On the Structure of Finite Boolean Algebra

Delin Tan, Ph.D. †

Abstract

Boolean algebra has very important applications in computer digital design. In this paper, we have investigated the structure of general finite Boolean Algebra and proved that the size of a Boolean Algebra is 2^n for some positive integer n and two finite Boolean Algebras are isomorphic if and only if they have the same size.

Introduction to Boolean Algebra

Boolean algebraic structure was firstly introduced by George Boole in 1854 [1]. The following definition was proposed by Edward V. Huntington [2]. Let B be a set having two operators + and · satisfying the following conditions:

1. B is commutative under operators + and ·, i.e.

   $\forall x, y \in B, x+ y= y+x$ and $x\cdot y= y\cdot x$.
2. B is associative under operators + and ·, i.e.

   $\forall x, y, z\in B, (x+ y) + z = x+(y+ z)$ and $(x\cdot y)\cdot z = x\cdot(y\cdot z)$.
3. B has identity elements 0 with respect to +, i.e. $\forall x\in B, x+ 0 = x$.

   B has identity elements 1 with respect to ·, i.e. $\forall x\in B, x\cdot 1 = x$.
4. Operator · is distributive over operator +, i.e.

   $\forall x, y, z \in B, x\cdot(y + z)= x\cdot y + x\cdot z$.

   Operator + is distributive over operator ·, i.e.

   $\forall x, y, z \in B, x+ (y\cdot z)= (x+ y)\cdot(x + z)$.
5. $\forall x\in B, \exists x'\in B$ (called the complementary element of x) such that

   $x+ x'=1$ and $x\cdot x'=0$.

then {B, +, ·} is called a Boolean Algebra.

Notes:

1. The following properties can be derived from the above definitions

   Property 1: $\forall x\in B,\ x + x = x$.

   Property 2: $\forall x\in B,\ x\cdot x = x$.

   Property 3: $\forall x\in B,\ x + 1 = 1$.

   Property 4: $\forall x\in B,\ x\cdot 0 = 0$.

   Property 5: $\forall x\in B,\ x'$ is unique and $(x')' = x$.

   Property 6: $\forall x, y\in B,\ (x + y)' = x'\cdot y'$.

   Property 7: $\forall x ,y\in B,\ (x\cdot y)' = x' + y'$.

   Property 8: $\forall x, y\in B,\ x + x\cdot y = x$.

   Property 9: $\forall x ,y\in B,\ x\cdot(x + y) = x$.

   The detail proofs can be found in [3].
2. There are no inverse operators for both + and · in a Boolean Algebra,
3. Let B_1, B_2 be two Boolean algebras. If there exists a 1-1 mapping ϕ from B_1 onto B_2 such that ϕ keeps operations, i.e. $\forall x, y \in B_1$,

$$\phi(x+y) = \phi(x) + \phi(y),\ \phi(x \cdot y) = \phi(x) \cdot \phi(y), \text{ and } \phi(x') = [\phi(x)]',$$

then B_1 is called isomorphic to B_2, ϕ is called an isomorphism from B_1 to B_2.

Examples:

1. Let B be a two elements set {true, false}. Let the operator + be the logic operator OR and operator $\cdot$ be the logic operator AND. The {B, OR, AND} is a Boolean Algebra.
2. Let B be the set of all subsets of a set U. Let the operator + be the set operator union $\cup$ and operator $\cdot$ be the set operator intersection $\cap$. Then {B, $\cup$, $\cap$} is a Boolean Algebra.

Some Lemmas

Definition of minimal element:

Let B be a Boolean Algebra and let e be a non-zero element of B. If $\forall x \in$ B and $x \neq 1$ and $x \neq e$, we always have $x \cdot e = 0$, then e is called a minimal element of B.
Note: A Boolean Algebra may have more than one minimal elements.

Lemma 1: If e is a minimal element of Boolean algebra B, then $\forall x \in$ B,

either $x \cdot e = 0$ or $x \cdot e = e$.

This is because if $x \cdot e \neq 0$, then either $x=1$ or $x=e$, therefore $x \cdot e = e$.

Definition of partial relation <:

Let x, y be two distinct non-zero elements of a Boolean Algebra B. If $x \cdot y = x$, then we say $x<y$ or x is smaller than y.
Note: Two elements of a Boolean algebra may not have smaller relation < at all.

