Samedi 26 août 2023 | 1 | The Foundations: Logic and Proofs

1.1 Propositional Logic

The rules of logic give precise meaning to mathematical statements. These rules are used to distinguish between valid and invalid mathematical arguments.
Because a major goal of this book is to teach the reader how to understand and how to construct correct mathematical arguments, we begin our study of discrete mathematics with an introduction to logic.

Propositions

Our discussion begins with an introduction the basic building blocks of logic: propositions.

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

Example 1 | All the following declarative sentence are propositions.
(I.) Washington, D.C. is the capital of the U.S.A.
(II.) Toronto is the capital of Canada.
(III.) $1+1=2$
(IV.) $2+2=3$

Propositions (I.) and (III.) are true whereas (II.) and (IV.) are false.

Example 2 | Consider the following sentences.
(I.) What time is it?
(II.) Read this carefully.
(III.) $x+1=2$
(IV.) $x+y=z$

Sentences (I.) and (II.) are not propositions because they are not declarative sentences.
Sentences (III.) and (IV.) are not propositions because they are neither true or false. Note that each of sentences (III.) and (IV.) can be turned into a proposition if we assign values to the variables.

We use letters to denote **propositional variables** (or **sentential variables**), that is, variables that represent propositions, just as letter are used to denote numerical variables. The conventional letters used for propositional variables are $p, q, r, s, \ldots$ The **truth value** of a proposition are true (T) or false (F).
Propositions that cannot be expressed in terms of simpler propositions are called **atomic proposition**. The area of logic that deals with proposition is called the **propositional calculus** or **propositional logic**. (Introduced by Greek philosopher Aristotle more than 2300 years ago)
Many mathematical statements are constructed by combining one or more propositions. New propositions, called **compound propositions**, are formed from existing proposition using **logical operators**.

Definition 1. Let p be a proposition. The **negation** of p, denoted by $\neg p$ (also denoted by $\bar{p}$) is the statement "It is not that p." The proposition $\neg p$ is read "not p".
The truth value of the negation of p, $\neg p$, is the opposite of the truth value of p.
Remark: The notation for the negation operator is not standardized. Other notations you might see are $\sim p$, $-p$, p', Np, and $!p$.

It can also be considered the result of the operation of the negation operator on a proposition.

Example 3 | Find the negation of the proposition "Michael's PC runs Linux"
"It is not the case that Michael's PC runs Linux."
or more simply "Michael's PC does not run Linux."

Example 4 | Find the negation of the proposition "Vandana's smartphone has at least 32 GB of memory"
"It is not the case that ... "
also "Vandana's smartphone does not have at least 32GB of memory"
or even more simply "Vandana's smartphone has less than 32 GB of memory"

Definition 2. Let p and q be proposition. The **conjunction** of p and q, denoted by $p \wedge q$, is the proposition "p and q"
The conjunction $p \wedge q$ is true when both p and q are true and is false otherwise.
Note that in logic the word "but" sometimes is used instead of "and" in a conjunction. Eg. "The suns is shining, but it is raining" ≡ "The sun is shinning and it is raining."
(In natural language, there is a subtle difference in meaning between "and" and "but"; we will not be concerned with this nuance here.

Example 5 | Find the conjunction of the propositions p and q where p: "Rebecca's PC has more than 16 GB free hard disk space"
and q: "The processor in Rebecca's PC runs faster than 1 GHz"

"Rebecca's PC has more than 16 GB free hard disk space, and its processor runs faster than 1GHz." For this conjunction to be true, both conditions given must be true. It is false when one or both of these conditions are false.

Definition 3. Let p and q be proposition. The **disjunction** of p and q, denoted by $p \vee q$, is the proposition "p or q".
The disjunction $p \vee q$ is false when both p and q are false and is true otherwise (inclusive or).
A disjunction is true when at least one of the two propositions is true.

Example 7 | What is the disjunction of the propositions p and q same as Ex.5?
"Rebecca's PC has at least 16 GB free hard disk space, or the processors in Rebecca's PC runs faster than 1 GHz." It is false when both of these conditions are false, that is, when Rebecca's PC has less than 16 GB free hard disk space and the processor in her PC runs at 1GHz or slower.

Definition 4. Let p and q be propositions. The **exclusive or** of p and q, denoted by $p \oplus q$ (or p XOR q) is the proposition that is true when exactly one of p and q is true and it is false otherwise.

Example 8 | Let p and q be the propositions that state "A student can have a salad with dinner" and "A student can have soup with dinner", respectively. What is $p \oplus q$, the exclusive or of p and q?
"A student can have soup or salad, but not both, with dinner."
or "A student can have soup or a salad with dinner" without explicitly stating that taking both is not permetted.

Example 9 | Express the statement "I will use all my savings to travel to Europe or to buy an electric car" in propositional logic.
To translate this statement, we first note that the or in this statement must be an exclusive or because this student can either use all his or her savings to travel to Europe or use all these savings to buy an electric car, but cannot both go to Europe and buy an electric car. (This is clear because either option requires all his savings.) Hence, this statements can be expressed as $p \oplus q$.

Conditional Statements

Definition 5. Let p and q be propositions. The **conditional statement** $p \rightarrow q$ is the proposition "if p, then q". The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise.
conclusion (or consequence).
hypothesis (or antecedent or premise)
A conditional statement is also called an **implication**.

A usefull way to understand the truth value of a conditional statement is to think of an obligation or contract.
For example, the pledge many politicians make when running for office is "if I am elected, then I will lower taxes."
It is only when the politician is elected but does not lower taxes that voters can say that the politician has broken the compaign pledge.
This last scenario corresponds to the case when p is true but q is false in $p \rightarrow q$.
Similarly, consider a statement that a professor might make: "If you get 100% on the final, then you will get an A."
If you manage to get 100% on the final, then you would expect to receive an A. However, if you do not get 100%, you may or may not receive an A depending on other factors. However, if you do get 100%, but the proffessor does not give you an A, you will feel cheated.
Remark: "p only if q" says that p cannot be true when q is not true. That is, the statement is false if p is true, but q is false.
When p is false, q may be either true or false, because the statement say nothing about the truth value of q.
For example, suppose the proffessor tells you "You can $\underbrace{\text{receive an A}}_{p}$ in the course only if you score on the final $\underbrace{\text{is at least 90\%}}_{q}$."
≡ q is necessary for p.
≡ p is suffisant for q.

Because conditional statements play such an essential role in mathematical reasoning, a variety of terminology is used to express $p \rightarrow q$:

"if p, then q"	"q if p"
"p implies q"	"q when p"
"if p, q"	"q whenever p"
"p only if q"	"q is necessary for p"
"p is sufficient for q"	"A sufficient condition for q is p"
"A necessary condition for p is q"	"q unless $\neg p$"
	"q follows from p"
	"q provided that p"

To remember that "q unless $\neg p$" expresses the same conditional statement as "if p, then q", note that "q unless $\neg p$" means that if $\neg p$ is false, then q must be true.
That is, the statement "q unless $\neg p$" is false when p is true but q is false, but it is true otherwise. Consequently, "q unless $\neg p$" and $p \rightarrow q$ always have the same truth value.

Example 10 | Let p be the statement "Maria learns discrete mathematics" and q the statement "Maria will find a good job."
Express the statement $p \rightarrow q$ as a statement in English.
"If Maria learns discrete mathematics, then she will find a good job."
"Maria will find a good job when she learns discrete mathematics."
"For Maria to get a good job, it is sufficient for her to learn dm."
"Maria will find a good job unless she does not learn dm."

The mathematical concept of a conditional statement is independent of a cause-and-effect relationship between hypothesis and conclusion.
Our definition of a conditional statement specifies its truth values; it is not based on English usage.

Converse, Contrapositive, and Inverse

Implication $p \rightarrow q$ ≡ Contrapositive $\neg q \rightarrow \neg p$

The contrapositive is false when $\neg p$ is false and $\neg q$ is true.
that is, only when p is true and q is false.

Converse (Réciproque) $q \rightarrow p$ $\underbrace{\equiv}_{\text{equivalent}}$ Inverse $\neg p \rightarrow \neg q$

Take note that one of the most common logical errors is to assume that the converse or the inverse of a conditional statement is equivalent to this conditional statement.

Example 12 | Find the contrapositive, the converse and the inverse of the conditional statement "$\underbrace{\text{The home team wins}}_{q}$ whenever $\underbrace{\text{it is raining}}_{p}$."
Original statement: "If it is raining, then the home team wins."
Contrapositive: "If the home team does not win, then it is not raining."
Converse: "If the home team wins, then it is raining."
Inverse: "If it is not raining, the the home team does not win."

Definition 6. Let p and q be propositions. The **biconditional statement** $p \leftrightarrow q$ is the proposition "p if and only if q", also called bi-implications.
$(q \rightarrow p) \wedge (p \rightarrow q)$
The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and false otherwise.

Note that the statement $p \leftrightarrow q$ is true when both the conditional statements $p \rightarrow q$ and $q \rightarrow p$ are true and is false otherwise.
There are some common ways to express $p \leftrightarrow q$:
"p is necessary and sufficient for q"
"If p then q, and conversely"
"p iff q"
"p exactly when q"

Example 13 | Let p be the statement "You can take the flight", and let q be the statement "You buy a ticket."
The $p \leftrightarrow q$ is the statement "You can take the flight if and only if you buy a ticket."

Example 14 | Construct the truth table of the compound proposition $(p \vee \neg q) \rightarrow (p \wedge q)$

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

Truth Tables and Compound Propositions

TABLE 1 The Truth Table for the Negation of a Proposition.

p	$\neg p$
T	F
F	T

TABLE 2 The Truth Table for the Conjunction of Two Propositions.

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

TABLE 3 The Truth Table for the Disjunction of Two Propositions.

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

TABLE 4 The Truth Table for the Exclusive Or of Two Propositions.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

TABLE 5 The Truth Table for the Conditional Statement $p \rightarrow q$.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

TABLE 6 The Truth Table for the Biconditional $p \leftrightarrow q$.

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

Precedence of Logical Operators

TABLE 8 Precedence of Logical Operators.

Operator	*Precedence*
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

It is an accepted rule that the conditional and biconditional operators, $\rightarrow$ and $\leftrightarrow$, have lower precedence than the conjunction and disjunction operators, $\wedge$ and $\vee$.
$p \rightarrow q \vee r$ means $p \rightarrow (q \vee r)$ rather than $(p \rightarrow q) \vee r$

Logic and Bit Operations

Binary digit

TABLE 9 Table for the Bit Operators *OR*, *AND*, and *XOR*.

Boolean variable

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Definition 7. A **bit string** is a sequence of zero or more bits. The **length** of this string is the number of bits in the string.

We can extend bit operations to bit strings. We define the **bitwise OR**, **bitwise AND** and **bitwise XOR** of two strings of the same length.

