Logic

Propositional Logic - A declarative statement that is either true or false but not both

Operations

Precedence: 1^{st} ↓

Negation (not)	$\neg$
Conjunction (and)	$\wedge$
Disjunction (or)	$\vee$
Exclusive or (Xor)	$\oplus$
Implication	$\rightarrow$
Bicondition	$\leftrightarrow$

Conditional Statement

Contrapositive

- contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p \; (\equiv p \rightarrow q)$

Only if

- q only if p $\equiv \neg p \rightarrow \neg q \equiv q \rightarrow p$

Nescescary & Sufficient condition

- Nescescary - Must be satisfied
  - If p is the nescescary condition for q $\equiv \neg p \rightarrow \neg q$
- Sufficient - If satisfied then guaranteed
  - If p is the sufficient condition for q $\equiv p \rightarrow q$

Converse & Inverse

$$\left.\begin{array}{l} \text{Converse of } p \rightarrow q \text{ is } q \rightarrow p \\ \text{Inverse of } p \rightarrow q \text{ is } \neg p \rightarrow \neg q \end{array}\right\} \not\equiv p \rightarrow q$$

Valid Argument

$$\underbrace{p; q; r; \ldots}_{\text{hypotheses}} \quad \underbrace{\therefore f}_{\text{Conclusion}}$$

An argument is valid means that if all hypotheses are true, the condition is also true

Consistency (ความต้องกัน)

There must be an assignment of truth value to every expressions that make all the expression true

e.g. given expressions: $p \vee q$, $\neg p$, $p \rightarrow q$

$p \equiv F$ and $q \equiv T$: T T T

Therefore specifications are consistent

Tautology / Contradiction / Contingency

- Tautology (สัจนิรันดร์) - Always True
- Contradiction (ข้อขัดแย้ง) - Always False
- Contingency (การจร) - Neither a tautology nor a contradiction

Logical Equivalences

The proposition p and q are logical equivalent ($p \equiv q$) (สัมมูลเชิงตรรกะ) when $p \leftrightarrow q$ is a tautology

Proving

1. Construct truth tables
2. Use series of established equivalences

Theorem

1. Commutative laws

   $p \land q \equiv q \land p$

   $p \lor q \equiv q \lor p$

2. Associative laws

   $(p \land q) \land r \equiv p \land (q \land r)$

   $(p \lor q) \lor r \equiv p \lor (q \lor r)$

3. Distributive laws

   $p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$

   $p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$

4. Identity laws

   $p \land T \equiv p$

   $p \lor F \equiv p$

5. Domination laws (Universal bound laws)

   $p \lor T \equiv T$

   $p \land F \equiv F$

6. Idempotent laws

   $p \lor p \equiv p$

   $p \land p \equiv p$

7. Negation laws

   $p \lor \neg p \equiv T$

   $p \land \neg p \equiv F$

8. Double negation law

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

9. De Morgan's laws

   $\neg(p \lor q) \equiv \neg p \land \neg q$

   $\neg(p \land q) \equiv \neg p \lor \neg q$

10. Absorption laws

    $p \lor (p \land q) \equiv p$

    $p \land (p \lor q) \equiv p$

Predicate Logic

e.g. "All students go to school" has two parts

students (denoted by variable x)

go to school (the predicate denoted by P)

Therefore this statement can be denoted by $P(x)$

$P(x)$ is said to be the value of the propositional function P at x

Universal Quantifiers

$\forall x P(x)$ means $P(x)$ for all values of x in the universal of discourse i.e. $P(x_1) \land P(x_2) \land \ldots \land P(x_n)$

Existential Quantifiers

$\exists x P(x)$ means there exists an element x in the universal of discourse such that $P(x)$ i.e. $P(x_1) \lor P(x_2) \lor \ldots \lor P(x_n)$

Precedence of quantifiers

$\forall x P(x) \lor Q(x)$ means $(\forall x (P(x))) \lor Q(x)$

Negating Quantified Expressions

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

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

Quantifiers

Consider a statement $\forall x (P(x) \rightarrow Q(x))$

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

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

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

The order of quantifiers

$\forall x \exists y \ P(x,y)$ is not the same as $\exists y \forall x \ P(x,y)$

Nested quantifiers

$\forall x P(x) \land \exists y Q(y)$

$\forall x \exists y (P(x) \land Q(y))$

$\exists y \forall x (P(x) \land Q(y))$

Prenex normal form (PNF)

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

$\forall x \forall y (P(x) \land Q(y))$

Rules of Inference

1. Disjunctive Addition

$$\frac{P}{\therefore P \vee Q}$$

2. Conjunctive Simplification

$$\frac{P \wedge Q}{\therefore P}$$

3. Conjunction Addition

$$\frac{\begin{array}{l} P \\ Q \end{array}}{\therefore P \wedge Q}$$

4. Modus Ponens

$$\frac{\begin{array}{l} P \to Q \\ P \end{array}}{\therefore Q}$$

5. Modus Tollens

$$\frac{\begin{array}{l} P \to Q \\ \neg Q \end{array}}{\neg P}$$

6. Hypothetical syllogism

$$\frac{\begin{array}{l} P \to Q \\ Q \to R \end{array}}{\therefore P \to R}$$

7. Disjunctive syllogism

$$\frac{\begin{array}{l} P \vee Q \\ \neg P \end{array}}{\therefore Q}$$

8. Resolution

$$\frac{\begin{array}{l} P \vee Q \\ \neg P \vee R \end{array}}{\therefore Q \vee R}$$

