Proofs

Chapter 1
Rules of Inference

To prove mathematical statements, we must give valid arguments for them:

1. Start with statements we already know are true
2. Deduce new true statements from the ones we already know
3. Reach a conclusion

**Rules of Inference:**
The means for deducing new true statements.

e.g.

1. If you know your eCampus password, **then** you can see your grade.
2. You know your eCampus password.
3. **Conclusion:** You can see your grade.

If $p \rightarrow q$ is true and $p$ is true, then $q$ is true.
Rules of inference
Templates

Rules of Inference

Rules of inference have templates for constructing arguments.

1. Start with a collection of propositions, \( p_1, p_2, \ldots, p_n \): the premises
2. End with another proposition, \( q \): the conclusion.

*Let’s review!*
Rules of Inference

- Modus Ponens
- Modus Tollens
- Hypothetical syllogism
- Disjunctive syllogism
- Addition
- Simplification
- Conjunction
- Resolution

Modus Ponens

* Latin for: *mode that affirms*

The tautology \([p \land (p \rightarrow q)] \rightarrow q\) is the basis of the rule of inference.

\[
\begin{align*}
p \\
p \rightarrow q \\
\hline \\
\therefore q
\end{align*}
\]
Modus Tollens

* Latin for: method of denying

\[ \neg q \]
\[ p \rightarrow q \]
---------
\[ \therefore \neg p \]

\[ (\neg q \land (p \rightarrow q)) \rightarrow \neg p \]

Hypothetical syllogism

\[ p \rightarrow q \]
\[ q \rightarrow r \]
---------
---------
\[ \therefore p \rightarrow r \]

\[ (p \rightarrow q \land q \rightarrow r) \rightarrow (p \rightarrow r) \]
Disjunctive syllogism

\[ p \lor q \\
\neg p \\
\hline \\
\therefore q \]

\[ ((p \lor q) \land \neg p) \rightarrow q \]

Addition

\[ p \\
\hline \\
\therefore p \lor q \]

\[ p \rightarrow p \lor q \]
Simplification

\[ p \land q \]

--------

\[ \therefore p \]

\[ p \land q \rightarrow p \]

Conjunction

\[ p \]

\[ q \]

----------

----------

\[ \therefore p \land q \]

\[ [(p) \land (q)] \rightarrow p \land q \]
Resolution

\[ p \lor q \]
\[ \neg p \lor r \]
\[------------- \]
\[ \therefore q \lor r \]

\[ [(p \lor q) \land (\neg p \lor r)] \rightarrow q \lor r \]

e.g.:
Either you know the password or you use your fingerprint.
Either you don’t know password or you buy a new laptop.
\[ \therefore \] Either you use your fingerprint or you buy a new laptop.

Fallacies

- **Fallacy** = error in reasoning that results in an **invalid argument**
- Types:
  1. Converse Error
  2. Inverse Error
Converse Error

\[ \begin{align*}
  p & \rightarrow q \\
  q \\
  \hline
  \therefore p
\end{align*} \]

Let \( p = \) it rains, \( q = \) the grass is wet

If it rains, then the grass will be wet
The grass is wet
\( \therefore \) It rained

The grass could be wet from another source

Converse Error – Truth Table

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

Observe the critical rows where the conclusion is false. This argument form is invalid.
Inverse Error

\[ p \rightarrow q \\
\neg p \\
\hline \\
\therefore \neg q \]

Let \( p = \) it rains, \( q = \) the grass is wet
If it rains, then the grass will be wet
It is not raining
\( \therefore \) The grass is not wet
The grass could be wet from another source

Inverse Error – Truth Table

<table>
<thead>
<tr>
<th>Premises</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p \</td>
<td></td>
</tr>
<tr>
<td>( q \</td>
<td></td>
</tr>
<tr>
<td>( p \rightarrow q \</td>
<td></td>
</tr>
<tr>
<td>( \neg p \</td>
<td></td>
</tr>
<tr>
<td>( \neg q \</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Observe the critical rows where the conclusion is false.
This argument form is invalid.
Example

Is the following argument valid or invalid?

- If you invest in the Bitcoin, then you get rich.
- You did not invest in Bitcoin.
- Therefore, you did not get rich.

Application of rules of Inference

Suppose we know these facts about a program:

1. $x$ is not equal to 5 and $x$ is greater than $y$.
2. If $y$ is prime, then $x$ equals 5.
3. If $y$ is not prime, then $z$ is odd.
4. If $z$ is odd, then $z$ is less than $x$.

Can we conclude that $z$ is less than $x$?
Application of rules of Inference

Let’s use propositional variables instead:

\( p \): “\( x \) equals 5”
\( q \): “\( x \) is greater than \( y \)”
\( r \): is “\( y \) is prime”
\( s \): “\( z \) is odd”
\( t \): “\( z \) is less than \( x \)”

Formalize the premises as propositions:

(a) \( \neg p \land q \)
(b) \( r \rightarrow p \)
(c) \( \neg r \rightarrow s \)
(d) \( s \rightarrow t \)

The conclusion is the proposition \( t \).
Proof

A proof is a valid argument that establishes the truth of a mathematical statement.

**Formal proof:**
Every step is the application of just one rule

**Informal proof:**
Combine multiple steps in one step

Example

This chapter focuses on mathematical statements
e.g. If $5x + 2 = 27$, then $x = 5$
This is a mathematical statement
You could prove this by applying algebra
Application to Computer Science and Engineering

We need to develop programs to solve mathematical problems
• Not just addition, subtraction, etc., but problems that require mathematical \textit{methods}
• e.g. graphics, security analysis, modeling, data analysis

We need to determine if our programming approach can solve our problem!

