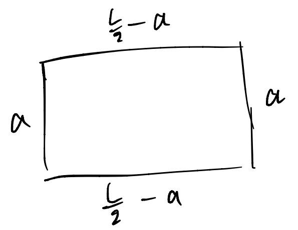
Discrete Structure & Computability



$L = 100$ m

max: $(\frac{L}{2} - a)a$

$$\frac{d}{da}\left(\frac{L}{2}a - a^2\right) = 0$$

$$\frac{L}{2} - 2a = 0$$

$$2a = \frac{L}{2}$$

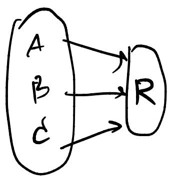
$$a = \frac{L}{4} \rightarrow \frac{100}{4} = 25 \text{ m}$$

$\therefore$ Square yields max area.

09/08/22

Terminology

- Propositions - ประพจน์ : a block / sentence which is <u>either T or F.</u> not both
  - └ เชื่อมด้วย logical operators → compound propositions.
- Truth Table : - 2^n yields #rows (combination of propositions)
  - 2^{2^n} yields # of every results → equivalent combinations yields same results in 2^{2^n} → "expressive power"
  - └ Many-to-one



㊀ One of them uses least operators

- Contrapositive : $f(p, q) \equiv f(\sim p, \sim q)$

  eg. $p \rightarrow q \equiv \sim q \rightarrow \sim p$

- Converse $p \rightarrow q \xrightarrow{C} q \rightarrow p$
- Inverse $p \rightarrow q \xrightarrow{I} \sim p \rightarrow \sim q$

㊀ Precedence (Priority) $\neg > \wedge > \vee > \rightarrow > \leftrightarrow$

Natural Language Conversion

- **Sufficiency**

  "If q, then p" or "p if q"
  ↳ q is sufficient for p.

  $\boxed{q \to p}$

  * p เกิดโดยขาด q ได้ | แต่ถ้ามี q แล้ว p ต้องเกิด

- **Necessity**

  "p only if q"
  ↳ q is necessary for p

  $\boxed{p \to q}$

  * p เกิดโดยขาด q ไม่ได้

- **Consistency**
  ↳ มีอย่างน้อย 1 กรณี ที่ทำให้เงื่อนไข A, B, C, ... เป็น T ได้พร้อมกัน

- **Satisfaction**
  ↳ มีอย่างน้อย 1 กรณี ที่ทำให้เงื่อนไข A, B, C, ... เป็น T อย่างน้อย 1 เงื่อนไข

- **Tautology**
  Any combination always yields T.

- **Contradiction**
  Any combination always yields F.

- **Contingency**
  Neither Tauto. nor Contradict.

- **Equivalency**
  - Same truth table results.
  - Rules & properties

eg. $p \to (\sim p \to q)$ using $p \to q \equiv \sim p \vee q$

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

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

$\equiv T \vee q$

$\equiv T \quad \blacksquare$

eg. $(p \leftrightarrow q) \wedge (\sim p \wedge q)$ using $p \leftrightarrow q \equiv (\sim p \wedge \sim q) \vee (p \wedge q)$

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

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

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

$\equiv [\sim p \wedge F] \vee [F \wedge q]$

$\equiv F \quad \blacksquare$

Predicate Logic

Arithmetic: $f(x) = x + 7$

Logic : $P(x) \equiv$ x goes to school.

Universal Quantification (For All)

eg. $P(x) \equiv x \leq x^2$

$P(10) \equiv 10 < 10^2$

$P(10) \equiv T$

$\forall x P(x) \equiv \ldots$ (Universal Domain)

Restricted Domain : $\forall (x \in D) P(x)$, $\forall_{x \in D} P(x)$ // Notation

Existential Quantification (For Each / For Some)

$\exists x P(x) \equiv \ldots$

Unique value : $\exists ! x P(x)$ (Uniqueness Quantification)

(scoping)
Precedence : $\forall x, \exists x, \exists ! x, \ldots$ are higher than logical operators.

Binding vars. : ✗ $\exists x P(x, y)$: y is free, x is bound. * can't conclude proposition.
✓ $\exists x \exists y P(x, y)$: x is bound, y is bound.

(+) Some equivalency rules & properties can be applied.

eg. De Morgan's : $\sim \forall x P(x) \equiv \exists x (\sim P(x))$ "ไม่ใช่ทั้งหมดที่เป็นจริง" → "มีบางตัวที่ไม่เป็นจริง"

$\sim \exists x P(x) \equiv \forall x (\sim P(x))$ "ไม่มีสักตัวที่เป็นจริง" → "ทุกตัวไม่เป็นจริง"

→ Nested Quant. ≡ Nested Loop & Break points.

As loop: $\forall x \exists y P(x, y) \not\equiv \exists y \forall x P(x, y)$ *order matters.

$\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$

$\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y)$

Equivalency of Quantifiers

eg. $\forall x (P(x) \rightarrow Q(x)) \overset{?}{\equiv} \forall x P(x) \rightarrow \forall x Q(x)$

$\forall x (P(x) \vee Q(x)) \not\equiv \forall x P(x) \vee \forall Q(x)$

$\forall x (P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$

$\exists x (P(x) \wedge Q(x)) \not\equiv \exists x P(x) \wedge \exists x Q(x)$

$\exists x (P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$

$\forall x P(x) \overset{def}{\equiv} \bigwedge_{i=1}^{N} P(x_i) \sim \prod_{i=1}^{N} P(x_i)$

$\exists x P(x) \overset{def}{\equiv} \bigvee_{i=1}^{N} P(x_i) \sim \sum_{i=1}^{N} P(x_i)$

Null Quantification

$$\forall x(P(x) \land A) \equiv \forall x P(x) \land A$$

$$\bigwedge_{i=1}^{N}(P(x_i) \land A) \equiv \left(\bigwedge_{1}^{N} P(x_i)\right) \land A$$

$$\forall x(P(x) \lor A) \equiv \forall x P(x) \lor A$$

$$\exists x(P(x) \land A) \equiv \exists x P(x) \land A$$

$$\exists x(P(x) \lor A) \equiv \exists x P(x) \lor A$$

$$\forall x(A \to P(x)) \equiv A \to \forall x P(x)$$

$$\exists x(A \to P(x)) \equiv A \to \exists x P(x)$$

$$\forall x(P(x) \to A) \equiv \exists x P(x) \to A$$

$$\exists x(P(x) \to A) \equiv \forall x P(x) \to A$$

$$\forall x(P(x) \to A) \to (\forall x P(x) \to A) \equiv T$$

$$(\forall x P(x) \to A) \to \forall x(P(x) \to A) \equiv F$$

$$\exists x(P(x) \to A) \to (\exists x P(x) \to A) \equiv F$$

$$(\exists x P(x) \to A) \to \exists x(P(x) \to A) \equiv T$$

Inference

Argument { statements ($\bigwedge_{i}^{N} p_i$) : เป็น Tautology ≡ Valid Arg.
$\downarrow$
conclusion

eg. If a user has password, he/she can login.
You either have a correct password or are not a user.
Both you and your friends are user.

Rules

Notation : $\dfrac{\begin{matrix} p \\ q \end{matrix}}{\therefore\ r} \equiv (p \equiv T) \wedge (q \equiv T) \rightarrow (r \equiv T)$

$(p \wedge q \rightarrow r)$

Addition $\dfrac{p}{\therefore\ p \vee q}$

Simplification $\dfrac{p \wedge q}{\therefore\ p}$

Conjunction $\dfrac{\begin{matrix} p \\ q \end{matrix}}{\therefore\ p \wedge q}$

Modus ponen (Law of Detachment) $\dfrac{\begin{matrix} p \\ p \rightarrow q \end{matrix}}{\therefore\ q}$

Modus tollens $\dfrac{\begin{matrix} \sim q \\ p \rightarrow q \end{matrix}}{\sim p}$ ⇝ $\sim q \rightarrow \sim p$

Hypothetical s. $\dfrac{\begin{matrix} p \rightarrow q \\ q \rightarrow r \end{matrix}}{p \rightarrow r}$

Resolution : $\dfrac{\begin{matrix} p \vee q \\ \sim p \vee r \end{matrix}}{\therefore\ q \vee r}$

Disjunctive s. $\dfrac{\begin{matrix} p \vee q \\ \neg p \end{matrix}}{q}$

Use Rules for them.

Universal Instantiation	∀xP(x) ∴ P(c)
Universal Generalization	P(c) for an arbitrary c ∴ ∀xP(x)
Existential Instantiation	∃xP(x) ∴ P(c) for some element c
Existential Generalization	P(c) for some element c ∴ ∃xP(x)

→ ถ้าทุกตัวใช้แล้วเป็นจริง หยิบตัวไหนมาต้องเป็นจริง
→ หยิบตัวใดส่วนหนึ่งมา ต้องเป็นจริงเสมอ
→ ถ้าบางตัวเป็นจริง
→ ถ้าหยิบบางตัวมาแล้วเป็นจริง → มี $\exists x P(x)$

Observe elements make rules

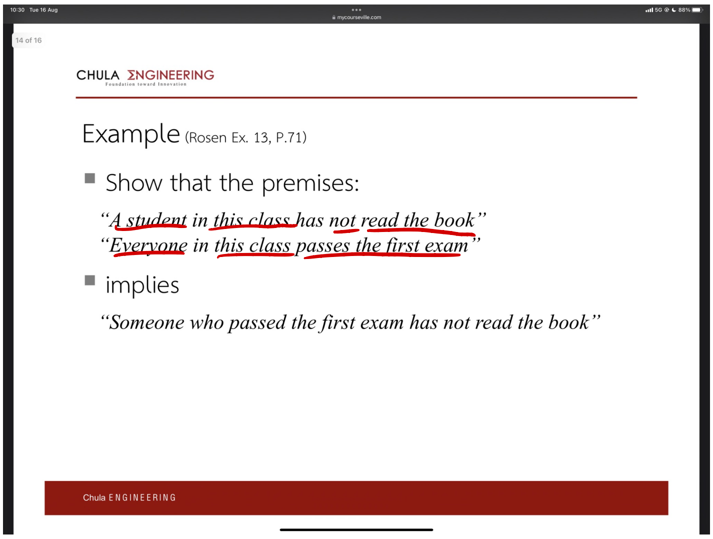
* c ใดๆ ตัวเดียวกัน

Addition $\dfrac{p}{p \vee q}$ Modus p. $\dfrac{\begin{matrix} p \rightarrow q \\ p \end{matrix}}{q}$

Simplify $\dfrac{p \wedge q}{p}$ Modus t. $\dfrac{\begin{matrix} p \rightarrow q \\ \neg q \end{matrix}}{\neg p}$

Conjunction $\dfrac{\begin{matrix} p \\ q \end{matrix}}{p \wedge q}$ Hypo.s. $\dfrac{\begin{matrix} p \rightarrow q \\ q \rightarrow r \end{matrix}}{p \rightarrow r}$

Res. $\dfrac{\begin{matrix} p \vee q \\ \neg p \vee r \end{matrix}}{q \vee r}$ Disj.s. $\dfrac{\begin{matrix} p \vee q \\ \neg p \end{matrix}}{q}$



eg.

