CHƯƠNG 1: MỆNH ĐỀ VÀ VỊ TỪ

I- MỆNH ĐỀ

1. Định nghĩa mệnh đề

- Mệnh đề là một phát biểu khẳng định, là đúng hoặc sai
- Một phát biểu mà có biến chưa được gọi là mệnh đề

2. Các phép tính mệnh đề

- Những chữ cái thường dùng để kí hiệu mệnh đề P, Q, R,.....

- Mệnh đề chỉ có một giá trị đơn (luôn đúng hoặc sai) được gọi là mệnh đề nguyên từ (atomic proposition).

- Các mệnh đề không phải là mệnh đề nguyên từ được gọi là mệng đề phức hợp (compound propositions).

Phép phủ định (NEGATION)

Bảng chân trị

P	¬P
T	F
F	T

Quy tắc: Đảo ngược lại

Phép hội (CONJUNCTION)

Bảng chân trị

P	Q	P∧Q
T	T	T
T	F	F
F	T	F
F	F	F

Quy tắc: Cả 2 đều đúng thì mới đúng

Phép tuyển (DISJUNCTION)

Bảng chân trị

P	Q	P∨Q
T	T	T
T	F	T
F	T	T
F	F	F

Quy tắc: Chỉ cần 1 cái đúng là đúng

Phép XOR

Bảng chân trị

P	Q	P⊕Q
T	T	F
T	F	T
F	T	T
F	F	F

Quy tắc: Ngược lại với phép tương đương, chỉ cần và đủ 1 cái đúng thì đúng

Phép kéo theo (IMPLICATION)

Bảng chân trị

P	Q	P→Q
T	T	T
T	F	F
F	T	T
F	F	T

Quy tắc: P sai hoặc Q đúng thì đúng

Chú ý: Từ **P→ Q**

Q → P là mệnh đề đảo

$\bar{Q} \to \bar{P}$ là mệnh đề phản đảo

Phép tương đương (BICONDITIONAL)

Bảng chân trị

P	Q	P↔Q
T	T	T
T	F	F
F	T	T
F	F	T

Quy tắc: Cùng tính chất thì đúng

3. Biểu thức mệnh đề (LOGICAL CONNECTIVES)

Cho P, Q, R,... là các mệnh đề. Nếu các mệnh đề này liên kết với nhau bằng các phép toán thì ta được một biểu thức mệnh đề.

4. Mệnh đề hệ quả và mệnh đề tương đương.

Một hằng đúng là một mệnh đề luôn có chân trị là **đúng**.

Một hằng sai là một mệnh đề luôn có chân trị là **sai**.

Một tiếp liên là một biểu thức mệnh đề không phải là hằng đúng và không phải là hằng sai.

Mệnh đề hệ quả: Cho F và G là 2 biểu thức mệnh đề. Người ta nói rằng G là mệnh đề hệ quả của F hay G được suy ra từ F nếu F → G là hằng đúng.

Tương đương Logic (logically equivalent):

- Mệnh đề P và mệnh đề Q được gọi là tương đương logic nếu phép tương đương của P và Q (P↔Q) là hằng đúng.

- Hoặc P và Q có cùng chân trị

Các quy tắc tương đương logic thường dùng

1. $\begin{cases} P \lor T = T \\ P \land F = F \end{cases}$ Domination laws (Luật thống trị)

2. $\begin{cases} P \land T = P \\ P \lor F = P \end{cases}$ Identity laws (Luật trung hòa)

3. $\begin{cases} P \lor P = P \\ P \land P = P \end{cases}$ Idempotent laws (Luật lũy đẳng)

4. $\overline{\overline{P}} = P$ Complement laws (Phủ định của phủ định)

5. $\begin{cases} P \lor \overline{P} = T \\ P \land \overline{P} = F \end{cases}$ Complement laws (Luật phần tử bù)

6. $\begin{cases} P \lor Q = Q \lor P \\ P \land Q = Q \land P \end{cases}$ Commutative laws (Luật giao hoán)

7. $\begin{cases} P \lor Q \lor R = (P \lor Q) \lor R = P \lor (Q \lor R) \\ P \land Q \land R = (P \land Q) \land R = P \land (Q \land R) \end{cases}$ *Associative laws (Luật kết hợp)*

8. $\begin{cases} P \lor (Q \land R) = (P \lor Q) \land (P \lor R) \\ P \land (Q \lor R) = (P \land Q) \lor (P \land R) \end{cases}$ *Distributive laws (Luật phân phối)*

9. $\begin{cases} \overline{P \lor Q} = \bar{P} \land \bar{Q} \\ \overline{P \land Q} = \bar{P} \lor \bar{Q} \end{cases}$ De Morgan's laws

10. $\begin{cases} P \lor (Q \land P) = P \\ P \land (Q \lor P) = P \end{cases}$ Absorption laws (Luật hấp phụ)

11. $P \to Q = \overline{P} \lor Q$ Implication law (Luật kéo theo)

5. Các ứng dụng

II- VỊ TỪ

1. Các định nghĩa

Một vị từ là một khẳng định P(x, y, ...) trong đó có chứa một số biến x, y, ... lấy giá trị trong những tập hợp A,B,... cho trước, sao cho:

- Bản thân P(x, y,...) **không phải** là mệnh đề.

- Nếu thay x, y ,... bằng những giá trị cụ thể thuộc tập hợp A, B,... cho trước ta sẽ được một mệnh đề P(x, y, ...), nghĩa là khi đó chân trị của P(x, y,...) hoàn toàn xác định. Các biến x, y,... được gọi là các biến tự do của vị từ.

Không gian của vị từ: Không gian mẫu của một biến

Trọng lượng của vị từ: Số biến

2. Phép toán vị từ

Hằng: Giá trị được xác định tại không gian của vị từ

Biến: Thể hiện các lớp tổng quát của các đối tượng hay thuộc tính

Vị từ: Là một sự kiện để khẳng định tính chất hay thuộc tính của đối tượng

Luật: Dùng để diễn tả sự việc

Hàm: Quan hệ trên các đối tượng

Hàm mệnh đề: Cho P là một vị từ có không gian là A. Tập A là một tập hợp không rỗng sao cho ứng với mỗi $x \in A$ ta có một mệnh đề, ký hiệu là P(x). Bấy giờ ta nói P (hay P(x)) là một hàm mệnh đề theo biến $x \in A$.

