LỜI NÓI ĐẦU

Nhằm đáp ứng nhu cầu học tập của sinh viên ngành Công nghệ thông tin, chúng tôi biên soạn bài giảng 'Toán rời rạc'' theo hướng tinh giản nội dung, cập nhật kiến thức mới, đồng thời đảm bảo khối kiến thức tối thiểu về cơ sở Toán cho Tin học để sinh viên có điều kiện tiếp thu tốt các môn học chuyên ngành trong chương trình đào tạo của ngành Khoa học máy tính và ngành Sư phạm Tin học.

Nội dung chính của bài giảng được trình bày trong 6 chương:

Chương 1: Tập hợp – ánh xạ

Chương 2: Logic

Chương 3: Quan hệ

Chương 4: Phương pháp đếm

Chương 5: Đại số Boole

Chương 6: Lý thuyết số

Đầu mỗi chương giới thiệu mục tiêu của chương, cùng các tài liệu tham khảo được sử dụng trong bài giảng. Chúng tôi cố gắng trình bày những vấn đề lý thuyết cơ bản nhất, đồng thời chú ý đưa ra nhiều ví dụ minh hoạ nhằm giúp người đọc hiểu rõ bản chất vấn đề. Cuối mỗi mục và mỗi chương có hệ thống các câu hỏi và bài tập khá phong phú để người đọc kiểm chứng và làm sâu sắc thêm

các vấn đề lý thuyết. Phần cuối tài liệu có phần hướng dẫn giải hoặc đáp án của một số bài tập, nhằm giúp sinh viên có định hướng trong khi làm bài tập.

Chắc chắn bài giảng còn nhiều thiếu sót về nội dung và hình thức, tác giả mong nuốn tiếp tục nhận được ý kiến đóng góp bạn đọc để tài liệu được hoàn thiện hơn.

Tác giả

MỤC LỤC

Chương I
TẬP HỢP – ÁNH XẠ

MỤC TIÊU CỦA CHƯƠNG

Chương này có mục đích hệ thống hóa, củng cố những kiến thức mà người học đã biết ở mức độ nhất định ở trường phổ thông, đồng thời nâng cao, bổ sung một số nội dung mới mà người học cần phải có để nghiên cứu tốt hơn những nội dung thuộc chuyên ngành của tin học.

- Bổ túc và nâng cao kiến thức cơ bản về tập hợp, bao gồm khái niệm tập hợp, phép toán của tập hợp, tích Đề-các, tính chất của tập hợp.

- Bổ túc và nâng cao kiến thức về ánh xạ, bao gồm các khái niệm ánh xạ, tính chất của ánh xạ, ánh xạ hợp.

- Cuối mỗi phần là hệ thống các câu hỏi và bài tập.

TÀI LIỆU THAM KHẢO

1. Nguyễn Hữu Anh, 1999, Toán rời rạc, NXB Giáo dục
2. Đại học Cần Thơ, 2003, Bài giảng Toán rời rạc 1, 2, 3
3. Phạm Thế Long (chủ biên), Nguyễn Xuân Viên, Nguyễn Thiện Luân, Nguyễn Đức Hiếu, Nguyễn Văn Xuất, 2005, Toán rời rạc, NXB Đại học Sư phạm
4. Kenneth H. Rosen (Bùi Xuân Toại dịch), 2010, Toán rời rạc và những ứng dụng trong Tin học, NXB Lao động
5. Seymour Lipschutz, 1964, Set theory and related topics, Mc Hraw Hill.

I. TẬP HỢP

1.1. Khái niệm tập hợp

a) Khái niệm tập hợp:

Theo nghĩa thông thường tập hợp được hiểu là một tuyển tập để chứa các đối tượng nhất định nào đó. Chẳng hạn, tập hợp các máy tính trong mạng, tập hợp các quả cam, tập hợp các số tự nhiên,…

Trong toán học, tập hợp là một khái niệm nguyên thủy, nghĩa là không định nghĩa nó. Bản chất của tập hợp được hiểu thông qua các phép toán và tính chất được khẳng định trên tập hợp.

b) Ký hiệu tập hợp:

Ta thường dùng các chữ cái in hoa, như A, B, C,…, X, Y, Z,… để kí hiệu tập hợp, còn các phần tử của tập hợp kí hiệu bằng các chữ cái thường, như a, b, c, …, x, y, z, ...

c) Tập hợp rỗng:

Một tập hợp không có phần tử nào gọi là tập hợp rỗng và kí hiệu là $\varnothing$.

d) Biểu diễn tập hợp:

Để biểu diễn một tập hợp cụ thể, có hai cách chính:

- *Cách 1*: Biểu diễn tập hợp bằng liệt kê, nghĩa là phải chỉ ra từng phần tử trong tập hợp đó.

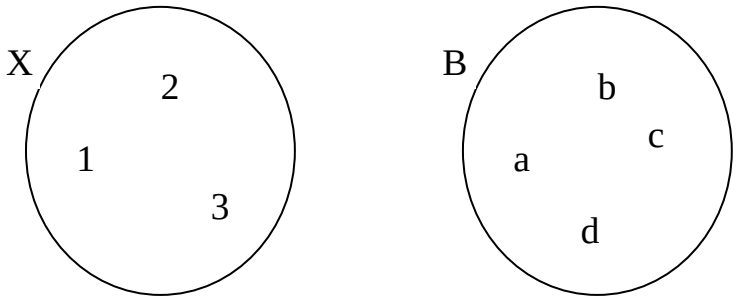
Ví dụ 1: A = {1; 2; 3; 4}; B = {máy 1; máy 2; máy 3; máy 4; máy 5}

Trong ngôn ngữ lập trình, các kiểu dữ liệu có thể dùng phương pháp liệt kê để xác định tầm vực của kiểu dữ liệu, nghĩa là cho biết kiểu dữ liệu đó có khả năng lưu trữ những giá trị dữ liệu nào.

- *Cách 2*: Biểu diễn tập hợp bằng cách nêu thuộc tính đặc trưng, là thuộc tính để nhận biết một phần tử có thuộc một tập hợp hay không.

Ngoài ra, có thể sử dụng biểu đồ Venn để biểu diễn tập hợp một cách trực quan. Biểu đồ Venn biểu diễn bằng một hình tròn, bên trong hình tròn thể hiện các phần tử của tập hợp.

Ví dụ 2: Biểu đồ Venn biểu diễn cho tập hợp X = {1; 2; 3} và tập hợp B = {a; b; c; d}.



