Set Theory, Logic and Boolean Algebra

1 Notation

We’ll use the following notation. If $A$ and $B$ are sets and $p, q$ are (true/false) statements, then:

- $x \in A$ means that $x$ is an element of $A$.
- $A \ni x$ means that $A$ contains $x$.
- $A \cup B$ is the union of $A$ and $B$, i.e. $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$ (in mathematics “or” means “and/or”).
- $A \cap B$ is the intersection of $A$ and $B$, i.e. $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.
- $A \subseteq B$ means that $A$ is a subset of $B$, i.e. $x \in A \implies x \in B$.
- $A \supseteq B$ means that $A$ is a superset of $B$, i.e. $B \subseteq A$.
- $A \subset B$ means that $A$ is a proper subset of $B$, i.e. $A \subseteq B$ and $A \neq B$.
- $A \supset B$ means that $A$ is a proper superset of $B$, i.e. $B \subset A$.
- $A \setminus B$ (or $A - B$) is $A$ take $B$, i.e. the set $\{x \in A \mid x \notin B\}$.
- $\emptyset$, \{\} is the empty set, i.e. the set with no elements.
- Note that $\emptyset$ is a subset of every set.

- $A^\prime$, $\overline{A}$, $A^c$ is the complement of $A$, i.e. $A^\prime = \{x \mid x \notin A\}$.
- Here $x$ belongs to some “universal set” which should be clear from the context.

- $\neg p$, $p'$ is the negation of $p$, i.e. if $p$ is true then $\neg p$ is false
- and if $p$ is false then $\neg p$ is true.

- $p \rightarrow q$, $p \implies q$ means $p$ implies $q$, i.e. if $p$ is true then so is $q$.
- $p \leftrightarrow q$, $p \iff q$ means $p$ and $q$ are logically equivalent, i.e. $p$ is true (false) precisely when $q$ is true (false).

- $\mathbb{P}$ is the set of prime numbers $\{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$.
- $\mathbb{N}$ is the set of natural numbers $\{1, 2, 3, \ldots\}$.
- Note that some texts include 0 in $\mathbb{N}$. Our definition is equivalent to $\mathbb{Z}^+$. 

- $\mathbb{Z}$ is the set of integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- $\mathbb{Q}$ is the set of rational numbers, i.e. $\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$.
- $\mathbb{R}$ is the set of all real numbers.
2 Specifying sets, Set-builder notation

The simplest way to describe a set is by enumeration, i.e. by listing its elements explicitly between curly braces. Thus \{1, 2\} denotes the set whose only elements are 1 and 2. Note the following two properties of sets:

- Order of elements is immaterial, e.g. \{1, 2\} = \{2, 1\}.
- Repetition (multiplicity) of elements is irrelevant, e.g. \{1, 1, 2, 2\} = \{1, 2, 2, 2\} = \{1, 2\}.

The alternative way to represent a set is with set-builder notation, which has the form

$$\{\text{pattern} \mid \text{condition(s)}\}.$$

Typically, we write \(\{x \mid P(x)\}\), or \(\{x : P(x)\}\), to denote the set containing all objects \(x\) such that the condition or property \(P\) holds. E.g. we may write

$$\{x \mid x \text{ is a prime}\},$$

literally read as:

the set of all \(x\) such that \(x\) is a prime,

which, in this case, we could say more succinctly as: the set of prime numbers. Usually, we read the symbol ‘’ as ‘such that’. The pattern may also be an expression, e.g.

$$\{p^2 \mid p \text{ is a prime}\}$$

is the set of all numbers that are the squares of prime numbers.

There are a few variants of set builder notation. A summary of most of the variants are as follows:

- \(\{x \in A \mid P(x)\}\) denotes the set of all \(x\) that are already in \(A\) such that \(x\) has the property \(P\), e.g. \(\{x \in \mathbb{Z} \mid x \text{ is even}\}\) is the set of all even integers.

- \(\{f(x) \mid x \in A\}\) denotes the set of all objects with pattern \(f(x)\) such that \(x\) is in \(A\). We saw this form above, in the definition of the rational numbers \(\mathbb{Q}\). For a simpler example, consider: \(\{2x \mid x \in \mathbb{Z}\}\) is another way of specifying the set of all even integers.

- \(\{f(x) \mid P(x)\}\) is the most general form of set builder notation, e.g. above we saw: \(\{p^2 \mid p \text{ is a prime}\}\), the set of squared prime numbers.

