Course Outline – Discrete structure -CS 1005

- Logic and Proofs
- Sets and Functions
- Sequences and Series
- Relations
- Number Theory
- Proof techniques
- Induction and Recursion
- Counting and Recurrence Relations
- Graphs
- Trees

TEXT Book:

- Discrete Mathematics & its Applications, 8th edition. By Kenneth H. Rosen.

References Book:

- Invitation to Discrete Maths, 2nd edition. By Matousek and Nesetril.
- Discrete Mathematics. By Lovasz, Pelikan and Vesztergombi.

The Foundations: Logic and Proofs

Chapter 1, Part I: Propositional Logic

Discrete Mathematics

Discrete mathematics is the part of mathematics devoted to the study of discrete objects (Kenneth H. Rosen, 8th edition).

- How to think (and argument) mathematically.
- Learn mathematical facts and their applications.
- **Discrete mathematics** is the mathematical study of properties, and relationships among discrete objects.
- **Discrete mathematics** is the study of mathematical **structures** that are fundamentally discrete rather than continuous.

Discrete Vs Continuous

- Continuous Data: A set of data is said to be continuous if the values belonging to the set can take on any value within a finite or infinite interval.
- Continuous data is information that can be measured on a continuum or scale. , e.g., [0, 70].
- Continuous data can have almost any numeric value and can be meaningfully subdivided into finer and finer increments, depending upon the precision of the measurement system.

- Discrete Data: A set of data is said to be discrete if the values belonging to the set are distinct and separate. It is counted e.g., {1,2,3,4,5,6}

Discrete vs Continuous

- Examples of discrete Data
  - Number of boys in the class.
  - Number of candies in a packet.
  - Number of suitcases lost by an airline.
- Examples of continuous Data
  - Height of a person.
  - Time in a race.
  - Distance traveled by a car.

Why DM?

- Digital computers are based on discrete “atoms” (bits).
- Therefore, both a computer’s
  - structure (circuits) and
  - operations (execution of algorithms)

  can be described by discrete mathematics.

Applications

- How many ways are there to choose a valid password on a computer system?
- What is the probability of winning a lottery?
- Is there a link between two computers in a network?
- How can I identify spam e-mail messages?
- How can I encrypt a message so that no unintended recipient can read it?
- What is the shortest path between two cities using a transportation system?
- How can a list of integers be sorted so that the integers are in increasing order?
- How many steps are required to do such a sorting?
- How can it be proved that a sorting algorithm correctly sorts a list?
- How can a circuit that adds two integers be designed?
- How many valid Internet addresses are there?

Course Description:

- This class teaches students
  - how to think logically and mathematically.
  - It stresses mathematical reasoning and different ways to solve problems.

  It enhance your ability to formulate and solve applied problems, to analyze and interpret algorithms and functions and to use them effectively.

- Five important themes are interwoven in this class:
  - mathematical reasoning,
  - combinatorial analysis,
  - discrete structures,
  - algorithmic thinking,
  - applications and modeling

Applications: Logic

Hardware and software specifications

One-bit Full Adder with

Carry-In and Carry-Out

4-bit full adder

Formal: Input_wire_A value in {0, 1}

Example 1: Adder

Example 2: System Specification:

–The router can send packets to the edge system only if it supports the new address space.

–For the router to support the new address space it's necessary that the latest software release be installed.

–The router can send packets to the edge system if the latest software release is installed.

–The router does not support the new address space.

How to write these specifications in a rigorous /formal way? Use Logic

Applications: Number Theory
RSA and Public-key Cryptography

Alice and Bob have never met but they would like to exchange a message. Eve would like to eavesdrop.

E.g. between you and the Bank of America.

They could come up with a good encryption algorithm and exchange the encryption key – but how to do it without Eve getting it? (If Eve gets it, all security is lost.)

CS folks found the solution: public key encryption. Quite remarkable that is feasible.

Applications: Coloring a Map

How to color this map so that no two adjacent regions have the same color?

Applications: Graph representation

Coloring the nodes of the graph:
What's the minimum number of colors such that any two nodes connected by an edge have different colors?

Logic

- Logic is fundamental because it allows us to understand meaning of statements, deduce information about mathematical structures and uncover further structures.

- The rules of logic specify the meaning of mathematical statements.

- These rules are used to distinguish between valid and invalid arguments.

- Logic is a system based on propositions.

- A proposition is a (declarative) statement that is either true or false (not both).

- We say that the truth value of a proposition is either true (T) or false (F).

  Corresponds to 1 and 0 in digital circuits

Propositional Logic

Introduction

- A proposition is a declarative sentence (a sentence that declares a fact) that is either true or false, but not both.
- Are the following sentences propositions?
  - Islamabad is the capital of Pakistan. (Yes)
  - Read this carefully. (No)
  - $1+2=3$ (Yes)
  - $x+1=2$ (No)
  - What time is it? (No)

"Elephants are bigger than mice."

Is this a statement? Yes

Is this a proposition? Yes

What is the truth value of the proposition? True

"520 < 111"

Is this a statement? Yes

Is this a proposition? Yes

What is the truth value of the proposition? False

"If I have 100 camels, then I will be rich."

Is this a statement? Yes

Is this a proposition? Yes

What is the truth value of the proposition? Probably True

Proposition

Definition

proposition (or statement):
a declarative sentence that is either true or false

- law of the excluded middle:
  a proposition cannot be partially true or partially false
- law of contradiction:
  a proposition cannot be both true and false

propositions

- The Moon revolves around the Earth.
- Elephants can fly.
- $3 + 8 = 11$

not propositions

- What time is it?
- Exterminate!
- $x < 43$

Examples: Propositions

Is the following sentence a proposition? If it is a proposition, determine whether it is true or false.

Islamabad is the capital of Pakistan.

This makes a declarative statement, and hence is a proposition. The proposition is TRUE (T).

Can Ali come with you?.

This is a question not the declarative sentence and hence not a proposition.

Take two aspirins.

This is an imperative sentence not the declarative sentence and therefore not a proposition.

$x + 4 > 9$.

Because this is true for certain values of x (such as $x = 6$) and false for other values of x (such as $x = 5$), it is not a proposition.

He is a college student.

Because truth or falsity of this proposition depend on the reference for the pronoun *he*. it is not a proposition.

Propositional Variable

- propositional variable:
  a name that represents the proposition

examples

- p_1: The Moon revolves around the Earth. (T)
- p_2: Elephants can fly. (F)
- p_3: $3 + 8 = 11$ (T)

Notations

- The small letters are commonly used to denote the propositional variables, that is, variables that represent propositions, such as, p, q, r, s, ...

- The truth value of a proposition is true, denoted by T or 1, if it is a true proposition and false, denoted by F or 0, if it is a false proposition.

Compound Propositions

Logical operators are used to form new propositions also called compound propositions from two or more existing propositions.

- compound propositions are obtained by applying logical operators

  The logical operators are also called connectives.

- truth table:
  a table that lists the truth value of the compound proposition for all possible values of its variables

Propositional Logic - the area of logic that deals with propositions

1. Negation:

DEFINITION 1:

Let p be a proposition. The negation of p, denoted by ¬p, is the statement "It is not the case that p."

The proposition ¬p is read "not p." The truth value of the negation of p, ¬p is the opposite of the truth value of p.

- Examples
  - Find the negation of the proposition "Today is Friday." and express this in simple English.

    Solution: The negation is "It is not the case that today is Friday."
    In simple English, "Today is not Friday." or "It is not Friday today."
  - Find the negation of the proposition "At least 10 mm of rain fell today in Karachi." and express this in simple English.

    Solution: The negation is "It is not the case that at least 10 mm of rain fell today in Karachi."
    In simple English, "Less than 10 mm of rain fell today in Karachi."

Negation:

- Note: Always assume fixed times, fixed places, and particular people unless otherwise noted.
- Truth table:

The Truth Table for the Negation of a Proposition.	
p	¬p
T	F
F	T

examples

- $\neg p_1$: The Moon does not revolve around the Earth.
  $\neg T : F$
- $\neg p_2$: Elephants cannot fly.
  $\neg F : T$

2. Conjunction:

DEFINITION 2

Let p and q be propositions. The conjunction of p and q, denoted by p ∧ q, is the proposition "p and q". The conjunction p ∧ q is true when both p and q are true and is false otherwise.

- Examples
  - Find the conjunction of the propositions p and q where p is the proposition "Today is Friday." and q is the proposition "It is raining today.", and the truth value of the conjunction.

    Solution: The conjunction is the proposition "Today is Friday and it is raining today." The proposition is true on rainy Fridays.

$p \wedge q$

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

examples

- $p_1 \wedge p_2$: The Moon revolves around the Earth and elephants can fly.
  $T \wedge F : F$
- $p_1 \wedge p_3$: The Moon revolves around the Earth and $3 + 8 = 11$.
  $T \wedge T : T$

3. Disjunction:

DEFINITION 3

Let p and q be propositions. The disjunction of p and q, denoted by p v q, is the proposition "p or q". The disjunction p v q is false when both p and q are false and is true otherwise.

- Note:

  inclusive or : The disjunction is true when at least one of the two propositions is true.

  - E.g. "Students who have taken calculus or computer science can take this class." – those who take one or both classes.

  exclusive or : The disjunction is true only when one of the proposition is true.

  - E.g. "Students who have taken calculus or computer science, but not both, can take this class." – only those who take one of them.
- Definition 3 uses inclusive or.

Disjunction (OR)

$p \vee q$

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

example

- $p_1 \vee p_2$: The Moon revolves around the Earth or elephants can fly.
  $T \vee F : T$

4. Exclusive OR:

DEFINITION 4

Let p and q be propositions. The exclusive or of p and q, denoted by $p \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise.

The Truth Table for the Conjunction of Tw Propositions.
o

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

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

The Truth Table for the Exclusive Or (XOR) of Two Propositions.

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

Examples

1. Find the *exclusive or* of the propositions p and q, where

p : Atif will pass the course CSC102.

q : Atif will fail the course CSC102.

The *exclusive or* is

$p \oplus q$: Atif will pass or fail the course CSC102.

The following proposition uses the (English) connective "or". Determine from the context whether "or" is intended to be used in the inclusive or exclusive sense.

1. "Nabeel has one or two brothers".

A person cannot have both one and two brothers. Therefore, "or" is used in the exclusive sense.

Examples (OR vs XOR)

2. To register for BSC you must have passed the qualifying exam or be listed as an Math major.

Presumably, if you have passed the qualifying exam and are also listed as an Math major, you can still register for BCS. Therefore, “or” is inclusive.

Logical Operators

Logical Operators

We have the following logical operators:

Negation	(NOT, $\neg$)
Conjunction	(AND, $\wedge$)
Disjunction	(OR, $\vee$)
Exclusive-or	(XOR, $\oplus$)
Implication	(if – then, $\rightarrow$)
Biconditional	(if and only if, $\leftrightarrow$) or iff,

Truth tables can be used to show how these operators are defined and how can they be used to combine propositions to compound propositions.

Negation (NOT)

Unary Operator, Symbol: ¬

P	¬ P
true (T)	false (F)
false (F)	true (T)

Conjunction (AND)
Binary Operator, Symbol: $\wedge$

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction (OR)
Binary Operator, Symbol: $\vee$

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Exclusive Or (XOR)
Binary Operator, Symbol: $\oplus$

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

Implication (if – then)
Binary Operator, Symbol: $\rightarrow$

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Biconditional (if and only if)
Binary Operator, Symbol: $\leftrightarrow$

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Statements and operators can be combined in any way to form new statements.

