Discrete Structures

Week#1 →Lecture # 1

FAST - National University of Computer and

Emerging Sciences, CFD Campus

Saba Naseem

saba.naseem@nu.edu.pk

Do not worry about your difficulties in Mathematics. I can assure you, mine are still greater!

-Albert Einstein-

Outline

- ❑What is DS and when can it be used?
- ❑Why study DS?
- ❑Topics
- ❑Today’s Lecture

Course organization

- **Class Schedule**
  - **Lecture # 1:** Check the Timetable ☺
  - **Lecture # 2:** Check the Timetable ☺

- Class will be conducted using Slides

- **Text Book**
  - Susana Epp, ***Discrete Mathematics with its Applications***, (4^{th} Edition)
  - Kenneth H. Rosen, **Discrete Mathematics and Its Applications**, 4th Edition

Discrete Structure/ Discrete Math

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).

Why Study DS??

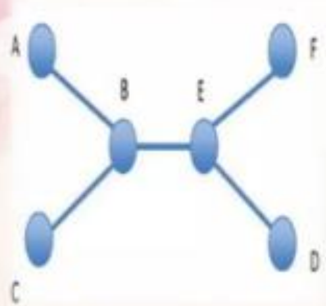
> Logic
> Information Theory
> Set Theory
> Graph Theory
> Operation Research
> Theoretical computer science
> Number Theory

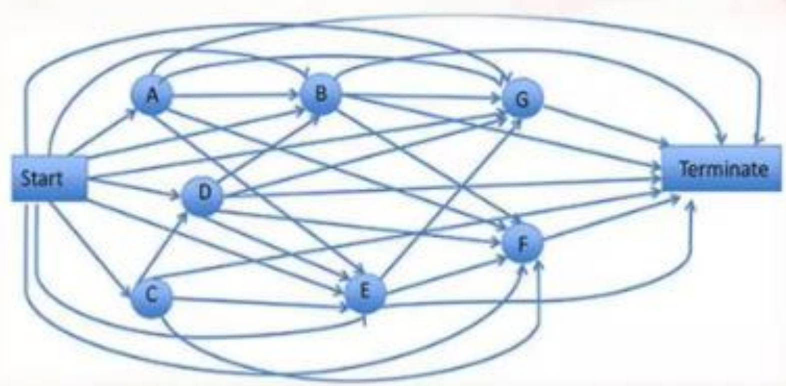
> Probability Theory
> Combinatories
> Algebra
> Geometry
> Topology
> Games Theory
> Utility Theory
> Decision Theory
> Social Choice Theory

Computers run software and store files. The software and files are both stored as huge string of 1s and 0s Binary math is discrete mathematics. All computer data is represented using binary. Binary digits can be grouped together into bytes

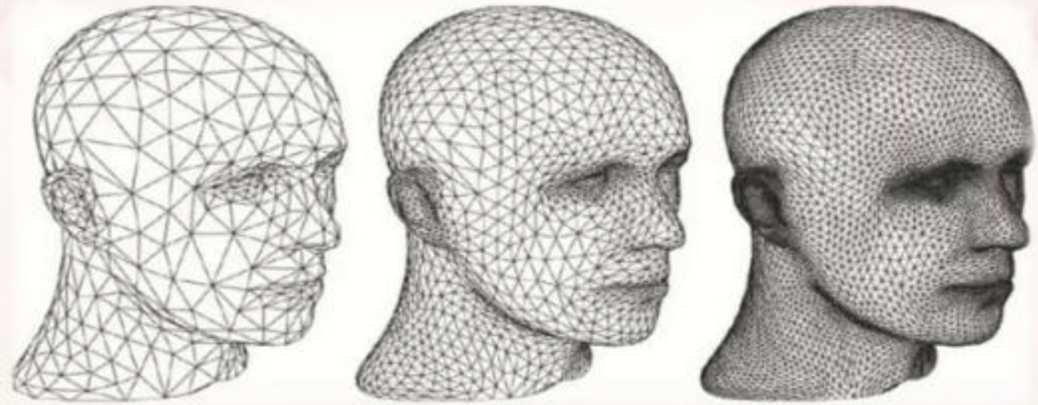
A + B	SUM	CARRY
0 + 0	0	0
0 + 1	1	0
1 + 0	1	0
1 + 1	0	1

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 system.



Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography provide secure any data or passwords in encryption methods.

Example.

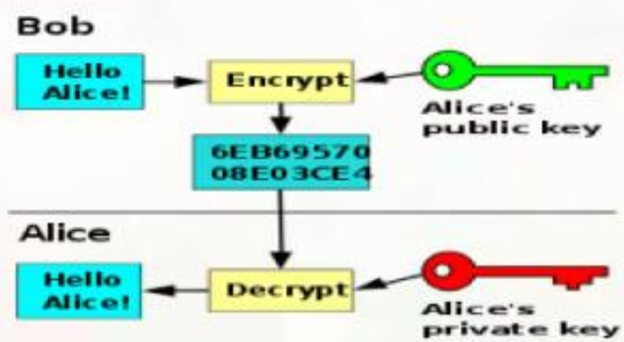


Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It convert image as two dimensional signals.

Relational database they play an important part in almost every organization that keep track of its employees,clients and resources.A relation data base help to join a different peace of information.This is all done concepts of discrete math set.

Discrete Structures

- Study of $\underbrace{\text{Discrete}}_{\text{Consisting of Distinct Objects}}$ (individually separate and distinct) Objects

- Problems Solved Using Discrete Structures
  - How many ways are there to choose a valid password?
  - What's the probability of winning a lottery?
  - How to encrypt a message?
  - What is the shortest path b/w two cities?
  - How to sort a list of integers? OR How many steps are needed to sort a list using a given method?
  - How to prove that an algorithm works correctly?
  - How can you identify a spam message?
  - How can we prove our algorithm is more efficient than another?
  - ….

