CS 309: Discrete Math (Notes)

Matthew Kosloski

Contents

Chapter 1: Sets and Logic

1.1 Sets

Denoting Sets

A **set** is simply a collection of objects, or elements.
If a set is finite and not large, we can describe it by simply listing the elements:

$$A = \{1, 2, 3, 4\}$$

The above set A is made up of four elements. **The order of the elements in a set does not matter**, therefore, a could also be specified like so:

$$A = \{1, 3, 4, 2\}$$

The elements of a set are assumed to be distinct, so any duplicate occurence of an element can be ignored. Therefore, we could also specify set A like so:

$$A = \{1, 2, 2, 3, 4, 4\}$$

If a set is very large or infinite, we can describe it using a property necessary for membership:

$$B = \{x \mid x \text{ is a positive, even integer}\}$$

The above set B is made up of positive, even integers. The vertical bar "|" is read as "such that" and the text after the bar is the property. Therefore, B can be read as "the set of all x such that x is a positive, even integer." Some sets of numbers occur frequently in mathematics and are given symbols.

Symbol	Set	Example of Members
Z	Integers	-3, 0, 2, 145
Q	Rational numbers	-1/3, 0, 24/15
R	Real numbers	-3, -1.766, 0, 4/15, $\sqrt{2}$, 2.666, …, π

Rational numbers are quotients of integers, thus **Q** for *quotient*. The set of real numbers **R** consists of all points on a straight line extending indefinitely in either direction.

We can denote the positive elements in a set using the superscript plus (e.g., $\mathbf{Z}^+$ for positive integers) and the negative elements in a set using the superscript minus (e.g., $\mathbf{Q}^-$ for negative rational numbers).

Set Cardinality

If X is a finite set, we let

$$|X| = \text{number of elements in } X$$

We call $|X|$ the **cardinality** of X.

If we let $A = \{1, 2, 3, 4\}$, then the cardinality of A is 4, or $|A| = 4$. The cardinality of $\{\mathbf{R}, \mathbf{Z}\}$ is 2 since it contains two elements, which just happen to be sets.

Remember: an element in a set can be anything, even a set.

If x is in the set X, we write $x \in X$. If x is NOT in the set X, we write $x \notin X$. For example, both of these are true:

$$3 \in \{1, 2, 3, 4\}$$
$$3 \notin \{x \mid x \text{ is a positive, even integer}\}$$

Empty Set

A set with no elements is called an **empty set** and is denoted by $\varnothing$. In other words, $\varnothing = \{\}$.

Set Equality

Two sets X and Y are **equal** $(X = Y)$ if X and Y have the same elements. To put it differently, for $X = Y$ to be true:

$$\text{For every } x \text{, if } x \in X \text{, then } x \in Y$$
$$\text{For every } x \text{, if } x \in Y \text{, then } x \in X$$

Here are two examples that demonstrate *equality* among sets:

If

$$A = \{1, 3, 2\} \text{ and } B = \{2, 3, 2, 1\},$$

then, by inspection, A and B have the same elements. Therefore $A = B$.

Remember: The elements in a set are unique, so duplicates are removed when evaluating a set.

If

$$A = \{x \mid x^2 + x - 6 = 0\} \text{ and } B = \{2, \text{-}3\},$$

then, $A = B$ in this case, too.

Set Inequality

For a set X to NOT be equal to a set Y $(X \neq Y)$, X and Y must NOT have the same elements. In other words, there must be at least one element in X that is not in Y or at least one element in Y that is not in X (or both).

Here is an example that demonstrates *inequality* among sets:

If

$$A = \{1, 3, 2\} \text{ and } B = \{4, 2\},$$

Then, by inspection, $A \neq B$.

Subsets

Suppose X and Y are sets. If every element of X is an element of Y, we say X is a **subset** of Y and write $X \subseteq Y$. In other words,

If

$$X \text{ and } Y \text{ are sets and, for every x, } x \in X \text{ and } x \in Y.$$

Then, $X \subseteq Y$. Here are some examples demonstrating subsets:

If

$$C = \{1,\ 3\} \text{ and } A = \{1,\ 2,\ 3,\ 4\},$$

then, every element of C is an element of A. Therefore, $C \subseteq A$.

Let

$$X = \{x \mid x^2 + x - 2 = 0\}$$

We can show that $X \subseteq \mathbf{Z}$:

Remember, $\mathbf{Z}$ is a set of integers, so

$$\mathbf{Z} = \{x \mid x \text{ is an integer}\}.$$

We can solve for the subset X

$$\begin{aligned} x^2 + x - 2 &= 0 \\ (x+2)(x-1) &= 0 \end{aligned}$$

which gives $x = -2$ and $x = 1$. So $X = \{\text{-2, 1}\}$. Since every element of set X is an element of set $\mathbf{Z}$, $X \subseteq \mathbf{Z}$.

For a set X to NOT be a subset of a set Y, there must be at least one element of X that is NOT a member of Y.

Let

$$X = \{x \mid 3x^2 - x - 2 = 0\}$$

We can show that X is NOT a subset of $\mathbf{Z}$:

If $x \in X$, then

$$3x^2 - x - 2 = 0.$$

Solving for x, we obtain $x = 1$ and $x = -\frac{2}{3}$, so $X = \{1, -\frac{2}{3}\}$. Since $-\frac{2}{3} \notin \mathbf{Z}$, X is NOT a subset of $\mathbf{Z}$.

Given a set X, $X \subseteq X$, since every element of X is an element of itself.

Proper Subsets

If X is a subset of Y and $X \neq Y$, then X is a **proper subset** of Y and we write $X \subset Y$. If $X \subset Y$, then X is ALWAYS smaller than Y.

Let

$$C = \{1,\ 3\} \text{ and } A = \{1,\ 2,\ 3,\ 4\},$$

Then $C \subset A$ since $C \neq A$.

Understanding subsets versus proper subsets:

- The symbol for a subset ($\subseteq$) is analogous to $\leq$. In other words, a subset *can* be the same size as the parent set.
- The symbol for a proper subset ($\subset$) is analogous to $<$. In other words, a proper subset is smaller than the parent set.

Power Set

The set of all subsets (proper or not) of a set X, denoted $\mathcal{P}(X)$, is called the **power set** of X.

If A = {a, b, c}, then

$$\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

All but {a, b, c} are proper subsets of A. $|A| = 3$ and $|\mathcal{P}(A)| = 2^3 = 8$.

In other words, given a set X with n elements, $|\mathcal{P}(X)| = 2^n$.

Given two sets X and Y, there are several operations that can be performed on the sets to produce a new set.

Union, Intersection, and Difference

The **union** of X and Y,

$$X \cup Y = \{x \mid x \in X \text{ or } x \in Y\},$$

is a set that consists of all elements belonging to X or Y (or both).

The **intersection** of X and Y,

$$X \cap Y = \{x \mid x \in X \text{ and } x \in Y\},$$

is a set that consists of all elements belonging to X and Y.

The **difference** of X and Y,

$$X - Y = \{x \mid x \in X \text{ and } x \notin Y\},$$

is a set that consists of all elements in X that are not in Y.

If

$$\text{A} = \{1, 3, 5\} \text{ and } \text{B} = \{4, 5, 6\}$$

then,

$$
\begin{aligned}
A \cup B &= \{1, 3, 4, 5, 6\} \\
A \cap B &= \{5\} \\
A - B &= \{1, 3\} \\
B - A &= \{4, 6\}
\end{aligned}
$$

In general, A - B $\neq$ B - A.

Union of a Family of Sets

Just like how we took the union of two sets above, we can take the union of a family of sets $\mathcal{S}$.

