

Discrete Mathematics

Propositional & Predicate Logic

Lecture Notes

By

I. PAVAN KUMAR | Assistant Professor

| Dept.of Information Technology | Mobile: 8886307052

| VNR Vignana Jyothi Institute of Engineering & Technology

**“LOGIC IS THE BEGINNING OF WISDOM, NOT THE
END.”**

LEONARD NIMOY

QuotesIdeas.com

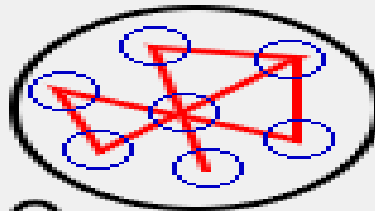
Discrete Mathematics in the Real World

Secure knowledge of number facts and applied appropriately

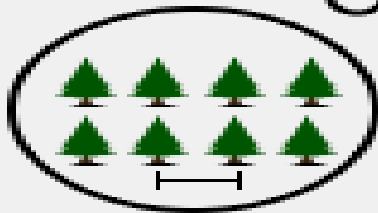
1,1,2,3,5,8

1,4,9,16,25

Apply appropriate mathematical concepts and techniques



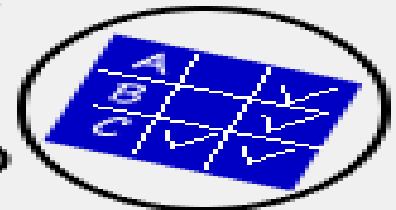
To analyse and solve problem in real life application



Analyse information and generate rules to solve problems

$$\begin{aligned} 2x+y &= 10 \\ y-x &= 3 \\ x=? \quad y=? \end{aligned}$$

Use mathematical reasoning in solving problems



What is Discrete Mathematics?

- Discrete mathematics is the part of mathematics devoted to the study of **discrete** (as opposed to continuous) **objects**.
- Calculus deals with continuous objects and is not part of discrete mathematics.
- Examples of discrete objects: **integers**, **distinct paths** to travel from point A to point B on a map along a road network, **ways** to pick a winning set of numbers in a lottery.
- A course in discrete mathematics **provides the mathematical background needed for all subsequent courses in computer science**.

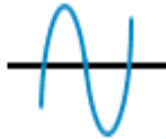
Discrete Math

The topics included in the study of discrete math

Set Theory

$\{2,4,6,8\}$

Graph Theory



Logic

AND, OR &
NOT

Permutation

$\{a,b\}$ is
 $(a,b), (b,a)$

Combination

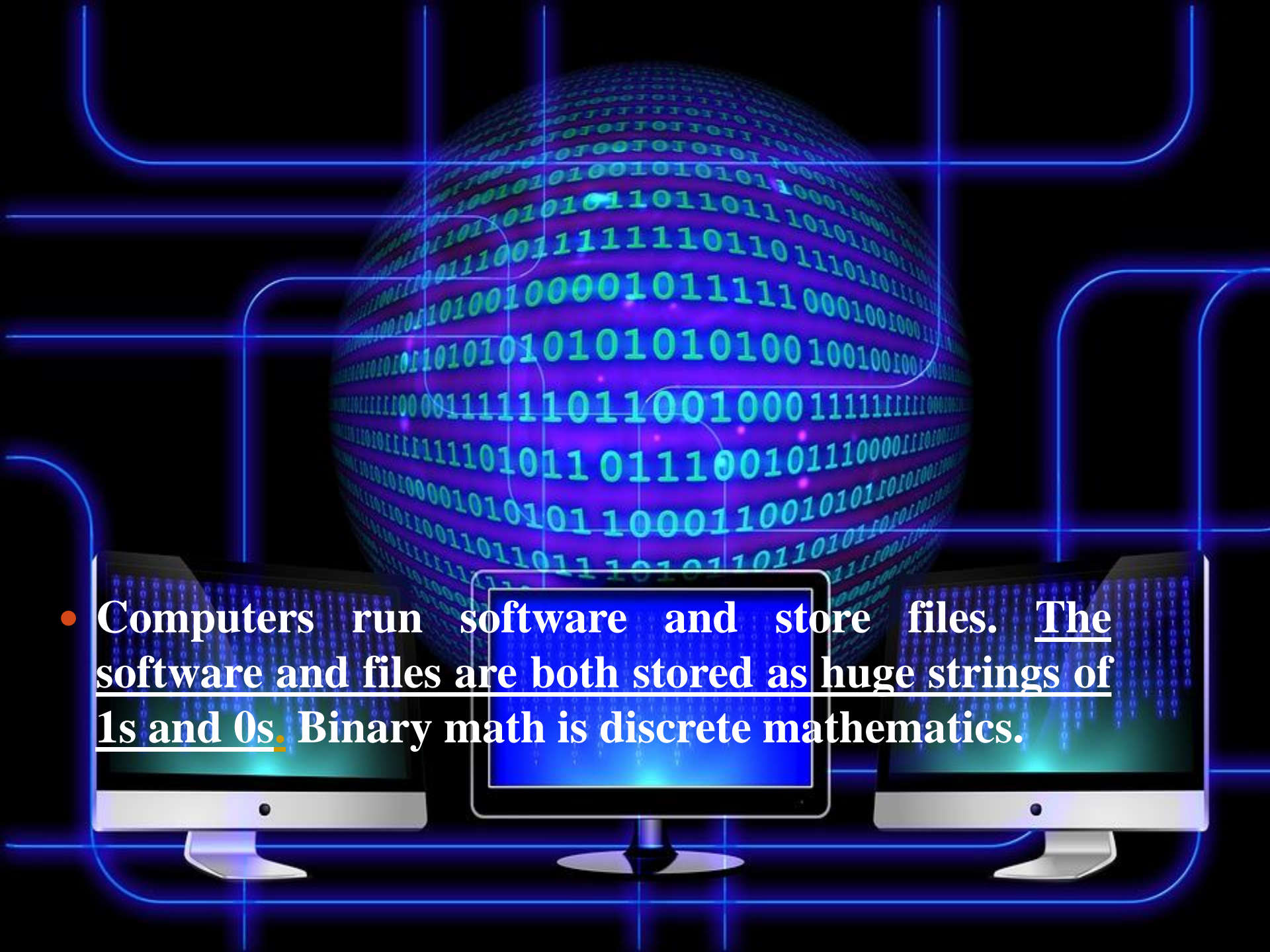
$${}^n C_r = \frac{n}{r! (n-r)!}$$

Sequence

$N = \{1, 2, 3, \dots\}$

Series

$s_1 + s_2 + s_3 + s_4 \dots$
is the sum of
the series.

- 
- Computers run software and store files. The software and files are both stored as huge strings of 1s and 0s. Binary math is discrete mathematics.

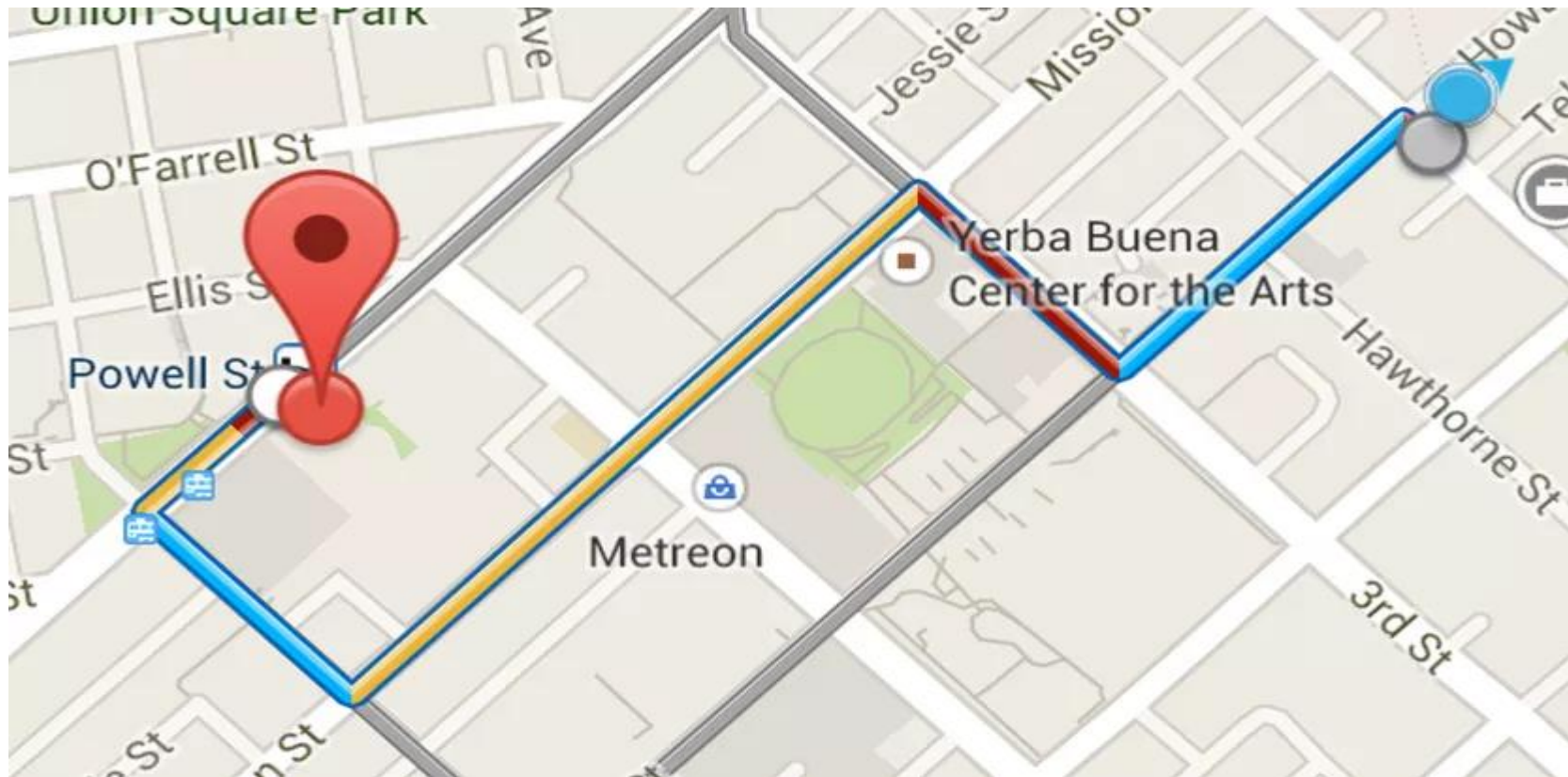
- Encryption and decryption are part of cryptography, which is part of discrete mathematics. For example, secure internet shopping uses public-key cryptography.



- An analog clock has gears inside, and the sizes/teeth needed for correct timekeeping are determined using discrete math.



- **Google Maps** uses discrete mathematics to determine fastest driving routes and times.



- Railway planning uses discrete math: deciding how to expand train rail lines, train timetable scheduling, and scheduling crews and equipment for train trips use both graph theory and linear algebra.



- Computer graphics (such as in video games) use linear algebra in order to transform (move, scale, change perspective) objects. That's true for both applications like game development, and for operating systems.



- Cell phone communications: Making efficient use of the broadcast spectrum for mobile phones uses linear algebra and information theory. Assigning frequencies so that there is no interference with nearby phones can use graph theory or can use discrete optimization.



