Discrete Maths

Date:

CS 231

DISCRETE MATHEMATICS is the part of mathematics devoted to the study of discrete objects.

⇒ discrete refers to consisting of distinct or unconnected elements.

The kind of problems solved using discrete mathematics include:

- How many ways are there to choose a valid password on a computer system?
- Is there a link between two computers in a network?
- How can I identify spam e-mail messages?
- How can I encrypt a message so that no unintended recipient can read it?
- What is the shortest path between two cities using a transportation system?
- How can a circuit that adds two integers be designed?
- How many valid Internet addresses are there?

Out of all these questions that arise, the most CE-centric is the following:

'How can a circuit that adds two integers be designed?'

↳ ties directly to digital logic design (core of CE).

↳ involves boolean algebra (discrete math backbone).

Date:

- The rules of logic specify the meaning of mathematical statements. For instance, these rules help us understand and reason with statements such as, 'For every positive integer n, the sum of the positive integers not exceeding n is $n(n+1)/2$'. ⇒ e.g. this statement is verified and true: Taking 7 as the positive integer n;

$\therefore n = 7$

$\Rightarrow 1+2+3+4+5+6+7 = 28$ } sum of all numbers not exceeding n

$\Rightarrow \frac{n(n+1)}{2} = \frac{7(7+1)}{2} = \frac{7(8)}{2} = 28$

$\therefore$ verified.

The basic building blocks of logic are propositions.

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

DE MORGAN'S LAWS

Date:

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

} two compound propositions are logically equivalent

$\Rightarrow$ $\wedge$ (AND) - $\times$

$\Rightarrow$ $\vee$ (OR) - $+$

e.g. Use De Morgan's laws to express the negation of :

"Professor Brehm has a dog and she has a pool."

Let p be 'Professor Brehm has a dog' and q 'Professor Brehm has a pool.'

$\therefore \quad p \wedge q$

$\therefore \quad \neg(p \wedge q)$

$\Rightarrow \quad \neg p \vee \neg q$

$\Rightarrow$ Professor Brehm does not have a dog or she does not have a pool.

e.g. $\neg(p \vee (\neg p \wedge q))$ $\Rightarrow$ De Morgan's second law can be applied:

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

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

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

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

$\Rightarrow F \vee (\neg p \wedge \neg q)$

$\Rightarrow (\neg p \wedge \neg q) \vee F$

$\Rightarrow \underline{\neg p \wedge \neg q}$ } If an expression is combined with an OR gate, and with a false (0), then, the expression is the answer.

Date:

In logic, the conditional $A \rightarrow B$ is equivalent to:

$$A \rightarrow B \equiv \neg A \vee B \rightarrow \text{negation } A \text{ OR } B$$

$$\neg A + B$$

$$\neg A \vee B$$

$\wedge$ - AND - $\times$

$\vee$ - OR - $+$

Date:

Q. Show that $f(x) = x^2 + 2x + 1$ is $O(x^2)$.

$\Rightarrow \quad x^2+2x+1 \leq x^2 + 2x^2 + x$

$x^2+2x+1 \leq 4x^2 \dashrightarrow f(n) \leq c \cdot g(n)$

for $x_0 = 1$;

$\Rightarrow \quad (1)^2 + 2(1) + 1 \leq 4(1)$

$1 + 2 + 1 \leq 4$

$4 \leq 4$

$\therefore$ By definition of Big O, with $c = 4$ and $x_0 = 1$,
Therefore, $f(x) = x^2+2x+1$ is $O(x^2)$ since
$x^2 + 2x + 1 \leq 4x^2$ for $x \geq 1$

Q. Show that $7x^2$ is $O(x^3)$.

$\Rightarrow \quad 7x^2 \leq 7x^3$

$\therefore$ By definition of Big O, with $c = 7$ and $x_0 = 1$,
Therefore, $f(x) = 7x^2$ is $O(x^3)$ since
$7x^2 \leq 7x^3$ for $x \geq 1$.