P	Q	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

Statements and operators can be combined in any way to form new statements

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$
T	T	T	F	F
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

Equivalent Statements

The statements $\neg(P \wedge Q)$ and $(\neg P) \vee (\neg Q)$ are logically equivalent, since they have the same truth table, $\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$ is always true

P	Q	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$	$\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$
T	T	F	F	T
T	F	T	T	T
F	T	T	T	T
F	F	T	T	T

Example Truth Table

- Construct a truth table for

$$p \vee q \rightarrow \neg r$$

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

5. Implication / 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. In the conditional statement $p \rightarrow q$, p is called the hypothesis (or antecedent or premise) and q is called the conclusion (or consequence).

- A conditional statement is also called an implication.
- Example: "If I am elected, then I will lower taxes." $p \rightarrow q$

implication:

elected, lower taxes.	T	T	T
not elected, lower taxes.	F	T	T
not elected, not lower taxes.	F	F	T
elected, not lower taxes.	T	F	F

Example: Conditional Statements

- Example:
  - 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.

    Solution: Any of the following –

    "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 discrete mathematics."

    "Maria will find a good job unless she does not learn discrete mathematics."

Examples: Implication

Examples of implications:

If you stand in the rain, then you'll get wet.
If you got an A in this class, I gave you \$5.

An implication $P \Longrightarrow Q$ is false only when P is true and Q is false. For example, the first statement would be false only if you stood in the rain but didn't get wet. The second statement above would be false only if you got an "A," yet I didn't give you \$5.

Here is the truth table for $P \Longrightarrow Q$:

P	Q	$P \Longrightarrow Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

[1] P is also called the *antecedent* and Q the *consequent*.

Examples: Implication

Note that $P \Longrightarrow Q$ is always true when P is false. This means that many statements that sound nonsensical in English are true, mathematically speaking. Examples are statements like: "If pigs can fly, then horses can read" or "If 14 is odd then $1+2=18$." When an implication is stupidly true because the hypothesis is false, we say that it is **vacuously true**. Note also that $P \Longrightarrow Q$ is logically equivalent to $\neg P \vee Q$, as can be seen in the above truth table.

$P \Longrightarrow Q$ is the most common form mathematical theorems take. Here are some of the different ways of saying it:

(1) If P, then Q.
(2) Q if P.
(3) P only if Q.
(4) P is sufficient for Q.
(5) Q is necessary for P.

Some other cases of implications:

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

Implication Example

- "If I weigh over 70 kg, then I will exercise."

Implication Example

- "If I weigh over 70 kg, then I will exercise."

- p: I weigh over 70 kg.
- q: I exercise.
- when is this claim false?

$p \to q$

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

Implication Examples

- p_4: $3 < 8$, p_5: $3 < 14$, p_6: $3 < 2$, p_7: $8 < 6$

- $p_4 \to p_5$:
  if $3 < 8$, then $3 < 14$
  $T \to T : T$
- $p_4 \to p_6$:
  if $3 < 8$, then $3 < 2$
  $T \to F : F$
- $p_6 \to p_4$:
  if $3 < 2$, then $3 < 8$
  $F \to T : T$
- $p_6 \to p_7$:
  if $3 < 2$, then $8 < 6$
  $F \to F : T$

- Other conditional statements:
  - Converse of $p \rightarrow q$: $q \rightarrow p$
  - Contrapositive of $p \rightarrow q$: $\neg q \rightarrow \neg p$
  - Inverse of $p \rightarrow q$: $\neg p \rightarrow \neg q$

The contrapositive of "If you got an A in this class, I gave you \$5," is "If I did not give you \$5, you didn't get an A in this class." The converse is "If I gave you \$5 you must have received an A in this class." Does the contrapositive say the same thing as the original statement? Does the converse?

Let's look at the truth table:

P	Q	$\neg P$	$\neg Q$	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$\neg Q \Longrightarrow \neg P$	$P \Longleftrightarrow Q$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	F	F
F	T	T	F	T	F	T	F
F	F	T	T	T	T	T	T

Note that the contrapositive of $P \Longrightarrow Q$ has the same truth values, while the converse does not. Many students unreasonably assume that the converse is true, but the above truth table shows that it is not necessarily the case. When two propositional forms have the same truth values, they are said to be **logically equivalent** – they mean the same thing. We'll see next time how useful this can be for proving theorems.

Converse, Contrapositive, and Inverse

- From $p \rightarrow q$ we can form new conditional statements .
  - $q \rightarrow p$ is the **converse** of $p \rightarrow q$
  - $\neg q \rightarrow \neg p$ is the **contrapositive** of $p \rightarrow q$
  - $\neg p \rightarrow \neg q$ is the **inverse** of $p \rightarrow q$

Example: Find the converse, inverse, and contrapositive of "It is raining is a sufficient condition for my not going to town."

Solution:

converse: If I do not go to town, then it is raining.

inverse: If it is not raining, then I will go to town.

contrapositive: If I go to town, then it is not raining.

Contrapositive:

- Contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$
- Any proposition and its contrapositive are logically equivalent (have the same truth table values) – Check with the truth table.
- E.g. The contrapositive of "If you get 100% in this course, you will get an A+" is "If you do not get an A+ in this course, you did not get 100%".

Converse:

- Converse of $p \rightarrow q$ is $q \rightarrow p$
- Both are not logically equivalent.
- Ex 1: "If you get 100% in this course, you will get an A+" and "If you get an A+ in this course, you scored 100%" are not equivalent.
- Ex 2: If you won the lottery, you are rich.

Inverse:

- Inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$
- Both are not logically equivalent.
- Ex1 : "If you get 100% in this course, you will get an A+" and "If you didn't 100%, then won't have an A+ in this course." are not equivalent.
- Ex2: You can not ride the roller coaster if you are under 4 feet. What is its inverse statement?

Example of converse (1/2)

- Find the converse of the following statement:
- R: ‘Raining tomorrow is a sufficient condition for my not going to town.’
- Step 1: Assign propositional variables to
- component propositions
- P: It will rain tomorrow
- Q: I will not go to town

Example of converse (2/2)

- Step 2: Symbolize the assertion R: $P \rightarrow Q$
- Step 3: Symbolize the converse $Q \rightarrow P$
- Step 4: Convert the symbols back into words

  'If I don't go to town then it will rain tomorrow' or

  'Raining tomorrow is a necessary condition for my not going to town.' or

  'My not going to town is a sufficient condition for it raining tomorrow.'

6. Bi-implications:

DEFINITION 6

Let p and q be propositions. The biconditional statement $p \leftrightarrow q$ is the proposition "p if and only if q." The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise. Biconditional statements are also called bi-implications.

- $p \leftrightarrow q$ has the same truth value as $(p \rightarrow q) \wedge (q \rightarrow p)$
- "if and only if" can be expressed by "iff"
- Example:
  - Let p be the statement "You can take the flight" and let q be the statement "You buy a ticket." Then $p \leftrightarrow q$ is the statement "You can take the flight if and only if you buy a ticket."

    Implication:

    If you buy a ticket you can take the flight.

    If you don't buy a ticket you cannot take the flight.

Bi-implications:

If p denotes "I am at home." and q denotes "It is raining." then $p \leftrightarrow q$ denotes "I am at home if and only if it is raining."

If both $P \Longrightarrow Q$ and $Q \Longrightarrow P$ are true, then we say "P if and only if Q" (abbreviated P iff Q). Formally, we write $P \Longleftrightarrow Q$. P if and only if Q is true only when P and Q have the same truth values.

For example, if we let P be "3 is odd," Q be "4 is odd," and R be "6 is even," then $P \Longrightarrow R$, $Q \Longrightarrow P$ (vacuously), and $R \Longrightarrow P$. Because $P \Longrightarrow R$ and $R \Longrightarrow P$, P if and only if R.

Given an implication $P \Longrightarrow Q$, we can also define its

(a) **Contrapositive**: $\neg Q \Longrightarrow \neg P$
(b) **Converse**: $Q \Longrightarrow P$

The contrapositive of "If you got an A in this class, I gave you \$5," is "If I did not give you \$5, you didn't get an A in this class." The converse is "If I gave you \$5 you must have received an A in this class." Does the contrapositive say the same thing as the original statement? Does the converse?

The Truth Table for the Biconditional $p \longleftrightarrow q$.

p	q	$p \longleftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Expressing the Biconditional

- Some alternative ways “p if and only if q” is expressed in English:
  - p is necessary and sufficient for q
  - if p then q , and conversely
  - p iff q

Without changing their meanings, convert each of the following sentences into a sentence having the form "p iff q"

For a matrix to be invertible, it is necessary and sufficient that its determinant is not zero.

Answer: A matrix is invertible if and only if its determinant is not zero.

If $xy = 0$ then $x = 0$ or $y = 0$, and conversely.

Answer: $xy = 0$ if and only if $x = 0$ or $y = 0$

For an occurrence to become an adventure, it is necessary and sufficient for one to recount it.

Answer: An occurrence becomes an adventure if and only if one recounts it.

Truth Tables of Compound Propositions

- We can use connectives to build up complicated compound propositions involving any number of propositional variables, then use truth tables to determine the truth value of these compound propositions.
- Example: Construct the truth table of the compound proposition

$$(p \vee \neg q) \rightarrow (p \wedge q).$$

The Truth Table of $(p \vee \neg q) \rightarrow (p \wedge q)$.					
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

Problem:

- How many rows are there in a truth table with n propositional variables?

  Solution: 2^n We will see how to do this in Chapter 6.

- Note that this means that with n propositional variables, we can construct 2^n distinct (i.e., not equivalent) propositions.

Precedence of Logical Operators

- We can use parentheses to specify the order in which logical operators in a compound proposition are to be applied.
- To reduce the number of parentheses, the precedence order is defined for logical operators.

Precedence of Logical Operators.	
Operator	Precedence
$\neg$	1
$\wedge$ $\vee$	2 3
$\rightarrow$ $\leftrightarrow$	4 5

E.g. $\neg p \wedge q = (\neg p) \wedge q$

$p \wedge q \vee r = (p \wedge q) \vee r$

$p \vee q \wedge r = p \vee (q \wedge r)$

Translating English Sentences

(1) If P, then Q.
(2) Q if P.
(3) P only if Q.
(4) P is sufficient for Q.
(5) Q is necessary for P.

- English (and every other human language) is often ambiguous. Translating sentences into compound statements removes the ambiguity.
- Example: How can this English sentence be translated into a logical expression?

  "You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old."

Solution: Let q, r, and s represent "You can ride the roller coaster," "You are under 4 feet tall," and "You are older than 16 years old." The sentence can be translated into:

$$(r \wedge \neg s) \rightarrow \neg q.$$

You cannot ride the coaster if You are under 4 feet tall and you are not older than 16 Years old.

Translating English Sentences

(1) If P, then Q.
(2) Q if P.
(3) P only if Q.
(4) P is sufficient for Q.
(5) Q is necessary for P.

- Steps to convert an English sentence to a statement in propositional logic
  - Identify atomic propositions and represent using propositional variables.
  - Determine appropriate logical connectives
- "If I go to Harry's or to the country, I will not go shopping."
  - p: I go to Harry's
  - q: I go to the country.
  - r: I will go shopping.

If p or q then not r.

$$(p \vee q) \rightarrow \neg r$$

Translating English Sentences

- Example: 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."

Solution: Let a, c, and f represent "You can access the Internet from campus," "You are a computer science major," and "You are a freshman." The sentence can be translated into:

$$a \rightarrow (c \vee \neg f).$$

(1) If P, then Q.
(2) Q if P.
(3) P only if Q.
(4) P is sufficient for Q.
(5) Q is necessary for P.

System Specifications

- System and Software engineers take requirements in English and express them in a precise specification language based on logic.

Example: Express in propositional logic:

"The automated reply cannot be sent when the file system is full"

Solution: One possible solution: Let p denote "The automated reply can be sent" and q denote "The file system is full."

$$q \rightarrow \neg p$$

1.1 Propositional Logic

Logic and Bit Operations

- Computers represent information using bits.
- A **bit** is a symbol with two possible values, 0 and 1.
- By convention, 1 represents T (true) and 0 represents F (false).
- A variable is called a Boolean variable if its value is either true or false.
- Bit operation – replace true by 1 and false by 0 in logical operations.