EXAMPLE 16 Find the bitwise *OR*, bitwise *AND*, and bitwise *XOR* of the bit strings 01 1011 0110 and 11 0001 1101. (Here, and throughout this book, bit strings will be split into blocks of four bits to make them easier to read.)

Solution: The bitwise *OR*, bitwise *AND*, and bitwise *XOR* of these strings are obtained by taking the *OR*, *AND*, and *XOR* of the corresponding bits, respectively. This gives us

01 1011 0110
11 0001 1101

11 1011 1111 bitwise *OR*
01 0001 0100 bitwise *AND*
10 1010 1011 bitwise *XOR*

1.2 Applications of Propositional Logic

Statements in mathematics and the sciences and in natural language often are imprecise or ambiguous. To make such statements precise, they can be translated into the language of logic.

Example 3 | Express the specification "The automated reply cannot be sent when the file system is full" using logical connectives.

Let p: "The automated reply can be sent"
q: "The file system is full"

Consequently, our specification can be represented by the conditional statement $q \to \neg p$.

System Specifications

System specification should be consistent, that is, they should not contain conflicting requirements that could be used to derive a contradiction.
When specifications are not consistent, there would be no way to develop a system that satisfied all specifications.

Example 4 | Determine whether these system specifications are consistent:
(I.) "The diagnostic message is stored in the buffer or it is retransmitted."
(II.) "The diagnostic message is not stored in the buffer."
(III.) "If the diagnostic message is stored in the buffer, then it is retransmitted."

To determine whether these specification are consistent, we first express them using logical expressions.
Let p: "The diagnostic message is stored in the buffer."
q: "The diagnostic message is retransmitted."
The specifications can be written as (I.) $p \vee q$
(II.) $\neg p$
(III.) $p \to q$

An assignment of truth values that makes all three specifications true must have p false to make $\neg p$ true.
Because we want $p \vee q$ to be true but p must be false, q must be true.
Because $p \to q$ is true when p is false and q is true, we conclude that these specifications are consistent, because they are all true when p is false and q is true.

Example 5 | Do the system specification in Ex. 4 remain consistent if the specification "The diagnostic message is not retransmitted" is added?

This new specification is $\neg q$, which is false when q is true. Consequently, these four specifications are inconsistent.

Translating English Sentences

Example 1 | How can this English sentence be translated into a logical expression?
"You can access the Internet from campus only if you are a computer science major or you are not a freshman."
Let a: "You can access the Internet from campus."
c: "You are a CS major."
f: "You are a freshman."
The sentence can be represented as $a \to (c \vee \neg f)$

Example 2 | How can this English sentence be translated into logical expression?
"You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 y.o."
Let q: "You can ride the roller coaster"
r: "You are under 4 feet tall"
s: "You are older than 16 y.o."
Then, the sentence can be translated to $(r \wedge \neg s) \to \neg q$
$\neg(r \to s) \to \neg q$

Example 7 | As a reward for savings his daughter from the pirates, the King has given you the opportunity to win a treasure hidden inside one of three trunks. Two trunks that do not hold the treasure are empty. To win, you must select the correct trunk. Trunks 1 and 2 are each inscribed with message "This trunk is empty" and trunk 3 is inscribed with the message "The treasure is in trunk 2." The Queen, who never lies, tells you that only one of these inscription is true, while the other two are wrong. Which trunk should you select to win?

Let p_i be the proposition that the treasure is in Trunk i, for $i = 1, 2, 3$. To translate into propositional logic the Queen's statement that exactly one of the inscriptions is true, we observe that the inscription on Trunk 1, Trunk 2 and Trunk 3 are $\neg p_1$, $\neg p_2$ and p_2, respectively. So, her statement can be translated to $(\neg p_1 \wedge \neg(\neg p_2) \wedge \neg p_2) \vee (\neg(\neg p_1) \wedge \neg p_2 \wedge \neg p_2) \vee (\neg(\neg p_1) \wedge \neg(\neg p_2) \wedge p_2)$

Using the rules for propositional logic, we see that this equivalent to $(\neg p_1 \wedge p_2 \wedge \neg p_2) \vee (p_1 \wedge \neg p_2 \wedge \neg p_2) \vee (p_1 \wedge p_2 \wedge p_2)$, Double negation
$\equiv (\neg p_1 \wedge F) \vee (p_1 \wedge \neg p_2) \vee (p_1 \wedge p_2)$, Negation/Idempotance
$\equiv F \vee [p_1 \wedge (\neg p_2 \vee p_2)]$, Domination/Distributivite
$\equiv p_1 \wedge T$, Identite/Negation
$\equiv p_1$, Identite
So the treasure is in Trunk 1. ∎

$p \oplus q \equiv \neg(p \leftrightarrow q)$
$\equiv \neg[(p \to q) \wedge (q \to p)]$
$\equiv \neg[(\neg p \vee q) \wedge (\neg q \vee p)]$
$\equiv (p \wedge \neg q) \vee (q \wedge \neg p)$
$\Rightarrow$ $p_1 \oplus \neg p_2 \oplus p_2$
$\equiv p_1$ ∎

Example 8 | Smullyan posed many puzzles about an island that has two kinds of inhabitants, knights, who always tell the truth, and their opposites, knave, who always lie. You encounter two people A and B. What are A and B if A says "B is a knight" and B say "The two of us are opposite types"?

Let p and q be the statements that A is a knight and B is a knight, respectively, so that $\neg p$ and $\neg q$ are the statements that A is a knave and B is a knave, respectively.
We first consider the possibility that A is a knight; this is the statement that p is true. If A is a knight then he is telling the truth when he says that B is a knight, so that q is true, and A and B are the same type. However, if B is a knight, then B's statements that A and B are opposite types, the statement $(p \wedge \neg q) \vee (\neg q \wedge p)$, would have to be true, which is not, because A and B are both knights.
Consequently, we can conclude that A is not a knight, that is, that p is false.
If A is a knave, then because everything a knave say is false, A's statement that B is a knight, that is, that q is true, is a lie. This means that q is false and B is also a knave.
Furthermore, if B is a knave, then B's statement that A and B are opposite types is a lie, which is consistent with both A and B being knaves. We can conclude that both A and B are knaves. ∎

1.3 Propositional Equivalences

A important type of step used in mathematical arguments is the replacement of a statement with another statement with the same truth value.

Definition 1. A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a tautology.
A compound proposition that is always false is called a contradiction.
A compound proposition that is neither a tautologie nor a contradiction is called a contingency.

Definition 2. The compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology.
The notation $p \equiv q$ denotes that p and q are logically equivalent.
or $\Leftrightarrow$

Example 1 | We can construct examples of tautologies an contradictions using one propositional variable.

Because $p \vee \neg p$ is always true, it is a tautology (Negation)

TABLE 1 Examples of a Tautology and a Contradiction.

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

Because $p \wedge \neg p$ is always false, it is a contradiction.

Example 2 | Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

TABLE 3 Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$.

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

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

It follows that $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$ is a tautology and that these compound propositions are logically equivalent.

Example 3 | Show that $p \to q$ and $\neg p \vee q$ are logically equivalent
(This is know as the conditional-disjunction equivalence.)

TABLE 4 Truth Tables for $\neg p \vee q$ and $p \to q$.

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

Example 4 | Show that $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are logically equivalent.
(This is the distributive law of disjunction over conjunction).

TABLE 5 A Demonstration That $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ Are Logically Equivalent.

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

In general, 2^n rows are required if a compound proposition involves n propositional variables.
Because of the rapid growth of 2^n, more efficient ways are needed to establish logical equivalences, such as by using ones we already know.

TABLE 6 Logical Equivalences.

Equivalence	Name
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws (I.)
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws (II.)
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws (III.)
$\neg(\neg p) \equiv p$	Double negation law (IV.)
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws (V.)
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws (VI.)
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws (VII.)
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws (VIII.)
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws (IX.)
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws (X.)

TABLE 7 Logical Equivalences Involving Conditional Statements.

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

TABLE 8 Logical Equivalences Involving Biconditional Statements.

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q$
$\equiv p \oplus q$

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

The use of truth tables to establish equivalences becomes impractical as the number of variables grows. It is quicker to use other methods, such as employing logical equivalences that we already know.

(VII.) Furthermore, note that De Morgan's laws extend to $\underbrace{\neg\left(\bigvee_{j=1}^{n} p_j\right) \equiv \bigwedge_{j=1}^{n} \neg p_j}_{\text{Proof by induction}}$ and $\neg\left(\bigwedge_{j=1}^{n} p_j\right) \equiv \bigvee_{j=1}^{n} \neg p_j$

Example 6 | Show that $\neg(p \to q)$ and $p \wedge \neg q$ are equivalent.

$\neg(p \to q) \equiv \neg(\neg p \vee q)$, Conditional-disjunction equivalence
$\equiv \neg(\neg p) \wedge \neg q$, De Morgan
$\equiv p \wedge \neg q$, Double negation ∎

Example 7 | Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent by developing a series of logical equivalences.

$\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg(\neg p \wedge q)$, De Morgan
$\equiv \neg p \wedge (\neg(\neg p) \vee \neg q)$, De Morgan
$\equiv \neg p \wedge (p \vee \neg q)$, Double negation
$\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q)$, Distributivity
$\equiv F \vee (\neg p \wedge \neg q)$, Negation
$\equiv \neg p \wedge \neg q$, Identity ∎

Example 8 | Show that $(p \wedge q) \to (p \vee q)$ is a tautology.

$(p \wedge q) \to (p \vee q) \equiv \neg(p \vee q) \vee (p \vee q)$, Conditional-disjunctive equivalence
$\equiv (\neg p \wedge \neg q) \vee (p \vee q)$, De Morgan
$\equiv (\neg p \vee p) \vee (\neg q \vee q)$, Associativity/Commutativity
$\equiv T \vee T$, Negation
$\equiv T$, Domination ∎

1.3.5 Satisfiability

A compound proposition is **satisfiable** if there is an assignment of truth values to its variables that makes it true (that is, when it is a tautology or a contingency). When no such assignments exists, that is, when the compound proposition is false for all assignments of truth values to its variables, the compound proposition is **unsatisfiable**. Note that a compound proposition is unsatisfiable if and only if its negation is true for all assignments of truth values to the variables, that is, if and only if its negation is a tautology.

When we find a particular assignment of truth values that makes a compound proposition true, we have shown that it is satisfiable; such an assignment is called a **solution** of this particular satisfiability problem. However, to show that a compound proposition is unsatisfiable, we need to show that *every* assignment of truth values to its variables makes it false. Although we can always use a truth table to determine whether a compound proposition is satisfiable, it is often more efficient not to, as Example 9 demonstrates.