Ví dụ: Nếu X yêu Z và Y yêu Z thì 2 người X và Z không yêu nhau

Love(X, Y) = {X loves Y}

=> $\text{Love}(X, Z) \land \text{Love}(Y, Z) \to \overline{\text{Love}(X, Y)} \land \overline{\text{Love}(Y, X)}$

3. Các lượng từ

Lượng từ tồn tại (∃): Chỉ cần một giá trị thỏa mãn là đúng, bản chất là phép toán **tuyển**

Lượng từ với mọi (∀): Tìm một giá trị sai thì nó sai, bản chất là phép toán **hội**

Nếu không gian là tập hợp rỗng:

$$\forall x\, P(x) = T$$

$$\exists x\, P(x) = F$$

- Định lý 1: $\forall a \forall b\, P(a,b) = \forall b \forall a\, P(a, b)$

Ký hiệu: $\forall (a,b)\, P(a,b)$

$\exists a \exists b\ P(a,b) = \exists b \exists a\ P(a, b)$

Ký hiệu: $\exists(a,b)\ P(a,b)$

Nếu $\exists a \forall b\ P(a,b) \rightarrow \forall b \exists a\ P(a,b)$

Nếu $\exists b \forall a\ P(a,b) \rightarrow \forall a \exists b\ P(a,b)$

Định lý 2:

$\overline{\forall x P(x)} = \exists x \overline{P(x)}$

$\overline{\exists x P(x)} = \forall x \overline{P(x)}$

Công thức:

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

$\exists x\ P(x) \land Q(x) \quad \rightarrow \quad \exists x\ P(x) \land \exists x\ Q(x)$

$\exists x\ P(x) \lor Q(x) \quad \leftrightarrow \quad \exists x\ P(x) \lor \exists x\ Q(x)$

$\forall x\ P(x) \lor Q(x) \quad \rightarrow \quad \forall x\ P(x) \lor \forall x\ Q(x)$

4. Dịch các câu thông thường thành biểu thức logic.

$$\forall x(C(x) \lor \exists y\ (C(y) \land F(x,y))$$

C(x): x has a computer F(x,y): x and y are friends

"Everyone x either has a computer or has a friend y who has a computer."

$$\exists \boldsymbol{x} \forall y \forall z\ ((F(x,y) \land F(x,z) \land (y \neq z)) \rightarrow \overline{F(y,z)})$$

"There exists a person x such that for all people y and z, if x is friends with both y and z and y is not equal to z, then y and z are not friends with each other."

Ex: "If a person is female and is a parent, then this person is someone's mother."

F(x) : x is female. P(x): x is a parent.

M(x,y): x is the mother of y

$\rightarrow\ \forall x((F(x) \land P(x)) \rightarrow \exists y M(x,y))$

CHƯƠNG II: SUY LUẬN TOÁN HỌC.

I- MỞ ĐẦU

II- CÁC QUY TẮC SUY LUẬN

Quy tắc	Hằng đúng	Tên
$\dfrac{P}{\therefore P \vee Q}$	$P \rightarrow (P \vee Q)$	Cộng
$\dfrac{P \wedge Q}{\therefore P(Q)}$	$P \wedge Q \rightarrow P(Q)$	Rút gọn
P $\underline{P \rightarrow Q}$ $\therefore Q$	$[P \wedge (P \rightarrow Q)] \rightarrow Q$	Khẳng định Modus Ponens
$\bar{Q}$ $\underline{P \rightarrow Q}$ $\therefore \bar{P}$	$[\bar{Q} \wedge (P \rightarrow Q)] \rightarrow \bar{P}$	Phủ định Modus Tollens
P $\underline{Q}$ $\therefore P \wedge Q$	$(P) \wedge (Q) \rightarrow (P \wedge Q)$	Kết hợp
$P \vee Q$ $\underline{\bar{P} \vee R}$ $\therefore Q \vee R$	$(P \vee Q) \wedge (\bar{P} \vee R) \rightarrow (Q \vee R)$	Phân giải
$P \rightarrow Q$ $\underline{Q \rightarrow R}$ $\therefore P \rightarrow R$	$[(P \rightarrow Q) \wedge (Q \rightarrow R)] \rightarrow (P \rightarrow R)$	Tam đoạn luận giả định
$\bar{P}$ $\underline{P \vee Q}$ $\therefore Q$	$\bar{P} \wedge (P \vee Q) \rightarrow Q$	Tam đoạn luận tuyển

Name	Rule	Example
Universal Instantiation (Suy diễn với lượng từ với mọi)	$\dfrac{\forall x P(x)}{\therefore P(c)}$	"All women are brave" "Therefore, Lily is brave"
Universal Generalization (Tổng quát hóa với lượng từ với mọi)	$\dfrac{P(c) \text{ for an arbitrary}}{\therefore \forall x P(x)}$	"Lily is brave" "Therefore, all women are brave"
Existential Instantiation (Suy diễn với lượng từ tồn tại)	$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some element c}}$	"There is someone who ran a mile in 4 minutes "Let's call him Sparky and say that Sparky ran a mile in 4 minutes"
Existential Generalization (Tổng quát với lượng từ tồn tại)	$\dfrac{P(c) \text{ for some element c}}{\therefore \exists x P(x)}$	"Sparky ran a mile in 4 minutes" "Therefore, someone ran a mile in 4 minutes"

III- CÁC PHƯƠNG PHÁP CHỨNG MINH

1. Chứng minh rỗng (P là sai)

Chứng minh P sai dù cho Q là sai hay đúng thì $P \rightarrow Q$ là đúng

2. Chứng minh tầm thường (Q là đúng)

Chứng minh Q đúng thì dù P đúng hay sai thì $P \rightarrow Q$ là đúng

3. Chứng minh trực tiếp.

Chứng minh rằng nếu P đúng thì Q đúng

4. Chứng minh gián tiếp.

$P \rightarrow Q \Leftrightarrow \bar{Q} \rightarrow \bar{P}$

5. Chứng minh phản chứng.

Giả sử Q = F đi đến P → Q = T, với P = T, ta nhận thấy có mâu thuẫn do vì đặt Q = F

6. Chứng minh qui nạp

$\forall n \geq n_0, P(n)$

B1: Kiểm chứng $P(n_0) = T$

B2: Giả sử P(k) = T, chứng minh P(k+1) = T

B3: Kết luận $\forall n \geq n_0$, P(n) luôn đúng

Một số biểu thức cần phải nhớ

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \qquad \sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$$

$$\sum_{i=1}^{n} i(i+1)(i+2) = \frac{n(n+1)(n+2)(n+3)}{4} \qquad \sum_{i=1}^{n} i(i+2) = \frac{n(n+1)(2n+7)}{6}$$

7. Chứng minh từng trường hợp

$$P_1 \vee P_2 \vee \ldots \vee P_n \rightarrow Q$$

$$\Leftrightarrow (P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q) \wedge \ldots \wedge (P_n \rightarrow Q)$$

8. Chứng minh tương đương

$$[P_1 \leftrightarrow P_2 \leftrightarrow P_3] \Leftrightarrow (P_1 \rightarrow P_2) \wedge (P_2 \rightarrow P_3) \wedge (P_3 \rightarrow P_1)$$

CHƯƠNG III: QUAN HỆ

I- KHÁI NIỆM VỀ QUAN HỆ.