Table for the Bit Operators OR, AND, and XOR.

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

1.1 Propositional Logic

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.

- Example: Find the bitwise OR, bitwise AND, and bitwise XOR of the bit string 01 1011 0110 and 11 0001 1101.

Solution:

```
 01 1011 0110
 11 0001 1101
-------------
 11 1011 1111    bitwise OR
 01 0001 0100    bitwise AND
 10 1010 1011    bitwise XOR
```

Propositional Equivalences

DEFINITION 1

A compound proposition that is always true, no matter what the truth values of the propositions that occurs in it, is called a tautology.
A compound proposition that is always false is called a contradiction.
A compound proposition that is neither a tautology or a contradiction is called a contingency.

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

Tautologies and Contradictions

- Tautology is a statement that is always true regardless of the truth values of the individual logical variables

- Examples:
- $R \vee (\neg R)$
- $\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q)$

Tautologies and Contradictions

- A Contradiction is a statement that is always false regardless of the truth values of the individual logical variables

Examples

- $R \wedge (\neg R)$
- $\neg(\neg(P \wedge Q) \leftrightarrow (\neg P) \vee (\neg Q))$
- The negation of any tautology is a contradiction, and the negation of any contradiction is a tautology.

Propositional Equivalences

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.

- Compound propositions that have the same truth values in all possible cases are called logically equivalent.
- Example: Show that $\neg p \vee q$ and $p \rightarrow q$ are logically equivalent.

Truth Tables for $\neg p \vee q$ and $p \rightarrow q$.

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

Propositional Equivalences

- In general, 2^n rows are required if a compound proposition involves n propositional variables in order to get the combination of all truth values.

- Prove that $\neg(\neg p) \equiv p$

Solution

p	¬p	¬ (¬p)
T	F	T
F	T	F

As you can see the corresponding truth values of p and ¬ (¬p) are same, hence equivalence is justified.

Propositional Equivalences

Example

Show that the proposition forms $\neg(p \wedge q)$ and $\neg p \wedge \neg q$ are NOT logically equivalent.

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

Here the corresponding truth values differ and hence equivalence does not hold

Applications: Boolean Searches

- Logical connectives are used extensively in searches of large collections of information.
  - Example: indexes of Web pages.

- AND –used to match records that contain both of two search terms.
- OR –used to match one or both of two search terms.
- NOT –used to exclude a particular search term.

- Read about: Web Page Searching

Applications: Logic Puzzles

- Puzzles (important job interview question) that can be solved using logical reasoning

- [Sm78] Smullyan: An island that has two kinds of inhabitants.
  - knights, who always tell the truth.
  - knaves, who always lie.
- You encounter two people A and B.
- What are A and B if:
  - A says "B is a knight" and
  - B says "The two of us are opposite types?"

Example 1:

- p: A is a knight $\neg p$: A is a knave
- q: B is a knight $\neg q$: B is a knave

- Consider the possibility that A is a knight;
  - So, p is true. And he is telling truth.
  - So, q is true. So, A and B are the same type.

- However, if B is a knight, then B 's statement that A and B are of opposite types, the statement $(p \wedge \neg q) \vee (\neg p \wedge q)$, would have to be true, which it 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.

Example 1: Solution (cont..)

- Consider the possibility that A is a knave,
  - everything a knave says is false; q is true, is a lie.
  - So, q is false. B is also a knave.
  - 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.

Example 2:

- A father tells his two children, a boy and a girl, to play in their backyard without getting dirty.
- However, while playing, both children get mud on their foreheads. When the children stop playing, the father says “At least one of you has a muddy forehead,” and then asks the children to answer “Yes” or “No” to the question: “Do you know whether you have a muddy forehead?”
- The father asks this question twice. What will the children answer each time this question is asked, assuming that a child can see whether his or her sibling has a muddy forehead, but cannot see his or her own forehead?
- Assume that both children are honest and that the children answer each question simultaneously.

Example 2:

Solution: S denotes "Son has a muddy forehead" and D denotes " Daughter has a muddy forehead". The father states that $S \vee D$ is True. Boy can know D is True but can't know S. Girl can know D is True but can't know S. So no for the first time. After that they can conclude that both D and S are True. Since one of them will say yes for the first time if one of D and S is not True.

Example 3:

6. Determine whether these system specifications are consistent:
   "the diagnostic message is stored in the buffer or it is retransmitted"
   "the diagnostic message is not stored in the buffer"
   "if the diagnostic message is stored in the buffer, then it is retransmitted"

Solution: p denotes "the diagnostic message is stored in the buffer", q denotes "the diagnostic message is retransmitted". Then the specifications can be written as $p \vee q$, $\neg p$ and $p \rightarrow q$. $\neg p$ is True, so p is False. $p \vee q$ is True, so q is True. So $p \rightarrow q$ is True. They are consistent.

De Morgan's laws

De Morgan's laws state that:

The negation of an **and** proposition is logically equivalent to the **or** proposition in which each component is negated.

1. $\neg(p \wedge q) \equiv \neg p \vee \neg q$

The negation of an **or** proposition is logically equivalent to the **and** proposition in which each component is negated.

2. $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Applying De-Morgan's Law

Question: Negate the following compound Propositions

1. John is six feet tall and he weights at least 200 pounds.

2. The bus was late or Tom's watch was slow.

Applying De-Morgan's Law

Question: Negate the following compound Propositions

1. John is six feet tall and he weights at least 200 pounds.

2. The bus was late or Tom's watch was slow.

Solution

a) John is not six feet tall or he weighs less than 200 pounds.

b) The bus was not late and Tom's watch was not slow.

Inequalities and De Morgan's Laws

Question Use De Morgan's laws to write the negation of

$$-1 < x \leq 4$$

Solution: The given proposition is equivalent to

$$-1 < x \quad \text{and} \quad x \leq 4,$$

By De Morgan's laws, the negation is

$$-1 \geq x \quad \text{or} \quad x > 4.$$

Laws of Logic

1. Commutative laws

   $p \wedge q \equiv q \wedge p$; $p \vee q \equiv q \vee p$

2. Associative laws

   $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$; $p \vee (q \vee r) \equiv (p \vee q) \vee r$

3. Distributive laws

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

Laws of Logic

4. Identity laws

   $p \wedge t \equiv p$; $p \vee c \equiv p$

5. Negation laws

   $p \vee \neg p \equiv t$; $p \wedge \neg p \equiv c$

6. Double negation law

   $\neg(\neg p) \equiv p$

7. Idempotent laws

   $p \wedge p \equiv p$; $p \vee p \equiv p$

Laws of Logic

8. Universal bound laws

$p \vee t \equiv t$; $p \wedge c \equiv c$

9. Absorption laws

$p \wedge (p \vee q) \equiv p$; $p \vee (p \wedge q) \equiv p$

10. Negation of *t* and *c*

$\neg t \equiv c$; $\neg c \equiv t$

Example

Show that the proposition form $p \vee \neg p$ is a tautology and the proposition form $p \wedge \neg p$ is a contradiction.

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

Exercise: If t is a tautology and c is contradiction, show that $p \vee t \equiv p$ and $p \wedge c \equiv c$?

Propositional Equivalences

Constructing New Logical Equivalences

- Example: Show that $\neg(p \rightarrow q)$ and $p \wedge \neg q$ are logically equivalent.

  Solution:

  $\neg(p \rightarrow q) \equiv \neg(\neg p \vee q)$ by example discussed in slide 66

  $\equiv \neg(\neg p) \wedge \neg q$ by the second De Morgan law

  $\equiv p \wedge \neg q$ by the double negation law

- Example: Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

  Solution: To show that this statement is a tautology, we will use logical equivalences to demonstrate that it is logically equivalent to T.

  $(p \wedge q) \rightarrow (p \vee q) \equiv \neg(p \wedge q) \vee (p \vee q)$ by example already discussed

  $\equiv (\neg p \vee \neg q) \vee (p \vee q)$ by the first De Morgan law

  $\equiv (\neg p \vee p) \vee (\neg q \vee q)$ by the associative and communicative law for disjunction

  $\equiv T \vee T$

  $\equiv T$

- Note: The above examples can also be done using truth tables.

Exercise

Using laws of logic, show that

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

Solution

Take $\neg(\neg p \wedge q) \wedge (p \vee q)$

$\equiv (\neg(\neg p) \vee \neg q) \wedge (p \vee q)$, (by De Morgan's laws)

$\equiv (p \vee \neg q) \wedge (p \vee q)$, (by double negative law)

$\equiv p \vee (\neg q \wedge q)$, (by distributive law)

$\equiv p \vee (q \wedge \neg q)$, (by the commutative law)

$\equiv p \vee c$, (by the negation law)

$\equiv p$, (by the identity law)

Skill in simplifying proposition forms is useful in constructing logically efficient computer programs and in designing digital circuits.

Exercise

Prove that $\neg[r \vee (q \wedge (\neg r \rightarrow \neg p))] \equiv \neg r \wedge (p \vee \neg q)$

$\neg[r \vee (q \wedge (\neg r \rightarrow \neg p))]$	
$\equiv \neg r \wedge \neg(q \wedge (\neg r \rightarrow \neg p))$,	De Morgan's law
$\equiv \neg r \wedge \neg(q \wedge (\neg\neg r \vee \neg p))$,	Conditional rewritten as disjunction
$\equiv \neg r \wedge \neg(q \wedge (r \vee \neg p))$,	Double negation law
$\equiv \neg r \wedge (\neg q \vee \neg(r \vee \neg p))$,	De Morgan's law
$\equiv \neg r \wedge (\neg q \vee (\neg r \wedge p))$,	De Morgan's law, double negation
$\equiv (\neg r \wedge \neg q) \vee (\neg r \wedge (\neg r \wedge p))$,	Distributive law
$\equiv (\neg r \wedge \neg q) \vee ((\neg r \wedge \neg r) \wedge p)$,	Associative law
$\equiv (\neg r \wedge \neg q) \vee (\neg r \wedge p)$,	Idempotent law
$\equiv \neg r \wedge (\neg q \vee p)$,	Distributive law
$\equiv \neg r \wedge (p \vee \neg q)$,	Commutative law

Exercise

Prove that:

$\neg(P \leftrightarrow Q) \equiv P \leftrightarrow \neg Q$

** $P \rightarrow Q \equiv \neg P \vee Q$

$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$

$\equiv (\neg P \vee Q) \wedge (\neg Q \vee P)$

$\neg(P \leftrightarrow Q)$

$\equiv \neg((\neg P \vee Q) \wedge (\neg Q \vee P))$ ##

$\equiv \neg(\neg P \vee Q) \vee \neg(\neg Q \vee P)$ *De Morgan's Laws*

$\equiv (P \wedge \neg Q) \vee (Q \wedge \neg P)$ *De Morgan's Laws*

$\equiv ((P \wedge \neg Q) \vee Q) \wedge ((P \wedge \neg Q) \vee \neg P)$ *Distributive Laws*

$\equiv ((P \vee Q) \wedge (\neg Q \vee Q)) \wedge ((P \vee \neg P) \wedge (\neg Q \vee \neg P))$ *Distributive Laws*

$\equiv (P \vee Q) \wedge T \wedge T \wedge (\neg Q \vee \neg P)$ *Negation Laws*

$\equiv (P \vee Q) \wedge (\neg Q \vee \neg P)$ *Identify Laws*

$\equiv P \leftrightarrow \neg Q$ ##

Rules of Inference

Section 1.6

Section Summary

- Valid Arguments
- Inference Rules for Propositional Logic
- Using Rules of Inference to Build Arguments
- Rules of Inference for Quantified Statements
- Building Arguments for Quantified Statements

Revisiting the Socrates Example

- We have the two premises:
  - “All men are mortal.”
  - “Socrates is a man.”
- And the conclusion:
  - “Socrates is mortal.”
- How do we get the conclusion from the premises?