1.2. Các phép toán trên tập hợp

Để thao tác trên tập hợp, cần có một số phép toán của tập hợp, như kiểm tra một phần tử có thuộc một tập hợp hay không, hợp của hai tập hợp, giao của hai tập hợp, hiệu của hai tập hợp, phần bù của một tập hợp trong một tập hợp vũ trụ.

a) Kiểm tra một phần tử thuộc/ không thuộc một tập hợp:

- Kí hiệu: $\in$ và $\notin$

Ví dụ 3: $1 \in \{1; 2; 3\}$ là đúng, $4 \in \{1; 2; 3\}$ là sai, nhưng $4 \notin \{1; 2; 3\}$ là đúng.

Từ phép toán này dẫn đến khái niệm tập hợp con: Tập hợp A là một tập hợp con của tập hợp B nếu mỗi phần tử của A đều là phần tử của B, kí hiệu $A \subset B \Leftrightarrow \forall x \in A$ thì $x \in B$.

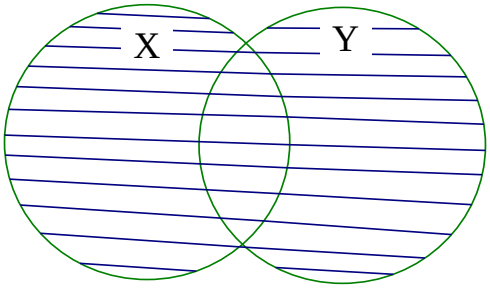
Để biểu thị trực quan mối quan hệ tập con, khi $A \subset B$ ta vẽ một đường mũi tên từ A đến B, bằng cách này sẽ dễ dàng nhìn thấy mối quan hệ giữa các tập hợp. $A \longrightarrow B$

b) Hợp của hai tập hợp (union):

- Hợp của hai tập hợp X và Y là một tập hợp Z gồm tất cả các phần tử của cả X và Y.

- Kí hiệu: $Z = X \cup Y = \{x \mid x \in X \text{ hoặc } x \in Y\}$

- Biểu đồ Venn cho hợp của hai tập hợp X và Y:



Ví dụ 4: Cho X = {a; b; c; d} và Y = {f; b; d; g}

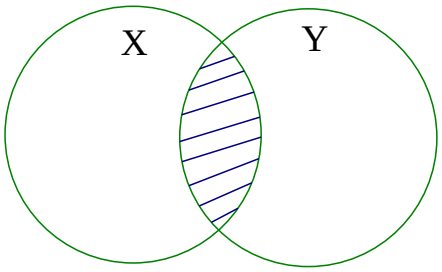
thì $X \cup Y$ = {a; b; c; d; f; g}

c) *Giao của hai tập hợp (intersection)*:

- Giao của hai tập hợp X và Y là một tập hợp Z gồm tất cả các phần tử vừa thuộc X, vừa thuộc Y.

- Kí hiệu: $Z = X \cap Y = \{x \mid x \in X \text{ và } x \in Y\}$

- Biểu đồ Venn cho giao của hai tập hợp X và Y:



Ví dụ 5: Cho S = {a; b; c; d} và T = {f; b; d; g}

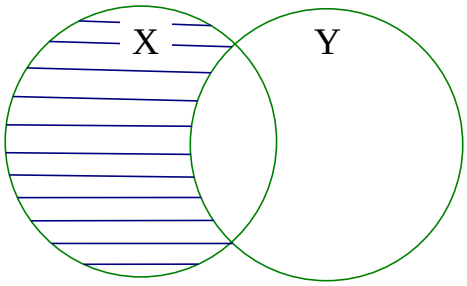
Thì $S \cap T$ = {b; d}

d) Hiệu của hai tập hợp (difference):

- Hiệu giữa tập hợp X với tập hợp Y là một tập hợp Z gồm tất cả các phần tử thuộc X nhưng không thuộc Y.

- Kí hiệu: Z = X - Y = {x | x∈X và x∉Y} hoặc Z = X \ Y = {x | x∈X và x∉Y}

- Biểu đồ Venn cho hiệu của hai tập hợp X và Y:



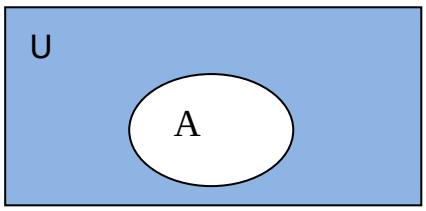
Ví dụ 6: Cho S = {a; b; c; d} và T = {f; b; d; g}

Thì S - T = {a; c}

e) Phần bù của tập hợp (complement):

- Cho tập hợp vũ trụ U và A là một tập hợp con của U. Phần bù của A trong U kí hiệu C_U^A hoặc nếu không nhầm lẫn có thể kí hiệu ngắn gọn là $\bar{A}$, là hiệu giữa U và A.

- Biểu đồ Venn cho phần bù của tập hợp A trong tập vũ trụ U:



Ví dụ 7: Cho T = {b; e; g} và U = {a; b; c; d; e; f; g}
thì $\bar{T}$= {a; c; d; f}

1.3. Tích Đề-các (Descartes)

a) Tích Đề-các của hai tập hợp:

Tích Đề-các của tập hợp X và Y là một tập hợp, kí hiệu X×Y:

X×Y = {(x, y)| x∈X và y∈Y}.

Ví dụ 8: X = {Toán; Tiếng Anh}; Y = {6; 7; 8} thì X×Y = {(Toán,6); (Toán,7); (Toán,8); (Tiếng Anh,6); (Tiếng Anh,7); (Tiếng Anh,8)}

b) Tích Đề-các của nhiều tập hợp:

Tích Đề-các giữa n tập hợp $X_1, X_2, \dots, X_n$ kí hiệu $X_1 \times X_2 \times \dots \times X_n$:

$X_1 \times X_2 \times \dots \times X_n = \{(x_1, x_2, \dots, x_n) | x_1 \in X_1, x_2 \in X_2, \dots, x_n \in X_n\}$

Khi $X_1 = X_2 = \dots = X_n = X$ thì kí hiệu tích Đề-các $\prod_{i=1}^{n} X_i$ là X^n.

Trong tin học, tích Đề-các cùng với khái niệm quan hệ là cơ sở để xây dựng lý thuyết cơ sở dữ liệu quan hệ.

1.4. Tính chất của các phép toán trên tập hợp

a) Phép hợp và phép giao có tính giao hoán

Với mọi tập hợp X, Y thì $X \cup Y = Y \cup X$ và $X \cap Y = Y \cap X$

b) Phép hợp và giao có tính kết hợp

Với mọi tập hợp X, Y, Z thì $X \cup (Y \cup Z) = (X \cup Y) \cup Z$

và $X \cap (Y \cap Z) = (X \cap Y) \cap Z$

c) Giữa phép hợp và giao có tính phân phối

Với mọi tập hợp X, Y, Z thì $X \cup (Y \cap Z) = (Y \cup X) \cap (X \cup Z)$

và $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

d) Công thức De Morgan

Với mọi tập hợp X, Y thì $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$ và $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$

e) Gọi $\mathbb{P}(A)$ là tập hợp tất cả các tập con của A và gọi |A| là số phần tử của A (hay bản số của A trong trường hợp A có vô hạn phần tử) thì số phần tử của $\mathbb{P}(A)$ bằng $2^{|A|}$.

f) Nếu $A \subset B$ thì $A \cap B = A$.

g) Nếu $A \subset B$ thì $A \cup B = B$.

h) Nếu $A \subset B$ thì $\bar{B} \subset \bar{A}$.