EXAMPLE 9 Determine whether each of the compound propositions $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$, $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$, and $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is satisfiable.

Solution: Instead of using a truth table to solve this problem, we will reason about truth values. Note that $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ is true when the three variables p, q, and r have the same truth value (see Exercise 42 of Section 1.1). Hence, it is satisfiable as there is at least one assignment of truth values for p, q, and r that makes it true. Similarly, note that $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is true when at least one of p, q, and r is true and at least one is false (see Exercise 43 of Section 1.1). Hence, $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is satisfiable, as there is at least one assignment of truth values for p, q, and r that makes it true.

Finally, note that for $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ to be true, $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ and $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ must both be true. For the first to be true, the three variables must have the same truth values, and for the second to be true, at least one of the three variables must be true and at least one must be false. However, these conditions are contradictory. From these observations we conclude that no assignment of truth values to p, q, and r makes $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ true. Hence, it is unsatisfiable. ◀

1.4 Predicates and Quantifiers

Propositional logic, studied in 1.1–1.3, cannot adequately express the meaning of all statements in mathematics and in natural language. In this section we will introduce a more powerful type of logic called **predicate logic**. We will see how predicate logic can be used to express the meaning of a wide range of statements in mathematics and in computer science in ways that permit us to reason and explore relationships between objects (Chap. 9)

Predicates

Subject, x

The statement "x is greater than 3" has two parts: $\underbrace{\text{is greater than 3}}_{\text{predicate, } P}$; propositional function, $P(x)$

Once a value has been assigned to the variable x, the statement $P(x)$ becomes a proposition and has a truth value.

We can also have statements that involve more than one variable. For instance, consider the statement "$x = y + 3$". We can denote this statements by $Q(x, y)$, where x and y are variables and Q is the predicate. When values are assigned to the variables x and y, the statement $Q(x,y)$ has a truth value. Similarly, we can let $R(x,y,z)$ denote the statement "$x+y=z$". When values are assigned to the variables x, y, and z, this statement has truth value.

Quantifiers

Quantification expresses the extent to which a predicate is true over a range of elements. In English, the words all, some, many, none, and few are used in quantifications. We will focus on two types of quantification here: universal quantification and existential quant. The area of logic that deals with predicates and quantifiers is called the **predicate calculus**.

(I.) The Universal Quantifier

Many mathematical statements assert that a property is true for all values of a variable in a particular domain, called the **domain of discourse** (or the universe of discourse)

The domain must always be specified when a universal quantifier is used; without it, the universal quantification of a statement is not defined.

Definition 1. The universal quantification of $P(x)$ is the statement "$P(x)$ for all values of x in the domain". The notation $\forall x P(x)$ denotes the universal quantification of $P(x)$.

$\forall$ is called the universal quantifier

$\forall x P(x) \equiv$ "for all x $P(x)$" $\equiv$ "for every x $P(x)$" $\equiv$ "all of" $\equiv$ "for each" $\equiv$ "given any" $\equiv$ "for arbitrary" $\equiv$ "for each" $\equiv$ "for any"

A element for which $P(x)$ is false is called a counterexample to $\forall x P(x)$

Note that single counterexample is all we need to establish that $\forall x P(x)$ is false.

Remark: Generally, an implicit assumption is made that all domains of discourse for quantifiers are nonempty. Note that if the domain is empty, then $\forall x P(x)$ is true for any propositional function $P(x)$ because there are no elements x in the domain for which $P(x)$ is false.

(II.) The Existential Quantifier

With existential quantification, we form a proposition that is true iff $P(x)$ is true for at least one value of x in the domain.

Definition 2. The existential quantification of $P(x)$ is the proposition "There exist an element x in the domain such that $P(x)$". We use the notation $\exists x P(x)$ for the existential quantification of $P(x)$.

$\exists$ is called the existential quantifier.

$\exists x P(x) \equiv$ "for some" $\equiv$ "for at least one" $\equiv$ "there is"

Remark: Generally, an implicit assumption is made that all domains of discourse for quantifiers are nonempty. If the domain is empty, then $\exists x Q(x)$ is false whenever $Q(x)$ is a propositional function because when the domain is empty, there can be no element x in the domain for which $Q(x)$ is true.

(III.) The Uniqueness Quantifier

The notation $\exists! x P(x)$ or $\exists_1 x P(x)$ states "There exists a unique x such that $P(x)$ is true"

$\exists! x P(x) \equiv$ "There is exactly" $\equiv$ "There is one and only one"

$\exists x \neg P(x) \vee [\exists x, y\, P(x) \wedge P(y)] \wedge (x \neq y)$

Observe that we can use quantifiers and propositional logic to express uniqueness, so the uniqueness quantifier can be avoided. Generally, it is best to stick with existential an universal quantifiers so that rules of inference for these quantifiers can be used.

Quantifiers with Restricted Domains

Note that the restriction of a universal quantification is the same as the universal quantification of a conditional statement. (implication)

For instance, $\forall x<0\,(x^2>0)$ is another way of expressing $\forall x(x<0 \rightarrow x^2>0)$

On the other hand, the restriction of an existential quantification is the same as the existential quantification of a conjunction. ($\wedge$)

For instance, $\exists z>0\,(z^2=2)$ is another way of expressing $\exists z(z>0 \wedge z^2=2)$.

Precedence of Quantifiers

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus $(\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \oplus)$. For example, $\forall x P(x) \vee Q(x)$ is the disjunction of $\forall x P(x)$ and $Q(x)$. In other words, it means $(\forall x P(x)) \vee Q(x)$ rather than $\forall x(P(x) \vee Q(x))$.

Logical Equivalences Involving Quantifiers

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

$\exists x(P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$

This logical equivalence shows that we can distribute a universal quantifier over a conjunction. Furthermore, we can also distribute an existential quantifier over a disjunction.

However, we cannot distribute a universal quantifier over a disjunction, $\forall x(P(x) \vee Q(x)) \not\equiv \forall x P(x) \vee \forall x Q(x)$ nor can we distribute an existence quantifier over a conjunction. $\exists x(P(x) \wedge Q(x)) \not\equiv \exists x P(x) \wedge \exists x Q(x)$

First, we show that if $\forall x(P(x) \wedge Q(x))$ is true then $\forall P(x) \wedge \forall x Q(x)$ is true.
Second, we show that if $\forall x P(x) \wedge \forall x Q(x)$ is true then $\forall x(P(x) \wedge Q(x))$ is true.

Instanciation univ. + Généralisation univ.: So, suppose that $\forall x(P(x) \wedge Q(x))$ is true. This means that if a is in the domain, then $P(a) \wedge Q(a)$ is true. Hence, $P(a)$ is true and $Q(a)$ is true. Because $P(a)$ is true and $Q(a)$ is true for every element a in the domain, we can conclude that $\forall x P(x)$ and $\forall x Q(x)$ are both true. This means that $\forall x P(x) \wedge \forall Q(x)$ is true

Idem.: Next, suppose that $\forall x P(x) \wedge \forall x Q(x)$ is true. It follows that $\forall x P(x)$ is true and $\forall x Q(x)$ is true. Hence, if a is in the domain, then $P(a)$ is true and $Q(a)$ is true. It follows that for all a, $P(a) \wedge Q(a)$ is true. It follows that $\forall x(P(x) \wedge Q(x))$ is true.

Negating Quantified Expressions

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

De Morgan's law for quantifiers.

Example 23 Express the statement "Every student in this class has studied calculus" using predicates and quantifiers.

First, we rewrite the statement so that we can clearly identify the appropriate quantifiers to use. Doing so, we obtain: "For every student in this class, that student has studied calculus."

Next we introduce a variable x so that our statement becomes: "For every student x in this class, x has studied calculus."

Continuing, we introduce $C(x)$, which is the statement "x has studied calculus." Consequently, if the domain for x consists of the students in the class, we can translate our statement as $\forall x C(x)$.

However, there are other correct approaches; we may be interested in a wider group of people than only those in this class. If we change the domain to consist of all people, we will need to express our statement as:

"For every person x, if person x is a student in this class, then x has studied calculus."

If $S(x)$: "x is in this class", we see that our statement can be expressed as $\forall x(S(x) \rightarrow C(x))$ — $Q(x, \text{calculus})$

Caution! Our statement cannot be expressed as $\forall x(S(x) \wedge C(x))$ because this statement say that all people are students in this class and have studied calculus. $\cdots$ $\forall x(S(x) \wedge C(x)) \equiv \forall x S(x) \wedge \forall x C(x)$

Example 24 Express the statements "Some student in this class has visited Mexico" (I.) and "Every student in this class has visited either Canada or Mexico" (II.) using predicates and quantifiers.

(I.) We can introduce a variable x, so that our statement becomes: "There is a student x in this class having the property that x has visited Mexico"

We introduce $M(x)$, which is the statement "x has visited Mexico"

If the domain for x consists of the students in this class, we can translate (I.) as $\exists x M(x)$.

However, if we are interested in people other than those in this class, we look at the statement a little differently.

Our statement can be expressed as: "There is a person x having the properties that x is a student in this class and x has visited Mexico."

In this case, the domain for the variable x consists of all people.

We introduce $S(x)$ to represent "x is a student in this class." Our solution becomes $\exists x(S(x) \wedge M(x))$ because the statement is that there is a person x who is a student in this class and who has visited Mexico.

Caution! Our statement cannot be expressed as $\exists x(S(x) \rightarrow M(x))$, which is true when there is someone not in the class because, in that case, for such a person x, $S(x) \rightarrow M(x)$ becomes either $F \rightarrow T$ or $F \rightarrow F$ both of which is true.

(II.) can be expressed as "For every x in this class, x has the property that x has visited Mexico or has visited Canada." (We are assuming the inclusive, rather than exclusive.)

We let $C(x)$ be "x has visited Canada." and (II.) can be expressed as $\forall x(C(x) \vee M(x))$.

However, if the domain for x consists of all people, our statement can be expressed as "For every person x, if x is a student in this class, then x has visited Mexico or has visited Canada."

In this case, the statement can be expressed as $\forall x(S(x) \rightarrow (C(x) \vee M(x)))$

We could use a two-place predicate $V(x,y)$: "x has visited country y." $\Rightarrow V(x, \text{Canada})$ and $V(x, \text{Mexico})$

Example 25 Use predicates and quantifiers to express the system specifications "Every mail message larger than one megabyte will be compressed" and "If a user is active, at least one network link will be available."

Let $S(m,y)$ be "Mail message m is larger than y megabytes", where the variable x has the domain of all mail messages and the variable y is a positive real number, and let $C(m)$ denote "Mail message m will be compressed."

Then the specification "Every mail message larger than one megabyte will be compressed" can be rep. as $\forall m(S(m,1) \rightarrow C(m))$

Let $A(u)$: "User u is active", where the variable u has the domain of all users,

Let $S(n,x)$: "Network link n is in state x", where n has the domain of all network links and x has the domain of all possible states for a network link.