We define the union of a family $\mathcal{S}$ of sets to be those elements x belonging to at least one set X in the family $\mathcal{S}$. In other words,

$$\cup\, \mathcal{S} = \{x \mid x \in X \text{ for some } X \in \mathcal{S}\}.$$

We can calculate the union of $\mathcal{S}$ like so:

$$\bigcup \mathcal{S} = \bigcup_{i=1}^{n} X_i$$

where X is some set in $\mathcal{S}$ and n is the cardinality of $\mathcal{S}$.

Let

$$
\begin{aligned}
A_1 &= \{1, 2, 6, 7, 9\} \\
A_2 &= \{2, 5, 6, 7, 8, 9, 10\} \\
A_3 &= \{1, 2, 3, 4, 9\} \\
\mathcal{S} &= \{A_1, A_2, A_3\}
\end{aligned}
$$

Then, the union of $\mathcal{S}$ is

$$\bigcup \mathcal{S} = \bigcup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3 = \{1, 2, 3, \ldots, 10\}.$$

Intersection of a Family of Sets

Just like how we took the intersection of two sets above, we can take the intersection of a family of sets $\mathcal{S}$.

We define the intersection of a family $\mathcal{S}$ of sets to be those elements x belonging to at least one set X in the family $\mathcal{S}$. In other words,

$$\cap\, \mathcal{S} = \{x \mid x \in X \text{ for all } X \in \mathcal{S}\}.$$

We can calculate the intersection of $\mathcal{S}$ like so:

$$\bigcap \mathcal{S} = \bigcap_{i=1}^{n} X_i$$

where X is some set in $\mathcal{S}$ and n is the cardinality of $\mathcal{S}$.

Let

$$\begin{aligned} A_1 &= \{1, 2, 6, 7, 9\} \\ A_2 &= \{2, 5, 6, 7, 8, 9, 10\} \\ A_3 &= \{1, 2, 3, 4, 9\} \\ \mathcal{S} &= \{A_1, A_2, A_3\} \end{aligned}$$

Then, the intersection of $\mathcal{S}$ is

$$\bigcap \mathcal{S} = \bigcap_{i=1}^{3} A_i = A_1 \cap A_2 \cap A_3 = \{2, 9\}.$$

Disjoint Sets

Sets X and Y are **disjoint** if $X \cap Y = \varnothing$. In other words, if X and Y share no elements, they are disjoint.

Pairwise Disjoint

A collection of sets $\mathcal{S}$ is said to be **pairwise disjoint** if every pair of sets within the set are disjoint.

Let

$$\mathcal{S} = \{A_1,\ A_2,\ A_3,\ \ldots,\ A_n\}.$$

If

$$\text{For every } i \text{ and } j \text{ in } \mathcal{S},\ A_i \cap A_j = \varnothing, \text{ where } i \neq j.$$

then, $\mathcal{S}$ is a pairwise disjoint set.

For example, If

$$\mathcal{S} = \{\{1,\ 4,\ 5\},\ \{2,\ 6\},\ \{3\},\ \{7,\ 8\}\}.$$

then, by inspection, $\mathcal{S}$ is pairwise disjoint because no set within $\mathcal{S}$ contains common elements.

Universal Set

Every set is a subset of U, which is the universal set. The universal set must be explicitly defined or given from context.

Complement Set

A set $\overline{X} = U - X$ is the **complement** of X. In other words, a *complement* of a set X is the set that contains all elements except those in X.

Let

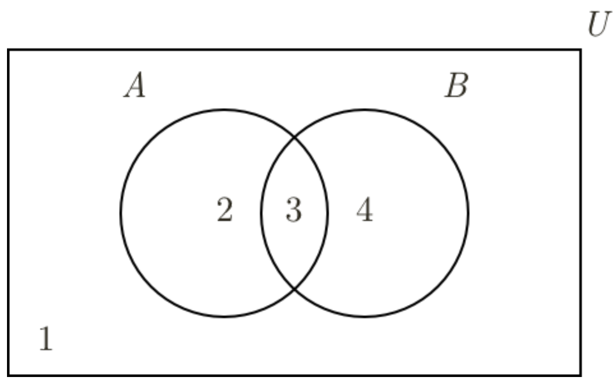
$$A = \{1, 3, 5\}$$
$$U = \{1, 2, 3, 4, 5\}.$$

Then the complement of A is

$$\overline{A} = U - A = \{2, 4\}$$

Venn Diagrams

Venn Diagrams provide pictorial views of a set. In a Venn Diagram, a rectangle depicts a universal set. Subsets of the universal set are drawn as circles, and the members of a set are within the circle.



In the above diagram,

$$
\begin{aligned}
1 &= \overline{(A \cup B)} \\
2 &= A - B \\
3 &= A \cap B \\
4 &= B - A
\end{aligned}
$$

Ordered Pairs

As previously stated, a set is an *unordered* collection of elements. However, sometimes we want to consider the order of elements. An **ordered pair** of elements, written (a, b), is considered distinct from (b, a) so long as $a \neq b$.

Cartesian Product

If X and Y are sets, we let $X \times Y$ denote the set of all ordered pairs (x, y), where $x \in X, y \in Y$. We call this set of ordered pairs a **Cartesian product**.

If $X = \{1, 2, 3\}$ and $Y = \{a, b\}$, then

$$X \times Y = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$
$$Y \times X = \{(a, 1), (b, 1), (a, 2), (b, 2), (a, 3), (b, 3)\}$$

Note, in general, $X \times Y \neq Y \times X$. Also note that $|X \times Y| = |X| \cdot |Y| = 6$. It is always true that $|X \times Y| = |X| \cdot |Y|$.

If $X = \{1, 2\}$ and $Y = \{a, b\}$, and $Z = \{\alpha, \beta\}$, then

$$X \times Y \times Z = \{(1, a, \alpha), (1, a, \beta), (1, b, \alpha), (1, b, \beta), (2, a, \alpha), (2, a, \beta), (2, b, \alpha), (2, b, \beta)\}$$

Set Laws

Let U be a universal set and sets A, B, and C be subsets of U. The following properties hold.

Associative laws:

$$(A \cup B) \cup C = A \cup (B \cup C)$$
$$(A \cap B) \cap C = A \cap (B \cap C)$$

Commutative laws:

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

Distributive laws:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cup (A \cup C)$$

Identity laws:

$$A \cup \varnothing = A, A \cap U = A$$

Complement laws:

$$A \cup \overline{A} = U, A \cap \overline{A} = \varnothing$$

Idempotent laws:

$$A \cup A = A, A \cap A = A$$

Bound laws:

$$A \cup U = U, A \cap \varnothing = \varnothing$$

Absorption laws:

$$A \cup (A \cap B) = A, A \cap (A \cup B) = A$$

Involution law:

$$\overline{\overline{A}} = A$$

0/1 laws:

$$\overline{\varnothing} = U$$
$$\overline{U} = \varnothing$$

De Morgan's laws for sets

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$$
$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$$

1.2 Propositions

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

The following are examples of propositions:

(a) There are 200 bones in the human body.

(b) Earth is the only planet in the universe that contains life.

(c) The only positive integers that divide 7 are 1 and 7 itself.

The following are *not* propositions:

(i) $x + 4 = 6$.

(ii) Fetch me a stack of papers, please.

(i) is *not* a proposition because the truth value of the equation is predicated on the value of x. (ii) is *not* a proposition because it is neither true nor false, rather a command.

The variables p, q, and r are conventionally used to represent propositions. To define a variable, such as p, to be a proposition, use the following notation:

$$p\colon\ 1 + 1 = 3$$

In everyday language, we combine propositions, such as "It is raining" and "It is cold", with connectives, such as *and* and *or*, to form a single proposition, such as "It is raining and it is cold."