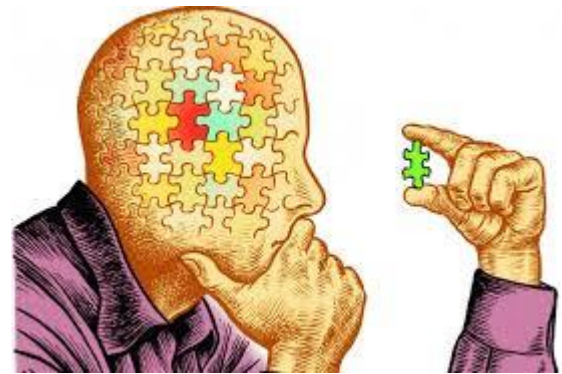
- Graph theory and linear algebra can be used in speeding up Facebook performance.



- Graph theory is used in DNA sequencing.



**How does learning discrete mathematics
make you a better programmer?**



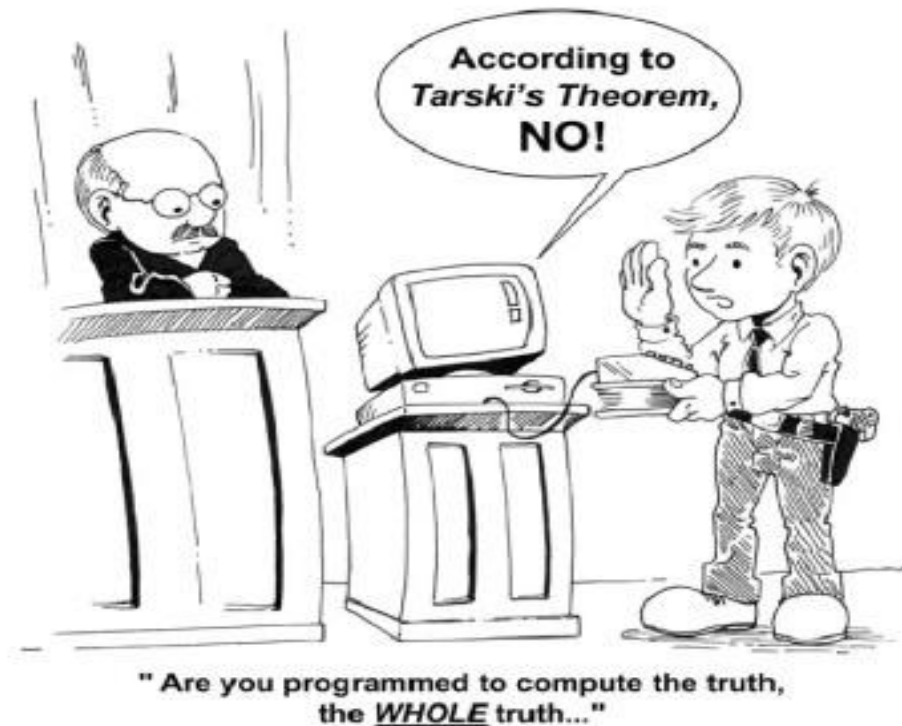
- One of the most important competences – probably even the single most important competence – that one must have as a program developer is to be able to choose the right algorithms and data structures for the problem that the program is supposed to solve.
- The importance of discrete mathematics lies in its central role in the analysis of algorithms and in the fact that many common data structures – and in particular graphs, trees, sets and ordered sets – and their associated algorithms come from the realm of discrete mathematics.

- Why proofs? The analysis of an algorithm requires one to carry out (or at the very least be able to sketch) a proof of the correctness of the algorithm and a proof of its complexity



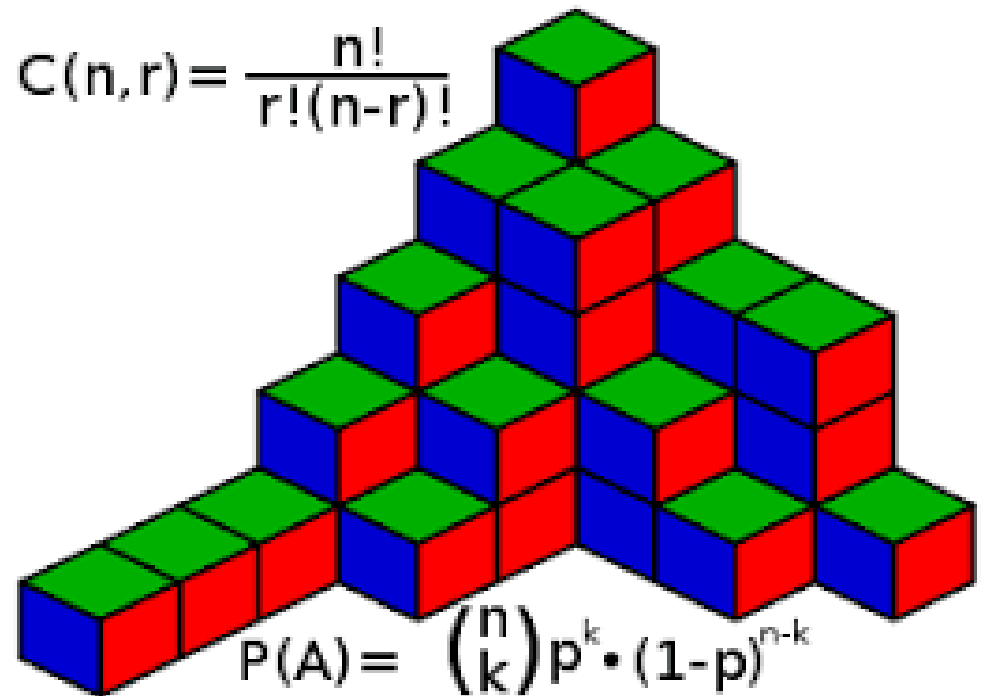
Logic and Proofs:

- Programmers use logic. All the time. While everyone has to think about the solution, a formal study of logical thinking helps you organize your thought process more efficiently.



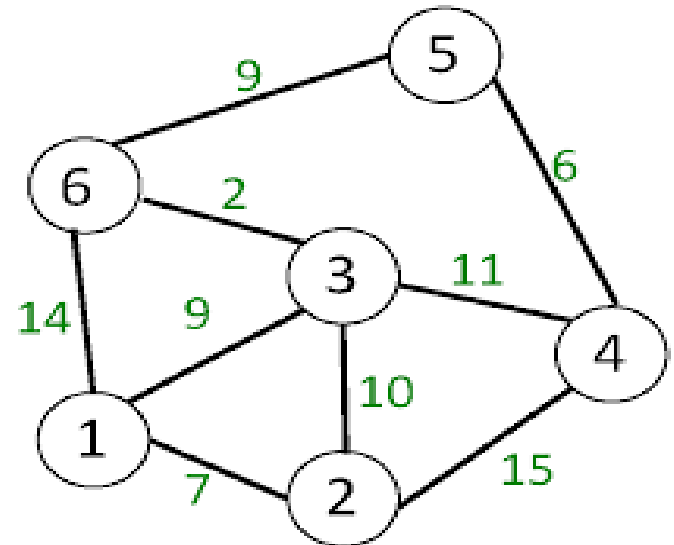
Combinatorics:

- One cannot program without loops or recursion. (I mean we could, but it wouldn't be very useful) Getting a sense of the Mathematics behind these very essential programming concepts help you *optimise your code*.



Graphs:

- One cannot overestimate the importance of graphs in CS today, what with the emergence of social networks and the need to represent all types of complex relationships between entities. Learning Graphs can help you visualise a lot of data structures better. Also, there is a lot of room for better programming in graphs. Having mathematical knowledge about them is essential to do that



- **Is discrete mathematics important for Google Java software engineering interview preparation?**

YES

Discrete Mathematics is important for any Software Engineering interview. One cannot call him/herself a software engineer without having a solid basic knowledge of discrete mathematics.

Moral of the Story???

- Discrete Math is needed to see mathematical structures in the object you work with, and understand their properties. This ability is important for software engineers, data scientists, security and financial analysts.
- **it is not a coincidence that math puzzles are often used for interviews.**

Problems Solved Using Discrete Mathematics

1. **The foundations: Logic and Proofs**

- How can we represent English sentences so that a computer can deal with them?

2. Basic Structures: Sets, Functions, Sequences, Sums, and Matrices

- How can we describe the relationship between different set?

3. **Algorithms**

- How can a list of integers be sorted so that the integers are in increasing order?

4. Number Theory and Cryptography

- How can we represent the even integer and odd integer?

Problems Solved Using Discrete Mathematics

5. Introduction and Recursion

- How can we prove that there are infinitely many prime numbers?
- How can it be proved that a sorting algorithm always correctly sorts a list?

6. Counting

- How many valid Internet addresses are there?
- How many ways can a password be chosen following specific rules?

7. **Discrete Probability**

- What is the probability of winning a particular lottery?

8. Advanced Counting Techniques

- How can I encrypt a message so that no unintended recipient can read it?

Problems Solved Using Discrete Mathematics

9. Relations

- How can we deal with the relationships between elements of sets

10. Graphs

- Find the shortest tour that visits each of a group of cities only once and then ends in the starting city.

11. Trees

- Binary search tree
- Huffman coding

12. Boolean Algebra

- The circuits in computers and other electronic devices have inputs, each of which is either a 0 or a 1

13. Modeling Computation

- Can a task be carried out using a computer? How can the task be carried out?

Goals

- **Mathematical Reasoning:**
 - Ability to read, understand, and construct mathematical arguments and proofs.
- **Combinatorial Analysis:**
 - Techniques for counting objects of different kinds.
- **Discrete Structures:**
 - Abstract mathematical structures that represent objects and the relationships between them.
 - Examples are sets, permutations, relations, graphs, trees, and finite state machines.

Goals

- **Algorithmic Thinking:**

- One way to solve many problems is to specify an algorithm.
- An algorithm is a sequence of steps that can be followed to solve any instance of a particular problem.
- Algorithmic thinking involves specifying algorithms, analyzing the memory and time required by an execution of the algorithm, and verifying that the algorithm will produce the correct answer.

- **Applications and Modeling:**

- It is important to appreciate and understand the wide range of applications of the topics in discrete mathematics and develop the ability to develop new models in various domains.

Discrete Mathematics is a Gateway Course

- Topics in discrete mathematics will be important in many courses that you will take in the future:
 - **Computer Science:** Computer Architecture, Data Structures, Algorithms, Programming Languages, Compilers, Computer Security, Databases, Artificial Intelligence, Networking, Graphics, Game Design, Theory of Computation, Game Theory, Network Optimization
 - **Other Disciplines:** You may find concepts learned here useful in courses in philosophy, economics, linguistics, and other departments.

Thank you!



Any Questions?



Mathematical Logic

Logic is the Science dealing with the Methods of Reasoning.

Reasoning plays a very important role in every area of knowledge

A symbolic Language has been developed over past two centuries to express the principles of logic in precise & unambiguous manner.

Logic expressed in such a language has come to be called “symbolic language” or Mathematical Logic”.

Some basic notions of Mathematical Logic are Introduced in subsequent slides.

Many proofs in Mathematics and many algorithms in Computer Science use logical expression such as...

if P then Q

or

if P1 and P2, then Q1 or Q2

It is therefore, Necessary to know the cases in which these expressions are either **True** or **False**

We refer them as Truth value of the that expression

We use different types of sentences to express our ideas.. Such as


- Declarative
- Interrogative
- Exclamatory
- Imperative
- But in Mathematics we use the sentences which are declarative and possible to judge, weather they are true or false to draw the conclusion and/or to prove theorems.
- Such sentences are **Statements**
- The value associated with truthfulness or falsity of statement is called its **truth value**.