1. Quan hệ giữa hai tập hợp

Tập hợp A = {1, 2, 3, 4, 5} , B = {11, 12, 13}

a là phần tử thuộc A, b là phần tử thuộc B

a có quan hệ với b ⇔ a là ước của b

Phát biểu: Một phần tử a của A được gọi là có quan hệ với phần tử b của B ⇔ a là ước của b

Biểu diễn quan hệ:

{(1, 11), (1, 12), (1, 13), (2, 12), (3, 12), (4, 12)}

Đây được gọi là tập hợp con của tích Descartes AxB

2. Ký hiệu một quan hệ.

$\in$ (thuộc về)	$\subset$ (là tập hợp con) ….	
= (bằng)	< (nhỏ thua)	$\leq$ (nhỏ thua hoặc bằng)
// (song song)	$\perp$ (vuông góc)	

……………………………

3. Đồ thị của một quan hệ.

Kí hiệu quan hệ: aRb

Như ví dụ trong phần 1 là aRb ⇔ a là ước của b

Đồ thị của quan hệ R:

R = {(1, 11), (1, 12), (1, 13), (2, 12), (3, 12), (4, 12)}

Hai quan hệ bằng nhau, viết là $R_1 \equiv R_2$, khi chúng cùng đồ thị

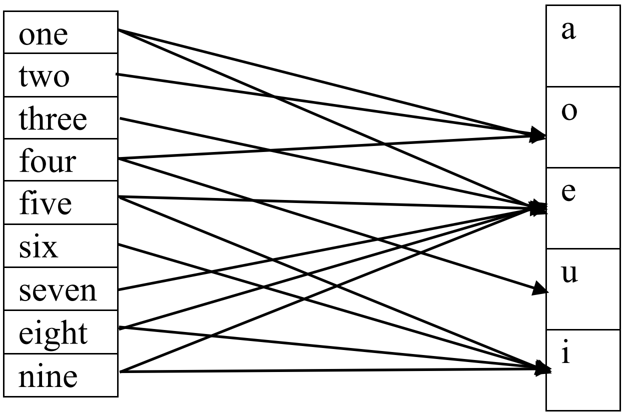
4. Biểu diễn một quan hệ

A = {one, two, three, four, five, six, seven, eight, nine}

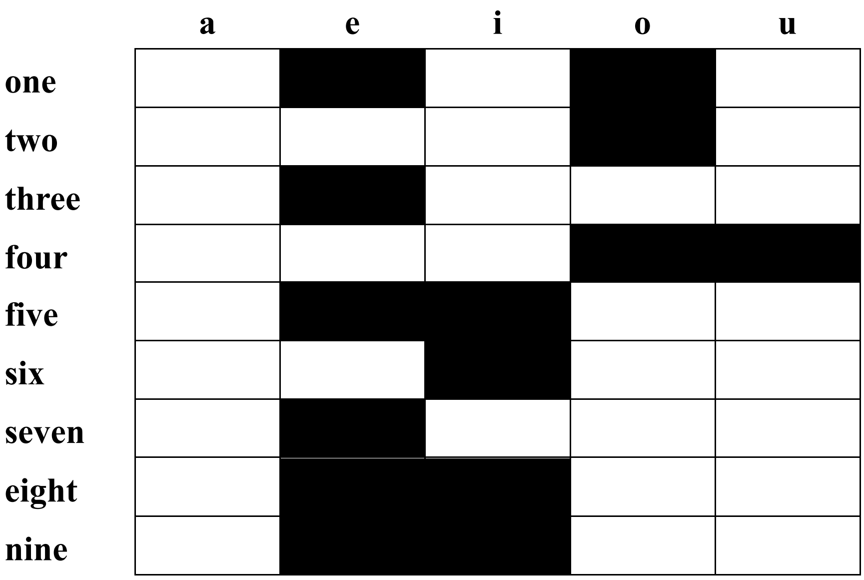
B = {e, a, i, o, u}

aRb ⇔ một từ trong tập hợp A có quan hệ với một kí tự của tập hợp B ⇔ từ đó có chứa kí tự đó

a. Dùng giản đồ



b. Bảng Descartes



c. Ma trận:

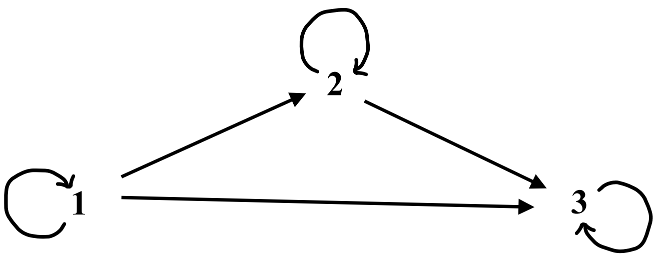
Tương tự như bảng Descartes nhưng không tô là 0, có tô là 1

II- CÁC TÍNH CHẤT CỦA QUAN HỆ HAI NGÔI TRÊN MỘT TẬP HỢP.

1. Quan hệ hai ngôi trên một tập hợp.

Một quan hệ R giữa tập hợp A và chính nó được gọi là một quan hệ hai ngôi trên tập hợp A, ta viết (A, R)

Cho tập A = {1, 2, 3} quan hệ $\leq$ trên A được biểu diễn bằng giản đồ như sau:



2. Các tính chất của quan hệ trên một tập hợp.

a. Phản hồi

$\forall a \in A,\ aRa$

b. Đối xứng

$\forall a, b \in A, \text{nếu } aRb \rightarrow bRa$

c. Phản đối xứng

$\forall a, b \in A, \text{nếu } aRb \text{ và } bRa \rightarrow a = b$

d. Quan hệ bắc cầu

$\forall a, b, c \in A, \text{nếu } aRb \text{ và } bRc \rightarrow aRc$

III- QUAN HỆ TƯƠNG ĐƯƠNG

1. Quan hệ tương đương

Một quan hệ R trên tập hợp A được gọi là quan hệ tương đương khi và chỉ khi R thỏa 3 tính chất

