Course Objectives

This course is meant to introduce you to various aspects of mathematics.

• You will be introduced to concepts in logic, set theory, number theory and abstract algebra.

• You will learn to read and produce formal proofs.

This course will conclude with a unit which applies what we have learned (in particular group theory) to coding theory. Although we won’t touch on them, the number theory we learn has pertinent applications to cryptography (e.g., see Section 1.6 on public key cryptography in the textbook).
Mathematics is founded on logic. The first, most basic form of logic is propositional logic (or symbolic logic) due to George Boole – the logic of and or without quantifiers or mathematical objects. The next layer of logic is first (and higher-order) logic which involves quantifiers, sets and functions. We start with propositional logic.

1.1 Propositions and Statements

Propositional logic is needed to make very basic mathematical arguments. Mathematical propositions, like “7 is prime”, have definite truth values and are the building blocks of propositional logic. Connectives like “and”, “or” and “not” join mathematical propositions into complex statements whose truth depends only on its constituent propositions. You can think of these statements as polynomials in propositions which act like variables. We want to know when two statements are logically equivalent, or when one implies the other. That is, we want to learn how to reason with mathematical statements.

Consider the following statement:

If the budget is not cut, then a necessary and sufficient condition for prices to remain stable is that taxes will be raised. Taxes will be raised only if the budget is not cut. If prices remain stable, then taxes will not be raised. Hence, taxes will not be raised.

Is this argument logically sound? That is, is the conclusion “taxes will not be raised” true if the premises of the statement are true? To answer this question, we need logic: “propositional calculus.”

Definition 1.1. A proposition is a sentence or assertion that is true (T) or false (F), but not both.

Example 1.2. Some (non-mathematical) propositions:

- $p$ = “prices will remain stable”
- $b$ = “the budget will be cut”
- $r$ = “taxes will be raised”
Definition 1.3. A statement is one of two things:

- a proposition, or
- (two) statements joined by a connective.

The above is a “recursive definition” in that it defines a statement in terms of other statements.

Example 1.4. If $p$ and $q$ are propositions then $p$ and $q$ are also statements. If $\land$ and $\lor$ are connectives then $p \land q$, $p \land p$, $p \lor q$, $(p \land q) \lor p$, and so on are all statements. You should think of these as “logical polynomials in $p$ and $q$”.

1.2 Connectives

Connectives (a.k.a. truth-functionals, or boolean operators) are functions that take one or more (say up to $n$) truth values and output a truth value: i.e., functions of the form

$$f : \{T,F\}^n \to \{T,F\}.$$

We now give a list of common connectives.

Definition 1.5 (Negation). Let $p$ be a proposition (or statement). The negation of $p$, denoted by $\neg p$, is the denial of $p$:

- If $p$ is T, then $\neg p$ is F.
- If $p$ is F, then $\neg p$ is T.

The definition of negation is summarized by the following truth table.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\neg p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The negation or “not” gate is depicted by

\[\text{Diagram of negation gate}\]
Definition 1.6 (Conjunction). Let $p$ and $q$ be two propositions. The conjunction of $p$ and $q$, denoted by $p \land q$, is another proposition whose truth values are defined by the following table:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \land q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Conjunction is also known as “and” and its gate is depicted by

![NOR gate](image)

Example 1.7. $r \land p = “taxes will be raised and prices will remain stable”$

Definition 1.8 (Disjunction). Let $p$ and $q$ be two propositions. The disjunction of $p$ and $q$, denoted by $p \lor q$, is another proposition whose truth values are defined by the following table:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \lor q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Disjunction is also called “or” and its gate is depicted by

![OR gate](image)

Definition 1.9 (Conditional). Let $p$ and $q$ be two propositions. The conditional of $p$ and $q$, denoted by $p \rightarrow q$, is another proposition whose truth values are defined by the following table:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \rightarrow q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>
In \( p \rightarrow q \), \( p \) is called the **antecedent** and \( q \) is called the **consequent** of the conditional. The conditional operation can be thought of as “implies.” So \( p \rightarrow q \) stands for “\( p \) implies \( q \),” “\( p \) is a sufficient condition for \( q \),” “if \( p \), then \( q \),” “\( q \) is a necessary condition for \( p \),” “\( q \) if \( p \)” and “\( p \) only if \( q \).”

One may question why this is the correct truth-table for our intuitive notion of “implies” (particularly the cases where \( p = F \)). Here are some explanations:

- The way we use implication is through modus ponens: If we know \( p \rightarrow q \) is true and we also know that \( p \) is true, then we should be able to deduce that \( q \) is true. This justifies the first line of the truth table.