Lemma 2: Let $x<y<z$ be three elements of a Boolean algebra, then $x<z$.
Proof: If $x = z$, then $x = x \cdot y = z \cdot y = y$. It is a contradiction to $x<y$. So we have $x \neq z$. Moreover, $x = x \cdot y = x \cdot (y \cdot z) = (x \cdot y) \cdot z = x \cdot z$. Therefore we have $x < z$.

Lemma 3: Let B be a finite Boolean algebra, then minimal element exists.
Proof: If the size of B is 2, then 1 is a minimal element. Now assume the size of B>2, so there exists an element x of B such that $x \neq 1, 0$. If x is not a minimal element of B, then there exists an element y of B such that $x \cdot y \neq x$ and $x \cdot y \neq 0$. Define $x_2 = x \cdot y$. Because $x_2 \neq x$ and $x \cdot x_2 = x \cdot (x \cdot y) = (x \cdot x) \cdot y = x \cdot y = x_2$, we get $x_2 < x$. If x_2 is not minimal, we can use the same way to find $x_3 \neq 0$ such that $x_3 < x_2$. If x_3 is not minimal, then we can continue to find smaller element x_4. If each step cannot yield a minimal element, we always can find a new smaller element by the above construction. From lemma 2, those constructed elements are all different. However, the size of B is finite; the above constructing procedure must be end after finite steps and yield a minimal element.
Note:

1. If the size of B is 2, then 1 is its only one minimal element.

2. If size of B > 2, then we have an element $x \neq 1, 0$. From the above proof, we can find a minimal element a small than x. However, we also can find another minimal element b smaller than x'. Then

$$a \cdot b = (a \cdot x) \cdot (b \cdot x') = 0.$$

So a and b are different and the count of minimal elements is ≥2.

Lemma 4: Let B be a finite Boolean algebra and $e_1, e_2, e_3, \ldots, e_n$ be all its minimal elements, then $e_1 + e_2 + e_3 + \ldots + e_n = 1$.
Proof: If the size of B is 2, then 1 is its only one minimal element and the theorem holds. If the size of B>2, then $n \geq 2$. Let $y = e_1 + e_2 + e_3 + \ldots + e_n$. If $y \neq 1$, then $y' \neq 0$. From the proof of Lemma 3, there exists a minimal element $x < y'$. If $x = e_k$ for some k ($1 \leq k \leq n$) , then

$$e_k = e_k \cdot e_k = e_k \cdot x = e_k \cdot (x \cdot y') = e_k \cdot x \cdot (e_1 + e_2 + \ldots + e_n)' = e_k \cdot x \cdot (e_1' \cdot e_2' \cdot \ldots \cdot e_n') = 0.$$

This is a contradiction to the definition of the minimal element. Therefore we have $e_1 + e_2 + e_3 + \ldots + e_n = 1$.

Lemma 5: Let B be a finite Boolean algebra and let $e_1, e_2, e_3, \ldots, e_n$ be all minimal elements of B. Then every element x of B has a unique linear expression

$$x = c_1 \cdot e_1 + c_2 \cdot e_2 + c_3 \cdot e_3 + \ldots + c_n \cdot e_n,$$

where either $c_k = 0$ or $c_k = 1$ for each k ($1 \leq k \leq n$).
Therefore any element of B is a unique sum of several minimal elements.
Proof: Let $e_1, e_2, e_3, \ldots, e_n$ be all minimal elements of B. Then from Lemma 4
$\forall x \in B,\ x = x \cdot 1 = x \cdot (e_1 + e_2 + e_3 + \ldots + e_n) = x \cdot e_1 + x \cdot e_2 + x \cdot e_3 + \ldots + x \cdot e_n.$
From Lemma 1, $x \cdot e_k = 0$ or $x \cdot e_k = e_k$ for each k ($1 \leq k \leq n$). So x is a sum of several minimal elements and has expression

$$x = c_1 \cdot e_1 + c_2 \cdot e_2 + c_3 \cdot e_3 + \ldots + c_n \cdot e_n.$$

where $c_k = 0$ or $c_k = 1$ for each k ($1 \leq k \leq n$).
If x has another expression

$$x = d_1 \cdot e_1 + d_2 \cdot e_2 + d_3 \cdot e_3 + \ldots + d_n \cdot e_n.$$

where either $d_k = 0$ or $d_k = 1$ each k ($1 \leq k \leq n$).
Then $\quad c_1 \cdot e_1 + c_2 \cdot e_2 + c_3 \cdot e_3 + \ldots + c_n \cdot e_n = d_1 \cdot e_1 + d_2 \cdot e_2 + d_3 \cdot e_3 + \ldots + d_n \cdot e_n.$
For each k ($1 \leq k \leq n$),

$$e_k \cdot (c_1 \cdot e_1 + c_2 \cdot e_2 + c_3 \cdot e_3 + \ldots + c_n \cdot e_n) = e_k \cdot (d_1 \cdot e_1 + d_2 \cdot e_2 + d_3 \cdot e_3 + \ldots + d_n \cdot e_n).$$

Then we get $\quad c_k \cdot e_k = d_k \cdot e_k$
Because c_k and d_k are either 0 or 1, they must be the same.
Therefore the expression is unique.