1)- Phản hồi

2)- Đối xứng

3)- Bắc cầu

2. Lớp tương đương

Một lớp tương đương gồm những phần tử có tính đối xứng với nhau, thỏa mãn quan hệ R

3. Phép phân hoạch

IV- QUAN HỆ THỨ TỰ

1. Quan hệ phản đối xứng

Quan hệ R trên một tập hợp A được gọi là có tính chất phản đối xứng khi và chỉ khi không tồn tại cặp (a, b) với a ≠ b sao cho đồng thời a có quan hệ với b và b cũng có quan hệ với a.

$$\forall a, b \in A, \text{nếu } aRb \text{ và } bRa \rightarrow a = b$$

2. Quan hệ thứ tự - tập hợp thứ tự

Một quan hệ R trên tập hợp A được gọi là một quan hệ thứ tự khi và chỉ khi R thỏa các tính chất:

1)- Phản hồi

2)- Phản đối xứng

3)- Bắc cầu

3. Trội và bị trội

4. Sơ đồ Hasse của một tập hợp thứ tự

5. Tập hợp thứ tự toàn phần - riêng phần

6. Những phần tử đặc biệt của tập hợp thứ tự

V- DÀN

1. Mở đầu

2. Cận trên và cận dưới.

3. Dàn và các tính chất của dân

4. Tình phân phối trong dân

5. Phần tử bù - Dàn bị bù

VI- ĐẠI SỐ BOOL

1. Đại số bool..

2. Các tính chất của đại số bool

VII- ĐỊNH LÝ STONE

1. Đẳng cấu

2. Atom

3. Định lý Stone

CHƯƠNG IV - V: HÀM BOOL & ĐƠN GIẢN CÔNG THỨC

I- MỞ ĐẦU.

1. Cấu hình của mạch điện.

Nếu mạch điện có n ngắt thì mạch điện có 2^n cấu hình

→ Có số dãy nhị nhân tất cả là 2^{2^n}

Số ngắt lớn biểu diễn bằng hình vẽ không thuận lợi

→ Biểu diễn bằng bảng

2. Mô tả mạch điện bằng bảng.

3. Ví dụ

II- HÀM BOOL n BIẾN.

1. Đại số bool B^1.

2. Hàm bool

3. Đại số bool của các hàm bool.

III - DẠNG TUYỂN (v) CHUẨN TẮC

1. Nhắc lại định lý Stone

2. Từ tối tiểu

3. Biểu diễn từ tối tiểu dưới dạng tích các literal.

4. Viết dạng tuyển chuẩn tắc

1)- Lập bảng chân trị của hàm f

2)- Mỗi lần f nhận giá trị 1 tại bộ các bit ($a_1a_2 \ldots a_n$) thì:

Viết tích của các biến.

Đặt dấu bù lên biến mà bit tương ứng với nó bằng 0.

3)- Viết f bằng tổng của các tích vừa tìm.

IV- DẠNG HỘI (^) CHUẨN TẮC.

1. Từ tối đại

2. Biểu diễn từ tối đại dưới dạng tổng các literal

3. Viết dạng hội chuẩn tắc

1)- Lập bảng chân trị của hàm f

2)- Mỗi lần f nhận giá trị 0 tại bộ các bit ($a_1a_2 \ldots a_n$) thì:

Viết tổng của các biến.

Đặt dấu bù lên biến mà bit tương ứng với nó bằng 1.

3)- Viết f bằng tích của các tổng vừa xác định.

V- HỆ PHƯƠNG TRÌNH BOOL VÀ PHỦ TỐI TIỂU

1. Hệ phương trình bool

2. Phương pháp giải hệ phương trình bool

Giai đoạn 1: Biến thành về các tổng

Giai đoạn 2: Dùng định lý sau đây

$(G = D) \Leftrightarrow (GD \vee \bar{G}\bar{D}) = 1$

Biến đổi các tổng bằng 1

Giai đoạn 3: Biến đổi hệ phương trình tương đương thành:

$1 = F_1F_2F_3 \ldots F_k$

Giai đoạn 4: Thu gọn vế thành các tổng của các tích gọn nhất.

Giai đoạn 5: Biến đổi phương trình về dạng

$$1 = h_1 \lor h_2 \lor \dots \lor h_p \text{ với } h_i \text{ là tích các biến}$$

Phương trình biến đổi thành

$$\begin{cases} h_1 = 1 \\ h_2 = 1 \\ h_3 = 1 \\ \dots \\ h_p = 1 \end{cases}$$

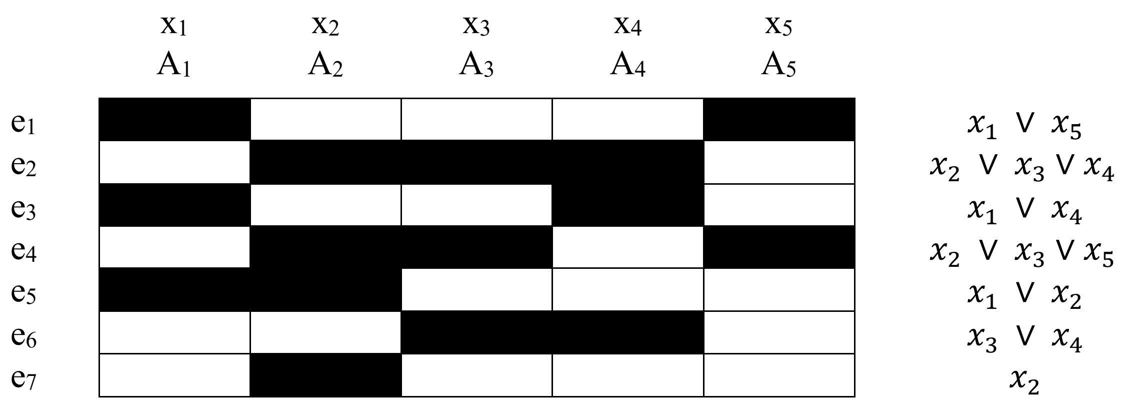
Biến đổi thành dạng bảng

Kết thúc bài toán

3. Phủ tối tiểu

Người ta sử dụng hệ phương trình bool để giải quyết bài toán phủ tối tiểu được phát biểu như sau: Cho $e_1, e_2, \dots e_n$ là các phần tử của tập hợp E và $A_1, A_2, \dots A_n$ là p tập hợp con của E. Hãy tìm một hệ nhỏ nhất trong số các tập hợp con này sao cho tập hợp của chúng phủ { $e_1, e_2, \dots e_n$ }. Hệ tìm được này được gọi là phủ tối tiểu.