In class $\equiv C(x)$

Read $\equiv P(x)$

Pass $\equiv Q(x)$

$C(k)$

① $\exists x\,(C(x) \land \neg P(x))$

② $\forall x\,(C(x) \rightarrow Q(x))$

ⓒ $\exists x\,(\neg P(x) \land Q(x))$

Choose some k

① $\exists x\,(C(x) \land \neg P(x))$

$C(k) \land \neg P(k) \xrightarrow{\text{simpf.}} \neg P(k)$

② $\forall x\,(C(x) \rightarrow Q(x))$

$C(k) \rightarrow Q(k)$

MP: $Q(k)$

$\therefore \quad \neg P(k) \land Q(k)$

Rev.k $\exists x\,(\neg P(x) \land Q(x))$ ■

eg. All nat. numbers are integers

Some numbers are nat. numbers

Pv. Some numbers are integers

$N(x)$: x is $\mathbb{N}$

$I(x)$: x is $\mathbb{Z}$

Peano Axiom

① $\forall x\,(N(x) \rightarrow I(x))$

② $\exists x\, N(x)$

ⓒ $\exists x\, I(x)$

Choose some k

②: $\exists x\, N(x)$

$N(k)$

①: $\forall x\,(N(x) \rightarrow I(x))$

$N(k) \rightarrow I(k)$

MP: $I(k)$

Rev. k $\exists x\, I(x)$ ■

Sets

$A = \{0,1\}, \quad B = \{j,k\}, \quad C = \{x,y,z\}$

$$A \times B \times C = \{(0,j,x),(0,j,y),(0,j,z),(0,k,x),(0,k,y),(0,k,z),(1,j,x),(1,j,y),(1,j,z),(1,k,x),(1,k,y),(1,k,z)\}$$

$n(A \times B \times C) = n(A) \times n(B) \times n(C)$

$12 = 2 \times 2 \times 3$ ✓ (True)

New Notation:

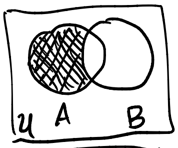
$n(A) = |A|$

Quantifier: $\forall x \in \mathbb{R}(x^2 \geq 0)$

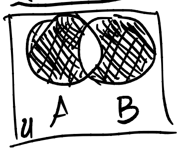
Set Operations: $\cup, \cap, {}', -, \oplus$

Difference

Symmetric Difference

$A - B =$ 

$= A \cap B'$

$A \oplus B =$ 

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

General form of Excl., Incl.

$$\left| \bigcup_{i=1}^{N} A_i \right| = \sum_{i=1}^{N} \left((-1)^{i+1} \left| \bigcap_{j=1}^{i} A_j \right| \right)$$

Membership Table ~ **Truth Table**

- Surjective (onto)
- Injective (1-1)

Relations

$*$ $R \neq \mathbb{R}$

$R = \{(x,y) \mid \text{Conditions } (X \times Y)\}$ (binary)

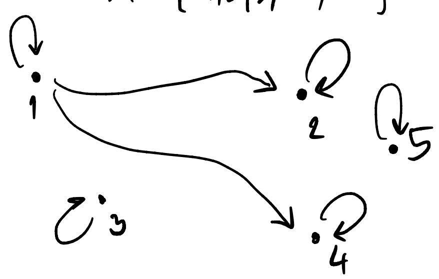
For N-ary, $A_1 \times A_2 \times A_3 \times \dots \times A_n = \{(a_1, a_2, a_3, \dots, a_n) \mid \dots\}$

properties

Reflexive : R on A is reflexive $\leftrightarrow \forall a((a,a) \in R)$; $a \in A$

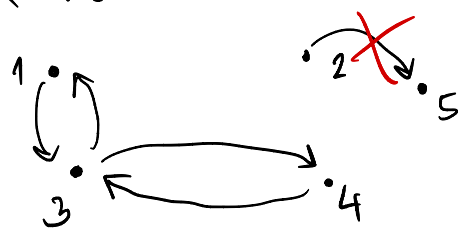
หมายถึง R must contain $(1,1), (2,2), (3,3), \dots, (n,n)$;

$A = \{1, 2, 3, \dots, n\}$



Symmetric : R on A is symmetric $\leftrightarrow \forall a \forall b ((a,b) \in R \rightarrow (b,a) \in \mathbb{R})$

R must contain (a,b) & (b,a)



$(a,b) \notin R \vee (b,a) \notin R \vee (a=b)$

⊕ R on A is antisymmetric $\leftrightarrow$

$\forall a \forall b (((a,b) \in R \wedge (b,a) \in R) \rightarrow (a=b))$

ไม่สน sym แค่ a=b ได้

Transitive $\forall a \forall b \forall c ((a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R)$

เช่น $\{(\underline{1,2}), (\underline{2},3), (1,3), (2,4)\}$

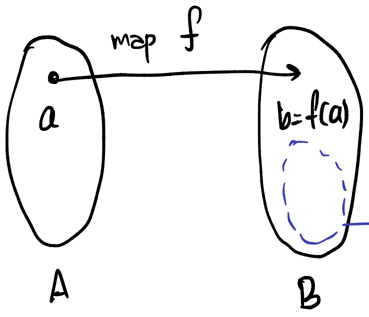
Composite Relations

$S(R(x))$: $R: A \rightarrow B$, $S: B \rightarrow C$

$S \circ R \subseteq X: A \rightarrow C$

Functions

Def. $f: A \to B$



e.g. $y = x^2$

A: Domain
B: Codomain } e.g. $\mathbb{R} \times \mathbb{R}$

a: pre-image

b: image

Range → e.g. $[0, +\infty)$

One-to-one functions

Def.

Strictly increasing — Strictly decreasing

$$f_{1-1} \leftrightarrow \underbrace{\forall x \forall y ((x<y) \to (f(x) < f(y)))}_{\text{Strictly increasing}} \vee \underbrace{\forall x \forall y ((x<y) \to (f(x) > f(y)))}_{\text{Strictly decreasing}}$$

Onto functions (Surjective)

$$f_{onto} \leftrightarrow \forall y \exists x (y = f(x))$$

"ทุก pre-image จะมี image เสมอ"

(Range = Codomain)

One-to-one & Onto functions (Bijection)

Theory of proving

eg. Show that if $f(x)$ & $g(x)$ is injective, then $fog(x)$ is injective

Def. $fog(x) = f(g(x))$

Given a. $\forall(x_1 \in A, x_2 \in A)(f(x_1) = f(x_2) \rightarrow x_1 = x_2)$

b. $\forall(x_1 \in B, x_2 \in B)(g(x_1) = g(x_2) \rightarrow x_1 = x_2)$

Show that $\forall(x_1 \in A, x_2 \in A)(g \circ f(x_1) = g \circ f(x_2) \rightarrow x_1 = x_2)$

Step	Reason
1. Choose $a \in S, b \in S$; S ใดๆ	Universal Instantiation a.
2. Choose $f(a) \in U, f(b) \in U$; U ใดๆ	Universal Instantiation b.
3. $g(f(a)) = g(f(b)) \rightarrow f(a) = f(b)$	2.
4. $f(a) = f(b) \rightarrow a = b$	1.
5. $g(f(a)) = g(f(b)) \rightarrow a = b$	Hypothetical Syllogism 3., 4.
6. $g \circ f(a) = g \circ f(b) \rightarrow a = b$	Definition
7. $\forall(x_1 \in A, x_2 \in A)(g \circ f(x_1) = g \circ f(x_2) \rightarrow x_1 = x_2)$	Universal Generalization 6.
8. $g \circ f$ is injective	Definition

∎

Proving $p \to q$ eg: The sum of two odds (odd $\mathbb{Z}$) is even.

① DIRECT PROOF

Claim $\forall (m,n \in \mathbb{Z})(\overset{p}{m,n \in \mathbb{Z}_{odd}} \to \overset{q}{m+n \in \mathbb{Z}_{even}})$

Definition
1. Odd : $m = 2a+1$; $a \in \mathbb{Z}$
2. Odd : $n = 2b+1$; $b \in \mathbb{Z}$
3. Even integer : $s = 2k$; $k \in \mathbb{Z}$

	Step	Reason
1.	$m+n = (2a+1)+(2b+1)$	Def. 1., 2. (U. Instantiation)
2.	$m+n = 2a+2b+2$	1.
3.	$m+n = 2(a+b+1)$	2.
4.	$m+n = 2k$	Substitution $k = k+a+b$
5.	$m+n$ is even integer.	Def. 3. (U. Gen)

■

eg. The square of an even integer is even

Claim $\forall (m \in \mathbb{Z})(m \in \mathbb{Z}_{even} \to m^2 \in \mathbb{Z}_{even})$

Definition Even integer : $s = 2k$; $k \in \mathbb{Z}$

	Step	Reason
1.	$m^2 = m \times m$	-
2.	$m^2 = (2a)(2a)$	Definition (Universal Instantiation)
3.	$m^2 = 2(2a^2)$	-
4.	$m^2 = 2k$	Substitution $k = 2a^2$
5.	m^2 is even integer	Definition (U. Gen.)