Statements & Notations

Consider the Following Sentences

- 1) New Delhi is in India.
- 2) Three is a Prime Number.
- 3) Seven is divisible by 3.
- 4) Every Rectangle is a square.

Each of the above is a Declarative Sentence which can be decisively said to be either **True** or **False but not both.**



Definition: A Proposition(Statement): It is a well defined argument, which is either **True** or **False, But not both**. The truth or falsity of a statement is called its truth value.

- Example 1: Tirupathi is in Andhra Pradesh
- Example 2: $8+3=11$
- Example 3: Close the door.
- Example 4: Where are you going?
- Example 5: Put the home work on the Table.

Examples 1 and 2 are Statements or Propositions.

3, 4 and 5 are not statements since neither true nor false.

More Examples

- “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

- “ $y > 5$ ”

Is this a statement? **yes**

Is this a proposition? **no**

Its truth value depends on the value of y , but this value is not specified.

We call this type of statement a propositional function or open sentence.

- “Today is January 1 and $99 < 5$.”

Is this a statement?

yes

Is this a proposition?

yes

What is the truth value
of the proposition?

false

- “Please do not fall asleep.”

Is this a statement? **no**

It’s a request.

Is this a proposition? **no**

Only statements can be propositions.

- “If elephants were red, they could hide in cherry trees.”

Is this a statement?

yes

Is this a proposition?

yes

**What is the truth value
of the proposition?**

probably false

- “ $x < y$ if and only if $y > x$.”

Is this a statement? **yes**

Is this a proposition? **yes**

... because its truth value does not depend on specific values of x and y .

What is the truth value of the proposition? **true**

Primitive statement.

- Any statement which do not contain any of the connectives is called **Simple** statement or **atomic statement** or **primary** or **Primitive statement**.

Compound Statement

- A statement Which contain one or more simple statements and some connectives is called compound or composite or molecular statement.
- Example: Five is a Prime number and 6 is divisible by 2.

- In general we denote statements by P,Q,R...
- Simple Statements are connected by certain symbols called **Connectives**.

Connectives

- There are Five basic logical connectives which are used frequently.

S.No	Symbol	Name	Connective word
1	\neg or \sim	Negation	Not
2	\wedge	Conjunction	and
3	\vee	Disjunction	or
4	\rightarrow	Implication or Conditional	Implies or If.... Then.....
5	\rightarrow \leftarrow or \leftrightarrow	Bi-conditional or Equivalence	If and only if

Negation (NOT)

- Unary Operator, Symbol: \neg

P	$\neg P$
true (T)	false (F)
false (F)	true (T)

Example

- Let the Proposition “3 is a Prime number” be denoted by P; that is

P: 3 is a Prime number

- Then the Negation of P is “3 is not a Prime number” that is

\neg P: 3 is not a Prime number

Conjunction (AND)

- Binary Operator, Symbol: \wedge

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

Examples

- Let us consider the following Propositions

P: $\sqrt{2}$ is an irrational number.

Q: 9 is a Prime number.

R: All triangles are equilateral.

S: $2+5=7$.

Here P and S are True Propositions

Q and R are False Propositions

$P \wedge Q$ is False

$Q \wedge R$ is False

$R \wedge S$ is False

$S \wedge P$ is True

Disjunction (OR)

- Binary Operator, Symbol: \vee

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

Examples

- Let us consider the following Propositions

P: $\sqrt{2}$ is an irrational number.

Q: 9 is a Prime number.

R: All triangles are equilateral.

S: $2+5=7$.

Here P and S are True Propositions

Q and R are False Propositions

$P \vee Q$ is True

$Q \vee R$ is False

$R \vee S$ is True

$S \vee P$ is True

Exclusive Or (XOR)

- Binary Operator, Symbol: \oplus
 - $P \oplus Q$ is same as $P \nabla Q$

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

Implication or Conditional

- Given Two Propositions P and Q, We can form the conditionals “ if P then Q” and if Q then P”
- If P then Q is denoted by $P \rightarrow Q$
- If Q then P is denoted by $Q \rightarrow P$

Note: $Q \rightarrow P$ is not same as $P \rightarrow Q$

The Following rule is adopted in deciding the truth value of the conditional.

The Conditional $P \rightarrow Q$ is false only when P is true and Q is false; in all other cases it is true

Implication (if - then)

- Binary Operator, Symbol: \rightarrow

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

Here the statement P is called Antecedent and Q is called Consequent in $P \rightarrow Q$. other representations of $P \rightarrow Q$ are

- Q is necessary for P
- P is sufficient for Q
- Q if P
- P only if Q
- P implies Q

Illustration

- Let us consider the following Propositions

P: 2 is a Prime number. (True proposition)

Q: 3 is a Prime number. (True proposition)

R: 6 is a Perfect square. (False proposition)

S: 9 is a multiple of 6. (False proposition)

Here

$P \rightarrow Q$: If 2 is a Prime number, then 3 is a Prime number.

$P \rightarrow R$: If 2 is a Prime number, then 6 is a Perfect square.

$R \rightarrow P$: If 6 is a Perfect square, then 2 is a Prime Number.

$R \rightarrow S$: If 6 is a Perfect square, then 9 is a multiple of 6.

From truth table we can infer that $P \rightarrow Q$ is true

$P \rightarrow R$ is false

$R \rightarrow P$ is true

$R \rightarrow S$ is true

Example 1:

- If I get the book then I begin to read

Symbolic form is $P \rightarrow Q$

here P: I get the book

Q: I began to read

Example 2:

- Express in English the statement $P \rightarrow Q$ where

P: The sun rises in the east.

Q: $4+3=7$.

Solution: if the sun rises in the east then $4+3=7$

Example 3

- Write the following statement in symbolic form.

Statement: if either John prefers tea or Jim prefers coffee, then Rita prefers milk.

Solution: P: John prefers tea

Q: Jim prefers Coffee

R: Rita Prefers milk

Symbolic form is $(P \vee Q) \rightarrow R$

Biconditional

- Let P and Q be two propositions. Then the conjunction of the conditionals $P \rightarrow Q$ and $Q \rightarrow P$ is called the biconditional of P and Q . It is denoted by $P \leftrightarrow Q$.
- Thus, $P \leftrightarrow Q$ is same as $(P \rightarrow Q) \wedge (Q \rightarrow P)$.
- $P \leftrightarrow Q$ is read as 'if P then Q and if Q then P '.

The Following rule is adopted in deciding the truth value of the conditional

$P \leftrightarrow Q$ is true only when both P and Q have the same truth values.

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

$P \leftrightarrow Q$ may be read as

- P if and only if Q
- P is equivalent to Q
- P is necessary and sufficient condition for Q
- Q is necessary and sufficient condition for P

Illustration

- Let us consider the following Propositions

P: 2 is a Prime number. (True proposition)

Q: 3 is a Prime number. (True proposition)

R: 6 is a Perfect square. (False proposition)

S: 9 is a multiple Of 6. (False proposition)

From truth table we can infer that

$P \leftrightarrow Q$ is true

$P \leftrightarrow R$ is false

$P \leftrightarrow S$ is false

$Q \leftrightarrow R$ is false

$Q \leftrightarrow S$ is false

$R \leftrightarrow S$ is true

Example 1

- $P: 8 > 4$
- $Q: 8 - 4$ is positive
- $P \leftrightarrow Q: 8 > 4$ if and only if $8 - 4$ is positive

Example 2

- Write the following statement in symbolic form

Statement: If ABC isosceles, then it is not equilateral, and if ABC is not equilateral ,then it is isosceles.

Solution: P: ABC is isosceles.

Q: ABC is Equilateral

If ABC isosceles, then it is not equilateral can be represented as

$$P \rightarrow \neg Q$$

if ABC is not equilateral ,then it is isosceles can be represented as

$$\neg Q \rightarrow P$$

Whole statement: $(P \rightarrow \neg Q) \wedge (\neg Q \rightarrow P)$ which is equivalent to $P \leftrightarrow (\neg Q)$

Well-formed formulas(Wff)

- While representing a Proposition involving connectives in a symbolic form, care has to be taken to ensure that the symbolic representation conveys the **intended meaning of the statement without any ambiguity**.
- Appropriate parenthesis(brackets) are to be used at appropriate places to achieve this objective.

Example

Negation of the conjunction of the propositions P and Q must be symbolically represented as follows.

$$\neg(P \wedge Q) \text{ not as } \neg P \wedge Q$$

Because $\neg P \wedge Q$ can also be interpreted as conjunction of $\neg P$ and Q which is not the intended proposition

here $\neg(P \wedge Q)$ is Wff.

Example 2

How to represent the conditional “if P and Q, then R”

$$(P \wedge Q) \rightarrow R$$

not as $P \wedge Q \rightarrow R$

Because There is a possibility of interpreting it as the conjunction of P and $Q \rightarrow R$

Hence $(P \wedge Q) \rightarrow R$ is Wff .

- Finally, Statements represented in symbolic forms which cannot be interpreted in more than one way are called Well-formed formulas in the context of mathematical logic.

The well-formed formulas of propositional logic are obtained by using the construction rules below:

- An atomic proposition P is a well-formed formula.
- If P is a well-formed formula, then so is $\neg P$.
- If P and Q are well-formed formulas, then so are $P \wedge Q$, $P \vee Q$, $P \rightarrow Q$, and $P \leftrightarrow Q$.
- If P is a well-formed formula, then so is (P) .

Propositional Logic Exercise

Example 1:

Express the following Statements in symbolic forms

1. If Ravi does not visit a friend this evening, then he studies this evening.
2. If there is a cricket telecast this evening, then Ravi does not study and does not visit a friend this evening.
3. If there is no cricket telecast this evening, then Ravi does not study but visits a friend this evening.
4. If there is no cricket telecast this evening, then Ravi does not study and does not visit a friend this evening.

Example 2:

Express the following Compound propositions in words

Let P: A circle is a conic.

Q: $\sqrt{5}$ is a real number

R: Exponential series is convergent

- a) $P \wedge (\neg Q)$ b) $(\neg P) \vee Q$ c) $Q \rightarrow (\neg P)$ d) $(\neg P) \leftrightarrow Q$

Example 3:

Let P and Q be Primitive statements for which the implication $P \rightarrow Q$ is false. Determine truth values of following:

- a) $P \wedge Q$ b) $(\neg P) \vee Q$ c) $Q \rightarrow P$ d) $(\neg Q) \rightarrow (\neg P)$

Example 4:

Let P, Q and R are be propositions having truth values 0,0 and 1 respectively. Find the truth values of the following.

- a) $(P \vee Q) \vee R$ b) $(P \wedge Q) \wedge R$ c) $(P \wedge Q) \rightarrow R$ d) $P \rightarrow (Q \wedge R)$
e) $P \rightarrow (Q \wedge R)$ f) $P \wedge (R \rightarrow Q)$ g) $P \rightarrow (Q \rightarrow (\neg R))$

Example 5:

Find the truth values of P, Q and R in the following cases.

- a) $P \rightarrow (Q \vee R)$ is false.
b) $P \wedge (Q \rightarrow R)$ is true

Example 6:

State weather the following are well-formed formulas or not.