1.5. Tập hợp mờ

Trong thực tế, nhiều khi việc xem xét một đối tượng có thuộc một tập hợp nào đó hay không là điều không rõ ràng. Ví dụ, quần áo như thế nào gọi là dầy hay mỏng để máy giặt biết để tự động điều chỉnh chế độ giặt và sấy một cách hợp lý nhất.

Một cách tiếp cận mới về tập hợp để có khả năng lưu trữ những đối tượng có độ không rõ ràng khác nhau, đó là lý thuyết tập mờ do giáo sư Lotfi Zadeh ở trường đại học California – Hoa Kỳ xây dựng vào năm 1965.

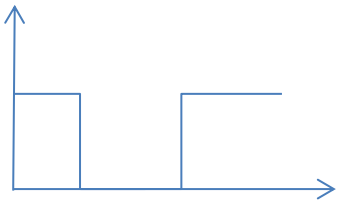
a) Khái niệm tập mờ (Fuzzy set):

Như chúng ta đã biết, tập hợp thường là kết hợp của một số phần tử có cùng một số tính chất chung nào đó, chẳng hạn tập hợp các sinh viên. Ta có :

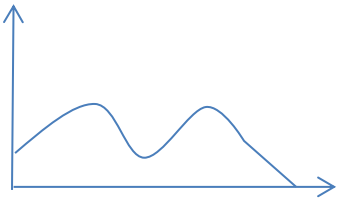
T = { t | t là sinh viên }

Vậy, nếu một người nào đó là sinh viên thì thuộc tập T, ngược lại là không thuộc tập T. Tuy nhiên, trong thực tế cuộc sống cũng như trong khoa học kỹ thuật có nhiều khái niệm không được định nghĩa một cách rõ ràng. Ví dụ, khi nói về một "nhóm sinh viên khá", thì thế nào là khá? Khái niệm về khá không rõ ràng vì có thể sinh viên có điểm thi trung bình bằng 8.4 là khá, cũng có thể điểm thi trung bình bằng 6.6 cũng là khá (phổ điểm khá có thể từ 6.5 đến 8.5),... Nói cách khác, "nhóm sinh viên khá" không được định nghĩa một cách tách bạch rõ ràng như khái niệm thông thường về tập hợp. Hoặc, khi chúng ta nói đến một “lớp các số lớn hơn 10” hoặc “ một đống quần áo cũ”,... là chúng ta đã nói đến những khái niệm mờ, hay những khái niệm không được định nghĩa một cách rõ ràng. Các phần tử của nhóm trên không có một tiêu chuẩn rõ ràng về tính “thuộc về” (thuộc về một tập hợp nào đó). Đây chính là những khái niệm thuộc về tập mờ. Trong đối thoại hàng ngày chúng ta bắt gặp rất nhiều khái niệm mờ này. Ví dụ, một ông giám đốc nói: “Năm qua chúng ta đã gặt hái được một số thành tích đáng khen ngợi. Năm tới đây chúng ta phải cố gắng thêm một bước nữa”.

Đây là một câu chứa rất nhiều khái niệm mờ, không rõ ràng. Như vậy, logic rõ có thể biểu diễn bằng như Hình a) là đồ thị rời rạc, logic mờ cũng có thể biểu diễn như Hình b) là đồ thị liên tục.



Hình a)



Hình b)

Cho Ω là không gian nền, một tập mờ A trên Ω tương ứng với một ánh xạ từ Ω đến đoạn [0,1].

Ánh xạ A : Ω →[0;1] được gọi là hàm thuộc về (membership function).

Kí hiệu A = {(a, $\mu_A(a)$) | a∈ Ω}

Trong đó, $\mu_A(a)$ ∈[0,1] chỉ mức độ thuộc về (membership degree) của phần tử a vào tập mờ A.

Khoảng xác định của hàm $\mu_A(a)$ là đoạn [0,1], trong đó giá trị 0 chỉ mức độ không thuộc về, còn giá trị 1 chỉ mức độ thuộc về hoàn toàn.

Ví dụ 9: Cho Ω= {1; 2; 3; 4; 5}, tập mờ A trên Ω tương ứng với ánh xạ μ_A như sau:

μ_A: 1 → 0

2 →1

3 →0.5

4 →0.3

5 →0.2

Ta có tập mờ A = {(1,0); (2,1); (3,0.5); (4,0.3); (5,0.2)}

Cách viết trên là sự liệt kê các phần tử khác nhau cùng với mức độ thuộc về tập hợp A.

Từ định nghĩa trên chúng ta có thể suy ra:

- Tập mờ A là rỗng nếu và chỉ nếu hàm thuộc về $\mu_A(a)$= 0, ∀a∈ Ω

- Tập mờ A là toàn phần nếu và chỉ nếu $\mu_A(a) = 1, \forall a \in \Omega$

- Hai tập mờ A và B bằng nhau nếu $\mu_A(x) = \mu_B(x)$ với mọi x trong **Ω**.

Ví dụ 10: Cho **Ω**= {1; 2; 3; 4; 5}, tập mờ A trên **Ω** tương ứng với ánh xạ μ_A như ví dụ trên.

A = {(1,0); (2,1); (3,0.5); (4,0.3); (5,0.2)}

Tập mờ B trên **Ω** tương ứng với ánh xạ μ_B như sau:

μ_B: $1 \rightarrow 0$

$2 \rightarrow 1$

$3 \rightarrow 0.5$

$4 \rightarrow 0.3$

$5 \rightarrow 0.2$

Ta có tập mờ B = {(1,0); (2,1); (3,0.5); (4,0.3); (5,0.2)}

Nhận thấy, $\mu_A(x) = \mu_B(x)$ với mọi x trong **Ω**. Vậy A= B.

b) Các phép trên tập mờ:

Để có thể tiến hành mô hình hóa các hệ thống có chứa tập mờ và biểu diễn các qui luật vận hành của hệ thống này, trước tiên chúng ta cần tới việc suy rộng các phép toán logic cơ bản với các mệnh đề có chân trị trên đoạn [0; 1].