Q. Prove that $2n+3$ is NOT $O(1)$.

Proof by contradiction :-

Suppose $2n+3$ is $O(1)$,
Then, there exists a positive constant c and a positive integer n_0 such that $2n+3 \leq c \cdot 1$ for $n \geq n_0$, by the definition of big O.

This is a contradiction as $2n+3$ grows infinitely so it cannot be bounded by a constant. Thus, $2n+3$ is not $O(1)$.

Date:

$n^n \longrightarrow$ highest order

$n!$

c^n

n^c

$n\log n$

n

$\sqrt{n}$

$\log n$

$c \longrightarrow$ lowest order

Q. Prove that $10\ln(n^2)$ is $O(\log n)$. equivalent to $O(\log_2 n)$

$\Rightarrow 10\ln(n^2) \leq c\cdot\log n$ for all $n \geq n_0$

$\Rightarrow 10\ln(n^2) = 10(2\ln(n)) = 20\ln(n) = 20\log_e n$

$\log_b a = \dfrac{\log_c a}{\log_c b}$; $\dfrac{20\log_2 n}{\log_2 e}$; $\left(\dfrac{20}{\log_2 e}\right)\log_2 n$

$\therefore\ c = \dfrac{20}{\log_2 e}$

$\Rightarrow 10\ln(n^2) \leq \dfrac{20}{\log_2 e}\cdot\log_2 n$

for $n_0 = 1$

$\Rightarrow 10\ln(1) \leq \dfrac{20}{\log_2 e}\log_2(1)$

$\Rightarrow 0 \leq 0$.

$\therefore$ By definition of Big O, with $c = 20/\log_2 e$ and $n_0 = 1$,
Therefore $10\ln(n^2)$ is $O(\log n)$ since
$10\ln(n^2) \leq \dfrac{20}{\log_2 e}(\log_2 n)$ for $n \geq 1$.

Date:

Q. Prove that 5^n is NOT $O(4^n)$.

Suppose 5^n is $O(4^n)$;

Then, there exists a positive constant c and a positive integer n_0 such that :

$$5^n \leq c \cdot 4^n \quad \text{for} \quad n \geq n_0$$

$$\Rightarrow \frac{5^n}{4^n} \leq c \; ; \; \left(\frac{5}{4}\right)^n \leq c \; ; \; (1.25)^n \leq c.$$

This is a contradiction as 1.25^n grows infinitely so it cannot be bounded by a constant. Thus, 5^n is not $O(4^n)$.

Q. Show that x^3 is NOT $O(7x^2)$.

Suppose x^3 is $O(7x^2)$;

Then, there exists a positive constant c and a positive integer x_0 such that :

$$x^3 \leq c \cdot 7x^2 \quad \text{for} \quad x \geq x_0$$

$$\Rightarrow \frac{x^3}{7x^2} \leq c \; ; \; \left(\frac{1}{7}\right)x \leq c \; ; \; (1/7)x \leq c$$

This is a contradiction as $(1/7)x$ grows infinitely so it cannot be bounded by a constant. Thus, x^3 is not $O(7x^2)$.

Big-O Estimates

1. $\log(n^2) = O(\log n)$

   $\log_2 n = O(\log n)$

2. $\log n! = O(n \log n)$

PROOF : $\boxed{\log n! = O(n \log n)}$ Date:

A big-O estimate for $n!$ can be obtained by noting that each term in the product does not exceed n. Hence,

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n \leq n \cdot n \cdot n \cdot \ldots \cdot n$$

$$\Rightarrow n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n \leq n^n$$

$\Rightarrow$ This inequality shows that $n!$ is $O(n^n)$, taking $C=1$ and $k=1$ as witnesses. Taking logarithms of both sides of the inequality established for $n!$, we obtain :

$$\log n! \leq \log n^n = n \log n$$

$\Rightarrow$ This implies that $\log n!$ is $O(n \log n)$, again taking $C=1$ and $k=1$ as witnesses.