- Next, consider what it means for \( p \rightarrow q \) to be false. The only time that \( p \rightarrow q \) should be false is if we have an instance where \( p \) is true, but \( q \) is false. We thus have the second line of the truth table.

- Instances where \( p \) is false do not provide evidence that \( p \) does not imply \( q \). To further justify the third and fourth lines of the truth table, observe that one would expect the proposition \( r \land s \rightarrow s \) to be always true; in this light, examining the truth table of \( r \land s \rightarrow s \), we obtain that when the antecedent \( r \land s \) is false no matter what the truth value of the consequent \( s \) is (either true or false), we have a true value for \( r \land s \rightarrow s \) (in this argument, \( r \land s \) stands for \( p \) and \( s \) stands for \( q \)).

It is hoped you will find that the above explanations provide a convincing justification of the table. With experience working with implications, it may become more natural. For now, you can also treat this as simply a definition.

**Definition 1.10** (Biconditional). Let \( p \) and \( q \) be two propositions. The **biconditional of \( p \) and \( q \)**, denoted by \( p \leftrightarrow q \), is another proposition whose truth values are defined by the following table:

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( p \leftrightarrow q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The biconditional operation can be thought of as “if and only if.”
The symbols $\neg, \land, \lor, \rightarrow, \leftrightarrow$ are called **connectives**, **truth functionals**, **boolean operators**, among other things.

The **converse** of $p \rightarrow q$ is $q \rightarrow p$.

The **inverse** of $p \rightarrow q$ is $\neg p \rightarrow \neg q$.

The **contrapositive** of $p \rightarrow q$ is $\neg q \rightarrow \neg p$. An implication is “logically equivalent” to its contrapositive (see Definition 1.15 for the definition of “logical equivalence”).

### 1.3 Valid Arguments

#### Example 1.11.

*If the budget is not cut, then a necessary and sufficient condition for prices to remain stable is that taxes will be raised. Taxes will be raised only if the budget is not cut. If prices remain stable, then taxes will not be raised. Hence, taxes will not be raised.*

Let $p$, $b$ and $r$ be the following propositions:

- $p = \text{“prices will remain stable”}$
- $b = \text{“the budget will be cut”}$
- $r = \text{“taxes will be raised”}$

We have the following premises:

- If the budget is not cut, then a necessary and sufficient condition for prices to remain stable is that taxes will be raised: $\neg b \rightarrow (p \leftrightarrow r)$
- Taxes will be raised only if the budget is not cut: $r \rightarrow \neg b$
- If prices remain stable, then taxes will not be raised: $p \rightarrow \neg r$

The conclusion is:

- Hence, taxes will not be raised: $(\neg r)$.

Is this argument valid?

A statement is called a **tautology** (or logical identity) if it is always true (i.e., it is true for all possible truth-value assignments of its propositions).
Example 1.12. \( s = p \lor \neg p \) is a tautology.

\[
\begin{array}{c|c|c}
 p & \neg p & p \lor \neg p \\
 T & F & T \\
 F & T & T \\
\end{array}
\]

A statement is called a **contradiction** (or fallacy) if it is always false.

Example 1.13. \( s = p \land \neg p \) is a contradiction.

\[
\begin{array}{c|c|c}
 p & \neg p & p \land \neg p \\
 T & F & F \\
 F & T & F \\
\end{array}
\]

**Definition 1.14** (Logical Implication). Let \( s \) and \( q \) be two statement forms involving the same set of propositions. We say that \( s \) **logically implies** \( q \) and write \( s \implies q \) if whenever \( s \) is true, \( q \) is also true (i.e., if every assignment of truth values making \( s \) true also makes \( q \) true).

**Definition 1.15** (Logical Equivalence). Let \( s \) and \( q \) be two statement forms involving the same set of propositions. We say that \( s \) **logically equivalent** \( q \) and write \( s \iff q \) if both \( s \) and \( q \) have identical truth tables (i.e., for all truth assignments of their propositions).

Note that \( \implies \) and \( \iff \) are logical relationships between statements, while \( \rightarrow \) and \( \leftrightarrow \) are connective operators used to make statements.

Example 1.16.