3 Universal sets and complements

The relative complement of \(B\) relative to \(A\), also known as the set difference of \(A\) and \(B\), is the set of all objects that belong to \(A\) but not to \(B\), i.e. it is the set

$$A \setminus B = \{x \in A \mid x \notin B\}.$$ 

Often we consider all sets as being subsets of some given universal set. E.g., if we are investigating properties of the real numbers \(\mathbb{R}\) (and subsets of \(\mathbb{R}\)), then we may take \(\mathbb{R}\) as our universal set.
4 DE MORGAN’S LAWS

The (absolute) complement $B'$ of a set $B$ (in a universal set $U$) using the set difference notation is $U \setminus B$. Given a universal set $U$ and a subset $B$ of $U$, we may define the complement of $B$ (in $U$) as

$$B^c = \{ x \in U \mid x \notin B \}.$$ 

In other words, $B^c$ (‘$B$-complement’) is the set of all elements of $U$ which are not elements of $B$. The notations $B'$ (the one we will usually use) and $\overline{B}$ are also commonly used to represent the complement of $B$. Thus, the complement $E'$ of the set $E = \{2x \mid x \in \mathbb{Z}\}$ (the set of all even integers) in $\mathbb{Z}$, is the set of all odd integers, while the complement of $E$ in $\mathbb{R}$ is the set of all real numbers that are either odd integers or not integers at all.

4 De Morgan’s Laws

The following statements, known as de Morgan’s Laws, are true for any sets $A$ and $B$.

$$(A \cup B)' = A' \cap B' \quad (A \cap B)' = A' \cup B'$$

Each is easy to prove using Venn diagrams. Note that when we draw a Venn diagram that is supposed to represent a general situation each set should be drawn to intersect each other set (this represents a general situation, since it can still happen that any region may actually be empty). Thus, a Venn diagram with two sets $A$ and $B$ should be drawn as two intersecting circles in a rectangle representing the universal set $U$.

5 Sets of sets

The term for a set of sets is a collection. One particular collection of importance is the following.

Definition 1. The power set of a set $A$ is the set of all subsets of $A$, written $\mathcal{P}(A)$. For example, if $A = \{x, y, z\}$ then

$$\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}.$$ 

Observe that the cardinality (number of members) of the power set of a set $A$ in our example above is $8 = 2^3$. In general, we have for a set $A$,

$$|\mathcal{P}(A)| = 2^{|A|},$$ 

where $|X|$ represents the cardinality of $X$. The reason for this is that for a given subset $S$ of $A$, each element of $A$ is either in $S$ or not in $S$ (i.e. two possibilities for each element of $A$).

6 The connection between Set Theory and Logic

Logic deals with statements that are either true or false, whereas Set Theory deals with elements of sets – a given element can either be in a given set or not in the set. Let $A, B$ represent sets. Also, let $p, q$ represent statements and $p'$ represents the negation of $p$ (if $p$ is true then $p'$ is false, and vice-versa).

A right arrow ($\rightarrow$) denotes implies. If $p \rightarrow q$, then, when $p$ is true so is $q$. 
A double-arrow ($\leftrightarrow$) is the corresponding symbol for equals; it denotes its operands are logically equivalent. If $p \leftrightarrow q$ then, when $p$ is true, so is $q$, and when $p$ is false, so is $q$.

A way of viewing the connection between Set Theory and Logic: is to say that the statements in Logic tell us which regions of a given Universal set are non-empty. With this view, one can often convert a Set Theory statement to a Logic one by sticking ‘$x \in$’ in front of it, e.g.

$$A \cup B \rightarrow x \in (A \cup B)$$

$$\leftrightarrow x \in A \text{ or } x \in B$$

Now, $x \in A$ and $x \in B$ are examples of statements $p$ and $q$, respectively.

We give a few examples of this correspondence between Set Theory and Logic:

<table>
<thead>
<tr>
<th>Set Theory Identity</th>
<th>Logic Tautology</th>
<th>Name of Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A \cup B = B \cup A$</td>
<td>$p \lor q \leftrightarrow q \lor p$</td>
<td>commutativity</td>
</tr>
<tr>
<td>$A \cap B = B \cap A$</td>
<td>$p \land q \leftrightarrow q \land p$</td>
<td>commutativity</td>
</tr>
<tr>
<td>$(A \cup B) \cup C = A \cup (B \cup C)$</td>
<td>$(p \lor q) \lor r \leftrightarrow p \lor (q \lor r)$</td>
<td>associativity</td>
</tr>
<tr>
<td>$(A \cap B) \cap C = A \cap (B \cap C)$</td>
<td>$(p \land q) \land r \leftrightarrow p \land (q \land r)$</td>
<td>associativity</td>
</tr>
<tr>
<td>$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$</td>
<td>$p \lor (q \land r) \leftrightarrow (p \lor q) \land (p \lor r)$</td>
<td>distribution</td>
</tr>
<tr>
<td>$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$</td>
<td>$p \land (q \lor r) \leftrightarrow (p \land q) \lor (p \land r)$</td>
<td>distribution</td>
</tr>
<tr>
<td>$A \cup A = A$</td>
<td>$p \lor p \leftrightarrow p$</td>
<td>idempotence</td>
</tr>
<tr>
<td>$A \cap A = A$</td>
<td>$p \land p \leftrightarrow p$</td>
<td>idempotence</td>
</tr>
<tr>
<td>$A \cup (A \cap B) = A$</td>
<td>$p \lor (p \land q) \leftrightarrow p$</td>
<td>absorption</td>
</tr>
<tr>
<td>$A \cap (A \cup B) = A$</td>
<td>$p \land (p \lor q) \leftrightarrow p$</td>
<td>absorption</td>
</tr>
<tr>
<td>$A \cup A' = U$</td>
<td>$p \lor \neg p \leftrightarrow \text{true}$</td>
<td></td>
</tr>
<tr>
<td>$A \cap A' = \emptyset$</td>
<td>$p \land \neg p \leftrightarrow \text{false}$</td>
<td></td>
</tr>
</tbody>
</table>

A subset of the above rules can be taken as axioms for a Boolean Algebra. Notice how the identities/tautologies come in dual pairs.

7 Truth tables

The truth value of a statement is the classification of the statement as true or false, which we generally abbreviate to T or F, respectively.
If we represent a sequence of statements by the letters \( p, q, r, \ldots \), then a **compound statement** may be constructed from \( p, q, r, \ldots \) using the logical operators \( \lor \) (‘or’), \( \land \) (‘and’), \( \neg \) (‘not’ – negation), \( \rightarrow \) (‘implies’) and \( \leftrightarrow \) (‘(logically) equivalent’). We call the statements \( p, q, r, \ldots \), **simple statements** (by analogy to chemistry, they are the *atoms* from which the compound statements are formed). A convenient way of determining the the truth value of a compound statement is to construct a **truth table**. A truth table is a listing of all possible combinations of the simple statements as true or false, along with the resulting truth value of the compound statement. It should be clear that a truth table for a compound statement involving \( n \) simple statements will necessarily have \( 2^n \) rows.

We now give the truth tables for each of the logical operators \( \lor \) (‘or’), \( \land \) (‘and’), \( \neg \) (‘not’ – negation), \( \rightarrow \) (‘implies’) and \( \leftrightarrow \) (‘(logically) equivalent’). We may regard these truth tables as the definitions of these operators.

\[
\begin{array}{c|c|c}
p & q & p \lor q \\
\hline
T & T & T \\
T & F & T \\
F & T & T \\
F & F & F \\
\end{array}
\quad
\begin{array}{c|c|c}
p & q & p \land q \\
\hline
T & T & T \\
T & F & F \\
F & T & F \\
F & F & F \\
\end{array}
\quad
\begin{array}{c|c}
p & \neg p \\
\hline
T & F \\
F & T \\
\end{array}
\quad
\begin{array}{c|c|c}
p & q & p \rightarrow q \\
\hline
T & T & T \\
T & F & F \\
F & T & T \\
F & F & T \\
\end{array}
\quad
\begin{array}{c|c|c}
p & q & p \leftrightarrow q \\
\hline
T & T & T \\
T & F & F \\
F & T & F \\
F & F & T \\
\end{array}
\]

**Theorem 2.** \( p \rightarrow q \) is logically equivalent to \( \neg p \lor q \).

**Proof.** The result follows by establishing that the last column of the following truth table is a tautology.

\[
\begin{array}{c|c|c|c|c|c|c}
p & q & p \rightarrow q & \neg p & \neg p \lor q & (p \rightarrow q) \leftrightarrow (\neg p \lor q) \\
\hline
T & T & T & F & T & T \\
T & F & F & F & F & T \\
F & T & T & T & T & T \\
F & F & T & T & T & T \\
\end{array}
\]

**Theorem 3.** \( p \leftrightarrow q \) is logically equivalent to \((p \rightarrow q) \land (q \rightarrow p)\).

**Proof.** Exercise (as for Theorem 2, use a truth table).

8 Logic with Quantifiers

The following are known as the **universal quantifier** and **existential quantifier**, respectively.

\( \forall \) (which is an inverted \( \mathbb{A} \)) means “for All”.

\( \exists \) (a back-to-front \( \mathbb{E} \)) means “there Exists”.