The Argument

- We can express the premises (above the line) and the conclusion (below the line) in predicate logic as an argument:

$$\frac{\begin{array}{c}\forall x(Man(x) \rightarrow Mortal(x)) \\ Man(Socrates)\end{array}}{\therefore \quad Mortal(Socrates)}$$

- We will see shortly that this is a valid argument.

Valid Arguments

- We will show how to construct valid arguments in two stages; first for propositional logic and then for predicate logic. The rules of inference are the essential building block in the construction of valid arguments.

1. Propositional Logic

   Inference Rules

2. Predicate Logic

   Inference rules for propositional logic plus additional inference rules to handle variables and quantifiers.

Valid Arguments (Propositional Logic)

- “If you have a current password, then you can log onto the network.”
- “You have a current password.”
- Therefore, “You can log onto the network.”

- Sequence of propositions (argument) is valid; the conclusion must be true when both premise are true.

Argument Form

- p: “You have a current password”
- q: “You can log onto the network.”
- the argument has the form

$$p \rightarrow q$$
$$p$$
$$\therefore q$$

the statement $((p \rightarrow q) \wedge p) \rightarrow q$ is a tautology

Argument Form

- p: ““You have access to the network”
- q: “You can change your grade”
- the argument has the form

“If you have access to the network, then you can change your grade.”

“You have access to the network.”

∴“You can change your grade.”

- The argument is valid, but if premise is false, we cannot conclude that the conclusion is true.

Arguments in Propositional Logic

- A argument in propositional logic is a sequence of propositions. All but the final proposition are called premises. The last statement is the conclusion.
- The argument is valid if the premises imply the conclusion. An argument form is an argument that is valid no matter what propositions are substituted into its propositional variables.
- If the premises are $p_1, p_2, \ldots, p_n$ and the conclusion is q then $(p_1 \text{ A } p_2 \text{ A} \ldots \text{A } p_n) \rightarrow q$ is a tautology.
- Inference rules are all argument simple argument forms that will be used to construct more complex argument forms.

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
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism

TABLE 1 **Rules of Inference.**

Rule of Inference	*Tautology*	*Name*
p $\therefore\ p \vee q$	$p \rightarrow (p \vee q)$	Addition
$p \wedge q$ $\therefore\ p$	$(p \wedge q) \rightarrow p$	Simplification
p q $\therefore\ p \wedge q$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore\ q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

Rules of Inference for Propositional Logic: **Modus Ponendo Ponens**

$$\frac{P \to Q, P}{\therefore Q}$$

- Latin for "the way that affirms by affirming"

- **Implication elimination**
- Abbreviated to MP or **modus ponens**

- whenever p → q is true
- and p is true,
- q must also be true.

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

Modus Ponens

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

Corresponding Tautology:

$(p \wedge (p \rightarrow q)) \rightarrow q$

Example:

Let *p* be "It is snowing."

Let *q* be "I will study discrete math."

"If it is snowing, then I will study discrete math."

"It is snowing."

"Therefore , I will study discrete math."

Modus Ponens

- State which rule of inference is the basis of the following argument:
- "If it snows today, then we will go skiing". "It is snowing today", "therefore we will go skiing".
- Let p be the proposition "It is snowing today" and q the proposition "We will go skiing" Then this argument is of the form

$$p \rightarrow q$$
$$p$$
$$\therefore q$$

- This is an argument that uses the Modus Ponens rule.

Modus Tollendo Tollens

$$\frac{P \to Q, \neg Q}{\therefore \neg P}$$

- Latin for "the way that denies by denying"

- **Denying the consequent**
- **Abbreviated to modus tollens**

- in every instance in which
- p → q is true and q is false,
- p must also be false.

p	q	p → q
T	T	T
T	F	F
F	T	T
F	F	T

Modus Tollens

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

Corresponding Tautology:

$(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$

Example:
Let *p* be “it is snowing.”
Let *q* be “I will study discrete math.”

“If it is snowing, then I will study discrete math.”
“I will not study discrete math.”

“Therefore , it is not snowing.”

Hypothetical Syllogism

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

Corresponding Tautology:
$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

Example:
Let *p* be "it snows."
Let *q* be "I will study discrete math."
Let *r* be "I will get an A."

"If it snows, then I will study discrete math."
"If I study discrete math, I will get an A."

"Therefore , If it snows, I will get an A."

Hypothetical Syllogism

- State which rule of inference is used in the argument:
- If it rains today, then we will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. Therefore, if it rains today, then we will have a barbecue tomorrow.

$$p \rightarrow q$$

$$q \rightarrow r$$

$$\therefore p \rightarrow r$$

- Hence, this argument is a hypothetical syllogism.

Disjunctive Syllogism

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

Corresponding Tautology:
$(\neg p \wedge (p \vee q)) \rightarrow q$

Example:
Let *p* be “I will study discrete math.”
Let *q* be “I will study English literature.”

“I will study discrete math or I will study English literature.”
“I will not study discrete math.”

“Therefore , I will study English literature.”

Addition

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

Corresponding Tautology:

$p \rightarrow (p \vee q)$

Example:
Let *p* be "I will study discrete math."
Let *q* be "I will visit Las Vegas."

"I will study discrete math."

"Therefore, I will study discrete math or I will visit Las Vegas."

Addition Rule

- State which rule of inference is the basis of the following argument:
- "It is below freezing now. Therefore, it is either below freezing or raining now."
- Let p be the proposition "It is below freezing now" and q the proposition "It is raining now." Then this argument is of the form

$$p$$
$$\therefore p \vee q$$

- This is an argument that uses the addition rule.

Simplification

$$\frac{p \wedge q}{\therefore q}$$

Corresponding Tautology:

$(p \wedge q) \rightarrow p$

Example:
Let *p* be “I will study discrete math.”
Let *q* be “I will study English literature.”

“I will study discrete math and English literature”

“Therefore, I will study discrete math.”

Simplification Rule

- State which rule of inference is the basis of the following argument:
- “It is below freezing and raining now. Therefore, it is below freezing now.”
- Let p be the proposition “It is below freezing now,” and let q be the proposition “It is raining now.” This argument is of the form

pAq

∴p

- This argument uses the simplification rule.

Conjunction

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

Corresponding Tautology:
$((p) \wedge (q)) \rightarrow (p \wedge q)$

Example:
Let *p* be "I will study discrete math."
Let *q* be "I will study English literature."

"I will study discrete math."
"I will study English literature."

"Therefore, I will study discrete math and I will study English literature."

Resolution

Resolution plays an important role in AI and is used in Prolog.

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

Corresponding Tautology:
$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$

Example:
Let *p* be "I will study discrete math."
Let *r* be "I will study English literature."
Let q be "I will study databases."

"I will not study discrete math or I will study English literature."
"I will study discrete math or I will study databases."

"Therefore, I will study databases or I will English literature."

Using the Rules of Inference to Build Valid Arguments

- A valid argument is a sequence of statements. Each statement is either a premise or follows from previous statements by rules of inference. The last statement is called conclusion.
- A valid argument takes the following form:

$$
\begin{array}{l}
S_1 \\
S_2 \\
\vdots \\
S_n \\
\\
\therefore C
\end{array}
$$

Fallacies

- Arguments are based on tautologies.
- Fallacies are based on contingencies.
- The proposition $((p \rightarrow q) \wedge q) \rightarrow p$ 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.**
- Example:
- If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics. Therefore, you did every problem in this book.

Fallacy of denying the hypothesis.

- The proposition $((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$ is not a tautology, because it is false when p is false and q is true.
- Is it correct to assume that you did not learn discrete mathematics if you did not do every problem in the book, assuming that if you do every problem in this book, then you will learn discrete mathematics?
- It is possible that you learned discrete mathematics even if you did not do every problem in this book. This incorrect argument is of the form $p \rightarrow q$ and $\neg p$ imply $\neg q$, which is an example of the fallacy of denying the hypothesis.

Fallacies

- **Are the following arguments correct?**
  - **Example 1 (Fallacy of affirming the conclusion)**

    Hypothesis
    - If you success, you work hard $p \rightarrow q$
    - You work hard q

    Conclusion $\therefore\ p$
    - You success

    ✗
  - **Example 2 (Fallacy of denying the hypothesis)**

    Hypothesis
    - If you success, you work hard $p \rightarrow q$
    - You do not success $\neg p$

    Conclusion $\therefore\ \neg q$
    - You do not work hard

    ✗

V. Tell the validity of each argument by choosing one of the following:

MP- Modus Ponens **LS- Law of Syllogism (Hypothetical)**
MT- Modus Tollens **LC- Law of Contrapositive**
NVC- No Valid Conclusion

a. _____

$p \rightarrow \sim r$
$\sim p$
_____
$\therefore r$

b. _____

$s \rightarrow t$
$\sim t$
_____
$\therefore \sim s$

c. _____

$r \rightarrow \sim t$
$\sim t \rightarrow v$
_____
$\therefore r \rightarrow v$

d. _____

$r \rightarrow p$
p
_____
$\therefore r$

e. _____

$\sim w \rightarrow \sim s$
$\sim w$
_____
$\therefore \sim s$

f. _____

$t \rightarrow (r \rightarrow s)$
$\sim(r \rightarrow s)$
_____
$\therefore \sim t$

g. _____

$p \rightarrow \sim r$
_____
$\therefore r \rightarrow \sim p$

h. _____

$r \rightarrow q$
$s \rightarrow q$
_____
$\therefore r \rightarrow s$

V. Tell the validity of each argument by choosing one of the following:

MP- Modus Ponens **LS- Law of Syllogism (Hypothetical)**
MT- Modus Tollens **LC- Law of Contrapositive**
NVC- No Valid Conclusion

a. NVC

$p \rightarrow \sim r$
$\sim p$

$\therefore r$

b. M.T

$(s \rightarrow t)$ ✓
$\wedge (\sim t)$

$\therefore \boxed{\sim s}$

c. LS (H.S)

$r \rightarrow \cancel{\sim t}$
$\cancel{\sim t} \rightarrow v$

$\therefore r \rightarrow v$

d. NVC

$r \rightarrow p$
p

$\therefore r$

e. M.P

$\sim w \rightarrow \sim s$ ✓
$\sim w$

$\therefore \sim s$

f. M.T

$t \rightarrow (r \rightarrow s)$ ✓
$\sim(r \rightarrow s)$

$\therefore \sim t$

g. L.C

$p \rightarrow \sim r$

$\therefore r \rightarrow \sim p$

h. N.V.C

$r \rightarrow q$
$s \rightarrow q$

$\therefore r \rightarrow s$

Comparison between Inference and Equivalence

- **Inference ($p \rightarrow q$)**
  - Meaning:
    If p, then q
  - $p \rightarrow q$ does not mean $q \rightarrow p$
  - Either inference or equivalence rules can be used
  - $p \leftrightarrow q$ implies $p \rightarrow q$
  - $\Rightarrow$ is used in proof
- **Equivalence ($p \leftrightarrow q$)**
  - Meaning:
    p is equal to q
  - $p \leftrightarrow q$ mean $q \leftrightarrow p$
  - Only equivalence rules can be used
  - $p \leftrightarrow q$ can be proved by showing $p \rightarrow q$ and $q \rightarrow p$
  - $\Leftrightarrow$ is used in proof
- Equivalence ($\leftrightarrow$) is a **more restrictive** relation than Inference ($\rightarrow$)

Using Rules of Inference

- Example 1:
  - **Given:**
    - It is not 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
  - Can these propositions lead to the **conclusion** "We will be home by sunset" ?