■

eg. If n is odd, then n^2 is odd.

Claim $\forall(n \in \mathbb{Z})(n \in \mathbb{Z}_{odd} \rightarrow n^2 \in \mathbb{Z}_{odd})$

Def Odd: $n = 2a+1$

Short:
$$n^2 = (2a+1)^2$$
$$n^2 = 4a^2+4a+1$$
$$n^2 = 2(2a^2+2a)+1$$
$$n^2 = 2k+1 \ ; \ k = 2a^2+2a$$

n^2 is odd. ∎

eg. If m, n are perfect sq. then mn is perfect sq.

Def. Perfect Square: $y = x^2$

Claim $\forall(a,b,c \in \mathbb{R})(m = a^2 \wedge n = b^2 \rightarrow mn = c^2)$

mn	$= (a^2)(b^2)$	Universal Inst. by Def.
mn	$= (ab)^2$	-
mn	$= k^2$	Substitution $k = ab$
mn	is perfect sq.	Universal Generalization by Def

∎

eg. Sum of 2 rational no. is rational.

Def. x is Rational $\leftrightarrow (x = \frac{p}{q} \ ; \ p,q \in \mathbb{R}, q \neq 0)$

Claim $\forall(x,y \in \mathbb{R})(x, y$ is rational $\rightarrow x+y$ is rational$)$

1. $x = \frac{p_1}{q_1}$ ✓
2. $y = \frac{p_2}{q_2}$ ✓
3. $x+y = \frac{p_1}{q_1} + \frac{p_2}{q_2}$ ✓
4. $x+y = \frac{p_1 q_2 + q_1 p_2}{q_1 q_2}$ ✓
5. $x+y = \frac{k_1}{k_2}$ Substitution
6. $x+y$ is rational ✓ ∎

1 $q_1 \neq 0, q_2 \neq 0$
$\rightarrow q_1 q_2 \neq 0$

② PROOF BY CONTRAPOSITION $((p \to q) \leftrightarrow (\neg q \to \neg p))$

eg. Prove that if $n = ab$; $a, b > 0 \in \mathbb{Z}$, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$

By contraposition;

Claim $\quad a > \sqrt{n} \land b > \sqrt{n} \to n \neq ab$

Given $\quad a \in \mathbb{Z}, b \in \mathbb{Z}, a > 0, b > 0$

1.	$ab > \sqrt{n} \cdot \sqrt{n}$	By inequalities.
2.	$ab > n$	1.
3.	$ab \neq n$	2.

■

fixed.

eg. If $n \in \mathbb{Z}$ and n^2 is odd, then n is odd.

For $n \notin \mathbb{Z}$, the statement is True.

By contraposition;

Def $\quad n$ is odd $\leftrightarrow n = 2k+1$

$\quad n$ is even $\leftrightarrow n = 2k$

Claim $\quad \forall (n \in \mathbb{Z})(n \text{ is even} \to n^2 \text{ is even})$

1.	$n = 2a$	U. Inst.
2.	$n^2 = (2a)(2a)$	1.
3.	$n^2 = 2(2a^2)$	2.
4.	$n^2 = 2k$	Def.
5.	n^2 is even	U. Gen.

■

Direct proof:

$$n^2 = 2k+1$$
$$n = \sqrt{2k+1}$$
$$k = 2a^2 + 2a$$
$$n = \sqrt{4a^2 + 4a + 1}$$
$$n = \sqrt{(2a+1)^2}$$
$$n = 2a+1$$

■

สุญญากาศ - ว่างเปล่า , เงื่อนไขว่างเปล่า

③ **VACUOUS PROOF** : $p \to q$: พิสูจน์ให้ $p \equiv F$

④ **TRIVIAL PROOF** : $p \to q$: พิสูจน์ให้ $q \equiv T$

ไม่ตรงเงื่อนไขของ สมาชิกนอก set (ไม่เกี่ยวข้องกัน)

เป็นจริงตลอดอยู่แล้ว!

eg. $P(n) \equiv$ " $n > 1 \to n^2 > n$ " . Show that $P(0)$ is true.

$P(0) \equiv$ " $0 > 1 \to 0 > 0$ " .

$P(0) \equiv F \to F$

$P(0) \equiv T$ ■

แปลก !

eg. $P(n) \equiv$ " $(a>0) \wedge (b>0) \wedge (a \geq b) \to (a \geq b)$ " Show that $P(0)$ is true.

$P(0) \equiv$ " $(0>0) \wedge (0>0) \wedge (0 \geq 0) \to (0 \geq 0)$ "

$P(0) \equiv F \to T$

$P(0) \equiv T$ ■

eg. If f is strictly increasing, then f is injective.

⑤ **PROOF BY CONTRADICTION**

Assumption ($\neg S$ เป็น tautology)

ต้องการ prove S เป็น tautology
ให้ $\neg S$ เป็น contradiction โดยให้ S เป็น contradiction ก่อน ถ้าผลลัพธ์ contradict
กับ Assumption แปลว่า S เป็น tautology ($\lightning$) Which is absurd.
↳ แปลว่า S กับ $\neg S$ เป็น tautology พร้อมกันไม่ได้ !

eg. No integer y, z exist for which $24y + 12z = 1$

By contradiction : There exists y, z which $24y + 12z = 1$

$$12(2y+z) = 1$$

$$2y + z = \frac{1}{12}$$ which the sum of two integers

can't be a non-integer sum. $\lightning$

Therefore, there is no y, z which $24y + 12z = 1$ ■

eg. At least 10 of any 64 days chosen must fall on the same day of the week.

By contradiction: At most 9 days of 64 days chosen are same days.

The Total days is $9 \times 7 = 63$ days which is not 64 days $\lightning$

eg. There is no greatest even integer.

By contradiction: There is the greatest even integer.

Construct a set of ALL even integer $E = \{e_1, e_2, e_3, \ldots, e_n\}$; $|E| = n$,

$e_k > e_{k-1}$; $k \in \{2, 3, 4, \ldots, n\}$

Using the sum of two even integers is an even integer,

$$e = e_n + e_{n-1} \text{ ; } e \text{ is an even.}$$

$$\therefore e > e_n \text{ ; } e \notin E. \lightning$$

eg. There are infinitely many primes.

Using contradiction, there are finite number of primes.

Construct a set of ALL primes $P = \{p_1, p_2, p_3, \ldots, p_n\}$; $|P| = n$,

$p_k > p_{k-1}$; $k \in \{2, 3, 4, \ldots, n\}$

A composite number N: $N = \prod_{i=1}^{n} p_i$ which $N > \prod_{i=a}^{b} p_i$; $a \leq b < n$

There is a composite number $N+1$; $N+1 < p_1 N$ but $p \in P$ can't construct $N+1$, so there must be primes other than $p \in P$ $\lightning$

For example: $N = 8 = 2^3$; $P = \{2\}$

$N+1 = 9 = 3^2$; $3 \notin P$

eg. $\sqrt{2}$ is irrational

By contradiction, $\sqrt{2}$ is rational.

By definition of rational number :

$$\sqrt{2} = \frac{a}{b} \quad ; \quad a, b \in \mathbb{Z}, \; b \neq 0, \; \gcd(a,b) = 1$$

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2$$

By fact , a^2 is even $\rightarrow$ a is even ; $a \in \mathbb{Z}$:

$$a = 2k$$

$$2b^2 = (2k)^2$$

$$b^2 = 2k^2$$

By fact , b^2 is even $\rightarrow$ b is even ; $b \in \mathbb{Z}$:

$$b = 2h$$

But, $\gcd(a,b) = \gcd(2k, 2h)$

$$\gcd(a,b) \neq 1 \quad \lightning$$

Prove If n is an integer and n^3+5 is odd, then n is even.

1.) Direct proof

By fact: The sum of odd integer and even integer is odd.

By def. $n = 2k$, $n^3 = 8k^3$

$n^3 = 2(4k^3)$

$n^3 = 2q$; $q = 4k^3$

$\therefore$ By definition, n^3 is even and 5 is odd.

Yields: n^3+5 is odd while n is even ■

2.) By contraposition, $n \in \mathbb{Z}$, If n is odd, then n^3+5 is even.

Using contradiction, If n is odd, n^3+5 is odd.