If \( P(x) \) represents a statement that depends on \( x \), then the following are logical equivalences:

\[
\exists x P(x) \leftrightarrow \neg \forall x (\neg P(x)) \\
\forall x P(x) \leftrightarrow \neg \exists x (\neg P(x)).
\]

Sometimes we write the quantifiers at the back of an expression rather than at the front. The meaning is the same, but a trailing ‘\( \exists x \)’ reads better as: ‘for some \( x \)”.

9 Propositions

The rules of Logic that we have seen in the previous two sections underpin the **propositions** of mathematics. We will define a **proposition** to be a **statement** that can be demonstrated to be true, (and by true we mean: *for all instances of the statement it is true*). In this context, it is customary to use ‘\( \implies \)’ rather than ‘\( \rightarrow \)’, and ‘\( \iff \)’ rather than ‘\( \leftrightarrow \)’.
Thus, if \( P \) and \( Q \) are statements then
\[
P \implies Q
\]
means: \( P \) implies \( Q \), i.e. that whenever \( P \) is true then \( Q \) must also be true. There are several other ways of saying this; simplest is just “If \( P \) then \( Q \)”. One can also say: “\( P \) only if \( Q \)” or switch them around and say: “\( Q \) if \( P \)” (symbolically: \( Q \iff P \)); or that: “\( P \) is a sufficient condition for \( Q \)” or that: “\( Q \) is a necessary condition for \( P \)”.

For example, if \( A \) is the statement “\( n \) is a prime” and \( B \) is the statement “\( n \) is a natural number” then \( A \implies B \) is a proposition.

Also, \( \neg P \) is the negation of \( P \), e.g. if \( A \) is the statement “\( n \) is a prime” then \( \neg A \) would mean “\( n \) is not a prime.”

Finally, if \( P \implies Q \) and \( Q \implies P \) we write: \( P \iff Q \) or \( P \text{ if and only if } Q \). Observe how this is made up of ‘\( P \) if \( Q \)’ \(( P \iff Q ) \) and ‘\( P \) only if \( Q \)’ \(( P \implies Q ) \).

We can also say \( P \) is a necessary and sufficient condition for \( Q \). A shorthand way of writing “if and only if” is the odd-looking word \( \text{iff} \).

The sort of propositions that are important in mathematics are theorems, corollaries (singular: corollary) and lemmas. Theorems are the most important: everybody knows about Pythagoras’ Theorem. In this course, (and in other advanced mathematics) a theorem appears in two parts. The first is a statement of the theorem, with some sort of label like “Theorem 5” or “Lagrange’s Theorem”. The second part is the proof of the theorem which begins with the word “Proof” and ends with the symbol \( \square \). Lemmas are (usually short, easy) propositions that are used to prove theorems; corollaries are propositions that follow easily from theorems.

**Definition 4.** The converse of \( P \implies Q \) is \( Q \implies P \).

Note that we might have \( P \implies Q \) being true but \( Q \implies P \) being false. Can you think of statements \( P \) and \( Q \) for which this is so?

**Definition 5.** The contrapositive of \( P \implies Q \) is \( \neg Q \implies \neg P \).

If \( P \implies Q \) is true then its contrapositive is true, and vice versa. Thus we can say for any statements \( P \) and \( Q \),
\[
P \implies Q \quad \text{iff} \quad \neg Q \implies \neg P.
\]

Logical statements come up frequently in the solution of engineering problems. Engineers like to choose capital letters \( A, B, C, \ldots \) rather than \( p, q, r, \ldots \), to represent \( \land \) by multiplication (so that \( A \land B \) is written \( AB \)), to represent \( \lor \) by addition (so that \( A \lor B \) is written \( A + B \)), and for \( \text{true} \) they write 1 and for \( \text{false} \) they write 0.

With the Engineering conventions and using a Carroll diagram, which the engineers call a Karnaugh map, as demonstrated in the lecture, try the following problems.

**Exercises.**

1. Prove that \( B + A(B + C) + BC = B + AC \).
2. Prove that \( C + A(C + B) + BC = C + AB \).
3. Prove that \( A + BC = (A + B)(A + C) \).
4. Prove that \( A + AB = A \).
5. Prove that \( (A + C)A + AC + C = A + C \).
6. Prove that \( BC + A(B + C) = AB + BC + AC \).
7. Let \( A, B, C, D \) represent the binary digits of a decimal number in the range 0 to 15. Construct a simplified expression that is a prime number checker, i.e. if \( f(A, B, C, D) \) is the expression then \( f(A, B, C, D) \) should return 1 exactly when \((ABCD)_{two}\) is the binary representation of a prime number less than 16.