Propositional Logic

A proposition is a declarative sentence that is either true or false, but not both.

Examples

<table>
<thead>
<tr>
<th>Proposition</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 + 1 = 2</td>
<td>yes, true</td>
</tr>
<tr>
<td>2 + 2 = 3</td>
<td>yes, false</td>
</tr>
<tr>
<td>read this carefully</td>
<td>no, not declarative</td>
</tr>
<tr>
<td>x + 1 = 2</td>
<td>no, neither true, non-false</td>
</tr>
</tbody>
</table>

Proposition variables: variables, denoted by letters, that represent propositions.

Truth value of a proposition:

T, for a true proposition
F, for a false proposition

Propositional logic or propositional calculus: logic that deals with propositions.
Compound propositions: propositions formed from existing propositions using logic operators.

Logic operators:

1. Negation ($\neg$)
   - Given proposition $p$, proposition $\neg p$ (or $\overline{p}$) is the negation of $p$.

2. Conjunction (AND, ∧)
   - Given propositions $p$ and $q$, $p \land q$ is the conjunction of $p$ and $q$.
     - $p \land q$ is true, if both $p$ and $q$ are true.
     - false, otherwise.

3. Disjunction (OR, ∨)
   - Given propositions $p$ and $q$, $p \lor q$ is the disjunction of $p$ and $q$.
     - $p \lor q$ is false, if both $p$ and $q$ are false.
     - true, otherwise.
4) Exclusive OR (⊕)

Given propositions p and q, \( p \oplus q \) is the exclusive or of p and q.

\( p \oplus q \) is true, if exactly one of p and q is true, otherwise.

\[ p \oplus q = (p \land \neg q) \lor (\neg p \land q) \]

Truth Tables:

<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>

<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>

<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>

<table>
<thead>
<tr>
<th>P</th>
<th>q</th>
<th>p \oplus q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</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>
5. **Conditional Statement** (implication, \(\rightarrow\))

Let \(p\) and \(q\) be propositions. The conditional statement \(p \rightarrow q\) is the proposition "if \(p\) then \(q\)."

\(p \rightarrow q\) is

- false, if \(p\) is true and \(q\) is false
- true, otherwise

In \(p \rightarrow q\), \(p\) is called the **hypothesis**, and \(q\) is called the **conclusion**.

A conditional statement is also called an **implication**.

**Truth 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>

\(p \rightarrow q = (\neg p) \lor q\)

**Note:** if \(p\) is false, then \(p \rightarrow q\) is true.
A variety of terminology is used to express $p \Rightarrow q$ in mathematical reasoning.

We use notation $u \equiv v$ to denote that propositions $u$ and $v$ are logically equivalent (i.e., $u$ and $v$ have the same truth value)

"if $p$ then $q$"
\equiv "$q$ follows from $p$"
\equiv "$p$ is a sufficient condition of $q$"

"if $p$ then $q$"
\equiv "$p$ cannot be true if $q$ is false"
\equiv "$q$ is a necessary condition of $p$"
\equiv "$p$ only if $q$"
Example: \( p: a > b \text{ and } c > d \)

\( g: a + c > b + d \)

where \( a, b, c, d \) are real numbers

\[ p \rightarrow g \]

\[ \equiv \text{"if } a > b \text{ and } c > d \text{ then } a + c > b + d \"} 

\[ \equiv \text{"} a > b \text{ and } c > d \text{ is a sufficient condition for } a + c > b + d \"} 

\[ \equiv \text{"} a > b \text{ and } c > d \text{ only if } a + c > b + d \"} 

\[ \equiv \text{"} a + c > b + d \text{ is a necessary condition for } a > b \text{ and } c > d \"} 

\[ a = 2 \neq 5 = b \quad c = 5 > 1 = d \]

but \( a + c = 7 > 6 = b + d \). Thus, \( a + c > b + d \) is necessary but not sufficient for \( a > b \) and \( c > d \).
9 \implies p \text{ is the converse of } p \implies q
\neg q \implies \neg p \text{ is the contrapositive of } p \implies q
\neg p \implies \neg q \text{ is the inverse of } p \implies q

Note: p \implies q \equiv \neg q \implies \neg p

Verification: \neg q \implies \neg p \text{ is false only if }
\neg q \text{ is true and } \neg p \text{ is false}

\begin{array}{|c|c|c|c|}
\hline
p & q & p \implies q & \neg q \implies \neg p \\
\hline
T & T & T & T \\
T & F & F & F \\
F & T & T & T \\
F & F & T & T \\
\hline
\end{array}
Given propositions $p$ and $q$. The biconditional statement $p \leftrightarrow q$ is the proposition "$p$ if and only if $q$".

$p \leftrightarrow q$ is true, when $p$ and $q$ have the same truth values.

$p \leftrightarrow q$ is false, otherwise.

$p \leftrightarrow q$ is true, if both $p \rightarrow q$ and $q \rightarrow p$ are true.

$p \leftrightarrow q$ is false, otherwise.