Main Theorems

Definition of Boolean Algebra B_n:
Let $n>0$ be an integer. Define set B_n as the set like the following:

$$B_n = \{ (a_1, a_2, a_3, \ldots, a_n) \},$$

where a_k is integer 0 or 1 for each k ($1 \leq k \leq n$).
Define operators +, · and complementary operator ' in B_n as the following:

$\forall x, y \in B_n$, write

$$x = (a_1, a_2, a_3, \ldots, a_n),\ \ y = (b_1, b_2, b_3, \ldots, b_n),$$

Define $x+y = (a_1+b_1, a_2+b_2, a_3+b_3, \ldots, a_n+b_n)$,
where the operation rule for each component is $0 + 0 = 0$, $0 + 1 = 1$, $1 + 1 = 1$.
Define $x \cdot y = (a_1b_1, a_2b_2, a_3b_3, \ldots, a_nb_n)$,
where the operation rule for each component is the regular multiplication
Define $x' = (1 - a_1, 1 - a_2, 1 - a_3, \ldots, 1 - a_n)$,
where the operation rule for each component is the regular subtraction.
Then we can verify that B_n is a Boolean algebra. We omit the detail verification process here.

Now we have our main theorems:
Theorem 1: Every finite Boolean Algebra is isomorphic to a finite Boolean Algebra B_n for some integer $n>0$.
Proof: Let B be a finite Boolean algebra and let $e_1, e_2, e_3, \ldots, e_n$ be its all minimal elements of B. From lemma 5, $\forall x \in B$, x has a unique linear expression

$$x = c_1 \cdot e_1 + c_2 \cdot e_2 + c_3 \cdot e_3 + \ldots + c_n \cdot e_n.$$

where $c_k = 0$ or $c_k = 1$ for each k $(1 \le k \le n)$.
Then define a mapping ϕ: $B \to B_n$ as the following:

$$\phi(x) = (a_1, a_2, a_3, \ldots, a_n)$$

where $a_k = 0$ if $c_k = 0$ and $a_k = 1$ if $c_k = 1$ for each k $(1 \le k \le n)$.
If we accept the elements 1 and 0 in B as integers in B_n, we can simply define

$$\phi(x) = (c_1, c_2, c_3, \ldots, c_n)$$

It is obviously the mapping ϕ is 1-1 and onto.
Moreover, because for each k $(1 \le k \le n)$

$$e_k + 0 = e_k,\ \ e_k + e_k = e_k,\ \ e_k \cdot 0 = e_k,\ \ e_k \cdot e_k = e_k,$$

we can verify that $\forall x, y \in B$

$$\phi(x + y) = \phi(x) + \phi(y) \ \text{ and } \ \phi(x \cdot y) = \phi(x) \cdot \phi(y)$$

This is because the elements on both sides of the equations have exactly the same coordinate expressions.
Also it is easy to verify that

$$\phi(x') = [\phi(x)]',$$

We omit the detail verification steps here too.
Therefore B is isomorphic to B_n for some integer $n>0$

Theorem 2: The size of any finite Boolean Algebra is 2^n for some positive integer n.
Proof: We only need to calculate the size of B_n for integer $n>0$.
There is only one element in B_n having all ones as its component values.
For integer k $(1 \le k \le n)$. there are $\binom{n}{k}$ elements in B_n having k zeros as their component values. Therefore the size of B_n is

$$1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \ldots + \binom{n}{n} = 2^n.$$

Corollary: Two finite Boolean Algebras are isomorphic if and only if they have the same size.

† *Delin Tan, Ph.D.,* Southern University of New Orleans, USA

References

1. Cori, Rene; Lascar, Daniel (2000), Mathematical Logic, Oxford University Press,
2. Huntington, E. V. (1933), "New sets of independent postulates for the algebra of logic", Transactions of the American Mathematical Society 35 (1): 274–304.
3. Mano and Ciletti (2006), Digital Design, Addison Wesley Longman.