Discrete

- Logic: Study of principles / methods that distinguish b/w a valid / invalid argument
- Discrete: Anything that can take distinct values, clear gaps b/w values
- proposition: A declarative sentence i.e either True or False
- continuous: Anything that can take any value, no clear gap b/w values

e.g: Grass is green
$4+2=6$

NOT ≠
- x is greater than 2
- close The Door
- He is very rich

] Unknowns / vagueness present

- Logical connectives

- Negation / NOT : $\sim$, $\neg$
- Conjunction / AND : $\wedge$
- Disjunction / OR : $\vee$
- conditional : $\rightarrow$
- Biconditional : $\leftrightarrow$

e.g: p = It is hot , q = It is sunny

a. It is not hot but sunny
$\neg p \wedge q$

Properties

- Negation of 'OR' is 'and', vice versa

- $\sim(p \wedge q) \equiv \neg p \vee \neg q$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$

] De morgan's Law

a. $-1 < x \le 4 \implies x > -1$ and $x \le 4$
$\rightarrow x \le -1$ or $x > 4$

- commutative
- $p \wedge q \equiv q \wedge p$
- $p \vee q \equiv q \vee p$

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

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

- Identity Law
- $p \wedge t \equiv p$
- $p \vee c \equiv p$

- Negation Laws
- $p \vee \sim p \equiv t$
- $p \wedge \sim p \equiv c$

- Double - Negation Law:
$\sim(\sim p) \equiv p$

- Logical equivalency using TT or Laws

- Tautology when always true (t)
- contradiction when always false (c)
- $\sim t \equiv c$
- $\sim c \equiv t$
- An expression is satisfiable if it results in at least one T, else unsatisfiable

- Idempotent Laws
- $p \wedge p \equiv p$
- $p \vee p \equiv p$

- De-morgan's Law
- $\sim(p \vee q) \equiv \sim p \wedge \sim q$
- $\sim(p \wedge q) \equiv \sim p \vee \sim q$

- Universal Bound Law:
- $p \vee t \equiv t$
- $p \wedge c \equiv c$

- Absorption Laws
- $p \vee (p \wedge q) \equiv p$
- $p \wedge (p \vee q) \equiv p$

- Negation of t and c
- $\sim t \equiv c$
- $\sim c \equiv t$

Conditional

- If p, then q $\equiv p \to q$
  p implies q

p: hypothesis
q: conclusion

$p \to q$

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

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

- Implication Law:
- $p \to q \equiv \sim p \vee q$

- Negation of Conditional
- $p \to q \equiv \sim p \vee q$

$\sim(p \to q) \equiv \sim(\sim p \vee q)$
$\equiv p \wedge \sim q$

- negation of if p, then q is equivalent to p, and not q

Q- If Ali lives in Pakistan, then he lives in Lahore

* can convert into p,q,r form, and then convert

- Ali lives in Pakistan, and he does not live in Lahore

- If n is prime then n is odd or n is 2
- n is prime and n is even and n is not 2
  but

- If n is divisible by 6, then n is divisible by 2. and n is divisible by 3
- n is divisible by 6 but n is not divisible by 2 or by 3

- Implication = contrapositive
- Implication ≠ converse
- Inverse = Converse
- Implication = contrapositive

- Inverse of Conditional
- $p \to q \Rightarrow \sim p \to \sim q$
- Not logically equivalent

Q- If today is Friday, then $2+3=5$
If today is not Friday, then $2+3 \neq 5$

Q- If my car is in repair shop, then I cannot get to the class
If my car is not in repair shop, then I can get to the class

- Converse of a conditional statement
- $p \to q \Rightarrow q \to p$
- conditional and converse not equivalent

- Contrapositive:
- $p \to q \equiv \sim q \to \sim p$
- conditional and contrapositive are equivalent

Exclusive OR

- $p \oplus q \equiv (p \lor q) \land \sim(p \land q)$
  $\equiv \sim(p \leftrightarrow q)$

Bi-conditional

- $p \leftrightarrow q \equiv (p \to q) \land (q \to p)$
- p, if and only if q
- $p \leftrightarrow q \equiv q \leftrightarrow p$
- p iff q $\equiv$ q iff p

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

- p is necessary, and sufficient for q
- If p then q, and conversely
- p is equivalent to q

TABLE 7 Logical Equivalences Involving Conditional Statements.
$p \to q \equiv \neg p \lor q$
$p \to q \equiv \neg q \to \neg p$
$p \lor q \equiv \neg p \to q$
$p \land q \equiv \neg(p \to \neg q)$
$\neg(p \to q) \equiv p \land \neg q$
$(p \to q) \land (p \to r) \equiv p \to (q \land r)$
$(p \to r) \land (q \to r) \equiv (p \lor q) \to r$
$(p \to q) \lor (p \to r) \equiv p \to (q \lor r)$
$(p \to r) \lor (q \to r) \equiv (p \land q) \to r$