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

Other ways to express $p \leftrightarrow q$:

"$p$ is necessary and sufficient for $q$"

"if $p$ then $q$, and conversely"

"$p$ iff $q$"
Example \[ a = 2^k \iff k = \log_2 a \]

\[ \begin{align*}
 p & \rightarrow q : \quad a = 2^k \rightarrow k = \log_2 a \\
 q & \rightarrow p : \quad k = \log_2 a \rightarrow a = 2^k
\end{align*} \]

Precedence of logical operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \neg )</td>
<td>1</td>
</tr>
<tr>
<td>( \land )</td>
<td>2</td>
</tr>
<tr>
<td>( \lor )</td>
<td>3</td>
</tr>
<tr>
<td>( \rightarrow )</td>
<td>4</td>
</tr>
<tr>
<td>( \iff )</td>
<td>5</td>
</tr>
</tbody>
</table>

Example \[ p \lor q \land \neg r \]

is the same as \[ p \lor (q \land (\neg r)) \]

Parentheses are used when necessary.
(to make the evaluation order clear)
Truth tables of Compound propositions

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( \neg q )</th>
<th>( p \lor \neg q )</th>
<th>( p \land q )</th>
<th>( (p \lor \neg q) \rightarrow (p \land q) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Tautology, Contradiction, Contingency

A compound proposition that is always true is called a **tautology**.

A compound proposition that is always false is called a **contradiction**.

A compound proposition that is neither a tautology nor a contradiction is called a **contingency**.

Tautologies and contradictions are important in mathematical reasoning.
Example

Tautology: \( p \lor \neg p \)
Contradiction: \( p \land \neg p \)

Logical Equivalences

The compound propositions \( p \) and \( q \) are called **logically equivalent** if \( p \iff q \) is a tautology.

The notation \( p \equiv q \) denotes that \( p \) and \( q \) are logically equivalent.

Remark

\( \equiv \) is not a logical connective.

\( p \equiv q \) is not a compound proposition but rather is the statement that \( p \iff q \) is a tautology.

One way to determine whether two compound propositions are equivalent is to use a truth table.
Example

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

| TABLE 3 Truth Tables for \( \neg(p \lor q) \) and \( \neg p \land \neg q \). |
|-----------------|-----------------|-----------------|-----------------|-----------------|
| \( p \lor q \) | \( \neg(p \lor q) \) | \( \neg p \) | \( \neg q \) | \( \neg p \land \neg q \) |
| T | T | F | F | F |
| T | F | T | F | F |
| T | F | T | T | T |
| F | F | F | F | F |

De Morgan's Laws

\[ \neg(p_1 \lor p_2 \lor \cdots \lor p_n) \equiv \neg p_1 \land \neg p_2 \land \cdots \land \neg p_n \]

\[ \neg(p_1 \land p_2 \land \cdots \land p_n) \equiv \neg p_1 \lor \neg p_2 \lor \cdots \lor \neg p_n \]

Important Equivalences

| TABLE 6 Logical Equivalences. |
|-----------------|-----------------|
| **Equivalence** | **Name** |
| \( p \land T \equiv p \) | Identity laws |
| \( p \lor F \equiv p \) | |
| \( p \lor T \equiv T \) | Domination laws |
| \( p \land F \equiv F \) | Idempotent laws |
| \( p \lor p \equiv p \lor p \) | Double negation law |
| \( p \land p \equiv p \land p \) | Commutative laws |
| \( (p \lor q) \lor r \equiv p \lor (q \lor r) \) | Associative laws |
| \( (p \land q) \land r \equiv p \land (q \land r) \) | |
| \( p \lor (q \land r) \equiv (p \lor q) \land (p \lor r) \) | Distributive laws |
| \( \neg(p \land q) \equiv \neg p \land \neg q \) | De Morgan's laws |
| \( \neg(p \lor q) \equiv \neg p \lor \neg q \) | |
| \( p \lor (p \land q) \equiv p \) | Absorption laws |
| \( p \land (p \lor q) \equiv p \) | |
| \( p \lor \neg p \equiv T \) | Negation laws |
| \( p \land \neg p \equiv F \) | |

| TABLE 7 Logical Equivalences Involving Conditional Statements. |
|-----------------|-----------------|
| **Equivalence** | **Name** |
| \( p \rightarrow q \equiv \neg p \lor q \) | |
| \( p \rightarrow q \equiv \neg q \rightarrow \neg p \) | |
| \( p \lor q \equiv \neg p \rightarrow q \) | |
| \( p \lor q \equiv \neg q \rightarrow \neg p \) | |
| \( p \land q \equiv \neg(p \rightarrow \neg q) \) | |
| \( (p \rightarrow q) \land (p \rightarrow r) \equiv (p \land r) \rightarrow q \) | |
| \( (p \rightarrow q) \land (p \rightarrow r) \equiv (p \lor q) \rightarrow r \) | |
| \( (p \rightarrow q) \lor (p \rightarrow r) \equiv (p \land q) \rightarrow r \) | |
| \( (p \rightarrow q) \lor (p \rightarrow r) \equiv (p \land q) \rightarrow r \) | |

| TABLE 8 Logical Equivalences Involving Biconditionals. |
|-----------------|-----------------|
| **Equivalence** | **Name** |
| \( p \leftrightarrow q \equiv (p \rightarrow q) \land (q \rightarrow p) \) | |
| \( p \leftrightarrow q \equiv \neg(p \rightarrow \neg q) \) | |
| \( p \leftrightarrow q \equiv \neg q \rightarrow \neg p \) | |
| \( p \leftrightarrow q \equiv \neg(q \rightarrow \neg p) \) | |
| \( \neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q \) | |
EXAMPLE 7  Show that \( \neg(p \lor \neg p \land q) \) and \( \neg p \land \neg q \) are logically equivalent by developing a series logical equivalences.

