Finite Boolean Algebras

Madhav P. Desai

January 9, 2018

1 Introduction

A Boolean algebra over a finite set Ω is defined as follows:

- There are two operations . and $+$, each of which is commutative and associative. Associativity and commutativity imply that expressions such as $a+b+c+d$ or $a.b.c.d$ (without parentheses) make sense.
- There exist elements 0 and 1 in Ω such that, for all $x \in \Omega$,

$$\begin{aligned} (0+x) &= x \\ (1.x) &= x \end{aligned}$$

- If $x \in \Omega$, there exists a $y \in \Omega$, such that

$$\begin{aligned} (x+y) &= 1 \\ (x.y) &= 0 \end{aligned}$$

  Such a y is called a complement of x.

- The operation . distributes over $+$, and the operation $+$ distributes over .. That is, for any $a, b, c \in \Omega$,

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

The Boolean algebra is then denoted by

$$\mathbf{B} = \{\Omega, ., +, 0, 1\}$$

Elements of Ω will be called elements of $\mathbf{B}$ (for convenience).

2 Some additional properties (Theorems) that can be derived from the base axioms

Several simple consequences of the axioms can be derived.

1. For each $a \in \Omega$, there is a unique complement. To prove this, assume the contrary, that is a has two distinct complements x and y. Then

$$x = x.1 = x.(a+y) = x.a + x.y = 0 + x.y = x.y$$
$$y = y.1 = y.(a+x) = y.a + y.x = 0 + y.x = y.x = x.y$$

   resulting in a contradiction of the assumption that $x \neq y$. Thus a has a unique complement, denoted by $\overline{a}$ or $\sim a$.

2. If $a \in \Omega$, the $a.a = a$ and $a + a = a$. We prove the first part:

$$a.a = a.a + 0 = a.a + a.\overline{a} = a.(a + \overline{a}) = a.1 = a$$

   This means + and . operators are idempotent.

3. If $a \in \Omega$, then $a + 1 = 1$ and $a.0 = 0$. To prove the first part:

$$a + 1 = a + (a + \overline{a}) = (a + a) + \overline{a} = a + \overline{a} = 1$$

4. If $a, b \in \Omega$, then $a + \overline{a}.b = a + b$. To see this

$$a + \overline{a}.b = (a + \overline{a}).(a + b) = 1.(a + b) = a + b$$

5. If $a, b, c \in \Omega$, then $a.c + \overline{a}.b = a.c + \overline{a}.b + b.c$. To see this

$$\begin{aligned} a.c + \overline{a}.b &= (a.c + \overline{a}).(a.c + b) \\ &= ((a + \overline{a}).(c + \overline{a})).(a.c + b) \\ &= 1.(\overline{a} + c).(a.c + b) \\ &= \overline{a}.b + a.c + b.c \end{aligned}$$

   This last identity is called the consensus identity, and $b.c$ is called the consensus term generated out of $\overline{a}.b$ and $a.c$.

6. If $a, b \in \Omega$, then

$$\begin{aligned} \overline{a+b} &= \overline{a}.\overline{b} \\ \overline{a.b} &= \overline{a}+\overline{b} \end{aligned}$$

   To prove the first equality, we see that

$$(a+b)+\overline{a}.\overline{b} = (a+b+\overline{a}).(a+b+\overline{b}) = (1+b).(1+a) = 1$$
$$(a+b).\overline{a}.\overline{b} = a.\overline{a}.b.\overline{b} = 0$$

   Thus, $\overline{a}.\overline{b}$ is the complement of $(a+b)$. These two identities are termed *DeMorgan's laws*.

3 An ordering of elements in a Boolean algebra

If $a, b \in \Omega$, we say that $a \leq b$ if and only if $a.b = a$. This induces an ordering which is reflexive ($a \leq a$) and transitive ($a \leq b$ and $b \leq c$ implies that $a \leq c$).

We prove a couple of useful results

1. $a \leq b$ if and only if $a+b = b$. To prove the if part, assume that $a+b = b$. Then $a.b = a.(a+b)$. But

$$a.(a+b) = a.a + a.b = a + a.b = a.(1+b) = a.1 = a$$

   Thus $a.b = a$ and $a \leq b$. Conversely, if $a.b = a$ then

$$a+b = a.b+b = b.(a+1) = b.1 = b$$

   thus completing the proof.