9. Dillemma

$$\frac{\begin{array}{l} P \vee Q \\ P \to R \\ Q \to R \end{array}}{\therefore R}$$

Predicate logic

1. Universal instantiation	$\forall x P(x)$	$\therefore P(c)$ if $c \in U$
2. Universal generalization	$P(c)$ for an arbitrary $c \in U$	$\therefore \forall x P(x)$
3. Existential instantiation	$\exists x P(x)$	$\therefore P(c)$ for some element $c \in U$
4. Existential generalization	$P(c)$ for some elements $c \in U$	$\therefore \exists x P(x)$

Sets, relation, function

Sets - unordered collections of objects

An empty set is denoted by $\varnothing$

Two sets are equal if and only if $\forall x(x \in A \leftrightarrow x \in B)$

$A \subseteq B$ indicate that A is a subset of B and is a proper subset when $A \neq B$

for every set S : $\varnothing \subseteq S \quad S \subseteq S$

Power set is set of all subsets $(n(P(S))) = 2^n$

Cartesian Product $A \times B = \{a, b \mid a \in A \wedge b \in B\}$

Operators

- Mutually disjoint
  - Sets $A_1, A_2, A_3, \ldots, A_n$ are mutually disjoint when $A_i \cap A_j = \varnothing$
- Set partition
  - A collection of non-empty sets $A = \{A_1, A_2, A_3, \ldots, A_n\}$ is a partition of a set A when $A = A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n$ and $A_1, A_2, A_3, \ldots, A_n$ are mutually disjoint
- Union $(\cup)$, Intersect $(\cap)$, Different $(-)$, Disjoint $(A \cap B = \varnothing)$, Complement $(U - A)$, Power set

$A - B = A \cap B'$

Theorem

1. Commutative laws

   $A \cap B = B \cap A$, $A \cup B = B \cup A$

2. Assosiative laws

   $(A \cap B) \cap C = A \cap (B \cap C)$

3. Distributive laws

   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

4. Idempotent laws

   $A \cap U = A \quad A \cup U = U$

5. De Morgan's laws

   $(A \cup B)' = A' \cap B' \quad (A \cap B)' = A' \cup B'$

6. Absorption laws

   $A \cup (A \cap B) = A \quad (A \cup B) \cap A = A$

Multisets - sets that can contains duplicates

$\{m_1 \cdot a_1, m_2 \cdot a_2, m_3 \cdot a_3, \ldots, m_r \cdot a_r\}$

- m_i are called the multiplicities of the elements a_i

Fuzzy sets is when $0 \leq m_i \leq 1$, m_i are called the degree of membership

Relations & functions

Binary relation (xRy)

A binary relation R from A to B is a subset of Cartesian product $A \times B$

Function $(F(x))$

A function F from A to B is a relation from A to B, $F : A \to B$ that satisfies:

- For every $x \in A$, there exists $y \in B$ such that $(x,y) \in F$
- For all $x \in A$ and $y, z \in B$, if $(x,y) \in F$ and $(x,z) \in F$ then $y = z$

$y = F(x)$ = image of x under F, x is called pre-image of y under F

A is called domain

B is called co-domain

The set of all images of F is called range

Composite function

$$f \circ g = f(g(x))$$

Addition & multiplication

$$(f_1 + f_2)(a) = f_1(a) + f_2(a)$$

$$(f_1 f_2)(a) = f_1(a) f_2(a)$$

Injective function (One-to-one) (1 ต่อ 1) iff $\forall x, y \in A\,((F(x) = F(y)) \to (x = y))$

Surjective function (Onto) (ทั่วถึง) iff $\forall y \in B\, \exists x \in A\, (y = F(x))$

Bijective function (Injective & Surjective) iff $\forall x, y \in A\,((F(x) = F(y)) \to (x = y)) \wedge \forall y \in B\, \exists x \in A\, (y = F(x))$

Properties

Let $A = \{a, b, c\}$

Let R be binary relation on A

- R is reflexive when $\forall x \in A\,(xRx)$
  - $\{(a,a), (b,b), (c,c)\} \subseteq R$
- R is symmetric when $\forall x \in A\,(xRy \to yRx)$
  - $(a,b) \in R \to (b,a) \in R$
- R is transitive when $\forall x, y, z \in A\,((xRy \wedge yRz) \to xRz)$
  - $\{(a,b), (b,c)\} \subseteq R \to (a,c) \in R$

Equivalence relation

R is equivalence relation on A when R is a binary relation on A, R is reflexive, symmetric, and transitive

Methods of Proof

Proposition $\xrightarrow{\text{Proof}}$ Theorem

Universal Instantation / Universal Generalization

"If n is an even integer, n^2 is an even integer"

$\forall n \in Z_{even} (P(n) \to Q(n))$

$P(n)$: n is an even integer

$Q(n)$: n^2 is an even integer

$\therefore P(c) \to Q(c)$ Universal Instantiation

Proof $\to$ $P(c) \to Q(c) \equiv T$ when c is any even integer

$\forall n \in Z_{even} (P(n) \to Q(n)) \equiv T$ Universal Generalization

Proving $p \to q$

Direct Proof	Show that if p is true, q must be true
Proof by contraposition	Show that if $\neg q$ is true, $\neg p$ must be true
Vacous Proof	Show that p is false. So, $p \to q$ is always true
Trivial Proof	Show that q is true. So, $p \to q$ is always true