- a) $P \wedge \neg Q$
b) $P \rightarrow (Q \vee R)$
c) $(P \rightarrow Q) \rightarrow \neg R$
d) $\neg P \rightarrow Q \rightarrow \neg R$
e) $P \leftrightarrow Q \wedge R$

Example 7:

Consider the following statement:

“It is not the case that houses are cold or haunted and it is false that cottages are warm or houses ugly”.

For what truth values will the above statement be true?

Example 8:

Write the symbolic statement of “ if Rita and Sita go to I.T camp and Jim and jhon go to P.C camp then college gets the good name.

Example 9

Construct the truth table for following Compound Proposition

a) $(P \vee Q) \wedge R$

b) $P \vee (Q \wedge R)$

c) $(P \wedge Q) \rightarrow (\neg R)$

d) $Q \wedge ((\neg R) \rightarrow P)$

Equivalence of Formulas

- Two Formulas A and B are said to be Equivalent to each other if and only if $A \leftrightarrow B$ is a Tautology.
- Represented by $A \iff B$
- \iff is a symbol not connective.
- \equiv also used to represent equivalence.

Example

Show that

$$\neg(P \leftrightarrow Q) \iff (P \wedge \neg Q) \vee (\neg P \wedge Q)$$

We can solve by constructing Truth table.

- How to solve without Constructing Truth tables???

By using Substitution instances

- A formula A is called a substitution instance of another formula B , if A can be obtained from B by substituting formulae for some variable in B , with one condition that the same formulae is substituted for the same variable each time it occurs.

- B: $P \rightarrow (E \wedge P)$
- Substitute $R \leftrightarrow S$ for P in B
- A: $(R \leftrightarrow S) \rightarrow (E \wedge (R \leftrightarrow S))$
- Then A is substitution instance of B.
- C: $(R \leftrightarrow S) \rightarrow (E \wedge P)$ is not a substitution instance of B because the variable P in $E \wedge P$ was not replaced by $R \leftrightarrow S$

Tautological Implications

For any Statement formula $P \rightarrow Q$

- The statement formula $Q \rightarrow P$ is called its Converse.
- The statement formula $\neg P \rightarrow \neg Q$ is called its inverse.
- $\neg Q \rightarrow \neg P$ is its Contra-Positive.

- A statement A is said to be tautologically imply to a statement B, if and only if $A \rightarrow B$ is a tautology.

Normal Forms

- The Problem of determining whether a given statement formula is tautology or a contradiction or satisfiable in a finite number of steps is known as a decision problem.
- If the statement formula has a truth value T for at least one combination of truth values assigned to its individual components, then that formula is said to be satisfiable.

- Generally we solve a given statement formula by construction truth table for n Atomic variables.
- If n is small, truth table will be small
- What if n is bigger??
- Construction of truth tables may not be practical if n is bigger.
- We therefor consider other procedures known as Reduction to normal forms.

Disjunctive Normal Form

- a logical formula is said to be in disjunctive normal form if it is a disjunction of conjunctions with every variable and its negation is present once in each conjunction.
- All disjunctive normal forms are non-unique, as all disjunctive normal forms for the same proposition are mutually equivalent.
- Disjunctive normal form is widely used in areas such as automated theorem proving.

Conjunctive Normal Form

- In conjunctive normal form, statements in logic formula are conjunctions of clauses with clauses of disjunctions. In other words, a statement is a series of ORs connected by ANDs.

Rules of Inference for Propositional Logic: Modus Ponens

$$\frac{p \rightarrow q \quad p}{\therefore q}$$

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 Tollens

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

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

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.”

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

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

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.”

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.”

Conjunction

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

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.

$$\frac{\neg p \vee r \quad p \vee q}{\therefore q \vee r}$$

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 study English literature.”

Test whether the following is a valid argument

if Sachin hits a century, then he gets a free car

Sachin hits a century

∴ Sachin gets a free car

if sachin hits a century,then he gets a free car
Saching does not get a free car.

∴ Sachin has not hit a century

if sachin hits a century,then he gets a free car
sachin gets a free car.

∴ sachin has hit a century

If I drive to work, then I will arrive tired.

I am not tired.

∴ I do not drive at work

I will become famous or I will not become musician
I will become a musician

•• I will become famous

If I Study, then I do not fail in the examonation

If I do not fail in the examination, my father gifts a two-wheeler to me.

• If I study, then my father gifts a two-wheeler to me
•

If I study, I will not fail in the examination.

If I do not watch TV in the evenings, I will study.

I failed in the examination.

∴ I must have watched TV in the evenings

Valid Arguments

Example 1: From the single proposition

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

Show that q is a conclusion.

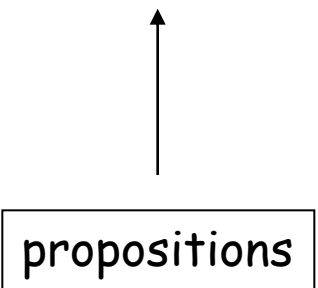
Solution:

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

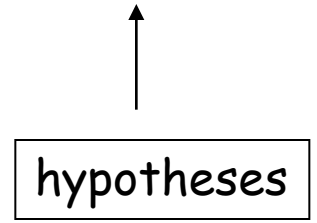
It is not sunny this afternoon and it is colder than yesterday.
If we go swimming it is sunny.
If we do not go swimming then we will take a canoe trip.
If we take a canoe trip then we will be home by sunset.
We will be home by sunset

1. It is not sunny this afternoon and it is colder than yesterday.
2. If we go swimming it is sunny.
3. If we do not go swimming then we will take a canoe trip.
4. If we take a canoe trip then we will be home by sunset.
5. We will be home by sunset

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



1. $\neg p \wedge q$
2. $r \rightarrow p$
3. $\neg r \rightarrow s$
4. $s \rightarrow t$
5. t



Using the rules of inference to build arguments

An example

- p It is sunny this afternoon
- q It is colder than yesterday
- r We go swimming
- s We will take a canoe trip
- t We will be home by sunset (the conclusion)

1. $\neg p \wedge q$
2. $r \rightarrow p$
3. $\neg r \rightarrow s$
4. $s \rightarrow t$
5. t

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

Rule of inference	Tautology	Name
$\frac{p \rightarrow q \quad p}{\therefore q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$\frac{\neg q \quad p \rightarrow q}{\therefore \neg p}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$\frac{p \vee q \quad \neg p}{\therefore q}$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p \quad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{p \vee q \quad \neg p \vee r}{\therefore q \vee r}$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolution

Using the resolution rule (an example)

1. Anna is skiing or it is not snowing.
2. It is snowing or Bart is playing hockey.
3. Consequently Anna is skiing or Bart is playing hockey.

We want to show that (3) follows from (1) and (2)

Using the resolution rule (an example)

1. Anna is skipping or it is not snowing.
2. It is snowing or Bart is playing hockey.
3. Consequently Anna is skiing or Bart is playing hockey.

hypotheses

1. $p \vee \neg r$
2. $r \vee q$

propositions

- p Anna is skiing
 q Bart is playing hockey
 r it is snowing

$$p \vee q$$

$$\neg p \vee r$$

$$\therefore q \vee r$$

Resolution rule

Consequently Anna is skiing or Bart is playing hockey

Handling Quantified Statements

- Valid arguments for quantified statements are a sequence of statements. Each statement is either a premise or follows from previous statements by rules of inference which include:
 - Rules of Inference for Propositional Logic
 - Rules of Inference for Quantified Statements
- The rules of inference for quantified statements are introduced in the next several slides.

Universal Instantiation (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Example:

Our domain consists of all dogs and Fido is a dog.

“All dogs are cuddly.”

“Therefore, Fido is cuddly.”

Universal Generalization (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Used often implicitly in Mathematical Proofs.

Existential Instantiation (EI)

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

Example:

“There is someone who got an A in the course.”

“Let’s call her a and say that a got an A”

Existential Generalization (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

Example:

“Michelle got an A in the class.”

“Therefore, someone got an A in the class.”

Using Rules of Inference

Example 1: Using the rules of inference, construct a valid argument to show that

“John Smith has two legs”

is a consequence of the premises:

“Every man has two legs.” “John Smith is a man.”

Solution: Let $M(x)$ denote “ x is a man” and $L(x)$ “ x has two legs” and let John Smith be a member of the domain.

Valid Argument:

Step	Reason
1. $\forall x(M(x) \rightarrow L(x))$	Premise
2. $M(J) \rightarrow L(J)$	UI from (1)
3. $M(J)$	Premise
4. $L(J)$	Modus Ponens using (2) and (3)

Using Rules of Inference

Example 2: Use the rules of inference to construct a valid argument showing that the conclusion

“Someone who passed the first exam has not read the book.”
follows from the premises

“A student in this class has not read the book.”

“Everyone in this class passed the first exam.”

Solution: Let $C(x)$ denote “ x is in this class,” $B(x)$ denote “ x has read the book,” and $P(x)$ denote “ x passed the first exam.”

First we translate the premises and conclusion into symbolic form.

$$\frac{\begin{array}{l} \exists x(C(x) \wedge \neg B(x)) \\ \forall x(C(x) \rightarrow P(x)) \end{array}}{\therefore \exists x(P(x) \wedge \neg B(x))}$$

Continued on next slide →

Using Rules of Inference

Valid Argument:

Step	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	EI from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	UI from (4)
6. $P(a)$	MP from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conj from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	EG from (8)

Returning to the Socrates Example

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

$$Man(Socrates)$$

$$\therefore Mortal(Socrates)$$

Solution for Socrates Example

Valid Argument

Step

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

2. $Man(Socrates) \rightarrow Mortal(Socrates)$

3. $Man(Socrates)$

4. $Mortal(Socrates)$

Reason

Premise

UI from (1)

Premise

MP from (2)
and (3)

Universal Modus Ponens

Universal Modus Ponens combines universal instantiation and modus ponens into one rule.

$$\forall x(P(x) \rightarrow Q(x))$$

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

$$\therefore Q(a)$$

This rule could be used in the Socrates example.

Introduction to Proofs

Section 1.7

Section Summary

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
 - Proof of the Contrapositive
 - Proof by Contradiction

Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.
- In math, CS, and other disciplines, informal proofs which are generally shorter, are generally used.
 - More than one rule of inference are often used in a step.
 - Steps may be skipped.
 - The rules of inference used are not explicitly stated.
 - Easier for to understand and to explain to people.
 - But it is also easier to introduce errors.
- Proofs have many practical applications:
 - verification that computer programs are correct
 - establishing that operating systems are secure
 - enabling programs to make inferences in artificial intelligence
 - showing that system specifications are consistent

Definitions

- A *theorem* is a statement that can be shown to be true using:
 - definitions
 - other theorems
 - *axioms* (statements which are given as true)
 - rules of inference
- A *lemma* is a ‘helping theorem’ or a result which is needed to prove a theorem.
- A *corollary* is a result which follows directly from a theorem.
- Less important theorems are sometimes called *propositions*.
- A *conjecture* is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

Forms of Theorems

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
- Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

“If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ ”

really means

“For all positive real numbers x and y , if $x > y$, then $x^2 > y^2$.”

Proving Theorems

- Many theorems have the form:

$$\forall x(P(x) \rightarrow Q(x))$$

- To prove them, we show that where c is an arbitrary element of the domain, $P(c) \rightarrow Q(c)$
- By universal generalization the truth of the original formula follows.
- So, we must prove something of the form: $p \rightarrow q$

Proving Conditional Statements: $p \rightarrow q$

- *Trivial Proof*: If we know q is true, then $p \rightarrow q$ is true as well.