Solution: We will use one of the equivalences in Table 6 at a time, starting with \( \neg(p \lor \neg p \land q) \) and ending with \( \neg p \land \neg q \). (Note: we could also easily establish this equivalence using a truth table.) We have the following equivalences.

\[
\begin{align*}
\neg(p \lor \neg p \land q) & \equiv \neg p \land \neg(\neg p \land q) & \text{by the second De Morgan law} \\
& \equiv \neg p \land [\neg(\neg p) \lor \neg q] & \text{by the first De Morgan law} \\
& \equiv \neg p \land (p \lor \neg q) & \text{by the double negation law} \\
& \equiv (\neg p \land p) \lor (\neg p \land \neg q) & \text{by the second distributive law} \\
& \equiv F \lor (\neg p \land \neg q) & \text{because } \neg p \land p \equiv F \\
& \equiv (\neg p \land \neg q) \lor F & \text{by the commutative law for disjunction} \\
& \equiv \neg p \land \neg q & \text{by the identity law for } F
\end{align*}
\]

Consequently \( \neg(p \lor \neg p \land q) \) and \( \neg p \land \neg q \) are logically equivalent.

EXAMPLE 8  Show that \( (p \land q) \rightarrow (p \lor q) \) is a tautology.

Solution: To show that this statement is a tautology, we will use logical equivalences to demonstrate that it is logically equivalent to \( T \). (Note: This could also be done using a truth table.)

\[
\begin{align*}
(p \land q) \rightarrow (p \lor q) & \equiv \neg(p \land q) \lor (p \lor q) & \text{by Example 3} \\
& \equiv (\neg p \lor \neg q) \lor (p \lor q) & \text{by the first De Morgan law} \\
& \equiv (\neg p \lor p) \lor (\neg q \lor q) & \text{by the associative and commutative laws for disjunction} \\
& \equiv T \lor T & \text{by Example 1 and the commutative law for disjunction} \\
& \equiv T & \text{by the domination law}
\end{align*}
\]

Limitation of Propositional Logic

Propositional logic cannot adequately express the meaning of statements in math and in natural languages. We introduce a more powerful type of logic called predicate logic.
Predicates

Statement

"x is greater than 3"
\[ x \quad \text{variable} \quad P \quad \text{predicate} \]
can be denoted by \( P(x) \) which is the value of propositional function \( P \) at variable \( x \). Once a value is assigned to \( x \), statement \( P(x) \) becomes a proposition and has a truth value.

\[ P(4) \text{ is true} \]
\[ P(2) \text{ is false} \]

Generalization

A statement involving \( n \) variables \( x_1, \ldots, x_n \) can be denoted by \( P(x_1, \ldots, x_n) \). It is the value of propositional function \( P \) at the \( n \)-tuple \( (x_1, \ldots, x_n) \). \( P \) is called a \( n \)-ary predicate.

Example: Let \( Q(x, y) \) denote "\( x = y + 3 \)."
\[ Q(1, 2) \text{ is false} \]
\[ Q(3, 2) \text{ is true} \]
Quantifiers

Quantification can be used to create a proposition from a propositional function. The logic that deals with predicates and quantifiers is called the predicate calculus. (or predicate logic)

Universal Quantifier

For $P(x)$, the domain (universe) of discourse, or simply the domain is the domain of $x$ in $P(x)$.

The universal quantification of $P(x)$ is the statement

"$P(x)$ for all values of $x$ in the domain"

This is denoted by $\forall x P(x)$. $\forall$ is called the universal quantifier.

$\forall x P(x)$ is read as "for all $x$ $P(x)$" or "for every $x$ $P(x)$." An element for which $P(x)$ is false is called a counterexample of $\forall x P(x)$.
The existential quantification of \( P(x) \) is the proposition

"There exists an element \( x \) in the domain such that \( P(x) \)"

This denoted by \( \exists x P(x) \). It is called the existential quantifier.