Conjunction

The **conjunction** of p and q, denoted $p \wedge q$, is the proposition of p and q. If

$$p : \text{It is raining,}$$
$$q : \text{It is cold,}$$

then, the conjunction of p and q is

$$p \wedge q\text{: It is raining and it is cold.}$$

The truth values of propositions can be illustrated using **truth tables**. The amount of possible combinations of truth values is 2^n, where n is the amount of propositions.

Here is the truth table of the proposition $p \wedge q$:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction

The **disjunction** of p and q, denoted $p \vee q$, is the proposition of p or q. If

$$p : \text{It is spherical,}$$
$$q : \text{It is yellow,}$$

then, the disjunction of p and q is

$$p \vee q\text{: It is spherical or it is yellow.}$$

Here is the truth table of the proposition $p \vee q$, called the *inclusive-or* of p and q:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

In ordinary language, propositions being combined are normally related; but in logic, these propositions are not required to refer to the same subject matter. For example, this proposition is permitted:

$$3 < 5 \text{ or Paris is the capital of England.}$$

Remember: Logic is concerned with the form of propositions and the relation of propositions to each other and not with the subject matter.

Negation

The **negation** of p, denoted $\neg p$, is the proposition not p. If

$$p\text{: Paris is the capital of England,}$$

then, negation of p could be written as one of the following:

$\neg p$: It is not the case that Paris is the capital of England

$\neg p$: Paris is not the capital of England

The truth table of the proposition $\neg p$ is the following:

p	$\neg p$
T	F
F	T

Operator Precedence

In the absence of parentheses, we first evaluate $\neg$, then $\wedge$, and then $\vee$.

For example, consider the following proposition:

$$\neg p \vee q \wedge r$$

We can evaluate the above proposition using the following truth table:

p	q	r	$\neg p$	$q \wedge r$	$\neg p \vee q \wedge r$
T	T	T	F	T	T
T	T	F	F	F	F
T	F	T	F	F	F
T	F	F	F	F	F
F	T	T	T	T	T
F	T	F	T	F	T
F	F	T	T	F	T
F	F	F	T	F	T

From this truth table, it is clear that $\neg p \vee q \wedge r$ can be true in 5 cases and false in 3 cases.

1.3 Conditional Propositions and Logical Equivalence

Conditional Proposition

Consider the following proposition:

If it is raining outside, then I will bring an umbrella.

The above proposition is called a **conditional proposition**, and it states that on the condition that it is raining outside, then I will bring an umbrella.

If we let

p : It is raining outside,
q : I will bring an umbrella,

we can denote the conditional proposition as

$$p \to q.$$

The above can be pronounced as "if p then q" or "p implies q." The proposition p is called the **hypothesis** or **sufficient condition**, and the proposition q is called the **conclusion** or **necessary condition**.

How do you determine the truth value of a conditional proposition, such as the one above? Suppose I say,

If I buy a car, then I will let you drive it.

If I end up buying a car and letting you drive it, then the statement is *true*. However, if I do buy the car and do *not* let you drive it, then the statement is *false*. If I do *not* buy a car, the statement is still true (there is no car for you to drive, but there may be one in the future).

The following table illustrates the truth value of $p \to q$:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

From this, it is clear that a conditional proposition is only *false* when the hypothesis is *true* and the conclusion is *false*.

True by Default

To justify how a conditional proposition is always *true* when p is *false*, consider the following proposition:

For all real numbers x, if $x > 0$, then $x^2 > 0$

If we let

$$P(x) : x > 0,$$
$$Q(x) : x^2 > 0$$

Then we can denote the proposition as

if *P(x)* then *Q(x)*.

If we let $x = -2$, then *P(-2)* is *false* and *Q(-2)* is *true*. If we let $x = 0$, then *P(0)* and *Q(0)* are both *false*. This is why we must define $p \to q$ to be *true* no matter what the truth value of p is. This is called **true by default**.

Operator Precedence

In conditional propositions that involve logical operators $\wedge, \vee, \neg, and\ \to$, the conditional operator $\to$ is evaluated last. Therefore, we now have the following order of precedence:

Operator	*Precedence*
$\neg$	1
$\wedge$	2
$\vee$	3
$\to$	4

Let p be *true*, q be *false*, and r be *true*. Evaluate

(a) $p \wedge q \to r$

(b) $p \vee q \to \neg r$

(c) $p \wedge (q \to r)$

(d) $p \to (q \to r)$

(a) We first evaluate $p \wedge q$, which is $false$, and then we evaluate $p \wedge q \to r$, which is *true*.

(b) We first evaluate $\neg r$, which is $false$, then we evaluate $p \vee q$, which is $true$, and finally we evalute the entire proposition $p \vee q \to \neg r$, which is $false$.

(c) We first evaluate $(q \to r)$, which is $true$, and then evaluate $p \wedge (q \to r)$, which is $true$.

(d) We first evaluate $(q \to r)$, which is $true$, and then we evaluate $p \to (q \to r)$, which is $true$.

Rewriting Propositions as Conditional Propositions

For each proposition, rewrite it as a conditional proposition in the form $p \to q$:

(a) Mary will be a good student if she studies hard.

(b) John takes calculus only if he has sophomore, junior, or senior standing.

(c) When you sing, my ears hurt.

(d) A necessary condition for the Cubs to win the World Series is that they sign a right-handed relief pitcher.

(e) A sufficient condition for Maria to visit France is that she goes to the Eiffel Tower.

(a) - (e) can be rewritten as

(a) If Mary studies hard, then she will be a good student.

(b) "p only if q" is the same as "if p then q", therefore, the proposition can be rewritten as:

If John takes calculus, then he has sophomore, junior, or senior standing.

(c) *When* is the same as *if*; thus the proposition is rewritten as

If you sing, then my ears hurt.

(d) A **necessary condition** is a condition that is necessary for an outcome but does not guarantee the outcome, therefore, we can rewrite it as

If the Cubs win the World Series, then they signed a right-handed relief pitcher.

(e) A **sufficient condition** is a condition that, when met, guarantees an outcome; however, if it is *not* met, the outcome is still possible. We can rewrite this proposition as

If Maria goes to the Eiffel tower, then she visits France.

Converse

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

Let

$$p : 1 > 2,$$
$$q : 4 < 8.$$

Since p is false and q is true, $p \to q$ is *true*. However, its converse, $q \to p$ is *false*. Thus, a conditional proposition can be *true* while its converse is *false*.

For example, if we have the following conditional proposition $p \to q$, we can write its converse symbolically and in words.

If Jerry receives a scholarship, then he will go to college.

Let

p : Jerry receives a scholarship,
q : Jerry goes to college.

The converse is symbolically expressed as $q \to p$, which can be written in words as

If Jerry goes to college, then he receives a scholarship.

Now, if Jerry does *not* receive a scholarship but goes to college anyway, find the truth values of (a) and (b).

(a) $p \to q$

(b) $q \to p$

(a) Since Jerry did *not* receive a scholarship, p is *false*, but he is still going to college, so q is *true*. Therefore, $p \to q$ is *true*.

(b) Since Jerry is going to college, q is *true*. However, he did *not* receive a scholarship, so p is *false*. Therefore, $q \to p$ is *false*.

Biconditional Proposition

A **biconditional proposition**, expressed as $p \leftrightarrow q$ or "p if and only if q", is true when p and q have the same truth values. Thus, the truth value of $p \leftrightarrow q$ is defined by the following truth table:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

In a biconditional proposition, p is both necessary and sufficient for q.

Logical Equivalence

Propositions are said to be **logically equivalent** if they have the same truth value, regardless of the truth values of their constituent propositions $p_1, \dots, p_n$. If P and Q are made up of the propositions $p_1, \dots, p_n$, we say P and Q are logically equivalent and write

$$P \equiv Q$$

provided that, given any truth values of $p_1, \dots, p_n$, P and Q are both *true* or *false*.

