

CA 1 notes

Modulo

- $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$
- $a \equiv b \pmod{n}, b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$
- $a \equiv b \pmod{n}, c \equiv d \pmod{n} \implies (a+c) \equiv (b+d) \pmod{n}$
 $(ac) \equiv (bd) \pmod{n}$

Euler's $a^{\phi(n)} \equiv 1 \pmod{n}$; $(a,n)=1$

$a^{\phi(n)} \equiv 1 \pmod{n}$
 $a^{p-1} \equiv 1 \pmod{p}$

$\phi(42) = 42 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right)$
 $\phi(1000) = 1000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{5}\right) = 400$

Logic

proposition = ประโยค

paradox = ขัดแย้ง (e.g. this statement is false)

logical operators = $\{ \wedge, \vee, \neg, \rightarrow, \leftrightarrow \}$

conjunction, disjunction, negation, implies (if then), only if, iff, biconditional

equivalent = " $\equiv$ ", associativity = การจับคู่

commutative = สลับที่, distributive = กระจาย

contradiction = proposition that's always false

tautology = proposition that's always true

Arguments = premises + conclusion

"valid": (premise $\wedge$ premise) $\rightarrow$ conclusion

* Critical rows: rows that all premises are true

in all critical rows conclusion true $\rightarrow$ valid

* counter examples: critical rows with false conclusion

* fallacy: error in reasoning results in invalid argument

Inference rules

	conjunctive ($\wedge$)	disjunctive ($\vee$)
Addition	$p;$ $q;$ $\therefore p \wedge q$	$p;$ $\therefore p \vee q$
Simplification	$p \wedge q;$ $\therefore p$	$p \vee q;$ $\sim p;$ $\therefore q$

modus ponens

$p \rightarrow q;$
 $p;$
 $\therefore q$

hypothetical syllogism

$p \rightarrow q;$
 $q \rightarrow r;$
 $\therefore p \rightarrow r$

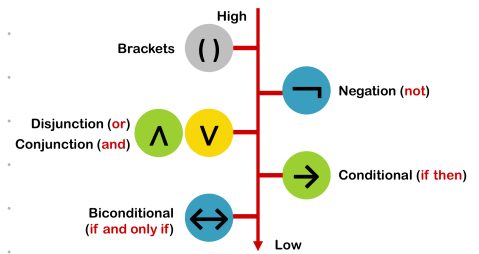
modus tollens

$p \rightarrow q;$
 $\sim q;$
 $\therefore \sim p$

proving technique

Dilemma

$p \vee q;$
 $p \rightarrow r;$
 $q \rightarrow r;$
 $\therefore r$



vacuously true, true by default

necessary condition for p
sufficient condition for q

Statement	$p \rightarrow q$
Converse	$q \rightarrow p$
Inverse	$\neg p \rightarrow \neg q$
Contrapositive	$\neg q \rightarrow \neg p$

De Morgan's:

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

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

Absorption:

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

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

Idempotent:

$$p \wedge p \equiv p$$

$$p \vee p \equiv p$$

Conversion theorem

$$p \rightarrow q \equiv \sim p \vee q$$

Predicate statements containing values $P(x)$

Domain of predicate variables $\sim \mathbb{Z}, \mathbb{R}, \dots$

Quantifier $\forall$ (universal), $\exists$ (existential)

universal gen.: every domain

universal instant.: $\forall x \in D, P(x)$

$\forall " \eta \in \mathbb{R}, x^2 > 0 \therefore 3^2 > 0 "$

existential gen.: some domain

existential instant.: $\exists x \in D, P(x)$

$\exists " \text{ มี } x \text{ บางตัวที่ } \in \mathbb{R}, x^2 = 4 \therefore \text{ จำนวน } 0^2 = 4 "$