By def., $n = 2k+1$, $n^3 = (2k+1)^3$

$n^3 = 8k^3 + 12k^2 + 6k + 1$

$n^3 = 2(4k^3+6k^2+3k)+1$

$n^3+5 = 2(4k^3+6k^2+3k+3)$

$n^3+5 = 2q$; $q = 4k^3+6k^2+3k+3$

$\therefore$ n^3+5 is even but n^3+5 is odd $\lightning$

Prove by Case

Prove $\forall x \in \mathbb{R}\ ((x>1) \vee (x<-1) \rightarrow |x| > 1)$

By contradiction, $(x>1) \vee (x<-1) \rightarrow |x| \leq 1$

By definition, $|x| = \begin{cases} x & x>0 \\ -x & x<0 \end{cases}$

<u>Prove</u> $|xy| = |x||y|$; $x, y \in \mathbb{R}$

By contradiction, $|xy| \neq |x||y|$

<u>Def.</u> $|a| = \begin{cases} a & a \geq 0 \\ -a & a < 0 \end{cases}$

Case $(x>0, y>0)$: $xy > 0$

$$\left.\begin{aligned} xy &\neq (x)(y) \\ \text{But } xy &= xy \end{aligned}\right\} \text{—(1)}$$

Case $(x>0, y<0)$: $xy < 0$

$$\left.\begin{aligned} -xy &\neq (x)(-y) \\ \text{But } -xy &= -xy \end{aligned}\right\} \text{—(2)}$$

รวบได้
(WLOG)

Case $(x<0, y<0)$: $xy > 0$

$$\begin{aligned} xy &\neq (-x)(-y) \\ xy &\neq xy \quad \text{—(3)} \end{aligned}$$

Case $(x<0, y>0)$: $xy < 0$

$$\begin{aligned} -xy &\neq (-x)(y) \\ -xy &\neq -xy \quad \text{—(4)} \end{aligned}$$

From (1), (2), (3), (4), All contradict premise $|xy| = |x||y|$ ↯

Prove $n \in \mathbb{Z}$, then $2n^2+n+1$ is not divisible by 3

Case $(n=3p)$: $2n^2+n+1 = 2(3p)^2+3p+1$

$= 18p^2+3p+1$

$= 3(6p^2+p)+1$

$= 3k+1$; $k = 6p^2+p$

Which $3 \equiv 3k+1 \pmod 1$: $3 \nmid 3k+1$

Case $(n=3p+1)$: $2n^2+n+1 = 2(3p+1)^2+(3p+1)+1$

$= 18p^2+15p+4$

$= 18p^2+15p+3+1$

$= 3(6p^2+5p+1)+1$

$= 3k+1$; $k = 6p^2+5p+1$

Which $3 \equiv 3k+1 \pmod 1$: $3 \nmid 3k+1$

Case $(n=3p+2)$:

Chain of Equivalence

$$p_1 \leftrightarrow p_2 \leftrightarrow p_3 \leftrightarrow \dots \leftrightarrow p_n$$

eg. $p_1 \leftrightarrow p_2 \leftrightarrow p_3$ $(n > 2)$

$$\equiv (p_1 \to p_2) \wedge (p_2 \to p_1) \wedge (p_2 \to p_3) \wedge (p_3 \to p_2) \wedge (p_1 \to p_3) \wedge (p_3 \to p_1)$$

$$\equiv \underbrace{(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge (p_3 \to p_1)} \wedge \underbrace{(p_3 \to p_2) \wedge (p_2 \to p_1) \wedge (p_1 \to p_3)}_{\text{Not necessary}}$$

* Prove this instead:

Either all p_n are False or all True.

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

- Constructive : pick an example k which makes $P(k)$ True.
- Non-constructive * Use other ways... for example, No k will make $P(k)$ True.

eg. Show that $\exists x \exists y (x^y$ is rational$)$ where X and Y are irrational

$\sqrt{2}$ is irrational

If $\sqrt{2}^{\sqrt{2}}$ is rational, the theorem is proved.

If $\sqrt{2}^{\sqrt{2}}$ is irrational: Set $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$:

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$$

$$x^y = \sqrt{2}^2$$

$x^y = 2$ which is rational, hence the theorem is also proved. ■

Uniqueness Proof

1. $\exists x P(x)$
2. $\forall y \{y \neq x\} P(x)$ is False

↳ $\exists x (P(x) \wedge \forall y (y \neq x \to \neg P(y)))$

eg Show that every integer has a unique additive inverse.

By contradiction, there is $q_1 \neq q_2$ which makes $p+q_1=0$ and $p+q_2=0$

Suppose integers p, q, q_1, q_2.

$$p+q=0$$
$$\therefore \quad q=-p \quad \text{(There exists an additive inverse of } p \text{ which is } q\text{)}$$

$$p+q_1 = p+q_2$$
$$\therefore \quad q_1 = q_2 \quad \lightning$$

<u>Counterexamples</u> : Show that $\forall x P(x)$ is False.

eg Every positive integer is the sum of sq. of 3 integers.

For example, $6 = 1^2 + 1^2 + 2^2$

But, takes 7 for example, it can't be any combination of sum of squares of 3 integers.

<u>Mathematical Induction</u> (Induce the fact that this works, then next might works too and so on.) "อุปนัย"

We want to proof $P(n)$; $n \in S$, $S = \{b, b+1, b+2, \dots\}$

<u>Proof</u> 1. $P(b)$ is True. (Starts) : Base case

2. $P(k) \rightarrow P(k+1)$ is True for every $k \in S$. (Next) : Step case

กล่าวคือ : $\boxed{\text{True}} \rightarrow \text{True} \rightarrow \text{True} \rightarrow \text{True} \rightarrow \dots$

eg. Sum of the first n odd positive integers is n^2

$P(n) \equiv 1+3+5+\ldots+(2n-1) = n^2$

$P(1) \equiv 1 = 1^2 \rightarrow P(1) \equiv T$

Inductive hypothesis, For P(k) $1+3+5+\ldots+(2k-1) = k^2$ —(1)

$1+3+5+\ldots+(2k-1)+(2k+1) = (k+1)^2$ —(2)

$(2)-(1): \quad ((2k+1)+(2k-1)+\ldots+5+3+1) - ((2k-1)+\ldots+5+3+1) = (k+1)^2 - k^2$

$2k+1 = k^2+2k+1-k^2$

$2k+1 = 2k+1$

Hence, P(n) is True ■

eg. Prove that $n < 2^n$ for all positive integers n.

$P(n) \equiv n < 2^n \; ; \; n \in \mathbb{Z}_{>0}$

Using inductive hypothesis,

$P(1) \equiv 1 < 2^1$

$P(1) \equiv T$

$P(k): \quad k < 2^k$

$k+1 < 2^k + 1$

$k+1 < 2^k+1 < 2^k + 2^k$

$\therefore \; k+1 < 2^{k+1}$

Hence, $P(k) \rightarrow P(k+1)$.

Therefore, P(n). ■

eg. Prove that the sum of first n positive integers is $\frac{(1+n)n}{2}$.

$P(n)$: $1+2+3+\ldots+n = \frac{(1+n)n}{2}$

Using inductive hypothesis,

$P(1)$: $1 = \frac{(1+1)\cdot 1}{2}$

$\therefore 1 = 1$

$\therefore P(1) \equiv T$

Suppose $P(k)$: $1+2+3+\ldots+k = \frac{(1+k)k}{2}$ —(1)

and $P(k+1)$: $1+2+3+\ldots+k+(k+1) = \frac{(1+k+1)(k+1)}{2}$ —(2)

Substitute (1) in (2) : $\frac{(1+k)k}{2} + (k+1) = \frac{(2+k)(1+k)}{2}$

$$\frac{k+k^2+2k+2}{2} = \frac{(2+k)(1+k)}{2}$$

$$\therefore \frac{k^2+3k+2}{2} = \frac{k^2+3k+2}{2}$$

Hence, $P(k) \rightarrow P(k+1)$.

Therefore, $P(n)$ ■

eg. Prove that $n^3 - n$ is divisible by 3 all pos. integers n

$P(n)$: $3 \mid n^3 - n$; $n \in \mathbb{Z}_{>0}$ or $n^3 - n = 3p$

Using inductive hypothesis,

$P(1)$: $3 \mid 1^3 - 1$

$3 \mid 0$ which is True.

$P(1) \equiv T$

หรือ Suppose

$P(k)$: $k^3 - k \equiv 0 \pmod 3$

Suppose $P(k)$: $3 \mid k^3 - k \leftrightarrow k^3 - k = 3p_k$ —(1)

and $P(k+1)$: $3 \mid (k+1)^3 - (k+1) \leftrightarrow (k+1)^3 - (k+1) = 3p_{k+1}$ —(2)

If $3 \mid m_1$ and $3 \mid m_2$, then $3 \mid m_2 - m_1$.

$$(2)-(1) : (\cancel{k^3} + 3k^2 + 3k + \cancel{1} - \cancel{k} - \cancel{1}) - (\cancel{k^3} - \cancel{k}) = 3p_{k+1} - 3p_k$$

$$3k^2 + 3k = 3p_{k+1} - 3p_k$$

$$3k^2 + 3k = 3(p_{k+1} - p_k)$$

$$3(k^2 + 3k) = q \quad ; \quad q = 3p_{k+1} - 3p_k$$

$$\therefore 3 \mid 3k^2 + 3k$$

Hence, $3 \mid k^3 - k$.

Therefore, $P(n)$ ∎

eg. Prove that $1^3 + 2^3 + 3^3 + \dots + n^3 = \dfrac{n^2(n+1)^2}{4}$

$$P(n) : 1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4} ; \quad n \in \mathbb{Z}_{>0}$$

Using inductive hypothesis,

$$P(1) : 1^3 = \frac{1^2(1+1)^2}{4}$$

$\therefore 1 = 1$ which is True.

$\therefore P(1) \equiv T$

$P(j) : j = k-1$

$$\cancel{1^3 + 2^3 + \dots + (k-1)^3} = \frac{(k-1)^2 k^2}{4}$$

$P(j+1)$

$$\cancel{1^3 + 2^3 + \dots + (k-1)^3} + k^3 = \frac{(k^2)(k+1)^2}{4}$$

$$k^3 = \frac{k^2}{4}\Big(\underbrace{(k+1)^2 - (k-1)^2}_{4k}\Big)$$

$$\therefore k^3 = k^3 \quad \blacksquare$$

Suppose $P(k) : 1^3 + 2^3 + 3^3 + \dots + k^3 = \dfrac{k^2(k+1)^2}{4}$ —(1)

and $P(k+1) : 1^3 + 2^3 + 3^3 + \dots + k^3 + (k+1)^3 = \dfrac{(k+1)^2(k+2)^2}{4}$ —(2)

$$(2) - (1) : [1^3 + 2^3 + 3^3 + \dots + k^3 + (k+1)^3] - [1^3 + 2^3 + 3^3 + \dots + k^3]$$

$$= \frac{(k+1)^2(k+2)^2}{4} - \frac{k^2(k+1)^2}{4}$$

$$(k+1)^3 = \frac{(k+1)^2}{4}\left((k+2)^2 - k^2\right)$$

$$(k+1)^3 = \frac{(k+1)^2}{4}(\cancel{k^2} + 4k + 4 - \cancel{k^2})$$

$$(k+1)^3 = \frac{(k+1)^2}{4}(4k+4)$$

$$\therefore (k+1)^3 = (k+1)^3$$

Hence, $P(k) \to P(k+1)$.