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

$\neg p \wedge q$	It is not sunny this afternoon and it is colder than yesterday
$r \rightarrow p$	We will go swimming only if it is sunny
$\neg r \rightarrow s$	If we do not go swimming, then we will take a canoe trip
$s \rightarrow t$	If we take a canoe trip, then we will be home by sunset
t	We will be home by sunset

Using Rules of Inference

Hypothesis:

$\neg p \wedge q$

$r \rightarrow p$

$\neg r \rightarrow s$

$s \rightarrow t$

Conclusion:

t

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

Therefore, the propositions can lead to the conclusion
We will be home by sunset

Using Rules of Inference

- Or, another presentation method:

Hypothesis:

$\neg p \wedge q$

$r \rightarrow p$

$\neg r \rightarrow s$

$s \rightarrow t$

Conclusion:

t

$(\neg p \wedge q) \wedge (r \rightarrow p) \wedge (\neg r \rightarrow s) \wedge (s \rightarrow t)$

$\Rightarrow \neg p \wedge (r \rightarrow p) \wedge (\neg r \rightarrow s) \wedge (s \rightarrow t)$ By Simplification

$\Rightarrow \neg r \wedge (\neg r \rightarrow s) \wedge (s \rightarrow t)$ By Modus Tollens

$\Rightarrow s \wedge (s \rightarrow t)$ By Modus Ponens

$\Rightarrow t$ By Modus Ponens

EXAMPLE #2

- **Given:**
  - 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
  - If I go to sleep early, then I will wake up feeling refreshed
- Can these propositions 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

$p \rightarrow q$

- If you send me an e-mail message, then I will finish writing the program

$\neg p \rightarrow r$

- If you do not send me an e-mail message, then I will go to sleep early

$r \rightarrow s$

- If I go to sleep early, then I will wake up feeling refreshed

---

$\neg q \rightarrow s$

- If I do not finish writing the program, then I will wake up feeling refreshed

Hypothesis:

$p \rightarrow q$

$\neg p \rightarrow r$

$r \rightarrow s$

Conclusion:

$\neg q \rightarrow s$

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

Therefore, the propositions can lead to the conclusion

If I do not finish writing the program,

then I will wake up feeling refreshed

- Or, another presentation method:

Hypothesis:

$p \to q$

$\neg p \to r$

$r \to s$

Conclusion:

$\neg q \to s$

$$\boxed{(p \to q)} \wedge (\neg p \to r) \wedge (r \to s)$$

$$\Leftrightarrow \boxed{(\neg q \to \neg p) \wedge (\neg p \to r)} \wedge (r \to s)$$ Contrapositive

$$\Rightarrow \boxed{(\neg q \to r) \wedge (r \to s)}$$ By Hypothetical Syllogism

$$\Rightarrow (\neg q \to s)$$ By Hypothetical Syllogism

Valid Arguments

Example 3: From the single proposition

$$p \wedge (p \rightarrow q)$$

Show that *q* is a conclusion.

Solution:

Step	**Reason**
1. $p \wedge (p \rightarrow q)$	Premise
2. p	Conjunction using (1)
3. $p \rightarrow q$	Conjunction using (1)
4. q	Modus Ponens using (2) and (3)

Valid Arguments (Predicate Logic)

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\forall x P(x)$ $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore \exists x P(x)$	Existential generalization

Universal Instantiation

- 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 ∀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.

Universal Generalization

- 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.
- •Universal generalization is used when we show that $\forall x P(x)$ is true by taking an arbitrary element c from the domain and showing that $P(c)$ is true.
- •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.

Existential Instantiation

- 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.

Existential Generalization

- 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.

The Foundations: Logic and Proofs

Chapter 1, Part II: Predicate Logic

Summary

- Predicate Logic (First-Order Logic (FOL), Predicate Calculus)
  - The Language of Quantifiers
  - Logical Equivalences
  - Nested Quantifiers
  - Translation from Predicate Logic to English
  - Translation from English to Predicate Logic

Predicates and Quantifiers

Section 1.4

Section Summary

- Predicates
- Variables
- Quantifiers
  - Universal Quantifier
  - Existential Quantifier
- Negating Quantifiers
  - De Morgan's Laws for Quantifiers
- Translating English to Logic
- Logic Programming (optional)

Propositional Logic Not Enough

- If we have:

  "All men are mortal."

  "Socrates is a man."
- Does it follow that "Socrates is mortal?"
- Can't be represented in propositional logic. Need a language that talks about objects, their properties, and their relations.
- Later we'll see how to draw inferences.

Introducing Predicate Logic

- Predicate logic uses the following new features:
  - Variables: x, y, z
  - Predicates: P(x), M(x)
  - Quantifiers (to be covered in a few slides):
- Propositional functions are a generalization of propositions.
  - They contain variables and a predicate, e.g., P(x)
  - Variables can be replaced by elements from their domain.

Propositional Functions

- Propositional functions become propositions (and have truth values) when their variables are each replaced by a value from the domain (or bound by a quantifier, as we will see later).
- The statement P(x) is said to be the value of the propositional function P at x.
- For example, let P(x) denote "$x > 0$" and the domain be the integers. Then:

  $P(-3)$ is false.

  $P(0)$ is false.

  $P(3)$ is true.
- Often the domain is denoted by U. So in this example U is the integers.

Examples of Propositional Functions

- Let "$x + y = z$" be denoted by $R(x, y, z)$ and U (for all three variables) be the integers. Find these truth values:

  $R(2,-1,5)$

  Solution: F

  $R(3,4,7)$

  Solution: T

  $R(x, 3, z)$

  Solution: Not a Proposition

- Now let "$x - y = z$" be denoted by $Q(x, y, z)$, with U as the integers. Find these truth values:

  $Q(2,-1,3)$

  Solution: T

  $Q(3,4,7)$

  Solution: F

  $Q(x, 3, z)$

  Solution: Not a Proposition

Compound Expressions

- Connectives from propositional logic carry over to predicate logic.
- If P(x) denotes "$x > 0$," find these truth values:

  $P(3) \vee P(-1)$ Solution: T

  $P(3) \wedge P(-1)$ Solution: F

  $P(3) \rightarrow P(-1)$ Solution: F

  $P(3) \rightarrow P(1)$ Solution: T
- Expressions with variables are not propositions and therefore do not have truth values. For example,

  $P(3) \wedge P(y)$

  $P(x) \rightarrow P(y)$
- When used with quantifiers (to be introduced next), these expressions (propositional functions) become propositions.

Quantifiers

Charles Peirce (1839-1914)

- We need quantifiers to express the meaning of English words including all and some:
  - "All men are Mortal."
  - "Some cats do not have fur."
- The two most important quantifiers are:
  - Universal Quantifier, "For all," symbol: $\forall$
  - Existential Quantifier, "There exists," symbol: $\exists$
- We write as in $\forall x\, P(x)$ and $\exists x\, P(x)$.
- $\forall x\, P(x)$ asserts $P(x)$ is true for <u>every</u> x in the domain.
- $\exists x\, P(x)$ asserts $P(x)$ is true for <u>some</u> x in the domain.
- The quantifiers are said to bind the variable x in these expressions.

Quantifiers

- Universal Quantifier, "For all," symbol: $\forall$
- Existential Quantifier, "There exists," symbol: $\exists$

TABLE 1 Quantifiers.

Statement	*When True?*	*When False?*
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

Universal Quantifier

$\forall x\, P(x)$ is read as " For all x, P(x)" or "For every x, P(x)"

Examples:

1) If P(x) denotes "$x > 0$" and U is the integers, then $\forall x$ P(x) is false.
2) If P(x) denotes "$x > 0$" and U is the positive integers, then $\forall x\, P(x)$ is true.
3) If P(x) denotes "x is even" and U is the integers, then $\forall\, x\, P(x)$ is false.

Existential Quantifier

- $\exists x\, P(x)$ is read as "For some x, P(x)", or as "There is an x such that P(x)," or "For at least one x, P(x)."

  Examples:

  1. If P(x) denotes "$x > 0$" and U is the integers, then $\exists x\, P(x)$ is true. It is also true if U is the positive integers.
  2. If P(x) denotes "$x < 0$" and U is the positive integers, then $\exists x\, P(x)$ is false.
  3. If P(x) denotes "x is even" and U is the integers, then $\exists x\, P(x)$ is true.

Uniqueness Quantifier (optional)

- $\exists! x\ P(x)$ means that $P(x)$ is true for <u>one and only one</u> x in the universe of discourse.
- This is commonly expressed in English in the following equivalent ways:
  - "There is a unique x such that $P(x)$."
  - "There is one and only one x such that $P(x)$"
- Examples:
  1. If $P(x)$ denotes "$x + 1 = 0$" and U is the integers, then $\exists! x\ P(x)$ is true.
  2. But if $P(x)$ denotes "$x > 0$," then $\exists! x\ P(x)$ is false.
- The uniqueness quantifier is not really needed as the restriction that there is a unique x such that P(x) can be expressed as:

$$\exists x\,(P(x) \wedge \forall y\,(P(y) \rightarrow y = x))$$

Thinking about Quantifiers

- When the domain of discourse is finite, we can think of quantification as looping through the elements of the domain.
- To evaluate $\forall x\ P(x)$ loop through all x in the domain.
  - If at every step $P(x)$ is true, then $\forall x\ P(x)$ is true.
  - If at a step $P(x)$ is false, then $\forall x\ P(x)$ is false and the loop terminates.
- To evaluate $\exists x\ P(x)$ loop through all x in the domain.
  - If at some step, $P(x)$ is true, then $\exists x\ P(x)$ is true and the loop terminates.
  - If the loop ends without finding an x for which $P(x)$ is true, then $\exists x\ P(x)$ is false.
- Even if the domains are infinite, we can still think of the quantifiers this fashion, but the loops will not terminate in some cases.

Properties of Quantifiers

- The truth value of $\exists x\, P(x)$ and $\forall x\, P(x)$ depend on both the propositional function $P(x)$ and on the domain U.
- Examples:
  1. If U is the positive integers and P(x) is the statement "$x < 2$", then $\exists x\, P(x)$ is true, but $\forall x\, P(x)$ is false.
  2. If U is the negative integers and P(x) is the statement "$x < 2$", then both $\exists x\, P(x)$ and $\forall x\, P(x)$ are true.
  3. If U consists of 3, 4, and 5, and P(x) is the statement "$x > 2$", then both $\exists x\, P(x)$ and $\forall x\, P(x)$ are true. But if P(x) is the statement "$x < 2$", then both $\exists x\, P(x)$ and $\forall x\, P(x)$ are false.

Precedence of Quantifiers

- The quantifiers $\forall$ and $\exists$ have higher precedence than all the logical operators.
- For example, $\forall x\, P(x) \vee Q(x)$ means $(\forall x\, P(x)) \vee Q(x)$
- $\forall x\, (P(x) \vee Q(x))$ means something different.
- Unfortunately, often people write $\forall x\, P(x) \vee Q(x)$ when they mean $\forall x\, (P(x) \vee Q(x))$.

Translating from English to Logic

Example 1: Translate the following sentence into predicate logic: "Every student in this class has taken a course in Java."

Solution:

First decide on the domain U.

Solution 1: If U is all students in this class, define a propositional function J(x) denoting "x has taken a course in Java" and translate as $\forall x\, J(x)$.

Solution 2: But if U is all people, also define a propositional function S(x) denoting "x is a student in this class" and translate as $\forall x\, (S(x) \rightarrow J(x))$.

$\forall x\, (S(x) \wedge J(x))$ is not correct. What does it mean?

For example,
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 Java.”
If S(x) represents the statement that person x is in this class, we see that our statement can be expressed as $\forall x(S(x) \rightarrow J(x))$.
[Caution! Our statement cannot be expressed as $\forall x(S(x) \wedge J(x))$ because this statement says that all people are students in this class and have studied Java!]

Translating from English to Logic

Example 2: Translate the following sentence into predicate logic: "Some student in this class has taken a course in Java."