Q. Give a big-O estimate for $f(x) = (x+1)\log(x^2+1) + 3x^2$.

When evaluating big-O estimates ;

- For the terms being multiplied, then simply multiply the big-O.
- If addition is being performed, then, firstly, find the big-O of all the operands ~~of~~ $\pm$ in the summation, and then, take the max of the big-O, based on the hierarchy.

$\therefore$ First term : $(x+1)\log(x^2+1)$

$\Rightarrow x+1 = O(x)$

$\log(x^2+1) = O(\log x)$

$\Rightarrow$ Since the terms are multiplied ; $(x+1)\log(x^2+1) = O(x \log x)$

Second term : $3x^2$

$\Rightarrow 3x^2 = O(x^2)$

Since the first and second terms are added :

$\Rightarrow \max(\cancel{O}\, x\log x, x^2) = x^2$

$\therefore f(x)$ is $O(x^2)$.

Q. $f(x) = \log[(5x+17)^3]$. Show $f(x)$ is $O(\log x)$.

$$f(x) = 3\log(5x+17)$$

$\Rightarrow$ $3\log(5x+17) \le 3\log(5x+17x)$; for $x > 2$

$3\log(5x+17) \le 3\log(22x)$ for $x > 2$

$3\log(5x+17) \le 3[\log 22 + \log x]$ for $x > 2$

$3\log(5x+17) \le 3[\log x + \log x]$ for $x > 22$

$3\log(5x+17) \le 3(2)(\log x)$ for $x > 22$

$3\log(5x+17) \le 6\log x$

$\therefore$ By definition of Big O, with $c = 6$ and $x_0 = 22$,

Therefore, $f(x) = \log[(5x+17)^3]$ is $O(\log x)$ since

$3\log(5x+17) \le 6\log x$ for $x > 22$.

$3\log 22^3 \le \log x$

2^x

$\log 22 \le \log x$

$2^{\log_2 22} \le 2^{\log_2 x}$

$22 \le x$

$x \ge 2^2$

Representation of Integers

Theorem # 1 :- Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form :

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0 ,$$

where k is a nonnegative integer, $a_0, a_1, \dots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

- In decimal notation, an integer n is written as a sum of the form $a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$, where a_j is an integer with $0 \leq a_j \leq 9$ for $j = 0, \dots, k$. For example, 965 is used to denote $9 \cdot 10^2 + 6 \cdot 10^1 + 5$.

⇒ The representation of n given in Theorem 1 is called the base b expansion of n.

e.g What is the decimal expansion of the number with octal expansion $(7016)_8$?
Using the definition of a base b expansion with $b = 8$ tells us that :

$$(7016)_8 = (7 \cdot 8^3) + (0 \cdot 8^2) + (1 \cdot 8^1) + (6 \cdot 8^0) = 3598.$$

3 2 1 0

What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?
Using the definition of a base b expansion with $b = 16$ tells us that :

$$(2AE0B)_{16} = (2 \cdot 16^4) + (10 \cdot 16^3) + (14 \cdot 16^2) + (0 \cdot 16^1) + (11 \cdot 16^0) = 175627.$$

4 3 2 1 0

- Each hexadecimal digit can be represented using four bits. For instance, we see that $(1110\ 0101)_2 = (E5)_{16}$, because $(1110)_2 = (E)_{16}$ and $(0101)_2 = (5)_{16}$.

⇒ Bytes, which are bit strings of length eight, can be represented by two hexadecimal digits.

BASE CONVERSION [Algorithm]

Date:

↳ describing an algorithm for constructing the base b expansion of an integer n.

⇒ First, divide n by b to obtain a quotient and remainder, that is;

$$n = bq_0 + a_0 , \quad 0 \leq a_0 < b.$$

The remainder, a_0, is the rightmost digit in the base b expansion of n.

Next, divide q_0 by b to obtain;

$$q_0 = bq_1 + a_1 , \quad 0 \leq a_1 < b$$

a_1 is the second digit from the right in the base b expansion of n.

Continue this process, successively dividing the quotients by b, obtaining additional base b digits as the remainders.

⇒ This process terminates when we obtain a quotient equal to zero. It produces the base b digits of n from the right to the left.