Therefore, $P(n)$ $\blacksquare$

Strong Induction

$$\underbrace{[P(1) \wedge P(2) \wedge \ldots \wedge P(k)]}_{\text{Base cases (Direct Determination)}} \rightarrow \underset{\text{Inductive Cases}}{\underset{\downarrow}{P(k+1)}}$$

eg. Show that for $n > 1$: n is a product of primes.

$P(n)$: $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$

Using inductive hypothesis,

Base Cases : $2 = 2$

Step Cases : $P(k+1)$: If $k+1$ is a prime the theorem is proven.

If $k+1$ is not a prime, $k+1 = ab$; $a, b < k$

and $P(a), P(b)$ ← IDea of Recursion.

COUNTING TECHNIQUES

- Counting by cases :

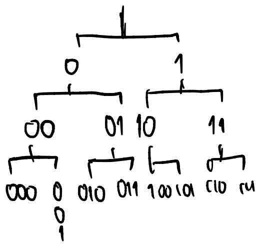
  $* \; S_i \cap S_{j \neq i} = 0$

  $* \; \bigcup_{i=1}^{N} S_i = \mathcal{U}$

★ The Sum Rule $[N = N_A + N_B + N_C + \dots]$

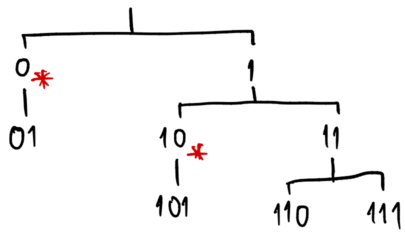
- Tree Diagram

eg. bit strings with 3 bits

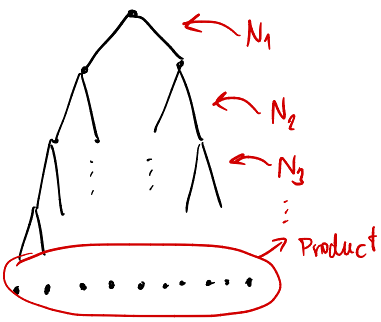


eg. bit strings without 00

if 0, next must not be 0



★ The Product Rule



$N = N_1 N_2 N_3 \dots$

* โดย N_i ต้อง consistent

eg. How many functions? $f_{X \to Y}$

$X \to Y$

$|X| = m$ $|Y| = n$ "cardinality"

$\{x_1, x_2, x_3, \dots, x_i, \dots, x_m\}$ $\{y_1, y_2, y_3, \dots, y_i, \dots, y_n\}$

ใช้หมด!

$$\left.\begin{array}{l} f_1 : \overbrace{(x_1, y_1), (x_1, y_2), \dots, (x_1, y_n)}^{n \text{ แบบ}} \\ f_2 : (x_2, y_1), (x_2, y_2), \dots, (x_2, y_n) \\ \vdots \\ f_m : (x_m, y_n) \end{array}\right\} m \text{ ครั้ง}$$

$$\#\text{แบบของ } f = \underbrace{n \times n \times \dots \times n}_{m \text{ ครั้ง}}$$

$$N = n^m$$

⊕ How many one-to-one f. $(f: X \xrightarrow{1-1} Y)$

(x_1, y_1) ← $\cancel{(x_2, y_1)}$, (x_2, y_2), … ← ( ) …

(x_1, y_2)

⋮

(x_1, y_n)

$(m=1)$	$(m=2)$	$(m=3)$	$(m=m)$
n แบบ	$n-1$ แบบ	$n-2$ แบบ	$n-(m-1)$ แบบ
	(Used y)	(Used 2 y's)	

$$\therefore N = n(n-1)(n-2)\ldots(n-m+1) = \frac{n!}{(n-m)!} \quad \text{(Permutation)}$$

eg. A password with 6 to 8 characters ; A–Z, how many pwd. are possible

$$N = N_6 + N_7 + N_8$$

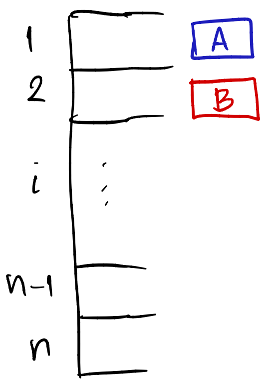
$$N_6 = \underbrace{26 \cdot 26 \cdot \ldots \cdot 26}_{6} = 26^6$$

$$N_7 = 26^7$$

$$N_8 = 26^8$$

$$N = 26^8 + 26^7 + 26^6$$

eg. A parking lot with a row of n parking spaces.
Only 2 cars can park. How many ways can they park



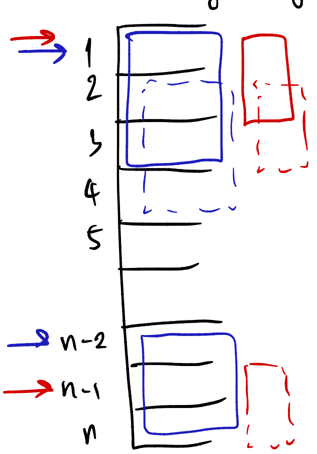
(A, B)

n แบบ, $n-1$ แบบ

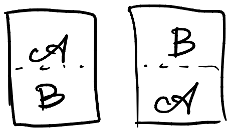
$\therefore N = n(n-1)$

⊕ How many ways if there can be at most one space.

Sol 1

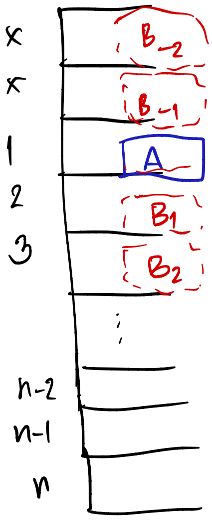


N = (Grouping of 3) × Swap
+ (Grouping of 2) × Swap



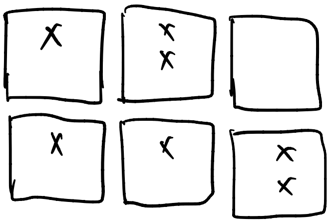
$$N = (n-2) \times 2 + (n-1) \times 2 \quad \divideontimes$$

Sol 2



There will be duplicates!

- The Pigeonhole Principle "If $n>k$ objects are placed into k objects, there are at least one box containing two or more objects"



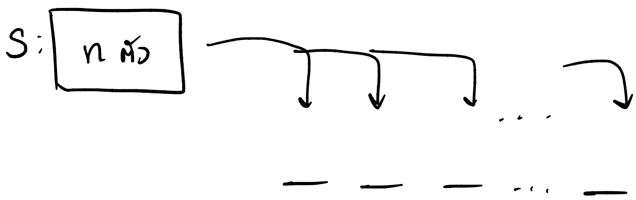
6 boxes 7 objects $(k=6,\ n=7)$

i.e., $\left\lceil \frac{N}{k} \right\rceil > 1$

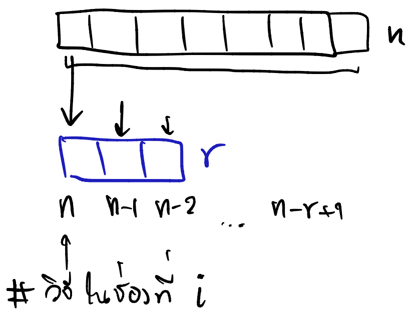
- Permutations

"Ordered arrangement of r elements" from a set with n elements → r-Permutation

* If $r=n$, เรียกว่า Permutation.



r-Permutation



$$\rightarrow P(n,r) = n(n-1)(n-2)\dots(n-r+1)$$

$$P(n,r) = \frac{n!}{(n-r)!}$$

eg. How many ways to select 1^{st}, 2^{nd}, 3^{rd} Prize from 100 ppl.

$$\underset{1^{st}}{\underbrace{100\ p.}} \quad \underset{2^{nd}}{\underbrace{99\ p.}} \quad \underset{3^{rd}}{\underbrace{98\ p.}}$$

$$P(n,r) = 100 \times 99 \times 98 \quad \Big| \quad P(n,r) = \frac{100!}{98!}$$

- Combinations

" A set of r elements from a set with n elements "

* (Unordered set) (Subset)

$\{1,2,3\} = \{3,1,2\} = \{2,1,3\} \ldots$

$$\underset{1}{\_\_} \ \underset{2}{\_\_} \ \underset{3}{\_\_} \ \underset{4}{\_\_} \ \ldots \ \underset{r}{\_\_}$$

Ordered list can be $P(n,r)$ ถอดลำดับออก
but it can be sorted $r!$ ways,
So there are $\frac{P(n,r)}{r!}$ combinations ✓

$$\therefore \quad C(n,r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

หรือ Prove ด้วย ให้ set ที่มีจำนวนสมาชิก r มาเรียงได้ r! วิธี → P(n,r) :

$$P(n,r) = C(n,r) \cdot r! \quad ✓$$

eg. Selecting 3 winners from 100 people

$$N = C(n,r) = \frac{100!}{3!\,97!}$$

eg. How many bit strings of length 10 contain more than 2 ones.

Case 1 $\quad$ 1 1 1 _ _ | _ _ _ _ _

Case 2 $\quad$ 1 1 1 1

Case 3 $\quad$ 1 1 1 1 1

⋮

Case 8 $(n-r+1)$ $\quad$ All 1

$$N = N_1 + N_2 + \ldots + N_8$$

$$N_1 = C(10,3)$$
$$N_2 = C(10,4)$$
$$\vdots$$
$$N_8 = C(10,10)$$

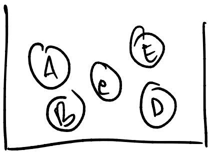
$$\therefore N = \sum_{i=3}^{10} C(10,i)$$

หรือ มี$\underbrace{\text{ทั้งหมด } 2^{10}}_{\text{All cases}}$ แบบ หัก $C(10,2)$, $C(10,1)$, $C(10,0)$ ออก

ได้สมบัติ : $\quad 2^n = \sum_{i=0}^{n} C(n,i)$

Generalizing Permutation & Combination.

i.e., When an element is used, it can be used again.



