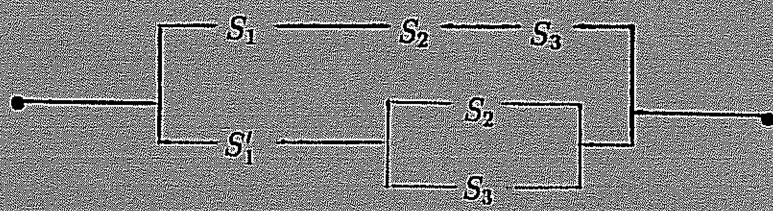
UNE

DEPARTMENT OF MATHEMATICS,
STATISTICS & COMPUTING SCIENCE

Pure Mathematics 200 Level

P	Q	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T



2. BOOLEAN ALGEBRA

The University of New England, Armidale, NSW, 2351

2. BOOLEAN ALGEBRA

This chapter is devoted to the study of *Boolean algebras* and their applications. As we shall see, an algebra of subsets is a prototypical example for any Boolean algebra. Before formally defining a Boolean algebra, it is therefore appropriate to review some basic set theory.

2.1 Set Theory

A **set** is a collection of objects specified by a rule which allows us to decide whether any given object is, or is not, in the set.

We will usually denote sets by capital letters; $A, B, C, \cdots$. The objects comprising a set are its **elements** (or **members**). Elements will normally be denoted by lower case letters; $a, b, c, \cdots$. We will write $a \in A$ to mean a is an element of the set A, and $a \notin A$ to mean a is not an element of A.

Typically the rule specifying a set will take one of two possible forms.

(a) The set is specified by listing all of its elements. For example, the set V of vowels has elements a, e, i, o and u. We indicate this by writing

$$V := \{a, e, i, o, u\}.$$

In general, we will use braces, { }, to indicate that the objects described within them are to be regarded as the elements of a set.

(b) A characteristic property $\mathcal{P}$ is given. For example, $\mathcal{P}$ might be; *is a prime number less than 20*. The set then consists of all those objects with the property $\mathcal{P}$, and only those objects.
We will indicate this by writing

$$\{x : x \text{ has } \mathcal{P}\},$$

read as:

$$\underbrace{\text{The set of}}\ x\ \underbrace{\text{such that}}\ x \text{ has } \mathcal{P}.$$

For example;

$$\begin{aligned} P &:= \{x : x \text{ is a prime less than } 20\} \\ &= \{2, 3, 5, 7, 11, 13, 17, 19\}. \end{aligned}$$

Other examples of sets specified this way are:

$$\begin{aligned} D &:= \{x : x \underset{\text{divides}}{|} 12\} \\ &= \{1, 2, 3, 4, 6, 12\}. \end{aligned}$$

$$S := \{x : \sqrt{x} \in \mathbf{Z}\} = \{0, 1, 4, 9, 16, 25, \cdots\}.$$

$$R := \{x : x^3 - x^2 + x - 1 = 0\}.$$

A useful concept is that of the **null set** (or **empty set**), which has no elements. We will denote the null set by $\emptyset$.

Given two sets A and B we say A is a **subset** of B, written $A \subseteq B$, if every element of A is an element of B. That is, $A \subseteq B$ if and only if $x \in A \Longrightarrow x \in B$. The null set is a subset of every set.

EXERCISE: Let A be a set with n elements. Show that there are 2^n distinct subsets of A.

Two sets A and B are **equal**, written $A = B$, if $A \subseteq B$ and $B \subseteq A$. That is, two sets are equal if and only if every element of each is an element of the other; $x \in A \Longleftrightarrow x \in B$. As a consequence of this we note that the order in which the elements of a set are specified is unimportant.
Thus,

$$\{a, b, c\} = \{b, c, a\}.$$

Also, it is redundant to specify the same element more than once;

$$\{a, a, b\} = \{a, b\}.$$

For the set $R := \{x : x^3 - x^2 + x - 1 = 0\}$, defined above, it is unclear whether we should take $R = \{1, i, -i\}$ or $R = \{1\}$.
In any given discourse only relevant objects need be considered. The set of all such relevant objects forms a **universal set** U for the purpose of the discussion. All sets entering into the discourse will be subsets of U.

For example:

If U is the set of real numbers then $R = \{1\}$.

If U is the set of complex numbers then $R = \{1, i, -i\}$.

If U is the set of Pterosauria, then $R = \emptyset$.

When the appropriate universal set is clearly understood from the context it may not be specified explicitly.

We now define some basic operations on sets.

Given two sets A and B their **union**, written $A \cup B$, is the set of all elements which belong to either A or B. That is,

$$A \cup B := \{x : x \in A \text{ or } x \in B\}.$$

$$S := \{x : \sqrt{x} \in \mathbf{Z}\} = \{0, 1, 4, 9, 16, 25, \cdots\}.$$

$$R := \{x : x^3 - x^2 + x - 1 = 0\}.$$

A useful concept is that of the **null set** (or **empty set**), which has no elements. We will denote the null set by $\emptyset$.

Given two sets A and B we say A is a **subset** of B, written $A \subseteq B$, if every element of A is an element of B. That is, $A \subseteq B$ if and only if $x \in A \Longrightarrow x \in B$. The null set is a subset of every set.

EXERCISE: Let A be a set with n elements. Show that there are 2^n distinct subsets of A.

Two sets A and B are **equal**, written $A = B$, if $A \subseteq B$ and $B \subseteq A$. That is, two sets are equal if and only if every element of each is an element of the other; $x \in A \Longleftrightarrow x \in B$. As a consequence of this we note that the order in which the elements of a set are specified is unimportant.
Thus,

$$\{a, b, c\} = \{b, c, a\}.$$

Also, it is redundant to specify the same element more than once;

$$\{a, a, b\} = \{a, b\}.$$

For the set $R := \{x : x^3 - x^2 + x - 1 = 0\}$, defined above, it is unclear whether we should take $R = \{1, i, -i\}$ or $R = \{1\}$.
In any given discourse only relevant objects need be considered. The set of all such relevant objects forms a **universal set** U for the purpose of the discussion. All sets entering into the discourse will be subsets of U.

For example:

If U is the set of real numbers then $R = \{1\}$.

If U is the set of complex numbers then $R = \{1, i, -i\}$.

If U is the set of Pterosauria, then $R = \emptyset$.

When the appropriate universal set is clearly understood from the context it may not be specified explicitly.

We now define some basic operations on sets.

Given two sets A and B their **union**, written $A \cup B$, is the set of all elements which belong to either A or B. That is,

$$A \cup B := \{x : x \in A \text{ or } x \in B\}.$$

The **intersection** of A and B, written $A \cap B$, is the set of all elements which belong to both A and B. That is,

$$A \cap B := \{x : x \in A \text{ and } x \in B\}.$$

The **complement** of A (relative to the universal set U) is the set of elements in U which do not belong to A. We denote this complement by A'. That is,

$$A' := \{x : x \in U \text{ and } x \notin A\}.$$

The set theoretic identities listed below are typical of the relationships which can be derived from the above definitions.

1) $A \cup B = B \cup A$ and $A \cap B = B \cap A$. [*Commutative laws.*]

2) $A \cup (B \cup C) = (A \cup B) \cup C$
and
$A \cap (B \cap C) = (A \cap B) \cap C$. [*Associative laws*, as a result of which one can unambiguously write $A \cup B \cup C$ and $A \cap B \cap C$.]

3) $A \cup A = A$ and $A \cap A = A$. [*Idempotent laws.*]

4) $A \cup \emptyset = A$ [$\emptyset$ is an *identity* for $\cup$]
and
$A \cap U = A$ [U is an *identity* for $\cap$].

5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
and
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. [*Distributive laws.*]

6) $A \cup A' = U$
and
$A \cap A' = \emptyset$. [*Laws of complements.*]

7) $(A \cup B)' = A' \cap B'$
and
$(A \cap B)' = A' \cup B'$. [*De Morgan's Laws.*]

8) $(A')' = A$.

9) $U' = \emptyset$
and
$\emptyset' = U$.

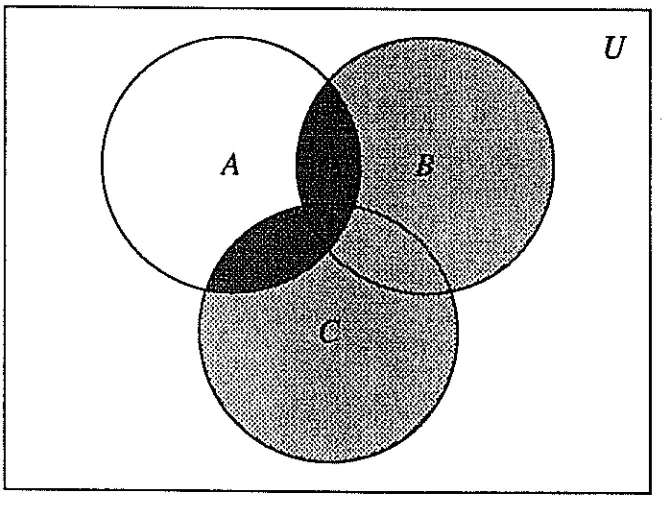
We will prove the first De Morgan law given in 7); proofs of the other identities are left as **exercises**.