\( \exists x P(x) \) is read as

"There exists an \( x \) s.t. \( P(x) \)"

"There is at least one \( x \) s.t. \( P(x) \)"

"For some \( x \) \( P(x) \)"

**TABLE 1 Quantifiers.**

<table>
<thead>
<tr>
<th>Statement</th>
<th>When True?</th>
<th>When False?</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \forall x P(x) )</td>
<td>( P(x) ) is true for every ( x ).</td>
<td>There is an ( x ) for which ( P(x) ) is false.</td>
</tr>
<tr>
<td>( \exists x P(x) )</td>
<td>There is an ( x ) for which ( P(x) ) is true.</td>
<td>( P(x) ) is false for every ( x ).</td>
</tr>
</tbody>
</table>
Examples

1. What is the truth value of \( \forall x \, Q(x) \) where \( Q(x) \) is "\( x < 2 \)" and the domain is the set of all real numbers?

   Answer: \( \forall x \, Q(x) \) is false

2. What is the truth value of \( \forall x \, (x^2 \geq x) \) if the domain is the set of all integers?

   Answer: \( \forall x \, (x^2 \geq x) \) is true for all integers.

   Remark: \( \forall x \, (x^2 \geq x) \) is false for the domain of real numbers.

   Counterexample: \( x = 0.1 \).

3. \( \exists x \, P(x) \) is true if \( P(x) \) is "\( x > 3 \)" and the domain is the set of all real numbers.

4. \( \exists x \, Q(x) \) is false if \( Q(x) \) is "\( x = x + 1 \)" and the domain is the set of all real numbers.
Quantifiers with restricted domains

Let the domain be the set of all real numbers

1. $\forall x < 0 \ (x^2 > 0) \equiv \forall x \ (x < 0 \Rightarrow x^2 > 0)$
2. $\forall y \neq 0 \ (y^3 \neq 0) \equiv \forall y \ (x \neq 0 \Rightarrow y^3 \neq 0)$
3. $\exists z > 0 \ (z^2 = 2) \equiv \exists z \ (z > 0 \land z^2 = 2)$

The restriction of a universal quantification is the same as the universal quantification of a conditional statement.

The restriction of an existential quantification is the same as the existential quantification of a conjunction.

Precedence of Quantifiers: $\forall$ and $\exists$ have higher precedence than all logical operators from propositional logic.

Example: $\forall x \ P(x) \lor Q(x)$ means $(\forall x \ P(x)) \lor Q(x)$
Binding Variables

When a quantifier is used on the variable x, we say that this occurrence of the variable is bound.

An occurrence of a variable that is not bound by a quantifier or set to a particular value is said to be free.

All the variables that occur in a propositional function must be bound or set to a particular value to turn the function into a proposition.

The part of a logical expression to which a quantifier is applied is called the scope of this quantifier.

Example

0. \( \exists x \ (x + y = 1) \)

x is bound by \( \exists x \)
y is free
(2) \( \exists x ( x + y = 1 \land y = 1 ) \)

- \( x \) is bound by \( \exists x \)
- \( y \) is set to 1

(3) \( \exists x ( P(x) \land Q(x) ) \lor \forall x R(x) \)

- All variables are bound
- Scope of \( \exists x \): \( P(x) \land Q(x) \)
- Scope of \( \forall x \): \( R(x) \)

We could have written the statement using two variables \( x \) and \( y \), as

\( \exists x ( P(x) \land Q(x) ) \lor \forall y R(y) \)
Logical Equivalence Involving Quantifiers

Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain of discourse is used for the variables in the propositional functions.

We use $S \equiv T$ to indicate that two statements $S$ and $T$ involving predicates and quantifiers are logically equivalent.

Example:

$$\forall x (P(x) \land Q(x)) \equiv \forall x (P(x)) \land \forall x Q(x)$$

if the same domain is used.
Negating Quantified Expressions

\[ \neg \forall x P(x) \equiv \exists x \neg P(x) \]
\[ \neg \exists x Q(x) \equiv \forall x \neg Q(x) \]

<table>
<thead>
<tr>
<th>Negation</th>
<th>Equivalent Statement</th>
<th>When Is Negation True?</th>
<th>When False?</th>
</tr>
</thead>
<tbody>
<tr>
<td>\neg \exists x P(x)</td>
<td>\forall x \neg P(x)</td>
<td>For every ( x ), ( P(x) ) is false.</td>
<td>There is an ( x ) for which ( P(x) ) is true.</td>
</tr>
<tr>
<td>\neg \forall x P(x)</td>
<td>\exists x \neg P(x)</td>
<td>There is an ( x ) for which ( P(x) ) is false.</td>
<td>( P(x) ) is true for every ( x ).</td>
</tr>
</tbody>
</table>

Example:

1. \[ \neg \forall x (x^2 > x) \]
   \[ \equiv \exists x \neg (x^2 > x) \]
   \[ \equiv \exists x (x^2 \leq x) \]

2. \[ \neg \exists x (x^2 = 2) \]
   \[ \equiv \forall x \neg (x^2 = 2) \]
   \[ \equiv \forall x (x^2 \neq 2) \]

3. Show \[ \neg \forall x (P(x) \rightarrow Q(x)) \]
   \[ \equiv \exists x (P(x) \land \neg Q(x)) \]

\[ \neg \forall x (P(x) \rightarrow Q(x)) \]
\[ \equiv \exists x \neg (P(x) \rightarrow Q(x)) \]
\[ \equiv \exists x \neg (\neg P(x) \lor Q(x)) \]
\[ \equiv \exists x (P(x) \land \neg Q(x)) \]
Valid Arguments

Proofs in math are valid arguments that establish the truth of mathematical statements.

