* $\overline{\overline{x}} = x$*.*

3.8. Proof of DeMorgan's Law. Recall one of DeMorgan's Laws: $\overline{xy} = \overline{x} + \overline{y}$ for all x, y in a Boolean algebra, $\mathcal{B}$.

PROOF. Let $x, y \in \mathcal{B}$.

$$\begin{aligned} xy + (\overline{x} + \overline{y}) &= [x + (\overline{x} + \overline{y})][y + (\overline{x} + \overline{y})] \\ &= [(x + \overline{x}) + \overline{y}][(y + \overline{y}) + \overline{x}] \\ &= (1 + \overline{y})(1 + \overline{x}) \\ &= 1 \cdot 1 \\ &= 1 \end{aligned}$$

$$\begin{aligned} (xy)(\overline{x} + \overline{y}) &= (xy)\overline{x} + (xy)\overline{y} \\ &= (x\overline{x})y + x(y\overline{y}) \\ &= 0 \cdot y + x \cdot 0 \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

Now apply Property 4 with $u = xy$ and $v = \overline{x} + \overline{y}$ to conclude that $\overline{x} + \overline{y} = \overline{xy}$. ☐

Discussion

As in ordinary algebra we may drop the $\cdot$ and indicate multiplication by juxtaposition when there is no chance for confusion. We adopt this convention in the previous proof, wherein we give the steps in the proof of one of DeMorgan's Laws. The proof invokes the uniqueness property of complements, Property 4 in Theorem 3.4.1, by showing that $\overline{x} + \overline{y}$ behaves like the complement of xy.

EXERCISE 3.8.1. *Give reasons for each of the steps in the proof of the DeMorgan's Law proven above. (Some steps may use more than one property.)*

EXERCISE 3.8.2. *Prove the other DeMorgan's Law,* $\overline{x+y} = \overline{x}\,\overline{y}$ *using the principle of duality.*

EXERCISE 3.8.3. *Prove the other DeMorgan's Law,* $\overline{x+y} = \overline{x}\,\overline{y}$ *directly (without invoking the duality principle).*

Notice. One of the morals from DeMorgan's Laws is that you must be careful to distinguish between $\overline{x \cdot y}$ and $\overline{x} \cdot \overline{y}$ (or between $\overline{xy}$ and $\overline{x}\,\overline{y}$), since they may represent different elements in the Boolean algebra.

3.9. Isomorphism.

DEFINITION 3.9.1. *Two Boolean algebras B_1 and B_2 are* **isomorphic** *if there is a bijection $f\colon B_1 \to B_2$ that preserves Boolean operations. That is, for all x and y in B_1,*

(1) $f(x+y) = f(x) + f(y)$,
(2) $f(x \cdot y) = f(x) \cdot f(y)$, *and*
(3) $f(\overline{x}) = \overline{f(x)}$.

The bijection f is called an **isomorphism** *between B_1 and B_2.*

Discussion

The adjective *isomorphic* was used earlier to describe two graphs that are the *same* in the sense that they share all of the same graph invariants. A graph *isomorphism* was defined to be a one-to-one correspondence (bijection) between the vertices of two (simple) graphs that preserves incidence. The terms isomorphic and isomorphism are used throughout mathematics to describe two mathematical systems are essentially the *same*.

EXAMPLE 3.9.1. *Let B be the Boolean algebra $\{0,1\}$, and let $P(S)$ be the Boolean algebra of subsets of the set $S = \{a\}$ (having just one element). Prove that B and $P(S)$ are isomorphic.*

PROOF. $P(S) = \{\emptyset, S\}$ has exactly two elements as does B. Thus, there are two bijections from B to $P(S)$. Only one of these, however, is an isomorphism of Boolean algebras, namely, the bijection $f\colon B \to P(S)$ defined by $f(0) = \emptyset$ and $f(1) = S$. We can check that the three properties of an isomorphism hold by using tables to check all possible cases:

x	$f(x)$	$\overline{x}$	$f(\overline{x})$	$\overline{f(x)}$
0	$\emptyset$	1	S	S
1	S	0	$\emptyset$	$\emptyset$

x	y	$f(x)$	$f(y)$	$x+y$	$x \cdot y$	$f(x+y)$	$f(x) \cup f(y)$	$f(x \cdot y)$	$f(x) \cap f(y)$
0	0	$\emptyset$	$\emptyset$	0	0	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
0	1	$\emptyset$	S	1	0	S	S	$\emptyset$	$\emptyset$
1	0	S	$\emptyset$	1	0	S	S	$\emptyset$	$\emptyset$
1	1	S	S	1	1	S	S	S	S