(Vacous Proof and Trivial Proof:) Used in Mathemetical Induction

Proof by Contradiction

Suppose we want to prove statement s
- Start by assuming $\neg s$ is true
- Show that $\neg s$ implies a contradiction ($\neg s \to F$)
- Then $\neg s$ must be false (s must be true)

- Start by assuming $\neg(p \to q)$ is true
- Therefore $p \wedge \neg q$ must be true
- Show that $p \wedge \neg q$ is a contradiction
- Then, $\neg(p \to q)$ must be false ($p \to q$ must be true)

Proof by cases

A: case1 $\cup$ case2 $\cup$ case3 $\cup \ldots$ casen

$\forall n \in \text{case1} (P(n) \to Q(n)) \equiv T$

$\forall n \in \text{case2} (P(n) \to Q(n)) \equiv T$

$\forall n \in \text{case3} (P(n) \to Q(n)) \equiv T$

...

$\forall n \in \text{casen} (P(n) \to Q(n)) \equiv T$

$\forall n \in A (P(n) \to Q(n))$

Proof of $p \leftrightarrow q$

- Since $(p \leftrightarrow q) \leftrightarrow (p \to q) \wedge (q \to p)$, then prove both $p \to q$ and $q \to p$
- Equivalent propositions ($p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$) are proven by proving $p_1 \to p_2, p_2 \to p_3, \ldots, p_n \to p_1$

Proof of proposition involving quantifiers

Existence proofs: A proof of $\exists x P(x)$

Constructive existence proof
- Find an element c such that $P(c)$ is true

Non-constructive existence proof
- Do not find an element c such that $P(c)$ is true, but use some other ways

Uniqueness proofs: showing that there is a unique element x such that $P(x)$

1. Existence : Show that $\exists x P(x)$
2. Uniqueness : Show that if $y \neq x$, $P(y)$ is false, is the same as proving $\exists x(P(x) \land \forall y(y \neq x \to \neg P(y)))$

Counterexamples : Show that $\forall x P(x)$ is false

Mathemetical Induction

A proof by induction that $P(n)$ is true for every positive integer n consists of 2 steps

Basis Step : Show that $P(1)$ is true

Induction Step: Show that $P(k) \to P(k+1)$ is true for every positive integer $k \geq 1$

Sometimes we want to prove that $P(n)$ is true for $n = b, b+1, b+2, \ldots$ where b is an integer other than 1

Basis Step : Show that $P(b)$ is true

Inductive Step: Show that $P(k) \to P(k+1)$ is true for every positive integer $k \geq b$

Proving mathematical induction

The well-ordering property: Every nonempty set of nonnegative integers has a least element

Strong Induction

A proof by induction that $P(n)$ is true for every positive integers n consists of 2 steps (Using a different induction step)

Basis Step : Show that $P(1)$ is true

Induction Step: Show that $[P(1) \land P(2) \land \ldots \land P(k)] \to P(k+1)$ is true for every positive integers k

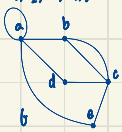
Graphs & Trees

Graphs

$G = (V, E)$

$V = \{v_1, v_2, \dots, v_n\} \rightarrow$ Set of vertices

$E = \{e_1, e_2, \dots, e_n\} \rightarrow$ Set of edges

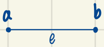


$V = \{a, b, c, d, e\}$

$E = \{(a,a), (a,b), (a,d), (a,e), (b,c), (b,c), (c,e), (d,c)\}$

G has 5 vertices and 8 edges.

Terminology



e is incident with a and b

a is an end point of e

b is another end point of e

a is adjacent to b

b is also adjacent to a

Types of graphs

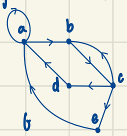
Simple graph : No more than 1 edge between any pairs of vertices. No loops.

Multigraph : There can be more than 1 edge between any pairs of vertices. No loops.

Pseudograph : Any graph.

Directed graphs

Edges are describe with "ordered pairs"



$V = \{a, b, c, d, e\}$

$E = \{(a,a), (a,b), (d,a), (e,a), (b,c), (c,b), (c,e), (c,d)\}$

Types of directed graphs

Simple directed graph : No repeated edges. No loops.

Directed multigraph : There can be repeated edges and/or loops.

Mixed graph : There are both directed and undirected graphs.

Degree of a vertex

Degree of v, deg(v) = number of edges incident with v * A loop contributes twice to the degree of a vertex

Out-degree of v, $deg^+(v)$ = numbers of edges, each of which has v as their initial vertex.

In-degree of v, $deg^-(v)$ = numbers of edges, each of which has v as their end vertex.

The Handshaking Theorem

Let $G = (V, E)$ be an undirected graph with e edges, then

$$2e = \sum_{v \in V} deg(v)$$

The number of vertices of odd degrees

"In an undirected graph, there must be an even number of vertices with odd degree."

Proof by contradiction

Assume: There exists an odd number (n) of vertices with an odd degrees

$\because n = 2k+1, k \in \mathbb{Z}$

Sum of the degree of these vertices is $\sum_{i=1}^{n}(2c_i+1) = 2\sum_{i=1}^{n} c_i + n$ $\because$ even + odd = odd

Sum of the degree of vertices with an even degree is $\sum_{i=1}^{m} 2d_i$ $\because$ even

$\therefore$ Sum of the degree of every vertex is odd

$\therefore$ From HST: Sum of the degree of every vertex is even

$\Big\}$ Contradict

Q.E.D.