“If it is raining then $1=1$.”

- *Vacuous Proof*: If we know p is false then $p \rightarrow q$ is true as well.

“If I am both rich and poor then $2 + 2 = 5$.”

[Even though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction, as we will see in Chapter 5)]

Even and Odd Integers

Definition: The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k , such that $n = 2k + 1$. Note that every integer is either even or odd and no integer is both even and odd.

We will need this basic fact about the integers in some of the example proofs to follow. We will learn more about the integers in Chapter 4.

Proving Conditional Statements: $p \rightarrow q$

- *Direct Proof:* Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

Example: Give a direct proof of the theorem “If n is an odd integer, then n^2 is odd.”

Solution: Assume that n is odd. Then $n = 2k + 1$ for an integer k . Squaring both sides of the equation, we get:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k$, an integer.

We have proved that if n is an odd integer, then n^2 is an odd integer. ◀

(◀ marks the end of the proof. Sometimes QED is used instead.)

Proving Conditional Statements: $p \rightarrow q$

Definition: The real number r is *rational* if there exist integers p and q where $q \neq 0$ such that $r = p/q$

Example: Prove that the sum of two rational numbers is rational.

Solution: Assume r and s are two rational numbers. Then there must be integers p, q and also t, u such that

$$r = p/q, \quad s = t/u, \quad u \neq 0, \quad q \neq 0$$

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} = \frac{v}{w} \quad \text{where } v = pu + qt \\ w = qu \neq 0$$

Thus the sum is rational. 

Proving Conditional Statements: $p \rightarrow q$

- *Proof by Contraposition:* Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow q$.

Why does this work?

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

Solution: Assume n is even. So, $n = 2k$ for some integer k . Thus

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j \text{ for } j = 3k + 1$$

Therefore $3n + 2$ is even. Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even), then n is odd (not even). ◀

Proving Conditional Statements: $p \rightarrow q$

Example: Prove that for an integer n , if n^2 is odd, then n is odd.

Solution: Use proof by contraposition. Assume n is even (i.e., not odd). Therefore, there exists an integer k such that $n = 2k$. Hence,

$$n^2 = 4k^2 = 2(2k^2)$$

and n^2 is even (i.e., not odd).

We have shown that if n is an even integer, then n^2 is even. Therefore by contraposition, for an integer n , if n^2 is odd, then n is odd. ◀

Proving Conditional Statements: $p \rightarrow q$

- *Proof by Contradiction: (AKA reductio ad absurdum).*

To prove p , assume $\neg p$ and derive a contradiction such as $p \wedge \neg p$. (an indirect form of proof). Since we have shown that $\neg p \rightarrow \mathbf{F}$ is true, it follows that the contrapositive $\mathbf{T} \rightarrow p$ also holds.

Example: Prove that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.

Solution: Assume that no more than 3 of the 22 days fall on the same day of the week. Because there are 7 days of the week, we could only have picked 21 days. This contradicts the assumption that we have picked 22 days. ◀

Proof by Contradiction

- A preview of Chapter 4.

Example: Use a proof by contradiction to give a proof that $\sqrt{2}$ is irrational.

Solution: Suppose $\sqrt{2}$ is rational. Then there exists integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (see Chapter 4). Then

$$2 = \frac{a^2}{b^2} \qquad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even (an exercise). Since a is even, $a = 2c$ for some integer c . Thus,

$$2b^2 = 4c^2 \qquad b^2 = 2c^2$$

Therefore b^2 is even. Again then b must be even as well.

But then 2 must divide both a and b . This contradicts our assumption that a and b have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational.



Proof by Contradiction

- A preview of Chapter 4.

Example: Prove that there is no largest prime number.

Solution: Assume that there is a largest prime number. Call it p_n . Hence, we can list all the primes $2, 3, \dots, p_n$. Form

$$r = p_1 \times p_2 \times \dots \times p_n + 1$$

None of the prime numbers on the list divides r .

Therefore, by a theorem in Chapter 4, either r is prime or there is a smaller prime that divides r . This contradicts the assumption that there is a largest prime. Therefore, there is no largest prime. ◀

Theorems that are Biconditional Statements

- To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Example: Prove the theorem: “If n is an integer, then n is odd if and only if n^2 is odd.”

Solution: We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude $p \leftrightarrow q$.

Sometimes *iff* is used as an abbreviation for “if and only if,” as in

“If n is an integer, then n is odd iff n^2 is odd.”

What is wrong with this?

“Proof” that $1 = 2$

Step

1. $a = b$

2. $a^2 = a \times b$

3. $a^2 - b^2 = a \times b - b^2$

4. $(a - b)(a + b) = b(a - b)$

5. $a + b = b$

6. $2b = b$

7. $2 = 1$

Reason

Premise

Multiply both sides of (1) by a

Subtract b^2 from both sides of (2)

Algebra on (3)

Divide both sides by $a - b$

Replace a by b in (5) because $a = b$

Divide both sides of (6) by b

Solution: Step 5. $a - b = 0$ by the premise and division by 0 is undefined.

Show that $R \rightarrow S$ can be derived from the Premises $P \rightarrow (Q \rightarrow S)$, $\neg R \vee P$, Q .

Introduce a third inference rule, known as rule CP or rule of Conditional Proof.

First Rule is Rule P

Second Rule is Rule T

Third Rule is Rule CP

Rule CP: If we can derive S from, R and a set of Premises, then we can derive $R \rightarrow S$ from the set of premises alone.

General Idea of Rule CP

- We may introduce a new Premise R Conditionally.
- Use R in conjunction with the original Premises to derive conclusion S .
- Then assert that the implication $R \rightarrow S$ follows from the original Premises alone.
- If S is a valid inference from the given premises and R , then $R \rightarrow S$ is a valid inference from original premises.

- Rule CP is not new for our purpose here because it follows from the following equivalence formula
- **$(P \wedge R) \rightarrow S \equiv P \rightarrow (R \rightarrow S)$**
- Where P denotes the conjunction of the set of Premises and R can any formula.
- The above Rule states that if R is included as an additional premise and **S** is derived from **$P \wedge R$** , then **$R \rightarrow S$** can be derived from the premises **P** alone. Rule CP also called **Deduction Theorem**.
- Rule CP is generally used if the conclusion is of the form **$R \rightarrow S$** . In such cases, R is taken as an additional premise and S is derived from the given premises and R.

- Show that $R \rightarrow S$ can be derived from the Premises $P \rightarrow (Q \rightarrow S)$, $\neg R \vee P$, Q .

1. $\neg R \vee P$ Rule P.
2. R Rule P(Additional Premise)
3. P Rule T(Disjunctive Syllogism) on 1 and 2
4. $P \rightarrow (Q \rightarrow S)$ Rule P.
5. $Q \rightarrow S$ Rule T(Modus Ponens) on 3 and 4
6. Q Rule P.
7. S Rule T(Modus Ponens) on 5 and 6
8. $R \rightarrow S$ Rule CP

Show that $P \rightarrow S$ can be derived from the
Premises $\neg P \vee Q, \neg Q \vee R, R \rightarrow S$

- 1. $\neg P \vee Q$ Rule P
- 2. P Rule P (additional premise)
- 3. Q Rule T on 1 and 2
- 4. $\neg Q \vee R$ Rule P
- 5. R Rule T on 3 and 4
- 6. $R \rightarrow S$ Rule P
- 7. S Rule T on 5 and 6
- 8. $P \rightarrow S$ Rule CP

- Notion of inconsistency is used In a procedure called **Proof by contradiction or direct Method of Proof.**

Technique is as follows

- In order to show that a conclusion C follows logically from the given premises we assume that C is false and consider $\neg C$ as an additional Premise.
- If the new set of premises is inconsistent then they imply a contradiction. Therefor C is true whenever the conjunction of given premises is true.
- Thus, C follows logically from given premises.

Show that $\neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$ by proof of contradiction(In direct method of proof)

We introduce $\neg\neg(P \wedge Q)$ as an additional premise and show that this additional premise leads to a contradiction.

1. $\neg\neg(P \wedge Q)$ Rule P(additional premise)
2. $P \wedge Q$ Rule T on 1(Double negation)
3. P Rule T on 2 (Simplification)
4. $\neg P \wedge \neg Q$ Rule P
5. $\neg P$ Rule T on 4(Simplification)
6. $P \wedge \neg P$ Contradiction(3 and 5)

Predicate Logic

- Open Statement
- Notation of Open Statements
- Universe/Universe of Discourse
- Free variable
- Bounded variable
- What is predicate?
- Converting open statement to Proposition
- Quantifiers
- Universal Quantifiers(\forall)
- Existential Quantifiers(\exists)

- Statement

- “7 is a prime number” is true.

- Predicate

- “ x is a prime number” is neither true nor false.

- Statements

- “ $\forall x \in \{2, 3, 5, 7\}, x$ is a prime number” is true.
- “ $\forall x \in \{2, 3, 6, 7\}, x$ is a prime number” is false.

Consider the following statements

- **All** squares are Rectangles
- **For every** integer x , x^2 is non-negative integer
- **Some** Determinates are equal to zero
- **There exist** a real number whose square is equal to it self.

All the words highlighted in Red are called Quantifiers(Associated with idea of quantity).

All squares are Rectangles

Let S be Set of squares(Universe)

Then the above statement can be written as

For all $x \in S$, x is a rectangle

Symbolically

$$\forall x \in S, P(x)$$

\forall Is called Universal Quantifier

$P(x)$ is a open statement , x is a Rectangle

For all, For every, For any, For each are said to be equivalent Phrases and called Universal Quantifiers

Some Determinates are equal to zero

- If D denotes set of all determinants then
For some $x \in D$, x is equal to zero

Symbolically

$$\exists x \in D, P(x)$$

\exists Is called Existential Quantifier

$P(x)$ is a open statement, x is equal to zero.

For some, There exist, at least once phrases are said to be equivalent and called Existential Quantifiers.

Quantified Statement

- A Proposition involving Universal/Existential Quantifier is called “ Quantified Statement”.
- $\forall x \in S, P(x)$
- $\exists x \in D, P(x)$ are called Quantified Statements
- The variable Present in the Quantified Statement is called **bound variable**. It is bounded by a Quantifier.

- When the Context tells what the universe is, the universe is not Explicitly indicated.
- In such cases Quantified statements are written as follows.
- $\forall x, P(x)$
- $\exists x, P(x)$

For the Universe of all Integers, Let

$P(x): x > 0$

$q(x): x$ is even

$r(x): x$ is a perfect square $s(x): x$ is divisible by 3

$t(x): x$ is divisible by 7

Write down the following statements in symbolic form.

1. At least one Integer is even
2. There exist a positive integer that is even
3. Some even integers are divisible by 3
4. If x is even and a perfect square, then x is not divisible by 3.
5. If x is odd or not divisible by 7, then x is divisible by 3.

Truth value of a quantified Statement

- The following rules are employed for determining the truth value of a quantified statement.
- Rule 1: the statement $\forall x \in S, P(x)$ is true only when $P(x)$ is true for each $x \in S$.
- Rule 2: the statement, $\exists x \in S, P(x)$ is false only when $P(x)$ is false for each $x \in S$.
- Accordingly to infer that $\forall x \in S, P(x)$ is false it is enough to exhibit one element a of S such $P(a)$ is false. This element a is called counterexample.
- Accordingly to infer that $\exists x \in S, P(x)$ is true it is enough to exhibit one element a of S such $P(a)$ is true.