- \( s = p \rightarrow p \) is a tautology.

\[
\begin{array}{c|c}
p & p \rightarrow p \\
T & T \\
F & T \\
\end{array}
\]

- If we suppose \( s = (p \rightarrow q) \rightarrow p \) and \( r = p \lor q \) then \( s \implies r \).

\[
\begin{array}{c|c|c|c|c}
p & q & p \rightarrow q & (p \rightarrow q) \rightarrow p & r = p \lor q \\
T & T & T & T & T \\
T & F & F & T & T \\
F & T & T & F & T \\
F & F & T & F & F \\
\end{array}
\]

Notice that whenever is \( s \) is true, \( r \) is also true. Thus, \( s \) logically implies \( r \).
Example 1.17. Consider the two statements \( s = p \lor q \) and \( r = \neg(p \leftrightarrow q) \). First note that \( r \) has the same truth-table as a boolean operator called “exclusive or” (xor). The importance of xor is that it corresponds to binary addition.

Now, look at the truth tables below. For every truth-assignment that makes \( r \) true, we also have that \( s \) is true. Thus \( r \) logically implies \( s \); \( r \Rightarrow s \).

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( r = \neg(p \leftrightarrow q) )</th>
<th>( s = p \lor q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Exercise 1.18.

• Show that \((p \rightarrow q) \iff \neg p \lor q\).

• Show that \((p \leftrightarrow q) \iff (\neg p \lor q) \land (\neg q \lor p)\).

Theorem 1.19. Let \( s \) and \( r \) be two statements in the same propositions.

(i) \( s \iff r \) if and only if \( s \iff r \) is a tautology.

(ii) \( s \Rightarrow r \) if and only if \( s \rightarrow r \) is a tautology.

(iii) \( s \iff r \) if and only if \( s \Rightarrow r \) and \( r \Rightarrow s \).

Proof.

(i) If \( s \iff r \) then \( s \) and \( r \) take the same values for every truth-assignment to their propositions. Thus, for a given truth-assignment, we either have \( s = r = T \) in which case \( s \iff r \) is true, or \( s = r = F \) in which case \( s \iff r \) is true. Since \( s \iff r \) is true for all truth assignments, it is a tautology. A similar argument works for the converse.

(ii) If \( s \Rightarrow r \) then whenever a truth-assignment yields \( s = T \), then the same truth assignment gives \( r = T \). Thus, for a given truth assignment, \( s \) is either false and hence \( s \rightarrow r \) is true, or \( s \) is true and consequently \( r \) and \( s \rightarrow r \) are true. A similar analysis of the cases tells us that if \( s \rightarrow r \) is a tautology then \( s \Rightarrow r \).
(iii) We know $s \iff r$ means that $s$ and $r$ always take the same truth-value on any assignment to their proposition. So, it’s clear that $s \iff r$ implies $s \implies r$ and $r \implies s$.

Now assume that both $s \implies r$ and $r \implies s$. Since $s \implies r$, whenever $s$ is true, $r$ is also true. Whenever a truth assignment gives $s = F$, then since $r \implies s$, $r$ must also be false. Thus $s$ and $r$ must have the same value for all truth-assignments. That is $s \iff r$.

\[\square\]

**Definition 1.20.** An argument with premises $p_1, \ldots, p_n$ and conclusion $q$ is **valid** if $p_1 \land \cdots \land p_n \implies q$.

**Example 1.21.** The argument in our motivating example was

$$(\neg b \to (p \leftrightarrow r)) \land (r \to \neg b) \land (p \to \neg r) \implies \neg r.$$

In order to show that it is a valid argument, it suffices to show that

$$s = [(\neg b \to (p \leftrightarrow r)) \land (r \to \neg b) \land (p \to \neg r)] \to \neg r$$

is a tautology. We can do this by examining all $2^3 = 8$ possible values for $b, p$ and $r$, and verify that, on each truth-assignment, $s$ is true.

Here’s a second approach: We will prove that $s$ is a tautology by contradiction. In a proof by contradiction, you make an unfounded assumption and look at the logical implications of that assumption. If, using that assumption, we can show something absurd (i.e., false), then we will know that the assumption is false.

In our case, we’ll assume that $s$ is **not** a tautology. If we can prove a false statement, then we’ll know that our assumption was wrong: we’ll have proven that $s$ is a tautology.

Assume that $s$ is not a tautology. Let

$$q_1 = \neg b \to (p \leftrightarrow r)$$
$$q_2 = r \to \neg b$$
$$q_3 = p \to \neg r$$

so that $s = (q_1 \land q_2 \land q_3) \to \neg r$. Since $s$ is not a tautology, there must be a truth-assignment making $\neg r = F$ and $q_1 = q_2 = q_3 = T$. Since $\neg r = F$,
we know \( r = T \) in our truth-assignment. Further, since \( q_3 = T \), we have \( T = p \rightarrow \lnot r = p \rightarrow F \) and therefore, we must have \( p = F \). As \( T = q_2 = r \rightarrow \lnot b \) and \( r = T \), we conclude that \( \lnot b = T \) and hence \( b = F \).