$\square$

EXERCISE 3.9.1. *Given B and $P(S)$ as in Example 3.9.1, show that the bijection $g\colon B \to P(S)$ defined by $g(0) = S$ and $g(1) = \emptyset$ does not define an isomorphism.*

3.10. Atoms.

DEFINITION 3.10.1. *An element a in a Boolean algebra B is called an* **atom** *if*

(1) $a \neq 0$, and
(2) for every x in B, either $ax = a$ or $ax = 0$.

THEOREM 3.10.1. *A nonzero element a in a Boolean algebra B is an atom if and only if for every $x, y \in B$ with $a = x+y$ we must have $a = x$ or $a = y$. In otherwords, a is* **indecomposable**.

Discussion

The method of exhausting all possible cases used in Example 3.9.1 to prove that a given bijection is an isomorphism is clearly not feasible for Boolean algebras that contain very many elements. The concept of an **atom** can be used to simplify the problem considerably. Atoms are in some sense *minimal* nonzero elements of a Boolean algebra, and, in the case of a finite Boolean algebra, they *generate* the algebra; that is, every nonzero element of the algebra can be written as a (finite) sum of atoms.

EXAMPLE 3.10.1. *Let* $B^2 = \{(0,0),(0,1),(1,0),(1,1)\}$ *be the Boolean algebra described in Example 2 with* $k = 2$. *The elements* $(0,1)$ *and* $(1,0)$ *are the atoms of* B^2. *(Why?) Notice that the only other nonzero element is* $(1,1)$, *and* $(1,1) = (0,1)+(1,0)$.

EXERCISE 3.10.1. *Let* $B^n = \{(x_1, x_2, ..., x_n)|x_i = 0 \text{ or } 1\}$ *be the Boolean algebra described in Example 2.*

(a) *Show that the atoms of* B^n *are precisely the elements*

$$a_i = (0,0,...,0,\underset{\substack{\uparrow \\ i^{th}\ coordinate}}{1},0,...,0),$$

$i = 1,2,...,n$. [Hint: Show (i) each a_i is an atom, and (ii) if $x \in B^n$ has two nonzero coordinates, then x is not an atom.]

(b) *Show that every nonzero element of* B^n *is a sum of atoms.*

PROOF OF THEOREM 3.10.1. Let $a \in B$.

First we show

$$\{\forall u \in B[(au = 0) \wedge (au = a)]\} \Rightarrow \{\forall x, y \in B[(a = x + y) \rightarrow ((a = x) \vee (a = y))]\}.$$

Assume a is such that $au = 0$ or $au = a$ for all $u \in B$ and let $x, y \in B$ be such that $x + y = a$. Then

$$\begin{aligned} ax = \;& x \cdot x + yx \\ &= x + yx \\ &= x(1 + y) \\ &= x \cdot 1 \\ &= x \end{aligned}$$

But by our assumption, $ax = 0$ or $ax = a$, so $x = 0$ or $x = a$. If $x = 0$ then we would have $y = a$ proving $\forall x, y \in B[(a = x + y) \rightarrow ((a = x) \vee (a = y))]$

We now will show

$$\{\forall x, y \in B[(a = x + y) \rightarrow ((a = x) \vee (a = y))]\} \Rightarrow \{\forall u \in B[(au = 0) \wedge (au = a)]\}.$$

Assume a is such that $\forall x, y \in B[(a = x+y) \rightarrow ((a = x) \vee (a = y))]$ and let $u \in B$. Then

$$\begin{aligned} au + a\overline{u} &= a(u + \overline{u}) \\ &= a \cdot 1 \\ &= a \end{aligned}$$

Thus $au = a$ or $a\overline{u} = a$. Suppose $a\overline{u} = a$. Then

$$\begin{aligned} au &= (a\overline{u})u \\ & a(\overline{u} \cdot u) \\ & a \cdot 0 \\ & 0 \end{aligned}$$

□

3.11. Theorem 3.11.1.

THEOREM 3.11.1. *If a and b are atoms in a Boolean algebra $\mathcal{B}$, then either $a = b$ or $ab = 0$.*

Discussion

Theorem 3.11.1 gives a property of atoms that we will find very useful. It says that, in some sense, atoms in a Boolean algebra are *disjoint*. When applied to the example $P(S)$ of subsets of a set S, this is precisely what it is saying.

