Boolean Algebras

Sajjad
Department of Computer Science
Swansea University

December 08, 2008
Main Topic

- Boolean Rings.
- Boolean Algebras.
- Fields of Sets.
- Elementary Relations.
Definition

A ring is a set $R$ together two binary operations $+$, and $\cdot$ defined on $R$ such that:

- $R$ with addition is an abelian group.
- Multiplication is an associative.
- Left and right distributive laws hold i.e., for all $a, b, c$ belongs to $R$.

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{and} \quad (a + b) \cdot c = (a \cdot b) + (b \cdot c)$$
Definition

A Boolean ring \( R \) is a ring (with multiplicative identity) for which \( p = p^2 \), for all \( p \) in \( R \); that is, \( R \) consists only of idempotent elements.

OR

A Boolean ring \( R \) is a ring with unit in which every element is idempotent.

Ring with unit means a ring with multiplicative identity 1 which is different from additive identity 0, and hence every Boolean ring contains 0 and 1.
The set $2^X$, of all functions from an arbitrary non-empty set $X$ into 2 (here we denote the set of integers of modulo 2 by ordinary integer 2). Let $f$ be a function which maps elements of $X$ into integer modulo 2, that is, $Z_2 = 0’, 1’$, where $0’$ represents all those elements whose reminder after dividing by 2 is 0. Similarly $1’$, represents all those elements whose reminder after dividing by 2 is 1. This means 0 and 1 in $2^X$, are functions defined point wise, for each $x$ in $X$, by

$0(x) = 0’$ and $1(x) = 1’$

Now we define the set $2^X$, as the set of all those functions $f$ from arbitrary set $X$ into 2, i.e. $2^X = f : X \rightarrow Z_2$
If $p$ and $q$ (remember both are functions from $X$ into $Z_2$) belongs to $2^X$, then $(p + q)$ and $pq$ are defined by,

$$(p + q) \cdot (x) = p(x) + q(x)$$

and

$$(p \cdot q)(x) = p(x) \cdot q(x),$$

for all $x$ in $X$.

The right sides of these equations refer to $Z_2$ while left sides refer to $2^X$.

Our task is to show that $2^X$ is a Boolean ring i.e.

- $2^X$ is a ring under point wise addition and multiplication.

**Proof.**

As $2^X$ is a set of function from non empty set $X$ to set of integers of modulo 2, i.e. $Z_2$, while is a ring with point wise addition and multiplication obviously.
$2^X$ has a multiplicative identity.

**Proof.**

Let $1$ a function from $2^X$, then $1(x) = 1'$, $1'$ belong to $Z_2$. So for all $p$ belong to $2^X$

$$(p.1)(x) = p(x).(1) = p(x).1' = p(x)$$

This implies $1$ is a multiplicative identity in $2^X$. 

All the elements of $2^X$ are idempotent.

**Proof.**

Finally we need to show that all the elements of $2^X$ are idempotent i.e $p^2 = p$ for all $p$ in $2^X$.

$L.H.S \cdot p^2 = p \cdot \left( p \cdot x \right) = p(x) \cdot (x) = [p(x)]^2 (1)$

And as $p(x)$ belongs to set of integers modulo 2, $\mathbb{Z}_2 = 0', 1'$

So $p(x)$ on the right hand side of (1) is either $0'$ or $1'$ the square of both is equal to themselves, i.e. if $p(x) = 0'$ then $0'^2 = 0$ similarly if $p(x) = 1'$ then $1'^2 = 1'$.

Hence (1) implies $p^2(x) = [p(x)]^2 = p(x)$ hence all the elements of $2^X$ are idempotent.

Hence Proved that $2^X$ is a Boolean ring.
Boolean rings has characteristics 2, that is \((p + p = 0\) for all \(p\) in \(A\))

**Proof.**

Let \(p\) and \(q\) belongs to a Boolean ring \(A\) then consider
\[
(p + q)^2 = (p + q) \cdot (p + q)
\]
\[
(p + q)^2 = p^2 + p \cdot q + q \cdot p + q^2
\]
As \(A\) is idempotent so \((p + q)^2 = (p + q)\) and \(p^2 = p, q^2 = q\)
Put this in above equation we have:
\[
(p + q) = p + p \cdot q + q \cdot p + q
\]
\[
p \cdot q + q \cdot p = 0
\]
\[
Now\ put\ p = q\ in\ Eq(2),\ we\ get\n\]
\[
p^2 + p^2 = 0\ \text{idempotence implies}\n\]
\[
p + p = 0
\]
Proved
Special Results of Boolean Rings

Boolean ring is commutative.