Proof that $(A \cup B)' = A' \cap B'$.

$$
\begin{aligned}
x \in (A \cup B)' &\iff x \notin A \cup B \\
&\iff x \notin A \text{ and } x \notin B \\
&\iff x \in A' \text{ and } x \in B' \\
&\iff x \in A' \cap B'.
\end{aligned}
$$

Venn diagrams, in which each set is represented by the interior of a simple closed curve, provide a convenient way of illustrating relations such as those listed above.

For example, the left hand side of the distributive law for $\cap$ over $\cup$; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, is represented in figure 1,



$B \cup C$ corresponds to the whole of the shaded area.
Dark shaded area represents $A \cap (B \cup C)$.
Figure 1.

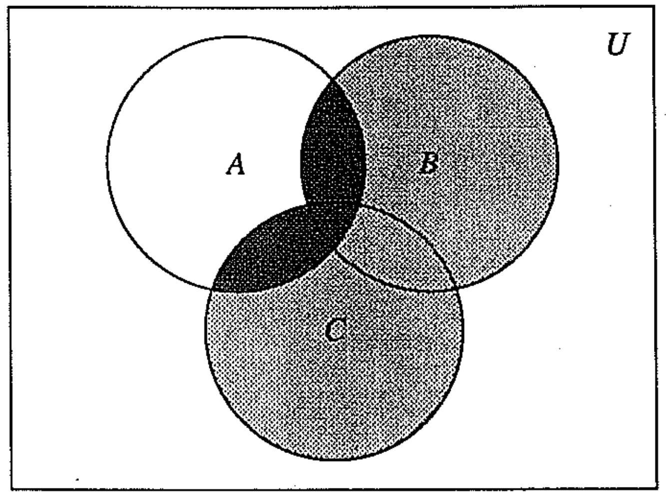
while the right hand side is represented in figure 2.

Proof that $(A \cup B)' = A' \cap B'$.

$$
\begin{aligned}
x \in (A \cup B)' &\iff x \notin A \cup B \\
&\iff x \notin A \text{ and } x \notin B \\
&\iff x \in A' \text{ and } x \in B' \\
&\iff x \in A' \cap B'.
\end{aligned}
$$

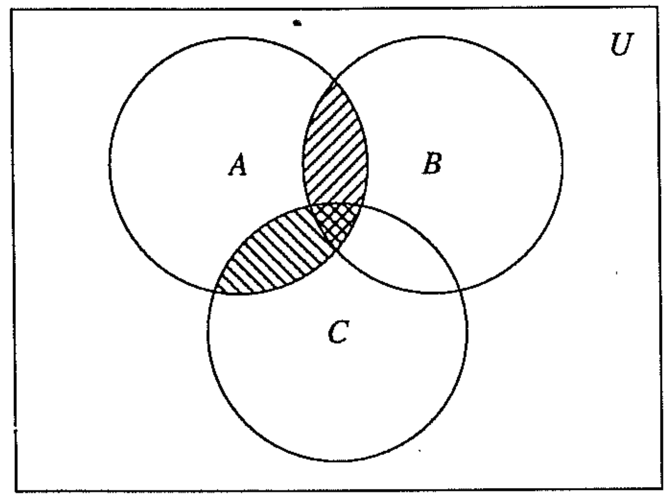
Venn diagrams, in which each set is represented by the interior of a simple closed curve, provide a convenient way of illustrating relations such as those listed above.

For example, the left hand side of the distributive law for $\cap$ over $\cup$; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, is represented in figure 1,



$B \cup C$ corresponds to the whole of the shaded area.
Dark shaded area represents $A \cap (B \cup C)$.
Figure 1.

while the right hand side is represented in figure 2.



Area hatched to the left represents $A \cap B$.
Area hatched to the right represents $A \cap C$.
$(A \cap B) \cup (A \cap C)$ is represented by the total hatched area.
Figure 2.

And, it is visually clear that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

You may find it instructive to similarly analyse each of the identities given above.

NOTE: Venn diagrams for general situations involving four, or more, sets are not quite so pleasant. (Try drawing such a diagram in which all of the fifteen sets $A, B, C, D, A \cap B, A \cap C, A \cap D, B \cap C, B \cap D, C \cap D, A \cap B \cap C, A \cap B \cap D, A \cap C \cap D, B \cap C \cap D, A \cap B \cap C \cap D$ are represented by distinct nonempty regions.)

EXERCISE. Show that $A \subseteq B$ if and only if $A \cap B' = \emptyset$.

2.2 Definition and basic results for Boolean Algebras

A **Boolean algebra** is an abstract system consisting of a set $S = \{a, b, \cdots\}$ on which two *binary operations*; $(a,b) \longmapsto a+b$ and $(a,b) \longmapsto a \cdot b$, and one *unary operation* $a \longmapsto a'$, are defined and satisfy the following axioms:

A1) If $a, b \in S$ then $a+b \in S$, $a \cdot b \in S$ and $a' \in S$. That is, S is *closed* under the operations of $+, \cdot$, and $'$.

A2) $a+b = b+a$ and $a \cdot b = b \cdot a$ for all $a, b \in S$. That is, $+$ and $\cdot$ are *commutative.*

A3) If a, b and c are in S then

(i) $a \cdot (b+c) = a \cdot b \ + \ a \cdot c$

and

(ii) $a + (b \cdot c) = (a+b) \cdot (a+c)$

That is, each of the binary operations is *distributive* over the other.

A4) There exists $0 \in S$ such that for all $a \in S$ we have $0 + a = a$, and there exists $I \in S$ such that for all $a \in S$ we have $I \cdot a = a$. That is, there exist *identities* for $+$ and $\cdot$.

A5) For all $a \in S$ we have $a + a' = I$ and $a \cdot a' = 0$. The *laws of complements.*

At this point you may wish to glance ahead to section 2.3.1 to see some examples of such a system. In particular example 1) should help make the results which follow more transparent. You might also note that if S is the set of integers (or real numbers) and $+$, $\cdot$ are interpreted as ordinary addition and multiplication with 0 equal to zero, and $I = 1$, then axioms A1) for $+$ and $\cdot$, A2), A3) (i), and A4) are satisfied, but A3) (ii) does not hold true and it is impossible to define a unary operation satisfying A5). Thus, ordinary arithmetic does not provide an example of a Boolean algebra.

Observe, that if we interchange the operations $+$ and $\cdot$, and the symbols 0 and I throughout the axioms of a Boolean algebra, then we obtain precisely the same list of axioms. This symmetry leads to the **principle of duality**:

Every statement or identity deducible from the axioms of a Boolean algebra remains valid if we interchange the operations $+$ and $\cdot$, and the symbols 0 and I, throughout.

As consequences of the axioms we may deduce the following theorems, which are therefore true in any Boolean algebra. In each case the enunciation contains both a statement and its *dual* (obtained by interchanging $+$ and $\cdot$, and also 0 and I). Of course it is only necessary to prove one of these two statements. The dual statement is then valid by the principle of duality. Indeed its proof may be obtained by making the above interchanges at each step of the proof given.

2.2 Definition and basic results for Boolean Algebras

A **Boolean algebra** is an abstract system consisting of a set $S = \{a, b, \cdots\}$ on which two *binary operations*; $(a,b) \longmapsto a+b$ and $(a,b) \longmapsto a \cdot b$, and one *unary operation* $a \longmapsto a'$, are defined and satisfy the following axioms.

A1) If $a, b \in S$ then $a+b \in S$, $a \cdot b \in S$ and $a' \in S$. That is, S is *closed* under the operations of $+, \cdot$, and $'$.

A2) $a+b = b+a$ and $a \cdot b = b \cdot a$ for all $a, b \in S$. That is, $+$ and $\cdot$ are *commutative.*

A3) If a, b and c are in S then

(i) $a \cdot (b+c) = a \cdot b \ + \ a \cdot c$

and

(ii) $a + (b \cdot c) = (a+b) \cdot (a+c)$

That is, each of the binary operations is *distributive* over the other.

A4) There exists $0 \in S$ such that for all $a \in S$ we have $0 + a = a$, and there exists $I \in S$ such that for all $a \in S$ we have $I \cdot a = a$. That is, there exist *identities* for $+$ and $\cdot$.