Then the specification "If a user is active, at least one network link will be available" can be rep. by $\exists u A(u) \rightarrow \exists n S(n, \text{available})$

Examples from Lewis Carroll

Example 26 Consider these statements.

"All lions are fierce"
"Some lions do not drink coffee" } Premises
"Some fierce creatures do not drink coffee" } Conclusion

The entire set is called an argument.

Let $P(x)$: "x is a lion"
$Q(x)$: "x is fierce"
$R(x)$: "x drinks coffee"

Assuming that the domain consist of all creatures, express the statements in the argument using quantifiers and $P(x)$, $Q(x)$, and $R(x)$

We can express these statements as

$\forall x(P(x) \rightarrow Q(x))$
$\exists x(P(x) \wedge \neg R(x))$
$\exists x(Q(x) \wedge \neg R(x))$

Notice that the second statement cannot be written as $\exists x(P(x) \rightarrow \neg R(x))$. The reason is that $P(x) \rightarrow \neg R(x)$ is true whenever x is not a lion, so that $\exists x(P(x) \rightarrow \neg R(x))$ is true as long as there is at least one creature that is not a lion, even if every lion drinks coffee.

Similarly, the third statement cannot be written as $\exists x(Q(x) \rightarrow \neg R(x))$

Example 27 Consider these statements,

"All hummingbirds are richly colored"
"No large birds live on honey"
"Birds that do not live on honey are dull in color"
"Hummingbirds are small"

Let $P(x)$: "x is a hummingbird"
$Q(x)$: "x is large"
$R(x)$: "x lives on honey"
$S(x)$: "x is richly colored"

Assuming that the domain consist of all birds, express the statements in the argument using quantifiers, $P(x)$, $Q(x)$, $R(x)$ and $S(x)$.

We can express the statements in the argument as:

$\forall x(P(x) \rightarrow S(x))$
$\forall x(Q(x) \rightarrow \neg R(x)) \equiv \neg \exists x(Q(x) \wedge R(x))$
$\forall x(\neg R(x) \rightarrow \neg S(x))$
$\forall x(P(x) \rightarrow \neg Q(x))$

1.5 Nested Quantifiers

In Section 1.4 we avoided **nested quantifiers**, where one quantifier is within the scope of another, such as $\forall x \exists y(x+y=0)$

$\forall x Q(x)$, where $Q(x)$ is $\exists y P(x,y)$, where $P(x,y)$ is $x+y=0$

Example 1

Assume that the domain for the variable x and y consist of all real numbers.

The statement $\forall x \forall y(x+y=y+x)$ says that $x+y=y+x$ for all real numbers x and y. (This is the commutative law for addition of real numbers.)

Likewise, the statement $\forall x \exists y(x+y=0)$ says that for every real number x there is a real number y such that $x+y=0$. (This states that every real number has an additive inverse.)

Similarly, the statement $\forall x \forall y \forall z(x+(y+z)=(x+y)+z)$ is the associative law for addition of real numbers.

Example 2 Translate into English the statement $\forall x \forall y((x>0) \wedge (y<0) \rightarrow (xy<0))$ where the domain for both variables consists of all real numbers.

This statements says that for every real number x and for every number y, if x is positive and y is negative, Then xy is negative.

This can be stated more succintly as "The product of a positive real number and a negative real number is always a negative real number."

Thinking of Quantification as loops

In working with quantifications of more than one variable, it is sometimes helpful to think in terms of nested loops.

(I.) For example, to see whether $\forall x \forall y P(x,y)$ is true, we loop through the values for x, and for each x we loop through the values for y.

(II.) Similarly, to determine whether $\forall x \exists y P(x,y)$ is true, we loop through the values for x. For each x we loop through the values for y until we find a y for which $P(x,y)$ is true.

(III.) To see whether $\exists x \forall y P(x,y)$ is true, we loop through the values for x until we find an x for which $P(x,y)$ is always true when we loop through all values for y.

(IV.) Finally, to see whether $\exists x \exists y P(x,y)$ is true, we loop through the values for x, where for each x we loop through the values for y until we hit an x for which we hit a y for which $P(x,y)$ is true.

It is important to note that the order of quantifiers is important, unless all the quantifiers are universal quant. or all are existential quant.

Example 4 Let $Q(x,y)$ denote "$x+y=0$". What are the truth values of the quantifications $\exists y \forall x Q(x,y)$ and $\forall x \exists y Q(x,y)$, where the domain for all variables consists of all real numbers?

$\exists y \forall x Q(x,y)$ denotes "There is a real number y such that for every real number x, $Q(x,y)$."

No matter what value of y is chosen, there is only one value of x for which $x+y=0$. Because there is no real number y such that $x+y=0$ for all real numbers x, the statement $\exists y \forall x Q(x,y)$ is false.

$\forall x \exists y Q(x,y)$ denotes "For every real number x there is a real number y such that $Q(x,y)$."

Given a real number x, there is a real number y such that $x+y=0$; namely, $y=-x$. Hence, the statement $\forall x \exists y Q(x,y)$ is true.

Example 5 Let $Q(x,y,z)$ be the statement "$x+y=z$". What are the truth values of the statements $\underbrace{\forall x \forall y \exists z Q(x,y,z)}_{\text{true}}$ and $\underbrace{\exists z \forall x \forall y Q(x,y,z)}_{\text{false}}$ where $x, y, z \in \mathbb{R}$

TABLE 1 Quantifications of Two Variables.

Statement	When True?	When False?
$\forall x \forall y P(x,y)$ $\forall y \forall x P(x,y)$	$P(x, y)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x,y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x,y)$	There is an x for which $P(x, y)$ is true for every y.	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x,y)$ $\exists y \exists x P(x,y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y.

Example 6 | Translate the statement "The sum of two positive integers is always positive" into a logical expression.

We can rewrite it so that the implied quantifiers and a domain are shown: "For every two integers, if these integers are both positive, then the sum of these integers is positive."

Next, we introduce the variables x and y to obtain "For all positive integers x and y, $x+y$ is positive."

Consequently, we can express this as: $\forall x \forall y((x>0)\wedge(y>0) \to (x+y>0))$, where $x, y \in \mathbb{R}$.

Note that we could also translate this using the positive integers as the domain: $\forall x \in \mathbb{N}^* \forall y \in \mathbb{N}^* (x+y>0)$

Example 11 | Express the statement "If a person is female and is a parent, then this person is someone's mother" as a logical expression involving predicates, quantifiers with a domain consisting of all people, and logical connectives.

It can be expressed as "For every x, if person x is female and person x is a parent, then there exists a person y such that person x is the mother of person y."

We introduce the propositional functions $F(x)$: "x is female"
and $P(x)$: "x is a parent"
and $M(x,y)$: "x is the mother of y"

The original statement can be represented as $\forall x[(F(x)\wedge P(x)) \to \exists y M(x,y)]$

By null quantification rule (or $\forall x \exists y[(F(x)\wedge P(x)) \to M(x,y)]$

Example 7 | Translate: "Every real number except zero has a multiplicative inverse."

(A multiplicative inverse of a real number x is a real number y such that $xy=1$)

$\forall x((x\neq 0) \to \exists y(xy=1))$

Example 12 | Express the statement "Everyone has exactly one best friend" as a logical expression. With domain consisting of all people.

It can be expressed as "For every person x, person x has exactly one best friend."

To say that x has exactly one best friend means that there is a person y who is the best friend of x, and furthermore, that for every person z, if person z is not person y, then z is not the best friend of x.

When we introduce the predicate $B(x,y)$: "y is the best friend of x", the statement can be represented as $\forall x \exists y[B(x,y) \wedge \forall z((z\neq y) \to \neg B(x,z))]$

or $\forall x \exists! y B(x,y)$.

Example 9 | Translate $\forall x(C(x) \vee \exists y(C(y) \wedge F(x,y)))$, where $C(x)$: "x is a computer" and $F(x,y)$: "x and y are friends" and the domain for both x and y consists of all students in your school.

"For every student x in your school, x has a computer or there is a student y such that y has a computer and x and y are friends."

In other words, "Every student in your school has a computer or has a friend who has a computer."

Example 10 | Translate $\exists x \forall y \forall z((F(x,y)\wedge F(x,z) \wedge (y\neq z)) \to \neg F(y,z))$

"There is a student x such that for all students y and all students z other than y, if x and y are friends and x and z are friends, then y and z are not friends."

In other words, "There is a student none of whose friends are also friends with each other."

Example 13 | Use quantifiers to express the statement: "There is a woman who has taken a flight on every airline in the world"

Let $P(w,f)$: "w has taken f"
and $Q(f,a)$: "f is a flight on a"

We can express the statement as: $\exists w \forall a \exists f[P(w,f) \wedge Q(f,a)]$

Where the domains of discourse for w consist of all the women in the world
f consist of all airplane flight,
and a; all airlines

or simply $\exists w \forall a \exists f\, R(w,f,a)$, where $R(w,f,a)$: "w has taken f on a."

Negating Nested Quantifiers

Statements involving nested quant. can be negated by successively applying the rules for negating statements involving a single quantifier.

Example 14 | Express the negation of the statement $\forall x \exists y(xy=1)$ so that no negation precedes a quantifier.

$\neg \forall x \exists y(xy=1) \equiv \exists x \neg \exists y(xy=1) \equiv \exists x \forall y \neg(xy=1) \equiv \exists x \forall y(xy\neq 1)$

Example 15 | Use quantifiers to express the statement "There does not exist a women who has taken a flight on every airline in the world."

This statement is the negation of the statement "There is a women who has taken a flight on every airline in the world" from Ex 13, our statement can be expressed as $\neg\exists w \forall a \exists f[P(w,f)\wedge Q(f,a))$, where $P(w,f)$: "w has taken f" and $Q(f,a)$: "f is a flight on a"

We find: $\neg \exists w \forall a \exists f(P(w,f)\wedge Q(f,a)) \equiv \forall w \exists a \forall f[\neg P(w,f) \vee \neg Q(f,a)]$.

1.6 Rules of Inference

Proofs in mathematics are valid arguments that establish the truth of mathematical statements. By arguments, we mean a sequence of statements that end with a conclusion. By valid, we mean that the conclusion, or final statement of the argument, must follow from the truth of preceding statements, or premises, of the argument.

That is, 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 which are template for constructing valid arguments.

These rules of inference are among the most important ingredients in producing valid arguments.

(I.) Rules of inference for proposition

(II.) Rules of inference for quantifiers

These rules of inference for statements involving existential and universal quantifiers play an important role in proofs in computer science and mathematics

Can be combined.
These combinations of rules of inference are often used together in complicated arguments.