Cho **Ω**= $\{P_1; P_2; ...\}$ với P_1, P_2, ... là các mệnh đề. Tập mờ A trên **Ω** tương ứng với ánh xạ v như sau:

$v : \Omega \rightarrow [0; 1]$

$\forall P_i \in \Omega \rightarrow v(P_i)$

Ta gọi $v(P_i)$ là chân trị của mệnh đề P_i trên [0; 1].

b1. Phép bù

Phép phủ định trong logic kinh điển là một trong những phép toán cơ bản cho việc xây dựng phép bù của 2 tập hợp. Để mở rộng phép này trong tập mờ chúng ta cần tới toán tử v(NOT P). Toán tử này phải thỏa các tính chất sau:

- v(NOT P) chỉ phụ thuộc vào v(P).

- Nếu v(P)=1 thì v(NOT P)=0

- Nếu v(P)=0 thì v(NOT P)=1

- Nếu $v(P_1) \leq v(P_2)$ thì $v(\text{NOT } P_1) \geq v(\text{NOT } P_2)$

Định nghĩa 1: Hàm $n : [0;1] \rightarrow [0; 1]$ không tăng thỏa mãn các điều kiện $n(0) = 1$, $n(1) = 0$, được gọi là hàm phủ định.

Ví dụ 11: Hàm $n(x) = 1 - x$ hay $n(x) = 1 – x^2$ là các hàm phủ định.

Ta có nhận xét:

- Nếu $v(P_1) < v(P_2)$ thì $v(\text{NOT } P_1) > v(\text{NOT } P_2)$

- v(NOT P)phụ thuộc liên tục vào v(P)

- v(NOT (NOT P)) = v(P)

Định nghĩa 2 (*Phần bù của một tập mờ*): Cho *n* là hàm phủ định, phần bù A của tập mờ A (có hàm thuộc về μ_A), kí hiệu A^C là một tập mờ với hàm thuộc về $\mu_A{}^C$ được xác định bởi :

$\mu_A{}^C(a) = n(\mu_A(a))$, với mỗi $a \in \Omega$.

Ví dụ 12: Với n(x) = 1 - x thì ta có:

$\mu_A{}^C(a) = n(\mu_A(a)) = 1-\mu_A(a)$, với mỗi $a \in \Omega$.

Cho $\Omega = \{1; 2; 3; 4; 5\}$, và A là tập mờ trong Ω như sau:

A = {(1,0); (2,1); (3,0.5); (4,0.3); (5,0.2)}

Ta có :

A^C = {(1,1); (2,0); (3,0.5); (4,0.7); (5,0.8)}

Định nghĩa 3:

a. Hàm phủ định *n* là nghiêm ngặt nếu nó là hàm liên tục và giảm nghiêm ngặt.

b. Hàm phủ định *n* là mạnh nếu nó là chặt và thỏa $n(n(x)) = x \ \forall x \in [0;1]$.

Định nghĩa 4:

Hàm $\varphi: [a; b] \rightarrow [a; b]$ gọi là một tự đồng cấu (automorphism) của đoạn [a; b] nếu nó là hàm liên tục, tăng nghiêm ngặt và $\varphi(a) = a$, $\varphi(b) = b$.

Định lý 1: Hàm $n:[0; 1] \rightarrow [0; 1]$ là hàm phủ định mạnh khi và chỉ khi có một tự đồng cấu φ của đoạn [0; 1] sao cho $n(x) = n(\varphi(x)) = \varphi^{-1}(1 - \varphi(x))$

Định lý 2: Hàm *n*: [0;1] →[0;1] là hàm phủ định nghiêm ngặt khi và chỉ khi có hai phép tự đồng cấu ψ, φ của [0; 1] sao cho n(x) = ψ(1- φ (x)).

b.2. Phép giao

Phép hội AND trong logic kinh điển là cơ sở để định nghĩa phép giao của 2 tập mờ.

Phép AND trong tập mờ thoả các tính chất sau:

- $v(P_1 AND\ P_2)$ chỉ phụ thuộc vào $v(P_1)$, $v(P_2)$.
- Nếu $v(P_1)=1$ thì $v(P_1 AND\ P_2) = v(P_2)$, với mọi P_2
- Giao hoán $v(P_1 AND\ P_2) = v(P_2 AND\ P_1)$
- Nếu $v(P1) \leq v(P2)$ thì $v(P1 AND\ P3) \leq v(P2 AND\ P3)$, với mọi P3
- Kết hợp $v(P1 AND\ (P2\ AND\ P3)) = v((P1 AND\ P2)\ AND\ P3)$

Định nghĩa 5: Hàm T: $[0;1]^2 \rightarrow [0;1]$ là phép hội (t-chuẩn) khi và chỉ khi thỏa các điều kiện sau:

- $T(1, x) = x$, với mọi $0 \leq x \leq 1$.
- T có tính giao hoán, nghĩa là: $T(x,y) = T(y,x)$, với mọi $0 \leq x, y \leq 1$.
- T không giảm theo nghĩa: $T(x,y) \leq T(u,v)$, với mọi $x \leq u, y \leq v$.
- T có tính kết hợp: $T(x,T(y,z)) = T(T(x,y),x)$, với mọi $0 \leq x, y, z \leq 1$.

Từ các tính chất trên có thể suy ra $T(0, x) = 0$.

Các ví dụ về các phép hội trên tập mờ:

$T(x,y) = \min(x, y)$

$T(x,y) = \max(0, x+y-1)$

$T(x,y) = x.y$ (tích đại số của x và y)

Định nghĩa 6: Cho hai tập mờ A, B trên cùng không gian nền Ω với hàm thuộc về $\mu_A(a)$, $\mu_B(a)$, cho T là một phép hội .

Ứng với phép hội T, tập giao của hai tập mờ A, B là một tập mờ trên Ω với hàm thuộc về cho bởi:

$\mu_{A \cap B}(a) = T(\mu_A(a), \mu_B(a)) \quad \forall a \in \Omega$

Với T(x,y)=min(x,y) ta có:

$\mu_{A \cap B}(a) = \min(\mu_A(a), \mu_B(a))$

Với T(x,y) = x.y ta có:

$\mu_{A\cap B}(a) = \mu_A(a).\mu_B(a)$ (tích đại số)

Ví dụ 13: Cho **Ω**= {1; 2; 3; 4; 5}, và A, B là các tập mờ trong **Ω** như sau:

A = {(1,0); (2,1); (3,0.5); (4,0.3); (5,0.2)}

B = {(1,0); (2,0.5); (3,0.7); (4,0.2); (5,0.4)}

Với T(x,y) = min(x,y), ta có :

A ∩ B = {(1,0); (2,0.5); (3,0.5); (4,0.2); (5,0.2)}

$A \cap A^C$ = {(1,0), (2,0.1), (3,0.5), (4,0.3), (5,0.2)}

b.3. Phép hợp

Phép tuyển OR trong logic kinh điển là cơ sở để định nghĩa phép hợp của 2 tập mờ. OR thoả các tính chất sau:

- v(P1OR P2) chỉ phụ thuộc vào v(P1), v(P2).
- Nếu v(P1) = 0 thì v(P1OR P2) = v(P2), với mọi P2
- Giao hoán v(P1OR P2) = v(P2OR P1)
- Nếu v(P1) ≤ v(P2) thì v(P1OR P3) ≤v(P2OR P3), với mọi P3
- Kết hợp v(P1OR (P2 OR P3)) = v((P1OR P2) OR P3).

