Proving that the Boolean Algebra forms a vector space

Bernardo Meurer

September 27, 2016

1 Defining the Boolean algebra

We define a Boolean algebra as a set of B elements $a, b, \ldots$ which satisfies the following axioms[1]:

1. B has two binary operators $\wedge$ or $\cdot$ (logical AND) and $\vee$ or $+$ (logical OR)
2. Idempotence
    - $a \wedge a = a \vee a = a$
3. Commutative law
    - $a \wedge b = b \wedge a$
    - $a \vee b = b \vee a$
4. Associative law
    - $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
    - $a \vee (b \vee c) = (a \vee b) \vee c$
5. Absorption law
    - $a \wedge (a \vee b) = a \vee (a \wedge b) = a$
6. Mutual distributiveness
    - $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
    - $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
7. B contains universal bounds $\emptyset$ (empty set) and I (universal set)
    - $\emptyset \wedge a = \emptyset$
    - $\emptyset \vee a = a$
    - $I \wedge a = a$
    - $I \vee a = I$
8. B has a unary operator $a \to a'$ such that
    - $a \wedge a' = \emptyset$
    - $a \vee a' = I$

If the truth values a, b are interpreted as integers $0, 1$ our operators can be expressed with ordinary arithmetic, or by minimum/maximum functions [2]:

1. $a \wedge b = a \times b = \min(a, b)$
2. $a \vee b = a + b - (a \times b) = \max(a, b)$
3. $\neg a$ or $\bar{a} = 1 - a$

We may also express $a \wedge b$, $a \vee b$, and $\neg a$ with a truth table

a	b	$a \wedge b$	$a \vee b$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

Table 1: Truth table for binary operators

a	$\neg a$
0	1
1	0

Table 2: Truth table for unary operator

2 Defining a field

We define a field as a triple $(F, +, \cdot)$ where F is a set, and $+$, $\cdot$ are binary operators that act on F, called addition and multiplication respectively, satisfying the following axioms[3]:

1. Addition $(+)$ is an associative operation on F
   - $\forall f, g, h \in F : f + (g + h) = (f + g) + h$
2. There is an identity element for addition
   - $\forall f \in F : f + \nu = f$
   - The identity ν is unique and we will denote it by 0
3. Every element x of F is invertible for $+$
   - The additive inverse of x is unique, and will be denoted by $-x$
4. Multiplication $(\cdot)$ is a commutative operation on F
   - $\forall f, g \in F : f \cdot g = g \cdot f$
5. There is an identity element for multiplication
   - $\forall f \in F : f \cdot \upsilon = f$
   - The identity υ is unique and we will denote it by 1
6. Every element x of F except 0 is invertible for $\cdot$
   - The multiplicative inverse of x is unique, we will denote it by x^{-1}
   - We do not assume 0 to be neither invertible nor non-invertible
7. Multiplication is distributive in regards to addition
   - $\forall x, y, z \in F : x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
8. The identities for addition and multiplication are distinct

- $0 \neq 1$

One might note that the commutativity of addition is not listed as an axiom, this is due to the fact that said property can be obtained from the other axioms

Theorem (Commutativity of addition)**.** *Let F be any field, then $+$ is a commutative operation on F.*

$$\forall f, g \in F : f + g = g + f$$

Proof. [4]

Let x, y be elements of F, from axiom 4. we have

$$(1 + x) \cdot (1 + y) = (1 + y) \cdot (1 + x)$$

Using axiom 7

$$((1 + x) \cdot 1) + ((1 + x) \cdot y) = ((1 + y) \cdot 1) + ((1 + y) \cdot x)$$

Axiom 5 gives us that 1 is the multiplicative identity

$$(1 + x) + ((1 + x) \cdot y) = (1 + y) + ((1 + y) \cdot x)$$

Using axiom 1

$$1 + (x + ((1 + x) \cdot y)) = 1 + (y + ((1 + y) \cdot x))$$

By means of axiom 3 we have the law of cancellation which yields

$$x + ((1 + x) \cdot y) = y + ((1 + y) \cdot x)$$

Using axiom 7

$$x + ((1 \cdot y) + (x \cdot y)) = y + ((1 \cdot x) + (y \cdot x))$$

With axioms 1, 4, and 5

$$x + y + (x \cdot y) = y + x + (x \cdot y)$$

Finally by axiom 3

$$x + y = y + x$$

□

3 Boolean algebra as a field

foobar

4 Fields as vector spaces

barfoo

5 Boolean algebra as a vector space

foobar

References

[1] Eric W. Weisstein. Boolean algebra. `http://mathworld.wolfram.com/BooleanAlgebra.html`.

[2] Boolean algebra. `https://en.wikipedia.org/wiki/Boolean_algebra`.

[3] Ray Mayer. The field axioms. `http://people.reed.edu/~mayer/math112.html/html1/node16.html`.

[4] Leonard Eugene Dickson. Definition of a group and a field by independent postulates. *Transactions of the American Mathematical Society*, pages 6:198–204, 1905.