Write the following in symbolic form

- Some thing is good
- Everything is good
- Nothing is good
- Something is not good
- Statement 1 means “ there is at least one x such that x is good”
- Statement 2 means “ for all x , x is good”
- Statement 3 means “ for all x , x is not good”
- Statement 4 means “ there is at least one x such that x is not good”

- Let $G(x)$: x is good, then
- Statement 1 is denoted as $(\exists x) (G(x))$
- *Statement 2 is denoted as* $(\forall x) (G(x))$
- Statement 3 is denoted as $(\forall x) (\neg G(x))$
- Statement 4 is denoted as $(\exists x) (\neg G(x))$

- All human being are good
- No human being are good
- Some human being are good
- Some human being are not good.

All Human being are good

- We assume that universe consists some of which are not men.
- Above statement can also be written as follows

for all x , if x is a human being, then x is good.

All integers are rational numbers and some rational numbers are not integers.

Let $p(x)$: x is a rational number

$q(x)$: x is an integer.

Z : set of all integers

Q : set of all rational numbers.

- All human being are mortal
- Every apple is red
- Any integer is positive or negative

For all x , if x is human being then x is mortal

For all x , if x is an apple, then x is red

For all x , if x is an integer, then x is either positive or negative.

- If all triangles are right-angled, then no triangle is equiangular.
- Let T denote the set of all triangles
- $P(x)$: x is right-angled
- $Q(x)$: x is equiangular



Negations of Universal Statements

- The negation of

$$\forall x \in S, P(x)$$

is the statement

$$\exists x \in S, \sim P(x).$$

- If “ $\forall x \in \mathbb{R}, x^2 > 10$ ” is false, then “ $\exists x \in \mathbb{R}, x^2 \leq 10$ ” is true.



Negations of Existential Statements

- The negation of

$$\exists x \in S, P(x)$$

is the statement

$$\forall x \in S, \sim P(x).$$

- If “ $\exists x \in \mathbb{R}, x^2 < 0$ ” is false, then “ $\forall x \in \mathbb{R}, x^2 \geq 0$ ” is true.



Example: Negation of a Universal Statement

- $p =$ “Everybody likes me.”
- Express p as
$$\forall x \in \{\text{all people}\}, x \text{ likes me.}$$
- $\sim p$ is the statement
$$\exists x \in \{\text{all people}\}, x \text{ does not like me.}$$
- $\sim p =$ “Somebody does not like me.”



Example: Negation of an Existential Statement

- $p =$ “Somebody likes me.”
- Express p as
$$\exists x \in \{\text{all people}\}, x \text{ likes me.}$$
- $\sim p$ is the statement
$$\forall x \in \{\text{all people}\}, x \text{ does not like me.}$$
- $\sim p =$ “Everyone does not like me.”
- $\sim p =$ “Nobody likes me.”



Multiple Quantified Statements

- Multiple universal statements
 - $\forall x \in S, \forall y \in T, P(x, y)$
 - The order does not matter.
- Multiple existential statements
 - $\exists x \in S, \exists y \in T, P(x, y)$
 - The order does not matter.



Multiple Quantified Statements

- Mixed universal and existential statements
 - $\forall x \in S, \exists y \in T, P(x, y)$
 - $\exists y \in T, \forall x \in S, P(x, y)$
 - The order *does* matter.
 - What is the difference?
- Compare
 - $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0.$
 - $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x + y = 0.$

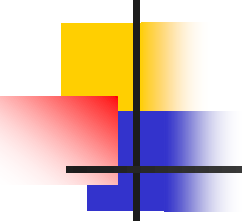


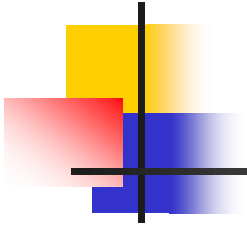
Negation of Multiple Quantified Statements

- Negate the statement

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \forall z \in \mathbb{R}, x + y + z = 0.$$

- $\sim(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \forall z \in \mathbb{R}, x + y + z = 0)$
 $\equiv \exists x \in \mathbb{R}, \sim(\exists y \in \mathbb{R}, \forall z \in \mathbb{R}, x + y + z = 0)$
 $\equiv \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \sim(\forall z \in \mathbb{R}, x + y + z = 0)$
 $\equiv \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \exists z \in \mathbb{R}, \sim(x + y + z = 0)$
 $\equiv \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \exists z \in \mathbb{R}, x + y + z \neq 0$

- 
-
- Negate the statement “Every integer can be written as the sum of three squares.”
 - $\sim(\forall n \in \mathbb{Z}, \exists r, s, t \in \mathbb{Z}, n = r^2 + s^2 + t^2)$.
 - $\exists n \in \mathbb{Z}, \sim(\exists r, s, t \in \mathbb{Z}, n = r^2 + s^2 + t^2)$.
 - $\exists n \in \mathbb{Z}, \forall r, s, t \in \mathbb{Z}, \sim(n = r^2 + s^2 + t^2)$.
 - $\exists n \in \mathbb{Z}, \forall r, s, t \in \mathbb{Z}, n \neq r^2 + s^2 + t^2$.



Negations

- $\neg \forall x P(x) \equiv \exists x \neg P(x).$
- $\neg \exists x P(x) \equiv \forall x \neg P(x).$
- Remember when the universe of discourse is finite, we have:
 - $\forall x P(x) \equiv P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n)$
 - $\exists x P(x) \equiv P(x_1) \vee P(x_2) \vee \dots \vee P(x_n)$

 - $\neg \forall x P(x) \equiv \neg (P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n))$
 $\equiv \neg P(x_1) \vee \neg P(x_2) \vee \dots \vee \neg P(x_n)$
 $\equiv \exists x \neg P(x)$
 - $\neg \exists x P(x) \equiv \neg (P(x_1) \vee P(x_2) \vee \dots \vee P(x_n))$
 $\equiv \neg P(x_1) \wedge \neg P(x_2) \wedge \dots \wedge \neg P(x_n)$
 $\equiv \forall x \neg P(x)$

Negating Quantifiers

<i>Negation</i>	<i>When True?</i>	<i>When False?</i>
$\neg\exists x P(x)$ ($\forall x \neg P(x)$)	When $P(x)$ is false for every x .	When there is an x for which $P(x)$ is true.
$\neg\forall x P(x)$ ($\exists x \neg P(x)$)	When there is an x for which $P(x)$ is false.	When $P(x)$ is true for every x .

In-class Exercise

- Consider the following predicates

- $P(x) = \text{“}x \text{ is a prime number”}$
- $Q(x,y) = \text{“}x \text{ is evenly divisible by } y\text{”}$

Using the above predicates, symbolize the following propositions. Assume the universe of discourse is the set of all positive integers.

1. Every integer that is evenly divisible by 10 is also evenly divisible by 5 and evenly divisible by 2.
2. There exists an odd integer that is not prime.

Solution

- Every integer that is divisible by 10 is also divisible by 5 and divisible by 2

$$\forall x [Q(x,10) \rightarrow (Q(x,5) \wedge Q(x,2))]$$

- There exists an odd integer that is not prime.

$$\exists x (\neg Q(x,2) \wedge \neg P(x))$$

Example

- Given the following predicates:

- $F(x,y)$: “ x is the father of y ”

- $M(x,y)$: “ x is the mother of y ”

Symbolize the predicate

$R(x,y)$: “ x is the father of the mother of y ”.

Solution

- Given the following predicates:

- $F(x,y)$: “ x is the father of y ”

- $M(x,y)$: “ x is the mother of y ”

Symbolize the predicate

$R(x,y)$: “ x is the father of the mother of y ”.

$$R(x,y) = \exists z (F(x,z) \wedge M(z,y))$$

Guidelines in Translating....

- The proposition

$$\forall y (P(y) \rightarrow Q(y))$$

can be translated as “All individuals having property P also have property Q ”

- What is the difference between

$$\forall y (P(y) \rightarrow Q(y))$$

and

$$\forall y (P(y) \wedge Q(y))$$

- The proposition

$$\exists y (P(y) \wedge Q(y))$$

an be translated as “Some individuals having property P also have property Q ”

- $\forall x \in D, P(x) \wedge Q(x)$

is logically equivalent to

$$(\forall x \in D, P(x)) \wedge (\forall x \in D, Q(x))$$

The meaning of this is that **every** element has property P and **every** element also has property Q — not at all the same thing as saying "every element **that has** property P also has property Q ".

- For example, if $D = \mathbf{N}$ (the set of natural numbers), $P(x)$ means " x is a prime number greater than 2", and $Q(x)$ means " x is odd", then

$$\forall x \in D, P(x) \wedge Q(x)$$

means: "every natural number **is** prime **and** greater than 2 **and** odd" — a statement that is clearly False because there are natural numbers that are not prime, for example.

By contrast, the statement

$$\forall x \in D, P(x) \Rightarrow Q(x)$$

means: "every natural number **that is** prime and greater than 2 **is also** odd" — a statement that is True.

Nested Quantifiers

- When we have more than one variable in a predicate, one way to make a proposition is to use nested quantifiers.
- When using nested quantifiers, we must pay attention to the order in which they are used.

Quantification of Two Variables

<i>proposition</i>	<i>When True?</i>	<i>When False?</i>
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$		
$\forall x \exists y P(x, y)$		
$\exists x \forall y P(x, y)$		
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$		

Quantification of Two Variables

<i>proposition</i>	<i>When True?</i>	<i>When False?</i>
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y .	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$		
$\exists x \forall y P(x, y)$		
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$		

Quantification of Two Variables

<i>proposition</i>	<i>When True?</i>	<i>When False?</i>
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y .	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$		
$\exists x \forall y P(x, y)$		
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y .

Quantification of Two Variables

<i>proposition</i>	<i>When True?</i>	<i>When False?</i>
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ 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. (y may depend on x .)	There is an x such that $P(x, y)$ is false for every y .
$\exists x \forall y P(x, y)$		
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y .

Quantification of Two Variables

<i>proposition</i>	<i>When True?</i>	<i>When False?</i>
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ 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. (y may depend on x .)	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 such that $P(x, y)$ is true for every y . (x may not depend on 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 .