For example, we can show that the negation of $p \to q$ is logically equivalent to $p \wedge \neg q$. That is,

$$\neg(p \to q) \equiv p \wedge \neg q.$$

p	q	$p \to q$	$\neg(p \to q)$	$\neg q$	$p \wedge \neg q$
T	T	T	F	F	F
T	F	F	T	T	T
F	T	T	F	F	F
F	F	T	F	T	F

The above demonstrates that $\neg(p \to q)$ is logically equivalent to $p \wedge \neg q$ regardless of the truth values of p and q.

We can use the logical equivalence of $\neg(p \to q)$ and $p \land \neg q$ to help us write the negation of conditional propositions. For example, to negate

if Jerry receives a scholarship, then he goes to college,

we let

$$p : \text{Jerry receives a scholarship,}$$
$$q : \text{Jerry goes to college.}$$

The above proposition can be symbolically written as $p \to q$, and its negation is $\neg(p \to q)$. Since $\neg(p \to q)$ is logically equivalent to $p \land \neg q$, we can negate the proposition by expressing $p \land \neg q$ as words like so:

Jerry receives a scholarship and he does not go to college.

Remember: When evaluating conditional propositions, it is easier to work with the logical operators $\land$, $\lor$, and $\neg$ than the conditional operator $\to$.

Additionally, $p \leftrightarrow q \equiv (p \to q) \land (q \to p)$. This is demonstrated by the following truth table:

p	q	$p \leftrightarrow q$	$p \to q$	$q \to p$	$(p \to q) \land (q \to p)$
T	T	T	T	T	T
T	F	F	F	T	T
F	T	F	T	F	F
F	F	T	T	T	T

De Morgan's Laws for Logic

De Morgan has the following two laws for logic:

$$\neg(p \lor q) \equiv \neg p \land \neg q,$$
$$\neg(p \land q) \equiv \neg p \lor \neg q$$

For the first law, we can demonstrate that $\neg(p \vee q)$ is logically equivalent to $\neg p \wedge \neg q$ using the following truth table:

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Additionally, For the second law, we can demonstrate that $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$ using the following truth table:

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

Contrapositive

The **contrapositive** of the conditional proposition $p \to q$ is the proposition $\neg q \to \neg p$.

For example, consider the following proposition (Assume the network is *not* down and Dale can access the Internet):

> If the network is down, then Dale cannot access the Internet

Let

$$p : \text{The network is down,}$$
$$q : \text{Dale cannot access the Internet}$$

The given proposition written symbolically is

$$p \to q.$$

Since the network is *not* down, the hypothesis p is *false*, therefore, the proposition is *true.* The contrapositive can be written symbolically as

$$\neg q \to \neg p$$

and in words

If Dale can access the Internet, then the network is not down.

Since the hypothesis $\neg q$ is *true* and the conclusion $\neg p$ is *true*, the contrapositive is *true*.

Thus, a conditional proposition and its contrapositive are logically equivalent, as demonstrated in this truth table:

p	q	$p \to q$	$\neg q \to \neg p$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

1.4 Arguments and Rules of Inference

Argument

An **argument** consists of hypotheses together with a conclusion. Any Argument has the form

If p_1 and p_2 and $\ldots$ and p_n, then q.

If p_1 and p_2 and $\ldots$ and p_n are *true*, then the conclusion q must also be true, therefore, the argument is **valid**. An argument is valid because of its form, not because of its content.

An argument is a sequence of propositions written as:

$$\begin{array}{c} p_1 \\ p_2 \\ . \\ . \\ . \\ p_n \\ \hline \therefore q \end{array}$$

The symbol $\therefore$ is read "therefore." The propositions p_1, p_2, $\ldots$, p_n are called the *hypotheses*, and the proposition q is called the *conclusion*.

Deductive Reasoning and Truth Tables

You can use deductive reasoning and truth tables to determine the validity of an argument.

Example 1

For example, consider the following argument and determine whether it is *valid*.

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

First Solution: Deductive Reasoning

For the above argument to be *valid*, both $p \to q$ and p must be *true*. For $p \to q$ to be *true*, q must be *true*. Since q must be *true* for $p \to q$ to be *true*, the argument is *valid*.

Second Solution: Truth Table

We can also determine the argument's validity using a truth table.

Remember: When constructing a truth table to reason about an argument, include a column for each proposition and hypothesis and reserve the last column for the conclusion.

In this instance, there are two propositions p and q, so we reserve the first two columns for them. There are two hypotheses $p \to q$ and p, so we reserve the next two columns for them. Finally, we reserve the last column for the conclusion q.

p	q	$p \to q$	p	q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	F

From this truth table, it is clear that when $p \to q$ and p are *true*, the conclusion q is also *true*. Therefore, the argument is *valid*.

Rules of Inference

A **rule of inference** is a valid argument that is used within an even larger argument. Here are seven rules of inference:

Modus Ponens	$\begin{array}{l} p \to q \\ \underline{p \qquad\quad} \\ \therefore q \end{array}$	**Modus Tollens**	$\begin{array}{l} p \to q \\ \underline{\neg q \qquad\quad} \\ \therefore \neg p \end{array}$
Addition	$\begin{array}{l} \underline{p \qquad\quad} \\ \therefore p \vee q \end{array}$	**Simplification**	$\begin{array}{l} \underline{p \wedge q} \\ \therefore p \end{array}$
Conjunction	$\begin{array}{l} p \\ \underline{q \qquad\quad} \\ \therefore p \wedge q \end{array}$	**Hypothetical Syllogism**	$\begin{array}{l} p \to q \\ \underline{q \to r \qquad} \\ \therefore p \to r \end{array}$
Disjunctive Syllogism	$\begin{array}{l} p \vee q \\ \underline{\neg p \qquad} \\ \therefore q \end{array}$		

Example 2

If the computer has one gigabyte of memory, then it can run Minecraft. If the computer can run Minecraft, then the graphics will be impressive. Therefore, if the computer has one gigabyte of memory, then the graphics will be impressive.

If we let

$$\begin{aligned} p &: \text{The computer has one gigabyte of memory,} \\ q &: \text{The computer can run Minecraft,} \\ r &: \text{The graphics will be impressive.} \end{aligned}$$

The argument can be written symbolically as

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

Therefore, the argument uses the Hypothetical Syllogism rule of inference.

Example 3

Represent the following argument symbolically and determine the validity.

$$\begin{array}{l} \text{If } 2 = 3, \text{ then I ate my hat.} \\ \text{I ate my hat.} \\ \hline \therefore 2 = 3 \end{array}$$

Let

$$p : 2 = 3,$$
$$q : \text{I ate my hat.}$$

The argument can be written

$$\begin{array}{l} p \to q \\ q \\ \hline \therefore p \end{array}$$

If the argument is *valid*, then whenever $p \to q$ and q are both *true*, p must also be *true*. Suppose that $p \to q$ and q are *true*. This is possible if p is *false* and q is *true*. In this case, p is *false* (because $2 = 3$ is *false*); thus, the argument is *invalid*.

Example 4

Represent the argument

$$\begin{array}{l} \text{The bug is either in module 17 or in module 81.} \\ \text{The bug is a numerical error.} \\ \text{Module 81 has no numerical error.} \\ \hline \therefore \text{The bug is in module 17.} \end{array}$$

symbolically and show that it is valid.

