Boolean Algebra

Boolean algebras arise in a number of different ways.

Power Set of a Set

Given a set S, we have certain algebraic operations on subsets of S. These are:

- $A \cap B$ is the collection of all elements of S that are in A as well as B. It is called the intersection of the two subsets.
- $A \cup B$ is the collection of all elements of S that are either in A or in B. It is called the union of the two subsets.
- A^c is the collection of all elements of S that are not in A. It is called the complement of the set A
- $A \setminus B$ is the collection of all elements of S that are in A but not in B. This is called the difference of A from B.

There are some natural relations between these operations. For example,

- $(A \cup B) = (A^c \cap B^c)^c$
- $(A \setminus B) = A \cap B^c$

Thus, all the operations can be defined in terms of $\cap$ and $()^c$. Moreover, we have relations like the following among these operations.

- $(A \cap B) \cap C = A \cap (B \cap C)$
- $A \cap A^c = S^c = \phi$, where ϕ denotes the empty set.
- $A \cap S = A$
- $(A^c)^c = A$

If we use $\mathcal{P}(S)$ to denote the collection of subsets of S, then these operations put an algebraic structure on $\mathcal{P}(S)$ which makes it a "Boolean algebra".

Basic set-theory is all about finding out which identities are true in this Boolean algebra. In high-school, we learned to do these using Venn diagrams. This is not too difficult for identities involving 2 or 3 sets but becomes much more complicated after that. Hence, we will look at a different approach below.

Propositional Logic

Propositional logic deals with "propositions" (also called "statements" or "assertions"). These are statements that have definite true or false values. For example:

- This is lecture hall 6

- We are studying MTH102

- It is cold in January in Mohali

We will denote propositions by capital letters of the Roman alphabet. Propositions can be combined to produce new propositions.

- $A \wedge B$ represents the combination A 'and' B. This proposition is only true when *both* A and B are true.

- $A \vee B$ represents the combination A 'or' B. This proposition is true whenever *either* or both of A and B are true.

- $\neg A$ represents the negation of A ('not' A). It is true exactly when A is false.

These are the basic operations of "Propositional Calculus". We have some natural properties of these operations:

- $A \wedge A = A = A \vee A$.

- $\neg(A \wedge B) = (\neg A) \vee (\neg B)$.

- $\neg(\neg A) = A$.

Further, if we use 0 for 'false' and 1 for 'true', then we have some more identities:

- $A \wedge (\neg A) = 0$.

- $A \vee (\neg A) = 1$.

- $A \wedge (B \wedge C) = (A \wedge B) \wedge C$.

- $A \vee (B \vee C) = (A \vee B) \vee C$.

- $A \vee B = (B \vee A)$.

- $A \wedge B = (B \wedge A)$.

- $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$.

We note the similarity of these identities with those for the subsets of a set. In fact, if we replace $\wedge$ with $\cap$, $\vee$ with $\cup$ and taking complements with negation, we have *exactly* the same relations as the ones above!

This shows that there is a common algebraic structure to both systems. In the next section, we will see how to understand this similarity conceptually.

In your course (IDC102) on electronics you must have encountered 'nand' gates which are defined by $A \dagger B = \neg(A \wedge B)$. You must have also learned that all other operations can be obtained from this by using the identities:

- $\neg(A) = A \dagger A$

- $A \vee B = (A \dagger A) \dagger (B \dagger B)$

- $A \wedge B = (A \dagger B) \dagger (A \dagger B)$

A construct called "Truth Tables" gives us a good way to check for the possible true/false values for an expression involving propositions A, B, C and so on. We put 0 or 1 as the value for each of the component propositions and look at the value of the combined statement. For this we need the basic table:

A	B	$A \wedge B$	$A \vee B$	$\neg A$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	0

While this is more convenient than Venn diagrams, it is still cumbersome for combining a large number of basic propositions as the number of rows is 2^k when there are k component basic propositions.

Indicator functions

To see the algebraic structure in both cases above more clearly, we will look at them in a slightly different way.

Given a subset A of S. For any element s of S, the statement $s \in A$ is a proposition which can be true or false. Moreover, we see that:

- $(s \in A) \wedge (s \in B)$ is the same as $s \in A \cap B$.
- $(s \in A) \vee (s \in B)$ is the same as $s \in A \cup B$.
- $\neg(s \in A)$ is the same as $s \in A^c$.

We can think of the possible truth values of the proposition $s \in A$ corresponding to different s in S by think of a "variable" s. We are thus led to the `indicator function` of A defined by:

$$\chi_A(s) = \begin{cases} 1 & \text{if } s \in A \\ 0 & \text{if } s \notin A \end{cases}$$

It follows that A is precisely the set of $s \in S$ for which $\chi_A(s) = 1$. Conversely, given a map $f : S \to \{0, 1\}$. The subset A_f of S is defined as the collection of elements s of S for which $f(s) = 1$.