Định nghĩa 7: Hàm S:[0,1]2→[0,1] được gọi là phép tuyển (t- đối chuẩn) nếu thỏa các tiên đề sau:

- S(0, x) = x, với mọi 0≤ x ≤1.
- S có tính giao hoán, nghĩa là : S(x,y) = S(y,x), với mọi 0≤ x,y ≤1.
- S không giảm theo nghĩa: S(x,y) ≤S(u,v), với mọi x ≤ u, y ≤ v.
- S có tính kết hợp : S(x,S(y,z)) = S(S(x,y),z), với mọi 0 ≤ x,y,z ≤ 1.

Từ các tính chất trên suy ra S(1,x) = 1.

Ví dụ 14:

S(x,y) = max(x,y)

S(x,y) = min(1, x+y)

S(x,y) = x + y - x.y

Định nghĩa 8: Cho hai tập mờ A, B trên cùng không gian nền **Ω** với hàm thuộc về $\mu_A(a)$, $\mu_B(a)$. Cho S là phép tuyển, phép hợp của hai tập mờ A, B là một tập mờ trên **Ω** với hàm thuộc về cho bởi:

$\mu_{A\cup B}(a) = S(\mu_A(a), \mu_B(a))$, $\forall a \in \Omega$

Với S(x,y) = max(x,y) ta có:

$\mu_{A\cup B}(a) = \max(\mu_A(a), \mu_B(a))$

Với S(x,y) = min(1, x+y)

$\mu_{A\cup B}(a) = \min(1, \mu_A(a) + \mu_B(a))$

Với S(x,y) = x + y + x.y

$\mu_{A\cup B}(a) = \mu_A(a) + \mu_B(a) - \mu_A(a).\mu_B(a)$

Ví dụ 15: Cho **Ω**= {1; 2; 3; 4; 5}, và A, B là các tập mờ trong **Ω** như sau:

A = {(1,0); (2,1); (3,0.5); (4,0.3); (5,0.2)}

B = {(1,0); (2,0.5); (3,0.7); (4,0.2); (5,0.4)}

Ta có : $A\cup B$ = {(1,0); (2,1); (3,0.7); (4,0.3); (5,0.4)}

$A\cup A^C$ = {(1,1); (2,1); (3,0.5); (4,0.7); (5,0.8)}

b.4. Một số qui tắc

Trong logic rõ với hai giá trị đúng, sai, có nhiều qui tắc đơn giản mà chúng ta thường sử dụng xem như tính chất hiển nhiên.

Ví dụ 16: Với bất kỳ tập rõ $A \subset \Omega$, ta có:

$A\cap A^C = \emptyset$ và $A \cup A^C = \Omega$.

Thực ra, những qui tắc này có được là nhờ vào sự xây dựng toán học trước đó.

Chuyển sang lý thuyết tập mờ thì hai tính chất quen dùng này đã không còn đúng nữa.

Do đó, chúng ta cần xem xét lại một số tính chất.

- Tính lũy đẳng (demportancy)

Chúng ta nói T là lũy đẳng nếu T(x,x) = x, $\forall x \in [0,1]$.

Tương tự, S là lũy đẳng nếu S(x,x) = x, $\forall x \in [0,1]$.

- Tính hấp thu (absorption)

Có hai dạng hấp thu:

- T(S(x,y),x) = x , $\forall x,y \in [0,1]$.

- S(T(x,y),x) = x , $\forall x,y \in [0,1]$.

• Tính phân phối (distributivity)

Có hai biểu thức xác định tính phân phối:

- S(x,T(y,z)) = T(S(x,y), S(x,z)), $\forall x,y,z \in [0,1]$.

- T(x,S(y,z)) = S(T(x,y), T(x,z)), $\forall x,y,z \in [0,1]$.

• Luật De Morgan

Cho T là t-chuẩn, S là t-đối chuẩn, *n* là phép phủ định. Chúng ta có bộ ba (T,S,*n*) là một bộ ba De Morgan nếu:

n(S(x,y)) = T(*n*(x),*n*(y)).

CÂU HỎI VÀ BÀI TẬP

1. Cho A = {1; 2; 3; 4}, B = {2; 4; 6; 8} và C = {3; 4; 5; 6}. Hãy tìm A∪B, A∪C, B∪C, B∪B, (A∪B)∪C, A∪(B∪C), A∪(B∩C), (A∪B)∩(A∪C).
2. Cho A và B là hai tập hợp. Hãy vẽ các đường mũi tên nối các tập hợp A, B, A∪B và A∩B.
3. Cho tập vũ trụ ∪ = {a; b; c; d; e; f; g} và A = {a; b; c; d; e}, B = {a; c; e; g}, C = {b ; d ; e}. Hãy tìm:

   1) A∪C 2) C-B 3) A-B 4) $\overline{A - C}$ 5) $\overline{A - B}$

   6) B∩A 7) $\bar{B}$ 8) $\bar{B} \cap C$ 9) $\bar{C} \cap A$ 10) $\overline{A \cap \bar{A}}$

4. Chứng minh rằng nếu A∩B = ∅ thì A⊂$\bar{B}$.
5. Hoàn thành các phát biểu dưới đây bằng cách điền ⊂, ⊃ hoặc ≠ giữa mỗi cặp tập hợp A và B tuỳ ý:

   1) A….A-B 2) $\bar{A}$….B-A 3) $\bar{A}$….A-B

   4) A….A∩B 5) A….A∪B 6) A….B-A

6. Chứng mính rằng A-B là tập con của A∪B.
7. Chứng mính rằng nếu A⊂B thì A∩B = A.
8. Chứng mính rằng để A∩B = ∅ thì B∩$\bar{A}$ =B.