By argument, we mean a sequence of statements that end with a conclusion.

By valid, we mean that the conclusion must follow from the truth of preceding statements, or premises, of the argument.

An argument is valid if and only if it is impossible for all the premises to be true and the conclusion to be false.

To deduce new statements from statements we already have, we use rules of inference for constructing valid arguments.

Valid Arguments in Propositional Logic

Example: "If you have a current password, then you can log onto the network. You have a current password." Therefore, "You can log on to the network."
\( ((p \to q) \land p) \to q \) is a tautology.

When both \( p \to q \) and \( q \) are true, \( q \) must be true. The form

\[
\begin{align*}
p \to q \\
p \\
\therefore q
\end{align*}
\]

is valid because whenever \( p \to q \) and \( p \) are true, the conclusion \( q \) must be also true.

An argument form in propositional logic is a sequence of compound propositions involving propositional variables. An argument form is valid if no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

\( ((p \to q) \land p) \to q \)

is an argument form. In general, argument form with premises \( p_1, p_2, \ldots, p_n \) and conclusion \( q \) is valid when \( (p_1 \land p_2 \land \ldots \land p_n) \to q \) is a tautology.
A set of simple argument forms are called rules of reference. They can be used as building blocks to construct more complicated valid argument forms.

<table>
<thead>
<tr>
<th>Rule of Inference</th>
<th>Tautology</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p )</td>
<td>( p \land (p \rightarrow q) \rightarrow q )</td>
<td>Modus ponens</td>
</tr>
<tr>
<td>( p \rightarrow q )</td>
<td>( \neg q \land (p \rightarrow q) \rightarrow \neg p )</td>
<td>Modus tollens</td>
</tr>
<tr>
<td>( p \rightarrow q )</td>
<td>((p \rightarrow q) \land (q \rightarrow r) \rightarrow (p \rightarrow r))</td>
<td>Hypothetical syllogism</td>
</tr>
<tr>
<td>( q \rightarrow r )</td>
<td>((p \lor q) \land \neg p \rightarrow q )</td>
<td>Disjunctive syllogism</td>
</tr>
<tr>
<td>( p \lor q )</td>
<td>((p \lor q) \land \neg p \rightarrow q )</td>
<td>Addition</td>
</tr>
<tr>
<td>( p \rightarrow (p \lor q) )</td>
<td>((p \land q) \rightarrow p )</td>
<td>Simplification</td>
</tr>
<tr>
<td>( p \land q )</td>
<td>((p \land q) \rightarrow (p \land q) )</td>
<td>Conjunction</td>
</tr>
<tr>
<td>( p \lor q )</td>
<td>((p \lor q) \land \neg (p \lor q) \rightarrow (q \lor r) )</td>
<td>Resolution</td>
</tr>
</tbody>
</table>
A valid argument can lead to an incorrect conclusion if one or more of its premises is false.

Example

1. "If you have access to the network, then you can change your grade." 
   
   "you have access to the network." 
   
   "you can change your grade.
   
   Valid argument form \( P \rightarrow q \), but we cannot conclude the conclusion is true because \( p \rightarrow q \) may not be true.

2. "If \( \sqrt{2} > \frac{3}{2} \), then \( (\sqrt{2})^2 > (\frac{3}{2})^2 \). We know that \( \sqrt{2} > \frac{3}{2} \). Therefore \( (\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = 2.25 \)."

   Valid argument form \( P \rightarrow q \), but wrong conclusion because the premise \( p \) is false.

   Remark: In this example, \( p \rightarrow q \) is true.
Using Rules of Inference to Build Argument

Example

Hypotheses:

\(-p \land q\)

"It is not sunny this afternoon and it is colder than yesterday."

\(r \rightarrow p\)

"We will go swimming only if it is sunny."

\(r \rightarrow s\)

"If we do not go swimming, then we will take a canoe trip."

\(s \rightarrow t\)

"If we take a canoe trip, then we will be home by sunset."

Conclusion: We will be home by sunset.

We construct an argument to show that our hypotheses lead to the desired conclusion as follows:

<table>
<thead>
<tr>
<th>Step</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>(-p \land q) Hypothesis</td>
</tr>
<tr>
<td>2.</td>
<td>(-p) Simplification using (1)</td>
</tr>
<tr>
<td>3.</td>
<td>(r \rightarrow p) Hypothesis</td>
</tr>
<tr>
<td>4.</td>
<td>(-r) Modus tollens using (2) and (3)</td>
</tr>
<tr>
<td>5.</td>
<td>(-r \rightarrow s) Hypothesis</td>
</tr>
<tr>
<td>6.</td>
<td>(s) Modus ponens using (4) and (5)</td>
</tr>
<tr>
<td>7.</td>
<td>(s \rightarrow t) Hypothesis</td>
</tr>
<tr>
<td>8.</td>
<td>(t) Modus ponens using (6) and (7)</td>
</tr>
</tbody>
</table>