A5) For all $a \in S$ we have $a + a' = I$ and $a \cdot a' = 0$. The *laws of complements.*

At this point you may wish to glance ahead to section 2.3.1 to see some examples of such a system. In particular example 1) should help make the results which follow more transparent. You might also note that if S is the set of integers (or real numbers) and $+, \cdot$ are interpreted as ordinary addition and multiplication with 0 equal to zero, and $I = 1$, then axioms A1) for $+$ and $\cdot$, A2), A3) (i), and A4) are satisfied, but A3) (ii) does not hold true and it is impossible to define a unary operation satisfying A5). Thus, ordinary arithmetic does not provide an example of a Boolean algebra.

Observe, that if we interchange the operations $+$ and $\cdot$, and the symbols 0 and I throughout the axioms of a Boolean algebra, then we obtain precisely the same list of axioms. This symmetry leads to the **principle of duality**:

Every statement or identity deducible from the axioms of a Boolean algebra remains valid if we interchange the operations $+$ and $\cdot$, and the symbols 0 and I, throughout.

As consequences of the axioms we may deduce the following theorems, which are therefore true in any Boolean algebra. In each case the enunciation contains both a statement and its *dual* (obtained by interchanging $+$ and $\cdot$, and also 0 and I). Of course it is only necessary to prove one of these two statements. The dual statement is then valid by the principle of duality. Indeed its proof may be obtained by making the above interchanges at each step of the proof given.

Theorem 1. (*Idempotent laws*) For every element a in a Boolean algebra,

$$a \cdot a = a \quad \text{and} \quad a + a = a.$$

Proof.

$$\begin{aligned} a &= I \cdot a && \text{by A4)} \\ &= (a + a') \cdot a && \text{by A5)} \\ &= a \cdot (a + a') && \text{by A2)} \\ &= a \cdot a + a \cdot a' && \text{by A3)} \\ &= a \cdot a + 0 && \text{by A5)} \\ &= 0 + a \cdot a && \text{by A2)} \\ &= a \cdot a && \text{by A4)} \end{aligned}$$

∎

Note how each step in the proof is justified by an appeal to the axioms. You should supply similar justifications in each of the subsequent proofs. Caution: In order to make these proofs more succinct, the justification for some of the steps may require the use of more than one axiom.

Theorem 2. For each element a in a Boolean algebra,

$$a \cdot 0 = 0 \quad \text{and} \quad a + I = I.$$

Proof.

$$\begin{aligned} 0 &= a \cdot a' \\ &= a \cdot (a' + 0) \\ &= a \cdot a' + a \cdot 0 \\ &= 0 + a \cdot 0 \\ &= a \cdot 0. \end{aligned}$$

∎

Theorem 3. (*Laws of absorption*) For each pair of elements a, b in a Boolean algebra,

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

Proof.

$$\begin{aligned} a &= a \cdot I \\ &= a \cdot (I + b) && \text{by theorem 2} \\ &= a \cdot I + a \cdot b \\ &= a + a \cdot b. \end{aligned}$$

∎

Theorem 4. (*Cancellation*) If for elements a, x, and y in a Boolean algebra we have

$$a + x = a + y \text{ and } a' + x = a' + y$$

or we have

$$a \cdot x = a \cdot y \text{ and } a' \cdot x = a' \cdot y$$

then

$$x = y.$$

Proof. If $a + x = a + y$ and $a' + x = a' + y$ then

$$(a + x) \cdot (a' + x) = (a + y) \cdot (a' + y).$$

Now the left hand side

$$\begin{aligned}(a + x) \cdot (a' + x) &= a \cdot a' + a \cdot x + x \cdot a' + x \cdot x \\ &= 0 + x \cdot (a + a') + x \\ &= x \cdot I + x \\ &= x + x \\ &= x,\end{aligned}$$

and similarly, the right hand side equals y.
Therefore, $x = y$, as required. ∎

Theorem 5. (*Associative laws*) For every a, b, and c in a Boolean algebra,

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

Proof (optional). Let $x := a \cdot (b \cdot c)$ and let $y := (a \cdot b) \cdot c$, then by theorem 4 it is enough to show that $a + x = a + y$ and that $a' + x = a' + y$.

Now,

$$\begin{aligned}a + x &= a + a \cdot (b \cdot c) \\ &= a \qquad \text{by theorem 3,}\end{aligned}$$

and

$$\begin{aligned}a + y &= a + ((a \cdot b) \cdot c) \\ &= (a + a \cdot b) \cdot (a + c) \qquad \text{by A3(ii)} \\ &= a \cdot (a + c) \qquad \text{by theorem 3} \\ &= a \qquad \text{again by theorem 3.}\end{aligned}$$

So, $a + x = a + y$.

Theorem 4. (*Cancellation*) If for elements a, x, and y in a Boolean algebra we have

$$a + x = a + y \quad \text{and} \quad a' + x = a' + y$$

or we have

$$a \cdot x = a \cdot y \quad \text{and} \quad a' \cdot x = a' \cdot y$$

then

$$x = y.$$

Proof. If $a + x = a + y$ and $a' + x = a' + y$ then

$$(a + x) \cdot (a' + x) = (a + y) \cdot (a' + y).$$

Now the left hand side

$$\begin{aligned}(a + x) \cdot (a' + x) &= a \cdot a' + a \cdot x + x \cdot a' + x \cdot x \\ &= 0 + x \cdot (a + a') + x \\ &= x \cdot I + x \\ &= x + x \\ &= x,\end{aligned}$$

and similarly, the right hand side equals y.
Therefore, $x = y$, as required. ∎

Theorem 5. (*Associative laws*) For every a, b, and c in a Boolean algebra,

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

Proof (optional). Let $x := a \cdot (b \cdot c)$ and let $y := (a \cdot b) \cdot c$, then by theorem 4 it is enough to show that $a + x = a + y$ and that $a' + x = a' + y$.

Now,

$$\begin{aligned}a + x &= a + a \cdot (b \cdot c) \\ &= a \qquad \text{by theorem 3,}\end{aligned}$$

and

$$\begin{aligned}a + y &= a + ((a \cdot b) \cdot c) \\ &= (a + a \cdot b) \cdot (a + c) \qquad \text{by A3(ii)} \\ &= a \cdot (a + c) \qquad \text{by theorem 3} \\ &= a \qquad \text{again by theorem 3.}\end{aligned}$$

So, $a + x = a + y$.

Also,

$$\begin{aligned}a' + x &= a' + (a \cdot (b \cdot c)) \\ &= (a' + a) \cdot (a' + (b \cdot c)) \\ &= I \cdot (a' + (b \cdot c)) \\ &= a' + (b \cdot c),\end{aligned}$$

while,

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

So, $a' + x = a' + y$, establishing the result. ∎

Theorem 6. (*Uniqueness of complements*) For each element a in a Boolean algebra, the element a' associated with a and satisfying A5) is unique.

Proof. Suppose that x satisfies $a + x = I$ and $a \cdot x = 0$.
Then

$$\begin{aligned}x &= I \cdot x \\ &= (a + a') \cdot x \\ &= a \cdot x \ + \ a' \cdot x \\ &= 0 \ + \ a' \cdot x \qquad \text{by assumption} \\ &= x \cdot a' \\ &= x \cdot a' \ + \ 0 \\ &= x \cdot a' \ + \ a \cdot a' \\ &= (x + a) \cdot a' \\ &= I \cdot a' \qquad \text{by assumption} \\ &= a'.\end{aligned}$$

∎

Since for every element a there is only one element a' satisfying the conditions of A5), we may unambiguously refer to it as the *complement* of a.

Corollary 7. For every element a in a Boolean algebra,

$$(a')' = a.$$

Proof. $(a')'$ is the unique element satisfying $a' + (a')' = I$ and $a' \cdot (a')' = 0$, but $a' + a = I$ and $a' \cdot a = 0$, thus we must have $(a')' = a$. ∎

EXERCISE. Prove that in any Boolean algebra:

(1) The elements 0 and I satisfying A4) are unique.

(2) For any elements a, b, and c we have the identity

$$a \cdot b + b \cdot c + c \cdot a = (a + b) \cdot (b + c) \cdot (a + c).$$

(3) $0' = I$ and $I' = 0$.

(4) For every pair of elements a and b,

$$(a \cdot b)' = a' + b' \qquad \text{and} \qquad (a + b)' = a' \cdot b'.$$

(5) For every pair of elements a and b,

$$a + a' \cdot b = a + b.$$

(6) If a, x, and y are elements such that both $a + x = a + y$ and $a \cdot x = a \cdot y$ then $x = y$.

Proof. $(a')'$ is the unique element satisfying $a' + (a')' = I$ and $a' \cdot (a')' = 0$, but $a' + a = I$ and $a' \cdot a = 0$, thus we must have $(a')' = a$. ∎

EXERCISE. Prove that in any Boolean algebra:

(1) The elements 0 and I satisfying A4) are unique.