EXERCISE 3.11.1. *Prove Theorem 3.11.1. [Hint: Use the definition to prove the logically equivalent statement: If $ab \neq 0$, then $a = b$.]*

3.12. Theorem 3.12.1.

THEOREM 3.12.1. *Suppose that an element x in a Boolean algebra $\mathcal{B}$ can be expressed as a sum of distinct atoms $a_1, ..., a_m$. Then $a_1, ..., a_m$ are unique except for their order.*

Discussion

Theorem 3.12.1 provides the rather strong result that an element of a Boolean algebra cannot be expressed as a sum of atoms in more than one way, except by reordering the summands. In particular, it shows that *each individual atom is indecomposable* in the sense that it cannot be written as a sum of two or more atoms in a nontrivial way.

PROOF OF THEOREM 3.12.1. Suppose x can be expressed as sums

$$x = a_1 + a_2 + \cdots + a_m = b_1 + b_2 + \cdots + b_n,$$

where each a_i and each b_j is an atom of $\mathcal{B}$, the a_i's are distinct, and the b_j's are distinct. Then, by the Distributive Law, for each $i = 1, ..., m$,

$$\begin{aligned} a_i x &= a_i(a_1 + a_2 + \cdots + a_m) &&= a_i(b_1 + b_2 + \cdots + b_n) \\ &= a_i a_1 + a_i a_2 + \cdots a_i a_m &&= a_i b_1 + a_i b_2 + \cdots + a_i b_n. \end{aligned}$$

By Theorem 3.11.1, $a_ia_j = 0$, if $i \neq j$, so that

$$a_ia_1 + a_ia_2 + \cdots a_ia_m = a_ia_i = a_i.$$

If $a_i \neq b_j$ for all j, then, again by Theorem 3.11.1, $a_ib_j = 0$ for all j, so that $a_ib_1 + a_ib_2 + \cdots + a_ib_n = 0$. This is not possible, however, since $a_i \neq 0$ and $a_i = a_ib_1 + a_ib_2 + \cdots + a_ib_n$. Thus, $a_i = b_j$ for some j.

By interchanging the roles of the a's and the b's, the same argument shows that for each j, $b_j = a_i$ for some i. Thus, $m = n$, and the sets $\{a_1, ..., a_m\}$ and $\{b_1, ..., b_m\}$ are equal.

□

3.13. Basis.

Theorem 3.13.1. *Suppose $\mathcal{B}$ is a finite Boolean algebra. Then there is a set of atoms $\mathcal{A} = \{a_1, a_2, ..., a_k\}$ in $\mathcal{B}$ such that every nonzero element of $\mathcal{B}$ can be expressed uniquely as a sum of elements of $\mathcal{A}$ (up to the order of the summands).*

Definition 3.13.1. *Given a Boolean algebra $\mathcal{B}$, a set $\mathcal{A}$ of atoms of $\mathcal{B}$ is called a* **basis** *if every nonzero element of $\mathcal{B}$ can be written as a finite sum of atoms in $\mathcal{A}$.*

Discussion

Theorem 3.13.1 shows that every **finite** Boolean algebra has a basis, as defined above. The finiteness condition is necessary as the following exercise makes clear.

Exercise 3.13.1. *Let $\mathbb{Z}$ denote the set of integers. Prove:*

(a) The atoms of $P(\mathbb{Z})$ are the sets $\{n\}$ for $n \in \mathbb{Z}$.
(b) $P(\mathbb{Z})$ does not contain a basis.

Proof of Theorem 3.13.1. Suppose $\mathcal{B} = \{x_1, x_2, ..., x_m\}$, where the x_i's are distinct. As in *Representing Boolean Functions*, define a **minterm** in the x_i's as a product $y_1y_2 \cdots y_m$, where each y_i is either x_i or $\overline{x_i}$. Using the Compliments Law, $x + \overline{x} = 1$, one can prove, by mathematical induction, that the sum of all possible minterms is 1:

$$\sum_{y_i = x_i \text{ or } y_i = \overline{x_i}} y_1y_2 \cdots y_m = 1.$$

(See Exercise 3.13.2.)