Proof Techniques

① Direct proof

② induction

basis $P(0), P(1)$ True

Inductive step : $P(k)$ True $\rightarrow P(k+1)$ True

③ Contradiction want $P(n) \rightarrow Q(n)$

assume $P(n) \wedge \sim Q(n)$

prove false

สมมติ $\sim Q(n)$ ก่อน
แล้วบอก ว่า $\sim P(n)$

Note: 11/11/17

$$A = \{1, 2, 3, 4\} \quad C = \{5, 6\}$$

$$B = \{3, 4, 5, 6\}$$

$$A \cap B = \{3, 4\}$$

$$A \cup B = \{1, 2, 3, 4, 5, 6\}$$

$$\checkmark C \subseteq B \leftrightarrow C \subseteq P(B)$$

$$\checkmark 1 \in A$$

$$\checkmark P(C) = \{\emptyset, \{5\}, \{6\}, \{5, 6\}\} \text{ 'ไม่ว่าจะจับคู่กัน'}$$

Linear recurrence relations $\rightarrow a_n = k \cdot a_{n-1} + m$

③ other linear homogenous eq. = เหมือนกับ a_{n-k}

geometric progression ① $a_n = (k) a_{n-1}$
 $a_0 = c$

$$\therefore a_n = (c)(k^n)$$

ค่าคงที่ (เปลี่ยนเลข)
ค่าคงที่ e.g. 2K
ถ้า $k(d)$ ② $a_n - a_{n-1} = d$

$$a_n = c + \sum_{i=1}^n d$$

① characteristic polyno. $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_d a_{n-d}$

② characteristic equat. $x^d = c_1 x^{d-1} + c_2 x^{d-2} + \dots + c_d$

* หรือ x กลาง min.

③ solve for x roots

$$④ a_n = u(x_1^n) + v(x_2^n)$$

$$a_n = u \cdot x_1^n + v \cdot n \cdot x_1^n + w \cdot n^2 \cdot x_1^n \dots$$

solve for u, v

⑤ substitute base case a_0, a_1

example : $a_n - 4a_{n-1} + 4a_{n-2} = 0$ where $a_0 = 1; a_1 = 3$

$$\begin{aligned} a_n &= 4a_{n-1} - 4a_{n-2} \\ x^n &= 4x^{n-1} - 4x^{n-2} \\ x^2 &= 4x - 4 \\ x^2 - 4x + 4 &= 0 \\ (x-2)^2 &= 0 \\ x &= 2 \end{aligned}$$

$$a_n = u(2)^n + v \cdot n \cdot (2)^n$$

$$a_1 = u(2) + v(1) \cdot (2)^1$$

$$a_1 = 2u + 2v \rightarrow 3 = 2u + 2v$$

$$a_0 = u(1) + 0$$

$$a_0 = u \rightarrow u = 1$$

$$\therefore a_n = 2^n + \left(\frac{1}{2}\right) \cdot (n) \cdot 2^n$$

$$a_n = 2^n + n \cdot 2^{n-1}$$

$$\begin{aligned} u &= 1 \\ v &= \frac{1}{2} \end{aligned}$$

Sets $\rightarrow$ explicit e.g. $A = \{2, 3\}$

$\rightarrow$ implicit e.g. $A = \{x | x \text{ is prime}\}$

* set ไม่ทับซ้อน !!



• partition = mutually disjoint = mutually ex

$$A - B = A \cap B'$$

$$\text{De Morgan's } \overline{(A \cup B)} = \overline{A} \cap \overline{B}$$

Identity	Name	Identity	Name
$A \cup \emptyset = A$ $A \cap U = A$	Identity laws	$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws	$A \cup (B \cap C) = (A \cup B) \cap C$ $A \cap (B \cup C) = (A \cap B) \cup C$	Associative laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws
$\overline{\overline{A}} = A$	Double Complement laws	$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws	$A - B = A \cap \overline{B}$	Alternate representation for set difference