(2) For any elements a, b, and c we have the identity

$$a \cdot b + b \cdot c + c \cdot a = (a + b) \cdot (b + c) \cdot (a + c).$$

(3) $0' = I$ and $I' = 0$.

(4) For every pair of elements a and b,

$$(a \cdot b)' = a' + b' \quad \text{and} \quad (a + b)' = a' \cdot b'.$$

(5) For every pair of elements a and b,

$$a + a' \cdot b = a + b.$$

(6) If a, x, and y are elements such that both $a + x = a + y$ and $a \cdot x = a \cdot y$ then $x = y$.

2.3 Examples, Boolean functions, and the representation of Boolean algebras

2.3.1 Examples of Boolean algebras

EXAMPLE 1) **Algebra of sets**

Let U be a given universal set, and let S be the set of all subsets of U (S is sometimes denoted by 2^U and termed the *power set* of U, a notation suggested by the number of elements in S, namely; $2^{\#U}$, where $\#U$ is the number of elements in U). Then, from the results of section 2.1 we see that S is a Boolean algebra if we define $+$ to be $\cup$, $\cdot$ to be $\cap$, 0 to be the null set $\emptyset$, I to be U, and a' to be the set complement of a in U for all $a \in S$. Note, $a \in S$ means $a \subseteq U$.

EXAMPLE 2) **The Boolean algebra** $\{0, 1\}$

Let S be the set consisting of the two numbers 0 and 1. Define; $\cdot$ to be ordinary multiplication, $+$ to be addition modulo 2, and complements by $0' = 1$, $1' = 0$, so that we have

a	b	$a \cdot b$
1	1	1
1	0	0
0	1	0
0	0	0

a	b	$a + b$
1	1	1
1	0	1
0	1	1
0	0	0

a	a'
1	0
0	1

It is readily verified that S with these operations is a Boolean algebra with $I = 1$. For example, to check the second distributive law, A3(ii), we calculate

a	b	c	$a + (b \cdot c)$	$(a + b) \cdot (a + c)$
1	1	1	1	1
1	1	0	1	1
1	0	1	1	1
1	0	0	1	1
0	1	1	1	1
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0

from which we see that, for all values of a, b and c, the expressions $a+(b \cdot c)$ and $(a+b) \cdot (a+c)$ have the same value, and so are equal.

Thus we see that the expressions $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ have identical truth values and so,

$$\neg(P \wedge Q) = \neg P \vee \neg Q.$$

It is now straight foreward to verify (do so as an EXERCISE) that the set of propositions with this definition of equality and with $+$ defined to be $\vee$, $\cdot$ defined to be $\wedge$, and $'$ defined to be negation $\neg$ is a Boolean algebra in which I corresponds to *tautology* (a proposition which is always true) and 0 corresponds to a proposition which is always false (*contradiction*). Indeed it was in this form that the English logician George Boole [1815 – 1864] first considered such algebras.

This enables us to manipulate and simplify logical expressions *algebraically* using the rules of Boolean algebra. In particular, any identity valid in an arbitrary Boolean algebra when appropriately translated becomes a valid statement in logic. For example, from exercise (2) at the end of section 2.2 we have

$$(P \wedge Q) \vee (Q \wedge R) \vee (P \wedge R) = (P \vee Q) \wedge (Q \vee R) \wedge (P \vee R).$$

EXERCISE. Verify this last identity by constructing truth tables for the left and right hand sides.

It is also worth noting that of necessity the principle of duality applies to logical statements and identities.

In our discussion of logic we have so far made no mention of the type of proposition most frequently encountered in mathematics; namely, P **implies** Q, or equivalently *If* P *then* Q, written $P \Longrightarrow Q$. However, it is not hard to see that what we mean by $P \Longrightarrow Q$ is the same as $\neg(P \wedge \neg Q)$, and so has the truth table

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note that, applying the rules of Boolean algebra to the expression $\neg(P \wedge \neg Q)$, we also have $P \Longrightarrow Q$ is the same as $\neg P \vee Q$.

It is also worth noting that the last two lines of the truth table for $P \Longrightarrow Q$ correspond to the observation that starting from a false premise we can deduce the *correctness* of anything, and exposes the fallacy in the all too common "schoolboy" method of proof; suppose what I want to prove is correct, compute $\cdots$ compute, deduce a truth, hence what I wanted to prove must have been correct! What lines of the table verify the correct method of proof; suppose the proposition I want to prove is false, compute $\cdots$ compute, arrive at a fallacy (or contradiction), hence what I wanted to prove is true?

Thus we see that the expressions $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ have identical truth values and so,

$$\neg(P \wedge Q) = \neg P \vee \neg Q.$$

It is now straight foreward to verify (do so as an EXERCISE) that the set of propositions with this definition of equality and with $+$ defined to be $\vee$, $\cdot$ defined to be $\wedge$, and $'$ defined to be negation $\neg$ is a Boolean algebra in which I corresponds to *tautology* (a proposition which is always true) and 0 corresponds to a proposition which is always false (*contradiction*). Indeed it was in this form that the English logician George Boole [1815 – 1864] first considered such algebras.

This enables us to manipulate and simplify logical expressions *algebraically* using the rules of Boolean algebra. In particular, any identity valid in an arbitrary Boolean algebra when appropriately translated becomes a valid statement in logic. For example, from exercise (2) at the end of section 2.2 we have

$$(P \wedge Q) \vee (Q \wedge R) \vee (P \wedge R) = (P \vee Q) \wedge (Q \vee R) \wedge (P \vee R).$$

EXERCISE. Verify this last identity by constructing truth tables for the left and right hand sides.

It is also worth noting that of necessity the principle of duality applies to logical statements and identities.

In our discussion of logic we have so far made no mention of the type of proposition most frequently encountered in mathematics; namely, P **implies** Q, or equivalently *If* P *then* Q, written $P \Longrightarrow Q$. However, it is not hard to see that what we mean by $P \Longrightarrow Q$ is the same as $\neg(P \wedge \neg Q)$, and so has the truth table

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note that, applying the rules of Boolean algebra to the expression $\neg(P \wedge \neg Q)$, we also have $P \Longrightarrow Q$ is the same as $\neg P \vee Q$.

It is also worth noting that the last two lines of the truth table for $P \Longrightarrow Q$ correspond to the observation that starting from a false premise we can deduce the *correctness* of anything, and exposes the fallacy in the all too common "schoolboy" method of proof; suppose what I want to prove is correct, compute $\cdots$ compute, deduce a truth, hence what I wanted to prove must have been correct! What lines of the table verify the correct method of proof; suppose the proposition I want to prove is false, compute $\cdots$ compute, arrive at a fallacy (or contradiction), hence what I wanted to prove is true?

EXERCISE. Prove that $P \Longrightarrow Q$ is the same as $\neg Q \Longrightarrow \neg P$. (Proving $P \Longrightarrow Q$ by establishing the *contrapositive* $\neg Q \Longrightarrow \neg P$ is an important method of proof often used in mathematics.)

2.3.2 Functions on Boolean algebras

Let B_1 and B_2 be two Boolean algebras. A function $f : B_1 \longrightarrow B_2$ is a Boolean **homomorphism** if $f(a+b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$, and $f(a') = f(a)'$, for all $a,\ b \in B_1$.
Note: Although we have used the same symbols, the operations in the left hand side of these expressions are those of B_1 while the operations in the right hand side are those of B_2.

For example, the function f from the Boolean algebra of propositions to the Boolean algebra $\{0,1\}$ which maps each proposition P to 1 if it is true and to 0 if it is false is easily shown to be a homomorphism. For instance, to verify $f(P \cdot Q) = f(P) \cdot f(Q)$ we need only compute the following table.

P	Q	$P \cdot Q$	$f(P)$	$f(Q)$	$f(P \cdot Q)$	$f(P) \cdot f(Q)$
T	T	T	1	1	1	1
T	F	F	1	0	0	0
F	T	F	0	1	0	0
F	F	F	0	0	0	0

It is this homomorphism which makes possible logical operations in a digital computer.

EXERCISES.

1) Let $f : B_1 \longrightarrow B_2$ be a homomorphism from the Boolean algebra B_1 to the Boolean algebra B_2. Show that $f(0) = 0$ and $f(I) = I$.

2) Let B_1 and B_2 be Boolean algebras. Show that $f : B_1 \longrightarrow B_2$ is a homomorphism if $f(a \cdot b) = f(a) \cdot f(b)$ and $f(a') = f(a)'$, for all $a,\ b \in B_1$. [Hint: Note that $a + b = (a' \cdot b')'$.]

A homomorphism f from the Boolean algebra B_1 to the Boolean algebra B_2 which is also *one-to-one* and *onto*, and so *invertible* with inverse f^{-1}, is termed a Boolean **isomorphism**. When there exists an isomorphism from B_1 to B_2 we say the two Boolean algebras are isomorphic. Two isomorphic Boolean algebras are essentially the same.