After we illustrate how rules of inference are used to produce valid arguments, we will describe some common forms of incorrect reasoning, called fallacies, which lead to invalid arguments.

Definition 1. An argument in propositional logic is a sequence of propositions. All but the final proposition in the argument are called premises and the final proposition is called the conclusion. An argument is valid if the truth of all its premises implies that the conclusion is 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.

Remark: An argument form is valid when $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ is a tautology.

(I.) Rules of Inference for Propositional Logic

When an argument form involves 10 different propositional variables, to use a truth table to show this argument form is valid requires $2^{10} = 1024$ different rows.
Fortunately, we do not have to always resort to truth tables. Instead, we can first establish the validity of some relatively simple argument forms, called rules of inference.
These rules of inference can be used as building blocs to construct more complicated valid argument forms.
We will now introduce the most important rules of inference in propositional logic.
The tautology $(p\wedge(p\to q))\to q$ is the basis of the rule of inference called modus ponens. (or the law of detachment)

or
p
$p \to q$) Premises must be true. If one of its premises is false, we cannot conclude that the conclusion is false.
$\therefore q$) Conclusion

$\therefore$ denotes "therefore"

All tautologies

TABLE 1 Rules of Inference.

Rule of Inference	Tautology	Name	
p, $p\to q$, $\therefore q$	$(p\wedge(p\to q))\to q$	Modus ponens	(I.)
$\neg q$, $p\to q$, $\therefore \neg p$	$(\neg q\wedge(p\to q))\to\neg p$	Modus tollens	(II.)
$p\to q$, $q\to r$, $\therefore p\to r$	$((p\to q)\wedge(q\to r))\to(p\to r)$	Hypothetical syllogism	(III.)
$p\vee q$, $\neg p$, $\therefore q$	$((p\vee q)\wedge\neg p)\to q$	Disjunctive syllogism	(IV.)
p, $\therefore p\vee q$	$p\to(p\vee q)$	Addition	(V.)
$p\wedge q$, $\therefore p$	$(p\wedge q)\to p$ or q	Simplification	(VI.)
p, q, $\therefore p\wedge q$	$((p)\wedge(q))\to(p\wedge q)$	Conjunction	(VII.)
$p\vee q$, $\neg p\vee r$, $\therefore q\vee r$	$((p\vee q)\wedge(\neg p\vee r))\to(q\vee r)$ $(\neg p\to q)\wedge(p\to r)\to(\neg q\to r)$	Resolution	(VIII.)

Computer programs have been developed to automate the task of reasoning and proving theorems.
Many of these programs make use of a rule of inference know as Resolution. Ex. Prolog

$\underbrace{[(p\vee q)\wedge(\neg p\vee r)]\to(q\vee r)}$ resolvent

When we let $q=r$, we obtain $(p\vee q)\wedge(\neg p\vee q)\to q$

Furthermore, when we let $r=F$, we obtain $(p\vee q)\wedge(\neg p)\to q$) Disjunctive syllogism

Because $\neg p\vee F\equiv\neg p$ Identity law.

Example 4 | State which rule of inference is the basis of the following argument:
"$\underbrace{\text{It is below freezing}}_{p}$ and $\underbrace{\text{raining now}}_{q}$. There, $\underbrace{\text{it is below freezing now}}_{p}$."

Let
This argument is of the form
$p\wedge q$
$\therefore p$) This argument uses the simplification rule

Example 5 | State the rule of inference is used in the argument:
"$\underbrace{\text{If it rains today}}_{p}$, then $\underbrace{\text{we will not have a barbecue today}}_{\neg p}$. $\overbrace{\text{If we do not have a barbecue today}}^{\neg q}$, then $\overbrace{\text{we will have a barbecue tomorrow}}^{r}$. Therefore, $\underbrace{\text{if it rains today}}_{p}$, then $\underbrace{\text{we will have a barbecue tomorrow}}_{r}$."

Let
The argument is of the form:
$p\to\neg p$
$\neg p\to r$
$\therefore p\to r$) Hypothetical syllogism.

Example 6 | Show that the premises "It is sunny this afternoon and it is colder than yesterday",
"We will go swimming only if it is sunny",
"If we do not go swimming, then we will take a canoe trip",
"If we take a canoe trip, then we will be home by sunset"
leads to the conclusion "We will be home by sunset."

Let p be the proposition "It is sunny this afternoon",
q the proposition "It is colder than yesterday",
r the proposition "We will go swimming",
s the proposition "We will take a canoe trip",
t the proposition "We will be home by sunset"

Then the premises become $\neg p\wedge q$,
$r\to p$,
$\neg r\to s$,
and $s\to t$,
The conclusion is simply t.

We construct an argument to show that our premises lead to the desired conclusion as follows.

Step	Reason
1. $\neg p\wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r\to p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r\to s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s\to t$	Premise
8. t ∎	Modus ponens (6) and (7)

Example 7 | Show that the premises "If you send me an e-mail message, then I will finish writing the program",
"If you do not send me an e-mail message, then I will go to sleep early",
and "If I go to sleep early, then I will wake up feeling refreshed"
lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed".

Let p: "You send me an e-mail message"
q: "I will finish writing the program"
r: "I will go to sleep early"
s: "I will wake up feeling refreshed"

Then the premises are $p\to q$,
$\neg p\to r$,
and $r\to s$.
The desired conclusion is $\neg q\to s$.

Step	Reason
1. $p\to q$	Premise
2. $\neg q\to\neg p$	Contrapositive of (1)
3. $\neg p\to r$	Premise
4. $\neg q\to r$	Hypothetical syllogism using (2) and (3)
5. $r\to s$	Premise
6. $\neg q\to s$ ∎	Hypothetical syllogism using (4) and (5)

1. $p\to q$
2. $\neg p\vee q$
3. $\neg p\to r$
4. $p\vee r$
5. $q\vee r$
6. $\neg q\to r$
7. $r\to s$
8. $\neg q\to s$ ∎

Example 9 | Show that premises $(p\wedge q)\vee r$ and $r\to s$ imply the conclusion $p\vee s$.

1. $(p\vee r)\wedge(q\vee r)\to(p\vee r)$ Simplification
2. $r\to s\equiv\neg r\vee s$
3. $(r\vee p)\wedge(\neg r\vee s)$ Conjunction
4. $p\vee s$ Resolution

Fallacies

Several common fallacies arise in incorrect arguments. These fallacies resemble rules of inference, but are based on contingencies rather than tautologies.

The proposition $\underbrace{[(p\to q)\wedge q]\to p}$ is not a tautology, because it is false when p is false and q is true.

This type of incorrect reasoning is called the fallacy of affirming the conclusion.

idem for $[(p\to q)\wedge\neg p]\to\neg q$ another type of fallacy called fallacy of denying the hypothesis.

(II.) Rules of Inference for Quantified Statements

We have discussed rules of inference for propositions. We will now describe some important rules of inference for statements involving quantifiers.
These rules of inference are used extensively in mathematical arguments, often without being explicitly mentioned.

(I.) Universal instantiation is the rule of inference used to conclude that $P(c)$ is true, where c is a particular member of the domain, given the premise $\forall x\, P(x)$.
Universal instantiation is used when we conclude from the statement "All women are wise" that Lisa is wise", where Lisa is a member of the domain of all women.

Trivial

(II.) Universal generalization is the rule of inference that states that $\forall x P(x)$ is true, given the premise that $P(c)$ is true for all elements c in the domain.
The element c that we select must be an arbitrary, and not a specific, element of the domain.
That is, when we assert from $\forall x P(x)$ the existence of an element c in the domain, we have no control over c and cannot make any other assumptions about c other than it comes from the domain.
Universal generalization is used implicitly in many proofs in mathematics and is seldom mentioned explicitly.
However, the error of adding unwarranted assumptions about the arbitrary element c when universal generalization is used is all too common in incorrect reasoning.

(I.) and (II.)
Arbitrary c

(III.) Existential instantiation is the rule that allows us to conclude that there is an element c in the domain for which $P(c)$ is true if we know that $\exists x P(x)$ is true.
We cannot select an arbitrary value of c here, but rather it must be a c for which $P(c)$ is true.
Usually we have no knowledge of what c is, only that it exists. Because it exists, we may give it a name (c) and continue our argument.

(IV.) Existential generalization is the rule of inference that is used to conclude that $\exists x P(x)$ is true when a particular element c with $P(c)$ true is known.
That is, if we know one element c in the domain for which $P(c)$ is true, then we know that $\exists x P(x)$ is true.

Trivial

(III.) and (IV.)
A particular c, where $P(c)$ is true

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	Name	
$\forall x P(x)$ $\therefore P(c)$	Universal instantiation	(I.)
$P(c)$ for an arbitrary c $\therefore \forall x P(x)$	Universal generalization	(II.)
$\exists x P(x)$ $\therefore P(c)$ for some element c	Existential instantiation	(III.)
$P(c)$ for some element c $\therefore \exists x P(x)$	Existential generalization	(IV.)

Combining Rules of Inference for Propositions and Quantified Statements

We have developed rules of inference both for propositions and for quantified statements.
Because universal instantiation and modus ponens are used so often together,
This combination of rules is sometimes called **universal modus ponens**, described as follows:

$$\begin{array}{l} \forall x\,[P(x)\to Q(x)] \\ \underline{P(a)} \\ \therefore Q(x) \end{array}$$

, where a is a particular element in the domain
$P(a)$ must be true

Another useful combination of a rule of inference from propositional logic and those for quantified statements is **universal modus tollens**, expressed in the following way:
Universal instantiation

$$\begin{array}{l} \forall x\,[P(x)\to Q(x)] \\ \underline{\neg Q(a)} \\ \therefore \neg P(a) \end{array}$$

, where a is a particular element in the domain
$P(a)$ must be true

Universal transitivity
$$\begin{array}{l} \forall x\,[P(x)\to Q(x)] \\ \underline{\forall x\,[Q(x)\to R(x)]} \\ \therefore \forall x\,[P(x)\to R(x)] \end{array}$$

Example 12 Show that the premises "Everyone in this discrete mathematics class has taken a course in computer science" and "Marla is a student in this class" imply the conclusion "Marla has taken a course in computer science."

Let $D(x)$ denote "x is in this dm class." and let $C(x)$ denote "x has taken a course in cs."
Then the premises are $\forall x[D(x)\to C(x)]$ and $D(\text{Marla})$. The conclusion is $C(\text{Marla})$.
The following steps can be used to establish the conclusion from premises.

Step	Reason
1. $\forall x[C(x)\to D(x)]$	Premise
2. $D(\text{Marla})\to C(\text{Marla})$	Universal instantiation from (1)
3. $D(\text{Marla})$	Premise
4. $C(\text{Marla})$	Modus ponens from (2) and (3)

∎

Example 13 Show that the premises "A student in this class has not read the book", and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."