① e.g. Find the octal expansion of $(12345)_{10}$. → recursively dividing by 8

$$12345 = 8 \cdot 1543 + (.125 \times 8) = 8 \cdot 1543 + \underline{1}$$
$$1543 = 8 \cdot 192 + (.875 \times 8) = 8 \cdot 192 + \underline{7}$$
$$192 = 8 \cdot 24 + (0 \times 8) = 8 \cdot 24 + \underline{0}$$
$$24 = 8 \cdot 3 + (0 \times 8) = 8 \cdot 3 + \underline{0}$$
$$3 = 8 \cdot 0 + (.375 \times 8) = 8 \cdot 0 + 3$$

⇒ The successive remainders that we have found, 1, 7, 0, 0, and, 3, are the digits from the right to the left of 12345 in base 8.

$$\therefore \quad (12345)_{10} = (30071)_8$$

② e.g. Find the hexadecimal expansion of $(177130)_{10}$. → recursively dividing by 16.

$$177130 = 16 \cdot 11070 + (.625 \times 16) = 16 \cdot 11070 + \underline{10}$$
$$11070 = 16 \cdot 691 + (.875 \times 16) = 16 \cdot 691 + \underline{14}$$
$$691 = 16 \cdot 43 + (.1875 \times 16) = 16 \cdot 43 + \underline{3}$$
$$43 = 16 \cdot 2 + (.6875 \times 16) = 16 \cdot 2 + \underline{11}$$
$$2 = 16 \cdot 0 + (.125 \times 16) = 16 \cdot 0 + \underline{2}$$

$\Rightarrow$ The successive remainders that we have found, 10, 14, 3, 11, and, 2, are the digits from the right to the left of 177130 in base 16.

$\therefore \quad (177130)_{10} = (2\,B\,3\,E\,A)_{16}.$

CONVERSION B/W BINARY, OCTAL, and, HEXADECIMAL expansions

- ALWAYS group from the right (LSB) when converting from binary to octal or hex.

$\Rightarrow$ Binary is positional : rightmost bit $= 2^0$, next $= 2^1$, etc.
When grouping for octal (base $8 = 2^3$), we group 3 bits at a time starting from the LSB to preserve positional values.

PIGEONHOLE PRINCIPLE :- When we have N objects, the generalized pigenhole principle tells us that there must be at least r objects in one of the boxes as long as $\lceil N/K \rceil \geq r$.

$\Rightarrow N = K(r-1)+1$

PERMUTATION : $\dfrac{n!}{(n-r)!}$ (order matters)

COMBINATION : $\dfrac{n!}{r!(n-r)!}$ (order DOES NOT matter)

Q. In how many ways can 5 people stand in a circle?

For 5 people : A, B, C, D, E

STEP 1 : Fix A in seat 1 (eliminating rotational duplicates)

STEP 2 : Arrange B, C, D, E in the ~~3~~ 4 remaining seats : ~~3!~~ $4! = 24$ ways

- At least one vowel $\Rightarrow \geq 1$ vowel

$\hookrightarrow$ COMPLEMENT $= < 1$ vowel $= 0$ vowels

GRAPHS

Date:

↳ A graph $G = (V, E)$ consists of V, a nonempty set of vertices (or nodes) and E, a set of edges. Each edge has either one or two vertices associated with it, called its endpoints. An edge is said to connect its endpoints.

⇒ A graph in which each edge connects two different vertices and where no two edges connect the same pair of vertices is called a simple graph.

⇒ Graphs that may have multiple edges connecting the same ≠ vertices are called multigraphs.

↳ When there are m different edges associated to the same unordered pair of vertices, $\{u, v\}$, then, $\{u, v\}$ is an edge of multiplicity m.

⇒ A pseudograph is a type of graph that allows for both, loops (edges connecting a vertex to itself) and multiple edges (more than one edge between the same pair of vertices).

A directed graph (V, E) consists of a nonempty set of vertices V and a set of directed edges, E. Each directed edge is associated with an ordered pair of vertices. The directed edge associated with the ordered pair (u, v) is said to start at u and end at v.