Note that we could have used a truth table to show that whenever each of the four hypotheses is true, the conclusion is also true. However, because we are working with five propositional variables, \(p, q, r, s,\) and \(t,\) such a truth table would have 32 rows.
Example

Hypotheses

\begin{align*}
\text{"If you send me an e-mail message,}\quad &\quad \text{\underline{p}} \\
\rightarrow &\quad \text{then I will finish writing the program."} \\
\quad &\quad \text{\underline{q}} \\
\text{"If you do not send me an e-mail message,}\quad &\quad \text{\underline{\neg p}} \\
\rightarrow &\quad \text{then I will go to sleep early."} \\
\quad &\quad \text{\underline{r}} \\
\text{"If I go to sleep early, then I will wake up feeling refreshed."} \\
\quad &\quad \text{\underline{s}}
\end{align*}

Conclusion

\begin{align*}
\text{"If I do not finish writing the program,}\quad &\quad \text{\underline{\neg q}} \\
\rightarrow &\quad \text{then I will wake up feeling refreshed."} \\
\quad &\quad \text{\underline{\neg s}}
\end{align*}

This argument form shows that the hypotheses \( p \) lead to the desired conclusion.

<table>
<thead>
<tr>
<th>Step</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ( p \rightarrow q )</td>
<td>Hypothesis</td>
</tr>
<tr>
<td>2. ( \neg q \rightarrow \neg p )</td>
<td>Contrapositive of (1)</td>
</tr>
<tr>
<td>3. ( \neg p \rightarrow r )</td>
<td>Hypothesis</td>
</tr>
<tr>
<td>4. ( \neg q \rightarrow r )</td>
<td>Hypothetical syllogism using (2) and (3)</td>
</tr>
<tr>
<td>5. ( r \rightarrow s )</td>
<td>Hypothesis</td>
</tr>
<tr>
<td>6. ( \neg q \rightarrow s )</td>
<td>Hypothetical syllogism using (4) and (5)</td>
</tr>
</tbody>
</table>
Resolution Rule

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

Resolution plays an important role in logic programming languages such as Prolog.

Resolution can be used to build automatic reasoning and theorem proving systems.
Fallacies

Some forms of incorrect reasoning, called fallacies, lead to invalid arguments.

Fallacy of affirming the conclusion

\[ p \rightarrow q \]

\[ q \]

\[ 	herefore p \]

This is not a valid argument form because

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

is not a tautology (it is false if \( p \) is false and \( q \) is true).

Example: "If you do every problem in this book \( p \) then you will learn discrete math." \( q \)

"you learned discrete math" \( q \)

\[ 	herefore \text{Then you did every problem in this book} \]

This is an incorrect reasoning based on fallacy of affirming the conclusion.
Fallacy of denying the hypothesis

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

This is not a valid argument form because

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

is not a tautology (it is false if \( p \) is false and \( q \) is true).

Example

"If you do every problem in this book, then you will learn discrete math"

\[ p \]
\[ q \]

"You did not do every problem in this book"

\[ \therefore \neg q \]

"you did not learn discrete math"

This is an incorrect reasoning based on fallacy of denying the hypothesis.
<table>
<thead>
<tr>
<th>Rule of Inference</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\forall x P(x)) (\vdash P(c))</td>
<td>Universal instantiation</td>
</tr>
<tr>
<td>(P(c)) for an arbitrary (c) (\vdash \forall x P(x))</td>
<td>Universal generalization</td>
</tr>
<tr>
<td>(\exists x P(x)) (\vdash P(c)) for some element (c)</td>
<td>Existential instantiation</td>
</tr>
<tr>
<td>(P(c)) for some element (c) (\vdash \exists x P(x))</td>
<td>Existential generalization</td>
</tr>
</tbody>
</table>

Example: "Everyone in this discrete math class has taken a course in CS." 
Premises: 
- "Mara is a student in this class."
- "Mara has taken a course in CS"

Conclusion: "\(D(x)\): \(x\) is in this discrete class."
- \(D(\text{Marla})\) \(\vdash C(\text{Marla})\)
- \(C(\text{Marla})\)

The following steps can be used to establish the conclusion from the premises.

<table>
<thead>
<tr>
<th>Step</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (\forall x (D(x) \rightarrow C(x)))</td>
<td>Premise</td>
</tr>
<tr>
<td>2. (D(\text{Marla}) \rightarrow C(\text{Marla}))</td>
<td>Universal instantiation from (1)</td>
</tr>
<tr>
<td>3. (D(\text{Marla}))</td>
<td>Premise</td>
</tr>
<tr>
<td>4. (C(\text{Marla}))</td>
<td>Modus ponens from (2) and (3)</td>
</tr>
</tbody>
</table>
promises:  "A student in this class has not read the book."
"Everyone in this class passed the first exam."

Conclusion:  "Someone who passed the first exam has not read the book."

C(x):  "x is in this class."
B(x):  "x has read the book."
P(x):  "x passed the first exam."