Let $C(x)$ be "x is in this class"
$B(x)$ be "x has read the book"
and $P(x)$ be "x passed the first exam"

The premises are $\exists x[C(x)\wedge\neg B(x)]$
and $\forall x[C(x)\to P(x)]$
The conclusion is $\exists x[P(x)\wedge\neg B(x)]$

These steps can be used to establish the conclusion from the premises.

Step	Reason
1. $\exists x[C(x)\wedge\neg B(x)]$	Premise
2. $C(a)\wedge\neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x[C(x)\to P(x)]$	Premise
5. $C(a)\to P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a)\wedge\neg B(a)$	Conjunction from (6) and (7)
9. $\exists x[P(x)\wedge\neg B(a)]$	Existential generalization from (8)

∎

Example 14 Assume that "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n" is true.
Use universal modus ponens to show that $100^2 < 2^{100}$

Let $P(n)$ denote "$n>4$" and $Q(n)$ denote "$n^2<2^n$".
The statement "For all positive integer n, if n is greater than 4, then n^2 is less than 2^n" can be represented by $\forall n\in\mathbb{Z}^+[P(n)\to Q(n)]$
We are assuming that $\forall n[P(n)\to Q(n)]$ is true.
Note that $P(100)$ is true because $100>4$.
It follows by universal modus ponens that $Q(100)$ is true, namely, that $100^2<2^{100}$ ∎

1.7 Introduction to Proofs

In mathematical writing, the term **theorem** is usually reserved for a statement that is considered at least somewhat important.
Less important theorems sometimes are called **propositions**. We demonstrate that a theorem is true with a **proof**. A proof is a valid argument that establishes the truth of a theorem. statement
The statements used in a proof can include **axioms (or postulates)**, which are statement assumed to be true, the premises of the theorem, and previously proven theorem.
Another less important theorem that is helpful in the proof of other results is called a **lemma**. Complicated proof are usually easier to understand when they are proved using a series of lemmas, where each lemma is proven individually.
A **corollary** is a theorem that can be established directly from a theorem that has been proved. A **conjecture** is a statement that is being proposed to be a true statement.

Direct Proofs

A **direct proof** of a conditional statement $p\to q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.
They are straightforward. However, direct proof sometimes require particular insights and can be quite tricky.

Definition 1. The integer n is **even** if there exists an integer k such that $n=2k$, and **odd** if there exists an integer k such that $n=2k+1$

Example 1 Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

To begin a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely,
We assume that n is odd.
By the definition of an odd integer, it follows that $n=2k+1$, where k is some integer.

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= (2k+1)(2k+1) \\ &= 4k^2+4k+1 \\ &= 2(2k^2+2k)+1 \end{aligned}$$

By the definition of an odd integer, we can conclude that n^2 is an odd integer. (it is one more than twice an integer)
Consequently, we have proved that if n is an odd integer, then n^2 is an odd integer.

Example 2 Give a direct proof that if m and n are both perfect squares, then $n\cdot m$ is also a perfect square.
An integer a is a perfect square if there is an integer b such that $a=b^2$)

We assume that m and n are both perfect squares.
By the definition of a perfect square, it follows that there are integer s and t such that $m=s^2$ and $n=t^2$.
$n\cdot m = s^2t^2=(ss)(tt)=(st)(st)^2$, using commutativity and associativity of multiplication.
By the definition of perfect square, it follows that $m\cdot n$ is also a perfect square, because it is the square of st, which is an integer.
We have proved that if m and n are both perfect squares, then $m\cdot n$ is also a perfect square.

Proof by contraposition.

We will often see that attemps at direct proofs often reach dead ends.
An extremely useful type of indirect proof is known as **proof by contraposition** $p\to q \equiv \neg q\to\neg p$

Example 3 Prove that if n is an integer and $3n+2$ is odd, then n is odd.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $3n+2$ is odd, then n is odd" is false; namely, assume that n is even.
Then, by the definition of an even integer, $n=2k$ for some integer k.
Subtituting $2k$ for n, we find that

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

This tells us that $3n+2$ is even (because it is a multiple of 2), and therefore not odd.
This is negation of the premise of the theorem. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false,
the original conditional statement is true. Our proof by contraposition succeeded; we have proved the theorem "If $3n+2$ is odd, then n is odd". □

Example 4 Prove that if $n=ab$, where a and b are positive integers, then $a\le\sqrt{n}$ or $b\le\sqrt{n}$

Because there is no obvious way of showing that $a\le\sqrt{n}$ or $b\le\sqrt{n}$ directly from the equation $n=ab$, where a and b are positive integers,
we attempt a proof by contraposition.
The first step in a proof by contraposition is to assume that the conclusion is false.
That is, we assume that the statement $(a\le\sqrt{n})\vee(b\le\sqrt{n})$ is false. This implies that $a>\sqrt{n}$ and $b>\sqrt{n}$.
We can multiply these inequalities together (using the fact that if $0<s<t$ and $0<u<v$, then $su<tv$)
to obtain

$$\begin{aligned} ab &> \sqrt{n}\cdot\sqrt{n} \\ &> n \end{aligned}$$

This shows that $ab\ne n$, which contradicts the statement $n=ab$.
Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true.
Our proof by contraposition succeeded; we have proved that if $n=ab$, where a and b are positive integers, then $a\le\sqrt{n}$ or $b\le\sqrt{n}$. ∎

Vacuous and Trivial Proofs

Section 5.1

We can quickly prove that a conditional statement $p \to q$ is true when we know that p is false, because $p \to q$ must be true when p is false.
Consequently, if we can show that p is false, then we have proof, called a **vacuous proof**, of the conditional statement $p \to q$.
Vacuous proofs are often used to establish special cases of theorems that state that a conditional statement is true for all positive integers [i.e. a theorem of the kind $\forall n P(n)$, where $P(n)$ is a proposition function]

We can also quickly prove a conditional statement $p \to q$ if we know that the conclusion q is true. By showing that q is true, it follows that $p \to q$ must also be true.
A proof of $p \to q$ that uses the fact that q is true is called a **trivial proof**.

A Little Proof Strategy

We have described two important approaches for proving theorems of the form $\forall x [P(x) \to Q(x)]$: direct proof and proof by contraposition.
When you want to prove a statement of the form $\forall x[P(x) \to Q(x)]$, first evaluate whether a direct proof looks promising. Begin by expanding the definitions in the hypotheses.
Start to reason using these hypotheses, together with axioms and available theorems. If a direct proof does not seem to go anywhere, for instance when there is no clear way to use hypotheses, to reach the conclusion, try the same thing with a proof by contraposition. (Hypotheses such as x is irrational or $x \neq 0$ that are difficult to reason from are clue that an indirect proof might be your best best.)

Definition 2. The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = \frac{p}{q}$.
A real number that not rational is called **irrational**.

Proof by Contradiction

Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \to q$ is true. Because q is false, but $\neg p \to q$ is true, we can conclude that $\neg p$ is false, which means that p is true.

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

Because the statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show $\neg p \to (r \wedge \neg r)$ is true for some proposition r.
Proof of this type are called **proofs by contradiction**.

Proof by contradiction can be used to proved conditional statements.
In such proofs, we first assume the negation of the conclusion. We then use the premises of the theorem and the negation of the conclusion to arrive at a contradiction. $p \to q \equiv (\underbrace{p}_{p \text{ true}} \wedge \underbrace{\neg q}_{q \text{ false}}) \to F$

Proofs of Equivalence

To proof a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \to q$ and $q \to p$ are both true.
The validity of this approach is based on the tautology: $(p \leftrightarrow q) \equiv (p \to q) \wedge (q \to p)$

Example 13 | Prove the theorem "If n is an integer, then n is odd if and only if n^2 is odd."

To prove this theorem, we need to show that $p \to q$ and $q \to p$ are true.
We have already shown (in Ex. 1) that $p \to q$ is true and (in Ex. 8) that $q \to p$ is true.
Because we have shown that both $p \to q$ and $q \to p$ are true, we have shown that the theorem is true. ∎

Sometimes a theorem states that several proposition are equivalent. $P_1 \leftrightarrow P_2 \leftrightarrow P_3 \leftrightarrow \ldots \leftrightarrow P_n$, which states that all n propositions have the same truth values, and consequently, that for all i and j will $1 \leq i \leq n$ and $1 \leq j \leq n$, P_i and P_j are equivalent.
One way to prove these mutually equivalent is to use the tautology $P_1 \leftrightarrow P_1 \leftrightarrow \ldots \leftrightarrow P_n \equiv (P_1 \to P_2) \wedge (P_2 \to P_3) \wedge \ldots \wedge (P_n \to P_1)$ } there are $n^2 - n$ such statements.
We can establish any chain of conditional statements we choose as long as it is possible to work trough the chain, $P_1 \to P_3$, $P_3 \to P_2$, $P_2 \to P_1$.

Example 14 | Show that these statements about the integer n are equivalent:
P_1: n is even
P_2: $n-1$ is odd
P_3: n^2 is even.

We will show that these three statements are equivalent by showing that the conditional statements $\underbrace{P_1 \to P_2}_{(\mathrm{I.})}$, $\underbrace{P_2 \to P_3}_{(\mathrm{II.})}$ and $\underbrace{P_3 \to P_1}_{(\mathrm{III.})}$ are true.

(I.) We use a direct proof to show that $P_1 \to P_2$.
Suppose that n is even.
Then $n = 2k$ for some integer k.
Consequently, $n-1 = 2k-1 = 2k-1+1-1 = 2(k-1)+1$
This means that $n-1$ is odd because it is of the form $2m+1$, where m is the integer $k-1$.

(II.) We also use a direct proof to show that $P_2 \to P_3$.
Now suppose $n-1$ is odd.
Then $n-1 = 2k+1$ for some integer k.
Hence, $n = 2k+2$ so that $n^2 = (2k+2)^2 = 4k^2+8k+4 = 2(k^2+4k+2)$
This means that n^2 is twice the integer $2k^2+4k+2$, and hence is even.

(III.) To prove $P_3 \to P_1$, we use a proof by contraposition.
That is, we prove that if n is not even, then n^2 is not even.
This the same as proving that if n is odd, then n^2 is odd, which we have already done in Ex 1.

This complete the proof. ∎

Example 8 | Prove that the sum of two rational numbers is rational.
"For every real number r and every real number s, if r and s a rational numbers, then $r+s$ is rational."

Suppose that r and s are rational numbers.
From the definition of a rational number, it follows that there are integers p and q, with $q \neq 0$ such that $r = \frac{p}{q}$ and integer t and u, with $u \neq 0$, such that $s = \frac{t}{u}$.