In-degree = Out-degree

Let $G=(V,E)$ be a directed graph, then $\sum_{v\in V} \deg^-(v) = \sum_{v\in V} \deg^+(v) = |E|$

Special graph

Completed Graphs (K_n)

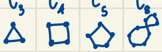
All vertices are connected $|E| = \binom{n}{2}$

K_1 K_2 K_3 K_4 K_5

Cycles (C_n)

$|E| = n$

C_3 C_4 C_5 C_6



Wheels (W_n)

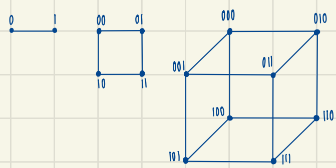
$|V| = n+1$ $|E| = 2n$

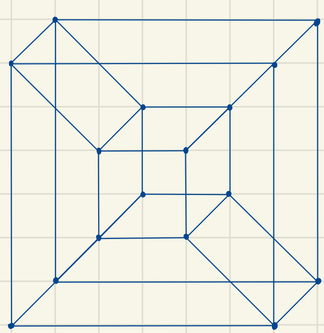
W_3 W_4 W_5 W_6

n-Dimensional Hypercube (Q_n)

$|V| = 2^n$ $\deg(v) = n$ $|E| = n \cdot 2^{n-1}$ $2 \cdot |E_{n-1}| + 1$ Tesseract

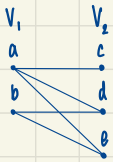
Q_1 Q_2 Q_3 Q_4





Bipartite Graphs

A simple graph $G=(V,E)$ is called bipartite when V can be partitioned into V_1 and V_2 so that no edges connects vertices from the same partition

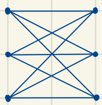


$V=\{a,b,c,d,e\}$

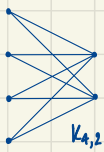
$V_1=\{a,b\}$ $V_2=\{c,d,e\}$

Complete Bipartite Graph ($K_{m,n}$)

- Vertices are partitioned into a set of m vertices and a set of n vertices
- There is an edge between two vertices when one vertex is in the first subset and the other vertex is in the second subset



$K_{3,3}$



$K_{4,2}$

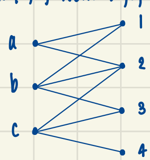
Complete matching

There exists at least one edge incident with every vertex in V_1 (Every vertex in V_1 is incident with some vertices in V_2)

Hall's Marriage Theorem

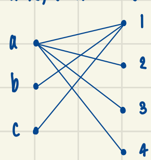
The bipartite graph $G=(V,E)$ with bipartition (V_1,V_2) has a complete matching from V_1 and V_2 if and only if $|N(A)|\geq|A|$ for all subsets A of V_1

$A=\{a,b\}$ $N(A)=\{1,2,3\}$



Complete

$A=\{B,C\}$ $N(A)=\{1\}$

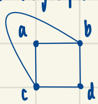


Not complete

Subgraphs

A subgraph of $G=(V,E)$ is a graph $H=(W,F)$ where $W\subseteq V$ and $F\subseteq E$

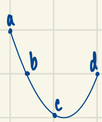
A subgraph H of G is a proper subgraph of G if $H\neq G$



$G=(V,E)$

$V=\{a,b,c,d\}$

$E=\{(a,b),(a,d),(b,c),(b,d),(c,d)\}$



$H=(W,F)$

$W=\{a,b,c,d\}$

$F=\{(b,c),(a,d),(b,d)\}$

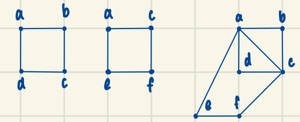
$W\subseteq V$

$F\subseteq E$

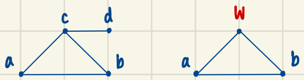
$\therefore H\subseteq G$

Union

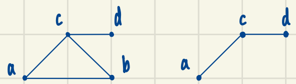
The union of two simple graphs $G_1=(V_1,E_1)$ and $G_2=(V_2,E_2)$ is a simple graph $H=(W,F)$ where $W=V_1\cup V_2$ and $F=E_1\cup E_2$ denoted by $G_1\cup G_2$



Edge Contraction



Vertex Removal



Show that a simple graph with at least two vertices has at least 2 vertices with the same degree

Proof by contradiction

Assume: Each vertex has different degree

Let $G=(V,E)$ be a simple graph with n vertices, $n\geq 2$

Let vertex$_i$; $1\leq i\leq n$ have $\deg(v_i)=i-1$

$\therefore \deg(v_1)=0$ $\because$ v_1 is not adjacent with any vertex

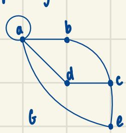
$\therefore \deg(v_n)=n-1$ $\because$ v_n is adjacent with all vertices