Step  Reason
1. \(\exists x(C(x) \land \neg B(x))\)  Premise
2. C(a) \land \neg B(a)  Existential instantiation from (1)
3. C(a)  Simplification from (2)
4. \(\forall x(C(x) \rightarrow P(x))\)  Premise
5. C(a) \rightarrow P(a)  Universal instantiation from (4)
6. P(a)  Modus ponens from (3) and (5)
7. \(\neg B(a)\)  Simplification from (2)
8. P(a) \land \neg B(a)  Conjunction from (6) and (7)
9. \(\exists x(P(x) \land \neg B(x))\)  Existential generalization from (8)
Combining Rules of Reference for Propositions and Quantified Statements

**Universal Modus Ponens**

∀x (P(x) → Q(x))

P(a), where a is an element in the domain

∴ Q(a)

**Universal Modus Tollens**

∀x (P(x) → Q(x))

¬Q(a), where a is an element in the domain

∴ ¬P(a)

**Example**

1. ∀n (n > 4 → n^2 < 2^n)

   100 > 4

   ∴ 100^2 < 2^{100}

2. ∀n (n > 4 → n^2 < 2^n)

   ¬(k^2 < 2^k)

   ∴ k < 4

   k = 1, 2, 3
Introduction to Proofs

Terminology

A **theorem** is a statement that can be shown to be true. The term theoren is usually reserved for important true statements.

Less important theorems are sometimes called **propositions** (or facts, or results).

A theorem is demonstrated true by a **proof**. A proof is a valid argument that establish the truth of a theorem.

A proof can include **axioms** which are basic statements assumed true.

A less important theorem that is helpful in the proof of other results is called a **lemma**. A **corollary** is a theorem that can be established directly from a proved theorem.
A conjecture is a statement that is being proposed to be a true statement. A conjecture may be true or false. A conjecture becomes a theorem if a proof is found.

Formal Proofs

Arguments involving propositions and quantified statements are shown all true.

Informal Proofs

More than one rule of inference may be used in each step, some steps may be skipped, and axioms assumed and inference rules used are not explicitly stated.

Informal proofs can be understood by humans why theorems are true, while formal proofs are used in computer-based automatic reasoning systems.
An example theorem:

For all positive real numbers \( x \) and \( y \), if \( x > y \) then \( x^2 > y^2 \).

Methods of Proving Theorems:

1. Direct Proofs

A direct proof of \( p \rightarrow q \) shows that if \( p \) is true then \( q \) must be true so that the combination of \( p \) true and \( q \) false never occurs.

Example

Theorem: If \( n \) is an odd integer then \( n^2 \) is odd.

Let \( P(n) \) be "\( n \) is an odd integer" and \( Q(n) \) be "\( n^2 \) is odd." We want to prove

\[ \forall n \ (P(n) \rightarrow Q(n)) \]
Proof:

For any odd \( n \), \( n = 2k + 1 \) where \( k \) is an integer. Then,

\[
    n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1
\]

We conclude that \( n^2 \) is odd.

Indirect proofs: proofs that do not start with hypothesis and end with the conclusion.

(2) Proof by Contraposition

An indirect proof method that makes use of

\[
p \rightarrow q \equiv \neg q \rightarrow \neg p
\]

Example: Prove that if \( n \) is an integer and \( 3n+2 \) is odd, then \( n \) is odd.

Proof: If \( n \) is even (i.e. \( \neg q \) is true),

then \( n = 2k \) for some integer \( k \).

Then \( 3n+2 = 3 \cdot 2k + 2 = 2(3k+1) \) is even.
Then "\( n \) is an integer AND \( 3n+2 \) is odd" is false (i.e. \( \neg p \) is true). Therefore, the statement 
\[
(3n+2 \text{ is odd and } n \text{ is an integer}) \\
\rightarrow (n \text{ is odd}) \quad (\text{i.e. } p \Rightarrow q)
\] is true.

(3) **Proofs by Contradiction**

An indirect proof method.
Suppose we want to prove \( p \) is true.
If we can find a contradiction \( q \) s.t. (such that) \( \neg p \Rightarrow q \) is true, then by \( q \) being false but \( \neg p \Rightarrow q \) being true, we conclude that \( \neg p \) is false (i.e. \( p \) is true).

Remark: proposition \( \neg p \Rightarrow \neg q \) is a contradiction.
Example Show that at least 4 of any 22 days must fall on the same day of the week.

Proof: 

P is "at least 4 of any 22 days fall on the same day of the week."

Suppose P is true. Then at most 3 of 22 days fall on the same day of the week. Because there are 7 days in a week, this implies at most 21 days could have been chosen for at most 3 days to fall on the same day of the week. This contradicts that we have 22 days under consideration. Therefore, P is true.

Remark: In this example, the contradiction is:

\[ \leq 3 \text{ of 22 days fall on the same day} \wedge \leq 3 \text{ of 21 days fall on the same day} \]
Exhaustive Proofs and Proof by Cases

They are useful if we cannot prove a theorem using a single argument that holds for all possible cases.