Let

$$\begin{aligned} p &: \text{The bug is in module 17.} \\ q &: \text{The bug is in module 81.} \\ r &: \text{The bug is a numerical error.} \end{aligned}$$

Therefore, the argument can be written as

$$\begin{array}{l} p \vee q \\ r \\ r \to \neg q \\ \hline \therefore p \end{array}$$

To determine the argument's validity, we can draw intermediate conclusions using the rules of inference.

From Modus Ponens,

$$\begin{array}{l} r \to \neg q \\ r \\ \hline \therefore \neg q \end{array}$$

we conclude $\neg q$ is *true*, which we can use as a hypothesis in subsequent, intermediate arguments.

From Disjunctive Syllogism,

$$\begin{array}{l} \neg q \\ p \vee q \\ \hline \therefore p \end{array}$$

we conclude that p is *true*, therefore, the argument as a whole is *valid*.

Example 5

Determine the validity of the argument using rules of inference.

If the Chargers get a good linebacker, then the Chargers can beat the Brancos. If the Chargers can beat the Brancos, then the Chargers can bet the Jets. If the Chargers can beat the Broncos, then the Chargers can beat the Dolphins. The Chargers get a good linebacker. Therefore, the Chargers can beat the Jets and the Chargers can beat the Dolphins.

Let

p : Chargers get a good linebacker.
q : Chargers can beat the Brancos.
r : Chargers can beat the Jets.
s : Chargers can beat the Dolphins.

Therefore, the argument can be written as

$$\begin{array}{l} p \to q \\ q \to r \\ q \to s \\ p \\ \hline \therefore r \wedge s \end{array}$$

To determine the argument's validity, we can draw intermediate conclusions using the rules of inference.

From Modus Ponens,

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

we conclude q, which we can use as a hypothesis in the following argument.
From Modus Ponens,

$$\begin{array}{l} q \to r \\ q \\ \hline \therefore r \end{array}$$

we conclude r.
From Modus Ponens,

$$\begin{array}{l} q \to s \\ q \\ \hline \therefore s \end{array}$$

we conclude s.

We used Modus Ponens three times to conclude that q, r, and s are *true*. Therefore, $r \wedge s$ is *true*, thus the argument is *valid*.

1.5 Quantifiers

Propositional Function

Consider the statement

p: n is an odd integer.

It is not a proposition because the truth value is predicated on n. Most statements in math are similar to this, therefore, we must extend the system of logic to include such statements.

A **propositional function** $P(x)$ is a function with respect to a set D, where each $x \in D$. We call D the **domain of discourse**.

Example 1

Let

$$P(n) : n \text{ is an odd integer.}$$

Then P is a propositional function with respect to set Z^+ (set of positive integers). For each $n \in Z^+$, $P(n)$ is a proposition.

Let

$$P(1) : 1 \text{ is an odd integer,}$$
$$P(2) : 2 \text{ is an odd integer}$$

Clearly, $P(1)$ is *true* and $P(2)$ is *false*.

Remember: A propositional function P by itself is neither *true* nor *false*; however, for each x in the domain of discourse, $P(x)$ is a proposition and is, therefore, either *true* or *false*.

The following is a list of valid propositional functions:

(a) $n^2 + 2n$ is an odd integer (domain of discourse = Z^+)

(b) $x^2 - x - 6 = 0$ (domain of discourse = R)

(c) The restaurant rated over two stars (domain of discourse = rated restaurants)

(c) by itself is not a proposition; however, "restaurant" can be replaced with a restaurant, such as "Portillo's", to produce a proposition.

Universally Quantified Statement

Let P be a propositional function with domain of discourse D. Then,

$$\forall x P(x)$$

is said to be a **universally quantified statement**. It is *true* if $P(x)$ is *true* for every x in D. It is *false* if $P(x)$ is *false* for at least one x in D. Such an x that makes $P(x)$ *false* is a **counterexample**. The symbol $\forall$ may be read “for every”, “for all”, or “for any.”

To prove that

$$\forall x P(x)$$

is *true*, we must examine *every* value of x in set D to show that for every x, $P(x)$ is *true*. However, it is much easier to find a counterexample such that $P(x)$ is *false*.

Remember: To disprove $\forall x P(x)$, find one x in set D such that $P(x)$ is *false*.

Example 2

Consider the universally quantified statement with domain of discourse **R**.

$$\forall x(x^2 \geq 0).$$

The statement is *true* because, *for every* real number x, $x^2 \geq 0$.

Example 3

The universally quantified statement

$$\text{for every real number } x, \text{ if } x > 1, \text{ then } x + 1 > 1$$

is *true*. If $x \leq 1$, the hypothesis $x > 1$ is *false*, therefore, the proposition is *true*. If $x > 1$, since

$$x + 1 > x \text{ and } x > 1,$$

we conclude that $x + 1 > 1$, so the conclusion is *true*. If $x > 1$, the hypothesis and conclusion are both *true*, hence the universally quantified statement is *true*.

Existentially Quantified Statement

Let P be a propositional function with domain of discourse D. Then,

$$\exists x P(x)$$

is said to be an **existentially quantified statement**. It is *true* if $P(x)$ is *true* for at least one x in D. It is *false* if $P(x)$ is *false* for every x in D. The symbol $\exists$ is read as "there exists", "for some", or "for at least one."

Example 4

Consider the existentially quantified statement with domain of discourse $\mathbf{R}$.

$$\exists x \left(\frac{x}{x^2+1} = \frac{2}{5} \right)$$

If we can find one real number x such that $\left(\frac{x}{x^2+1} = \frac{2}{5} \right)$, then the existentially quantified statement is *true*.

If $x = 2$, then,

$$\left(\frac{2}{2^2+1} = \frac{2}{5} \right)$$

therefore, $\exists x \left(\frac{x}{x^2+1} = \frac{2}{5} \right)$ is *true*.

Example 5

Verify that the following existentially quantified statement is *false*.

$$\exists x \in \mathbf{R} \left(\frac{1}{x^2+1} > 1 \right)$$

It is *false* if $\left(\frac{1}{x^2+1} > 1 \right)$ is *false* for every real number x.

$$\exists x \in \mathbf{R} \left(\frac{1}{x^2+1} > 1 \right)$$

is *false* when

$$\forall x \in \mathbf{R} \left(\frac{1}{x^2+1} \leq 1 \right)$$

is *true*. Therefore, we must show that $\left(\frac{1}{x^2+1} \leq 1 \right)$ is *true* for every real number x.

De Morgan's Laws for Logic

$$\neg(\forall x P(x)) \equiv \exists x \neg P(x)$$
$$\neg(\exists x P(x)) \equiv \forall x \neg P(x)$$

Example 6

Write the following statement symbolically and write the negation symbolically and in words.

Every rock fan loves U2.

Let

$$P(x) = x \text{ loves U2},$$
$$D = \text{ the set of rock fans.}$$

Then, the statement is symbolically written as

$$\forall x P(x).$$

And the negation, $\neg(\forall x P(x))$, is

$$\exists x \neg P(x),$$

which can be read as

There exists a rock fan who does not love U2.

Example 7

Write the following statement symbolically and write the negation symbolically and in words.

Some birds cannot fly

Let

$$P(x) = x \text{ can fly},$$
$$D = \text{ the set of all birds.}$$

Then, the statement is symbolically written as

$$\exists x \neg P(x).$$

And the negation, $\neg(\exists x \neg P(x))$, is

$$\forall x \neg\neg P(x) = \forall x P(x)$$

which can be read as

All birds can fly.