Why Study Discrete Structures???

- Ability to understand and create mathematical arguments
- Gateway to more advanced courses
  - Algorithms
  - Database theory
  - Automata theory
  - Compiler theory
  - Computer security
  - Operating system

Topics we'll study

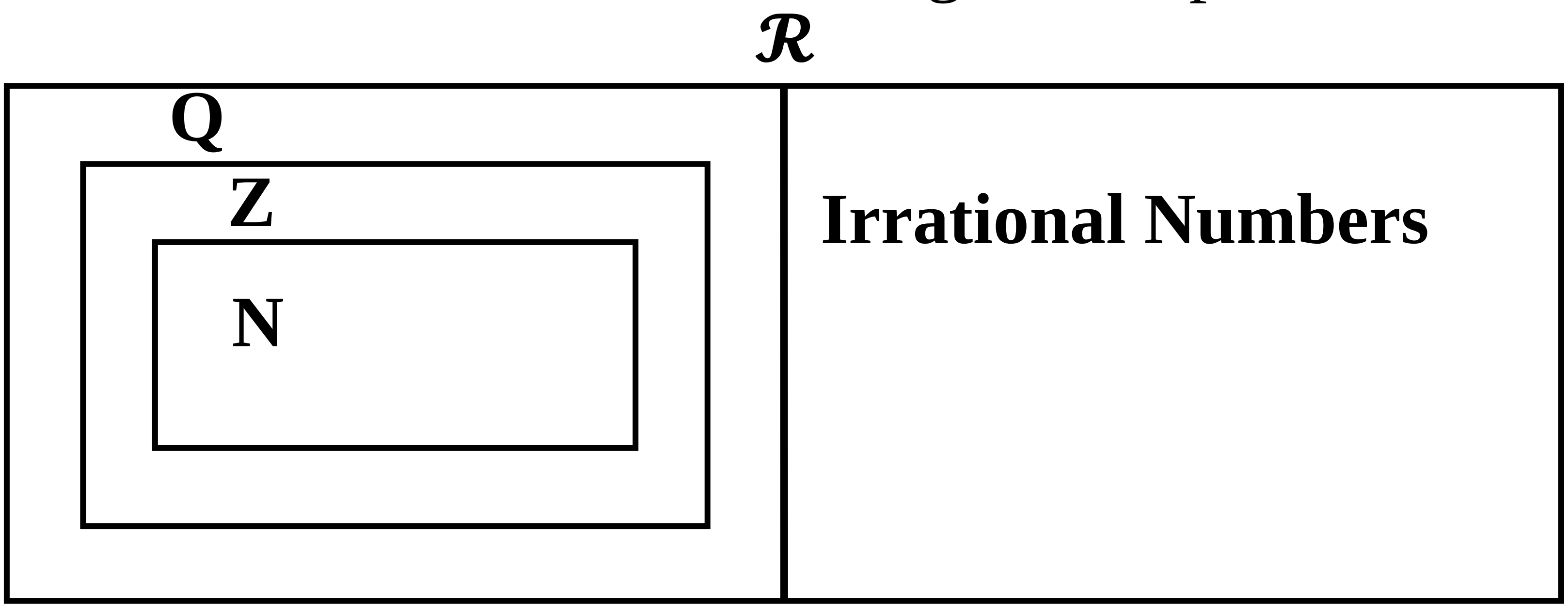
- Logic and Proofs
- Mathematical Induction
- Sequences and Recursion
- Set Theory (used in software engineering and databases)
- Functions
- Relations
- Counting and Probability (used in artificial intelligence, machine learning, and networking)
- Graph theory (used in networks, operating systems, and compilers)
- Trees
- Machine Learning (Tentative)

Today’s Lecture

- **Integers:**
  - Arithmetic Properties
  - Powers
  - Divisibility
  - Primes of Composite Numbers
- **Rational Numbers**
  - Equivalent fractions
  - Operating with fractions
  - Decimals
- **Irrational Numbers**
- **Real Numbers**
  - Square roots
  - N-th roots
  - Logarithms
  - Inequalities
- **Oder of Operations**

Numbers

- **N**= {1,2,3, . . .} The set of Natural Numbers
- **Z**= {. . . , -2,-1,0,1,2, . . .} The set of Integers
- **Q**= {p/q | p ϵ Z, and q ≠ 0} The set of rational numbers
- $\mathcal{R}$, the set of real number. e.g. Real Space



Integers

- **Simple rule of Addition**

  - For an integer a,
  - $0+a = a+0=a$
  - $a+(-a)=0$, and $(-a)+a=0$
  - -a is the **additive inverse** of a.

We use "**Minus a**" rather than "**Negative a**"

Integers

- **Rules of Addition**
  - **Commutativity**
    - If a and b are integers, then
      - $a + b = b + a$
  - **Associativity**
    - If a , b and c are integers, then
    - $(a + b) + c = a + (b + c)$

Integers

❑ Rules of Addition

- If $a + b = 0$, then $b = -a$ and $a = -b$

- Proof

$$a + b = 0$$

Add $-a$ to both sides

$$-a + a + b = 0 - a$$

$$0 + b = 0 - a$$

$$\mathbf{b = -a}$$

As desired.

Similarly we can find ---- $a = -b$

Integers

- **Rules of Addition**
  - If a , b are positive integers, then a + b is also positive integer.
  - If a , b are negative integers, then a + b is also negative integer.