} Contradict

Representing graphs

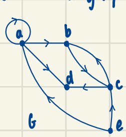
Adjacency lists

- represent graphs with no multiple edges
- specify vertices that are adjacent to each vertex



vertex	adjacent vertices
a	a b d e
b	a c
c	b d e
d	d a c
e	a c

- For directed graph, specify terminal vertices of each vertex

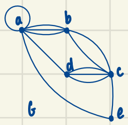


vertex	adjacent vertices
a	a b d
b	c
c	b d
d	-
e	a c

Adjacency Matrices

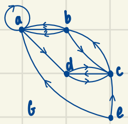
$G=(V,E)$, $V=\{v_1,v_2,\dots,v_n\}$

$A=[a_{ij}]$, a_{ij} = Number of edges corresponding to $\{v_i,v_j\}$



$$\begin{array}{c|c} & \begin{matrix} a & b & c & d & e \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} & \begin{bmatrix} 1 & 3 & 0 & 1 & 1 \\ 3 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 3 & 1 \\ 1 & 0 & 3 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Undirected Graph
↓
Symmetric Matrix

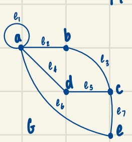


$$\begin{array}{c|c} & \begin{matrix} a & b & c & d & e \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} & \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Incidence Matrix

$G=(V,E)$, $V=\{v_1,v_2,\dots,v_n\}$, $E=\{e_1,e_2,\dots,e_m\}$

$M=[m_{ij}]$, $m_{ij}\begin{cases} 1 & \text{when } e_j \text{ is incident with } v_i \\ 0 & \text{otherwise} \end{cases}$



$$\begin{array}{c|c} & \begin{matrix} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} & \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

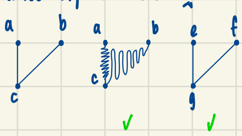
Isomorphism of Graphs

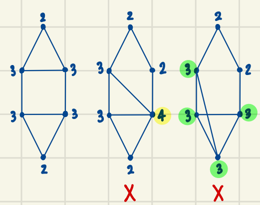
Simple graph $G_1=(V_1,E_1)$ and $G_2=(V_2,E_2)$ are isomorphic when:

There is a 1-1 and onto function f from V_1 to V_2 with the property that

$\forall_{a,b\in V_1}$ a and b are adjacent in G_1 $\leftrightarrow$ $f(a)$ are adjacent in G_2

f is called isomorphism (สมสัณฐาน)





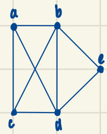
Graph Invariants

A property preserved by isomorphisms ($|V|$, $|E|$, $deg(v)$, adjacency between vertices with specified degrees, simple circuit, paths)

Graph connectivity

Paths

- A path is a sequence of edges that begins with a vertex of a graph and travels from vertex to vertex along edges
- The length of a path is the number of edges in that path
- A path is simple if it does not contain the same edge more than once
- A path is a circuit if it begins and ends on the same vertexs and the lenght is not 0

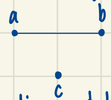


Non-simple path: (a,b,c,b,c,d,e)

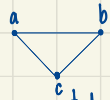
Circuit: (a,b,c,a)

Connectedness

An undirected graph is called connected when there is a path between every pair of distinct vertices in the graph



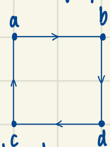
disconnected



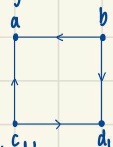
connected

A directed graph is strongly connected when there is a path from a to b and from b to a whenever a and b are distinct vertices

A directed graph is weakly connected when there is a path between every pair of distinct vertices (Regardless of directions)



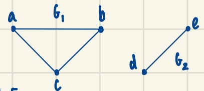
Strongly connected



Weakly connected

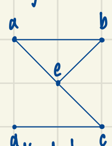
Connected components

A connected component of a graph is maximal connected subgraph of that graph



Cut Vertex / Cut Edges

- A vertex is called cut vertex (articulation point) if the removal of that vertex along with all edges incident with it produces a subgraph with more connected components
- An edge whose removal produces a subgraph with more connected components is called a cut edge (bridge)



Cut vertex : c, e

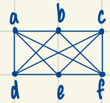
Cut edge : (c,e)

Counting paths between vertices

A number of path from v_i to v_j of lenght r is equals the a_{ij} of A^r when A is an adjacency matrix.

Euler circuits

An Euler circuit in a graph is a simple circuit containing every edges of that graph



a b c f e d a f b d c e a

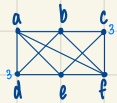
c f e d a f b d c e a b c

Conditions for Euler circuits

A connected multigraph with at least two vertices has an Euler circuit when each of it vertices has even degree

Euler paths

An Euler path in a graph is a simple path containing every edges of that graph



d e a d b a f b c f e c

c f b d e c b a f e a d

Condition for Euler paths

A connected multigraph with at least two vertices has an Euler path when it has exactly two vertices with odd degrees

Hamilton paths and circuit

A Hamilton path in a graph is a simple path that passes through every every vertex of the graph exactly once

For $G=(V,E)$ and $V=\{v_1,v_2,\ldots,v_n\}$, the simple circuit $v_1,v_2,\ldots,v_n,v_1$ is a Hamilton circuit if $v_1,v_2,\ldots,v_n$ is a Hamilton path

Conditions for Hamilton circuits

- No "nescessary & sufficient" conditions exist
- Certain properties can be use to show that no Hamilton circuit exist
  - Degree one vertex
  - There is a cut vertex
- Both edges incident of degree two vertex must be part of any Hamilton circuit
- While constructing a Hamilton circuit if a vertex is passed, all remaining edges of that can be removed from consideration