Generalizing Propositions

A universally quantified statement such as the one above generalizes the proposition

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n$$

in the sense that the individual propositions are replaced by a family $P(x)$. In other words,

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \equiv \forall x P(x).$$

Similarly, an existentially quantified statement generalizes the proposition

$$p_1 \vee p_2 \vee \cdots \vee p_n$$

in the sense that the individual propositions are replaced by a family $P(x)$. In other words,

$$p_1 \vee p_2 \vee \cdots \vee p_n \equiv \exists x P(x).$$

Example 7

If the domain of discourse of the propositional function P is {-1, 0, 1}, then $\forall x P(x)$ is equivalent to

$$P(-1) \wedge P(0) \wedge P(1).$$

And by De Morgan's laws of logic, the negation $\neg(P(-1) \wedge P(0) \wedge P(1))$ is logically equivalent to

$$\neg P(-1) \vee \neg P(0) \vee \neg P(1) \equiv \exists x \neg P(x)$$

Example 8

The following statement

All that glitters is not gold

has multiple interpretations. Such interpretations include

(a) Every object that glitters is not gold

(b) Some object that glitters is not gold

If we let

$$P(x) : x \text{ glitters},$$
$$Q(x) : x \text{ is gold},$$

then (a) is symbolically written as

$$\forall x(P(x) \to \neg Q(x))$$

and (b) is symbolically written as

$$\exists x(P(x) \wedge \neg Q(x)).$$

Since $\neg(p \to q) \equiv p \wedge \neg q$, (b) is logically equivalent to

$$\exists x \neg(P(x) \to Q(x)).$$

Since $\exists x \neg P(x) \equiv \neg(\forall x P(x))$, (b) is also logically equivalent to

$$\neg(\forall x P(x) \to Q(x)).$$

Thus, the correct interpretation results from negating the original statement.

Rules of Inference for Quantified Statements

Universal instantiation $\dfrac{\forall x P(x)}{\therefore P(d) \text{ if } d \in D}$

Universal generalization $\dfrac{P(d) \text{ for every } d \in D}{\therefore \forall x P(x)}$

Existential instantiation $\dfrac{\exists x P(x)}{\therefore P(d) \text{ for some } d \in D}$

Existential generalization $\dfrac{P(d) \text{ for some } d \in D}{\therefore \exists x P(x)}$

Example 9

Let

$$P(x) : x \text{ owns a laptop}$$
$$D : \{x \mid x \text{ is a student in MA 309}\}$$

Suppose that Matthew, who is taking MA 309, owns a laptop; in symbols, $P(Matthew)$ is *true*. Then, by existential generalization, $\exists x P(x)$ is *true*.

Example 10

Write the argument symbolically and then, using rules of inference, show that it is valid.

For every real number x, if x is an integer, then x is a rational number. The number $\sqrt{2}$ is not rational. Therefore, $\sqrt{2}$ is not an integer.

Let

$$P(x) : x \text{ is an integer,}$$
$$Q(x) : x \text{ is rational.}$$

Then the argument is written symbolically as

$$\begin{array}{l} \forall x \in \mathbf{R}(P(x) \to Q(x)) \\ \neg Q(\sqrt{2}) \\ \hline \therefore \neg P(\sqrt{2}) \end{array}$$

Since $\sqrt{2} \in \mathbf{R}$, we may use Universal instantiation to conclude $P(\sqrt{2}) \to Q(\pi)$. Combining $P(\sqrt{2}) \to Q(\pi)$ and $\neg Q(\pi)$, we use modus tollens to conclude $\neg P(\sqrt{2})$.

Chapter 2: Proofs

2.1 Mathematical Systems, Direct Proofs, and Counterexamples

A **mathematical system** consists of **axioms**, which are assumed to be true and **definitions**, which are used to create new concepts in terms of existing ones. Within a mathematical system, we can derive a **theorem**, which is a proposition that has been proved to be true.

There are two special types of theorems:

- **lemma:** not interesting in its own right, but useful for proving other theorems.
- **corollary:** follows easily from another theorem.

A **proof** is an argument that establishes the truth of a theorem. Logic is used to analyze proofs.

Mathematical Systems

Example 1

One example of a mathematical system is Euclidean geometry. This mathematical system contains the following theorem and corollary:

- **theorem:** If two sides of a triangle are equal, then the angles opposite them are equal.
- **corollary:** If a triangle is equilateral, then it is equiangular.

The corollary follows immediately from the theorem.

Example 2

Examples of theorems about real numbers are:

- $x \times 0 = 0$ for every real number x.
- For all real numbers x, y, z, if $x \leq y$ and $y \leq z$, then $x \leq z$.

Direct Proofs

Theorems are often of the form

For all $x_1, x_2, \ldots, x_n$, if $p(x_1, x_2, \ldots, x_n)$, then $q(x_1, x_2, \ldots, x_n)$.

The above is true provided that the conditional proposition $p \to q$ is true for all $x_1, x_2, \ldots, x_n$ in the domain. A **direct proof** assumes that $p(x_1, x_2, \ldots, x_n)$ is true and then, using $p(x_1, x_2, \ldots, x_n)$ as well as other axioms, definitions, previously derived theorems, and rules of inference, shows directly that $q(x_1, x_2, \ldots, x_n)$ is true.

For example, to use the terms "even integer" and "odd integer" in a proof, we must first define them.

An integer n is *even* if there exists an integer k such that $n = 2k$.
An integer n is *odd* if there exists an integer k such that $n = 2k + 1$.

Example 3

Give a direct proof of the following statement:

For all integers m and n, if m is odd and n is even, then $m + n$ is odd.

We begin by first writing out the hypothesis and conclusion:

m is odd and n is even. (Hypothesis)
$\ldots$
$m + n$ is odd. (Conclusion)

We begin to fill in the gaps using the definitions of even and odd:

m is odd and n is even. (Hypothesis)
$m = 2k_1 + 1$ (k_1 is an integer)
$n = 2k_2$ (k_2 is an integer)
...
$m + n$ is odd. (Conclusion)

Finally, to derive our conclusion, we use the definition of odd once again:

$$\begin{aligned} m + n &= (2k_1 + 1) + 2k_2 \\ &= 2(k_1 + k_2) + 1 \end{aligned}$$

Our final proof:

m is odd and n is even. (Hypothesis)
$m = 2k_1 + 1$ (k_1 is an integer)
$n = 2k_2$ (k_2 is an integer)
$m + n = 2(k_1 + k_2) + 1$
$m + n$ is odd. (Conclusion)

Example 4

Give a direct proof of the following statement:

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$

We begin by first writing out the hypothesis and conclusion:

X, Y, and Z are sets. (Hypothesis)
...
$X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$ (Conclusion)

We are trying to conclude that sets $X \cap (Y - Z)$ and $(X \cap Y) - (X \cap Z)$ are equal. Recall the definition of set equality:

For every x, if $x \in X$, then $x \in Y$
For every x, if $x \in Y$, then $x \in X$

X, Y, and Z are sets. (Hypothesis)
If $x \in X \cap (Y - Z)$, then $x \in (X \cap Y) - (X \cap Z)$
If $x \in (X \cap Y) - (X \cap Z)$, then $x \in X \cap (Y - Z)$
...
$X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$ (Conclusion)

We begin to fill in the gaps using the definition of set equality:
To derive our conclusion, we must first prove

If $x \in X \cap (Y - Z)$, then $x \in (X \cap Y) - (X \cap Z)$

and

If $x \in (X \cap Y) - (X \cap Z)$, then $x \in X \cap (Y - Z)$.

To prove the former, let $x \in X \cap (Y - Z)$. By the definition of intersection, if $x \in X \cap (Y - Z)$, then $x \in X$ and $x \in Y - Z$. By the definition of set difference, if $x \in Y - Z$, then $x \in Y$, but $x \notin Z$. If $x \in X$ and $x \in Y$, then $x \in X \cap Y$. If $x \in X \cap Y$ and $x \notin Z$, then $x \notin X \cap Z$. Therefore, if $x \in X \cap (Y - Z)$, then $x \in (X \cap Y) - (X \cap Z)$.