For example, it is readily verified that the Boolean algebra $\{0,1\}$ is isomorphic to the algebra of sets $\{\emptyset, U\}$ whose elements are the two subsets of the universal set $U = \{a\}$ with only one member a.

EXERCISES.

3) Let f be an isomorphism from the Boolean algebra B_1 onto the Boolean algebra B_2, show that f^{-1} is also an isomorphism.

4) Show that *is isomorphic to* defines an equivalence relation on the set of Boolean algebras.

We now study the structure of those functions f from a Boolean algebra B into itself which can be formed by combining several variables $x_1, x_2, \cdots$ and constants (fixed elements of B) using the operations of $+, \cdot,$ and $'$. Such functions are termed **Boolean functions**, and are the analogue of polynomials. For example, $f(x_1, x_2) = a \cdot x_1 \cdot x_2 + b \cdot x_1'$ is such a function, where a, b are fixed elements of B.

Theorem 1. Let B be a Boolean algebra and let $f(x_1, x_2, \cdots, x_n)$ be a Boolean function on B which contains no constants, then f can be expressed as a sum of terms of the form

$$\underbrace{\nu_1 \cdot \nu_2 \cdot \cdots \cdot \nu_n}_{n \text{ factors}},$$

where ν_i is either x_i or x_i'. We will refer to this as the **disjunctive normal form** of f.

An application of the principal of duality shows that we could also express f as a product of sums each of the form $\nu_1 + \nu_2 + \cdots + \nu_n$ known as the **conjunctive normal form** of f.

Proof. Wherever expressions of the form $(\alpha + \beta)'$ or $(\alpha \cdot \beta)'$ occur, replace them by $\alpha' \cdot \beta'$ and $\alpha' + \beta'$, respectively. Continue this process until the only complements present are of individual variables x_i.
Use the distributive law of $\cdot$ over $+$ as many times as is necessary to reduce the expression for f to a sum of products of variables and their complements.
Now suppose a term does not contain either the variable x_i or its complement x_i'. Multiply the term by $(x_i + x_i')$ and use the distributive rule to replace the term by a sum of two products, one having x_i as a factor and the other having x_i' as a factor. Continue this procedure for each missing variable in each of the terms.
Finally, use the idempotent laws to remove any duplicate terms. The resulting expression for f has the desired form.

∎

For example, to express the function $f(x_1, x_2) = x_1 \cdot x_2 + x_1'$ in disjunctive normal form we proceed as follows.

$$\begin{aligned} f(x_1, x_2) &= x_1 \cdot x_2 + x_1' \\ &= x_1 \cdot x_2 + (x_2 + x_2') \cdot x_1' \\ &= x_1 \cdot x_2 + x_1' \cdot x_2 + x_1' \cdot x_2'. \end{aligned}$$

EXERCISES.

3) Let f be an isomorphism from the Boolean algebra B_1 onto the Boolean algebra B_2, show that f^{-1} is also an isomorphism.

4) Show that *is isomorphic to* defines an equivalence relation on the set of Boolean algebras.

We now study the structure of those functions f from a Boolean algebra B into itself which can be formed by combining several variables $x_1, x_2, \cdots$ and constants (fixed elements of B) using the operations of $+, \cdot$, and $'$. Such functions are termed **Boolean functions**, and are the analogue of polynomials. For example, $f(x_1, x_2) = a \cdot x_1 \cdot x_2 + b \cdot x_1'$ is such a function, where a, b are fixed elements of B.

Theorem 1. Let B be a Boolean algebra and let $f(x_1, x_2, \cdots, x_n)$ be a Boolean function on B which contains no constants, then f can be expressed as a sum of terms of the form

$$\underbrace{\nu_1 \cdot \nu_2 \cdot \cdots \cdot \nu_n}_{n \text{ factors}},$$

where ν_i is either x_i or x_i'. We will refer to this as the **disjunctive normal form** of f.

An application of the principal of duality shows that we could also express f as a product of sums each of the form $\nu_1 + \nu_2 + \cdots + \nu_n$ known as the **conjunctive normal form** of f.

Proof. Wherever expressions of the form $(\alpha + \beta)'$ or $(\alpha \cdot \beta)'$ occur, replace them by $\alpha' \cdot \beta'$ and $\alpha' + \beta'$, respectively. Continue this process until the only complements present are of individual variables x_i.
Use the distributive law of $\cdot$ over $+$ as many times as is necessary to reduce the expression for f to a sum of products of variables and their complements.
Now suppose a term does not contain either the variable x_i or its complement x_i'. Multiply the term by $(x_i + x_i')$ and use the distributive rule to replace the term by a sum of two products, one having x_i as a factor and the other having x_i' as a factor. Continue this procedure for each missing variable in each of the terms.
Finally, use the idempotent laws to remove any duplicate terms. The resulting expression for f has the desired form. ∎

For example, to express the function $f(x_1, x_2) = x_1 \cdot x_2 + x_1'$ in disjunctive normal form we proceed as follows.

$$\begin{aligned} f(x_1, x_2) &= x_1 \cdot x_2 + x_1' \\ &= x_1 \cdot x_2 + (x_2 + x_2') \cdot x_1' \\ &= x_1 \cdot x_2 + x_1' \cdot x_2 + x_1' \cdot x_2'. \end{aligned}$$

EXERCISES.

5) What is the conjunctive normal form of the function $f(x_1, x_2) = x_1 \cdot x_2 + x_1'$?

6) Express in disjunctive normal form the function

$$f(x_1, x_2, x_3) = (x_1 \cdot x_2' + x_3')' \cdot x_2.$$

Remark. Any Boolean function in which the only constants are 0 or I can also be expressed in disjunctive (conjunctive) normal form. Indeed, if necessary we may first replace 0 by $x_i \cdot x_i'$ and I by $x_i + x_i'$, where x_i is any variable in the function, to obtain an expression free of constants. In particular *any Boolean function on the algebra* $\{0,1\}$ *can be expressed in disjunctive (conjunctive) normal form.* In fact, if $f(x_1, x_2, \cdots, x_n)$ is the function on $\{0,1\}$ determined by the table of values

x_1	x_2	$\cdots$	f
1	1	$\cdots$	$f(1,1,\cdots)$
1	0	$\cdots$	$f(1,0,\cdots)$
.	.		.
.	.		.
.	.		.
0	0	$\cdots$	$f(0,0,\cdots)$

then it is readily confirmed by direct substitution that

$$f(x_1, x_2, \cdots) = f(1,1,\cdots) \cdot x_1 \cdot x_2 \cdots + f(1,0,\cdots) \cdot x_1 \cdot x_2' \cdots + \cdots + f(0,0,\cdots) \cdot x_1' \cdot x_2' \cdots.$$

For example, if f is the function on $\{0,1\}$ given by

x_1	x_2	f
1	1	1
1	0	0
0	1	0
0	0	1

then

$$\begin{aligned} f(x_1, x_2) &= 1 \cdot x_1 \cdot x_2 + 0 \cdot x_1 \cdot x_2' + 0 \cdot x_1' \cdot x_2 + 1 \cdot x_1' \cdot x_2' \\ &= x_1 \cdot x_2 \ + \ x_1' \cdot x_2'. \end{aligned}$$

2.3.3 The representation of Boolean algebras

In 1936 the American mathematician M.H. Stone proved that every Boolean algebra is essentially an algebra of sets. Since sets and the set operations are relatively simple things about which we can develop a good intuition, Stone's result is an extremely important one. It means that any statement or identity which we can establish for arbitrary sets is true in any Boolean algebra. It also means that devices such as Venn diagrams may be used to help our reasoning in any Boolean algebra.

A proof of Stone's general result is beyond the scope of these notes, we will however prove the particular case for finite Boolean algebras.

What appears to be missing in an arbitrary Boolean algebra, but present in an algebra of sets, is the notion of one element being a subset of the other. The exercise at the end of section 2.1 suggests a way around this.

Definition (*inclusion relation*): For two elements a, b of a Boolean algebra B we will say $a \leq b$ if $a \cdot b' = 0$.
In an algebra of sets $a \leq b$ corresponds exactly to $a \subseteq b$.

We begin by showing that the relationship "$\leq$" has the properties we would expect from the case of sets.

Theorem 2. Let a, b and c be three elements of a Boolean algebra.

(1) $a \leq a$. That is "$\leq$" is *reflexive*.

(2) If $a \leq b$ and $b \leq a$ then $a = b$. That is "$\leq$" is *anti-symmetric*.

(3) If $a \leq b$ and $b \leq c$ then $a \leq c$. That is "$\leq$" is *transitive*.

(4) $0 \leq a \leq I$.

(5) If $a \leq b$ then $a \cdot c \leq b \cdot c$.

Proof.

(1) $a \cdot a' = 0$, so $a \leq a$.