Some sufficient conditions

Dirac's theorem

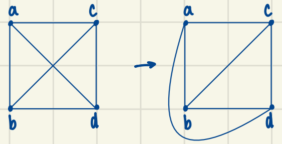
If G is a simple graph with n vertices ($n \geq 3$) such that the degree of every vertex in G is at least $n/2$ then G has a Hamilton circuit

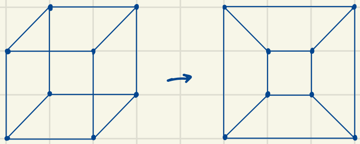
Ore's Theorem

If G is a simple graph with n vertices ($n \geq 3$) such that $\deg(u)+\deg(v) \geq n$ for all non-adjacent vertices u and v then G has a Hamilton circuit

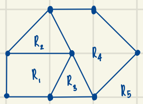
Planar graph

A graph is planar if it can be drawn in a plane without any edges crossing





Regions



$r = 5$

$e = 11$

$v = 8$

Euler's Formula

Let G be a connected planar graph with

e: number of edges

v: number of vertices

r: number of regions in planar representation of G

Then,

$$r = e - v + 2$$

Some conditions for planar graph

- If G is a planar simple graph with e edges and v vertices where $v \geq 3$ then $e \leq 3v - 6$
- If G is a planar simple graph with e edges and v vertices where $v \geq 3$ and no circuit of length 3 then $e \leq 2v - 4$
- If G is a planar simple graph, then G has a vertex of degree not exceeding five

Kuratowski's Theorem

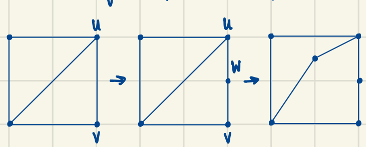
A graph is non planar when it contains a subgraph homeomorphic to $K_{3,3}$ or K_5

Homeomorphism

$G = (V, E)$ and $H = (W, F)$ are homeomorphic if they can be obtained from the same graph by a sequence of elementary subdivisions

Elementary Subdivision

An elementary subdivision is an operation that removes an edge $\{u, v\}$ and adding a new vertex w together with edges $\{u, w\}$ and $\{w, v\}$ (The reverse operation is called smoothing)



Graph Coloring

- A coloring of a simple graph is the assignment of a color to each vertex of the graph so that no two adjacent vertices are assigned the same color
- The Chromatic Number of G, $\chi(G)$, is the least number of colors needed for the coloring

Chromatic numbers of different types of graph

$$C_n \begin{cases} 2 \text{ if } n \text{ is even} \\ 3 \text{ if } n \text{ is odd} \end{cases}$$

$$W_n \begin{cases} 3 \text{ if } n \text{ is even} \\ 4 \text{ if } n \text{ is odd} \end{cases}$$

$K_{m,n}$ 2 } bipartite
Q_n 2

K_n n

The four color theorem

The chromatic number of a planar graph is no greater than 4

Trees

An undirected graph is a tree when there is a unique path between any two of its vertices

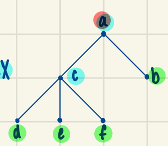
Tree : A connected graph with no simple circuit

Forest : A graph with no simple circuits but not nescessarily connected

Rooted Trees

A rooted tree is tree in which one vertex has been designated as the root and every edge is directed away from the root

root
internal vertex
leaf

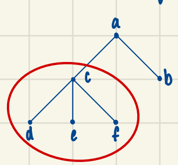


a is a parent of c,b
c is a child of a
b is a child of a

a is ancestor of d,e,f
d,e,f are descendants of a

Subtrees

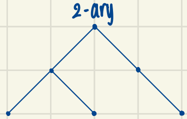
The subtree with v as its root is the subgraph of the tree consisting of v and its descendants and all edges incident to these descendants



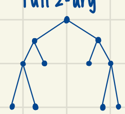
M-ary Trees

An M-ary tree is a rooted tree whose every internal vertex has no more than m children

2-ary



Full 2-ary



Full M-ary tree: When every internal internal vertex has exactly m children

Properties of Trees

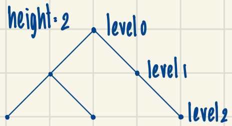
- A tree with n vertices has $n-1$ edges
- A full m-ary tree with i internal vertices contains $mi+1$ vertices
- A full m-ary tree with

vertices	internal vertices	leaves
n	$\frac{n-1}{m}$	$\frac{n(m-1)+1}{m}$
$mi+1$	i	$i(m-1)+1$
$\frac{ml-1}{m-1}$	$\frac{l-1}{m-1}$	l

Level and Height

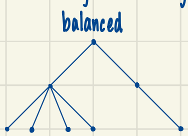
The level of a vertex in a rooted tree is the length of the unique path from the root to this vertex

Height = maximum of levels



There are at most m^h leaves in an m-ary tree of height h

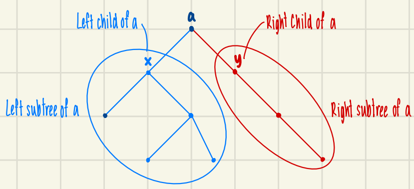
An m-ary tree of height h is balanced if all leaves are at level h or $h-1$



Ordered Rooted Trees

Sibling are ordered from left to right

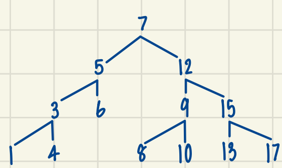
Ordered binary tree



Tree Applications

Binary Search Trees

- Each vertex is labeled with a key
- The key of a vertex is:
  - larger than the keys of all vertices in its left subtree
  - smaller than the keys of all vertices in its right subtree