We add up r and s, we find that: $r + s = \frac{p}{q} + \frac{t}{u} = \frac{up + tq}{uq}$, because $q \neq 0$ and $u \neq 0$, it follows that $uq \neq 0$
Consequently, we have expressed $r+s$ as the ratio of two integers, $v = up + tq$ and $w = uq$, where $w \neq 0$.
This means that $r+s$ is rational. ∎

Application of the pigeonhole principle.

Example 10 | Show that at least four of any 22 days must fall on the same day of the week.

Let p be the proposition "At least four of 22 chosen days fall on the same day of the week."
Suppose that $\neg p$ is true. This means that at most three of the 22 days fall on the same day of the week.
Because there are 7 days of the week, this implies at most 21 days could have been chosen, as for each of the week, at most three of the chosen days could fall on that day.
This contradicts the premise that we have 22 days under consideration.
That is, if r is the statement that 22 days are chosen, then we have shown that $\neg p \to (r \wedge \neg r)$.
Consequently, we know that p is true. ∎

Example 12 | Give a proof by contradiction of theorem "If $3n+2$ is odd, then n is odd."

Let p be "$3n+2$ is odd" and q be "n is odd".
To construct a proof by contradiction, assume that both p and $\neg q$ are true.
That is assume that $3n+2$ is odd and that n is even.
Because n is even, there is an integer k such that $n = 2k$.
This implies that
$$\begin{aligned} 3n+2 &= 3(2k)+2 \\ &= 2(3k)+2 \\ &= 2(3k+1) \\ &= 2t \quad , t = 3k+1 \text{ integer} \end{aligned}$$

We can also prove by showing that q must be also be true.
This observation tells us that we can turn a direct proof into a proof by contradiction.

Note that the statement "$3n+2$ is even" is equivalent to the statement $\neg p$.
Because both p and $\neg p$ are true, we have a contradiction.
This completes the proof by contradiction, proving that if $3n+2$ is odd, then n is odd. ∎

Counterexamples

To show that a statement of the form $\forall x P(x)$ is false, we only need to find a **counterexample**.

Example 15 | Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

To show that this statement is false, we look for a counterexample, which is a particular integer that is not the sum of the squares of two integers.

For example, 3 cannot be written as the sum of the squares of two integers.
To show this is the case, note that the only perfect sq. not exceeding 3 are $0^2 = 0$ and $1^2 = 1$.
Furthermore, there is no way to get 3 as the sum of two terms each of which is 0 or 1.
Consequently, we have shown that the statement is false. ∎

Example 5 | Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

Note that $P(0)$ is "If $0 > 1$, then $0^2 > 0$." We can show $P(0)$ using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false. This tells us that $P(0)$ is automatically true.
Remark: The fact that the conclusion of this conditional statement, $0^2 > 0$ is false is irrelevant to the truth value of the conditional statement, because a conditional statement with a false hypothesis is guaranteed to be true.

Example 6 | Prove that if n is an integer with $10 \leq n \leq 15$ which is a perfect square, then n is also also a perfect cube.

Note that there are no perfect squares n with $10 \leq n \leq 15$, because $3^2 = 9$ and $4^2 = 16$.
Hence, the statement that n is an integer with $10 \leq n \leq 15$ which is a perfect square is false for all integers n. Consequently, the statement to be proved is true for all integers n.

Example 7 | Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$", where the domain consists of all nonnegative integers. Show that $P(0)$ is true.

The proposition $P(0)$ is "If $a \geq b$, the $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the cond. statement "If $a \geq b$, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is $P(0)$, is true.
This an example of a trivial proof. Note that the hypothesis, which is the statement "$a \geq b$", was not needed in this proof.

Example 9 | Prove that if n is an integer and n^2 is odd, the n is odd.

Suppose that the conclusion of the statement is false, that is n is even.
This implies that exists an integer k such that $n = 2k$.
We find that, $n^2 = (2k)^2 = 2k \cdot 2k = 2(2k^2)$
Which implies that n^2 is also even because $n^2 = 2t$, where $t = 2k^2$
By contraposition, we have proved that if n is an integer and n^2 is odd, then n is odd. ∎

Example 11 | Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Let p be the proposition "$\sqrt{2}$ is irrational"
To start the proof by contradiction, we suppose that $\neg p$ is true.
Note that $\neg p$ is the statement "$\sqrt{2}$ is rational." We will show that assuming that $\neg p$ is true leads to a contradiction.
If $\sqrt{2}$ is rational, there exist integers a and b with $\sqrt{2} = \frac{a}{b}$, where $b \neq 0$ and a and b have no common factors.
fraction a/b is in lowest terms
Because $\sqrt{2} = \frac{a}{b}$, it follows that
$$\begin{aligned} \sqrt{2} = \frac{a}{b} &\Leftrightarrow 2 = \frac{a^2}{b^2} \\ &\Leftrightarrow 2b^2 = a^2 \\ &\Leftrightarrow 2b^2 = 4c^2 \quad , \text{By the definition of an even integer it follows that } a^2 \text{ is even.} \\ &\Leftrightarrow b^2 = 2c^2 \quad , \text{idem for } b \text{, it must be even.} \end{aligned}$$

We have shown that the assumption of $\neg p$ leads to the equation $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors.
But both a and b are even, that is, 2 divides both a and b.
Because our assumption of $\neg p$ leads to the contradiction that 2 divides both a and b and 2 does not divide both a and b, $\neg p$ must be false.
That is, the statement p, "$\sqrt{2}$ is irrational", is true. We have proved that $\sqrt{2}$ is irrational. ∎

Mistakes in Proofs

Each step of a mathematical proof need to be correct and the conclusion needs to follow logically from the steps that precede it. Many mistakes result from the introduction of steps that do not logically follow from those that precede it. Even professional mathematicians make such errors, especially when working with complicated formulae.

EXAMPLE 16 What is wrong with this famous supposed "proof" that 1 = 2?

"Proof": We use these steps, where a and b are two equal positive integers.

Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

The error is that $a - b = 0$

EXAMPLE 17 What is wrong with this "proof"?

"Theorem": If n^2 is positive, then n is positive. $\forall n [P(n) \to Q(n)]$

"Proof": Suppose that $\underbrace{n^2 \text{ is positive}}_{Q(n)}$. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n is positive.

$(Q(n) \wedge \forall n [P(n) \to Q(n)]) \to P(n)$
Not a valid rule of inference.
This is an example of the fallacy of affirming the conclusion.

A counterexample is supplied by $n = -1$ for which $n^2 = 1$ is positive, but n is negative.

EXAMPLE 18 What is wrong with this "proof"?

"Theorem": If n is not positive, then n^2 is not positive. (This is the contrapositive of the "theorem" in Example 17.) $\forall n [P(n) \to Q(n)]$

"Proof": Suppose that $\underbrace{n \text{ is not positive}}_{\neg P(n)}$. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n^2 is not positive.

$(\neg P(n) \wedge \forall n [P(n) \to Q(n)]) \to \neg Q(n)$
This is an example of the fallacy of denying the hypothesis.
A counterexample is supplied by $n = 1$, as in Ex 17.

Another incorrect arguments are based on a fallacy called **begging the question**. This fallacy arises when a statement is proved using itself, or a equivalent to it.
This is why this fallacy is also called **circular reasoning**.

EXAMPLE 19 Is the following argument correct? It supposedly shows that n is an even integer whenever n^2 is an even integer.

Suppose that n^2 is even. Then $n^2 = 2k$ for some integer k. $\underbrace{\text{Let } n = 2l \text{ for some integer } l}_{\text{Circular reasoning}}$. This shows that n is even.

1.8 Proof Methods and Strategy

We will introduce several other commonly used proof methods, including (I.) Exhaustive proof and proof by cases,
(II.) Existence proofs
(III.) Uniqueness proofs
(IV.) Foward and backward reasoning. (Strategy)

When mathematicians work, they formulate conjectures and attempt to prove or disprove them.

(I.) Exhaustive Proof and Proof by Cases.

To prove a conditional statement of the form $(P_1 \vee P_2 \vee \dots \vee P_n) \to q$, the tautology $[(P_1 \vee P_2 \vee \dots \vee P_n) \to q] \equiv [(P_1 \to q) \wedge (P_2 \to q) \wedge \dots \wedge (P_n \to q)]$ can be used as a rule of inference.

(i.) Exhaustive proof.

Some Th. can be proved by examining small number of examples. An exhaustive proof is a special type of proof by cases where each case involves checking a single example.

Example 1 | Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

We use a proof by exhaustion.
We only need to verify the inequality $(n+1)^3 \geq 3^n$ when $n = 1, 2, 3$ and 4.
For $n=1$, we have $(n+1)^3 = 2^3 = 8$ and $3^n = 3^1 = 3$;
For $n=2$, we have $(n+1)^3 = 3^3 = 27$ and $3^n = 3^2 = 9$;
For $n=3$, we have $(n+1)^3 = 4^3 = (2^2)^3 = 2^6 = 64$ and $3^n = 3^3 = 27$;
And for $n=4$, we have $(n+1)^3 = 5^3 = 125$ and $3^n = 3^4 = 81$;
In each of these four cases, we see that $(n+1)^3 \geq 3^n$.
We have used the method of exhaustion to prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$ ∎

Example 2 | Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9.
(An integer n is a perfect power if it equals m^a, where m is an integer and a is an int. greater than 1.)

We use a proof by exhaustion.
The sq. not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, 100
The cube not exceeding 100 are 1, 8, 27 and 64
⋮
There are no other positive integer higher than 6^{th} power not exceeding 100 other than 1.
Looking at this list, we see that $n=8$ is the only perfect power n for which $n+1$ is also a perfect power.
That is, $2^3 = 8$ and $3^2 = 9$ … ∎

(ii.) Proof by Cases

EXAMPLE 3 Prove that if n is an integer, then $n^2 \geq n$.

Extra Examples

Solution: We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

Case (i): When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.

Case (ii): When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer n, we obtain $n \cdot n \geq n \cdot 1$. This implies that $n^2 \geq n$ for $n \geq 1$.

Case (iii): In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$. ◀

EXAMPLE 4 Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers. (Recall that $|a|$, the absolute value of a, equals a when $a \geq 0$ and equals $-a$ when $a \leq 0$.)

Solution: In our proof of this theorem, we remove absolute values using the fact that $|a| = a$ when $a \geq 0$ and $|a| = -a$ when $a \leq 0$. Because both $|x|$ and $|y|$ occur in our formula, we will need four cases: *(i)* x and y both nonnegative, *(ii)* x nonnegative and y negative, *(iii)* x negative and y nonnegative, and *(iv)* x negative and y negative. We denote by p_1, p_2, p_3, and p_4, the proposition stating the assumption for each of these four cases, respectively.

(Note that we can remove the absolute value signs by making the appropriate choice of signs within each case.)

Case (i): We see that $p_1 \to q$ because $xy \geq 0$ when $x \geq 0$ and $y \geq 0$, so that $|xy| = xy = |x||y|$.