9. Chứng mính rằng nếu A⊂B thì A∪B = B.

10. Chứng minh rằng $\bar{A}$- $\bar{B}$ = B-A.

11. Chứng minh rằng nếu A∩B = ∅ thì A∪$\bar{B}$ = $\bar{B}$.

12. Chứng minh rằng nếu A⊂B thì A∪(B-A) = B.

13. Cho **Ω** = {6, 2, 7, 4, 9}, các tập mờ A, B, C trên **Ω** tương ứng với ánh xạ μ_A , μ_B và μ_C như sau:

A = {(6,0.2), (2,0.9), (7,0.5), (4,0.3), (9,0.2)}

B = {(6,0), (2,1), (7,0.5), (4,0.6), (9,0.1)}

C = {(6,0.3), (2,0.1), (7,1), (4,0), (9,0.5)}

a) Tính các tập A^C, B^C và C^C với hàm nghịch đảo là n(x)=1-x

b) Tính A∩B, B∩C, A∩B∩C, A∩C^C, A∩C^C với T(x,y) = min(x,y)

c) Tính A∪B, B∪C, A∪B∪C, A∪C^C, A∪C^C với S(x,y) = max(x,y)

14. Cho các tập mờ A, B, C được định nghĩa trên nền số nguyên **Ω** = [0,5] với các hàm thuộc về như sau:

$$\mu_A = \frac{1}{x+2}\,,\ \mu_B = \frac{1}{x+1} \text{ và } \mu_C = \frac{1}{x+3}$$

Hãy xác định các tập mờ sau ở dạng liệt kê và đồ thị:

a) Tính các tập A^C, B^C và C^C với hàm nghịc đảo n(x) = 1 – x

b) Tính A∩B, B∩C, A∩B∩C, A∩C^C, A∩C^C với T(x,y) = min(x,y)

c) Tính A∪B, B∪C, A∪B∪C, A∪C^C, A∪C^C với S(x,y) = max(x,y)

15. Thiết lập mô hình phân loại sinh viên qua các tập mờ sinh viên cần cù, sinh viên thông minh và sinh viên lười.

16. Cho A là tập mờ xác định trên nền X. Hãy chỉ ra rằng biểu thức A∩C^C = X không đúng như đối với tập hợp kinh điển.

17. Kiểm tra xem tập mờ A, B với các hàm thuộc về xác định ở bài tập 2 là

thỏa hai công thức của De Morgan.

Bài tập trên máy tính

18. Viết chương trình cài đặt cấu trúc dữ liệu cho tập hợp và xây dựng các phép toán trên tập hợp.

II. ÁNH XẠ

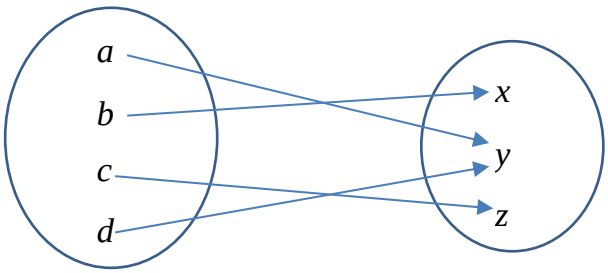
2.1. Khái niệm ánh xạ

Định nghĩa 1: Cho hai tập hợp X và Y. Một ánh xạ *f* từ tập hợp X vào tập hợp Y, kí hiệu *f*: X→Y là một qui tắc đặt tương ứng mỗi phần tử X với một phần tử duy nhất y (kí hiệu *f*(x) = y). Khi đó x gọi là một tạo ảnh của y và y là ảnh của x qua ánh xạ *f*.

Ví dụ 1:

1) *f*: N→ N sao cho ∀n∈N, *f*(n) = 2n + 1 là một ánh xạ.

2) Cho A = {a; b; c; d} và B = {x; y; z}. Ánh xạ f: A→B cho bởi sơ đồ sau:



c) Chú ý: Để *f*: X→Y là một ánh xạ cần phải thỏa:

- Mọi phần tử của X phải có ảnh tương ứng, nhưng có thể tồn tại một phần tử của Y không có tạo ảnh.

- Mỗi phần tử của X có duy nhất một ảnh.

2.2. Các loại ánh xạ

a) Đơn ánh:

Định nghĩa 2: Ánh xạ f: X→Y được gọi là đơn ánh nếu $\forall x_1, x_2 \in X$ mà $x_1 \neq x_2$ thì $f(x_1) \neq f(x_2)$ (hoặc $f(x_1) = f(x_2)$ thì $x_1 = x_2$).

Ví dụ 2:

+ Ánh xạ f: N$\to$ N, $\forall n\in N$, $f(n) = 2n + 1$ là đơn ánh vì: $\forall n_1, n_2\in N$ mà $f(n_1) = f(n_2) \Rightarrow 2n_1 + 1 = 2n_2 + 1 \Rightarrow n_1 = n_2$.

+ Ánh xạ g: Z$\to$Z sao cho $\forall z\in Z$, $g(z) = z^2$ không phải đơn ánh, vì $\exists z_1=1, z_2= -1, z_1\neq z_2$ nhưng $g(z_1) = 1 = g(z_2)$.

b) Toàn ánh:

Định nghĩa 3: Ánh xạ f: X$\to$Y được gọi là toàn ánh nếu $\forall y\in Y$, $\exists x\in X$ sao cho $f(x)=y$ (hoặc $f(X) = Y$).

Ví dụ 3: Ánh xạ f: R$\to$[0;1] sao cho $\forall x\in R$, $f(x) = \sin(x)$ là toàn ánh, vì $\forall y\in[0;1]$ luôn tồn tại $x\in R$ để $\sin(x)=y$ (theo tính chất của hàm sin).

c) Song ánh:

Định nghĩa 4: Ánh xạ f: X$\to$Y được gọi là song ánh nếu f vừa là đơn ánh, vừa là toàn ánh.

Ví dụ 4: Ánh xạ f: R$\to$R sao cho $\forall x\in R$, $f(x) = 2x + 1$ là toàn ánh, vì:

+ f là đơn ánh (dễ nhận thấy)

+ f là toàn ánh, vì $\forall y\in Y$, giả sử $f(x) = y \Rightarrow 2x + 1 = y \Rightarrow x = \frac{y-1}{2} \in R$

2.3. Một số ánh xạ đặc biệt

a) Ánh xạ đồng nhất:

Định nghĩa 5: Cho X là một tập hợp. Ánh xạ f: X$\to$X gọi là ánh xạ đồng nhất nếu $f(x) = x$ với mọi $x\in X$. Ta thường kí hiệu ánh xạ đồng nhất này bởi 1 hoặc 1_X.

b) Ánh xạ hằng:

Định nghĩa 6: Ánh xạ f: X$\to$Y gọi là ánh xạ hằng nếu $f(x) = b$ với mọi $x\in X$ và b là phần tử xác định của Y.

c) *Ánh xạ đặc trưng*:

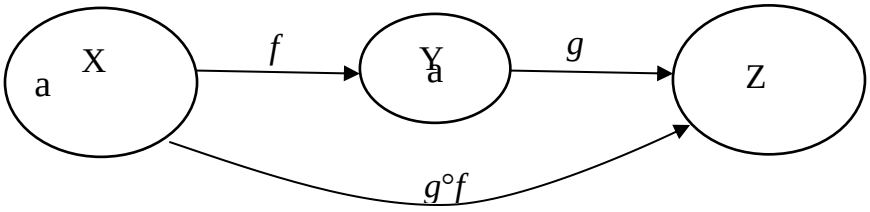
Định nghĩa 7: Ánh xạ dạng π: X$\to\{0; 1\}$ gọi là ánh xạ đặc trưng của tập hợp X. Ánh xạ này thường sử dụng để xác định một phần tử của X có thuộc một tập hợp nào đó hay không.

d) *Hàm dấu*:

Định nghĩa 8: Ánh xạ dạng *sign*: X→{-1; 0; 1} gọi là hàm dấu của tập hợp X.