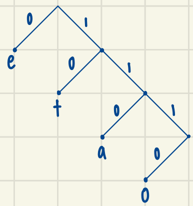


Decision Trees

Character Encoding

Prefix Code

The bit string for a letter nevers occurs as the first part of the bit string for another letter



e = 0

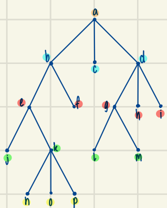
t = 10

a = 110

o = 1110

tea = 10 0 110

Tree traversal

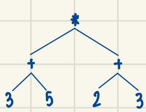


post order traversal j n o p k e f b c l m g h i d a

pre order traversal a b e j k n o p f c d g l m h i

in order traversal j e n k o p b f a c l g m d h i

Postfix Calculator



(3+5) * (2+3) → 35+23+*

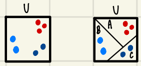
Spanning Trees

A spanning tree of G is a subgraph of G that is a tree containing every vertex of G

Counting

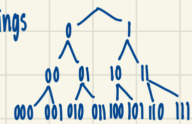
Counting by cases

The sum rule $\quad \# = N_A + N_B + N_C$



Tree diagram : Help counting things composing of successive steps

Eg. all 3-bits strings



The product rule $\quad N = N_1 \cdot N_2 \cdot \ldots \cdot N_k$

The Pigeonhole principle

- If $k+1$ objects are placed into k boxes then there is at least one box containing two or more objects
- If N objects are placed into k boxes then there is at least one box containing $\lceil \frac{N}{k} \rceil$ objects

Permutation

- An ordered arrangement of r elements of a set is called an r-permutation
- The number of r-permutations of a set with n distinct elements is $P(n,r) = \frac{n!}{(n-r)!}$

Combination

- An r-combination of elements of a set is an unordered selection of r elements from a set (subset with r elements)
- The number of r-combination of a set with n distinct elements is $C(n,r) = \frac{n!}{(n-r)!\,r!}$

Permutation with indistinguishable objects / Distributing objects into boxes

$\frac{n!}{n_1! n_2! \ldots n_k!}$ $\quad n_1 - n_k$ = indistinguishable of each types / boxes of sizes

Combinations with repetition : $C(n+r-1, r-1) = \frac{(n+r-1)!}{(n+r-1)!(r-1)!}$ $\quad \binom{\text{stars} + \text{bars}}{\text{bars}}$

The binomial theorem

- A binomial expression is a sum of two terms
- The binomial theorem concerns the sum of two terms

E.g. $(x+y)^3 = \underbrace{\overset{\binom{3}{0}}{x^3} + \overset{\binom{3}{1}}{3x^2y} + \overset{\binom{3}{2}}{3xy^2} + \overset{\binom{3}{3}}{y^3}}$

Binomial Coefficient

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \ldots \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$$

Combinatorial Proof

A combinatorial proof is a proof that uses counting arguments to prove a theorem rather than some other method such as algebric technique

$A = B$

Example: Pascal's Identity

Let n,k be positive integers with $n \geq k$, Then $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

$$\binom{0}{0}$$
$$\binom{1}{0} \quad \binom{1}{1}$$
$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$
$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$
$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

Example: Vandermonde's Identity

Let m,n,r be nonnegative integers with r not exceeding m or n. Then $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$

The principle of inclusion-exclusion

Let $A_1, A_2, \ldots, A_n$ be finite sets then $|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{1\leq i\leq n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{1\leq i<j<k\leq n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|$

Another Notation:

- To find elements with all properties $Q_1, Q_2, \ldots, Q_n$
- Define properties $P_1, P_2, \ldots, P_n$ so that P_i is the opposite of Q_i
- Let A_i be the subset of elements with property P_i
- Let $N(P_1'P_2'\ldots P_n')$ denote the number of elements with none of the properties $P_1, P_2, \ldots, P_n$

$N(Q_1Q_2\ldots Q_n) = N(P_1'P_2'\ldots P_n') = N - |A_1 \cup A_2 \cup \ldots \cup A_n|$

The number of onto functions : $m^n - (\binom{m}{1}(m-1)^n - \binom{m}{2}(m-2)^n + \binom{m}{3}(m-3)^n - \ldots + (-1)^m \binom{m}{m-1}(m-(m-1))^n$

Derangements

A derangement is a permutation of objects that leaves no object in its original position

Example: Consider a sequence 12345

21453 ✓

43512 ✓

42351 ✗

The number of derangements of a set with n elements, $D_n = n!\left(\frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{(-1)^n}{n!}\right)$

Recurence Relations ไปอ่านเอง

Number Theory (เนื้อหาไม่ครบ ไปอ่านเพิ่มเอง)

Floor function $\lfloor x \rfloor$: The greatest integer that is less than or equals to x $\lfloor x \rfloor = n$ when $n \in Z$ & $x-1 < n \leq x$

Ceiling function $\lceil x \rceil$: The smallest integer that is greater than or equals to x $\lceil x \rceil = n$ when $n \in Z$ & $x \leq n < x+1$

$\lfloor F(x) \rfloor = \lfloor F(\lfloor x \rfloor) \rfloor$ and $\lceil F(x) \rceil = \lceil F(\lceil x \rceil) \rceil$ when F is a continuous & monotonically increasing function and $F(x) \in Z \rightarrow x \in Z$

