Logic and Proof
An argument is a sequence of statements.
All statements but the first one are called assumptions or hypothesis.
The final statement is called the conclusion.
An argument is valid if:

whenever all the assumptions are true, then the conclusion is true.

If today is Wednesday, then yesterday is Tuesday.

Today is Wednesday.

\[ \therefore \text{ Yesterday is Tuesday.} \]
Modus Ponens

If p then q.

\[
p \quad \therefore \quad q
\]

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>( p \rightarrow q )</th>
<th>p</th>
<th>q</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Modus ponens is Latin meaning “method of affirming”.
Modus Tollens

If $p$ then $q$.

\[ \sim q \]

\[ \therefore \sim p \]

Modus tollens is Latin meaning "method of denying".
A student is trying to prove that propositions \( P, Q, \) and \( R \) are all true. She proceeds as follows.

First, she proves three facts:

- \( P \) implies \( Q \)
- \( Q \) implies \( R \)
- \( R \) implies \( P \)

Then she concludes,

``Thus \( P, Q, \) and \( R \) are all true.''

---

**Proposed argument:**

\[
\begin{align*}
(P \rightarrow Q), \quad (Q \rightarrow R), \quad (R \rightarrow P) \\
\hline
P \land Q \land R
\end{align*}
\]
Valid Argument?

Conclusion true whenever all assumptions are true.

<table>
<thead>
<tr>
<th>assumptions</th>
<th>conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To prove an argument is not valid, we just need to find a counterexample.
Valid Arguments?

If \( p \) then \( q \).
\[
\begin{align*}
q \\
\therefore p
\end{align*}
\]

If you are a fish, then you drink water.
You drink water.
You are a fish.

If \( p \) then \( q \).
\[
\begin{align*}
\neg p \\
\therefore \neg q
\end{align*}
\]

If you are a fish, then you drink water.
You are not a fish.
You do not drink water.
Exercises

\[ p \]
\[ \therefore \quad p \lor q \]
\[ p \land q \]
\[ \therefore \quad p \]
\[ p \lor q \]
\[ \neg q \]
\[ \therefore \quad p \]

\[ p \]
\[ \therefore \quad p \land q \]
\[ p \lor q \]
\[ \therefore \quad p \]
\[ p \lor q \]
\[ q \rightarrow r \]
\[ \therefore \quad p \rightarrow r \]
More Exercises

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

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

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

\[ 1 = -1 \]
\[ \therefore \text{Today is Tuesday.} \]
Contradiction

\[ \neg p \rightarrow c \]

\[ \therefore p \]

If you can show that the assumption that the statement \( p \) is false leads logically to a contradiction, then you can conclude that \( p \) is true.

You are working as a clerk.

If you have won Mark 6, then you would not work as a clerk.

\[ \therefore \text{You have not won Mark 6.} \]
Arguments with Quantified Statements

Universal instantiation:
\[ \forall x, P(x) \]
\[ P(a) \]

Universal modus ponens:
\[ \forall x, P(x) \rightarrow Q(x) \]
\[ P(a) \]
\[ \therefore Q(a) \]

Universal modus tollens:
\[ \forall x, P(x) \rightarrow Q(x) \]
\[ \neg Q(a) \]
\[ \therefore \neg P(a) \]
Universal Generalization

\[ A \rightarrow R(c) \]
\[ \frac{}{A \rightarrow \forall x.R(x)} \]

valid rule

providing \( c \) is independent of \( A \)

e.g. given any number \( x \), \( 2x \) is an even number

\[ \Rightarrow \] for all \( x \), \( 2x \) is an even number.
Not Valid

\[ \forall z \ [ Q(z) \lor P(z) ] \rightarrow [ \forall x. Q(x) \lor \forall y. P(y) ] \]

Proof: Give countermodel, where

\[ \forall z \ [ Q(z) \lor P(z) ] \text{ is true,} \]

but \[ \forall x. Q(x) \lor \forall y. P(y) \] is false.

Find a domain, and a predicate.

In this example, let domain be integers,

\[ Q(z) \text{ be true if } z \text{ is an even number, i.e. } Q(z)=\text{even}(z) \]

\[ P(z) \text{ be true if } z \text{ is an odd number, i.e. } P(z)=\text{odd}(z) \]
Validity

\[ \forall z [Q(z) \land P(z)] \rightarrow [\forall x. Q(x) \land \forall y. P(y)] \]

Proof strategy: We assume \( \forall z [Q(z) \land P(z)] \)
and prove \( \forall x. Q(x) \land \forall y. P(y) \)
Proof and Logic

We prove mathematical statement by using logic.

\[
P \rightarrow Q, \quad Q \rightarrow R, \quad R \rightarrow P
\]

\[
P \land Q \land R \quad \text{not valid}
\]

To prove something is true, we need to assume some **axioms**!