• ถ้า P มี 2^x

$$|P(P(A))| = 2^{2^{n(A)}}$$

• subset $\subseteq$

• empty set $\emptyset, \{y\} \neq \{\emptyset\}$

• set ไม่

• Cardinality : $|S| = |\{1, 2, 3\}| = 3$

จำนวนสมาชิก

• Power set $P(S)$ จ.สมาชิก 2^n

set of subsets

• cartesian product $A \times B$

ทุกคู่สมาชิกที่จับคู่กันได้

e.g. $A = \{1, 2\}, B = \{a, b\}$

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

subset of $A \times B$ with certain conditions
Relations - Binary relations: between 2 sets ex. e.g. (x, y) that $x - y = \text{even}$

• denotes with 'R' e.g. $A = \{2, 3, 4\}, B = \{3, 6, 8\}, (x, y) \in R \leftrightarrow x \text{ divides } y$

• Inverse of binary relation

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}$$

matrix transpose

$$R^t = R + (a, b) \text{ transitive}$$

• Composite of relations

$$R \circ S = \{(a, c) \in A \times C \mid \exists b \text{ s.t. } (a, b) \in R, (b, c) \in S\}$$

	→ Reflexivity $\forall x, x R x$ ทุกตัวใน R	→ Symmetry $\forall x, y, x R y \rightarrow y R x$ สลับที่กันได้	→ Transitivity $\forall x, y, z, (x R y) \wedge (y R z) \rightarrow x R z$ ถ้า	Antisymmetry $\forall x, y, (x R y) \wedge (y R x) \rightarrow x = y$ ไม่สลับที่กันได้ (ถ้าตัวกัน)
Equivalence relations	✓	✓	✓	
partial order	✓		✓	✓
Transitive closure			✓ ทุกตัว	

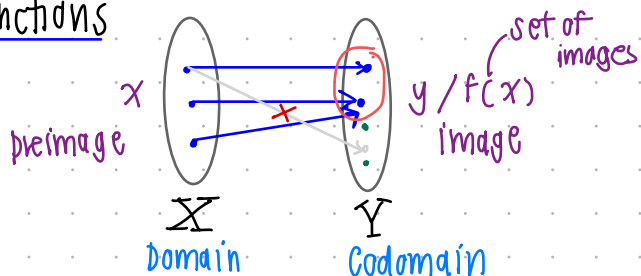
• n-ary relations (≥ 2 variables)

• complement of relations $U - R$

• operations $\cup, \cap,$

• equivalence classes

Functions



* set well

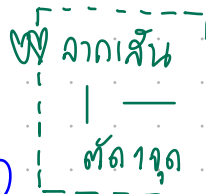
* Domain มีทุกตัว

* Codomain มีบางตัว OK

1. injectivity (1-to-1)

$$f(x_1) = f(x_2) \rightarrow x_1 = x_2$$

$$x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)$$



2. Onto/surjective

$$\forall y \in Y, \exists x \in X, f(x) = y$$



3. Bijective 1-to-1 + onto / 1-1 correspondence

Inverse function (must be bijective) มีตัว y สู่ x

$$f^{-1}(b) = a \text{ when } f(a) = b$$

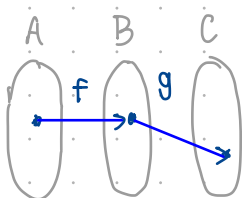
Composition function

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

• $f \circ g \neq g \circ f$ (no commutative)