(2) If $a \cdot b' = 0$ and $b \cdot a' = 0$ then $a' + b = a' + b'' = (a \cdot b')' = 0' = I$ and $a' \cdot b = 0$, so

$$\begin{aligned} b &= a'' \qquad \text{by theorem 6) of section 2.2} \\ &= a \end{aligned}$$

(3) If $a \cdot b' = 0$ and $b \cdot c' = 0$ then

$$\begin{aligned} a \cdot c' &= (a \cdot c') \cdot (b + b') \\ &= (a \cdot c' \cdot b) + (a \cdot c' \cdot b') \\ &= (a \cdot 0) + (c' \cdot 0) \\ &= 0, \end{aligned}$$

so $a \leq c$.

(4) $0 \cdot a' = 0$, so $0 \leq a$, and $a \cdot I' = a \cdot 0 = 0$, so $a \leq I$.

one. It means that any statement or identity which we can establish for arbitrary sets is true in any Boolean algebra. It also means that devices such as Venn diagrams may be used to help our reasoning in any Boolean algebra.

A proof of Stone's general result is beyond the scope of these notes, we will however prove the particular case for finite Boolean algebras.

What appears to be missing in an arbitrary Boolean algebra, but present in an algebra of sets, is the notion of one element being a subset of the other. The exercise at the end of section 2.1 suggests a way around this.

Definition (*inclusion relation*): For two elements a, b of a Boolean algebra B we will say $a \leq b$ if $a \cdot b' = 0$.
In an algebra of sets $a \leq b$ corresponds exactly to $a \subseteq b$.

We begin by showing that the relationship "$\leq$" has the properties we would expect from the case of sets.

Theorem 2. Let a, b and c be three elements of a Boolean algebra.

(1) $a \leq a$. That is "$\leq$" is *reflexive*.

(2) If $a \leq b$ and $b \leq a$ then $a = b$. That is "$\leq$" is *anti-symmetric*.

(3) If $a \leq b$ and $b \leq c$ then $a \leq c$. That is "$\leq$" is *transitive*.

(4) $0 \leq a \leq I$.

(5) If $a \leq b$ then $a \cdot c \leq b \cdot c$.

Proof.

(1) $a \cdot a' = 0$, so $a \leq a$.

(2) If $a \cdot b' = 0$ and $b \cdot a' = 0$ then $a' + b = a' + b'' = (a \cdot b')' = 0' = I$ and $a' \cdot b = 0$, so

$$\begin{aligned} b &= a'' \qquad \text{by theorem 6) of section 2.2} \\ &= a \end{aligned}$$

(3) If $a \cdot b' = 0$ and $b \cdot c' = 0$ then

$$\begin{aligned} a \cdot c' &= (a \cdot c') \cdot (b + b') \\ &= (a \cdot c' \cdot b) + (a \cdot c' \cdot b') \\ &= (a \cdot 0) + (c' \cdot 0) \\ &= 0, \end{aligned}$$

so $a \leq c$.

(4) $0 \cdot a' = 0$, so $0 \leq a$, and $a \cdot I' = a \cdot 0 = 0$, so $a \leq I$.

(5) If $a \cdot b' = 0$ then

$$\begin{aligned} (a \cdot c) \cdot (b \cdot c)' &= (a \cdot c) \cdot (b' + c') \\ &= (a \cdot b' \cdot c) + (a \cdot c \cdot c') \\ &= (0 \cdot c) + (a \cdot 0) \\ &= 0, \end{aligned}$$

so $a \cdot c \leq b \cdot c$. ∎

EXERCISE. Prove that for a, b and c elements in a Boolean algebra:

(1) If $a \leq b$ then $a + c \leq b + c$.

(2) If $a \leq b$ and $a \leq c$ then $a \leq b \cdot c$.

(3) $a \leq b$ if and only if $b' \leq a'$.

(4) $a \cdot b \leq a \leq a + b$.

(5) $a \leq b$ if and only if $a \cdot b = a$.

(6) $a \leq b$ if and only if $a + b = b$.

Definition: We say $a \neq 0$ is an **atom** in a Boolean algebra B if for each $x \in B$ either $a \cdot x = 0$ or $a \cdot x = a$.

EXERCISE.

(7) Let $U = \{a, b, c, d\}$ and let B be the Boolean algebra of subsets of U. What are the atoms of B?

(8) Show that $a \neq 0$ is an atom in the Boolean algebra B if and only if for each $x \in B$ either $a \leq x$ or $a \leq x'$.

(9) Show that $a \neq 0$ is an atom in the Boolean algebra B if and only if $y \leq a$ implies $y = 0$ or $y = a$.

Theorem 3. Let B be a Boolean algebra with only a finite number of distinct elements, then B is isomorphic to an algebra of sets.

Proof (optional). We first show that every element $x \neq 0$ in B "contains" an atom.
If x is itself not an atom then there exists $x_1 \in B$ with $x \cdot x_1 \neq 0$ or x. If $x \cdot x_1$ is not an atom then there exists $x_2 \in B$ with $x \cdot x_1 \cdot x_2 \neq 0$ or $x \cdot x_1$ and also not equal to x (if $x \cdot x_1 \cdot x_2 = x$, then $x \cdot x_1 = (x \cdot x_1 \cdot x_2) \cdot x_1 = x \cdot x_1 \cdot x_2 = x$ contradicting our choice of x_1). Repeating this procedure yields a sequence of distinct non-zero elements $x,\ x \cdot x_1,\ x \cdot x_1 \cdot x_2,\ x \cdot x_1 \cdot x_2 \cdot x_3,\ \cdots$. This cannot continue indefinitely as there are only a finite number of distinct elements in B. Thus, eventually we must arrive at a term $x \cdot x_1 \cdot x_2 \cdots \cdot x_m \leq x$ which is an atom.

Now, let $A := \{a_1, a_2, \cdots, a_n\}$ be the set of all atoms in B. From the argument above we know that $A \neq \emptyset$. We next show that A *partitions* I in the sense that

$$a_1 + a_2 + \cdots + a_n = I.$$

Suppose this were not the case. That is, $z := a_1 + a_2 + \cdots + a_n \neq I$. Then, taking complements $z' = a_1' \cdot a_2' \cdots a_n' \neq 0$, so by the first part of the proof z' contains an atom, say a_i, which is necessarily in A. But, then

$$a_i = a_i \cdot z' = a_i \cdot (a_1' \cdot a_2' \cdots a_i' \cdots a_n') = 0,$$

contradicting a_i is an atom and so non-zero. Thus $a_1 + a_2 + \cdots + a_n = I$.

For $x \in B$ let $A_x := \{a : a \in A \text{ and } a \leq x\}$. That is, A_x is the set of atoms contained in x. Then, for $a \in A_x$ we have $a \cdot x = a$, and for any atom $a \notin A_x$ we necessarily have $a \cdot x = 0$. Thus,

$$\begin{aligned} x &= I \cdot x \\ &= (a_1 + a_2 + \cdots + a_n) \cdot x \\ &= a_1 \cdot x + a_2 \cdot x + \cdots + a_n \cdot x \\ &= \sum_{a \in A_x} a \cdot x \qquad \text{all other terms of the above sum are 0} \\ &= \sum_{a \in A_x} a. \end{aligned}$$

That is, each element $x \in B$ is the sum of the atoms contained in it.

The function $f : B \longrightarrow 2^A : x \mapsto A_x$ is now readily verified to be a Boolean isomorphism from B to the algebra of subsets of A, thereby establishing the result. ■

EXERCISE (optional). Using the notation introduced in the previous proof show that:

(i) For $x, y \in B$ we have $A_{x+y} = A_x \cup A_y$, $A_{x \cdot y} = A_x \cap A_y$, and $A_{x'} = A_x'$.

(ii) The function f is *one-to-one* and *onto*.

Hence conclude that f is indeed an isomorphism as required.

Now, let $A := \{a_1, a_2, \cdots, a_n\}$ be the set of all atoms in B. From the argument above we know that $A \neq \emptyset$. We next show that A *partitions* I in the sense that

$$a_1 + a_2 + \cdots + a_n = I.$$

Suppose this were not the case. That is, $z := a_1 + a_2 + \cdots + a_n \neq I$. Then, taking complements $z' = a_1' \cdot a_2' \cdots a_n' \neq 0$, so by the first part of the proof z' contains an atom, say a_i, which is necessarily in A. But, then

$$a_i = a_i \cdot z' = a_i \cdot (a_1' \cdot a_2' \cdots a_i' \cdots a_n') = 0,$$

contradicting a_i is an atom and so non-zero. Thus $a_1 + a_2 + \cdots + a_n = I$.