This is invented by Euclid in 300 BC, who begins with 5 assumptions about geometry, and derive many theorems as logical consequences.

http://en.wikipedia.org/wiki/Euclidean_geometry
Proofs
Proving an Implication

Goal: If $P$, then $Q$.  ($P$ implies $Q$)

Method 1: Write assume $P$, then show that $Q$ logically follows.

Claim: If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$
Proving an Implication

Goal: If P, then Q. (P implies Q)

Method 1: Write assume P, then show that Q logically follows.

Claim: If r is irrational, then \( \sqrt{r} \) is irrational.

How to begin with?

What if I prove “If \( \sqrt{r} \) is rational, then \( r \) is rational”, is it equivalent?

Yes, this is equivalent; proving “if P, then Q” is equivalent to proving “if not Q, then not P”.
Proving an Implication

Goal: If P, then Q. (P implies Q)

Method 2: Prove the *contrapositive*, i.e. prove "not Q implies not P".

Claim: If r is irrational, then √r is irrational.
Proving an “if and only if”

**Goal:** Prove that two statements P and Q are “logically equivalent”, that is, one holds if and only if the other holds.

**Example:**
An integer is a multiple of 3 if and only if the sum of its digits is a multiple of 3.

**Method 1:** Prove P implies Q and Q implies P.

**Method 1’:** Prove P implies Q and not P implies not Q.

**Method 2:** Construct a chain of if and only if statement.
Proof the Contrapositive

Statement: If $m^2$ is even, then $m$ is even

Try to prove directly.
Proof the Contrapositive

Statement: If $m^2$ is even, then $m$ is even

Contrapositive: If $m$ is odd, then $m^2$ is odd.

Proof (the contrapositive):
Proof by Contradiction

\[ \overline{P} \rightarrow F \]
\[ \overline{P} \]
\[ P \]

To prove \( P \), you prove that not \( P \) would lead to ridiculous result, and so \( P \) must be true.

You are working as a clerk.
If you have won Mark 6, then you would not work as a clerk.
\[ \therefore \text{ You have not won Mark 6.} \]
Proof by Contradiction

**Theorem:** \( \sqrt{2} \) is irrational.

**Proof (by contradiction):**
**Proof by Contradiction**

**Theorem:** $\sqrt{2}$ is irrational.

**Proof (by contradiction):**

- Suppose $\sqrt{2}$ was rational.
- Choose $m, n$ integers without common prime factors (always possible) such that $\sqrt{2} = \frac{m}{n}$
- Show that $m$ and $n$ are both even, thus having a common factor 2, a contradiction!
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Proof (by contradiction): Want to prove both $m$ and $n$ are even.
Proof by Contradiction

**Theorem:** \( \sqrt{2} \) is irrational.

Proof (by contradiction):

Want to prove both \( m \) and \( n \) are even.

\[
\sqrt{2} = \frac{m}{n}
\]

\[
\sqrt{2} \cdot n = m
\]

\[
2n^2 = m^2
\]

so \( m \) is even.

so can assume \( m = 2l \)

\[
m^2 = 4l^2
\]

\[
2n^2 = 4l^2
\]

\[
n^2 = 2l^2
\]

so \( n \) is even.
Proof by Cases

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

e.g. want to prove a nonzero number always has a positive square.

\[ x \text{ is positive or } x \text{ is negative} \]
\[ \text{if } x \text{ is positive, then } x^2 > 0. \]
\[ \text{if } x \text{ is negative, then } x^2 > 0. \]
\[ \therefore x^2 > 0. \]
Rational vs Irrational

**Question:** If a and b are irrational, can $a^b$ be rational??

We know that $\sqrt{2}$ is irrational, what about $\sqrt{2} \sqrt{2}$?

**Case 1:** $\sqrt{2} \sqrt{2}$ is rational

**Case 2:** $\sqrt{2} \sqrt{2}$ is irrational

So in either case there are a, b irrational and $a^b$ be rational.

We don’t need to know which case is true!
Extra
Power and Limits of Logic

Good news: Gödel's Completeness Theorem

Only need to know a few axioms & rules, to prove all validities.

That is, starting from a few propositional & simple predicate validities, every valid assertion can be proved using just universal generalization and modus ponens repeatedly!

\[
\text{modus ponens} \quad \begin{array}{c} P \rightarrow Q, P \end{array} \quad \hline Q
\]
Thm 2, bad news:

Given a set of axioms,

there is no procedure that decides

whether quantified assertions are valid.

(unlike propositional formulas).
Thm 3, worse news:
For any “reasonable” theory that proves basic arithmetic truth, an arithmetic statement that is true, but not provable in the theory, can be constructed.

No hope to find a complete and consistent set of axioms!

An excellent project topic:
Application: Logic Programming
Other Applications

Digital logic:

Database system:

Making queries

Data mining