Proof.

2 implies \( p \cdot q = -q \cdot p \)
and from (3) put \( p = -p \) on the left handside to get
\[
p \cdot q = q \cdot p - - - - - - - - - - - - (4)
\]
Hence \( A \) is a Boolean ring.
Defining Boolean Algebra

Definition

A Boolean algebra is a mathematical structure that is similar to a Boolean ring, but that is defined using the meet and join operators instead of the usual addition and multiplication operators.

Or

A Boolean algebra is a non-empty set $A$ together with two distinct distinguished elements 0 and 1, two binary operations $\land$ and $\lor$ and a unary operation $'$ satisfying the identities of Boolean rings in terms of meet, join, and complement;

Those axioms are the following
Defining Boolean Algebra

1. $(0' = 1), (1' = 0)$
2. $(p \land 0 = 0), (p \lor 1 = 1)$
3. $(p \land 1 = p), (p \lor 0 = p)$
4. $(p \land p' = 0), (p \lor p' = 1)$
5. $(p'' = p)$
6. $(p \land p = p), (p \lor p = p)$
7. $(p \land q)' = p' \lor q', (p \lor q)' = p' \land q'$
8. $(p \land q) = (q \land p), (p \lor q) = (q \lor p)$
9. $p \land (q \land r) = (p \land q) \land r, p \lor (q \lor r) = (p \lor q) \lor r$
10. $p \land (q \lor r) = (p \land q) \lor (p \land r), p \lor (q \land r) = (p \lor q) \land (p \lor r)$
Every Boolean ring is a Boolean algebra, and vice versa. More precisely, we can split it into two parts.

(I) If $R$ is a Boolean ring, for $p$ and $q$ in $R$, then we can define:

1. $p \land q = p \cdot q$
2. $p \lor q = p + q + p \cdot q$
3. $p' = 1 + p$

(II) If $A$ is a Boolean algebra, for $p$ and $q$ in $A$, then we can define:

1. $p \cdot q = p \land q$
2. $p + q = (p \land q') \lor (p' \land q)$
Proof of some axioms of Boolean algebra by given definition of Boolean ring in (I)

Proof.

De Morgan’s law, \((p \land q)' = p' \lor q'\)

\[ p' \lor q' = p' + q' + p'q' \]

\[ = p' + q'(1 + p'), \text{ using def(3) and axiom(5), we get} \]

\[ = p' + 1 + q'p \]

\[ = 1 + p(1 + q') \text{ again using def(3) and axiom(5), we get} \]

\[ = 1 + pq \]

\[ = 1 + (p \land q) \]

\[ = (p \land q)' \text{ Proved} \]
Proof of some axioms of Boolean algebra by given definition of Boolean ring in (I)

Proof.

- Left distributive law, $p \land (q \lor r) = (p \land q) \lor (p \land r)$
  
  $$(p \land q) \lor (p \land r) = (p \cdot q) \lor (p \cdot r)$$
  
  $$= (p \cdot q) + (p \cdot r) + (p \cdot q \cdot p \cdot r)$$
  
  $$= (p \cdot q) + (p \cdot r) + (p \cdot q \cdot r), \text{ Idempotence } p^2 = p$$
  
  $$= p \cdot (q + r + q \cdot r)$$
  
  $$= p \cdot (q \lor r)$$
  
  $$= p \land (q \lor r) \quad \text{Proved}$$

Similarly we can prove all other axioms as well.
Proof of some axioms of Boolean ring by given definition of Boolean algebra $A$ in (II)

Proof.

