Boolean algebra

This note is about Boolean algebras. A formal definition of Boolean algebra was given in the lectures and you can easily find it in textbooks. Let me repeat them with slightly different notation.

1. A Boolean algebra is a set with two binary operations $\vee$ and $\wedge$, one unary operation $\bar{}$, and two (special) elements 0 and 1 such that the following hold for all $x, y, z \in B$.

$$\left.\begin{aligned} x \vee y = y \vee x \\ x \wedge y = y \wedge x \end{aligned}\right\} \text{Commutative laws} \tag{1a}$$

$$\left.\begin{aligned} (x \vee y) \vee z = x \vee (y \vee z) \\ (x \vee y) \vee z = x \vee (y \vee z) \end{aligned}\right\} \text{Associative laws} \tag{1b}$$

$$\left.\begin{aligned} x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \\ x \wedge (y \vee z) = (x \vee y) \wedge (x \vee z) \end{aligned}\right\} \text{Distributive laws} \tag{1c}$$

$$x \vee 0 = x, x \wedge 1 = x \quad \text{Identity laws} \tag{1d}$$

$$x \vee \bar{x} = 1, x \wedge \bar{x} = 0 \quad \text{Complementation laws} \tag{1e}$$

2. Some important things to remember.

   i. The '0' and '1' in the definition of Boolean algebra should not be confused with natural numbers. They are simply members of B with special properties.

   ii. The definition of Boolean algebra uses what is called the *axiomatic* method. Certain relations among the strings are assumed to always hold. These are the axioms of the particular mathematical structure we are dealing with. Pick any undergraduate algebra book and you will see many such structure. The axiomatic method is all-pervasive in mathematics and computer science.

   The axioms are necessary for general mathematical structures. Some need not hold for some structures. For example, matrix multiplication is not commutative in general.

iii. We use the axioms and rules of logic to derive new results called *theorems*. Theorems are certain relations that hold in the particular structure we are dealing with (Boolean algebras in our case). A board game like chess is a good analogy. There is a well-defined starting position—the 'axioms'. Then there are well-defined rules of the game and the legal new positions are the theorems!

Let us prove some theorems of Boolean algebra. Look up the examples of Boolean algebra. The theorems we prove will seem obvious for them. But we have to prove them using the above axioms and rules of logic. Below B will denote an arbitrary Boolean algebra.

1. For all $x \in B$

$$x \vee x = x \text{ and } x \wedge x = x \quad \text{Idempotent laws}$$

Proof. The proof will be in a sequence of steps.
$x = x \vee 0$ Eqn. 1d
$x \vee 0 = x \vee (x \wedge \bar{x})$ Eqn. 1e
$x \vee (x \wedge \bar{x}) = (x \vee x) \wedge (x \vee \bar{x})$ Eqn. 1c
$(x \vee x) \wedge (x \vee \bar{x}) = (x \vee x) \wedge 1 = x \vee x$ Eqn. 1e and 1d

We are done! The second equation can be proved similarly starting with $x = x \wedge 1 = x \wedge (x \vee \bar{x})$.

2. In a Boolean algebra B the special elements 0 and 1 are unique. For all $x \in B$, its complement $\bar{x}$ is the unique element satisfying $x \vee \bar{x} = 1$ and $x \wedge \bar{x} = 0$.

Proof. By definition 0 and 1 have special properties $x \vee 0 = x$ and $x \wedge 1 = x$. The uniqueness result says that in fact these are the only elements satisfying these properties. Let us take 0 first suppose another element say $0'$ which has the property that for all $x \in B$, $x \vee 0' = x$. Then

$$\begin{aligned} 0 \vee 0' &= 0 \quad \text{from the assumption on } 0' \\ 0' \vee 0 &= 0' \quad \text{from the identity laws} \end{aligned}$$

Since from the commutative laws the left sides are equal $0 = 0'$. You can prove uniqueness of 1 similarly. Now let us prove the uniqueness of the complement $\bar{x}$. Fix $x \in B$ and suppose there is some x' such that $x \vee x' = 1$ and $x \wedge x' = 0$. Then

$$\begin{aligned} \bar{x} \wedge (x \vee x') &= \bar{x} \wedge 1 = \bar{x} \quad \text{Identity laws} \\ \bar{x} \wedge (x \vee x') &= (\bar{x} \wedge x) \vee (\bar{x} \wedge x') \quad \text{Dist. laws} \\ &= 0 \vee (\bar{x} \wedge x') = (\bar{x} \wedge x') \quad \text{Comp. laws and Id. laws} \end{aligned}$$

So $\bar{x} = x\bar{x} \wedge x'$. Now by definition $x \vee \bar{x} = 1$. So we can interchange x' and $\bar{x}$ in the line of reasoning given above and get $x' = x' \wedge \bar{x}$. It follows that $x' = \bar{x}$.

3. From the uniqueness of the complement it follows that: $\bar{0} = 1$ and $\bar{1} = 0$. Also for any x, $\bar{\bar{x}} = x$, taking complement twice we recover the original element.

4. $x \vee 1 = 1$ and $x \wedge 0 = 0$

   Proof.

$$
\begin{aligned}
x \vee 1 &= x \vee (x \vee \bar{x}) && \text{Comp. laws} \\
&= (x \vee x) \vee \bar{x} && \text{Assoc. laws} \\
&= x \vee \bar{x} = 1 && \text{Idempotent and Comp. laws}
\end{aligned}
$$

   Note that we used the idempotent laws which we first proved as a theorem. This is perfectly legitimate—you can use any theorem you have already proved just like axioms. This method is often used in mathematics and computer science. You prove 'smaller' theorems (often called *lemmas*) to prove a 'big' theorem. Try proving the second result: $x \wedge 0 = 0$.

5. For all $x, y \in B$, $\overline{x \vee y} = \bar{x} \wedge \bar{y}$ and $\overline{x \wedge y} = \bar{x} \vee \bar{y}$. These are called De Morgan's laws.

   Proof. We will use the uniqueness theorem for complements. So if we set $x \vee y = z$ we have to show that $(\bar{x} \wedge \bar{y}) \vee z = 1$ and $(\bar{x} \wedge \bar{y}) \wedge z = 0$. We have

$$
\begin{aligned}
(\bar{x} \wedge \bar{y}) \vee z &= (\bar{x} \vee z) \wedge (\bar{y} \vee z) \\
&= (\bar{x} \vee (x \vee y)) \wedge (\bar{y} \vee (x \vee y)) \\
&= ((\bar{x} \vee x) \vee y) \wedge ((\bar{y} \vee y) \vee x) \\
&= (1 \vee y) \wedge (1 \vee x) \\
&= 1 \wedge 1 = 1
\end{aligned}
$$

   In the first line we used dist. laws, second line is just the definition of z and the third line used both associative and commutative laws. In the last but one line we use the theorem preceding this one. Try proving the second equation.

We have seen some basic theorems of Boolean algebra. These are quite useful and can be used to prove more complex theorems. Manas Patra