Một ví dụ của bảng tối tiểu:



Sau khi giải hệ phương trình ta được các phủ tối tiểu:

x_1	x_2	x_3	x_4	x_5	**Phủ tối tiểu**
1	1	1			$A_1A_2A_3$
1	1		1		$A_1A_2A_4$
	1		1	1	$A_2A_4A_5$

CHƯƠNG VI: LÝ THUYẾT CHIA VÀ ĐỒNG DƯ

I- PHÉP CHIA HẾT VÀ CÓ DƯ.

1. Phép chia hết

Xét a, b $\in \mathbb{Z}$ và b $\neq 0$

b chia hết a (b là ước của a)

a chia hết cho b (a là bội của b)

Kí hiệu: b | a $\Leftrightarrow \exists q \in \mathbb{Z}$ sao cho a = bq $\Leftrightarrow$ a $\vdots\, b$

Với $\forall b \neq 0$

0 chia hết cho b vì $\exists 0 \in \mathbb{Z}$ sao cho 0 = 0b

→ 0 là bội của mọi số nguyên

Với $\forall a$ thì

1|a vì $\exists a \in \mathbb{Z}$ sao cho a = 1a

→ 1 là ước của mọi số nguyên

Tính chất của phép chia hết

1- b | a ⇔ $\pm \boldsymbol{b}$ | $\pm\, \boldsymbol{a}$

2- $\forall a \neq 0\ a|a$

3- $\forall a \quad 1|a$

4- $\forall a \neq 0\ a|0$

5- (a|b và b|a) khi và chỉ khi a = $\pm b$

6- Nếu (a|b và b|c) thì a|c (Tính bắc cầu)

7- Nếu c|a và c|b thì (c|ax+by)

8- Nếu a|x và b|y thì ab|xy

2. Phép chia có dư

Định lý

a, b $\in \mathbb{Z}$ và b $\neq 0$

Tồn tại duy nhất cặp số nguyên q và r $\in \mathbb{Z}$ sao cho:

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

q được gọi là thương, r được gọi là dư

II- ƯỚC CHUNG LỚN NHẤT VÀ BỘI CHUNG NHỎ NHẤT...

1. Ước chung lớn nhất (UCLN)

$a_1, a_2, a_3, \dots, a_n$ là các số nguyên không đồng thời bằng 0

Ước chung

Số nguyên $d \in \mathbb{Z}$ được gọi là ước chung của các a_i ($i = 1, 2, \dots, n$) khi và chỉ khi d là ước của mỗi a_i

Ước chung lớn nhất

Ước chung d của các a_i ($i = 1, 2, \dots, n$) được gọi là ước chung lớn nhất (UCLN) của các a_i nếu và chỉ nếu d là bội của mọi ước chung khác của a_i

Nếu d là ước chung lớn nhất của các a_i, giữa chúng sẽ có một giá trị dương. Người ta quy ước UCLN là một số dương.

Định lý: Tồn tại ước chung lớn nhất của các số nguyên không đồng thời bằng 0

Nhận xét:

$(a, b) = (|a|, |b|)$

$(a, b) = (b, a)$ (Tính giao hoán)

$(a, b, c) = ((a, b), c) = (a, (b, c))$ (Tính kết hợp)

Số nguyên tố cùng nhau: Khi UCLN của những số a_i bằng 1

Số nguyên tố sánh đôi: Khi bất kì cặp số nào cũng có UCLN bằng 1

Tính chất:

1- Nếu $(a_1, a_2, a_3, \dots a_n) = d$ thì $\exists$ các số nguyên $x_1, x_2, \dots, x_n$ sao cho:

$$a_1.x_1 + a_2.x_2 + \dots + a_n.x_n = d$$

2- Nếu m là số nguyên dương thì

$$(m.a_1, m.a_2, \dots, m.a_n) = m(a_1, a_2, \dots, a_n)$$

3- Nếu $d > 0$ là ước chung của $a_1, a_2, a_3, \dots a_n$ thì

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) = \frac{(a_1, a_2, \dots, a_n)}{d}$$

4- Nếu $d > 0$ là UC của $a_1, a_2, \dots, a_n$ thì d là UCLN của $a_1, a_2, \dots a_n$ khi và chỉ khi

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) = 1$$

5- Nếu $b > 0$ là ước của a thì $(a, b) = b$, đặc biệt $(0, b) = b$

6- Nếu $c|ab$ và $(a, c) = 1$ thì $c|b$

7- Nếu b|a và c|a và (b,c) = 1 thì bc|a

8- Nếu (a, b) = 1 thì (ac, b) = (c, b)

9- Nếu (a, b) = (a, c) = 1 thì (a, bc) = 1

Định lý:

Nếu a và b là 2 số nguyên dương và a = bq + r với $0 \leq r < b$ thì:

(a, b) = (b, r)

Thuật toán Euclide tìm UCLN

(a, b) = (b, r) (nếu a = bq + r)

…

(f, 0) = f

2. Bội chung nhỏ nhất (BCNN)

$a_1, a_2, a_3, \ldots, a_n$ là các số nguyên khác 0

Bội chung:

Số nguyên M được gọi là bội chung của các a_i (i = 1, 2, …, n) khi và chỉ khi M là bội của mỗi a_i

Bội chung lớn nhất:

Bội chung M của các a_i (i = 1, 2, …, n) được gọi là BCNN của các a_i nếu và chỉ nếu nó là ước của mọi bội chung khác của các a_i

Bội chung nhỏ nhất được quy ước là một số nguyên dương

Nhận xét:

[a, b] = [|a|, |b|]

[a, b] = [b, a] tính giao hoán

[a, b, c] = [[a, b], c] = [a, [b, c]] tính kết hợp

Định lý về sự tồn tại BCNN

Luôn luôn tồn tại BCNN của các số nguyên khác 0 cho trước

Định lý tìm BCNN

Với hai số nguyên a và b khác 0, ta có

$$[a, b] = \frac{|ab|}{(a,b)}$$

Tính chất của BCNN

$a_1, a_2, \ldots, a_n$ là các số nguyên tố khác 0

1- Nếu số nguyên M > 0 là bội chung của các $a_1, a_2, \ldots, a_n$, thì

$$M = [a_1, a_2, \dots, a_n] \text{ khi và chỉ khi } \left(\frac{M}{a_1}, \frac{M}{a_2}, \dots, \frac{M}{a_n}\right) = 1$$

2- Nếu k > 0 là một số nguyên thì:

$[ka_1, ka_2, \dots, ka_n] = k[a_1, a_2, \dots, a_n]$

3- Nếu $d = (a_1, a_2, \dots, a_n)$ thì

$$\left[\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right] = \frac{[a_1, a_2, \dots, a_n]}{d}$$

4- Nếu $a_1, a_2, \dots, a_n$ là các số nguyên sánh đôi thì;

$[a_1, a_2, \dots, a_n] = a_1.a_2. \dots .a_n$

III- SỐ NGUYÊN TỐ VÀ HỢP SỐ.