  - If we have the relationship b/w three integers.
    - $a + b = c$

  Then we can drive other relationships b/w them.

  $$\mathbf{a = c - b} \qquad \mathbf{b = c - a}$$

- Example: Solve for x.

$$\mathbf{x + 3 = 5}$$
$$\mathbf{x = 5 - 3}$$
$$\mathbf{x = 2}$$

Integers

- **Rules of Addition**

  - Cancellation rule for addition

    - If $a + b = a + c$, then $b = c$

Exercise:

Prove that if $a + b = a$, then $b = 0$?

Integers

- **Rules of Multiplication**

  - **Commutativity**

    - If a and b are integers, then
      - $a * b = b * a$

  - **Associativity**

    - If a , b and c are integers, then
      - $(a * b) * c = a * (b * c)$

  - For any integer a
    - $1 * a = a$ and $0 * a = 0$

Integers

- **Rules of Multiplication**

  - **Distributivity**

    - **a * (b + c) = a * b + a * c**
    - **(b + c) * a = b * a + c * a**

    Using all these properties

    - **-1 * a = -a**
    - **-(a * b) = (-a) * (b) or -(a * b) = a * (-b)**
    - **(-a) * (-b) = a * b**

Integers

- **Powers**
  - An exponent is used to indicate repeated multiplication.
  - Tells how many times the base is used as a factor.
    - $\mathbf{a * a = a^2}$
    - $\mathbf{a * a * a = a^3}$

In general if n is a positive integer,

- $\mathbf{a^n = a * a * a \ldots a}$ (product is taken n times)

We say a^n is the n-th power of a.

If m , n are positive integers, then

- $\mathbf{a^{m+n} = a^m * a^n}$

Integers

❑ Powers

- $(a^m)^n = a^{m * n}$

Some important formulas

- $(a + b)^2 = a^2 + b^2 + 2ab$
- $(a - b)^2 = a^2 + b^2 - 2ab$
- $(a + b)(a - b) = a^2 - b^2$

Integers

❑ Even and Odd integers

- ❑ An even integer is an integer which can be written in the form **2n** for some integer **n**
  - $2 = 2 * 1$
  - $4 = 2 * 2$
  - $6 = 2 * 3$
- ❑ An odd integer is an integer that differs from an even integer by 1.
- ❑ It can be written in the form **2m ± 1** for some integer **m.**
  - $1 = (2 * 1) - 1$
  - $3 = (2 * 2) - 1$
  - $7 = (2 * 3) + 1$

Integers

- **Theorem**

  - Let a , b be integers,

    - If a is even and b is also even, then a + b is also even

    - If a is even and b is odd, then a + b is odd

    - If a is odd and b is even, then a + b is odd

    - If a is odd and b is also odd, then a + b is also even

  - **Exercise.**

    - Let’s prove the Second statement ??

Integers

- **Divisibility**

  - Given two integers a and b, with $a \neq 0$, we say that **a divides b**, or that **b is divisible by a** if there is an integer c, such that **b = a * c**.

  - Remember that every integer is divisible by 1 because we can always write

    - $n = 1 * n$

- Also, every positive integer is divisible by itself.

Rational Numbers

- By a rational numbers, we mean a fraction as $\boldsymbol{\frac{m}{n}}$,

  where m and n are integers, n ≠ 0.

  - m is called numerator
  - n is called denominator

- Improper fraction

  - m larger than or equal to n

- Proper fraction

  - m smaller than n

Rational Numbers

Equivalent Fractions

- Two fractions that represent the same value.

  - $\frac{1}{2} = \frac{2}{4}$

    How can we know whether two fractions are equivalent?

- Rule for cross-Multiplication

  - Let m ,n ,r ,s be integers and assume that n $\neq 0$ and s $\neq 0$. Then

  - $\left(\frac{m}{n}\right) = \left(\frac{r}{s}\right)$, iff m * s = r * n

Rational Numbers

❑ Simplifying Fractions

- ❑ We can simplify four special fractions forms
  - ❑ Fractions that have the same numerator and denominator.
    - $1 = \frac{1}{1} = \frac{2}{2} = \frac{3}{3} = \frac{4}{4} = \ ...$
  - ❑ Fractions that have a denominator of 1.
    - $\frac{5}{1} = 5,\ \frac{24}{1} = 24,\ \frac{-6}{1} = -6$
  - ❑ Fractions that have a numerator of 0.
    - $\frac{0}{8} = 0,\ \frac{0}{71} = 0,\ \frac{0}{-10} = 0$
  - ❑ Fractions that have a denominator of 0
    - $\frac{7}{0} = \infty,\ \frac{-17}{0} = \infty,$ (∞=Infinity=Undefined Value)

Rational Numbers

- **Simplifying Fractions**
  - Cancellation Rule for Fractions
    - Let a be a non-zero integer. Let m , n be integers, and n $\neq$ 0, then
      - $\frac{am}{an} = \frac{m}{n}$
    - Proof: By applying the rule for cross-multiplication and using the associativity and commutativity laws.

Rational Numbers

- **Simplifying Fractions**

  - A fraction is in **simplest form** when the numerator and denominator have no common factors (or divisors) other than 1.

  - Theorem:

    - "Any positive rational number has an expression as a fraction in the lowest form."

Rational Numbers

- **Operating with Fractions**

  - Addition (or Subtraction) with same denominator.