Assumptions

• The basic laws of algebra apply
• The following properties of equality apply:
  – \( A = A \)
  – If \( A = B \), then \( B = A \)
  – If \( A = B \) and \( B = C \), then \( A = C \)
• The set of all integers \((\mathbb{Z})\) is \textit{closed} under addition, subtraction, and multiplication
Even and Odd Integers

We are looking at integers (set $\mathbb{Z}$)

An integer $n$ is **even** iff $n = \text{twice some integer}$

Formally: $n$ is even $\iff \exists \ k \in \mathbb{Z} \mid n = 2k$

An integer $n$ is **odd** iff $n = \text{twice some integer plus one}$

Formally: $n$ is odd $\iff \exists \ k \in \mathbb{Z} \mid n = 2k + 1$

Prime and Composite Integers

An integer $n$ is prime iff $n>1$ and for all positive integers $r$ and $s$, if $n = rs$, then either $r$ or $s$ equals $n$

More formally: $n$ is prime $\iff (n>1) \land (\forall \ r, s \in \mathbb{Z}^+, (n=rs) \rightarrow (r = 1 \land s=n) \lor (s=1 \land r=n))$

An integer $n$ is composite iff $n>1$ and there exists some integers $r, s (1<r<n, 1<s<n)$ where $n = rs$

More formally: $n$ is composite $\iff (n>1) \land (\exists \ r, s \in \mathbb{Z}^+, (1<r<n, 1<s<n) \land n = rs)$
Proving Existential Statements

\[ \exists x \in D \text{ such that } Q(x) \text{ is true iff } Q(x) \text{ is true for at least one } x \text{ in } D. \]

One way to prove this is to find an \( x \) in \( D \) that makes \( Q(x) \) true.
Another way is to give a set of directions for finding such an \( x \).
Both of these methods are called \textit{constructive proofs of existence}.

Example

\textbf{Prove}: \( \exists \) even integer \( n \) that can be written as a sum of two composite numbers

We need to find \textbf{at least one} \( n \) where this is true.

Composite numbers are 4,6,8,9,10,12…

\( 4 + 6 = 10 \), let \( n = 10 \). So this is true.
Disproving Universal Statements by Counterexample

To disprove a statement means to show that it is **false**.

**Disprove:** \( \forall x \in D, \text{ if } P(x) \text{ then } Q(x) \)

Showing that this statement is **false** is equivalent to showing that its negation is **true**.

The negation of the statement is existential: \( \exists x \in D \text{ such that } P(x) \text{ and not } Q(x) \).

Example

Given the following statement:

\( \forall x,y \in \mathbb{R}, \ (x^2 = y^2) \rightarrow (x = y) \)

Find a **counterexample** to disprove this statement

\( \exists x,y \in \mathbb{R} \mid (x^2 = y^2) \land \sim(x = y) \)

So let \( x = -2, y = 2 \)

\( x^2 = y^2 \rightarrow (-2)^2 = 4, 2^2 = 4, \text{ so } 4 = 4 \)

**But**, \( -2 \neq 2, \text{ so } \sim(x = y) \)
Proving Universal Statements

How to prove a universal statement?

The majority of mathematical statements to be proved are universal.

\[ \forall x \in D, \text{ if } P(x) \text{ then } Q(x) \]

When \( D \) is finite or when only a finite number of elements satisfy \( P(x) \), such a statement can be proved by the method of exhaustion.

Method of Exhaustion

\( \forall n \in \mathbb{Z}, \text{ if } n \text{ is even and } 4 \leq n \leq 16, \text{ then } n \text{ can be written as a sum of two prime numbers. Prime numbers are } 2, 3, 5, 7, 11, 13 \)

<table>
<thead>
<tr>
<th>n</th>
<th>sum of primes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2+2</td>
</tr>
<tr>
<td>6</td>
<td>3+3</td>
</tr>
<tr>
<td>8</td>
<td>3+5</td>
</tr>
<tr>
<td>10</td>
<td>3+7</td>
</tr>
<tr>
<td>12</td>
<td>5+7</td>
</tr>
<tr>
<td>14</td>
<td>7+7</td>
</tr>
<tr>
<td>16</td>
<td>5+11</td>
</tr>
</tbody>
</table>
Application to Computer Science

- We could “exhaustively” run a program to test all cases.
- For large data sets, it would take a “long” time (many years even with the fastest computer)
- We need a shortcut to verify the operation of our program.

Proving Universal Statements

By using the method of generalizing from the generic particular, we can then use the method of **direct proof** to prove *universal* statements
Method of Direct Proof

1. Express the statement to be proved in the form “\( \forall x \in D, \text{ if } P(x) \text{ then } Q(x) \)"

2. Start the proof by supposing that \( x \) is a particular but arbitrarily chosen element of \( D \) for which the hypothesis \( P(x) \) is true

3. Show that the conclusion \( Q(x) \) is true by use of definitions, algebra, and rules of logical inference

Direct Proof Template

1. Suppose variable(s) are [particular but arbitrarily chosen] type of numbers.

2. Use definitions, substitutions, and rules of algebra to prove

3. Conclude
Direct Proof Example

Prove the following statement:

"The sum of any two odd integers is even"

**Proof:** Suppose \( m \) and \( n \) are any [particular but arbitrarily chosen] odd integers. [We must show that \( m + n \) is even]

By definition of odd, there exist integers \( r \) and \( s \) such that \( m = 2r+1 \) and \( n = 2s+1 \)

by substitution

\[
m + n = (2r+1) + (2s + 1) = 2r + 2s + 2 = 2(r + s + 1)
\]

\( u = r + s + 1 \) is an integer
End