Solution:

First decide on the domain U.

Solution 1: If U is all students in this class, translate as

$$\exists x\, J(x)$$

Solution 1: But if U is all people, then translate as

$\exists x\, (S(x) \text{ A } J(x))$

$\exists x\, (S(x) \rightarrow J(x))$ is not correct. What does it mean?

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 studied Java.”
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 $\exists x(S(x) \wedge J(x))$ because the statement is that there is a person x who is a student in this class and who has studied Java.
[Caution! Our statement cannot be expressed as $\exists x(S(x) \rightarrow J(x))$, which is true when there is someone not in the class because, in that case, for such a person x, $S(x) \rightarrow J(x)$ becomes either $F \rightarrow T$ or $F \rightarrow F$, both of which are true.]

Returning to the Socrates Example

- Introduce the propositional functions Man(x) denoting "x is a man" and Mortal(x) denoting "x is mortal." Specify the domain as all people.
- The two premises are:

$$\forall x Man(x) \rightarrow Mortal(x)$$

$$Man(Socrates)$$

- The conclusion is:

$$Mortal(Socrates)$$

- Later we will show how to prove that the conclusion follows from the premises.

Equivalences in Predicate Logic

- Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value
  - for every predicate substituted into these statements and
  - for every domain of discourse used for the variables in the expressions.
- The notation $S \equiv T$ indicates that S and T are logically equivalent.
- Example: $\forall x \neg\neg S(x) \equiv \forall x\, S(x)$

Thinking about Quantifiers as Conjunctions and Disjunctions

- If the domain is finite, a universally quantified proposition is equivalent to a conjunction of propositions without quantifiers and an existentially quantified proposition is equivalent to a disjunction of propositions without quantifiers.
- If U consists of the integers 1,2, and 3:

$$\forall x P(x) \equiv P(1) \wedge P(2) \wedge P(3)$$

$$\exists x P(x) \equiv P(1) \vee P(2) \vee P(3)$$

- Even if the domains are infinite, you can still think of the quantifiers in this fashion, but the equivalent expressions without quantifiers will be infinitely long.

Negating Quantified Expressions

- Consider $\forall x\, J(x)$

  "Every student in your class has taken a course in Java."

  Here $J(x)$ is "x has taken a course in Java" and the domain is students in your class.

- Negating the original statement gives "It is not the case that every student in your class has taken a course in Java." This implies that "There is a student in your class who has not taken a course in Java."

  Symbolically $\neg\forall x\, J(x)$ and $\exists x\, \neg J(x)$ are equivalent

Negating Quantified Expressions (continued)

- Now Consider $\exists x\, J(x)$

  "There is a student in this class who has taken a course in Java."

  Where $J(x)$ is "x has taken a course in Java."
- Negating the original statement gives "It is not the case that there is a student in this class who has taken Java." This implies that "Every student in this class has not taken a course in Java"

  Symbolically $\neg\exists x\, J(x)$ and $\forall x\, \neg J(x)$ are equivalent

De Morgan's Laws for Quantifiers

- The rules for negating quantifiers are:

TABLE 2 De Morgan's Laws for Quantifiers.

Negation	*Equivalent Statement*	*When Is Negation True?*	*When False?*
$\neg\exists x P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

- The reasoning in the table shows that:

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

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

- These are important. You will use these.

Translation from English to Logic

Examples:

1. "Some student in this class has visited Mexico."

   Solution: Let M(x) denote "x has visited Mexico" and S(x) denote "x is a student in this class," and U be all people.

   $$\exists x \ (S(x) \text{ A } M(x))$$

2. "Every student in this class has visited Canada or Mexico."

   Solution: Add C(x) denoting "x has visited Canada." and U be all people.

   $$\forall x \ (S(x) \rightarrow (M(x) \vee C(x)))$$

Some Fun with Translating from English into Logical Expressions

- U ={Nitwits, Blubbers, Oddments}

  F(x): x is a Nitwit

  S(x): x is a Blubber

  T(x): x is a Oddment

  Translate "Everything is a Nitwit"

  Solution: $\forall x\, F(x)$

Translation (cont)

- U ={Nitwits, Blubbers, Oddments}

  F(x): x is a Nitwit

  S(x): x is a Blubber

  T(x): x is a Oddment

  "Nothing is a Blubber."

  Solution: $\neg\exists x\, S(x)$ What is this equivalent to?

  Solution: $\forall x \neg S(x)$

Translation (cont)

- U ={Nitwits, Blubbers, Oddments}

  F(x): x is a Nitwit

  S(x): x is a Blubber

  T(x): x is a Oddment

"All Nitwits are Blubbers."

Solution: $\forall x\ (F(x) \rightarrow S(x))$

Translation (cont)

- U ={Nitwits, Blubbers, Oddments}

  F(x): x is a Nitwit

  S(x): x is a Blubber

  T(x): x is a Oddment

"Some Nitwits are Oddments."

Solution: $\exists x\ (F(x)\ A\ T(x))$

Translation (cont)

- U ={Nitwits, Blubbers, Oddments}

  F(x): x is a Nitwit

  S(x): x is a Blubber

  T(x): x is a Oddment

  "No Blubber is a Oddment."

  Solution: $\neg\exists x\ (S(x) \text{ A } T(x))$ What is this equivalent to?

  Solution: $\forall x\ \neg\ (S(x) \text{ A } T(x))$

  $\forall x\ (\neg S(x) \vee \neg T(x))$

Translation (cont)

- U ={Nitwits, Blubbers, Oddments}

  F(x): x is a Nitwit

  S(x): x is a Blubber

  T(x): x is a Oddment

"If any Nitwit is a Blubber then it is also a Oddment."

Solution: $\forall x\ ((F(x) \text{ A } S(x)) \rightarrow T(x))$

System Specification Example

- Predicate logic is used for specifying properties that systems must satisfy.
- For example, translate into predicate logic:
  - "Every mail message larger than one megabyte will be compressed."
  - "If a user is active, at least one network link will be available."
- Decide on predicates and domains (left implicit here) for the variables:
  - Let L(m, y) be "Mail message m is larger than y megabytes."
  - Let C(m) denote "Mail message m will be compressed."
  - Let A(u) represent "User u is active."
  - Let S(n, x) represent "Network link n is state x.
- Now we have:

$$\forall m(L(m,1) \rightarrow C(m))$$

$$\exists u\, A(u) \rightarrow \exists n\, S(n, available)$$

Lewis Carroll Example

Charles Lutwidge Dodgson
(AKA Lewis Caroll)
(1832-1898)

- The first two are called premises and the third is called the conclusion.
  1. "All lions are fierce."
  2. "Some lions do not drink coffee."
  3. "Some fierce creatures do not drink coffee."
- Here is one way to translate these statements to predicate logic. Let P(x), Q(x), and R(x) be the propositional functions "x is a lion," "x is fierce," and "x drinks coffee," respectively.
  1. $\forall x\,(P(x) \rightarrow Q(x))$
  2. $\exists x\,(P(x) \wedge \neg R(x))$
  3. $\exists x\,(Q(x) \wedge \neg R(x))$
- Later we will see how to prove that the conclusion follows from the premises.

Nested Quantifiers

Section 1.5

Section Summary

- Nested Quantifiers
- Order of Quantifiers
- Translating from Nested Quantifiers into English
- Translating Mathematical Statements into Statements involving Nested Quantifiers.
- Translated English Sentences into Logical Expressions.
- Negating Nested Quantifiers.

Nested Quantifiers

- Nested quantifiers are often necessary to express the meaning of sentences in English as well as important concepts in computer science and mathematics.

  Example: "Every real number has an inverse" is

  $$\forall x\, \exists y (x + y = 0)$$

  where the domains of x and y are the real numbers.

- We can also think of nested propositional functions:

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

Thinking of Nested Quantification

- Nested Loops
  - To see if $\forall x \forall y P(x,y)$ is true, loop through the values of x :
    - At each step, loop through the values for y.
    - If for some pair of x andy, P(x,y) is false, then $\forall x \forall y P(x,y)$ is false and both the outer and inner loop terminate.

    $\forall x \forall y P(x,y)$ is true if the outer loop ends after stepping through each x.
  - To see if $\forall x \exists y P(x,y)$ is true, loop through the values of x:
    - At each step, loop through the values for y.
    - The inner loop ends when a pair x and y is found such that P(x, y) is true.
    - If no y is found such that P(x, y) is true the outer loop terminates as $\forall x \exists y P(x,y)$ has been shown to be false.

    $\forall x \exists y P(x,y)$ is true if the outer loop ends after stepping through each x.
- If the domains of the variables are infinite, then this process can not actually be carried out.

Order of Quantifiers

Examples:

1. Let $P(x,y)$ be the statement "$x + y = y + x$." Assume that U is the real numbers. Then $\forall x \forall y P(x,y)$ and $\forall y \forall x P(x,y)$ have the same truth value.
2. Let $Q(x,y)$ be the statement "$x + y = 0$." Assume that U is the real numbers. Then $\forall x \exists y P(x,y)$ is true, but $\exists y \forall x P(x,y)$ is false.

Questions on Order of Quantifiers

Example 1: Let U be the real numbers,
Define P(x,y) : $x \bullet y = 0$
What is the truth value of the following:

1. $\forall x \forall y P(x,y)$
   Answer: False
2. $\forall x \exists y P(x,y)$
   Answer: True
3. $\exists x \forall y\ P(x,y)$
   Answer: True
4. $\exists x\ \exists\ y\ P(x,y)$
   Answer: True

Questions on Order of Quantifiers

Example 2: Let U be the real numbers,
Define P(x,y) : $x / y = 1$
What is the truth value of the following:

1. $\forall x \forall y P(x,y)$
   Answer: False
2. $\forall x \exists y P(x,y)$
   Answer: True
3. $\exists x \forall y\ P(x,y)$
   Answer: False
4. $\exists x\ \exists\ y\ P(x,y)$
   Answer: True

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*

Translating Nested Quantifiers into English

Example 1: Translate the statement

$$\forall x\ (C(x) \vee \exists y\ (C(y) \wedge F(x, y)))$$

where C(x) is "x has a computer," and F(x,y) is "x and y are friends," and the domain for both x and y consists of all students in your school.

Solution: Every student in your school has a computer or has a friend who has a computer.

Translating Mathematical Statements into Predicate Logic

Example : Translate "The sum of two positive integers is always positive" into a logical expression.

Solution:

1. Rewrite the statement to make the implied quantifiers and domains explicit:

   "For every two integers, if these integers are both positive, then the sum of these integers is positive."

2. Introduce the variables x and y, and specify the domain, to obtain:

   "For all positive integers x and y, x +y is positive."

3. The result is:

$$\forall x \forall y ((x > 0) \wedge (y > 0) \rightarrow (x + y > 0))$$

where the domain of both variables consists of all integers

Translating English into Logical Expressions Example

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

Solution:

1. Let $P(w,f)$ be "w has taken f " and $Q(f,a)$ be "f is a flight on a ."
2. The domain of w is all women, the domain of f is all flights, and the domain of a is all airlines.
3. Then the statement can be expressed as:

$$\exists w \exists f \ \forall a \ (P(w,f) \text{ A } Q(f,a))$$

Questions on Translation from English

Choose the obvious predicates and express in predicate logic.

Example 1: "Brothers are siblings."

Solution: $\forall x \forall y\ (B(x,y) \rightarrow S(x,y))$

Example 2: "Siblinghood is symmetric."

Solution: $\forall x \forall y\ (S(x,y) \rightarrow S(y,x))$

Example 3: "Everybody loves somebody."

Solution: $\forall x \exists y\ L(x,y)$

Example 4: "There is someone who is loved by everyone."

Solution: $\exists y \forall x\ L(x,y)$

Example 5: "There is someone who loves someone."