    - $\frac{\mathrm{a}}{\mathrm{d}} + \frac{\mathrm{b}}{d} = \frac{\mathrm{a+b}}{\mathrm{d}}$ **<u>or</u>** $\frac{\mathrm{a}}{\mathrm{d}} - \frac{\mathrm{b}}{d} = \frac{\mathrm{a-b}}{\mathrm{d}}$

  - With different denominator:

    - $\frac{\mathrm{m}}{\mathrm{n}} + \frac{\mathrm{r}}{s} = \frac{\mathrm{ms+rn}}{\mathrm{ns}}$ **<u>or</u>** $\frac{\mathrm{m}}{\mathrm{n}} - \frac{\mathrm{r}}{s} = \frac{\mathrm{ms-rn}}{\mathrm{ns}}$

    - Follows the same basic rules as addition of integers (commutativity and association)

Rational Numbers

- **Multiplication:**

  - Let $a = \frac{\mathrm{m}}{\mathrm{n}}$

    - Then for any positive integer k, such that

    - $a^k = \left(\frac{m}{n}\right)^k = \frac{m^k}{n^k}$

  - Follows the same basic rules as multiplication of integers.

Rational Numbers

- **Division:**

  - If a is a rational number and $a \neq 0$, then there exists (∃) a rational number, denoted by

    - a^{-1} such that

    - $a^{-1} * a = a * a^{-1} = 1$

  - Note that if $a = \frac{m}{n}$ then $a^{-1} = \frac{n}{m}$

  - a^{-1} is called the multiplicative inverse of a.

Rational Numbers

Decimals:

- Finite decimals (and periodic) give us examples of rational numbers.

  - $1.4 \;=\; \frac{14}{10}$
  - $1.41 = \frac{141}{100}$
  - $0.2 \;=\; \frac{1}{5}$
  - $0.75 \;=\; \frac{3}{4}$
  - $0.3333 = 0.\overline{3} \;=\; \frac{4}{3}$
  - $\ldots$

Irrational Numbers

- A number that cannot be expressed as fraction of $\frac{p}{q}$ for any integers p and q.

  - Have decimal expressions that neither terminate nor become periodic

    - $\sqrt[2]{2} = 1.41421356237\ldots$
    - $\sqrt[2]{3} = 1.73205080757\ldots$
    - $\pi = 3.14159265359\ldots$
    - $\ldots$

Irrational Numbers

- Is $\sqrt[2]{25}$ an irrational number?
  - No!
  - Because $\sqrt[2]{25} = \pm 5$
- Is $\sqrt[2]{-1}$ an irrational number?
  - No or Yes??? In both cases HOW?

Real Numbers

- Integers, Rational and Irrational Numbers are part of a larger system.

- Real Numbers can be described as all the numbers that consist of a decimal expansion, possibly infinite.

Real Numbers

- **Properties of Real Numbers:**
  - Addition:
    - a + b = b + a
    - a + (b + c) = (a + b) + c
    - For all (∀) real numbers a, b, and c.
  - Multiplication
    - a * b = b * a
    - a * (b * c) = (a * b) * c
    - ∀ real numbers a, b , c.
  - Also
    - a * (b + c) = a * b + a * c
    - (b + c) * a = b * a + c * a

Real Numbers

- **Absolute Value**

  - The non-negative values of a real number without regard to it sign.

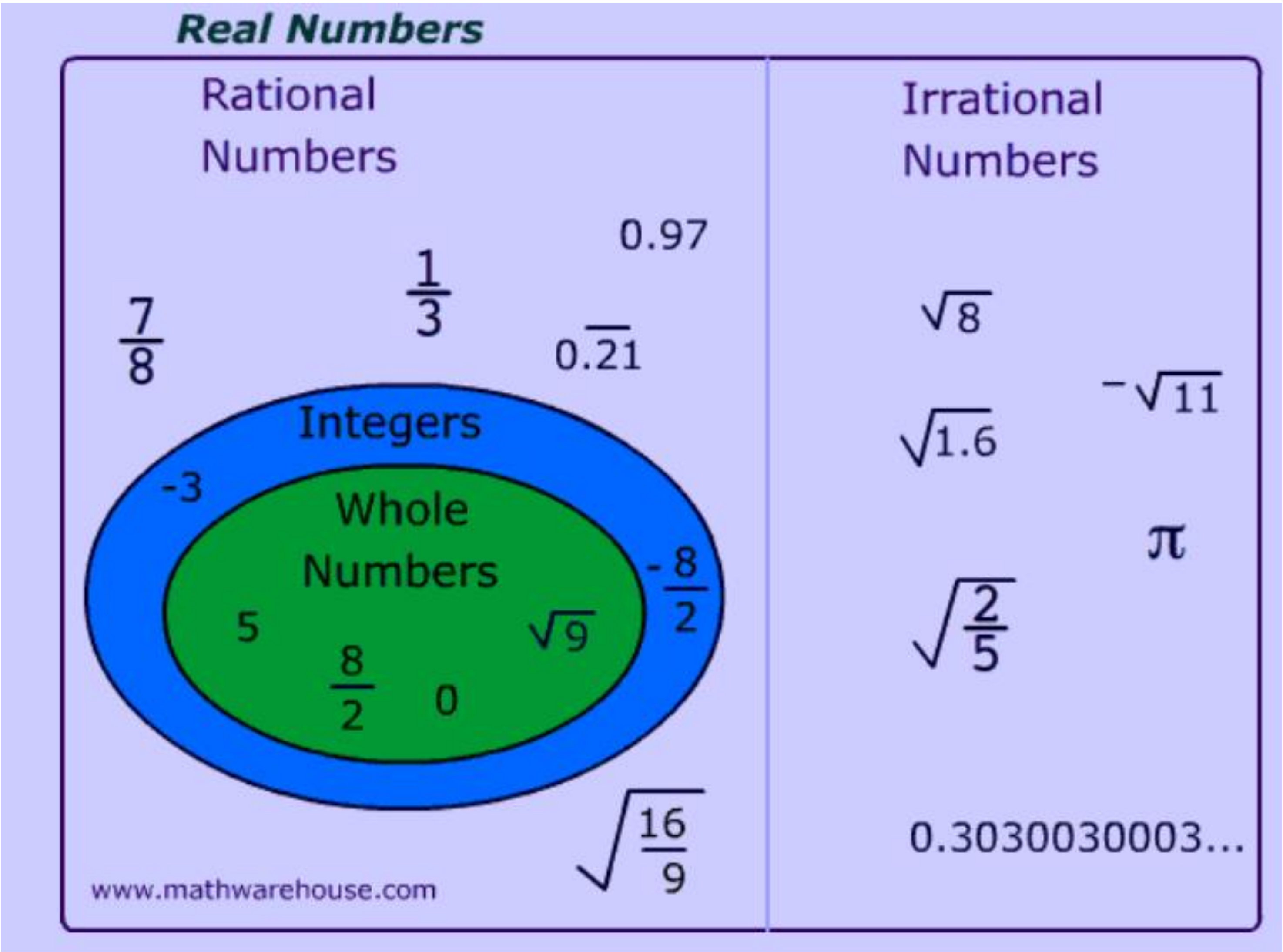
    - $|a| = a$ for a positive a.
    - $|a| = -a$ for a negative a
      (in which case –a is positive).
    - $|0| = 0$