1. Draw a sequence of 3 balls : $P(5,3)$
2. Draw and put it back a seq. of 3 balls :

$\_\ \_\ \_ \rightarrow N = 5^3$

5 แบบ 5 แบบ 5 แบบ

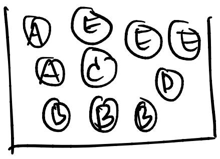
3. Draw 3 balls at once : $C(5,3)$

Unordered selection (duplicates allowed.)

eg. AAA, ABC, ABB, ... ?

$\_\ \_\ \_$

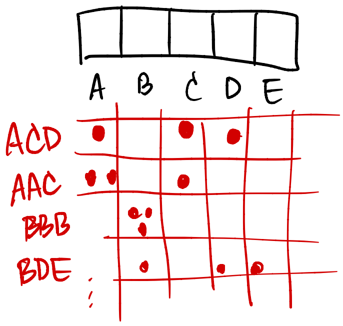
หรือ



?

• Combinations with Repetition

$\underline{5} \times \underline{4} \times \underline{3}\ (\div 3!)$



Case 1: ไม่ซ้ำเลย (1 ลูก, unique) $C(5,3) = \frac{5!}{3!2!} = 10$ แบบ

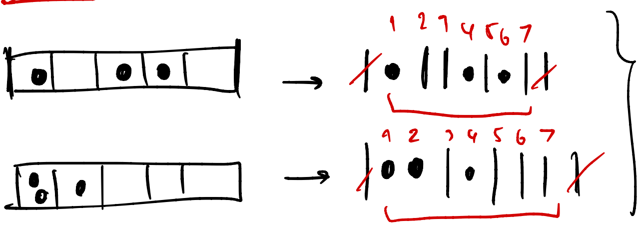
$\boxed{5} \times \underline{4}$ (สลับที่ไม่ได้ ไม่เหมือนกัน)

Case 2: มีซ้ำ 2 ลูก $5 \times 4 = 20$ แบบ

Case 3: มีซ้ำ 3 ลูก 5 แบบ $C(5,1) = \frac{5!}{4!1!} = 5$ แบบ

$\therefore N = 35$ แบบ.

* หรือ * เปลี่ยนช่องเป็นขีด



$\leftrightarrow$ Bit string length 7 with 3 zeroes.

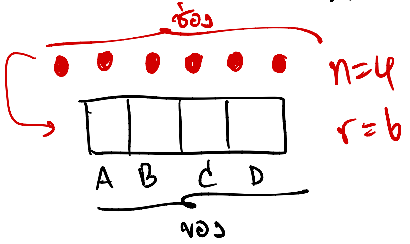
$C(7,3) = \frac{7 \times 6 \times 5}{3!} = 35$ แบบ

ของ n แบบ เลือกใส่ r : $N = C(r+n-1, r) = C(r+n-1, n-1)$

จะได้

(From $C(n,r) = C(n, n-r)$)

e.g. มี cookies 4 แบบ ต้องการซื้อ 6 ชิ้น $\qquad H(n,r) = C(r+n-1, r)$



$n=4$

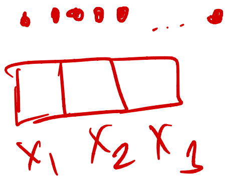
$r=6$

$\therefore N = C(6+4-1, 6) = H(4,6)$

$= C(9,6) = C(9,3)$

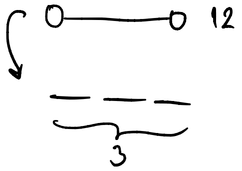
e.g. มีสมการ $x_1 + x_2 + x_3 = 11$; $x_i \in \mathbb{Z}_{\geq 0}$

(x_1, x_2, x_3) มีได้กี่แบบ



$H(3,11)$

Model $x_{max} = 11$, $x_{min} = 0 \rightarrow |X| = 11$



$\rightarrow N = C(11+3-1, 11) = C(13,11) = C(13,2)$

$= \cancel{C(14,12) = C(14,2)}$

Binomial Theorem

$$a^n - b^n = (a-b)\sum_{i=0}^{n-1} a^{(n-1)-i} b^i$$

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

Inclusion - Exclusion Principle

Generalized Form :

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n}|A_i| + \sum_{m=2}^{n}(-1)^{m+1}\left|\bigcap_{i=1}^{m} A_i\right|$$

$|A_1 \cup A_2 \cup \ldots \cup A_n|$ $\qquad$ $|A_1|+|A_2|+\ldots+|A_n|$

$\hookrightarrow -|A_1\cap A_2| - |A_1 \cap A_3| - \ldots - |A_{n-1}\cap A_n|$
$+ |A_1 \cap A_2 \cap A_3| + \ldots$
$\ldots$

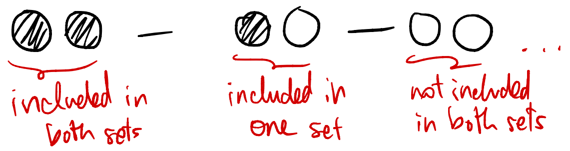
Total:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{m=1}^{n}(-1)^{m+1}\left|\bigcap_{i=1}^{m} A_i\right|$$

<u>Proof</u> : แต่ละ section x ที่ถูกนับใน union จะถูกนับแค่เพียง 1 ครั้งเท่านั้น (Goal)

$\hookrightarrow$ Let x be an element of exactly r sets.

r :



จาก Inc. Exc. Princ.

$\sum |A_i| \longrightarrow$ มี x ถูกนับ จำนวน r ตัว $= \binom{r}{1}$

$-\sum |A_i^{(1)} \cap A_i^{(2)}| \longrightarrow$ มี x ถูกนับ $\binom{r}{2}$ (intersect 2 ตัว ได้ $\binom{r}{2}$ แบบ)

$+\sum |A_i^{(1)} \cap A_i^{(2)} \cap A_i^{(3)}| \longrightarrow \binom{r}{3}$

$- \cdots + (-1)^{r+1}\sum |A_i \cap \ldots \cap A_r| \longrightarrow \binom{r}{r}$

$+ \cdots + (-1)^{n+1}\sum |A_i \cap \ldots \cap A_n| \longrightarrow$ x ไม่ถูกนับ (ไม่อยู่ใน r sets) [สมมติ]

$$\therefore |x| = \binom{r}{1} - \binom{r}{2} + \binom{r}{3} - \cdots + (-1)^{r+1}\binom{r}{r}$$

ใช้ $(x+y)^r = \sum_{k=0}^{r}\binom{r}{k}x^{r-k}y^k$; $x = 1,\ y = -1$

$$\underbrace{(1+(-1))^r}_{0} = \binom{r}{0} \underbrace{- \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \ldots + (-1)^r\binom{r}{r}}_{1 - |x|}$$

$0 = 1 - |x|$

$\therefore |x| = 1$ เสมอ

$\blacksquare$

eg. How many integers from 1 to 9,999 can be div. by 7, 10, or 13

i.e., 7, 14, 21, ... $\rightarrow \left\lfloor \frac{9999}{7} \right\rfloor$, $|A_a \cap A_b| = |A_{ab}|$

Let sets $A_7, A_{10}, A_{13} \longrightarrow |A_7 \cup A_{10} \cup A_{13}|$

$$= |A_7| + |A_{10}| + |A_{13}| - |A_{70}| - |A_{130}| - |A_{91}| + |A_{910}|$$

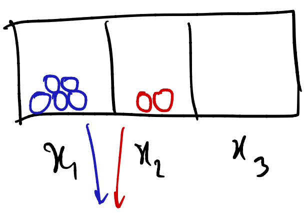
$$= \left\lfloor \frac{9999}{7} \right\rfloor + \left\lfloor \frac{9999}{10} \right\rfloor + \left\lfloor \frac{9999}{13} \right\rfloor - \left\lfloor \frac{9999}{70} \right\rfloor - \left\lfloor \frac{9999}{130} \right\rfloor - \left\lfloor \frac{9999}{91} \right\rfloor + \left\lfloor \frac{9999}{910} \right\rfloor$$

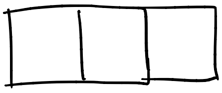
$$= \boxed{\quad} \quad \#$$

Finding $|A_1 \cap A_2 \cap \dots \cap A_n|$ $\longrightarrow C(102, 100)$

eg. $x_1 + x_2 + x_3 = 100$; $x_1, x_2, x_3 \in \mathbb{Z}_{\geq 0}$

① ... และ $x_1 \geq 5$, $x_2 \geq 2$ $\qquad H(3, 93)$



จาก $\underbrace{1, 1, 1, 1, 1, \dots, 1, 1, 1}_{100 - 5 - 2 = 93}$ $\longrightarrow$  จาก $\underbrace{1, 1, 1, 1, \dots}_{93}$

$x_1 \quad x_2 \quad x_3$

Fixed (constrained)

$\leadsto C(93 + 3 - 1, 93)$

$|A_1' \cap A_2' \cap A_3'| = |U| - |A_1 \cup A_2 \cup A_3|$
$= |U| - \sum IE.$

② ... และ $x_1 \leq 5$, $x_2 \leq 20$, $x_3 \leq 50$

Case ทั้ง : $C(102, 100)$

Case $x_1 \leq 5$: A_1 $\longrightarrow$ Case $x_1 > 5$ ($x_1 \geq 6$) : $C(100 - 6 + 3 - 1,\ 100 - 6)$: B_1

Case $x_2 \leq 20$: A_2 $\longrightarrow$ Case $x_2 > 20$ ($x_2 \geq 21$) : $C(100 - 21 + 3 - 1,\ 100 - 21)$: B_2