If a minterm $y_1y_2 \cdots y_m$ is not 0, then it must be an atom:

- $x_i(y_1y_2\cdots y_m) = y_1y_2\cdots(x_iy_i)\cdots y_m = 0$, if $y_i = \overline{x_i}$, and
- $x_i(y_1y_2\cdots y_m) = y_1y_2\cdots(x_iy_i)\cdots y_m = y_1y_2\cdots y_m$, if $y_i = x_i$.

Thus, for any i,

$$x_i = x_i \cdot 1 = x_i \cdot \sum_{y_i = x_i \text{ or } y_i = \overline{x_i}} y_1y_2\cdots y_m = \sum_{y_i = x_i \text{ or } y_i = \overline{x_i}} x_i(y_1y_2\cdots y_m).$$

As observed above, each product $x_i(y_1y_2\cdots y_m)$ is either 0 or is equal to the minterm $y_1y_2\cdots y_m$ itself. Thus, if $x_i \neq 0$, then x_i is a sum of nonzero minterms; hence, a sum of atoms. Thus, we have shown that each nonzero minterm in the x_i's is an atom and each nonzero element of $\mathcal{B}$ is a sum of nonzero minterms.

The theorem is now proved by letting $\mathcal{A} = \{a_1, a_2, ..., a_k\}$ be the set of all nonzero minterms in the x_i's. Every nonzero element of $\mathcal{B}$ can be expressed as a sum of elements of $\mathcal{A}$, and the uniqueness of this representation follows from Theorem 3.12.1.

$\square$

EXERCISE 3.13.2. *Use mathematical induction to prove that if $x_1, x_2, ..., x_r$ are arbitrary elements of a Boolean algebra $\mathcal{B}$, then the sum of all minterms $y_1y_2\cdots y_r$ in the x_i's is equal to 1. [Hint: Notice that the terms in the sum of all minterms*

$$\sum_{y_i = x_i \text{ or } y_i = \overline{x_i}} y_1y_2\cdots y_r$$

fall into two classes, those for which $y_1 = x_1$ and those for which $y_1 = \overline{x_1}$.]

EXERCISE 3.13.3. *Suppose $I_n = \{1, 2, ..., n\}$. Show that the set $\{\{1\}, \{2\}, ..., \{n\}\}$ is a basis for the Boolean algebra $P(I_n)$ of subsets of I_n.*

3.14. Theorem 3.14.1.

THEOREM 3.14.1. *Suppose that $\mathcal{B}$ is a finite Boolean algebra having a basis consisting of n elements. Then $\mathcal{B}$ is isomorphic to the Boolean algebra $P(I_n)$ of subsets of $I_n = \{1, 2, ..., n\}$.*

Discussion

Theorem 3.14.1, together with Theorem 3.13.1, provides the main characterization of finite Boolean algebras. Putting these two theorems together, we see that every finite Boolean algebra has a basis and, hence, is isomorphic to the Boolean algebra, $P(I_n)$, of subsets of the set $I_n = \{1, 2, ..., n\}$ for some positive integer n. This characterization puts a severe constraint on the number of elements in a finite Boolean algebra, since the Boolean algebra $P(I_n)$ has 2^n elements.

PROOF OF THEOREM 3.14.1. Let $\{a_1, a_2, ..., a_n\}$ be the basis for $\mathcal{B}$. Recall that in the Boolean algebra $P(I_n)$, "addition" is union, $\cup$, "multiplication" is intersection, $\cap$, and "complementation" is set-theoretic complementation, $^{-}$.

A nonempty subset J of I_n determines an element of $\mathcal{B}$ by taking the sum of the atoms of $\mathcal{B}$ having indices in the set J. For example, if $J = \{1, 3, 5\}$, then we get the element

$$x = a_1 + a_3 + a_5$$

of $\mathcal{B}$. In general, we can denote the element of $\mathcal{B}$ determined by an arbitrary subset J of I_n by

$$x = \sum_{i \in J} a_i,$$

provided we adopt the convention that the "empty sum" adds to 0:

$$\sum_{i \in \emptyset} a_i = 0.$$

Define an isomorphism

$$f \colon \mathcal{B} \to P(I_n)$$

as follows: Given a subset J of I_n, and an element

$$x = \sum_{i \in J} a_i$$

of $\mathcal{B}$, set

$$f(x) = J.$$

f is well-defined, since, by Theorem 3.13.1, each element of $\mathcal{B}$ can be expressed uniquely as a sum of atoms. (By the convention, this now includes 0.) f has an inverse

$$g \colon P(I_n) \to \mathcal{B}$$

defined by

$$g(J) = \sum_{i \in J} a_i.$$

Thus, f is a bijection, since it has an inverse. In order to see that f is an isomorphism, we must show that f preserves sums, products, and complements.