TABLE 8 Logical Equivalences Involving Biconditional Statements.
$p \leftrightarrow q \equiv (p \to q) \land (q \to p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \land q) \lor (\neg p \land \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

- Laws

- Commutative
- $p \leftrightarrow q \equiv q \leftrightarrow p$

- Implication Laws
- $p \to q \equiv \sim p \lor q$
- $p \to q \equiv \sim(p \land \sim q)$

- Exporation Law:
- $(p \land q) \to r \equiv p \to (q \to r)$

- Equivalence Law:
- $p \leftrightarrow q \equiv (p \to q) \land (q \to p)$

- Reductio ad absurdum
- $p \to q \equiv (p \land \sim q) \to c$

Arguments

- Argument is a list of premises

→ Argument is valid when conclusion is true, and all premises are true

i.e: $(p_1 \land p_2 \land p_3 \land \dots p_n) \to c$ is a tautology

→ Argument invalid if conclusion is false

- If conjunction false, then argument valid.
- If conjunction true, and conclusion false, then argument invalid

- In truth table see where all premises are T, and the conclusion in them. If conclusion is true in all, then argument is valid, else invalid

TABLE 1 Rules of Inference.		
Rule of Inference	*Tautology*	*Name*
p, $p \to q$, $\therefore q$	$(p \land (p \to q)) \to q$	Modus ponens
$\neg q$, $p \to q$, $\therefore \neg p$	$(\neg q \land (p \to q)) \to \neg p$	Modus tollens
$p \to q$, $q \to r$, $\therefore p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \lor q$, $\neg p$, $\therefore q$	$((p \lor q) \land \neg p) \to q$	Disjunctive syllogism
p, $\therefore p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$, $\therefore p$	$(p \land q) \to p$	Simplification
p, q, $\therefore p \land q$	$((p) \land (q)) \to (p \land q)$	Conjunction
$p \lor q$, $\neg p \lor r$, $\therefore q \lor r$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	Resolution

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

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

Predicates & Quantifiers

- Propositional Funcs
- Existential Quantification → $\exists x$ - need 1 counter example to prove it true
  - need all x values for false

$\exists x\, P(x) \rightarrow (P(x_1) \vee P(x_2) \vee \dots P(x_n))$

- Universal Quantification → $\forall x$ - need 1 counter example to prove it false
  - need all x values for true

$\forall x\, P(x) \rightarrow (P(x_1) \wedge P(x_2) \wedge \dots P(x_n))$

- $\forall\, x<0\,(x^2>0) \;=\; \forall x\,(x<0 \rightarrow x^2>0)$
- $\exists\, z>0\,(z^2=2) \;=\; \exists z\,(z>0 \wedge z^2=2)$

- $\neg \forall x\, C(x) \;=\; \exists x\, \neg C(x)$
- $\neg \exists x\, C(x) = \forall x\, \neg C(x)$

- Proofs de-morgan and stuff

Nested

- Order of quantifiers matter.
- If same quantifiers, then no issue
- Negations, and simplification

Proofs

- contradiction

→ suppose statement is false

→ show that this supposition leads logically to a contradiction

→ conclude the statement is true.

Methods of Proof
- Direct Proof
  - $p \rightarrow q$
- Indirect Proof
  - Contraposition
    - $p \rightarrow q$
    - $\equiv \neg q \rightarrow \neg p$
  - Contradiction
    - $p \rightarrow q \equiv (p \wedge \sim q) \rightarrow c$

- contraposition
- Express in form of if p, then q
- Re-write in form of if not q, then not p
- Prove by direct proof

Sets

- Set Representations:

- Tabular Form $A = \{1,2,3,4,5\}$
- Descriptive Form A = set of first five natural numbers
- Set-Builder Form $A = \{n \in N \mid n \leq 5\}$

- Natural Numbers → $N = \{1,2,3 \dots\}$
- Whole Numbers → $W = \{0,1,2,3 \dots\}$
- Integers → $Z = \{\dots -3,-2,-1,0,1,2,3,\dots\}$
- Even Integers $E = \{0, \pm 2, \pm 4, \pm 6, \dots\}$
- Odd Integers $O = \{\pm 1, \pm 3, \pm 5, \pm 7, \dots\}$
- Boolean Numbers → B = { true, false } (1, 0)
- Prime Numbers → $P = \{2,3,5,7,9,11,13,17,19,\dots\}$
- Rational Numbers → $Q = \{n \mid n = \frac{p}{q} ; p,q \in Z, q \neq 0\}$