Real Numbers

- **Square Roots**
  - If a > 0, then there exists (∃) a number b such that (s.t).
    - $b^2 = a$
- **N-th Roots**
  - There exists a unique real number r such that
    - $r^n = a$

      It is called the n-th root of a, and is denoted by
    - $a^{1/n}$ or $\sqrt[n]{a}$

Real Numbers



Logarithms

- Can be seen as the reverse operation of the exponentiation.
- The logarithm of a number is the exponent to which another fixed value, the **Base** must be raised to produce that number.
  - $\log_{10}(10000) = 4$, because 10^4=10000
  - $\log_{2}(16) = 4$, because 2^4=16
  - $\log_{3}\left(\frac{1}{3}\right) = -1$, because 3^{-1}= $\frac{1}{3}$

Logarithms

- **Properties of Logarithms:**
  - Product:
    - $\log_b(x * y) = \log_b(x) + \log_b(y)$
  - Quotient:
    - $\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y)$
  - Power:
    - $\log_b(x^p) = p * \log_b(x)$
  - Change of Base:
    - $\log_b(x) = \frac{\log_k(x)}{\log_k(b)}$

Inequalities

Symbol	Meaning	Example
$>$	Greater Than	$(X + 3) > 2$, for any X
$<$	Less Than	$(7X) < 28$, $X= \{\ldots, -2, -1, 0 , 1 , 2 , 3\}$
$\geq$	Greater Than or Equal	$5 \geq (X - 1)$, $X= \{\ldots, -2, -1, 0, 1, \ldots, 5 ,6\}$
$\leq$	Less Than or Equal	$(2Y + 1) \leq 7$, $Y= \{\ldots, -2, -1, 0, 1, 2, 3\}$

❑ Let a, b, c be real numbers,

- If $a > b$ and $b > c$ then $a > c$. (Transitivity)
- If $a > b$ and $c > 0$ then $a*c > b*c$.
- If $a > b$ and $c < 0$ then $a*c < b*c$.

Week#1 →Lecture # 2

Today’s Topic

The Foundations: Logic, Proposition, Predicate, Definitions

Truth Tables and Negation, OR, AND operators with examples

Exclusive Or with Examples

Logical Equivalence with Examples

De-Morgan’s Law with Examples

Tautology with Examples

Contradiction with Examples

Laws of Logic (Homework)!

The Foundations: Logic

- **Mathematical Logic** is a tool for working with compound statements

- **Logic** is the study of correct reasoning

- **Use of logic**

  - **In mathematics:** to prove theorems

  - **In computer science:** to prove that programs do what they are supposed to do

Propositional Logic

- Propositional logic: It deals with **propositions**.

- Predicate logic: It deals with **predicates**.

Definition of a Proposition

<u>Definition</u>: A **proposition** (usually denoted by *p*, *q*, *r*, …) is a declarative statement that is either **True** (T) or **False** (F), but not both or somewhere "in between!".

Propositional Variables

- Variables that represent propositions
- Conventional letters are : p, q, r, s, . . .
- Truth values: T(true), F(false)

Note: Commands and questions are not propositions.

Examples of Propositions

The following are **all** propositions:

- “It is raining” (In a given situation)
- “Amman is the capital of Jordan”
- “1 + 2 = 3” or "2+2 = 3”
- Two plus two is equal to four.
- Toronto is the capital of Canada.
- etc.

Examples of Propositions

But, the following are **NOT** propositions:

- "Who's there?" (Question)
- "La la la la la." (Meaningless)
- "Just do it!" (Command)
- "1 + 2" (Expression with a non-true/false value)
- "$1 + 2 = x$" (Expression with unknown value of x)

Operators / Connectives

An **operator** or **connective** combines one or more **operand** expressions into a larger expression. (e.g., "+" in numeric expression.)

- **Unary** operators take 1 operand (e.g. -3);
- **Binary** operators take 2 operands (e.g. 3×4).
- **Propositional** or **Boolean** operators operate on propositions (or their truth values) instead of on numbers.