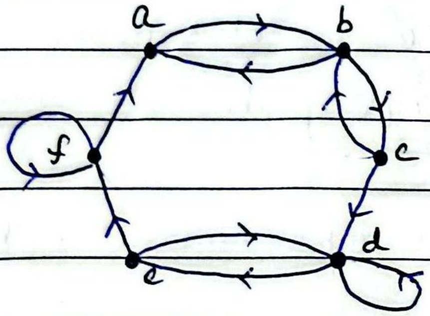
Telephone calls → directed multigraph
Web pages → directed graph
Friendships → simple undirected graph
Citation network → Simple directed graph (no loops)

Simple graph
Multigraph
Pseudograph
} undirected

Date:

Q. Why is a call graph a directed multigraph but a friendship graph is NOT ?

A call graph must be a directed multigraph because multiple calls can occur between the same pair of phone numbers. A friendship graph does not require multiple edges because friendship is a single relationship between two people.



Directed multigraph

A directed multigraph allows multiple edges, and, loops.

The degree of a vertex in an undirected graph is the number of edges incident with it, except a loop at a vertex that contributes twice to the degree of that vertex. The degree of the vertex v is denoted by deg (v).

⇒ In an undirected graph, every loop on a vertex contributes +2 to the degree of that vertex.

HANDSHAKING THEOREM :-

Let $G = (V, E)$ be an undirected graph with m edges. Then ;

$$\Rightarrow \sum_{v \in V} d(v) = 2 * |E|$$

Q. How many edges are there in a graph with 10 vertices each of degree six ?

According to the handshake lemma ;

$$\Rightarrow \sum \deg(v) = 2m = 2 * |E|$$

$$10+10+10+10+10+10 = 2 * |E|$$

$$60 = 2 * |E|$$

$$|E| = 30$$

$\therefore$ $m = 30$.

Date:

(i) In a graph, with directed edges, the *in-degree* of a vertex v, denoted by $deg^-(v)$, is the number of edges with v as their terminal vertex.
The *out-degree* of v, denoted by $deg^+(v)$, is the number of edges with v as their initial vertex.

⇒ A loop at a vertex contributes 1 to both the in-degree and the out-degree of this vertex.

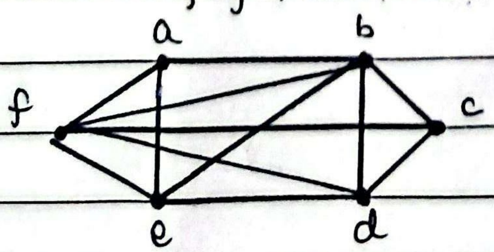
BIPARTITE GRAPHS

A simple graph G is called *bipartite* if its vertex set V can be partitioned into two disjoint sets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 and a vertex in V_2 (so that no adjacent vertices are in the same set).

To identify whether a given graph is bipartite, the following algorithm can be used:

i- Choose any vertex in the graph and assign it to one of the two sets, say X.
ii- Assign all of its neighbours to the other set, say Y.
iii- For each vertex in set Y assign all their unassigned neighbors to set X, and for each vertex in set X, assign all their unassigned neighbors to set Y.
iv- Check if any two adjacent vertices are in the same set.
- If YES, then the graph is NOT bipartite.
- If NO, then the graph is bipartite.

Q. Is the following graph bipartite :-



Date:

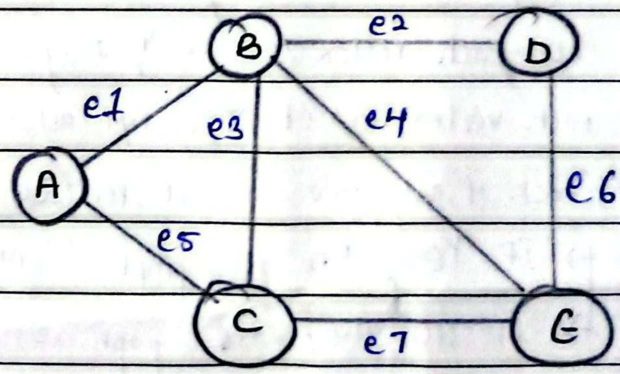
Set X	Set Y	
a	b	a : b, e, f
c	e	b : a, c, d, f
d	f	c : b, d, f
f	d	d : b, c, f
b	c	e : a, b, d, f
e	a	f : a, b, c, d, e

listing all the neighbors of every vertex in alphabetical order

Since a, and, b, which are neighbors to each other, are present in the same set (set X), therefore, this graph is NOT bipartite.

INCIDENCE MATRICES

The incidence matrix is a way of representing a graph where rows represents vertices and columns represent edges, and each entry in the matrix indicates whether a vertex is incident to an edge. ⇒ (if entry == 1, there is an incident edge on the vertex).



The incidence matrix for the graph is as follows :

	e1	e2	e3	e4	e5	e6	e7
A	1	0	0	0	1	0	0
B	1	1	1	1	0	0	0
C	0	0	1	0	1	0	1
D	0	1	0	0	0	1	0
E	0	0	0	1	0	1	1

101
110
000
101

Date:

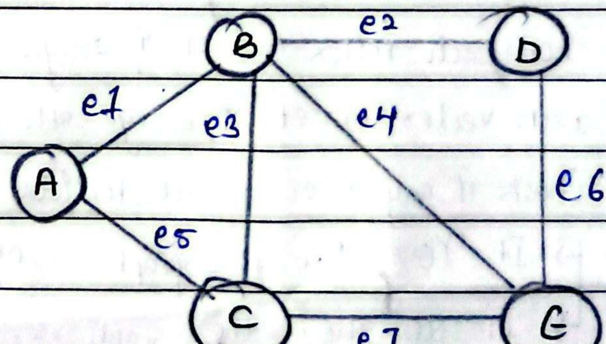
Set X	Set Y	
a	b	a : b, e, f
c	e	b : a, c, d, f
d	f	c : b, d, f
f	d	d : b, c, f
b	c	e : a, b, d, f
e	a	f : a, b, c, d, e

listing all the neighbors of every vertex in alphabetical order

Since a, and, b, which are neighbors to each other, are present in the same set (set X), therefore, this graph is NOT bipartite.

INCIDENCE MATRICES

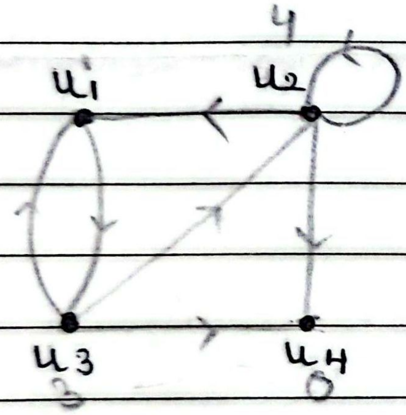
The incidence matrix is a way of representing a graph where rows represents vertices and columns represent edges, and each entry in the matrix indicates whether a vertex is incident to an edge. ⇒ (if entry = = 1, there is an incident edge on the vertex).

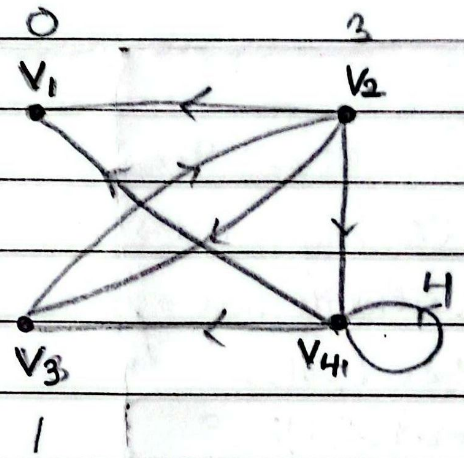


The incidence matrix for the graph is as follows :

	e1	e2	e3	e4	e5	e6	e7
A	1	0	0	0	1	0	0
B	1	1	1	1	0	0	0
C	0	0	1	0	1	0	1
D	0	1	0	0	0	1	0
E	0	0	0	1	0	1	1