1. Định nghĩa

Số nguyên tố

Số nguyên p > 1 được gọi là số nguyên tố nếu p không có ước số dương nào khác ngoài 1 và chính nó

Số nguyên tố là số chỉ chia hết cho 1 và chính nó

Hợp số

Số nguyên a > 1 được gọi là hợp số nếu a có ước số dương khác 1 và khác chính nó

Hợp số là số có thể chia hết cho ngoài 2 số 1 và chính nó

Định lý:

Ước số dương nhỏ nhất lớn hơn 1 của các số nguyên lớn hơn 1 là một số nguyên tố

Mọi số nguyên lớn hơn 1 đều có ước là số nguyên tố

2. Bảng số nguyên tố - Sàng Erathosthene

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- Viết dãy số từ 2 đến n

- Tìm các số nguyên tố từ 2 đến $\sqrt{n}$

- Xóa đi các bội thực sự của các số nguyên tố này

- Các số còn lại là số nguyên tố

3. Định lý cơ bản của số học.

4. Một số vấn đề về số nguyên tố

IV- PHƯƠNG TRÌNH NGUYÊN

1. Phương trình nguyên bậc nhất 2 ẩn

Định nghĩa:

a, b ∈ Z là các hệ số

x, y ∈ Z là các ẩn số cần xác định giá trị

Xét phương trình 2 ẩn: ax + by = c

d = (a, b)

Khi đó

1- Nếu d không là ước của c thì (1) không có nghiệm nguyên

2- Nếu d là ước của c thì (1) có vô số nghiệm nguyên

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \quad t \in Z$$

Nếu phương trình ax + by = c có |a| = 1 hoặc |b| = 1 thì việc tìm nghiệm coi như được giải quyết xong

VD: x + by = c

$$\begin{cases} x = c - bt \\ y = t \end{cases}$$

2. Phương trình nguyên bậc nhất nhiều ẩn

Định nghĩa

Phương trình nguyên bậc nhất n > 2 ẩn có dạng:

$a_1x_1 + a_2x_2 + \dots + a_nx_n = c$

$a_i, x_i \in Z$ i = 1, 2, ..., n

Phương trình nhiều ẩn nói chung là phức tạp, vậy cho nên chủ yếu chỉ là 3 ẩn

VD: ax + by + z = c

$$\begin{cases} z = c - at - bu \\ y = u \\ x = t \end{cases}$$

3. Phương trình bậc cao

V- QUAN HỆ ĐỒNG DƯ

a, b m > 0 là các số nguyên

a được gọi là đồng dư với b theo modulo m, kí hiệu a $\equiv\ b\ (mod\ m)$, nếu a có cùng số dư với b khi chia cho m

Nhận xét:

1)- a $\equiv b\ (mod\ m)$ ⇔ b $\equiv a\ (mod\ m)$

2)- a chia hết cho m ⇔ a $\equiv 0\ (mod\ m)$

3)- Quan hệ đồng dư là một quan hệ tương đương

Định lý: a, b, m > 0 là các số nguyên

Những mệnh đề sau đây là tương đương

1)- a $\equiv b\ (mod\ m)$

2)- a = b + mt (t là một số nguyên)

3)- (a-b) ≡ 0 (mod m)

Tính chất của quan hệ đồng dư:

1- Nếu $a_i \equiv b_i$ (mod m) (i = 1, 2, 3, … , n) thì

$(a_1 + a_2 + ... + a_n) \equiv (b_1 + b_2 + ... + b_n)$ (mod m)

$(a_1a_2 ...a_n) \equiv (b_1b_2 ... b_n)$ (mod m)

2- a ≡ b (mod m) ⇔ (a ± c) ≡ (b ± c) (mod m) (c là số nguyên)

3- a ≡ b (mod m) ⇔ a ≡ $b + km$ (mod m) (k là số nguyên)

⇔ a + km ≡ b (mod m)

4- a ≡ b (mod m) → $a^n \equiv b^n$ (mod m) (n là số nguyên dương)

5- a ≡ b (mod m) → ac ≡ bc (mod m) (c là số nguyên)

Nếu (c, m) = 1 thì a ≡ b (mod m) ⇔ ac ≡ bc (mod m)

6- Nếu c là số nguyên dương thì a ≡ b (mod m) ⇔ ac ≡ bc (mod mc)

7- Nếu d > 0 là ước chung của a, b, m thì

a ≡ b (mod m) ⇔ $\frac{a}{d} \equiv \frac{b}{d}$ (mod $\frac{m}{d}$)

8- Nếu d là ước chung của a và b và (d, m) = 1

$$a \equiv b \pmod{m} \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$$

9- $a \equiv b \pmod{m_i}$ (i = 1, 2, …, n) và m = $[m_1, m_2, m_3, .. m_n]$

$\rightarrow a \equiv b \pmod{m}$

10- $a \equiv b \pmod{m}$ và d > 0 là ước của m → $a \equiv b \pmod{d}$

11- $a \equiv b \pmod{m}$ và d là ước chung của a, m → d là ước của b

12- $a \equiv b \pmod{m}$ → (a, m) = (b, m)

Định lý Wilson phát biểu rằng: cho p là số tự nhiên lớn hơn 1, khi đó p là số nguyên tố, khi và chỉ khi (p-1)!+1 chia hết cho p.

$$(p-1)! \equiv -1 \pmod{p}$$

VI- VÀNH CÁC LỚP THẶNG DƯ...

1. Vành các lớp thặng dư

Định nghĩa:

Quan hệ đồng dư theo modulo m trên tập số nguyên Z là một quan hệ tương đương, nó phân hạch tập hợp này thành m lớp tương đương, gọi là lớp thặng dư, được kí hiệu như sau:

- Lớp $\bar{0}$ gồm các số đồng dư với 0 theo modulo m
- Lớp $\bar{1}$ gồm các số đồng dư với 1 theo modulo m
- Lớp $\bar{2}$ gồm các số đồng dư với 2 theo modulo m
- ……………
- Lớp $\overline{m-1}$ gồm các số đồng dư với (m-1) theo modulo m

Gọi Zm là tập hợp các lớp thặng dư

Ta định nghĩa Zm như sau:

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} \,.\, \bar{b} = \overline{a.b}$$

Phần tử khả nghịch

$\bar{a} \in Zm$

$\bar{a}$ được gọi là phần tử khả nghịch của Zm khi và chỉ khi tồn tại $\bar{b} \in Zm$ sao cho:

$$\bar{a} \,.\, \bar{b} = \bar{1}$$

→ **a và m là số nguyên tố cùng nhau**

2. Hệ thặng dư đầy đủ và hệ thặng dư thu gọn

Định nghĩa

Trong mỗi lớp của Zm người ta chọn ra một phần tử, gọi là phần tử đại diện. Tập hợp phần tử đại diện đó gọi là một hệ thặng dư đầy đủ theo modulo m.