Compound Statement (Propositions)

- Complicated logical statements build out of simple ones
- Three Symbols
  - ~ (not) --- ~ p (not p)
  - Λ (and) --- pΛq (p and q)
  - V (or) --- pVq (p or q)
- ~ p (Negation), pΛq (Conjunction), pVq (Disjunctions)
- English words to logic
  - "p but q" means "p and q"
  - "neither p nor q" means "~ p and ~ q"

Some Popular Boolean Operators

Formal Name	Nickname	Arity	Symbol
Negation operator	NOT	Unary	$\neg$
Conjunction operator	AND	Binary	$\wedge$
Disjunction operator	OR	Binary	$\vee$
Exclusive-OR operator	XOR	Binary	$\oplus$
Implication operator	IMPLIES	Binary	$\rightarrow$
Biconditional operator	IFF	Binary	$\leftrightarrow$

The Negation Operator

Definition: Let p be a proposition then $\neg p$ is the **negation** of p (Not p , it is not the case that p).

e.g. If p = "London is a city"

then $\neg p$ = "London is **not** a city" or " it is not the case that London is a city"

The **truth table** for NOT:

p	$\neg p$
F	T
T	F

Operand column

Result column

T :≡ True; F :≡ False
":≡" means "is defined as".

Examples

1. Let p = “Ahmad’s PC runs Linux”
   - ~ p ?
2. Let H = “It is hot”

   S= “It is Sunny”

   (i). “It is not hot but it is Sunny”

   “__________________”

   (ii). “It is neither hot nor Sunny”

   “__________________”

The Conjunction Operator

<u>Definition</u>: Let p and q be propositions, the proposition "p **AND** q" denoted by ($p \wedge q$) is called the **conjunction** of p and q.

The **conjunction of the statements P** and **Q** is the statement "**P and Q**" and its denoted by **P ∧ Q**. The statement **P ∧ Q** is true only when both P **and** Q are true.

e.g. If p = "I will have salad for lunch" and

q = "I will have steak for dinner", then

$p \wedge q$ = "I will have salad for lunch **and** I will have steak for dinner"

Remember: "$\wedge$" points up like an "A", and it means "AND"

Conjunction Truth Table

- Note that a conjunction $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ of n propositions will have 2^n rows in its truth table.

"And", "But", "In addition to", "Moreover". Ex: The sun is shining but it is raining

Operand columns

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

The Disjunction Operator

<u>Definition</u>: Let p and q be propositions, the proposition "p **OR** q" denoted by $(p \vee q)$ is called the **disjunction** of p and q.

The disjunction of the statements **P** and **Q** is the statement "**P or Q**" and its denoted by **P ∨ Q**. The statement **P ∨ Q** is true only when at least one of P or Q is true.

e.g. p = "My car has a bad engine"

q = "My car has a bad carburetor"

$p \vee q$ = "Either my car has a bad engine **or** my car has a bad carburetor"

Disjunction Truth Table

- Note that $p \vee q$ means that p is true, or q is true, **or both** are true!

- So, this operation is also called **inclusive or**, because it **includes** the possibility that both p and q are true.

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

Note the differences from AND

Takeaway

- Rather memorizing, it is easier to remember the rules summarized.

Operator	Symbolic	Summary of Truth Values
Conjunction	$P \land Q$	True only when both P and Q are true
Disjunction	$P \lor Q$	False only when both P and Q are false
Negation	(~ or ┐) ~P	Opposite truth value of P

Compound Statements

- Let p, q, r be simple statements. We can form other compound statements, such as
  - $(p \lor q) \land r$
  - $p \lor (q \land r)$
  - $\neg p \lor \neg q$
  - $(p \lor q) \land (\neg r \lor s)$
  - and many others…

Truth Table – Example

- Lets try to build table for

1. **$\sim P \land Q$**
2. **$\sim P \land (Q \lor \sim P)$**
3. **$(P \lor Q) \land \sim(P \land Q)$**
4. **$\sim(\sim P)$**

P	**Q**	**$\sim P$**	**$\sim P \land Q$**
T	T		
T	F		
F	T		
F	F		

Truth Table – Example – Cont..

- Lets try to build table for

1. **~P ∧ Q**

P	Q	~P	~P ∧ Q
T		F	
T		F	
F		T	
F		T	

Truth Table – Example – Cont..

- Lets try to build table for

1. ~P ∧ Q

P	Q	~P	~P ∧ Q
	T	F	F
	F	F	F
	T	T	T
	F	T	F

Truth Table – Example – Cont..

- Lets try to build table for

1. $\sim P \land Q$

P	**Q**	**~P**	**$\sim P \land Q$**
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	F

Truth Table – Example – $(p \vee q) \wedge r$

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

Truth Table – Example – Cont.. $(p \vee q) \wedge r$

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

Truth Table – Example

1. $\sim P \land (Q \lor \sim R)$

P	Q	R	~R	Q ∨ ~R	~P	~P ∧ (Q ∨~R)
T	T	T				
T	T	F				
T	F	T				
T	F	F				
F	T	T				
F	T	F				
F	F	T				
F	F	F				

Truth Table – Example – Cont..

1. $\sim P \wedge (Q \vee \sim R)$

P	Q	R	~R	Q ∨ ~R	~P	~P ∧ (Q ∨~R)
		T	F			
		F	T			
		T	F			
		F	T			
		T	F			
		F	T			
		T	F			
		F	T			

Truth Table – Example – Cont..

1. ~P ∧ (Q ∨~R)

P	Q	R	~R	Q ∨ ~R	~P	~P ∧ (Q ∨~R)
	T		F	T		
	T		T	T		
	F		F	F		
	F		T	T		
	T		F	T		
	T		T	T		
	F		F	F		
	F		T	T		

Truth Table – Example – Cont..

1. $\sim P \land (Q \lor \sim R)$

P	Q	R	~R	Q ∨ ~R	~P	~P ∧ (Q ∨~R)
T					F	
T					F	
T					F	
T					F	
F					T	
F					T	
F					T	
F					T	

Truth Table – Example – Cont..