For $x \in B$ let $A_x := \{a : a \in A \text{ and } a \leq x\}$. That is, A_x is the set of atoms contained in x. Then, for $a \in A_x$ we have $a \cdot x = a$, and for any atom $a \notin A_x$ we necessarily have $a \cdot x = 0$. Thus,

$$\begin{aligned} x &= I \cdot x \\ &= (a_1 + a_2 + \cdots + a_n) \cdot x \\ &= a_1 \cdot x + a_2 \cdot x + \cdots + a_n \cdot x \\ &= \sum_{a \in A_x} a \cdot x \qquad \text{all other terms of the above sum are 0} \\ &= \sum_{a \in A_x} a. \end{aligned}$$

That is, each element $x \in B$ is the sum of the atoms contained in it.

The function $f : B \longrightarrow 2^A : x \mapsto A_x$ is now readily verified to be a Boolean isomorphism from B to the algebra of subsets of A, thereby establishing the result. ∎

EXERCISE (optional). Using the notation introduced in the previous proof show that:

(i) For $x,\ y \in B$ we have $A_{x+y} = A_x \cup A_y$, $A_{x \cdot y} = A_x \cap A_y$, and $A_{x'} = A_x'$.

(ii) The function f is *one-to-one* and *onto*.

Hence conclude that f is indeed an isomorphism as required.

2.4 Application to switching circuits

We will analyse electrical networks of the type illustrated in figure 1 using the Boolean algebra $\{0, 1\}$.

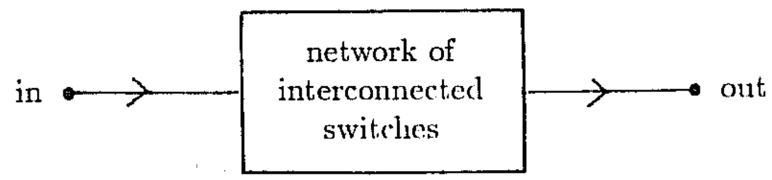


Figure 1.

Such a circuit is illustrated in figure 2.

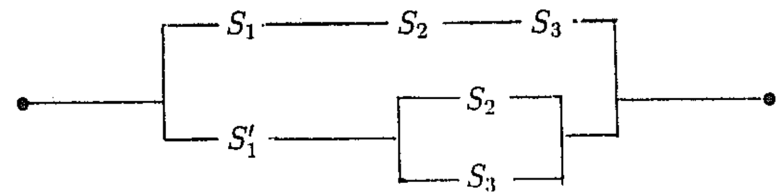


Figure 2.

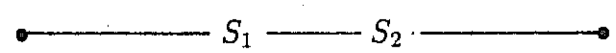
Switching circuits of this type are fundamental to the design of digital computers. In practice the switches may be realized by *relays* or *electronic switching circuits* controlled by outside electrical impulses.

We associate with the switches variables $S_1,\ S_2,\ \cdots$ so that when a switch is open the associated variable has the value 0, and when the switch is closed the variable has the value 1. When two, or more, switches are "mechanically" connected so that they all open and close together they will be associated with the same variable. For example, such a situation may be achieved by using a *multiple pole switch*. When a given switch is always open when some other particular switch associated with the variable S_i is closed, and is also closed whenever the other switch is open, then it will be associated with the variable S_i'. Such a situation may be achieved by using a *double throw switch*, for example.

We wish to associate with the network a Boolean function $f(S_1,\ S_2,\ \cdots)$ which will have the value 1 when the state of the switches will allow a current to pass through the network, and will have the value 0 when the state of the switches prevents a current from flowing.

Examples.

(1) For a pair of switches S_1 and S_2 connected in **series**



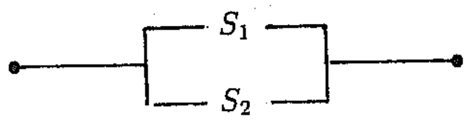
we see that the associated function f has the table of values

S_1	S_2	f
1	1	1
1	0	0
0	1	0
0	0	0

and so,

$$f(S_1, S_2) = S_1 \cdot S_2.$$

(2) For a pair of switches S_1 and S_2 connected in **parallel**



we see that the associated function f has the table of values

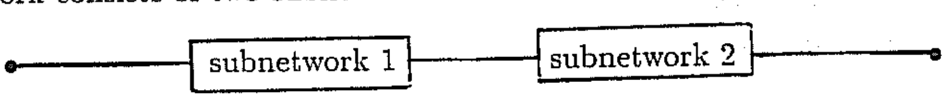
S_1	S_2	f
1	1	1
1	0	1
0	1	1
0	0	0

and so,

$$f(S_1, S_2) = S_1 + S_2.$$

These two examples may be generalized as follows.

(1') If a network consists of two subnetworks connected in series,

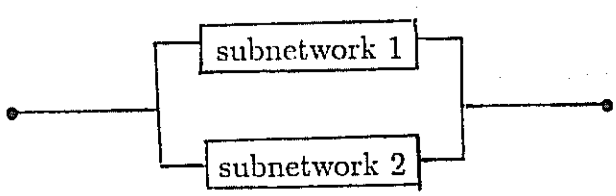


and if the Boolean functions associated with each of the subnetworks are f_1 and f_2 respectively, then the function associated with the entire network is

$$f = f_1 \cdot f_2.$$

Similarly,

(2') If a network consists of two subnetworks connected in parallel,



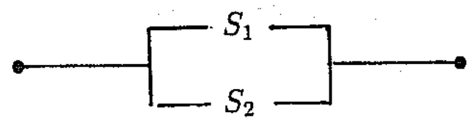
we see that the associated function f has the table of values

S_1	S_2	f
1	1	1
1	0	0
0	1	0
0	0	0

and so,

$$f(S_1, S_2) = S_1 \cdot S_2.$$

(2) For a pair of switches S_1 and S_2 connected in **parallel**



we see that the associated function f has the table of values

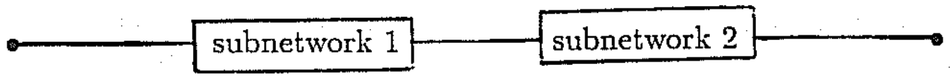
S_1	S_2	f
1	1	1
1	0	1
0	1	1
0	0	0

and so,

$$f(S_1, S_2) = S_1 + S_2.$$

These two examples may be generalized as follows.

(1') If a network consists of two subnetworks connected in series,

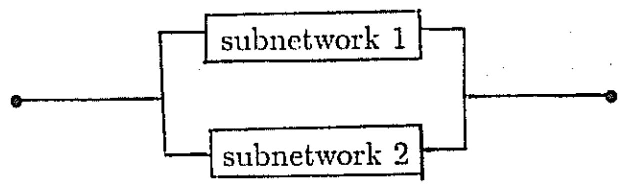


and if the Boolean functions associated with each of the subnetworks are f_1 and f_2 respectively, then the function associated with the entire network is

$$f = f_1 \cdot f_2.$$

Similarly,

(2') If a network consists of two subnetworks connected in parallel,



and if the Boolean functions associated with each of the subnetworks are f_1 and f_2 respectively, then the function associated with the entire network is

$$f = f_1 + f_2.$$

Using these results we may write down the Boolean function associated with any *series–parallel* network by inspection.

For example, the Boolean function associated with the network of figure 2 is

$$f(S_1, S_2, S_3) = S_1 \cdot S_2 \cdot S_3 + S_1' \cdot (S_2 + S_3).$$

EXERCISE. Write down the Boolean function associated with the network illustrated in figure 3.

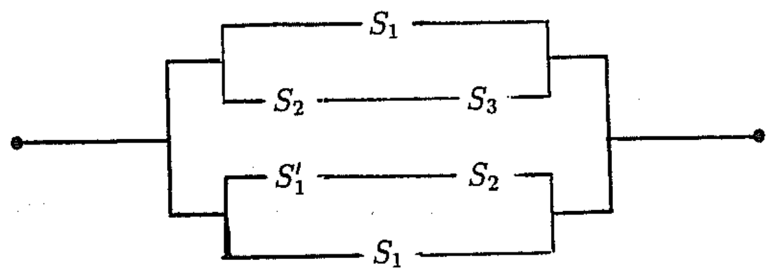


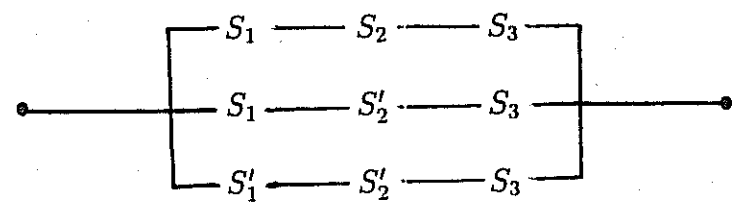
Figure 3.

We may also apply these results in reverse. For instance, given a Boolean function f which is expressed as a sum of products, in particular a function expressed in disjunctive normal form, we may construct a network, consisting of parallel connected banks of switches in series, for which f is the associated function.