2. We say that $a < b$ if $a \leq b$ and $a \neq b$.

3. If $a \leq b$, $a \neq b$, then $\overline{a}.b \neq 0$. To prove this, assume that $\overline{a}.b = 0$. Then

$$\begin{aligned} a &= a+0 \\ &= a+\overline{a}.b \\ &= a+b \\ &= b \end{aligned}$$

   which is a contradiction.

4 Every finite Boolean algebra is isomorphic to a finite set algebra

A finite power-set algebra can be constructed as follows: Take the power set 2^U of a finite universe set U. The elements of the power set are closed under the commutative and associative union $(+)$ and intersection $(.)$ operations. Union and intersection distribute over each other. The complement of an element in 2^U is also in 2^U. The empty set and the set U provide the identities for the union (0) and intersection (1) operations respectively. Thus, a power-set algebra is a Boolean algebra.

The converse is also true. That is, every finite Boolean algebra can be viewed as a power-set algebra. We prove this statement.

We say that $a \in \mathbf{B}$, $a \neq 0$ is a *minimal* element under $\leq$ if $x \leq a$ and $x \neq 0$ implies that $x = a$. Such a minimal element is called an *atom*. Clearly, a finite Boolean algebra will have a finite non-empty set of minimal atoms (why?). Note that if $a \leq b$ and $a \leq c$, then $a \leq b.c$, and if $a \leq b.c$, then $a \leq b$ and $a \leq c$.

Now, let $A = \{a_1, a_2, \ldots a_k\}$ be the set of atoms in $\mathbf{B}$. Then for any $x \in \mathbf{B}$, let A_x be

$$A_x \ = \ \{u \in A \text{ s.t. } u \leq x\}$$

Then A_x is non-empty for each $x \in \mathbf{B}$ (why?). Let

$$u_x \ = \ \sum_{a \in A_x} a$$

Clearly, $u_x \leq x$. We claim that $u_x = x$. Assume not. Then, since $u_x \leq x$ and $u_x \neq x$, as we noted above, it follows that $\overline{u_x}.x \neq 0$. Therefore there is some atom $a \leq \overline{u_x}.x$, so that $a \leq \overline{u_x}$ and $a.\overline{u_x} = a$. This atom a cannot be in A_x, because if it were, then $a.\overline{u_x} = 0$. This leads to a contradiction. Thus, $u_x = x$. We have shown that every element in $\mathbf{B}$ can be written as a sum of atoms.

It is easy to show that a sum of atoms is uniquely determined by the atoms that figure in that sum. For, if $a \neq b$ are two distinct atoms, then $a.b = 0$, and consequently, if

$$a_1 + a_2 + \ldots a_k \ = \ b_1 + b_2 + \ldots b_m$$

for atoms $a_1, a_2, \ldots a_k$ (mutually distinct), $b_1, b_2, \ldots, b_m$ (mutually distinct), then $m = k$ and each a_i is equal to some b_j. Thus, there is a one-one correspondence between subsets of the set of atoms and the elements of $\mathbf{B}$.

Finally, the addition of sums of subsets of atoms is equivalent to addition of the union of the subsets, and the . operation on subset sums is the same as the intersection of the subsets.

This completes the proof. Thus in the finite case, every element of the Boolean algebra can be identified as a subset of some universe set and can be represented by a 0/1 vector whose size is the number of elements in the universe set.

5 Problem set

Show the following (starting from the axioms of a Boolean algebra):

1. The 0 and 1 elements in a Boolean algebra are unique.
2. $a.0 = 0$ for each element a.
3. $a + 1 = 1$ for each element a.
4. For each element a, $a + a = a$, and $a.a = a$.
5. Prove the second De Morgan law:
$$\overline{a.b} \quad = \quad \overline{a} + \overline{b}$$
6. In a finite Boolean algebra with at least two elements, $0 \neq 1$.
7. In a finite Boolean algebra with at least two elements, the set of atoms is non-empty.
8. In a finite Boolean algebra with at least two elements, for every $x \neq 0$ there is at least one atom $a \leq x$.
9. If $a \leq b$ and $c \leq b$, then $(a + c) \leq b$.
10. If $a \leq b$ then $\overline{b} \leq \overline{a}$.
11. If $a \leq b$ and $a \leq c$, then $a \leq b.c$.
12. Prove that $\overline{a}.b + a.b = b$.
13. Prove that
$$a.\overline{b}.c + a.\overline{b}.\overline{c} + \overline{a}.\overline{b} = \overline{b}$$
(note: starting from the axioms).