Case (ii): To see that $p_2 \to q$, note that if $x \geq 0$ and $y < 0$, then $xy \leq 0$, so that $|xy| = -xy = x(-y) = |x||y|$. (Here, because $y < 0$, we have $|y| = -y$.)

Case (iii): To see that $p_3 \to q$, we follow the same reasoning as the previous case with the roles of x and y reversed.

Case (iv): To see that $p_4 \to q$, note that when $x < 0$ and $y < 0$, it follows that $xy > 0$. Hence, $|xy| = xy = (-x)(-y) = |x||y|$.

Because $|xy| = |x||y|$ holds in each of the four cases and these cases exhaust all possibilities, we can conclude that $|xy| = |x||y|$, whenever x and y are real numbers. ◀

(ii.) and (iii.) Without loss of generality.
WLOG
can lead to unfortunate errors or incomplete and possibly unsalvageable proof.

EXAMPLE 5 Formulate a conjecture about the final decimal digit of the square of an integer and prove your result.

Solution: The smallest perfect squares are 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, and so on. We notice that the digits that occur as the final digit of a square are 0, 1, 4, 5, 6, and 9, with 2, 3, 7, and 8 never appearing as the final digit of a square. We conjecture this theorem: The final decimal digit of a perfect square is 0, 1, 4, 5, 6, or 9. How can we prove this theorem?

We first note that we can express an integer n as $10a + b$, where a and b are positive integers and b is 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9. Here a is the integer obtained by subtracting the final decimal digit of n from n and dividing by 10. Next, note that $(10a + b)^2 = 100a^2 + 20ab + b^2 = 10(10a^2 + 2b) + b^2$, so that the final decimal digit of n^2 is the same as the final decimal digit of b^2. Furthermore, note that the final decimal digit of b^2 is the same as the final decimal digit of $(10 - b)^2 = 100 - 20b + b^2$. Consequently, we can reduce our proof to the consideration of six cases.

Case (i): The final digit of n is 1 or 9. Then the final decimal digit of n^2 is the final decimal digit of $1^2 = 1$ or $9^2 = 81$, namely, 1.

Case (ii): The final digit of n is 2 or 8. Then the final decimal digit of n^2 is the final decimal digit of $2^2 = 4$ or $8^2 = 64$, namely, 4.

Case (iii): The final digit of n is 3 or 7. Then the final decimal digit of n^2 is the final decimal digit of $3^2 = 9$ or $7^2 = 49$, namely, 9.

Case (iv): The final digit of n is 4 or 6. Then the final decimal digit of n^2 is the final decimal digit of $4^2 = 16$ or $6^2 = 36$, namely, 6.

Case (v): The final decimal digit of n is 5. Then the final decimal digit of n^2 is the final decimal digit of $5^2 = 25$, namely, 5.

Case (vi): The final decimal digit of n is 0. Then the final decimal digit of n^2 is the final decimal digit of $0^2 = 0$, namely, 0.

Because we have considered all six cases, we can conclude that the final decimal digit of n^2, where n is an integer is either 0, 1, 2, 4, 5, 6, or 9. ◀

Sometimes we can eliminate all but a few examples in a proof by cases, as Example 6 illustrates.

EXAMPLE 6 Show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$.

Solution: We can quickly reduce a proof to checking just a few simple cases because $x^2 > 8$ when $|x| \geq 3$ and $3y^2 > 8$ when $|y| \geq 2$. This leaves the cases when x equals $-2, -1, 0, 1$, or 2 and y equals $-1, 0$, or 1. We can finish using an exhaustive proof. To dispense with the remaining cases, we note that possible values for x^2 are 0, 1, and 4, and possible values for $3y^2$ are 0 and 3, and the largest sum of possible values for x^2 and $3y^2$ is 7. Consequently, it is impossible for $x^2 + 3y^2 = 8$ to hold when x and y are integers. ◀

EXAMPLE 7 Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.

Solution: We will use proof by contraposition, the notion of without loss of generality, and proof by cases. First, suppose that x and y are not both even. That is, assume that x is odd or that y is odd (or both). Without loss of generality, we assume that x is odd, so that $x = 2m + 1$ for some integer k.

To complete the proof, we need to show that xy is odd or $x + y$ is odd. Consider two cases: *(i)* y is even, and *(ii)* y is odd. In *(i)*, $y = 2n$ for some integer n, so that $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd. In *(ii)*, $y = 2n + 1$ for some integer n, so that $xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$ is odd. This completes the proof by contraposition. (Note that our use of without loss of generality within the proof is justified because the proof when y is odd can be obtained by simply interchanging the roles of x and y in the proof we have given.) ◀

Common errors with exhaustive proof and proof by cases.

A common error of reasoning is to draw incorrect conclusions from examples.
No matter how many seperate examples are considered, a theorem is not proved by considering examples unless every possible case is covered.
Another common error involves making unwarranted assumptions that lead to incorrect proofs by cases where not all cases are considered.

EXAMPLE 9 What is wrong with this "proof"?

"Theorem": If x is a real number, then x^2 is a positive real number.

"Proof": Let p_1 be "x is positive," let p_2 be "x is negative," and let q be "x^2 is positive." To show that $p_1 \to q$ is true, note that when x is positive, x^2 is positive because it is the product of two positive numbers, x and x. To show that $p_2 \to q$, note that when x is negative, x^2 is positive because it is the product of two negative numbers, x and x. This completes the proof.

Case of $x=0$ missing
$P \leftrightarrow P_1 \vee P_2 \vee P_3$

(II.) Existence Proofs

A proof of a proposition of the form $\exists x\, P(x)$ is called an existence proof.
There are several ways to prove a theorem of this type: (I.) Constructive: By finding an element a, called a witness, such that $P(a)$ is true.
(II.) Nonconstructive: By not finding an element a such that $P(a)$ is true
One common method of giving a nonconstructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction.

EXAMPLE 10 A Constructive Existence Proof Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Extra Examples

Solution: After considerable computation (such as a computer search) we find that

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied "No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways." ◀

EXAMPLE 11 A Nonconstructive Existence Proof Show that there exist irrational numbers x and y such that x^y is rational.

Solution: By Example 11 in Section 1.7 we know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational, namely, $x = \sqrt{2}$ and $y = \sqrt{2}$. On the other hand if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2$.

This proof is an example of a nonconstructive existence proof because we have not found irrational numbers x and y such that x^y is rational. Rather, we have shown that either the pair $x = \sqrt{2}$, $y = \sqrt{2}$ or the pair $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ have the desired property, but we do not know which of these two pairs works! ◀

Remark: Exercise 11 in Section 4.3 provides a constructive existence proof that there are irrational numbers x and y such that x^y is rational.

(III.) Uniqueness Proofs

The two parts of a uniqueness proof are:
(I.) Existence: We show that an element x with the desired property exists.
(II.) Uniqueness: We show that if x and y both have the desired proof, then $x = y$.

Remark: $\exists x \,[P(x) \wedge \forall y [(y \neq x) \to \neg P(y)]]$
OR
$\equiv \exists x \,[P(x) \wedge \forall y [P(y) \to (y = a)]]$

EXAMPLE 13 Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution: First, note that the real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$. Consequently, a real number r exists for which $ar + b = 0$. This is the existence part of the proof.

Second, suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides, we find that $ar = as$. Dividing both sides of this last equation by a, which is nonzero, we see that $r = s$. This establishes the uniqueness part of the proof. ◀

Extra Examples

(I.) Existence
$r = \frac{-b}{a} \Rightarrow \cancel{a}(\frac{-b}{\cancel{a}}) + b = -b + b = 0$
$a \neq 0$

(II.) Uniqueness
$ar + b = as + b \Leftrightarrow ar = as$
$\Leftrightarrow r = s, \; a \neq 0$

(IV.) Foward and Backward Reasoning

Forward reasoning is unfortunately often difficult to use to prove more complicated results, because the reasoning needed to reach the conclusion may be far from obvious. In such cases it may be helpful to use backward reasoning

EXAMPLE 14 Given two positive real numbers x and y, their **arithmetic mean** is $(x + y)/2$ and their **geometric mean** is $\sqrt{xy}$. When we compare the arithmetic and geometric means of pairs of distinct positive real numbers, we find that the arithmetic mean is always greater than the geometric mean. [For example, when $x = 4$ and $y = 6$, we have $5 = (4 + 6)/2 > \sqrt{4 \cdot 6} = \sqrt{24}$.] Can we prove that this inequality is always true?

Extra Examples

Solution: To prove that $(x + y)/2 > \sqrt{xy}$ when x and y are distinct positive real numbers, we can work backward. We construct a sequence of equivalent inequalities. The equivalent inequalities are

$$(x + y)/2 > \sqrt{xy},$$
$$(x + y)^2/4 > xy,$$
$$(x + y)^2 > 4xy,$$
$$x^2 + 2xy + y^2 > 4xy,$$
$$x^2 - 2xy + y^2 > 0,$$
$$(x - y)^2 > 0.$$

Because $(x - y)^2 > 0$ when $x \neq y$, it follows that the final inequality is true. Because all these inequalities are equivalent, it follows that $(x + y)/2 > \sqrt{xy}$ when $x \neq y$. Once we have carried out this backward reasoning, we can build a proof based on reversing the steps. This produces construct a proof using forward reasoning. (Note that the steps of our backward reasoning will not be part of the final proof. These steps serve as our guide for putting this proof together.)

Prove arith. mean > geo. mean
that is, $\frac{x+y}{2} > \sqrt{(x \cdot y)}$
When $(x, y) \in \mathbb{R}^+ \times \mathbb{R}^+$ and $(x \neq y)$

EXAMPLE 15 Suppose that two people play a game taking turns removing one, two, or three stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

Solution: To prove that the first player can always win the game, we work backward. At the last step, the first player can win if this player is left with a pile containing one, two, or three stones. The second player will be forced to leave one, two, or three stones if this player has to remove stones from a pile containing four stones. Consequently, one way for the first person to win is to leave four stones for the second player on the next-to-last move. The first person can leave four stones when there are five, six, or seven stones left at the beginning of this player's move, which happens when the second player has to remove stones from a pile with eight stones. Consequently, to force the second player to leave five, six, or seven stones, the first player should leave eight stones for the second player at the second-to-last move for the first player. This means that there are nine, ten, or eleven stones when the first player makes this move. Similarly, the first player should leave twelve stones when this player makes the first move. We can reverse this argument to show that the first player can always make moves so that this player wins the game no matter what the second player does. These moves successively leave twelve, eight, and four stones for the second player. ◀

Other Proof methods :- Mathematical induction for proving $\forall n \in \mathbb{N}, P(n)$
- Structural induction for proving results about recursively defined sets
- Cantor diagonalization for results about the size of infinite sets
- Combinatorial proofs for counting arguments.