Example: Prove \((n+1)^3 \geq 3^n\) if \(n\) is a positive integer \(\leq 4\).

Proof:
\[
\begin{align*}
n=1, \quad (n+1)^3 &= 8 \geq 3 = 3^n \\
n=2, \quad (n+1)^3 &= 27 \geq 9 = 3^n \\
n=3, \quad (n+1)^3 &= 64 \geq 27 = 3^n \\
n=4, \quad (n+1)^3 &= 125 \geq 81 = 3^n
\end{align*}
\]

Remark: Example 1 on page 87 of the textbook is wrong.

Example: Prove \(|xy| = |x||y|\) where \(x\) and \(y\) are real numbers.

Proof: Without loss of generality, we only consider 3 cases:
\begin{align*}
(1): & \quad x \geq 0, \quad y \geq 0 \\
(2): & \quad x \geq 0, \quad y < 0 \\
(3): & \quad x < 0, \quad y < 0
\end{align*}
Case (1). \( x \geq 0, \ y \geq 0 \)
Then \[ |x| = x \geq 0 \quad |y| = y \geq 0, \]
\[ |xy| = xy = |x||y| \]

Case (2). \( x \geq 0, \ y < 0 \)
Then \[ |xy| = x(-y) = |x||y| \]

Case (3). \( x < 0, \ y < 0 \)
Then \[ |xy| = (-x)(-y) = |x||y| \]

(5) **Existence Proofs**

**Proof of \( \exists x P(x) \)**

**Constructive Existence Proof**

Find one element \( a \) s.t. \( P(a) \) is true

**Example:** Show there is a positive integer that can be written as sum of cubes of positive integers in 2 different ways.

**Proof:** Consider 1729

\[ 1729 = 10^3 + 9^3 = 12^3 + 1^3. \]
Nonconstructive Existence Proof

Prove \( \exists x \ P(x) \) not by finding one element \( a \) s.t. \( P(a) \) is true, but by some other ways.

**Example:** A number is a rational number iff \( r = \frac{i}{j} \) where \( i \) and \( j \) are integers and \( j \neq 0 \).

Show that there exists irrational numbers \( x \) and \( y \) s.t. \( x^y \) is rational.

**Proof:** We know that \( \sqrt{2} \) is irrational. (will be shown later).

Consider \( \sqrt{2}^{\sqrt{2}} \).

If \( \sqrt{2}^{\sqrt{2}} \) is rational, then let \( x = \sqrt{2}, y = \sqrt{2} \), the statement is true.

If \( \sqrt{2}^{\sqrt{2}} \) is irrational, then let \( x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2} \),

\[ x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2, \] the statement is also true.

**Remark:** This proof also involves proof by cases.
(6) Uniqueness Proofs

Proof of \( \exists x \ (P(x) \land \forall y \ (y \neq x \Rightarrow \neg P(y))) \).

A uniqueness proof has 2 parts:
1. Existence
2. Uniqueness

Example: Show if \( a \) and \( b \) are real numbers and \( a \neq 0 \), then there is a unique real number \( r \) s.t. \( ar + b = 0 \).

Proof:

Existence
Let \( r = -b/a \). Then \( ar + b = 0 \)

Uniqueness
Suppose \( s \) is a real number s.t. \( as + b = 0 \). Then
\[ as + b = ar + b = 0, \]
where \( r = -b/a \).
Then from \( as = ar \) we have \( s = r \).
This means that if \( s \neq r \) then \( as + b \neq 0 \).
Adapt an existing proof to prove a new result.

First, consider the following example.

Example: Show \( \sqrt{2} \) is irrational.

Proof:

Proof by contradiction.

Suppose \( \sqrt{2} \) is rational. Then there exist integers \( a \) and \( b \) s.t. \( \sqrt{2} = \frac{a}{b} \), where \( a \) and \( b \) have no common factor.


\[
\neg P \equiv \sqrt{2} = \frac{a}{b} \\
\rightarrow \sqrt{2} \cdot b = a \rightarrow 2b^2 = a^2 \\
\rightarrow a^2 \text{ is even} \rightarrow a \text{ is even} \rightarrow a = 2c \text{ for some integer } c \\
\rightarrow 2b^2 = 4c^2 \rightarrow b^2 = 2c^2 \\
\rightarrow b^2 \text{ is even} \rightarrow b \text{ is even} \rightarrow b = 2d \text{ for some integer } d \\
\rightarrow \sqrt{2} = \frac{a}{b} = \frac{2c}{2d} \\
\rightarrow a \text{ and } b \text{ have common factor } 2 \\
\rightarrow \text{ Contradiction}
\]

Therefore, \( P \) must be true.
Example: Show $\sqrt{3}$ is irrational.

Proof: Can be proved in a similar way of proving "$\sqrt{2}$ is irrational" in the previous example.

Looking for counterexample

Given a conjecture C, we may prove C or disprove C (show C is false).

\[ \text{prove C} \leftrightarrow \text{disprove C} \]

One way of a conjecture is false is to find a counter example.

The process of finding a counter example can provide insights into the given problem.