Solution: $\exists x \exists y\ L(x,y)$

Example 6: "Everyone loves himself"

Solution: $\forall x\ L(x,x)$

Negating Nested Quantifiers

Example 1: Recall the logical expression developed three slides back:

$\exists w\ \forall a\ \exists f\ (P(w,f)\ A\ Q(f,a))$

Part 1: Use quantifiers to express the statement that "There does not exist a woman who has taken a flight on every airline in the world."

Solution: $\neg\exists w\ \forall a\ \exists f\ (P(w,f)\ A\ Q(f,a))$

Part 2: Now use De Morgan's Laws to move the negation as far inwards as possible.

Solution:

1. $\neg\exists w\ \forall a\ \exists f\ (P(w,f)\ A\ Q(f,a))$
2. $\forall w\ \neg\ \forall a\ \exists f\ (P(w,f)\ A\ Q(f,a))$ by De Morgan's for $\exists$
3. $\forall w\ \exists\ a\ \neg\ \exists f\ (P(w,f)\ A\ Q(f,a))$ by De Morgan's for $\forall$
4. $\forall w\ \exists\ a\ \forall f\ \neg\ (P(w,f)\ A\ Q(f,a))$ by De Morgan's for $\exists$
5. $\forall w\ \exists\ a\ \forall f\ (\neg\ P(w,f) \vee \neg\ Q(f,a))$ by De Morgan's for A.

Part 3: Can you translate the result back into English?

Solution:

"For every woman there is an airline such that for all flights, this woman has not taken that flight or that flight is not on this airline"

Some Questions about Quantifiers

- Can you switch the order of quantifiers?
  - Is this a valid equivalence? $\forall x \forall y P(x,y) \equiv \forall y \forall x P(x,y)$

Solution: Yes! The left and the right side will always have the same truth value. The order in which x and y are picked does not matter.

  - Is this a valid equivalence? $\forall x \exists y P(x,y) \equiv \exists y \forall x P(x,y)$

Solution: No! The left and the right side may have different truth values for some propositional functions for P. Try "x +y =0" for P(x,y) with U being the integers. The order in which the values of x and y are picked does matter.

- Can you distribute quantifiers over logical connectives?
  - Is this a valid equivalence? $\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$

Solution: Yes! The left and the right side will always have the same truth value no matter what propositional functions are denoted by P(x) and Q(x).

  - Is this a valid equivalence? $\forall x(P(x) \rightarrow Q(x)) \equiv \forall x P(x) \rightarrow \forall x Q(x)$

Solution: No! The left and the right side may have different truth values. Pick "x is a fish" for P(x) and "x has scales" for Q(x) with the domain of discourse being all animals. Then the left side is false, because there are some fish that do not have scales. But the right side is true since not all animals are fish.

Summary

- Valid Arguments and Rules of Inference
- Proof Methods
- Proof Strategies

The Foundations: Logic and Proofs

Chapter 1, Part III: Proofs

Proofs

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

Ingredients:

- hypotheses of the theorem
- axioms assumed to be true
- previously proven theorems
- rules of inference

You get:
truth of the statement being proved

Usefulness

Computer Science

Verifying that computer programs are correct.
Establishing that operating systems are secure.
Making inferences in artificial intelligence.
Showing that system specifications are consistent.

Mathematics

Defining Formalism.
Providing specification in a common language.
Justification for the results.

Definitions

Deriving Additional Results about Even and Odd Integers

Suppose that you have already proved the following properties of even and odd integers:

1. The sum, product, and difference of any two even integers are even.
2. The sum and difference of any two odd integers are even.
3. The product of any two odd integers is odd.
4. The product of any even integer and any odd integer is even.
5. The sum of any odd integer and any even integer is odd.
6. The difference of any odd integer minus any even integer is odd.
7. The difference of any even integer minus any odd integer is odd.

Definitions

1.An integer n is even if, and only if, $n = 2k$ for some integer k.

2. An integer n is odd if, and only if, $n = 2k + 1$ for some integer k.

3. An integer n is prime if, and only if, $n > 1$ and for all positive integers r and s, if $n = r \cdot s$, then $r = 1$ or $s = 1$.

4. An integer $n > 1$ is composite if, and only if, $n = r \cdot s$ for some positive
integers r and s with $r \neq 1$ and $s \neq 1$.

5. A real number r is rational if, and only if, $r = \frac{a}{b}$ for some integers a and b with $b \neq 0$.

6. If n and d are integers and $d \neq 0$, then d divides n, written $d|n$ if, and
only if, $n = d.k$ for some integers k.

7. An integer n is called a perfect square if, and only if, $n = k^2$ for some integer k.

Types of Proofs

Proving conditional Statements

- Direct Proofs
- Indirect Proofs
  - **Proof by Contraposition**
  - **Proofs by Contradiction**

Proving Non-conditional Statements

- Indirect Proofs
- If-And-Only-If Proof
- Constructive Versus Non-constructive Proofs
- Existence Proofs; Existence and Uniqueness Proofs
- Disproofs (Counterexample, Contradiction, Existence Statement)
- Proofs Involving Sets

Mathematical Induction

Direct Proofs

p →q

first step is the assumption that *p is true*
subsequent steps constructed using rules of inference.
final step showing that *q must also be true*

showing that if *p is true,*
then q must also be true,
so that the combination
p true and q false never occu

Outline for Direct Proof

Proposition If P, then Q.

Proof. Suppose P.

⋮

Therefore Q. ■

Activity Time

Prove that the sum of two odd integers is even.

Prove that the sum of two odd integers is even.

Let **m** and **n** be two odd integers. Then by definition of odd numbers

$m = 2k + 1$ for some $k \in Z$

$n = 2l + 1$ for some $l \in Z$

Now $m + n = (2k + 1) + (2l + 1)$

$= 2k + 2l + 2$

$= 2(k + l + 1)$

$= 2r$ where $r = (k + l + 1) \in Z$

Hence $m + n$ is even.

EXERCISE:

Prove that if n is any even integer, then $(-1)^n = 1$

SOLUTION:

Suppose n is an even integer. Then $n = 2k$ for some integer k.

Now

$$
\begin{aligned}
(-1)^n &= (-1)^{2k} \\
&= [(-1)^2]^k \\
&= (1)^k \\
&= 1 \qquad \text{(proved)}
\end{aligned}
$$

EXERCISE:

Prove that the product of an even integer and an odd integer is even.

SOLUTION:

Suppose m is an even integer and n is an odd integer. Then

$m = 2k$ for some integer k

and $n = 2l + 1$ for some integer l

Now

$$m \cdot n = 2k \cdot (2l + 1)$$
$$= 2 \cdot k\,(2l + 1)$$
$$= 2 \cdot r \quad \text{where } r = k(2l + 1) \text{ is an integer}$$

Hence $m \cdot n$ is even. (Proved)

EXERCISE:

Prove that the square of an even integer is even.

SOLUTION:

Suppose n is an even integer. Then $n = 2k$

Now

$$\begin{aligned} \text{square of } n = n^2 &= (2\cdot k)^2 \\ &= 4k^2 \\ &= 2\cdot(2k^2) \\ &= 2\cdot p \quad \text{where } p = 2k^2 \in Z \end{aligned}$$

Hence, n^2 is even. (proved)

proved that if *n is an odd integer, then* n^2 *is an odd integer*

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*.

Square both sides $n^2 = (2k + 1)^2$

$$4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Consequently, we have proved that if *n is an odd integer, then* n^2 *is an odd integer*

EXERCISE:

Prove that if n is an odd integer, then $n^3 + n$ is even.

SOLUTION:

Let n be an odd integer, then $n = 2k + 1$ for some $k \in Z$

Now $n^3 + n = n(n^2 + 1)$

$$= (2k + 1)((2k+1)^2 + 1)$$

$$= (2k + 1)(4k^2 + 4k + 1 + 1)$$

$$= (2k + 1)(4k^2 + 4k + 2)$$

$$= (2k + 1)\, 2.\, (2k^2 + 2k + 1)$$

$$= 2 \cdot (2k + 1)(2k^2 + 2k + 1) \qquad k \in Z$$

= an even integer

Proposition If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.

Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.

So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.

Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.

Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number.

EXERCISE:

Prove that, if the sum of any two integers is even, then so is their difference.

SOLUTION:

Suppose m and n are integers so that m + n is even. Then by definition of even numbers

$$m + n = 2k \qquad \text{for some integer } k$$

$$\Rightarrow \quad m = 2k - n \quad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Now $m - n = (2k - n) - n$ using (1)

$$= 2k - 2n$$

$$= 2(k - n) = 2r \qquad \text{where } r = k - n \text{ is an integer}$$

Hence m - n is even.

EXERCISE:

Prove that the sum of any two rational numbers is rational.

SOLUTION:

Suppose r and s are rational numbers.

Then by definition of rational

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d}$$

for some integers a, b, c, d with $b \neq 0$ and $d \neq 0$

Now

$$\begin{aligned} r + s &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad + bc}{bd} \\ &= \frac{p}{q} \end{aligned}$$

where $p = ad + bc \in Z$ and $q = bd \in Z$ and $q \neq 0$

Hence r + s is rational.

EXERCISE:

Given any two distinct rational numbers r and s with $r < s$. Prove that there is a rational number x such that $r < x < s$.

SOLUTION:

Given two distinct rational numbers r and s such that

$$r < s \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Adding r to both sides of (1), we get

$$r + r < r + s$$

$$2r < r + s$$

$$\Rightarrow \qquad r < \frac{r+s}{2} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Next adding s to both sides of (1), we get

$$r + s < s + s$$

$$\Rightarrow \qquad r + s < 2s$$

$$\Rightarrow \qquad \frac{r+s}{2} < s \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Combining (2) and (3), we may write

$$r < \frac{r+s}{2} < s \quad \text{.....(4)}$$

Since the sum of two rationals is rational, therefore $r + s$ is rational. Also the quotient of a rational by a non-zero rational, is rational, therefore $\frac{r+s}{2}$ is rational and by (4) it lies between r & s. Hence, we have found a rational number such that $r < x < s$. (proved)

EXERCISE:

Prove that the sum of any three consecutive integers is divisible by 3.

PROOF:

Let n, n + 1 and n + 2 be three consecutive integers.

Now

$$n + (n + 1) + (n + 2) = 3n + 3$$
$$= 3(n + 1)$$
$$= 3 \cdot k \quad \text{where } k = (n+1) \in Z$$

Hence, the sum of three consecutive integers is divisible by 3.

Activity Time

Give a direct proof that if *m and n are both perfect squares, then nm is also a perfect square.*

Proof

We assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares.

By the definition of a perfect square, It follows that there are integers s and t such that $m = s^2$ and $n = t^2$.

Multiplying both m and n to get s^2t^2.

Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication.

By the definition of perfect square, it follows that mn 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 mn is also a perfect square.

Activity Time

Give a direct proof that if *n is an integer and n is odd, then 3n + 2 is odd.*

Indirect Proofs

Direct proof begin with the premises, continue with a sequence of deductions, and end with the conclusion.
Attempts at direct proofs often reach dead ends
Proofs that **do not** start with the premises and end with the conclusion, are called **indirect proofs**

PROOF BY CONTRAPOSITION:

A proof by contraposition is based on the logical equivalence between a statement and its contrapositive. Therefore, the implication $p \rightarrow q$ can be proved by showing that its contrapositive $\sim q \rightarrow \sim p$ is true. The contrapositive is usually proved directly.

The method of proof by contrapositive may be summarized as:

1. Express the statement in the form if p then q.
2. Rewrite this statement in the contrapositive form
   if not q then not p.
3. Prove the contrapositive by a direct proof.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

$\vdots$

Therefore $\sim P$. ■

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

PROOF:

The contrapositive of the given conditional statement is

" if n is even then 3n + 2 is even"

Suppose n is even, then

$n = 2k$ for some $k \in Z$

Now $3n + 2 = 3(2k) + 2$

$= 2.(3k + 1)$

$= 2.r$ where $r = (3k + 1) \in Z$

Hence 3n + 2 is even. We conclude that the given statement is true since its contrapositive is true.