Divisibility and modularity

Divisibility

For any integers m and n, where m is not zero, m divides n, denoted by $m \mid n$ (or n is divisible by m), if there is an integer c such that $m \cdot c = n$. m is a factor of n and n is a multiple of m

Let $a,b,c \in Z$ then

1. $(a \mid b \wedge a \mid c) \rightarrow (a \mid b+c)$,
2. $(a \mid b) \rightarrow (a \mid bc)$ when $c \in Z$
3. $(a \mid b \wedge b \mid c) \rightarrow (a \mid c)$ when $b \neq 0$

Modularity

A modulo n function, where $n \in Z$, is a function from an integer m to the remainder of $\frac{m}{n}$, this is usually denoted by m mod n

Property of Number

Parity (E = even, O = odd)

$E + E = E$

$O + O = E$

$E + O = O$

$E \cdot E = E$

$O \cdot O = O$

$E \cdot O = E$

Primality: A positive integer $n > 1$ that has only 1 and itself is called prime otherwise, it is called composite

Multiplicativity: Every positive integer $n > 1$ can be written uniquely as the product of primes

Additivity

Every odd integer > 7 is the sum of 3 odd primes

Every even integer > 4 is the sum of 2 odd primes

Theory of Divisibility

Greatest common divisor (gcd, หรม)

Let a,b be integers, not both zero, The largest divisor d such that $d \mid a$ and $d \mid b$ is called gcd of a and b denoted by gcd(a,b)

a and b is called relative prime if gcd(a,b) is 1

$(\gcd(a,b) = 1 \wedge a \mid bc) \rightarrow a \mid c$

Least common multiple (lcm, ครน)

Let a,b be integers, not both zero, the smallest multiple d such that d is a multiple of a, and d is a smallest multiple of b is called lcm of a and b denoted by lcm(a,b)

Theory

1. $m = \gcd(a,b)$; $a,b \in \mathbb{Z}^+$

   Suppose x is common divisor of a,b then $x \mid m$

2. $m = \operatorname{lcm}(a,b)$; $a,b \in \mathbb{Z}^+$

   Suppose x is a common multiple of a,b then $m \mid x$

Euclid's division theorem

Given $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. There exist unique integers q,r such that

$$a = bq + r \quad \text{where } 0 \le r < b$$

Euclid's Algorithm

$\gcd(a,b) = \gcd(a \bmod b, b)$ if $b > 0$, $b < a$

For any integer a and any positive integer b, there are unique q_0 and r_1 such that

$$a = bq_0 + r_1 \,, \quad 0 \le r_1 < b$$
$$b = r_1 q_1 + r_2 \,, \quad 0 \le r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3 \,, \quad 0 \le r_3 < r_2$$
$$\cdots$$
$$r_{n-1} = r_n q_n + 0 \,, \quad r_{n+1} = 0$$
$$\therefore \gcd(a,b) = r_n$$

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{\ddots}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

ex. Find $\gcd(435, 246)$

i	r_i	q_i
	435	
0	246	1
1	189	1
2	57	3
3	18	3
4	3	6
5	0	

$a = 435 \quad b = r_0 = 246$

$a = r_0 q_0 + r_1 \longrightarrow 435 = 246 \cdot 1 + 189$

$r_0 = r_1 q_1 + r_2 \longrightarrow 246 = 189 \cdot 1 + 57$

$r_1 = r_2 q_2 + r_3 \longrightarrow 189 = 57 \cdot 3 + 18$

$r_2 = r_3 q_3 + r_4 \longrightarrow 57 = 18 \cdot 3 + 3$

$r_3 = r_4 q_4 + r_5 \longrightarrow 18 = 3 \cdot 6 + 0$

$\gcd(435, 246) = 3$, $n = 4$

$$\frac{435}{246} = 1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{6}}}}$$

Solving bilinear Diophantine equation

Given equation $ax + by = c$

1. $c = \gcd(a,b)$

   $x = (-1)^{n-1} Q_{n-1}$, $y = (-1)^n P_{n-1}$

2. $\gcd(a,b) \mid c$, there exists an integer e such that $e \cdot \gcd(a,b) = c$

   $x = (-1)^{n-1} Q_{n-1}$, $y = (-1)^n P_{n-1} \cdot e$

3. $\gcd(a,b) \nmid c$

   There is not any integral solution.

ex. Given an equation $435x+246y=3$

i	r_i	q_i		P_i	Q_i
	435				
0	246	1		1	1
1	189	1		2	1
2	57	3		7	4
3	18	3		23	13
4	3	6		145	82
5	0				

$P_0=q_0$ $\qquad$ $Q_0=1$

$P_1=q_1q_0+1$ $\qquad$ $Q_1=q_1$

$P_k=q_kP_{k-1}+P_{k-2}$ $\qquad$ $Q_k=q_kQ_{k-1}+Q_{k-2}$

$x=(-1)^{n-1}Q_{n-1}$ $\qquad$ $y=(-1)^nP_{n-1}$

$=(-1)^3\cdot 13$ $\qquad$ $=(-1)^4\, 23$

$=-13$ $\qquad$ $=23$

All Solution : $x=x_0-Q_nt$, $y=y_0+P_nt$

in this example $x=-13-82t$

$y=23+145t$ $\quad t\in\mathbb{Z}$