• f 1-1, g 1-1 : $g \circ f$ 1-1

• f onto, g onto : $g \circ f$ onto



Pigeon hole principle

k holes, n pigeon

small codomain

big domain

$n > k$
at least $\lceil \frac{n}{k} \rceil$
birds
in at least 1 net

Countable set

countable
uncountable

1-1 corres. to a set of $\mathbb{Q}$ int

→ proof uncountable sets: cantor diagonalisation

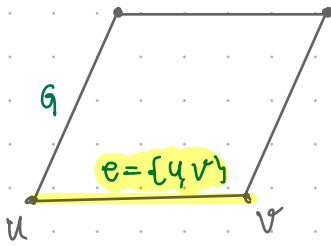
① suppose $\mathbb{R}$ countable

② get contradiction

③ 1-1 corres with positive int → can label

Graph Theory

graph $G = (V, E)$
 nodes/vertices V
 lines joining vertices/edges E



- $u \& v$ are adjacent
- e is an incident edge with vertices $u \& v$

subgraphs

$$V_{sub} \in V_{twj}$$

$$E_{sub} \in E_{twj}$$

simple graph

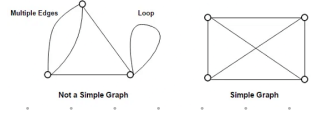
- no loop
- ≤ 1 edge / pair (no multi-edge)

Multigraph

- no loop
- at least 1 > 1 edge / pair (multi-edge)

Directed graph

- edges have direction
- allow parallel edges



Euler Theorem

- euler path walk all edges once
- Euler circuit

degree of a vertex = number of edges incident with it
 odd/even?

งัยทุกเส้น

- if G has euler circuit วนทุกเส้น = all even nodes + path

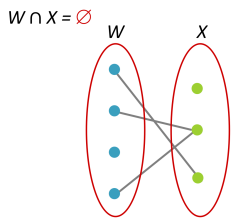
- G has euler path วนบางส่วน, มี/ไม่มี circuit = 2 odd nodes $\rightarrow$ เริ่ม + จบ

$$\text{Total degree / deg}(G) = \sum_{v \in V} \text{deg}(v) = 2e$$

(undirected) #edges

complete graphs = simple graph + วนรอบทุกจุด

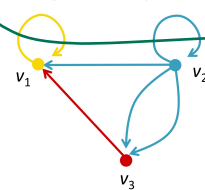
Bipartite graphs



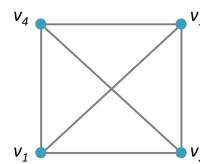
every edge on w join x
 each in w not adjacent to each other

triangle = 3 bipartite

adjacency matrix



$$A = \begin{matrix} & v_1 & v_2 & v_3 \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 1 & 0 & 0 \end{bmatrix} \end{matrix}$$

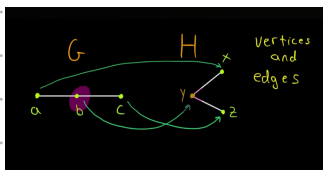


complete graph

$$\begin{matrix} & v_1 & v_2 & v_3 & v_4 \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{matrix}$$

Graph Isomorphism : same graph เปลี่ยนกันแล้วแบบ

same structure $G \cong H, H \cong G$



$$\phi: V(G) \rightarrow V(H)$$

$$\phi: \begin{pmatrix} a & b & c \\ x & y & z \end{pmatrix}$$

no 2 vertices map to same one aka. 1-1 (injective)

every node in H has node G map to it aka. onto (surjective)

$v_1, v_2 \in E(G)$ (adjacent) if & only if $\phi(v_1), \phi(v_2)$ (adjacent)
 $\hookrightarrow$ edge = adjacent also

ϕ is bijective! (1-1 correspondence)

* same # edges & # vertices $\neq$ isomorphic
 but diff. #edges & #vertices = non-isomorphic.

Hamiltonian Circuit walk all nodes once เริ่ม/จบที่ตัวเดิม

งัยทุกจุด



A graph $G = (V_G, E_G)$ is isomorphic to a graph $H = (V_H, E_H)$ if and only if there exists two bijections mapping the vertex sets and edge sets, respectively:

$$g: V_G \rightarrow V_H, h: E_G \rightarrow E_H$$

such that an edge $e \in E_G$ is incident on $v, w \in V_G \Leftrightarrow$ the edge $h(e) \in E_H$ is incident on $g(v), g(w) \in V_H$.