The distinguished elements 0 and 1 are obvious, here we have proved some other axioms

- Multiplication is associative, i.e. $p \cdot (q \cdot r) = (p \cdot q) \cdot r$

  
  
  $(p \cdot q) \cdot r = p \cdot (q \land r)$

  
  $= p \land (q \land r)$

  
  $= (p \land q) \land r$, Boolean algebra axiom

  
  $= (p \cdot q) \cdot r$

  
  proved
Proof of some axioms of Boolean ring by given definition of Boolean algebra $A$ in (II)

Proof.

- The distinguished elements 0 and 1 are obvious, here we have proved some other axioms

- Idempotence, i.e. for all $p$ in $R$, $p^2 = p$
  
  $p \cdot q = p \land q$, by replacing $q$ by $p$ we get
  
  $p \cdot p = p \land p$
  
  $p^2 = p$
Proof of some axioms of Boolean ring by given definition of Boolean algebra $A$ in (II)

**Proof.**

- The distinguished elements 0 and 1 are obvious, here we have proved some other axioms.

- Idempotence, i.e. for all $p$ in $R$, $p^2 = p$
  \[
  p^2 + q^2 = ((p^2) \land (q^2)') \lor ((p^2)' \land q^2)
  \]
  \[
  = [(p \land p) \land (q \land q)'] \lor [(p \land p)' \land (q \land q)]
  \]
  \[
  = [(p \land p) \land (q \land q)'] \lor [(p \land p)' \land (q \land q)], \text{ by (1)}
  \]
  \[
  = [(p \land q') \lor (p' \land q)]
  = p + q, \quad \text{Proved}
  \]

Similarly can prove other axioms.
Definition

A field of sets is a pair \( \langle X, A \rangle \) where \( X \) is a set and \( A \) is an algebra over \( X \) i.e., a non-empty subset of the power set of \( X \) closed under the intersection and union of pairs of sets and under complements of individual sets.

In other words \( A \) forms a subalgebra of the \( P(X) \), (Boolean algebra). Many authors refer to \( A \) itself as a field of sets.
To form $P(X)$ is not the only natural way to make a Boolean algebra out of a non-empty set $X$. A more general way is to consider an arbitrary non-empty subclass $A$ of $P(X)$ such that if $P$ and $Q$ are in $A$, then $P \cap Q$, $P \cup Q$ and $P'$ are also in $A$. Since $A$ contains at least one element, it follows that $A$ contains $\emptyset$ and $X$, and hence that $A$ is a Boolean algebra. Every Boolean algebra obtained in this way is called a field (of sets).

A subset $P(X)$ of a set $X$ is cofinite (in $X$) if its complement $p'$ is finite. The class $A$ of all those subsets of a non-empty set $X$ that are either finite or cofinite is a field of subsets of $X$. If $X$ itself is finite, then $A$ is simply $P(X)$; if $X$ is infinite, then $A$ is a Boolean algebra.
Example

A subset $P$ of a set $X$ is co-finite (in $X$), if its complement $p'$, is finite. The class $A$ of all those subsets of a non-empty set $X$ that are either finite or co-finite is a field of subsets of $X$. If $X$ itself is finite, then $A$ is simply $P(X)$; if $X$ is infinite, then $A$ is a new Boolean algebra.
Elementry Relations

Here we will discuss some of the elementary relations that hold in Boolean algebra. We just illustrate elementary relations and incidental purpose is to establish some notation that will be used freely throughout the sequel.

For this whole section $p, q, r, \ldots$ are elements of an arbitrary (but fixed) Boolean algebra.
Lemma 1

If \((p \lor q) = p\) for all \(p\) then \(q = 0\), if \((p \land q) = p\) for all \(p\) then \(q = 1\)

Proof.

As we know about elements of Boolean algebra that,
\[p \lor 0 = p\] and \[p \land 1 = p\]

Given that \((p \lor q) = p\)
put here \(p = 0\) and using the Boolean algebra axioms given above we get
\[q = 0\]

Again given that \((p \land q) = p\) here put here \(p = 1\) and using the Boolean algebra axioms given above we get
\[q = 1\], Hence shown
Lemma 2

If $p$ and $q$ are such that $(p \land q) = 0$ and $(p \lor q)$ then $q = p'$

**Proof.**

\[
q = 1q \\
= (p \lor p') \\
= (p \land q) \lor (p' \land q) \\
= 0 \lor (p' \land q) \\
= (p' \land p) \lor (p' \land q) \\
= p' \land (p \lor q) \\
= p' \land 1 \\
= p'
\]

From this lemma we can say, that (2.8) uniquely determines 0 and 1, and (2.9) uniquely determines , or we can say that 0, 1 and complementation are unique.
Lemma 3

For all $p$ and $q$, $p \lor (p \land q) = p$ and $p \land (p \lor q) = p$.