For example, a circuit corresponding to the function

$$f(S_1, S_2, S_3) = S_1 \cdot S_2 \cdot S_3 + S_1 \cdot S_2' \cdot S_3 + S_1' \cdot S_2' \cdot S_3$$

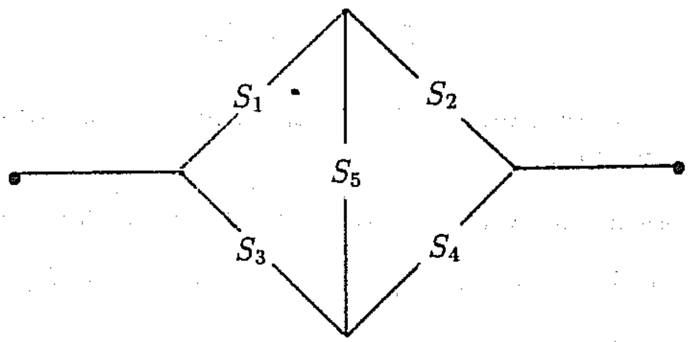
is



EXERCISE. Construct a circuit for which $f(S_1, S_2, S_3, S_4, S_5) = (S_1 \cdot S_2 + S_3 + S_4) \cdot S_5$ is the associated Boolean function.

From section 2.3.2 we know that every Boolean function on $\{0, 1\}$ can be written in disjunctive normal form, this shows that *every switching network is equivalent to a network of parallel connected banks of serially connected switches.*

For example, the non series–parallel *bridging* circuit



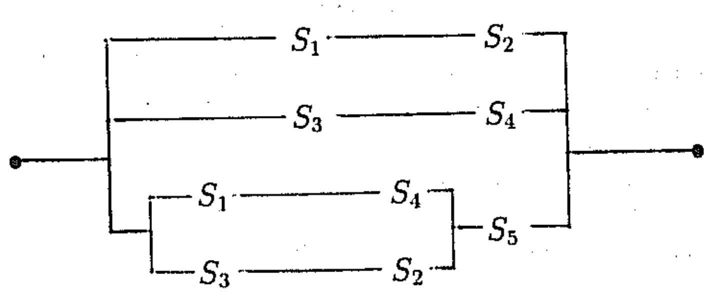
has the following possible paths through it.

$$S_1 \cdot S_2 \quad S_3 \cdot S_4 \quad S_1 \cdot S_5 \cdot S_4 \quad S_3 \cdot S_5 \cdot S_2$$

The associated Boolean function is therefore

$$\begin{aligned} f(S_1, S_2, S_3, S_4, S_5) &= S_1 \cdot S_2 + S_3 \cdot S_4 + S_1 \cdot S_5 \cdot S_4 + S_3 \cdot S_5 \cdot S_2 \\ &= S_1 \cdot S_2 + S_3 \cdot S_4 + S_5 \cdot (S_1 \cdot S_4 + S_3 \cdot S_2) \end{aligned}$$

and so an equivalent series–parallel network for the bridge is

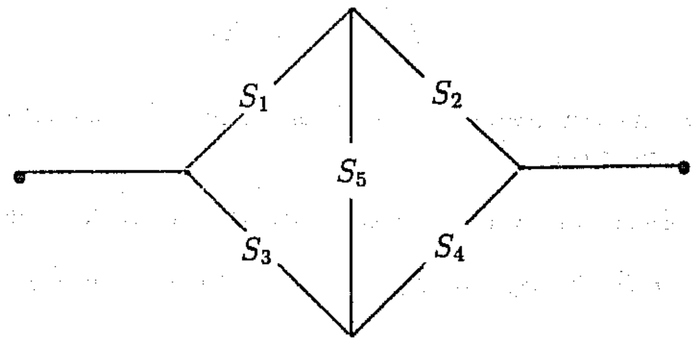


Similarly, a Boolean function which is expressed as a product of sums, in particular an function in conjunctive normal form, is the function associated with a circuit consisting o serially connected banks of parallel switches. And every switching network is equivalen to a network of this type.

These results suggest a powerful technique for establishing the equivalence of two circuits Find the Boolean functions associated with the given networks, and use the laws of Boolea algebra to show that the expressions for the two functions are equal, thereby establishin that the networks have identical switching properties.

Similarly we may **simplify a network** by finding an expression for the associated Boolea function f. If possible simplifying the expression. Then constructing a new networ corresponding to the simpler expression for f.

For example, the non series–parallel *bridging* circuit



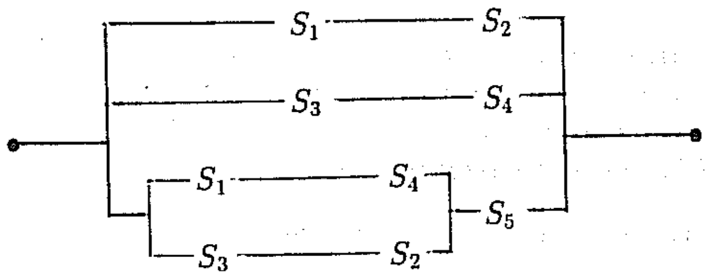
has the following possible paths through it.

$$S_1 \cdot S_2 \quad S_3 \cdot S_4 \quad S_1 \cdot S_5 \cdot S_4 \quad S_3 \cdot S_5 \cdot S_2$$

The associated Boolean function is therefore

$$\begin{aligned} f(S_1, S_2, S_3, S_4, S_5) &= S_1 \cdot S_2 + S_3 \cdot S_4 + S_1 \cdot S_5 \cdot S_4 + S_3 \cdot S_5 \cdot S_2 \\ &= S_1 \cdot S_2 + S_3 \cdot S_4 + S_5 \cdot (S_1 \cdot S_4 + S_3 \cdot S_2) \end{aligned}$$

and so an equivalent series–parallel network for the bridge is



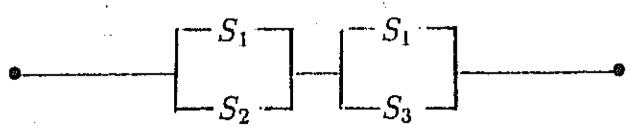
Similarly, a Boolean function which is expressed as a product of sums, in particular any function in conjunctive normal form, is the function associated with a circuit consisting of serially connected banks of parallel switches. And every switching network is equivalent to a network of this type.

These results suggest a powerful technique for establishing the equivalence of two circuits: Find the Boolean functions associated with the given networks, and use the laws of Boolean algebra to show that the expressions for the two functions are equal, thereby establishing that the networks have identical switching properties.

Similarly we may **simplify a network** by finding an expression for the associated Boolean function f. If possible simplifying the expression. Then constructing a new network corresponding to the simpler expression for f.

In this way both the problem of showing networks are equivalent, and the question of finding the "simplest" series–parallel network equivalent to a given one, are reduced to algebra.

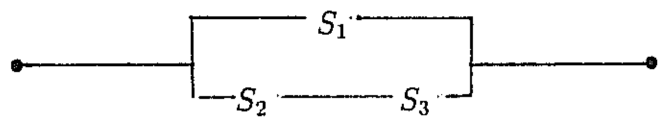
For example, the network



has associated function

$$\begin{aligned} f(S_1, S_2, S_3) &= (S_1 + S_2) \cdot (S_1 + S_3) \\ &= S_1 + (S_2 \cdot S_3) \end{aligned}$$

and so is equivalent to the network



EXERCISE. Show that the network of figure 3 is equivalent to S_1 and S_2 connected in parallel.

We conclude with a discussion of **the design of circuits with given switching properties.** In fact we have already solved this problem. Knowing the switching properties required of a circuit is the same as knowing an associated Boolean function for the network, and we have already seen how to construct a corresponding circuit.

For example, let us consider the problem of controlling a light from two different switch positions. Such a situation is often found in the lighting arrangement for a hallway or stairwell, where the light can be switched on or off from either end.

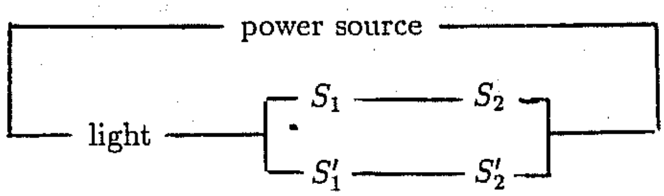
A moments thought will show that we want the state of our network (conducting, or nonconducting) to change if the state of either of the two switches S_1 and S_2 is changed. If we agree that the light is to be on when both of the switches are closed, then the Boolean function f associated with the network must be given by the table

S_1	S_2	f
1	1	1
1	0	0
0	1	0
0	0	1

Except for the change in variable names this is the function considered at the end of section 2.3.2, where it was shown that

$$f(S_1, S_2) \;=\; S_1 \cdot S_2 \;+\; S_1' \cdot S_2'.$$

Thus, a suitable circuit is



EXERCISE. Is it possible to find a network which will control a light from three different switch positions, and if so design an appropriate circuit.