Examples

- Let $P(x, y)$ denote “ $x + y = 5$.”
 - The universe of discourse for both x and y is $\{1, 2, 3, 4\}$
- Find the truth value for $\forall x \forall y P(x, y)$
 - *Solution:*
- Find the truth value for $\exists y \exists x P(x, y)$
 - *Solution:*

Examples

- Let $P(x, y)$ denote “ $x + y = 5$.”
 - The universe of discourse for both x and y is $\{1, 2, 3, 4\}$
- Find the truth value for $\forall x \forall y P(x, y)$
 - *Solution:* **False** (if $x = 1$ and $y = 3$, then $x + y \neq 5$)
- Find the truth value for $\exists y \exists x P(x, y)$
 - *Solution:* **True** (if $x = 3$ and $y = 2$, then $x + y = 5$)

Examples

- Let $P(x, y)$ denote “ $x + y = 5$.”
 - The universe of discourse for both x and y is $\{1, 2, 3, 4\}$
- Find the truth value for $\forall x \exists y P(x, y)$
 - *Solution:*
- Find the truth value for $\exists x \forall y P(x, y)$
 - *Solution:*

Examples

- Let $P(x, y)$ denote “ $x + y = 5$.”
 - The universe of discourse for both x and y is $\{1, 2, 3, 4\}$
- Find the truth value for $\forall x \exists y P(x, y)$
 - *Solution:* **True**; for any x , there exists a y such that $x + y = 5$; namely, for $x=1$, let $y=4$; for $x=2$, let $y=3$; for $x=3$, let $y=2$; and for $x=4$, let $y=1$;
- Find the truth value for $\exists x \forall y P(x, y)$
 - *Solution:* **False**; there is no one x such that for **each** y , we would have $x + y = 5$;
 - if $x=1$, then when $y=1$, $x + y \neq 5$; and
 - if $x=2$, then when $y=2$, $x + y \neq 5$; and
 - if $x=3$, then when $y=3$, $x + y \neq 5$; and, finally,
 - if $x=4$, then when $y=4$, $x + y \neq 5$;

Example

- Consider the following predicates:
 - $E(x)$ = “ x is an even integer”
 - $P(x)$ = “ x is prime”
 - $Q(x,y)$ = “integer x equals integer y ”
 - $L(x,y)$ = “integer x is less than integer y ”
- Using the above predicates and appropriate quantifiers, symbolize the following proposition. Assume the universe of discourse is all positive integers.
 - There are two distinct prime integers whose sum is even.

Solution

- Using
 - $E(x)$ = “ x is an even integer”
 - $P(x)$ = “ x is prime”
 - $Q(x,y)$ = “integer x equals integer y ”
 - $L(x,y)$ = “integer x is less than integer y ”
- There are two distinct prime integers whose sum is even.
 - Solution: $\exists x \exists y [\neg Q(x,y) \wedge E(x+y) \wedge P(x) \wedge P(y)]$

Interesting proposition

- The universe of discourse is the set of all positive integers \mathbb{N} .
- English: **Every** even integer (greater than 2) is the sum of two primes. $10 = 3+7$; $44 = 3 +41$;
- $\forall n \exists m \exists k ((n>2) \rightarrow (n = m+k))$
- This has never been proved or disproved!
- Written in terms of functions we have
 $\forall n \exists m \exists k ((GT(n,2)) \rightarrow (EQ(n, SUM(m, k)))$

Binding Variables

- Consider a propositional function $P(x)$
- A variable x is said to be *bound* when:
 - a value is assigned to x , or
 - a quantifier is used on x ,Otherwise, x is said to be *free*.
- When we have more than one variable in a propositional function, the order of the quantifiers is important (unless the quantifiers are of the same type).

Free and Bound Variables

- When all the variables of a propositional function are bound then it becomes a proposition.

Let $P(x, y)$ denote “ $x < y$ ”.

- In $\exists x P(x, y)$, variable x is bound but y is free, and $\exists x P(x, y)$ is not yet a proposition.
- $\exists x P(x, 2)$ is now a proposition; all the variables are bound now.
- $\forall x \exists y P(x, y)$ is also a proposition, all the variables are bound now.
- Note that once a variable is bound using a quantifier, it cannot be given a value. For example, $\exists x P(3, y)$ does not make sense.

Scope of the Quantifiers

- The *scope* of a quantifier (\exists or \forall) is the part of the expression that it applies to.
 - In $\forall x (S(x) \rightarrow P(x))$, the scope of \forall is $S(x) \rightarrow P(x)$.
 - In $(\exists x P(x)) \wedge Q(x)$, the scope of \exists is $P(x)$.
 - This latter expression is the same as $(\exists y P(y)) \wedge Q(x)$.

Rules of Inference for Quantifications

<i>Rule of Inference</i>	<i>Name</i>	<i>Comments</i>
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal Specification/Instantiation (US) or (UI)	for any c in the domain

Rules of Inference for Quantifications

<i>Rule of Inference</i>	<i>Name</i>	<i>Comments</i>
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal Specification/Instantiation (US) or (UI)	for any c in the domain
$\frac{P(c)}{\therefore \forall x P(x)}$	Universal generalization (UG)	for an arbitrary c , not a particular one

Rules of Inference for Quantifications

<i>Rule of Inference</i>	<i>Name</i>	<i>Comments</i>
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal Specification/Instantiation (US) or (UI)	for any c in the domain
$\frac{P(c)}{\therefore \forall x P(x)}$	Universal generalization (UG)	for an arbitrary c , not a particular one
$\frac{\exists x P(x)}{\therefore P(c)}$	Existential Specification/Instantiation (ES) or (EI)	for some specific c (unknown)

Rules of Inference for Quantifications

<i>Rule of Inference</i>	<i>Name</i>	<i>Comments</i>
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal Specification/Instantiation (US) or (UI)	for any c in the domain
$\frac{P(c)}{\therefore \forall x P(x)}$	Universal generalization (UG)	for an arbitrary c , not a particular one
$\frac{\exists x P(x)}{\therefore P(c)}$	Existential Specification/Instantiation (ES) or (EI)	for some specific c (unknown)
$\frac{P(c)}{\therefore \exists x P(x)}$	Existential generalization (EG)	Finding one c such that $P(c)$

Rules of Inference for Predicates

- All the Propositional logic rules.
- The *Universal Specification* (US) rule:
 $\forall x P(x) \Rightarrow P(y)$ for any y in the domain.
The rule is also known as **Instantiation** rule
- The *Existential Specification* (ES)
 $\exists x P(x) \Rightarrow P(y)$ for **some** y in the domain.
- The *Existential Generalization* (EG)
 $P(y) \Rightarrow \exists x P(x)$
- The *Universal Generalization* (EG)
 $P(y) \Rightarrow \forall x P(x)$

Example: Socrates is mortal

- *All men are mortal. Socrates is a man. Therefore, Socrates is mortal.*
- Define $M(x)$: “ x is mortal.”
- Define the universe to be all men.
- Then the argument being made is:

$$\frac{\forall x M(x)}{\therefore M(\text{Socrates})}$$

which is an example of *universal specification*

Other Facts

- $\exists x (A(x) \rightarrow B(x)) \equiv \forall x A(x) \rightarrow \exists x B(x)$
- $\exists x A(x) \rightarrow \forall x B(x) \equiv \forall x (A(x) \rightarrow B(x))$
- $\exists x (A(x) \vee B(x)) \equiv \exists x A(x) \vee \exists x B(x)$
- $\forall x (A(x) \wedge B(x)) \equiv \forall x A(x) \wedge \forall x B(x)$

Prove that $\forall x (H(x) \rightarrow M(x)) \wedge H(s) \Rightarrow M(s)$

- This is the famous Socrates's argument
 - All men are mortal
 - Socrates is a man
 - Therefore, Socrates is a mortal
- Let $H(x)$ be “ x is a man”,
- Let $M(x)$ be “ x is a mortal” and
- Let s be “Socrates”.

Prove that $\forall x (H(x) \rightarrow M(x)) \wedge H(s) \Rightarrow M(s)$

- | | | |
|----|-------------------------------------|----------------------------|
| 1. | $\forall x (H(x) \rightarrow M(x))$ | Premise |
| 2. | $H(s) \rightarrow M(s)$ | 1, Universal Specification |
| 3. | $H(s)$ | Premise |
| 4. | $M(s)$ | 2&3 and MP |

Prove that $\forall x (H(x) \rightarrow M(x)) \wedge \exists x H(x) \Rightarrow \exists x M(x)$

1. $\exists x H(x)$ Premise
2. $H(y)$ Existential Specification, for **some** y
3. $\forall x (H(x) \rightarrow M(x))$ Premise
4. $H(y) \rightarrow M(y)$ 3 & Universal Specification
5. $M(y)$ 2&4, Modus Ponens
6. $\exists x M(x)$ 5, Existential Generalization

Prove that $\exists x (A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x)$

- | | | |
|----|--|------------------------|
| 1. | $\exists x (A(x) \wedge B(x))$ | Premise |
| 2. | $A(y) \wedge B(y)$ | 1, ES, y is fixed now. |
| 3. | $A(y)$ | 2, Simplification |
| 4. | $B(y)$ | 2, Simplification |
| 5. | $\exists x A(x)$ | 3, EG |
| 6. | $\exists x B(x)$ | 4, EG |
| 7. | $\exists x A(x) \wedge \exists x B(x)$ | 5&6, Conjunction |

Prove that $\forall x (A(x) \vee B(x)) \Rightarrow \forall x A(x) \vee \exists x B(x)$

- | | | |
|-----|--|-----------------------------------|
| 1. | $\neg (\forall x A(x) \vee \exists x B(x))$ | Contrary Assumption |
| 2. | $\neg \forall x A(x) \wedge \neg \exists x B(x)$ | 1 & De Morgan's |
| 3. | $\neg \forall x A(x)$ | 2 |
| 4. | $\exists x \neg A(x)$ | 3 & De Morgan's |
| 5. | $\neg \exists x B(x)$ | 2 |
| 6. | $\forall x \neg B(x)$ | 5 & De Morgan's |
| 7. | $\neg A(y)$ | 4, ES, fixed y |
| 8. | $\neg B(y)$ | 6, US, free to choose y as in 7 |
| 9. | $\neg A(y) \wedge \neg B(y)$ | 7 & 8 |
| 10. | $\neg (A(y) \vee B(y))$ | 9, De Morgan's |
| 11. | $\forall x (A(x) \vee B(x))$ | Premise |
| 12. | $A(y) \vee B(y)$ | 11, US, any y , same as in 9 |
| 13. | Contradiction | 10 & 12 |

Automatic Theorem Proving

Proof methods and Informal Proofs

- After studying how to write **formal proofs** using rules of inference for predicate logic and quantified statements, we will move to **informal proofs**.
- Proving useful theorems using **formal proofs** would result in long and tedious proofs, where every single logical step must be provided.

Proof Methods

A proof is a valid argument that establishes the truth of a mathematical statement, using the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorems.

Using these ingredients and rules of inference, the proof establishes the truth of the statement being proved.

We move from formal proofs, as seen in the previous section, to **informal proofs**, where more than one inference rule may be used at each step, where steps may be skipped, and where axioms and rules of inference used are not explicitly stated.

Some terminology

Theorem: a statement that can be shown to be true (sometimes referred to as **facts** or **results**). Less important theorems are often called **propositions**.

A **lemma** is a less important theorem, used as an auxiliary result to prove a more important theorem.

A **corollary** is a theorem proven as an easy consequence of a theorem. A

conjecture is a statement that is being proposed as a true statement.

If later proven, it becomes a theorem, but it may be false. **Axiom** (or

postulates) are statements that we assume to be true (algebraic axioms specify rules for arithmetic like commutative laws). A **proof** is a valid argument that establishes the truth of a theorem. The

statements used in a proof include axioms, hypotheses (or premises),

and previously proven theorems. Rules of inference, together with

definition of terms, are used to draw conclusions from other assertions,

tying together the steps of a proof.

Methods of proving theorems

3 methods of showing statements of the type $p \rightarrow q$ are true:

- **Direct proofs:** Assume p is true; the last step establishes q is true.
- **Proof by Contraposition:** Uses a direct proof of the contrapositive of $p \rightarrow q$, which is $\neg q \rightarrow \neg p$. That is, assume $\neg q$ is true; the last step established $\neg p$ is true.
- **Proof by Contradiction:** To prove that P is true, we assume $\neg P$ is true and reach a contradiction, that is that $(r \wedge \neg r)$ is true for some proposition r .