So, we’ve determined the truth assignment that makes \((q_1 \land q_2 \land q_3) \rightarrow \lnot r = F\); it’s \( b = F, p = F \) and \( r = T \). However, with this truth assignment, \( q_1 = T \rightarrow (F \leftrightarrow T) = T \rightarrow F = F \) which shows that \( s = T \). This contradicts our choice of truth-assignment as one that makes \( s = F \). Thus our assumption must have been wrong: \( s \) is a tautology. Consequently, the original argument is valid.

### 1.4 Logical Identities

The logical identities listed in the theorem below allow you to manipulate a statement into another form that is logically equivalent to the original.

**Theorem 1.22.** The following logical identities hold for all statements \( p, q, r \).

\[
\begin{align*}
p \land p & \iff p & \text{Idempotence} \\
p \lor p & \iff p \\
p \land \lnot p & \iff F & \text{Contradiction} \\
p \lor \lnot p & \iff T & \text{Tautology} \\
p \land F & \iff F \\
p \land T & \iff p \\
p \lor T & \iff T \\
p \lor F & \iff p \\
p \land q & \iff q \land p & \text{Commutativity} \\
p \lor q & \iff q \lor p \\
p \land (q \land r) & \iff (p \land q) \land r & \text{Associativity} \\
p \lor (q \lor r) & \iff (p \lor q) \lor r \\
\lnot(p \land q) & \iff (\lnot p) \lor (\lnot q) & \text{DeMorgan’s Laws} \\
\lnot(p \lor q) & \iff (\lnot p) \land (\lnot q) \\
\lnot\lnot p & \iff p & \text{Double Negation} \\
p \land (q \lor r) & \iff (p \land q) \lor (p \land r) & \text{Distributivity} \\
p \lor (q \land r) & \iff (p \lor q) \land (p \lor r) 
\end{align*}
\]
\((p \rightarrow q) \iff (\neg q \rightarrow \neg p)\) \hspace{1cm} \text{Contrapositive}

\(p \land (p \lor q) \iff p\) \hspace{1cm} \text{Absorption}

\(p \lor (p \land q) \iff p\)

**Proof.** Write out the truth tables replacing \(\iff\) with \(\leftrightarrow\) and check that you get a tautology in each case.

**Example 1.23.** The logic circuit for the statement \((a \land c) \lor [\neg (a) \lor b]\) has three inputs \((a, b, c)\) and one output (the value of the statement) and four gates \((\land, \lor, \neg, \lor)\).

We can find a logically equivalent statement with fewer gates:

\[
(a \land c) \lor [\neg (a) \lor b] \iff [(a \land c) \lor (\neg a)] \lor b \quad \text{using associativity}
\]

\[
\iff [(\neg a) \lor (a \land c)] \lor b \quad \text{using commutativity}
\]

\[
\iff [(\neg a \lor a) \land (\neg a \lor c)] \lor b \quad \text{using distributivity}
\]

\[
\iff (T \land (\neg a \lor c)) \lor b \quad \text{using tautology}
\]

\[
\iff [(\neg a) \lor c] \lor b \quad \text{using the sixth identity}
\]

This abruptly ends our discussion of propositional logic. We’ve learned about propositions, statements, and connectives. We have one theorem which relates the conditional and biconditional connectives to logical implication and logical equivalence. This theorem lets us prove statements of the form \(s \Rightarrow r\) by showing that \(s \rightarrow r\) is a tautology — something that can be checked in the truth-table. We’ve also given an example of how one can prove a statement is tautological without using the truth-table (see Example 1.21). Finally, we have a list of rules for manipulating statements into other logically equivalent statements. Using the distributive property, we see that we can expand statements easily, but that logically equivalent statements, even when expanded, can take different forms.

In our last example, Example 1.23, we suggest that we might be able to factor statements to get them into some minimal form. This is, in fact, a difficult task. You might want to read Wikipedia’s articles on circuit minimization and Karnaugh maps.

The breakthrough connection between electrical switching circuits and symbolic logic was made by Claude Elwood Shannon in 1938, playing a catalyst role in the digital revolution. Shannon went on in the late 1940s to found the field of information theory, making him regarded as the father of the information age.
As a final note, I suggest you read Section 3.3 of the textbook. It contains a lot of practical advice on how to prove statements in mathematics. This is a skill that we’ll try to hone throughout the rest of this course.