Hệ thặng dư thường dùng theo modulo m là:

0 1 2 ……… (m-1)

Nếu m là số lẻ, hệ thặng dư đầy đủ giá trị tuyệt đối nhỏ nhất có dạng:

-(m-1)/2 ……… -2 -1 0 1 2 ……… (m-1)/2

Định nghĩa

Trong mỗi lớp là phần tử khả nghịch của Zm người ta chọn ra một phần tử, gọi là phần tử đại diện. Tập hợp các phần tử đại diện đó được gọi mà một hệ thặng dư thu gọn theo modulo m. Người ta cũng nói đến hệ thặng dư thu gọn không âm bé nhất và giá trị tuyệt đối nhỏ nhất.

VD: Một hệ thặng dư thu gọn trong Z_8 là: {1, 3, 5, 7}

Bổ đề:

a, b, m > 0 là các số nguyên, (a, m) = 1

1)- Nếu x chạy qua hệ thặng dư đầy đủ modulo m thì ax+ b cũng chạy qua hệ thặng dư đầy đủ modulo m.

2)- Nếu x chạy qua hệ thặng dư thu gọn modulo m thì ax cũng chạy qua hệ thặng dư thu gọn modulo m.

3. Định lý Euler

Hàm số Euler $\varphi(m)$

m là số nguyên dương.

Hàm số Euler $\varphi(m)$ được định nghĩa như sau:

1)- $\varphi(1) = 1$

2)- Với m > 1, $\varphi(m)$ là số các số nguyên tố cùng nhau với m không vượt quá m

$$\varphi(10) = 4$$

$$\varphi(7) = 6$$

Nhận xét: Nếu p là số nguyên tố thì $\varphi(p) = p - 1$

Định lý:

1)- Nếu m_1 và m_2 là hai số nguyên dương và nguyên tố cùng nhau thì:

$$\varphi(m_1 m_2) = \varphi(m_1).\varphi(m_2)$$

2)- Nếu m = p^{α} với p là số nguyên tố và α là một số nguyên dương thì:

$$\varphi(m) = \varphi(p^{\alpha}) = p^{\alpha}(1-\frac{1}{p})$$

3)- Nếu m > 1 và có dạng phân tích tiêu chuẩn m = ${p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots..{p_k}^{\alpha_k}$ thì:

$$\varphi(m) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k})$$

Định lý Euler:

Nếu a và m > 0 là hai số nguyên tố cùng nhau thì:

$$a^{\varphi(m)} \equiv 1 (\text{mod } m)$$

Định lý Fermat:

$$a^{p-1} \equiv 1 (\text{mod } p)$$

$$\rightarrow a^{p} \equiv a\ (\text{mod } p)$$

VII- PHƯƠNG TRÌNH ĐỒNG DƯ MỘT ẨN

1. Phương trình đồng dư một ẩn

Phép biến đổi tương đương **được sử dụng** trong phương trình đồng dư 1 ẩn:

1- a ≡ b (mod m) ⇔ (a ± c) ≡ (b ± c) (mod m) (c là số nguyên)

2- a ≡ b (mod m) ⇔ a ≡ $b + km$ (mod m) (k là số nguyên)

⇔ a + km ≡ b (mod m)

3- Nếu (c, m) = 1 thì a ≡ b (mod m) ⇔ ac ≡ bc (mod m)

4- Nếu c là số nguyên dương thì a ≡ b (mod m) ⇔ ac ≡ bc (mod mc)

5- Nếu d > 0 là ước chung của a, b, m thì

$$a \equiv b\ (\text{mod } m) \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} (\text{mod } \frac{m}{d})$$

6- Nếu d là ước chung của a và b và (d, m) = 1

$$a \equiv b\ (\text{mod } m) \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} (\text{mod } m)$$

2. Phương trình đồng dư bậc nhất một ẩn.

Xét phương trình ax ≡ b (mod m)

d = (a, m), khi đó

1)- Nếu d không là ước của b thì (2) vô nghiệm

2)- Nếu d là ước của b thì (2) có đúng d nghiệm

Gọi x_0 là một giá trị thỏa phương trình thì d nghiệm đó được xác định bởi công thức

$$\left[\begin{array}{ll} x \equiv x_0 + 0.\frac{m}{d} & (mod\ m) \\ x \equiv x_0 + 1.\frac{m}{d} & (mod\ m) \\ \dots\dots\dots\dots\dots & \\ x \equiv x_0 + (d-1).\frac{m}{d} & (mod\ m) \end{array}\right.$$

VIII- HỆ PHƯƠNG TRÌNH ĐỒNG DƯ BẬC NHẤT MỘT ẨN

Định lý Trung Quốc về phần dư

Nếu các modulo $m_1, m_2, \dots, m_n$ là các số nguyên tố sánh đôi thì hệ có duy nhất x xác định

Tính $M = [m_1, m_2, \dots, m_n] = m_1 m_2 \dots m_n$

Tính $M_i = \frac{M}{m_i}$ (i = 1, 2, …, n)

Giải các phương trình đồng dư $M_i\, y \equiv a_i$ (mod m_i)   (i = 1, 2, …, n)

→ Tìm được các nghiệm $y \equiv N_i$ (mod m_i)   (i = 1, 2, …, n)

Nghiệm của hệ:

$x = M_1 N_1 + M_2 N_2 + \dots + M_n N_n$ (mod M)

Phương pháp thế

$$\begin{cases} x \equiv a\ (mod\ m)\ (1) \\ x \equiv b\ (mod\ n)\ \ (2) \end{cases}$$

(1) $x \equiv a\ (mod\ m)$

⇔ x = mt + a (*)

Thay (*) vào (2)

mt + a ≡ $b\ (mod\ n)$

=> t ≡ $c\ (mod\ o)$

⇔ t = ok + c (**)

Thay (**) vào (*)

x = m(ok + c) + a

IX- PHƯƠNG TRÌNH ĐỒNG DƯ BẬC CAO MỘT ẨN

X- ỨNG DỤNG CỦA LÝ THUYẾT ĐỒNG DƯ

CHƯƠNG 7: PHÉP ĐẾM

I- CÁC NGUYÊN LÝ ĐẾM

Nguyên lý cộng: Giả sử để làm công việc A có 2 phương pháp

- Phương pháp 1: n cách - Phương pháp 2: m cách

→ Khi đó số cách làm công việc A là n + m

Nguyên lý nhân: Giả sử để làm công việc A cần 2 bước

- Bước 1: n cách - Bước 2: m cách

→ Khi đó số cách làm công việc A là n.m

Nguyên lý bù trừ:
$|A \cup B| = |A| + |B| - |A \cap B|$

$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |B \cap C| + |C \cap A|) + |A \cap B \cap C|$

Nguyên lý Dirichlet: Nếu có N vật được đặt vào trong k hộp thì sẽ tồn tại một hộp chứa ít nhất [N/k] vật.