2.4. Ánh xạ hợp

Định nghĩa 9: Cho hai ánh xạ *f*: X→Y và *g*: Y→Z. Ánh xạ *h*: X→Z gọi là ánh xạ hợp của ánh xạ f và g, kí hiệu $h = g \circ f$, nếu $\forall x \in X$, $h(x) = g(f(x))$.



Ví dụ 5: Ánh xạ *f*: R→R, $f(x) = 3x + 1$ và *g*: R→R, $g(x) = 2x$ thì ánh xạ hợp của $g \circ f$: R→R, $g(f(x)) = g(3x + 1) = 2(3x + 1) = 6x + 2$.

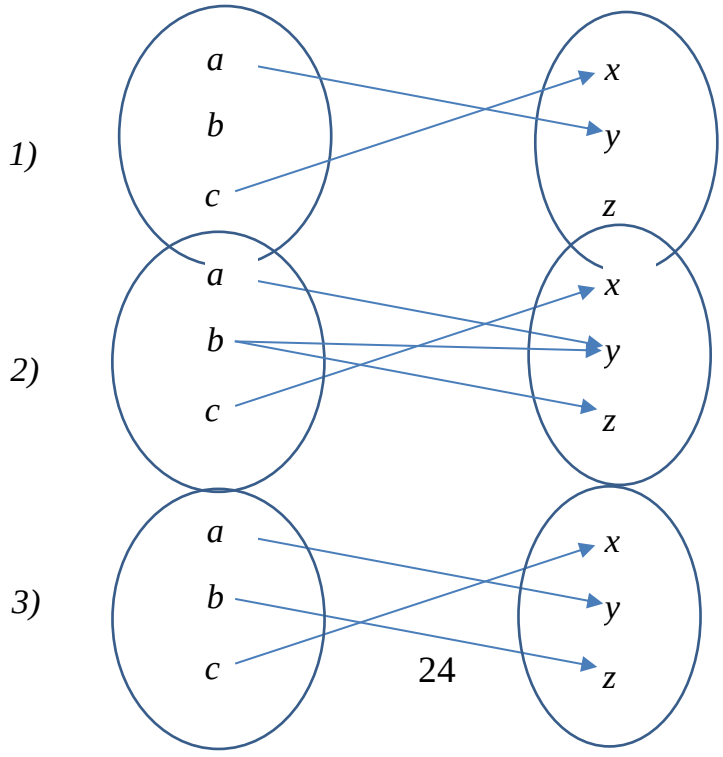
Nhưng ánh xạ hợp $f \circ g$: R→R, $f(g(x)) = f(2x) = 3(2x) + 1 = 6x + 1$.

Từ ví dụ trên, cho thấy nói chung $h \circ f \neq f \circ g$.

Lưu ý: Cho ánh xạ *f*: A→B thì $1_B \circ f = f$ và $f \circ 1_A = f$

CÂU HỎI VÀ BÀI TẬP

1. Cho biết trong các tương ứng từ tập hợp A = {a; b; c} vào tập hợp B = {x; y; z}, tương ứng nào là ánh xạ?



2. Đối với mỗi ánh xạ dưới đây, hãy xác định xem có phải là đơn ánh không? Tìm ảnh của miền xác định ánh xạ trên.

a) $f : Z \to Z$, $f(x) = 2x + 1$

b) $f : Q \to Q$, $f(x) = 2x + 1$

c) $f : Z \to Z$, $f(x) = x^3 - x$

d) $f : R \to R$, $f(x) = e^x$

e) $f : [-\frac{\pi}{2}; \frac{\pi}{2}] \to R$, $f(x) = \sin x$

f) $f : [0;\pi] \to R$, $f(x) = \sin x$

3. Với mỗi ánh xạ sau $f: Z \to Z$ dưới đây, hãy xác định xem có là đơn ánh hay toàn ánh không? Tìm $f(Z)$.

a) $f(x) = x + 7$ b) $f(x) = 2x - 3$ c) $f(x) = -x + 5$

d) $f(x) = x^2$ e) $f(x) = x^2 + x$ f) $f(x) = x^3$

4. Cho 3 ánh xạ $f: A \to B$, $g: B \to C$, $h: C \to D$. Hãy chứng minh rằng $(h \circ g) \circ f = h \circ (g \circ f)$

5. Xét 3 ánh xạ f, g, h từ Z vào Z xác định bởi:

$f(x) = x - 1$, $g(x) = 3x$ và $h(x) = \begin{cases} 0 \text{ nếu } x \text{ chẵn} \\ 1 \text{ nếu } x \text{ lẻ} \end{cases}$

a) Tìm $f \circ g$, $g \circ f$, $g \circ h$, $h \circ g$, $f \circ g \circ h$

b) Xác định f^2, f^3, g^2, g^3, h^2, h^3, h^{100}

6. Cho trước 2 tập hợp con cố định S, T của U. Chứng minh rằng $f^2 = f$.

7. Cho hai ánh xạ $f, g: R \to R$ xác định bởi $f(x) = ax + b$ và $g(x) = cx + d$, trong đó a, b, c, d là các hằng số thực. Hãy tìm các hệ thức giữa a, b, c, d để cho $f \circ g = g \circ f$.

8. Xét ánh xạ $f: R \to R$ định nghĩa bởi:

$$f(x) = \begin{cases} x + 7 \text{ nếu } x \leq 0 \\ -2x + 5 \text{ nếu } 0 < x < 3 \\ x - 1 \text{ nếu } 3 \leq x \end{cases}$$

a) Tìm $f^{-1}(-10)$, $f^{-1}(0)$, $f^{-1}(2)$, $f^{-1}(6)$

b) Tìm $f^{-1}([-5; -1])$, $f^{-1}([-2; 4])$

9. Xét hai ánh xạ f: A $\rightarrow$ B, g: B $\rightarrow$ C

a) Chứng minh rằng nếu $g \circ f$ đơn ánh thì f đơn ánh.

b) Chứng minh rằng nếu $g \circ f$ toàn ánh thì f toàn ánh.

c) Chứng minh rằng nếu f và g song ánh thì $g \circ f$ song ánh.

d) Cho ví dụ để $g \circ f$ song ánh nhưng f và g không phải song ánh.