1. **~P ∧ (Q ∨~R)**

P	Q	R	~R	Q ∨ ~R	~P	~P ∧ (Q ∨~R)
				T	F	F
				T	F	F
				F	F	F
				T	F	F
				T	T	T
				T	T	T
				F	T	F
				T	T	T

Truth Table – Example – Cont..

1. ~P ∧ (Q ∨~R)

P	Q	R	~R	Q ∨ ~R	~P	~P ∧ (Q ∨~R)
T	T	T	F	T	F	F
T	T	F	T	T	F	F
T	F	T	F	F	F	F
T	F	F	T	T	F	F
F	T	T	F	T	T	T
F	T	F	T	T	T	T
F	F	T	F	F	T	F
F	F	F	T	T	T	T

Truth Table – Example – Cont..

1. $(P \lor Q) \land \sim(P \land Q)$

P	Q	$P \lor Q$	$P \land Q$	$\sim(P \land Q)$	$(P \lor Q) \land \sim(P \land Q)$
T	T				
T	F				
F	T				
F	F				

Truth Table – Example – Cont..

1. **$(P \lor Q) \land \sim(P \land Q)$**

P	Q	$P \lor Q$	$P \land Q$	$\sim(P \land Q)$	$(P \lor Q) \land \sim(P \land Q)$
T	T	T			
T	F	T			
F	T	T			
F	F	F			

Truth Table – Example – Cont..

1. $(P \lor Q) \land \sim(P \land Q)$

P	Q	$P \lor Q$	$P \land Q$	$\sim(P \land Q)$	$(P \lor Q) \land \sim(P \land Q)$
T	T		T		
T	F		F		
F	T		F		
F	F		F		

Truth Table – Example – Cont..

1. $(P \vee Q) \wedge \sim(P \wedge Q)$

P	**Q**	**$P \vee Q$**	**$P \wedge Q$**	**$\sim(P \wedge Q)$**	**$(P \vee Q) \wedge \sim(P \wedge Q)$**
T	T		T	F	
T	F		F	T	
F	T		F	T	
F	F		F	T	

Truth Table – Example – Cont..

1. **$(P \lor Q) \land \sim(P \land Q)$**

P	Q	$P \lor Q$	$P \land Q$	$\sim(P \land Q)$	$(P \lor Q) \land \sim(P \land Q)$
T	T	T		F	F
T	F	T		T	T
F	T	T		T	T
F	F	F		T	F

Truth Table – Example – Cont..

1. $(P \vee Q) \wedge \sim(P \wedge Q)$

P	**Q**	**$P \vee Q$**	**$P \wedge Q$**	**$\sim(P \wedge Q)$**	**$(P \vee Q) \wedge \sim(P \wedge Q)$**
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

A Simple Exercise

Let p = "It rained last night",
q = "The sprinklers came on last night" ,
r = "The grass was wet this morning".

Translate each of the following into English:

$\neg p$ =

$r \wedge \neg p$ =

$\neg r \vee p \vee q$ =

A Simple Exercise

Let p = "It rained last night",
q = "The sprinklers came on last night" ,
r = "The grass was wet this morning".

Translate each of the following into English:

$\neg p$ = **"It didn't rain last night"**

$r \wedge \neg p$ = **"The grass was wet this morning, and it didn't rain last night"**

$\neg r \vee p \vee q$ = **"Either the grass wasn't wet this morning, or it rained last night, or the sprinklers came on last night"**

The Exclusive Or Operator

The binary **exclusive-or** operator "$\oplus$" (XOR) combines two propositions to form their logical "exclusive or" (exjunction?).

e.g. p = "I will earn an A in this course"

q = "I will drop this course"

$p \oplus q$ = "I will either earn an A in this course, **or** I will drop it (but not both!)"

Exclusive-Or Truth Table

- Note that $p \oplus q$ means that p is true, or q is true, but **not both**!
- This operation is called **exclusive or**, because it **excludes** the possibility that both p and q are true.

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

Note the difference from OR

Natural Language is Ambiguous

Note that <u>English</u> “or” can be <u>ambiguous</u> regarding the “both” case!

> “Justin Bieber is a singer or
> Justin Bieber is a writer” $\vee$
>
> “John Cena is a man or
> John Cena is a woman” $\oplus$

Need context to disambiguate the meaning!

For this class, assume “OR” means <u>inclusive</u>.

Logical Equivalence

- Two statement forms are called logically equivalent if and only if, they have identical truth values for all possible truth values for their statement variables.

- The logical equivalence of statement forms P and Q is denoted by writing $P \equiv Q$.

Truth Table – Example – Cont..

1. $\sim(\sim P) \equiv P$

P	**~P**	**~(~P)**
T	F	T
F	T	F

Same Truth Values in 1st and 3rd row

De Morgan's Laws

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

- Symbolically:

$$\sim(P \wedge Q) \equiv \sim P \vee \sim Q \text{ and } \sim(P \vee Q) \equiv \sim P \wedge \sim Q$$

De Morgan's Laws – Example – 1

- Prove $\sim(\boldsymbol{P} \land \boldsymbol{Q}) \equiv \sim\boldsymbol{P} \lor \sim\boldsymbol{Q}$

P	Q	~P	~Q	P ∨ Q	~(P ∨ Q)	~P ∧ ~Q
T	T					
T	F					
F	T					
F	F					

De Morgan's Laws – Example – 1

- Prove $\sim(\boldsymbol{P} \land \boldsymbol{Q}) \equiv \sim\boldsymbol{P} \lor \sim\boldsymbol{Q}$

P	**Q**	**~P**	**~Q**	**P ∨ Q**	**~(P ∨ Q)**	**~P ∧ ~Q**
T	T	F	F			
T	F	F	T			
F	T	T	F			
F	F	T	T			

De Morgan's Laws – Example – 1

- Prove $\sim(\boldsymbol{P} \wedge \boldsymbol{Q}) \equiv \sim\boldsymbol{P} \vee \sim\boldsymbol{Q}$