Proof.

$p \lor (p \land q) = (p1) \lor (p \land q)$
$= p \land (1 \land q)$
$= p \land 1$
$= p$

$p \land (p \lor q) = (p \lor p) \land (p \lor q)$
$= (p \lor 0) \land (p \lor q)$
$= (p \lor (0 \land q))$
$= (p \lor 0)$
$= p$

This is called the Laws of absorption.
Often the most concise and intuitive way to state an elementary property of Boolean algebras is to introduce a new operation. Thus, for instance, set-theoretic considerations suggest the operation of subtraction. We write,
\[ p - q = p \land q' \]
The symmetrised version of the difference \( p - q \) is the Boolean sum:
\[ (p - q) \lor (q - p) = p + q \]
As a sample of the sort of easily proved relation that the notation suggests consider the distributive law. One reason why Boolean algebras have something to do with logic is that the familiar sentential connectives and, or, and not have properties similar to the Boolean connectives \( \land \) and \( \lor \) and \( ' \).
Instead of meet, join and complement, the logical terminology uses conjunction, disjunction, and negation motivated by the analogy (resemblance), we now introduce into the study of Boolean algebra the operation suggested by logical implication,

\[ p \implies q = p' \lor q \]

And bi-conditional,

\[ p \iff q = (p \implies q) \land (q \implies p) \]

The source of these operations suggests that it is important to avoid the result of the operation \( \implies \) on the elements \( p \) and \( q \) of the Boolean algebra \( A \) as another element of \( A \); it is not an assertion about or a relation between the given elements \( p \) and \( q \). The same is true for \( \iff \).

That is why logicians refer to read \( p \implies q \) as if \( p \) then \( q \) instead of reading “\( p \) implies \( q \)”. Observe incidentally that if \( \lor \) is read as or, the disjunction \( \lor \) must be interpreted in the non-exclusive sense.
Sheffer Stroke

There is a well-known Boolean operation to be mentioned, called the (Sheffer) Stroke, and it is defined by
\[ p \text{\textbackslash} q = p' \land q' \]
In logical contexts this operation is known as binary rejection (neither \( p \) nor \( q \)).
The chief theoretical application of the Sheffer Stroke is a remark. A single operation, namely the stroke, is enough to define Boolean algebras.
To establish this remark, it is sufficient to show that complement, meet, and join can be expressed in terms of the Stroke, i.e.
\[ p' = p \text{\textbackslash} p \]
\[ p \land q = (p \text{\textbackslash} p) \text{\textbackslash} (q \text{\textbackslash} q) \]
\[ p \lor q = (p \text{\textbackslash} q) \text{\textbackslash} (p \text{\textbackslash} q) \]
Proof of Sheffer Stroke Remark

Proof.

1) \( p \downarrow p = p' \land p' \), by definition
   \[ \land \quad p' \], by axioms of Boolean algebra.

2) \((p \downarrow p) \downarrow (q \downarrow q) = (p' \land p') \downarrow (q' \land q')\), by definition
   \[ \downarrow \quad p' \downarrow q' \], by axioms of Boolean algebra.
   \[ \land \quad p'' \land q'' \], by definition
   \[ \land \quad p \land q \]

3) \((p \downarrow q) \downarrow (p \downarrow q) = (p' \land q') \downarrow (p' \land q')\)
   \[ \land \quad (p' \land q')' \land (p' \land q')', \text{by definition} \]
   \[ \land \quad (p'' \lor q'') \land (p'' \lor q''), \text{by axioms of Boolean algebra} \]
   \[ \land \quad (p \lor q) \land (p \lor q) \]
   \[ \land \quad p \lor q \]
Hence Proved