EXERCISE:

Prove that for all integers n, if n^2 is even then n is even.

PROOF:

The contrapositive of the given statement is:

"if n is not even (odd) then n^2 is not even (odd)"

We prove this contrapositive statement directly.

Suppose n is odd. Then $n = 2k + 1$ for some $k \in Z$

Now $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$= 2\cdot(2k^2 + 2k) + 1$

$= 2\cdot r + 1$ where $r = 2k^2 + 2k \in Z$

Hence n^2 is odd. Thus the contrapositive statement is true and so the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even.

PROOF:

Suppose n is an odd integer. Since, a product of two odd integers is odd, therefore $n^2 = n.n$ is odd; and $n^3 = n^2.n$ is odd.

Since a sum of two odd integers is even therefore $n^2 + 5$ is even.

Thus we have prove that if n is odd then $n^3 + 5$ is even.

Since this is the contrapositive of the given conditional statement, so the given statement is true.

EXERCISE:

Prove that if n^2 is not divisible by 25, then n is not divisible by 5.

SOLUTION:

The contra positive statement is:

"if n is divisible by 5, then n^2 is divisible by 25"

Suppose n is divisible by 5. Then by definition of divisibility

$$n = 5 \cdot k \qquad \text{for some integer } k$$

Squaring both sides

$$n^2 = 25 \cdot k^2 \qquad \text{where } k^2 \in Z$$

n^2 is divisible by 25

Proofs by Contradiction

A proof by contradiction is based on the fact that either a statement is true or it is false but not both. Hence the supposition, that the statement to be proved is false, leads logically to a contradiction, impossibility or absurdity, then the supposition must be false. Accordingly, the given statement must be true.

The method of proof by contradiction may be summarized as follows:

1. Suppose the statement to be proved is false.

2. Show that this supposition leads logically to a contradiction.

3. Conclude that the statement to be proved is true.

Basic Idea

Assume that the statement we want to prove is *false, and then show* that this assumption leads to nonsense!

We are then led to conclude that we were wrong to assume the statement was false, so the statement must be t

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

$\vdots$

Therefore $C \wedge \sim C$. ■

THEOREM:

There is no greatest integer.

PROOF:

Suppose there is a greatest integer N. Then $n \leq N$ for every integer n.

Let $M = N + 1$

Now M is an integer since it is a sum of integers.

Also $M > N$ since $M = N + 1$

Thus M is an integer that is greater than the greatest integer, which is a contradiction. Hence our supposition is not true and so there is no greatest integer.

EXERCISE:

Give a proof by contradiction for the statement:

"If n^2 is an even integer then n is an even integer."

PROOF:

Suppose n^2 is an even integer and n is not even, so that n is odd.

Hence $n = 2k + 1$ for some integer k.

Now
$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2\cdot(2k^2 + 2k) + 1 \\ &= 2r + 1 \qquad \text{where } r = (2k^2 + 2k) \in Z \end{aligned}$$

This shows that n^2 is odd, which is a contradiction to our supposition that n^2 is even. Hence the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using contradiction method.

SOLUTION:

Suppose that $n^3 + 5$ is odd and n is not even (odd). Since n is odd and the product of two odd numbers is odd, it follows that n^2 is odd and $n^3 = n^2 . n$ is odd. Further, since the difference of two odd numbers is even, it follows that

$$5 = (n^3 + 5) - n^3$$

is even. But this is a contradiction. Therefore, the supposition that $n^3 + 5$ and n are both odd is wrong and so the given statement is true.

THEOREM:

The sum of any rational number and any irrational number is irrational.

PROOF:

We suppose that the negation of the statement is true. That is, we suppose that there is a rational number r and an irrational number s such that r + s is rational. By definition of ration

$$r = \frac{a}{b} \quad \ldots\ldots\ldots\ldots\ldots(1) \qquad \text{and} \qquad r + s = \frac{c}{d} \quad \ldots\ldots\ldots\ldots\ldots(2)$$

for some integers a, b, c and d with $b \neq 0$ and $d \neq 0$.

Using (1) in (2), we get

$$\frac{a}{b} + s = \frac{c}{d}$$

$$\Rightarrow \qquad s = \frac{c}{d} - \frac{a}{b}$$

$$s = \frac{bc - ad}{bd} \qquad (bd \neq 0)$$

Now bc - ad and bd are both integers, since products and difference of integers are integers. Hence s is a quotient of two integers bc-ad and bd with $bd \neq 0$. So by definition of rational, s is rational.

This contradicts the supposition that s is irrational. Hence the supposition is false and the theorem is true.

EXERCISE:

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

PROOF:

Suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors so

$$\sqrt{2} = \frac{m}{n}$$

that

Squaring both sides gives

$$2 = \frac{m^2}{n^2}$$

Or $m^2 = 2n^2$ .....(1)

This implies that m^2 is even (by definition of even). It follows that m is even. Hence

$m = 2k$ for some integer k (2)

Substituting (2) in (1), we get

$$(2k)^2 = 2n^2$$

$$\Rightarrow \quad 4k^2 = 2n^2$$

$$\Rightarrow \quad n^2 = 2k^2$$

This implies that n^2 is even, and so n is even. But we also know that m is even. Hence both m and n have a common factor 2. But this contradicts the supposition that m and n have no common factors. Hence our supposition is false and so the theorem is true.

PROOF BY COUNTER EXAMPLE

Disprove the statement by giving a counter example.
For all real numbers a and b, if $a < b$ then $a^2 < b^2$.

SOLUTION:

Suppose $a = -5$ and $b = -2$
then clearly $-5 < -2$

But $a^2 = (-5)^2 = 25$ and $b^2 = (-2)^2 = 4$

But $25 > 4$

This disproves the given statement.

EXERCISE:

Prove or give counter example to disprove the statement.

For all integers n, $n^2 - n + 11$ is a prime number.

SOLUTION:

The statement is not true

For n = 11

we have , $n^2 - n + 11 = (11)^2 - 11 + 11$

$= (11)^2$

$= (11)(11)$

$= 121$

which is obviously not a prime number.

Chapter 5

Mathematical Induction

Conjecture: The sum of the first n odd natural numbers equals n^2.

n	sum of the first n odd natural numbers	n^2
1	$1 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	1
2	$1+3 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	4
3	$1+3+5 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	9
4	$1+3+5+7 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	16
5	$1+3+5+7+9 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	25
$\vdots$	$\vdots$	$\vdots$
n	$1+3+5+7+9+11+\cdots+(2n-1) = \ldots\ldots\ldots$	n^2
$\vdots$	$\vdots$	$\vdots$

An infinite ladder

Suppose that we have an infinite ladder, and we want to know whether we can reach every step on this ladder.

We know two things:

1. We can reach the first rung of the ladder.
2. If we can reach a particular rung of the ladder, then we can reach the next rung.

FIGURE 1 **Climbing an Infinite Ladder.**

Mathematical Induction

Mathematical statements assert that a property is true for all positive integers.

Proofs using mathematical induction have two parts.

- First, they show that the statement holds for the positive integer 1 (base case).
- Second, they show that if the statement holds for a positive integer then it must also hold for the next larger integer. (inductive case)

The method can be extended to prove statements about more general well-founded structures, such as trees; this generalization, known as structural induction, is used in mathematical logic and computer science.

NOTE

It is extremely important to note that mathematical induction can be used only to prove results obtained in some other way.

It is *not a tool for discovering formulae or* theorems.

Mathematicians sometimes find proofs by mathematical induction unsatisfying because they do not provide insights as to why theorems are true.

You can prove a theorem by mathematical induction even if you do not have the slightest idea why it is true!

FIGURE 2 Illustrating How Mathematical Induction Works Using Dominoes.

The Simple Idea Behind Mathematical Induction

Statements are lined up like dominoes.

(1) Suppose the first statement falls (i.e. is proved true);

(2) Suppose the kth falling always causes the $(k+1)^{th}$ to fall;

Then all must fall (i.e. all statements are proved true).

PRINCIPLE OF MATHEMATICAL INDUCTION:

Let P(n) be a propositional function defined for all positive integers n. P(n) is true for every positive integer n if

1.Basis Step:

The proposition P(1) is true.

2.Inductive Step:

If P(k) is true then P(k + 1) is true for all integers $k \geq 1$.

i.e. $\forall k \quad p(k) \rightarrow P(k+1)$

EXAMPLE:

Use Mathematical Induction to prove that

$$1+2+3+\cdots+n=\frac{n(n+1)}{2} \quad \text{for all integers } n \geq 1$$

SOLUTION:

Let $$P(n): 1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

1.Basis Step:

P(1) is true.

For n = 1, left hand side of P(1) is the sum of all the successive integers starting at 1 and ending at 1, so LHS = 1 and RHS is

$$R.H.S=\frac{1(1+1)}{2}=\frac{2}{2}=1$$

so the proposition is true for n = 1.

2. Inductive Step: Suppose P(k) is true for, some integers $k \geq 1$.

(1) $$1+2+3+\cdots+k=\frac{k(k+1)}{2}$$

To prove P(k + 1) is true. That is,

$$(2) \qquad 1+2+3+\cdots+(k+1)=\frac{(k+1)(k+2)}{2}$$

Consider L.H.S. of (2)

$$\begin{aligned}
1+2+3+\cdots+(k+1) &= 1+2+3+\cdots+k+(k+1) \\
&= \frac{k(k+1)}{2}+(k+1) \qquad \text{using (1)} \\
&= (k+1)\left[\frac{k}{2}+1\right] \\
&= (k+1)\left[\frac{k+2}{2}\right] \\
&= \frac{(k+1)(k+2)}{2} = \text{RHS of (2)}
\end{aligned}$$

Hence by principle of Mathematical Induction the given result true for all integers greater or equal to 1.

EXERCISE:

Use mathematical induction to prove that
$1+3+5+\ldots+(2n-1) = n^2$ for all integers $n \geq 1$.

SOLUTION:

Let P(n) be the equation $1+3+5+\ldots+(2n-1) = n^2$

1. **Basis Step:**

   P(1) is true
   For n = 1, L.H.S of P(1) = 1and
   R.H.S = $1^2 = 1$
   Hence the equation is true for n = 1

2. **Inductive Step:**

   Suppose P(k) is true for some integer $k \geq 1$. That is,
   $1 + 3 + 5 + \ldots + (2k - 1) = k^2$ .....(1)

To prove P(k+1) is true; i.e.,
$1 + 3 + 5 + \ldots + [2(k+1)-1] = (k+1)^2$ .....(2)

Consider L.H.S. of (2)

$$\begin{aligned}
1+3+5+\cdots+[2(k+1)-1] &= 1+3+5+\cdots+(2k+1) \\
&= 1+3+5+\cdots+(2k-1)+(2k+1) \\
&= k^2+(2k+1) \qquad \text{using (1)} \\
&= (k+1)^2 \\
&= \text{R.H.S. of (2)}
\end{aligned}$$

Thus P(k+1) is also true. Hence by mathematical induction, the given equation is true for all integers $n \geq 1$.

Exercise (cont.)

Proof.

1. $P(n)$: $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$
2. Basis step $P(0)$: $2^0 = 1 = 2^{0+1} - 1$.
3. Inductive step:
   Inductive hypothesis $P(k)$: $2^0 + 2^1 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$
   Let's prove $P(k+1)$:

$$\begin{aligned} 2^0 + 2^1 + 2^2 + \cdots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} && \text{(by IH)} \\ &= 2(2^{k+1}) - 1 && \text{(by arithmetic)} \\ &= 2^{k+2} - 1 && \text{(by arithmetic)} \end{aligned}$$