101
110
000





$f(u_1) = V_3$

$f(u_2) = V_4$

$f(u_3) = V_2$

$f(u_4) = V_1$

	u_1	u_2	u_3	u_4
u_1	0	0	1	0
u_2	1	1	0	1
u_3	1	1	0	1
u_4	0	0	0	0

	V_3	V_4	V_2	V_1
V_3	0	0	1	0
V_4	1	1	0	1
V_2	1	1	0	1
V_1	0	0	0	0

The two graphs are isomorphic.

Conditional : False when the antecedent is true and the consequent is false. True in all other courses.

$\Rightarrow$ 'if... then'

p	q	$p \to q$	
0	0	1	$0 \le 0 = 1$
0	1	1	$0 \le 1 = 1$
1	0	0	$1 \not\le 0 = 0$
1	1	1	$1 \le 1 = 1$

Biconditional : True when both have the same truth value.

$\Rightarrow$ 'iff (if and only if)'

p	q	$p \leftrightarrow q$
0	0	~~0~~ 1
0	1	0
1	0	0
1	1	1

CONDITIONALS can be re-written as three other forms. Some are equivalent to each other :-

Conditional : $p \to q$

Inverse : $\neg p \to \neg q$ (negate)

Converse : $q \to p$ (swap)

Contrapositive : $\neg q \to \neg p$ (negate + swap)

$$p \to q \equiv \neg q \to \neg p$$

$$\neg p \to \neg q \equiv q \to p$$

1. DeMorgan's Laws

$$\left.\begin{array}{l}\neg(p\wedge q) \leftrightarrow \neg p \vee \neg q \\ \neg(p\vee q) \leftrightarrow \neg p \wedge \neg q\end{array}\right\} \equiv \begin{array}{l}\overline{(A\cdot B)} = \bar{A}+\bar{B} \\ \overline{(A+B)} = \bar{A}\cdot\bar{B}\end{array}$$

2. Distributive Laws

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

3. Contrapositive law

$p \rightarrow q$

$\neg q \rightarrow \neg p$

$\therefore$ $p\rightarrow q \equiv \neg p \vee q$

$\equiv \neg q \rightarrow \neg p$

4. Conditional law

$p \rightarrow q$

$\neg p \vee q$

Translating English into logic

e.g. $\underbrace{\text{8 is an even integer}}_{A}$, $\underbrace{\boxed{\text{but}}}_{\text{AND } (\wedge)}$ it is $\underbrace{\text{not}}_{\neg}$ $\underbrace{\text{divisible by 6}}_{B}$.

$\therefore$ $A \wedge \neg B$

e.g. $\underbrace{\text{Although}}_{\text{AND } (\wedge)}$ $\underbrace{\text{7 is rational}}_{R}$, $\underbrace{\text{the square root of 7 is rational}}_{S}$ (not $\to \neg$).

$\therefore$ $R \wedge \neg S$

q unless $\neg p$ $\Rightarrow$ $q \rightarrow p$

Precedence of logical operators

Operators	Names	Precedence
$\neg$	Negation	1
$\wedge$	Conjunction	2
$\vee$	Disjunction	3
$\rightarrow$	Implication	4
$\leftrightarrow$	Biconditional	5

N
C
~~B~~D
I
B

1 2 3 4 5
N C D I B

Logical equivalence(s)

e.g. $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$

$\Rightarrow$ Applying the distributive law:

$\Rightarrow (\neg p \vee q) \wedge (\neg p \vee r)$

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

$\neg p \vee q \vee \neg p \vee q \wedge r$

$\neg p \vee \neg p \vee q \vee q \wedge r$

$\neg p \vee \underbrace{q \wedge r}_{s}$

$\Rightarrow \neg p \vee s \equiv p \rightarrow s = \cancel{\neg p}\ p \rightarrow (q \wedge r)$ Q.E.D.

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