Two key observations are that if J and K are subsets of I_n, then

$$\sum_{j \in J} a_j + \sum_{k \in K} a_k = \sum_{i \in J \cup K} a_i$$

and

$$\left(\sum_{j \in J} a_j\right) \cdot \left(\sum_{k \in K} a_k\right) = \sum_{i \in J \cap K} a_i.$$

The first follows from the Idempotent Law $x + x = x$, since, in the left-hand sum, if $i \in J \cap K$, then, after combining like terms, we get the summand $a_i + a_i = a_i$. That is, after simplifying using the Idempotent Law, we get a term a_i for each i in $J \cup K$, and no others.

The second follows from the Idempotent Law $x \cdot x = x$ and Theorem 3.11.1. After using the Distributive and Associative Laws, the left-hand side is a sum of terms $a_j a_k$, where j is in J and k is in K. Since the a_j's are atoms, Theorem 3.11.1 says that the only nonzero terms are terms in which $j = k$. This only occurs when $j = k \in J \cap K$, and, in this case, $a_j a_j = a_j$.

Thus, if $x = \sum_{j \in J} a_j$, $y = \sum_{k \in K} a_k$ are arbitrary elements of $\mathcal{B}$, then

$$x + y = \sum_{i \in J \cup K} a_i \quad \text{and} \quad xy = \sum_{i \in J \cap K} a_i,$$

so that

$$f(x + y) = J \cup K = f(x) \cup f(y) \quad \text{and} \quad f(xy) = J \cap K = f(x) \cap f(y).$$

In order to see that f preserves complements, we need one further observation: If $x = \sum_{j \in J} a_j$, and if $\overline{J}$ is the complement of J in I_n, then

$$\overline{x} = \sum_{j' \in \overline{J}} a_{j'}.$$

For example, if $n = 5$ and $x = a_1 + a_4$, then $\overline{x} = a_2 + a_3 + a_5$. This follows from Property 4 in Theorem 3.4.1: After using the Distributive Law, the terms in the product

$$\left(\sum_{j \in J} a_j \right) \cdot \left(\sum_{j' \in \overline{J}} a_{j'} \right)$$

are each of the form $a_j a_{j'}$, where j is in J and j' in $\overline{J}$. Since J and $\overline{J}$ are disjoint, $j \neq j'$ for any such term, and so, by Theorem 3.11.1, the product $a_j a_{j'} = 0$. That is,

$$\left(\sum_{j \in J} a_j \right) \cdot \left(\sum_{j' \in \overline{J}} a_{j'} \right) = 0.$$

On the other hand, we have already shown in the proof of Theorem 3.13.1 (and Exercise 3.13.2) that the sum of all of the atoms is 1, so that

$$\left(\sum_{j \in J} a_j \right) + \left(\sum_{j' \in \overline{J}} a_{j'} \right) = \sum_{i \in J \cup \overline{J}} a_i = \sum_{i \in I_n} a_i = a_1 + a_2 + \cdots + a_n = 1.$$

Property 4, Theorem 3.4.1, now guarantees that if $x = \sum_{j \in J} a_j$, then

$$\overline{x} = \sum_{j' \in \overline{J}} a_i,$$

and so

$$f(\overline{x}) = \overline{J} = \overline{f(x)}.$$

$\square$

Corollary 3.14.1.1. *Suppose that $\mathcal{B}_1$ and $\mathcal{B}_2$ are finite Boolean algebras having bases of the same size. Then $\mathcal{B}_1$ and $\mathcal{B}_2$ are isomorphic.*

Exercise 3.14.1. *Show that if $\mathcal{B}$ is a finite Boolean algebra, then $\mathcal{B}$ is isomorphic to B^n for some positive integer n.*