II- ĐẠI SỐ TỔ HỢP

Hoán vị: $P_n = n! = n*(n-1)*(n-2)*\ldots*1$

Chỉnh hợp: Sắp xếp **có thứ tự** của k phần tử vào n phần tử

$$A_n^k = \frac{n!}{(n-k)!} \quad (k \le n)$$

Tổ hợp: Sắp xếp không có thứ tự của k phần tử vào n phần tử

$$C_n^k = \frac{n!}{k!(n-k)!} \quad (k \le n)$$

$$C_n^0 = C_n^n = 1 \qquad C_n^k = C_n^{n-k}$$

$$C_n^k + C_n^{k-1} = C_{n+1}^k$$

Hoán vị lặp: Cho n đối tượng trong đó có n_i đối tượng loại i giống hệt nhau (i = 1, 2, …, k; $n_1 + n_2 + \ldots + n_k = n$). Mỗi cách sắp xếp có thứ tự n đối tượng đã cho gọi là một hoán vị lặp của n

$$P_n(n_1, n_2, \ldots, n_k) = \frac{n!}{n_1! * n_2! * \ldots * n_k!}$$

$$C_7^3 * C_4^2 * C_2^1 * C_1^1 = \frac{7!}{3! * 2! * 1! * 1!}$$

Chỉnh hợp lặp: Có n phần tử khác nhau, mỗi cách lấy k phần tử từ n phần tử có lặp, có kể thứ tự được gọi là chỉnh hợp chập k của n

$$B_n^k = n^k$$

Tổ hợp lặp: Mỗi cách chọn ra k vật từ n loại vật khác nhau (trong đó mỗi loại vật có thể được chọn lại nhiều lần) được gọi là tổ hợp lặp chập k của n

$$C_{n+k-1}^{k} = \frac{(n+k-1)!}{k!(n-1)!}$$

III- HỆ THỨC TRUY HỒI

Định nghĩa: Hệ thức truy hồi đối với dãy số $\{a_n\}$ được xác định bởi một hay nhiều số hạng đứng trước nó, cụ thể là $a_0, a_1, a_2, ..., a_{n-1}$ với mọi số nguyên $n \geq n_0$, $n_0 \geq 0$. Dãy số được gọi là lời giải hay là nghiệm của hệ thức truy hồi nếu các số hạng của nó thỏa mãn hệ thức truy hồi này.

Một số bài toán tiêu biểu:

1. Tháp Hà Nội

hanoi(n - 1, a, b, c); //chuyển n-1 đĩa từ cột a sang cột b với c làm trung gian

hanoi(1, a, c, b) //chuyển 1 đĩa từ cột a sang cột c với b làm cột trung gian

hanoi(n - 1, b, c, a); //chuyển n-1 đĩa từ cột b sang cột c với a làm trung gian

Số lần di chuyển đĩa:

$H_n = 2H_{n-1} + 1 = 2^n - 1$

2. Bài toán lãi kép

$P_n = (a)^n P_0$

3. Họ nhà thỏ và số Fibonacci

$$F(n) = \begin{cases} 0 & n = 0 \\ 1 & khi\, n = 1 \\ F(n-1) + F(n-2) & n > 1 \end{cases}$$

GIẢI HỆ THỨC TRUY HỒI

Định lý 1: Cho c_1, c_2 là hai số thực. Giả sử $r^2 - c_1r - c_2 = 0$ có hai nghiệm phân biệt là r_1 và r_2. Khi đó dãy $\{a_n\}$ là nghiệm của hệ thức truy hồi $a_n = c_1a_{n-1} + c_2a_{n-2}$ nếu và chỉ nếu $a_n = \alpha_1r_1^n + \alpha_2r_2^n$, với n = 0, 1, 2,…, trong đó α_1 và α_2 là các hằng số.

Định lý 2: Cho c_1, c_2 là hai số thực, với $c_2 \neq 0$. Giả sử $r^2 - c_1r - c_2 = 0$ chỉ có một nghiệm là r_0. Khi đó dãy $\{a_n\}$ là nghiệm của hệ thức truy hồi $a_n = c_1a_{n-1} + c_2a_{n-2}$ nếu và chỉ nếu $a_n = \alpha_1r_0^n + \alpha_2nr_0^n$, với n = 0, 1, 2,…, trong đó α_1 và α_2 là các hằng số.

Định lý 3: Cho $c_1, c_2, \ldots, c_k$ là các số thực. Giả sử rằng phương trình đặc trưng

$r^k - c_1r^{k-1} - \ldots - c_k = 0$

có k nghiệm phân biệt là $r_1, r_2, \ldots r_k$. Khi đó dãy $\{a_n\}$ là nghiệm của hệ thức truy hồi

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_kr_{n-k}$$

nếu và chỉ nếu $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \ldots + \alpha_k r_k^n$, với n = 0, 1, 2,…, trong đó α_1, $\alpha_2,\ldots,\alpha_k$ là các hằng số.

Các bước để giải một bài toán hệ thức truy hồi: Ví dụ đây là giải hệ thức truy hồi dạng hệ thức truy hồi $a_n = c_1a_{n-1} + c_2a_{n-2}$

1. Phương trình đặc trưng

$r^2 - c_1r - c_2 = 0 \rightarrow r = ?$

2. Nghiệm của hệ thức truy hồi có dạng:

$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ (*) hoặc $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$ (*)

Dựa vào a_0, a_1, (hoặc a_1, a_2 tùy bài toán) $\rightarrow \alpha_1$ và α_2

3. Thay vào (*) và cho ra kết quả cuối cùng

MỤC LỤC

Đây là tài liệu mình tự soạn, tóm tắt nội dung, donate:

Tran Minh Phu