- Irrational Numbers → $Q' = \{n \mid n$ is not rational$\}$
- Real Numbers → $R = Q \cup Q'$
- Complex Numbers → $C = \{z \mid z = x + iy ; x,y \in R\}$

- Every element of A is present in B, then $A \subseteq B$, A is a subset of B.
- B is the superset
- Every set is a subset of itself

- $A = \{1,3,5\}$, $B = \{1,2,3,5\}$

- $A \subset B$, A is a proper subset of B, as B's one eleement is not present in A
- If every element present, then equal sets

Power Set - All possible subsets

- Num elements in Power Set $= 2^n$

Q- $A = \{0,1,2\}$

$P(A) = \{\phi, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$

Q- $A = \{\phi\}$

$P(A) = \{\phi, \{\phi\}\}$

Cartesian Product

$x \in \{x\}$	TRUE
$\{x\} \subseteq \{x\}$	TRUE(because every set is subset of itself)
$\{x\} \in \{x\}$	FALSE(because {x} is not a member of {x})
$\{x\} \in \{\{x\}\}$	TRUE
$\varnothing \subseteq \{x\}$	TRUE
$\varnothing \in \{x\}$	FALSE

- $A \times B$
- $A \times B = B \times A$, only if $A = \phi$, and $B = \phi$

Q- $A = \{1,2\}$, $B = \{a,b\}$

$A \times B = \{(1,a), (1,b), (2,a), (2,b)\}$

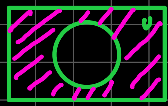
- Finite Sets → Countable
- Infinite Sets → Uncountable

Set Identities, Membership Tables, Venn Diagrams

- A^c

A	A^c
0	1
1	0

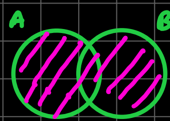
  NOT



- $A^c = U - A$
- $A \cap A^c = \phi$
- $A \cup A^c = U$

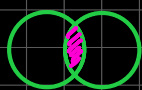
A	B	$A \cup B$
1	1	1
1	0	1
0	1	1
0	0	0

OR



- $A \cup B = B \cup A$
- $A \subseteq A \cup B$, and $B \subseteq A \cup B$

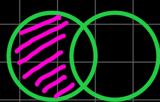
- $A \cap B = B \cap A$
- $A \cap B \subseteq A$, and $A \cap B \subseteq B$
- $A \cap B = \phi$, then disjoint sets



A	B	$A \cap B$
1	1	1
1	0	0
0	1	0
0	0	0

AND

- $A - B$ = Elements which belong to A, but not to B



A	B	$A - B$
1	1	0
1	0	1
0	1	0
0	0	0

- $A - B \neq B - A$
- $A - B \subseteq A$
- $A - B$, $A \cap B$, $B - A$ are mutually disjoint sets
  ↳ no elements in common

- **Idempotent**
- $A \cup A = A$
- $A \cap A = A$

- **Commutative**
- $A \cup B = B \cup A$
- $A \cap B = B \cap A$

- **Associative**
- $A \cup (B \cup C) = (A \cup B) \cup C$
- $A \cap (B \cap C) = (A \cap B) \cap C$

- **Distributive**
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

- **Identity**
- $A \cup \phi = A$ • $A \cap \phi = \phi$
- $A \cup U = U$ • $A \cap U = A$

- **Complement**
- $A \cup A^c = U$ • $U^c = \phi$
- $A \cap A^c = \phi$ • $\phi^c = U$

- **Double Complement**
- $(A^c)^c = A$

- **De-morgan**
- $(A \cup B)^c = A^c \cap B^c$
- $(A \cap B)^c = A^c \cup B^c$

- $A - B = A \cap B^c$

- **Subset Laws**
- $A \cup B \subseteq C$ iff $A \subseteq C$, and $B \subseteq C$
- $C \subseteq A \cap B$ iff $C \subseteq A$, and $C \subseteq B$

- **Absorption Laws**
- $A \cup (A \cap B) = A$
- $A \cap (A \cup B) = A$

Functions

NOT a function

- $a \to 1$
  $b \to 2$
  $c \to 3$
  $d \to 3$, $d \to 4$
  e $\quad 5$

- pre-image = domain
- image = Range
- Codomain = set of all possible output values
- Range = Actual output values

- Horizontal line test to check function validity and bijectivity
- vertical line test to check inverse

- Num of possible functions e.g: $X = \{1,2,3\}$, $Y = \{4,5,6\}$
  $\to 3 \times 3 \times 3$

- For well-defined function if $x_1 = x_2$, then $f(x_1) = f(x_2)$

- One-one / injective function:

$\to$ If $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

Contrapos $\to$ if $f(x_1) = f(x_2)$ then $x_1 = x_2$

NOT one-one

$a \to 1$
$b \to 2$
$c \to 2$
$\quad 3$

- Num of one-one funcs $\to n!$
  $X = \{x_1, x_2, x_3\}$, $Y = \{y_1, y_2\}$ $\to$ no func

- Onto / Surjective function
- $f: X \to Y$ is not onto iff there exists $y \in Y$ such that $\forall x \in X$, $f(x) \neq Y$

NOT onto

$a \to 1$
$b \to 2$
$\quad 3$ Not an image of any element in x
$c \to 4$

- Functions onto and one-one are bijective funcs

- Only inverse of bijective funcs are funcs

sequences

- **Arithmetic**

$a_n = a_0 + (n-1)d$ → 1st term $= a_0$
2nd term $= a+d$
3rd term $= a+2d$
$\vdots$

$S_n = \frac{n}{2}\left(2a + (n-1)d\right)$

$S_n = \frac{n}{2}\left(a + l\right)$

- IQ sequences

- **Geometric:**

- $a_n = ar^n$

1st term → ar
2nd term → ar^2
ar^3
$\vdots$

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

- $S_\infty = \frac{a}{1-r}$

Summation

- Summation expansion

→ $\sum_{i=0}^{n} \frac{(-1)^i}{i+1} = \frac{(-1)^0}{0+1} + \frac{(-1)^1}{1+1} + \frac{(-1)^2}{2+1} \dots \frac{(-1)^n}{n+1}$

$= 1 - \frac{1}{2} + \frac{1}{3} \dots \frac{(-1)^n}{n+1}$

- Summation simplification

a- $\sum_{i=1}^{n-1} \frac{i}{(n-i)^2}$; $j = i-1$

$j = 1-1 = 0$
$j = n-1-1 = n-2$

$= \sum_{0}^{n-2} \frac{1-j}{(n-j-1)^2}$

- **Properties:**

- $\sum_{k=m}^{n} a_k + b_k = \sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k$
- $\sum_{k=m}^{n} ca_k = c\sum_{k=m}^{n} a_k$
- $\sum_{k=a-i}^{b-i} (k+i) = \sum_{k=a}^{b} k$
- $\sum_{k=a-i}^{b-i} (k-i) = \sum_{k=a}^{b} k$
- $\sum_{k=1}^{n} c = c + c \dots c_n = nc$

Ch 4 Divisibility

- $n = d \cdot q + r$ (quotient q, remainder r, divisor d)

quotient = result of divison
divisor = num that divides another num
dividend = num that is being divided

- a is congurent to b modullo m if m divides a-b => $a \equiv b \pmod m$
- 2 integers are congurent mod m iff they have same remainder when divided by m

Q- 17 congurent to 5 modullo 6

- $17 \equiv 5 \pmod 6$ b/c $17-5=\underline{12}$ 6 divides 12

- Theorem 2: Congurence & Equality

- $a \equiv b \pmod m$ can be written as $a = b + km$

Q- $\underbrace{3x}_{a} \equiv \underbrace{5}_{b} \pmod{\underbrace{7}_{m}}$ → can also use inspection

- if $a \bmod m = r$, then $a \equiv r \pmod m$

- $a = b + km$
  $3x = 5 + k(5)$
  $x = \frac{5+5k}{3}$; min value of k · $k=1$, $x=4$

- Identities $a \equiv b \pmod m$, c is an arbitary integer

- $(a+c) \equiv (b+c) \pmod m$
- $(ac) \equiv bc \pmod m$
- $a^p \equiv b^p \pmod m$; p non-negative

Q- $17 \equiv 2 \pmod 3$, $10 \equiv 4 \pmod 3$
→ $17+10 \equiv (2+4) \bmod 3$

- if $a \equiv b \pmod m$, $c \equiv d \pmod m$

- $(a+c) \equiv (b+d) \pmod m$
- $ac \equiv bd \pmod m$

- $a +_m b = (a+b) \bmod m$ – Addition modullo
- $a \cdot_m b = (ab) \bmod m$ – Multiplication modullo

Assosc, Distribute,

- $a +_m (m-a) = 0$, $0 +_m 0 = 0$ m-a is an additive inverse of a modullo m
- $a +_m 0 = 0 +_m a = a$, $a \cdot_m 1 = 1 \cdot_m a = a$ identity

- $(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$
- $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

- GCD = greatest common divisor

- Prime = divisor is p and 1 only
- 2 integers are relatively prime if $\gcd(a,b) = 1$ // common factor = 1

Q- GCD(45, 36)

45 divisors = 1, 3, 5, 9, 15, 45
36 divisors = 1, 2, 3, 4, 6, 9, 12, 18, 36
$\gcd(45, 36) = \underline{9}$