P	Q	~P	~Q	P ∨ Q	~(P ∨ Q)	~P ∧ ~Q
T	T	F	F	T	F	
T	F	F	T	T	F	
F	T	T	F	T	F	
F	F	T	T	F	T	

De Morgan's Laws – Example – 1

- Prove $\sim(\boldsymbol{P} \wedge \boldsymbol{Q}) \equiv \sim\boldsymbol{P} \vee \sim\boldsymbol{Q}$

P	Q	~P	~Q	P ∨ Q	~(P ∨ Q)	~P ∧ ~Q
T	T	F	F			F
T	F	F	T			F
F	T	T	F			F
F	F	T	T			T

De Morgan's Laws – Example – 1

- Prove $\sim(P \wedge Q) \equiv \sim P \vee \sim Q$

P	**Q**	**~P**	**~Q**	**P ∨ Q**	**~(P ∨ Q)**	**~P ∧ ~Q**
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

De Morgan's Laws – Example – 2

- Prove $\sim(P \land Q)$ ***and*** $\sim P \land \sim Q$ are not equivalent

P	Q	~P	~Q	P ∧ Q	~(P ∧ Q)	~P ∧ ~Q
T	T	F	F			
T	F	F	T			
F	T	T	F			
F	F	T	T			

De Morgan's Laws – Example – 2

- Prove $\sim(P \wedge Q)$ *and* $\sim P \wedge \sim Q$ are not equivalent

P	Q	~P	~Q	P ∧ Q	~(P ∧ Q)	~P ∧ ~Q
T	T			T		
T	F			F		
F	T			F		
F	F			F		

De Morgan's Laws – Example – 2

- Prove $\sim(P \wedge Q)$ ***and*** $\sim P \wedge \sim Q$ are not equivalent

P	**Q**	**~P**	**~Q**	**P ∧ Q**	**~(P ∧ Q)**	**~P ∧ ~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

Exercise – 1

- Are the statements $(\boldsymbol{P} \wedge \boldsymbol{Q}) \wedge \boldsymbol{R}$ and $\boldsymbol{P} \wedge (\boldsymbol{Q} \wedge \boldsymbol{R})$ logically equivalent?

- Are the statements $(\boldsymbol{P} \wedge \boldsymbol{Q}) \vee \boldsymbol{R}$ and $\boldsymbol{P} \wedge (\boldsymbol{Q} \vee \boldsymbol{R})$ logically equivalent?

Tautology

- A tautology is a statement from that is always true regardless of the truth values of the statement variables.

- A tautology is represented by the symbol “t”.

Tautology – Example

- The statement $P \lor {\sim}P$ is Tautology.

$P \lor {\sim}P \equiv t$		
P	~P	P ∨~P
T	F	T
F	T	T

Contradiction

- A contradiction is a statement from that is always false regardless of the truth values of the statement variables.

- A contradiction is represented by the symbol “c”.

Contradiction – Example

- The statement $P \wedge \sim P$ is Contradiction.

$$P \wedge \sim P \equiv c$$

P	~P	P ∧~P
T	F	F
F	T	F

Example – 1

$$(P \wedge Q) \vee (\sim P \vee (P \wedge \sim Q)) \equiv t$$

P	**Q**	**~P**	**~Q**	**P ∧ Q**	**P ∧ ~Q**	**~P ∨ (P ∧ ~Q)**	**(P ∧ Q) ∨ (~P ∨ (P ∧ ~Q))**
T	T	F	F	T	F	F	**T**
T	F	F	T	F	T	T	**T**
F	T	T	F	F	F	T	**T**
F	F	T	T	F	F	T	**T**

Example – 2

$$(P \wedge \sim Q) \wedge (\sim P \vee Q) \equiv c$$

P	**Q**	**~P**	**~Q**	**P ∧ ~Q**	**~P ∨ Q**	**(P ∧ ~Q) ∧ (~P ∨ Q)**
T	T	F	F	F	F	**F**
T	F	F	T	T	F	**F**
F	T	T	F	F	T	**F**
F	F	T	T	F	T	**F**

Laws of Logic

Commutative Law: $P \wedge Q \equiv Q \wedge P$ and $P \vee Q \equiv Q \vee P$

Associative Law: $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$ and $(P \vee Q)$

Distributive Law: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (Q \wedge R)$ and $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (Q \vee R)$

Identity Law: $P \wedge t \equiv P$ and $P \vee c \equiv P$

Negation Law: $P \vee \sim P \equiv t$ and $P \wedge \sim P \equiv c$

Double Negation Law: $\sim(\sim P) \equiv P$

Idempotent Law: $P \wedge P \equiv P$ and $P \vee P \equiv P$

DeMorgan's Law: $\sim(P \wedge Q) \equiv \sim P \vee \sim Q$ and $\sim(P \vee Q) \equiv \sim P \wedge \sim Q$

Universal Bound Law: $P \vee t \equiv t$ and $P \wedge c \equiv c$

Absorption Law: $P \vee (P \wedge Q) \equiv P$ and $P \wedge (P \vee Q) \equiv P$

Negations of "t" and "c": $\sim t \equiv c$ and $\sim c \equiv t$

Proving Equivalence via Truth Tables

Example: Prove that $p \vee q$ and $\neg(\neg p \wedge \neg q)$ are logically equivalent.

p	q	p∨q	~p	~q	~p∧~q	~(~p∧~q)
F	F	F	T	T	T	F
F	T	T	T	F	F	T
T	F	T	F	T	F	T
T	T	T	F	F	F	T