To prove the latter, let $x \in (X \cap Y) - (X \cap Z)$. By set difference, if $x \in (X \cap Y) - (X \cap Z)$, then $x \in (X \cap Y)$ and $x \notin (X \cap Z)$. If $x \in (X \cap Y)$, then, by intersection, $x \in X$ and $x \in Y$. If $x \in X$ and $x \notin X \cap Z$, then $X \notin Z$. By the definition of set difference, since $x \in Y$ and $x \notin Z$, $x \in Y - Z$. Finally, since $x \in X$ and $x \in Y - Z$, then $x \in X \cap (Y - Z)$. Therefore, if $x \in (X \cap Y) - (X \cap Z)$, then $x \in X \cap (Y - Z)$.

Since we proved both of these equations, it follows that

$$X \cap (Y - Z) = (X \cap Y) - (X \cap Z).$$

The following example illustrates the use of **subproofs**.

Example 5

If a and b are real numbers, we define $min\{a, b\}$

$$min\{a, b\} = a \text{ (if } a < b)$$
$$min\{a, b\} = a \text{ (if } a = b)$$
$$min\{a, b\} = b \text{ (if } a > b).$$

Give a direct proof of the following statement.

For all real numbers d, d_1, d_2, x, if $d = min\{d_1, d_2\}$ and $x \leq d$, then $x \leq d_1$ and $x \leq d_2$.

We begin by first writing out the hypothesis and conclusion:

$d = min\{d_1, d_2\}$ and $x \leq d$ (Hypothesis)
...
$x \leq d_1$ and $x \leq d_2$ (Conclusion)

To help us better understand, we give an example using real numbers. Remember, since we are trying to prove a universally quantified statement, one example where the statement is true is not a proof.

Let

$$\begin{aligned} d_1 &= 2 \\ d_2 &= 4 \\ d &= min\{d_1, d_2\} = 2 \\ x &= 1 \end{aligned}$$

From the definition of $min\{a, b\}$ from above, the minimum d of two numbers, d_1 and d_2, is equal to one of the two numbers and less than or equal to the other one. In other words,

$$d \leq d_1 \text{ and } d \leq d_2.$$

We know that $x \leq d$, so, by the Theorem in Example 2,

If $x \leq d$ and $d \leq d_1$, then $x \leq d_1$.
If $x \leq d$ and $d \leq d_2$, then $x \leq d_2$.

The outline of our proof is now:

Disproving a Universally Quantified Statement

Recall that to disprove $\forall x P(x)$, you need to find one x in the domain of discourse such that $P(x)$ is false. Such a value for x is called a *counterexample*.

$d = min\{d_1, d_2\}$ and $x \le d$ (Hypothesis)
$d \le d_1$ and $d \le d_2$ (Definition of "minimum")
From $x \le d$ and $d \le d_1$, deduce $x \le d_1$ (Theorem).
From $x \le d$ and $d \le d_2$, deduce $x \le d_2$ (Theorem).
$x \le d_1$ and $x \le d_2$ (Conclusion)

Example 6

The statement

$$\forall n \in \mathbf{Z}^+(2^n + 1 \text{ is prime})$$

is false. If we assume that it is true, to disprove it, we just need to find one n that is a positive integer where $2^n + 1$ is false. A counterexample is $n = 3$, because $2^3 + 1 = 9$ is false.

Problem-Solving Tips

To construct a proof of a universally quantified statement, first write down the hypothesis and the conclusion. To construct the argument, remind yourself what you know about the terms (e.g., "even," "odd"), symbols (e.g., $X \cap Y$, $min\{d_1, d_2\}$). To understand what is to be proved, look at some specific values in the domain. When proving a universally quantified statement, simply showing the statement is true for specific values is not sufficient; however, it may help you understand the statement. To disprove a universally quantified statement, find one element x in the domain that makes the propositional function $P(x)$ false. If asked to prove or disprove a universally quantified statement, you can begin by trying to prove it. If you succeed, you are finished. If not, try to disprove it with a counterexample.

2.2 More Methods of Proof

Proof by Contradiction (Indirect Proof)

A **proof by contradiction**, or an indirect proof, establishes $p \to q$ by assuming the hypothesis p is true and that the conclusion q is false and then, using p and $\neg q$ as well as other axioms, definitions, previously derived theorems, and rules of inference to derive a **contradiction**. Basically, we derive $r \wedge \neg r$ and then conclude that q is true.

Note that

$$p \to q \equiv (p \wedge \neg q) \to (r \wedge \neg r)$$

Example 1

Give a proof by contradiction of the following statement:

For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

Since it is not clear how to get from $n^2 = 2k_1$ to $n = 2k_2$ with a direct proof, we will try a proof by contradiction and assume n is *odd*.

n^2 is even (Hypothesis)
$n = 2k + 1$ (k is an integer)
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
n^2 is odd. (Contradiction)
n is odd (Conclusion)

From the proof, we have deduced that n^2 is odd, which *contradicts* our hypothesis that n^2 is even. Thus, we have derived $r \wedge \neg r$, where

$$r : n^2 \text{ is even.}$$

Example 2

Give a proof by contradiction of the following statement:

For all real numbers x and y, if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

We will assume the conclusion, $x \geq 1 \vee y \geq 1$ is false, so by De Morgan's law of logic, our conclusion will be

$$\neg(x \geq 1 \vee y \geq 1) \equiv \neg(x \geq 1) \wedge \neg(y \geq 1) \equiv (x < 1) \wedge (y < 1)$$

We add the two inequalities and obtain

x + y ¡ 1 + 1 = 2

We have derived a contradition: $x + y < 2$ and $x + y \geq 2$.

Example 3

Prove by contradiction that $\sqrt{2}$ is irrational.

$\sqrt{2}$ is irrational (Hypothesis)

$$\begin{aligned}
\sqrt{2} &= \frac{p}{q} \text{ (p and q are integers and are not both even)} \\
2 &= \frac{p^2}{q^2} \\
2q^2 &= p^2 \text{ (p^2 is even, therefore p is even, so $p = 2k$)} \\
2q^2 &= (2k)^2 = 4k^2 \\
q^2 &= 2k^2 \text{ (q^2 is even, therefore q is even)}
\end{aligned}$$

$\sqrt{2}$ is rational (Conclusion)

From our proof, we derive that both p and q are even, which contradicts our assumption that p and q are not both even.

Proof by Contrapositive

Recall that the contrapositive of the conditional proposition $p \rightarrow q$ is $\neg q \rightarrow \neg p$ and both are logically equivalent. In a **proof by contrapositive**, we prove that $\neg q \rightarrow \neg p$.

Example 4

Use a proof by contrapositive to show that

For all $x \in \mathbf{R}$, if x^2 is irrational, then x is irrational.

Since we are using a proof by contrapositive, we want to prove that

If x is rational, then x^2 is rational.

If x is rational, then $x = \frac{p}{q}$ for some integers p and q.

x is rational (Hypothesis)
$x = \frac{p}{q}$ (x is rational, p and q are integers)
$x^2 = \frac{p^2}{q^2}$
x^2 is rational (Conclusion)

Proof by Cases

Proof by cases is used when the original hypothesis naturally divides itself into various cases. If p is equivalent to $p_1 \vee p_2 \vee \cdots \vee p_n$ (where $p_1, p_2, \ldots, p_n$ are the cases), instead of proving $(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$, we prove

$$(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q).$$

Sometimes the number of cases to prove is finite, so we check them all at once with an **exhaustive proof**.

Example 5

Using proof by cases, prove that $2m^2 + 3n^2 = 40$ has no solutions in positive integers.