Theorem

If n is an odd integer, then n^2 is odd.

Proof:

Let n be an odd integer.

By definition of odd, we know that there exists an integer k such that $n = 2k + 1$.

Squaring both sides of the equation, we get

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

Since $n^2 = 2k^j + 1$, where $k^j = 2k^2 + 2k$, by the definition of odd we conclude n^2 is odd.

Prove that for all Integers k and l , if k and l are both odd, then $k+l$ is even and kl is odd

- Take any two Integers k and l , and assume that both of these are odd(Hypothesis)
- Then $k=2m+1$, $l=2n+1$ for some integers m and n .
- Therefore $k+l= 2(m+n+1)$
- $kl= 4mn+2(m+n)+1$
- We observe that $k+l$ is divisible by 2
- kl is not divisible by 2
- Therefore $k+l$ is even and kl is odd.
- Since k and l are arbitrary integers the proof of the given statement(direct proof) is complete(in view of universal generalization).

Indirect Proof: Let n be an integer. Prove that if n^2 is odd, then n is odd

- Here the conditional to be proved is of the form $p \rightarrow q$, where
- p : n^2 is odd, q : n is odd
- We first prove the contrapositive $\neg q \rightarrow \neg p$ is true
- Assume that $\neg q$ is true
- That is n is not an odd integer
- Then $n=2k$ where k is an integer
- Now $n^2 = 2(2k^2)$, so that n^2 is not odd.
- that is p is false, or $\neg p$ is true
- This proves $\neg q \rightarrow \neg p$ is true
- Hence $p \rightarrow q$ is true.

Give an indirect proof of the statement: The product of two even integers is an even integer

- The given statement is equivalent to the following statement.
- If a and b are even integers, then ab is an even integer
- Thus the conditional to be proved is of the form $p \rightarrow q$ where
- p : a and b are even integers, q : ab is an even integer
- We first prove that contrapositive $\neg q \rightarrow \neg p$ is true.

- Assume that $\neg q$ is true.
- That is, assume that ab is not an even integer
- This means that ab is not divisible by 2.
- Hence a is not divisible by 2 and b is not divisible by 2.
- That is a is not an even integer and b is not an even integer.
- This means that the proposition a and b are even integers is false.
- That is p is false or $\neg p$ is true.
- This proves $\neg q \rightarrow \neg p$ is true
- Hence $p \rightarrow q$ is true.

Proof by contradiction

- Hypothesis: Assume that $p \rightarrow q$ is false. That is p is true and q is false.
- Analysis: Starting with the hypothesis that q is false and employing the rules of logic and other known facts, infer that p is false. This contradicts the assumption that p is true.
- Conclusion: Because of the contradiction arrived in the analysis, we infer that $p \rightarrow q$ is true.

Provide a proof by contradiction of the following statement: For every integer n , if n^2 is odd, then n is odd.

- Here the conditional to be proved is of the form $p \rightarrow q$, where
- p : n^2 is odd, q : n is odd
- Assume that $p \rightarrow q$ is false;
- That is p is true and q is false.
- q false means: n is even
- So $n = 2k$ for some integer k
- $n^2 = 4k^2$ which is even
- That is p is false, this contradicts the assumption that p is true.
- In view of contradiction we infer that given conditional
- $p \rightarrow q$ is true

- If n is odd integer, then $n+11$ is an even integer



Exhaustive proof

This is a special form of a proof by cases, when there is a finite and small number of examples for which we need to prove a fact.

Prove that $(n + 1)^2 \geq 3^n$ if n is a positive integer with $n \leq 2$.

We use a proof by exhaustion, by examining the cases $n = 1, 2$.

For $n = 1$, $(n + 1)^2 = 2^2 = 4 \geq 3 = 3^n$.

For $n = 2$, $(n + 1)^2 = 3^2 = 9 \geq 3^2 = 3^n$.

Existence Proofs

Existence proofs prove statements of the form $\exists xP(x)$.

Constructive existence proof: find a such that $P(a)$ is true.

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

Proof: $1729 = 10^3 + 9^3$ and $1729 = 12^3 + 1^3$.

- Disprove the proposition: The product of any two odd integers is a perfect square.
- Take $m = 3$ and $n = 5$ are odd integers
- But $mn = 15$ is not a perfect square.
- Thus the given proposition is disproved with $m = 3$ and $n = 5$ serving as counterexample.

The art of finding a proof method that works for a theorem

We need practice in order to recognize which type of proof to apply to a particular theorem/fact that we need to prove.

Inference engine

- In the field of Artificial Intelligence, **inference engine** is a component of the system that applies logical rules to the knowledge base to deduce new information.
- The first inference engines were components of [expert systems](#).
- In [artificial intelligence](#), an **expert system** is a computer system that emulates the decision-making ability of a human expert.

- The typical expert system consisted of a knowledge base and an inference engine.
- The knowledge base stores facts about the world.
- The inference engine applies logical rules to the knowledge base and deduce new knowledge.

- The logic that an inference engine uses is typically represented as IF-THEN rules.
- artificial intelligence researchers focused on more powerful [theorem prover](#) environments that offered much fuller implementations of [First Order Logic](#).
- Focusing on IF-THEN statements (what logicians call [Modus Ponens](#)) gave developers a very powerful general mechanism to represent logic.

- A simple example of Modus Ponens often used in introductory logic books is
- "If you are human then you are mortal". This can be represented as:
- Rule1: $\text{Human}(x) \Rightarrow \text{Mortal}(x)$
- A trivial example of how this rule would be used in an inference engine is as follows.
- The inference engine would find any facts in the knowledge base that matched $\text{Human}(x)$
- and for each fact it found, it would add the new information $\text{Mortal}(x)$ to the knowledge base.
- So if it found an object called Socrates that was Human, it would deduce that Socrates was Mortal.

Tutorial hour Questions

(b) If $3 + 5 = 8$, then $4 + 1 = 5$.

(c) $1 + 6 = 7$ or $2 + 4 = 7$.

4. State whether the following are well-formed formulas :

(a) $\neg(P \vee Q)$

(b) $\neg P \wedge Q$

(c) $(P \rightarrow Q) \rightarrow (\wedge Q)$

(d) $\sim p \vee (\sim q)$

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

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

5. Given the truth values of p and q as 1 and those of r and s as 0, find the truth values of the following :

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

(b) $(p \leftrightarrow r) \wedge ((\neg q) \rightarrow s)$

(c) $(p \wedge (q \rightarrow (r \vee \sim q))) \leftrightarrow (r \vee \sim p)$

6. Let P be 'He is tall' and Q be 'He is handsome'. Write each of the following in symbolic form using P and Q .

(a) He is tall and handsome.

(b) He is tall but not handsome.

(c) He is neither tall nor handsome.

7. Translate the following sentences into propositional forms.

(a) Amar is rich and happy

(b) Amar is rich but not happy

(c) Amar is rich or happy

(d) Amar is neither rich nor happy.

8. Write the inverse, converse and contra positive of the following propositions :

(a) $P \rightarrow \neg Q$

(b) $P \rightarrow (Q \rightarrow R)$

(c) $(P \wedge (P \rightarrow Q)) \rightarrow Q$.

9. Construct the truth tables for the following :

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

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

(c) $p \rightarrow (q \rightarrow r)$

(d) $q \leftrightarrow (\neg p \vee \neg q)$

(e) $[(p \wedge q) \vee (\neg r)] \leftrightarrow p$.

10. Determine whether the following are tautologies :

(a) $p \rightarrow (q \rightarrow p)$

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

(c) $p \rightarrow (p \vee q)$

(d) $p \vee (\sim(p \wedge q))$

11. Show that the truth values of the following formula is independent of their components.
 $(P \rightarrow Q) \leftrightarrow ((P \wedge Q) \vee (\neg P \wedge \neg Q))$

12. Verify if the proposition $((p \vee \neg q) \rightarrow r) \leftrightarrow s \vee \neg(((p \vee \neg q) \rightarrow r) \leftrightarrow s)$ is a tautology.

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

(b) $(\sim q \wedge p) \wedge q$

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

15. Show that the following :

(a) $((p \vee q) \rightarrow r) \leftrightarrow ((p \rightarrow r) \wedge (q \rightarrow r))$

(b) $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$

(c) $((p \rightarrow q) \wedge (p \rightarrow r)) \leftrightarrow p \rightarrow (q \wedge r)$

(d) $((p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p)) \leftrightarrow ((p \wedge q) \wedge (q \rightarrow r) \wedge (r \rightarrow p))$.

16. Prove the following logical equivalences without using truth tables.

(a) $p \vee (p \wedge (p \vee q)) \leftrightarrow p$

(b) $((\neg p \vee \neg q) \rightarrow (p \wedge q \wedge r)) \leftrightarrow p \wedge q$

$$(d) (p \vee q \vee (\sim p \wedge \sim q \wedge r)) \Leftrightarrow (p \vee q \vee r).$$

17. Prove that each of the following is a tautology.

$$(a) (\sim p \wedge (\sim q \wedge r)) \vee (q \wedge r) \vee (p \wedge r) \stackrel{?}{\Leftrightarrow} r \quad (b) (p \wedge (p \rightarrow q)) \rightarrow q.$$

18. Show that the following equivalences

$$(a) (P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (P \vee R) \rightarrow Q \quad (b) \neg(P \stackrel{?}{\Leftrightarrow} Q) \Leftrightarrow (P \vee Q) \wedge \neg(P \wedge Q).$$

[JNTU June, 2004 - Set-01]

EXERCISE 1.1

1. State which of the following sentences are propositions. If so find its truth value.
 - (a) A cow has four legs
 - (b) $3 + 5 = 7$
 - (c) $3 + 5 = 8$
 - (d) $\sqrt{3}$ is irrational number
 - (e) Moscow is the capital of Britain.
 - (f) Open the door.
2. Write the negation of each of the following statements :
 - (a) Arasavalli Surya Devalayam is in Andhra Pradesh.
 - (b) 2 divides 5
 - (c) Vijayawada is capital of Krishna District
 - (d) Taj Mahal is in Agra.
3. Determine the truth value of each of the following :
 - (a) Taj Mahal is in Agra and $5 + 4 = 8$

Predicate Logic Application in Artificial Intelligence

Inference Engine

In the field of Artificial Intelligence, inference engine is a component of the system that applies logical rules to the knowledge base to deduce new information. The first inference engines were components of expert systems. In artificial intelligence; an expert system is a computer system that emulates the decision-making ability of a human expert.

- The typical expert system consisted of a knowledge base and an inference engine.
- The knowledge base stores facts about the world.

The inference engine applies logical rules to the knowledge base and deduces new knowledge.

- The logic that an inference engine uses is typically represented as IF-THEN rules.
- Artificial intelligence researchers focused on more powerful theorem prover environments that offered much fuller implementations of First Order Logic.
- Focusing on IF-THEN statements (what logicians call Modus Ponens) gave developers a very powerful general mechanism to represent logic.

A simple example of Modus Ponens often used in introductory logic books is

- "If you are human then you are mortal". This can be represented as:
- Rule1: $\text{Human}(x) \Rightarrow \text{Mortal}(x)$
- A trivial example of how this rule would be used in an inference engine is as follows.
- The inference engine would find any facts in the knowledge base that matched $\text{Human}(x)$
- and for each fact it found, it would add the new information $\text{Mortal}(x)$ to the knowledge base.
- So if it found an object called Socrates that was Human, it would deduce that Socrates was Mortal.