Case $x_3 \leq 50$: A_3 $\longrightarrow$ Case $x_3 > 50$ ($x_3 \geq 51$) : $C(100 - 51 + 3 - 1,\ 100 - 51)$: B_3

จาก $|A_1 \cap A_2 \cap A_3| = |U| - |(A_1 \cap A_2 \cap A_3)'|$

$= |U| - |A_1' \cup A_2' \cup A_3'|$

$= |U| - |\underline{B_1 \cup B_2 \cup B_3}|$ $\longrightarrow$ กระจาย

(B_n คือ ตรงกันข้ามกับ A_n (A_n'))

We get

$|B_1 \cap B_2| = C(100 - 27 + 3 - 1,\ 100 - 27)$

$|B_1 \cap B_3| = C(100 - 57 + 3 - 1,\ 100 - 57)$

$|B_2 \cap B_3| = C(100 - 72 + 3 - 1,\ 100 - 72)$

$|B_1 \cap B_2 \cap B_3| = C(100 - 78 + 3 - 1,\ 100 - 78)$

Cont'd.

$$|A_1 \cap A_2 \cap A_3| = \underbrace{|U|}_{\text{Total cases w/o. constraints}} - \Big(\underbrace{|B_1| + |B_2| + |B_3| - |B_1 \cap B_2| - |B_1 \cap B_3| - |B_2 \cap B_3| + |B_1 \cap B_2 \cap B_3|}_{\text{Known}} \Big)$$

$$= C(102,100) - C(96,94) - C(81,79) - C(51,49) + C(75,73) + C(45,43) + C(40,38) - C(24,22) \quad \#$$

ต้องการ $f : X \xrightarrow{\text{onto}} Y$

Recurrence Relation

$\{a_n\} = a_0, a_1, a_2, \ldots, a_n$

e.g. $a_n = 5a_{n-1}$

$b_n = b_{n-1} - 2b_{n-1} + 100$

$c_n = c_{n-1} + c_{n-4} + \log_{10}(n) + e^n$

→ There is a sequence which is a solution to a_n [Recurring]

in a closed form.

e.g. $a_n = 3n$ is one of the solutions to $a_n = 2a_{n-1} - a_{n-2}$; $n \geq 2$

i.e., $3n = 2(3n-3) - (3n-6)$

$3n = 6n - 6 - 3n + 6$

$\therefore 3n = 3n$ ■

$a_n = n+1$ is also a solution. → "Initial Condition (ค่าตั้งต้น) มีผลกับค่าในลำดับตัวต่อ ๆ ไป"

เริ่ม when $n \geq 2$: a_0, a_1 are fixed as Init. Cond.

Goal: Solving / Modeling a solution to problem: sol. $= f(n)$ ...

By constructing $f(n)$ from smaller $f(k)$; $k < n$

e.g. Bit string ยาว n เป็นไปได้กี่แบบ : $f(n) = 2^n$

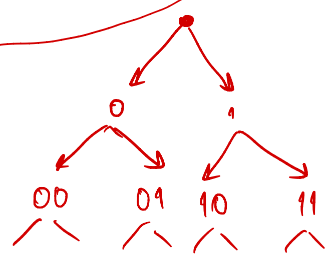
Closed form & Recurrence form

a_n ; จำนวน bit string ยาว n ที่เป็นไปได้

จะได้ $a_n = 2a_{n-1}$

*โดย $a_0 = 1$; $n = 1, 2, 3, \ldots$

หรือ $a_1 = 2$; $n = 2, 3, 4, \ldots$



$a_n = 2$

$a_{n+1} = 4$) 2

$a_{n+2} = 8$) 2

⋮

eg. A man running up n-step stairs, he can either takes either 1 or 2 steps.

How many different ways?

1 : 1 } $a_1 = 1$

2 : 1, 1 ; 2 } $a_2 = 2$

3 : 1, 1, 1 ; 1, 2 ; 2, 1 } $a_3 = 3$

4 : 1, 1, 1, 1 ; 1, 1, 2 ; 1, 2, 1 ; 2, 1, 1 ; 2, 2 } $a_4 = 5$

$a_n \xrightarrow{+1 \text{ step}} a_{n+1}$

$a_n \xrightarrow{+2 \text{ steps}} a_{n+2}$

$a_{n+1} \xrightarrow{+1} a_{n+2}$

$a_{n+1} \xrightarrow{+2} a_{n+3}$

$a_{n+2} \xrightarrow{+1} a_{n+3}$

$a_{n+2} \xrightarrow{+2} a_{n+4}$

$a_{n+2} = a_{n+1} + a_n$

Appear once.

$a_{n+3} = a_{n+2} + a_{n+1}$

Appear once.

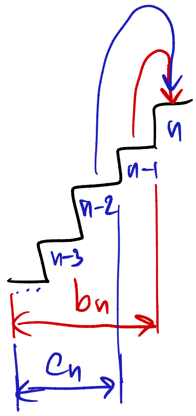
$\therefore a_n = a_{n-1} + a_{n-2}$

sol.

"ก้าวสุดท้ายก่อนมา a_n"

Sol. Case 1 step : b_n

case 2 steps : c_n } $a_n = b_n + c_n$



" การก้าวมาที่ a_n ก้าวมาได้ 2 แบบคือ

แบบ 1 ขั้น (b_n) และ 2 ขั้น (c_n) "

[Sums Rule] 1 วิธี ; 1 ขั้น only. 1 วิธี คือก้าว 2 ขั้น only.

จะได้ $a_n = \boxed{1}\, b_n + \boxed{1}\, c_n$

[Product Rules]

$b_n = a_{n-1}$

$c_n = a_{n-2}$

$\therefore a_n = a_{n-1} + a_{n-2}$; $a_1 = 1$, $a_2 = 2$, $n = 3, 4, 5, \ldots$

or $a_n = a_{n-1} + a_{n-2}$; $a_0 = 1$, $a_1 = 1$, $n = 2, 3, 4, \ldots$

วิธีการไม่ก้าว มีวิธีเดียว. (ทำอะไรไม่ได้เลย = 1)

ต่างกันที่ Information (Domain และ Range) ของปัญหา

กว้างกว่า = น่าจะดีกว่า หากครอบคลุมแล้วใช้ประโยชน์ได้

Homogeneous (linear combination)

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} \quad ; \quad c_i = \text{constants}$$

k^{th} Degree

* หากมี $a_k^{n>1} \rightarrow$ Non-linear (ไม่สนในวิชานี้)

Non-homogeneous

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} + F(n) \quad \text{(Linear)}$$

Solving Recurrence into a closed form.

$a_n = K_1 r^n$; K_1 can be anything at chosen r

is a solution of $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}$

Try: $a_n = \cancel{K} r^n = c_1 \cancel{K} r^{n-1} + c_2 \cancel{K} r^{n-2} + \dots + c_k \cancel{K} r^{n-k}$; $K \neq 0$

$$\frac{r^n}{r^{n-k}} = \left[c_1 r^{n-1} + c_2 r^{n-2} + \dots + c_k r^{n-k}\right] \frac{1}{r^{n-k}} \quad ; \quad r \neq 0$$

$$\boxed{r^k = c_1 r^{k-1} + c_2 r^{k-2} + \dots + c_k}$$

"Characteristic Equation"

สัมพันธ์ด้วยการเลือก r ที่สอดคล้องกับ a_n

$\rightarrow$ R_1 : $a_n = c_1 a_{n-1} + \dots + c_k a_{n-k}$

$a_n = D_1 r_1^n + D_2 r_2^n + \dots + D_k r_k^n$

$a_n \rightarrow R_1$; $\underbrace{D_1 r_1^n}_{S_1} + \underbrace{D_2 r_2^n}_{S_2} + \dots + \underbrace{D_k r_k^n}_{S_k} = c_1 D_1 r_1^{n-1} + c_1 D_2 r_2^{n-1} + \dots + c_1 D_k r_k^{n-1}$

$+ c_2 D_1 r_1^{n-2} + c_2 D_2 r_2^{n-2} + \dots + c_2 D_k r_k^{n-2}$

$\vdots$

$+ \underbrace{c_k D_1 r_1^{n-k}}_{S_1} + \underbrace{c_k D_2 r_2^{n-k}}_{S_2} + \dots + \underbrace{c_k D_k r_k^{n-k}}_{S_k}$

e.g. $\quad a_n = -5\overset{k=1}{a_{n-1}} - 6\overset{k=2}{a_{n-2}} \quad ; n \geq 2 \;,\; a_0 = 3 \;,\; a_1 = 7$

Char. eq. : $r^2 = -5r - 6$

$$r^2 + 5r + 6 = 0$$

$$r = -3, -2$$

$$\hookrightarrow a_n = A(-2)^n + B(-3)^n$$

จาก $\left.\begin{aligned} a_0 &= 3 = A + B \\ a_1 &= 7 = -2A - 3B \end{aligned}\right\}$ จะได้ $(A, B) = (16, -13)$

$$\therefore a_n = (-1)^n \left(16 \cdot 2^n - 13 \cdot 3^n\right)$$

$$a_n = (-1)^n \left(2^{n+4} - 13 \cdot 3^n\right)$$

$f_n = f_{n-1} + f_{n-2} \quad ; \quad r^2 = r + 1$

$$r^2 - r - 1 = 0$$

$$\rightarrow r = \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1}$$

$$= \frac{1}{2} \pm \frac{\sqrt{5}}{2} = \frac{\sqrt{5}+1}{2} \,,\; \frac{1-\sqrt{5}}{2}$$

$$\rightarrow a_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Necessary Conditions (Proof)

"All solution to ... must be in the form ... "

e.g. $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}$ (R1)

Sol: $a_n = K_1 r_1^n + K_2 r_2^n + \dots + K_k r_k^n$

Proof. If $r_1, r_2, r_3, \dots, r_k$ are roots of characteristic eqn. of R1.