It is clear that $A_{\chi_A} = A$ and $\chi_{A_f} = f$, so this is a natural one-to-one correspondence between functions from S to $\{0, 1\}$ and subsets of S.

We note that the above truth table for propositions has an analogue for the indicator function values:

χ_A	χ_B	$\chi_{A \cap B}$	$\chi_{A \vee B}$	χ_{A^c}
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	0

However, there is a more convenient way of doing this using arithmetic.

- $\chi_{A \cap B} = (\chi_A) \cdot (\chi_B)$
- $\chi_{A^c} = \chi_S - \chi_A$

where the operations on the right-hand side are the usual operations on functions. We note that the function χ_S is identically 1 for all elements of S, so it can also be called the constant function 1. Similarly, the indicator function χ_ϕ of the empty set takes the value 0 for all elements of S and can be considered as the constant function 0.

The usual sum of indicate functions is not an indicator function. Hence, it is convenient to define a new operation $\oplus$ on $\{0, 1\}$ by the relations

$$0 \oplus 0 = 0 = 1 \oplus 1; 0 \oplus 1 = 1 = 1 \oplus 0$$

This can also be seen as addition *modulo* 2. One can check that this addition has the usual properties with respect to multiplication on the set $\{0, 1\}$.

In terms of this operation we see that $\chi_{A^c} = 1 \oplus \chi_A$. Using the above description of the union in terms of complements and intersections, we see that

$$\chi_{A \cup B} = 1 \oplus \chi_{A^c \cap B^c} = 1 \oplus \chi_{A^c} \cdot \chi_{B^c} =$$
$$1 \oplus (1 \oplus \chi_A)(1 \oplus \chi_B) = 1 \oplus 1 \oplus \chi_A \oplus \chi_B \oplus \chi_A \chi_B =$$
$$\chi_A \oplus \chi_B \oplus \chi_A \chi_B$$

Similarly,
$$\chi_{A \setminus B} = \chi_{A \cap B^c} = \chi_A(1 \oplus \chi_B) = \chi_A \oplus \chi_A \chi_B$$
We also note that the following two useful identities hold.

$$\chi_A \oplus \chi_A = 0 \text{ and } \chi_A \cdot \chi_A = \chi_A$$

Using these identifications, any operation involving subsets of S can be converted into an algebraic operation involving the associated indicator functions. This clearly makes calculations involving large numbers of sets easier to write down.

We note that the truth table for $\chi_A \oplus \chi_B$ is:

χ_A	χ_B	$\chi_A \oplus \chi_B$
0	0	0
1	0	1
0	1	1
1	1	0

This table is similar to the truth table for the "exclusive or" operation between propositions (sometimes called "xor") which we can thus denote also by $\oplus$. When P and Q are propositions:

- $P \oplus Q$ represents the combination P 'or' Q but 'not both'.

This can be written as $P \oplus Q = (P \vee Q) \wedge \neg(P \wedge Q)$. Thus if we use the suggestive notation $P \otimes Q$ in place of $P \wedge Q$, then the above rules simplify into the familiar algebraic rules:

- $P \oplus Q = Q \oplus P$.
- $P \otimes Q = Q \otimes P$.
- $P \otimes (Q \oplus R) = P \otimes Q \oplus P \otimes R$.
- $P \oplus 0 = P$
- $P \otimes 1 = P$.
- $P \otimes 0 = 0$.

Along with these familiar rules, we have the slightly unfamiliar rules $P \oplus P = 0$ and $P \otimes P = P$. This again allows us to replace calculations in propositional logic (also called propositional calculus) into algebraic calculations using the rules given above.

The notion of "Boolean Algebra" abstracts these two examples. We can define a Boolean algebra $(\mathcal{B}, \oplus, \otimes)$ as a set $\mathcal{B}$ with two operations $\oplus$ for addition and $\otimes$ for multiplication. Moreover, there are elements 0 and 1 in $\mathcal{B}$ so that all the rules written above for propositions become true with these operations and these elements. In other words, we have the usual rules of addition and multiplication. Moreover, the *special* additional rules are $A \cdot A = A$ and $A + A = 0$; these are what makes the algebra "Boolean".

For all practical purposes, we can think of a Boolean algebra as a sub-collection of $\mathcal{P}(S)$ which is *closed* under taking unions, intersections and complements and contains the set S as well. (Hence, it also contains the empty set which is the complement of S!)

Alternatively, we can think of a Boolean Algebra as a collection of combinations of statements which may turn out to be true or turn out to be false.