If $2m^2 + 3n^2 = 40$, then m and n are restricted in size. In other words,

$$\begin{aligned} 2m^2 &\leq 40, \\ 3n^2 &\leq 40. \end{aligned}$$

Therefore,

$$\begin{aligned} m^2 &\leq 20, \\ n^2 &\leq \frac{40}{3} \approx 13.33. \end{aligned}$$

From this, we can see that m can be at most 4 (because when $m = 5$, $m^2 = 25$, which is not less than 20). Additionally, n can be at most 3. Thus, it suffices to check the cases

$$m = 1, 2, 3, 4$$
$$n = 1, 2, 3.$$

		m			
		1	2	3	4
	1	5	11	21	35
n	2	14	20	30	44
	3	29	35	45	59

Since $2m^2+3n^2 \neq 40$ for $m = 1, 2, 3, 4$ and $n = 1, 2, 3$, and $2m^2+3n^2 > 40$ for $m > 4$ or $n > 3$, $2m^2 + 3n^2 = 40$ has no solutions in positive integers.

Proofs of Equivalence

Theorems in the form "p if and only if q", or $p \leftrightarrow q$ are proved using the logical equivalence

$$(p \to q) \land (q \to p).$$

In other words, two propositions must be proved.

Example 6

Prove that for every integer n, n is odd if and only if $n - 1$ is even.

Let

$$p : n \text{ is odd},$$
$$q : n - 1 \text{ is even}.$$

We first prove $p \to q$:

n is odd (Hypothesis)
$n = 2k + 1$ (k is an integer)
$n - 1 = (2k + 1) - 1 = 2k$
$n - 1$ is even (Conclusion)

Now, we prove $q \to p$:

$n - 1$ is even (Hypothesis)
$n - 1 = 2k$ (k is an integer)
$n = 2k + 1$
n is odd (Conclusion)

Some theorems state that three or more statements are logically equivalent. To prove that $p_1, p_2, \ldots, p_n$ are equivalent, we must prove

$$(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n) \wedge (p_n \to p_1).$$

Existence Proofs

A proof of $\exists x P(x)$ is called an **existence proof**. To prove it, we must find one x such that $P(x)$ is true.

Example 7

Let a and b be real numbers with $a < b$. Prove that there exists a real number x satisfying $a < x < b$.

It suffices to find one real number x satisfying $a < x < b$. The real number is

$$x = \frac{a+b}{2}.$$

Example 8

Prove that there exists a prime p such that $2^p - 1$ is not prime.

By trial and error, we find that $2^p - 1$ is prime for $p = 2, 3, 5, 7$ but not $p = 11$. Thus, $p = 11$ makes the statement true.

Example 9

Let

$$A = \frac{s_1 + s_2 + \cdots + s_n}{n}$$

be the average of the real numbers $s_1 + s_2 + \cdots + s_n$. Prove that there exists i such that $s_i \geq A$. By proof of contradiction, we assume the negation of the conclusion, which is $\forall i (s_i < A)$.

there exists i (Hypothesis)
$s_1 + s_2 + \cdots + s_n < nA$
$\frac{s_1+s_2+\cdots+s_n}{n} < A$
$\forall i(s_i < A)$ (Conclusion)

2.4 Mathematical Induction

Suppose there are 5 blocks on an infinitely long table. Also, suppose that

The first block is marked with an "x",
For all n, if block n is marked, then block $n + 1$ is marked

By examining the five blocks on the table, one-by-one, and determining that they are marked with an "x", you are performing **mathematical induction**.

Let S_n denote the sum of the first n positive integers:

$$S_n = 1 + 2 + \cdots + n$$

Suppose someone claims that, for all $n \geq 1$,

$$S_n = \frac{n(n+1)}{2}.$$

In other words,

$$S_1 = \frac{1(2)}{2} = 1$$
$$S_2 = \frac{2(3)}{2} = 3$$
$$\dots$$

Obviously, the equation is true for S_1 and S_2, so we *assume* it is true for S_n. But what about S_{n+1}? Assuming S_n is true, we must show that

$$S_{n+1} = \frac{(n+1)(n+2)}{2}$$

is also true.

Recall that

$$S_n = 1 + 2 + \cdots + n.$$

Therefore,

$$S_{n+1} = 1 + 2 + \cdots + n + (n+1).$$

Notice that S_n is contained within S_{n+1}. In other words, the first part of S_{n+1} is S_n. Because of

$$S_n = \frac{n(n+1)}{2},$$

we have

$$S_{n+1} = S_n + (n+1) = \frac{n(n+1)}{2} + (n+1).$$

Performing algebraic manipulation, we have

$$
\begin{aligned}
S_{n+1} = \frac{n(n+1)}{2} + (n+1) &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{n^2 + 3n + 2}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}
$$

Thus, assuming $S_n = \frac{n(n+1)}{2}$, we have proved that S_{n+1} is

$$\frac{(n+1)(n+2)}{2}$$

and that all of the equations for all n are true. Our proof using mathematical induction consisted of two steps. We first verified that S_1 was true. Second, we *assumed* that S_n was true to prove that S_{n+1} is true. The trick is to relate a statement n to statement $n+1$.

Principle of Mathematical Induction

Suppose we have a propositional function $S(n)$ whose domain of discourse is all positive integers. Suppose that

$S(1)$ is true; **(Basis Step)**

for all $n \geq 1$, if $S(n)$ is true, then $S(n+1)$ is true. **(Inductive Step)**

Then, $S(n)$ is true for every positive integer n. The Basis Step is to prove that the propositional function $S(n)$ is true for the smallest value in the domain of discourse.

Example 1

Use induction to show that $n! \geq 2^{n-1}$ for all $n \geq 1$.

We define $n!$ (n factorial) as

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n(n-1)(n-2)\ldots 2 \cdot 1 & \text{if } n \geq 1 \end{cases}$$

In other words, if $n \geq 1$, $n!$ is equal to the product of all the integers between 1 and n inclusive. For example,

$$3! = 3 \cdot 2 \cdot 1 = 6.$$

We first perform the **basis step**, where we show that $n! \geq 2^{n-1}$ is true when $n = 1$:

$$1! = 1 \geq 2^{1-1} = 2^0 = 1$$

Next, for the **inductive step**, we *assume* that $n! \geq 2^{n-1}$ is true for all $n \geq 1$ and prove that it is also true for $(n+1)$. Therefore, we want to prove that

$$(n+1)! \geq 2^n$$

is true.

To prove the above, notice that

$$(n+1)! = (n+1)(n!)$$

Now,

$$\begin{aligned} (n+1)! &= (n+1)(n!) \\ &\geq (n+1)2^{n-1} \\ &\geq 2 \cdot 2^{n-1} \\ &= 2^n. \end{aligned}$$

Example 2

Use induction to show that if $r \neq 1$,

$$a + ar^1 + ar^2 + \cdots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1}$$

for all $n \geq 0$.

Basis Step

Since 0 is the smallest number in the domain, we must prove that the above equation is true for when $n = 0$. When $n = 0$,

$$a = \frac{a(r^1 - 1)}{r - 1}$$

which is true.

Inductive Step

We assume that, if $r \neq 1$,

$$a + ar^1 + ar^2 + \cdots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1}$$

is true for all $n \geq 0$.

We must prove that it is true for $n + 1$. Thus,

$$\begin{aligned} a + ar^1 + ar^2 + \cdots + ar^n + ar^{n+1} &= \frac{a(r^{n+1} - 1)}{r - 1} + ar^{n+1} \\ &= \frac{a(r^{n+1} - 1)}{r - 1} + \frac{ar^{n+1}(r - 1)}{r - 1} \\ &= \frac{a(r^{n+2} - 1)}{r - 1} \end{aligned}$$