Using proof by contradiction,

1. Let $r_1, r_2, \dots, r_k$ be roots of c.eqn. of R1
   but there is a_n which can't be written as $a_n = K_1 r_1^n + K_2 r_2^n + \dots + K_k r_k^n$

2. Let $b_n = E_1 r_1^n + E_2 r_2^n + \dots + E_k r_k^n$; therefore, b_n is a solution of R1 (by sufficient condition)

3. We can choose $E_1, E_2, \dots, E_k$ such that $b_0 = a_0$, $b_1 = a_1$, ..., $b_{k-1} = a_{k-1}$:

$$b_0 = E_1 r_1^0 + E_2 r_2^0 + \dots + E_k r_k^0$$
$$b_1 = E_1 r_1^1 + E_2 r_2^1 + \dots + E_k r_k^1$$
$$\vdots$$
$$b_{k-1} = E_1 r_1^{k-1} + E_2 r_2^{k-1} + \dots + E_k r_k^{k-1}$$

4. Since a_n, b_n are solutions to R1 and $a_n = b_n$ $\{n = 0, 1, 2, \dots, k-1\}$,
   $a_n = b_n$ $\{n = k, k+1, k+2, \dots\}$

5. From 3., 4., a_n must be written as $a_n = K_1 r_1^n + K_2 r_2^n + \dots + K_k r_k^n$
   which contradicts our assumption 1. ↯

e.g. Find sol : $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$; $a_0 = 2$, $a_1 = 5$, $a_2 = 15$

C.eqn. : $r^3 = 6r^2 - 11r + 6$

$$r^3 - 6r^2 + 11r - 6 = 0$$

$$(r-1)(r-2)(r-3) = 0$$

$$\therefore a_n = A + B \cdot 2^n + C \cdot 3^n$$

$$a_0 = A + B + C = 2$$
$$a_1 = A + 2B + 2C = 5$$
$$a_2 = A + 4B + 9C = 15$$

- Coeff. ซ้ำ (มี multiplicity)

e.g. $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$; $a_{0,1,2} = 1, -2, -1$

C.eqn. : $r^3 = -3r^2 - 3r - 1$

$$(r+1)^3 = 0 \rightarrow r = -1, m = 3$$

$$\therefore a_n = (A_0 + A_1 n + A_2 n^2)(-1)^n$$

$$a_0 = A_0(-1)^0 = 1 \longrightarrow A_0 = 1$$

$$\left.\begin{aligned} a_1 &= -A_0 - A_1 - A_2 = -2 \\ a_3 &= A_0 + 2A_1 + 4A_2 = -1 \end{aligned}\right\} A_1, A_2 = 3, -2$$

$$\therefore a_n = (1 + 3n - 2n^2)(-1)^n$$

$R_1: \ a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} + F(n)$ ⟶ Non-homogeneous RR.

homogeneous solution.

Let $a_n = a_n^{(h)} + a_n^{(p)}$ ⟶ particular solution.

ส่วนของคำตอบ
ที่เป็น homogeneous
$[c_1 a_{n-1} + \dots + c_k a_{n-k}]$

$$\rightarrow \underline{a_n^{(h)}} + a_n^{(p)} = \underline{c_1 a_{n-1}^{(h)}} + c_1 a_{n-1}^{(p)} + \dots + \underline{c_k a_{n-k}^{(h)}} + c_k a_{n-k}^{(p)} + F(n)$$

$$a_n^{(p)} = c_1 a_{n-1}^{(p)} + c_2 a_{n-2}^{(p)} + \dots + c_k a_{n-k}^{(p)} + F(n)$$

$$F(n) = a_n^{(p)} - c_1 a_{n-1}^{(p)} - c_2 a_{n-2}^{(p)} - \dots - c_k a_{n-k}^{(p)}$$

Suppose $a_n^{(p)} = D \cdot F(n)$

Key for solving non-homogeneous RR :

1. Solve homogeneous part.
2. Find particular solution.
3. Sum 1., 2. $a_n = a_n^{(h)} + a_n^{(p)}$

ขอบเขตโจทย์นี้ : $F(n) = (b_t n^t + b_{t-1} n^{t-1} + \dots + b_1 n + b_0) s^n$ ⟶ เป็น combination ของ polynomial · exponential

$$F(n) = \begin{cases} (p_t n^t + p_{t-1} n^{t-1} + \dots + p_1 n + p_0) s^n & ; \ s \text{ มีรากเดี่ยว} \\ n^m (p_t n^t + p_{t-1} n^{t-1} + \dots + p_1 n + p_0) s^n & ; \ s \text{ มีจำนวน } m \text{ ราก (multiplicity = m)} \end{cases}$$

e.g. $a_n = 3a_{n-1} + 2n \; ; \; a_1 = 3$

$\underbrace{3a_{n-1}}_{k=1} \quad \underbrace{2n}_{F(n) = 2n \cdot 1^n}$

$a_n = a_n^{(h)} + a_n^{(p)}$

$a_n^{(h)}$: $a_n = 3a_{n-1}$

$r_1 = 3 \, , \, m_1 = 1$

$a_n^{(h)} = A(3^n)$

$a_n^{(p)}$: $a_n^{(p)} = (Bn + C)(\underline{1^n})$ ไม่ซ้ำ OK.

แทน $a_n^{(p)}$ ใน R_1 :

a_n : $Bn + C = 3(B(n-1) + C) + 2n$

$Bn + C = 3Bn - 3B + 3C + 2n$

$n(B - 3B - 2) = -3B + 2C$

$\underbrace{n(-2B-2)}_{=0} = \underbrace{-3B + 2C}_{=0}$

$\therefore B = -1 \qquad \therefore C = -3/2$

หรือ

$Bn + C = (3B+2)n - 3B + 3C$

$B = 3B + 2 \qquad C = -3B + 3C$

$\therefore \; a_n^{(p)} = -n - 3/2$

$\therefore \; a_n = a_n^{(h)} + a_n^{(p)} = A(3^n) - n - \frac{3}{2}$

$a_1 = 3A - 3 - \frac{3}{2} \longrightarrow A = \frac{11}{6}$

$\therefore \; a_n = \frac{11}{6}(3^n) - n - \frac{3}{2}$ ## (Unique Solution) e.g. $a_n = 5a_{n-1} - 6a_{n-2} + 7^n$

$a_n^{(h)}$: $r^2 = 5r - 6$

$\therefore (r-2)(r-3) = 0$

$r = 2, 3$

$r_1 = 2 \quad m_1 = 1$

$r_2 = 3 \quad m_2 = 1$

$\therefore a_n^{(h)} = A(2^n) + B(3^n)$

$F(n) = 7^n$

$a_n^{(p)} = \lambda \cdot 7^n$

$\therefore a_n$: $\lambda \cdot \cancel{7^n} = 5 \cdot \lambda \cdot \cancel{7}^{n-1} - 6 \cdot \lambda \cdot \cancel{7}^{n-2} + \cancel{7^n}$

$\lambda = \frac{5}{7}\lambda - \frac{6}{49}\lambda + 1$

$\therefore \lambda = \frac{49}{20}$

$\therefore a_n^{(p)} = \frac{7^{n+2}}{20}$

$\therefore a_n = A(2^n) + B(3^n) + \frac{1}{20}(7^{n+2})$ ※ (General solution, ไม่มี initial condition) e.g. $a_n = 6a_{n-1} - 9a_{n-2} + F(n)$

$$a_n^{(h)} = (A_0 + A_1 n)3^n$$

$r^2 - 6r + 9 = 0$

$\therefore r_1 = \underline{3},\ m_1 = 2$

ราก ซ้ำสอง $(m_1 = 2)$

When: $F(n) = 3n$; $S = 1$; $a_n^{(p)} = \lambda_1 n + \lambda_0$

$F(n) = n \cdot \underline{3}^n$; S^n, $S = 3$; $a_n^{(p)} = n^2(\lambda_1 n + \lambda_0) \cdot \underline{3}^n$

เติมตัวนี้ไป

$$\therefore a_n^{(p)} = (\lambda_1 n^3 + \lambda_0 n^2) \cdot 3^n$$

$F(n) =$

e.g. Find solution of $a_n = \sum_{k=1}^{n} k = \underline{\frac{n}{2}(n+1)}$ → target.

RR: $a_n = a_{n-1} + n$; $a_1 = 1$, $n = 2, 3, 4, \dots$

or $a_0 = 0$, $n = 1, 2, 3, \dots$

c.eqn.: $r_1 = 1$, $m_1 = 1$

S ซ้ำ 1 แบบ

$$a_n^{(h)} = A(1)^n = A$$

$$a_n^{(p)} : F(n) = n$$

$$a_n^{(p)} = (\lambda_1 n + \lambda_0) \; ; \; s^n = 1^n \longrightarrow s = 1$$

$$\therefore a_n^{(p)} = (\lambda_1 n^2 + \lambda_0 n)$$

RR:
$$\lambda_1 n^2 + \lambda_0 n = \lambda_1 (n-1)^2 + \lambda_0 (n-1) + n$$

$$\cancel{\lambda_1 n^2} + \cancel{\lambda_0 n} = \cancel{\lambda_1 n^2} - 2\lambda_1 n + \lambda_1 + \cancel{\lambda_0 n} - \lambda_0 + n$$

$$0 = (1 - 2\lambda_1) n + (\lambda_1 - \lambda_0)$$

$$\underbrace{\lambda_0 - \lambda_1}_{=0} = \underbrace{(1 - 2\lambda_1)}_{=0} n$$

$$\therefore \lambda_1 = \frac{1}{2} \rightarrow \lambda_0 = \frac{1}{2}$$

$$\therefore a_n^{(p)} = \frac{1}{2}(n^2 + n)$$

$$\therefore a_n = A + \frac{1}{2}(n^2 + n)$$

$$a_0 = 0 = A \longrightarrow a_n = \frac{n}{2}(n+1) \quad ⋕$$

Note $a_1 = 1 = A + \frac{1}{2}(1+1) \rightarrow A = 0$ ได้เหมือนกัน.