Chương II
LOGIC

MỤC TIÊU CỦA CHƯƠNG

Học xong chương này, sinh viên phải nắm bắt được các vấn đề sau:

- Thế nào là mệnh đề, chân trị của mệnh đề, các phép toán mệnh đề
- Thực hiện được các phép toán mệnh đề
- Thế nào là vị từ, các lượng từ phổ dụng và tồn tại
- Biết kết hợp lượng từ với vị từ để biểu diễn các mệnh đề
- Hiểu được các ứng dụng của phép toán logic trong lập trình và trong đời sống hàng ngày.

TÀI LIỆU THAM KHẢO

1. Nguyễn Hữu Anh, 1999, Toán rời rạc, NXB Giáo dục
2. Đại học Cần Thơ, 2003, Bài giảng Toán rời rạc 2
3. Phạm Thế Long (chủ biên), Nguyễn Xuân Viên, Nguyễn Thiện Luân, Nguyễn Đức Hiếu, Nguyễn Văn Xuất, 2005, Toán rời rạc, NXB Đại học Sư phạm
4. Kenneth H. Rosen (Bùi Xuân Toại dịch), 2010, Toán rời rạc và những ứng dụng trong Tin học, NXB Lao động.

I. ĐẠI SỐ MỆNH ĐỀ

1.1. Định nghĩa mệnh đề

Định nghĩa 1: Một khẳng định có giá trị hoặc đúng hoặc sai (nhưng không thể vừa đúng vừa sai) được gọi là một mệnh đề.

Ví dụ 1: Các khẳng định dưới đây là các mệnh đề

1. 2 + 3 = 5
2. Tam giác đều có 3 cạnh bằng nhau
3. Toronto là thủ đô của Canada

4. Hà Nội là thủ đô của Việt Nam
5. Tam giác đều có 3 cạnh bằng nhau

Như vậy, một mệnh đề có thể là mệnh đề đúng hoặc mệnh đề sai. Hay nói cách khác, một mệnh đề chỉ có thể lựa chọn một trong hai giá trị là đúng hoặc là sai.

Một mệnh đề không thể vừa đúng vừa sai.

Ví dụ 2: Xét các câu phát biểu sau

1. Hôm nay là thứ mấy ?
2. Một số thực âm không phải là số chính phương
3. Hãy đọc kỹ đoạn này
4. x + 1 = 2

Câu **"**Hôm nay là thứ mấy?**"** không là mệnh đề vì nó chỉ là một câu hỏi không có giá trị đúng, sai. Câu "Một số âm không phải là số chính phương" có chân trị là đúng nếu xét trên tập hợp số thực R nhưng lại có chân trị sai khi xét trên tập hợp số phức. Câu "x+1 = 2" không phải là mệnh đề vì chúng chẳng đúng cũng chẳng sai bởi các biến trong những câu đó chưa được gán cho một giá trị cụ thể nào.

Giá trị đúng, sai của một mệnh đề được gọi là chân trị của mệnh đề đó. Chân trị của mệnh đề đúng ký hiệu là T (true), chân trị của mệnh đề sai ký hiệu là F (false).

Bảng chân trị của mệnh đề bao gồm các trường hợp đúng, sai có thể xảy ra của mệnh đề đó.

Mục đích của chúng ta là phân biệt các mệnh đề để xác định chân trị của nó. Sự xác định chân trị này dựa vào thực nghiệm và lý luận. Lý luận ở đây là xác định chân trị của mệnh đề bằng cách kết hợp các mệnh đề mà ta đã biết chân trị. Các luật lệ chế ngự cách kết hợp mang tính chính xác của phép toán đại số. Vì thế, chúng ta cần nói đến Đại số mệnh đề".

1.2. Các phép tính mệnh đề

Trong phép tính mệnh đề, người ta không quan tâm đến ý nghĩa của

câu phát biểu mà chỉ chú ý đến chân trị của các mệnh đề. Do đó, khi thực hiện các phép toán mệnh đề thông thường người ta không ghi rõ các câu phát biểu mà chỉ ghi ký hiệu. Các chữ cái sẽ được dùng để ký hiệu các mệnh đề. Những chữ cái thường dùng là p, q, r,… hoặc P, Q, R,…

Mệnh đề chỉ có một giá trị đơn (luôn đúng hoặc sai) được gọi là mệnh đề sơ cấp (atomic proposition), thường kí hiệu bằng chữ cái thường. Các mệnh đề không phải là mệnh đề sơ cấp được gọi là mệnh đề phức hợp (compound propositions), thường kí hiệu bằng chữ cái hoa. Thông thường, tất cả mệnh đề phức hợp là mệnh đề liên kết (có chứa phép tính mệnh đề).

Các phép tính mệnh đề được sử dụng nhằm mục đích kết nối các mệnh đề lại với nhau tạo ra một mệnh đề mới. Các phép toán mệnh đề được trình bày trong chương này bao gồm: phép phủ định, phép hội, phép tuyển, phép XOR, phép kéo theo, phép tương đương.

1.2.1. Phép phủ định (negation)

Định nghĩa 2: Cho P là một mệnh đề, câu **"**không phải là P**"** là một mệnh đề khác được gọi là phủ định của mệnh đề P. Kí hiệu: ¬ P (hoặc $\overline{P}$).

Ví dụ 3: P = "2 > 0"

Thì ¬ P = "2 ≤ 0"

Bảng chân trị (truth table)

P	¬P
T	F
F	T

Qui tắc: Nếu P có giá trị là T thì phủ định của P (kí hiệu ¬P) có giá trị là F và ngược lại nếu P có giá trị F thì ¬P có giá trị T.

1.2.2. Phép hội (conjunction)

Định nghĩa 3: Cho hai mệnh đề P, Q. Câu xác định "P và Q" là một mệnh đề mới được gọi là hội của 2 mệnh đề P và Q, kí hiệu P ∧ Q.

Ví dụ 4: Cho 2 mệnh đề P và Q như sau: P = "2 > 0" là mệnh đề đúng.

Q = "2 = 0" là mệnh đề sai.

P ∧ Q = "2> 0 và 2 = 0" là mệnh đề sai.

Bảng chân trị:

P	Q	P ∧ Q
T	T	T
T	F	F
F	T	F
F	F	F

Qui tắc: Hội của 2 mệnh đề **chỉ đúng** khi cả hai mệnh đề đều đúng. Các trường hợp còn lại là sai.

1.2.3. Phép tuyển (disjunction)

Định nghĩa 4: Cho hai mệnh đề P, Q. Câu xác định "P hay (hoặc) Q" là một mệnh đề mới được gọi là tuyển của 2 mệnh đề P và Q. Kí hiệu P ∨ Q.

Ví dụ 5: Cho 2 mệnh đề P và Q như sau

P = "2 > 0" là mệnh đề đúng

Q = "2 = 0" là mệnh đề sai

P ∨ Q = "2 ≥ 0" là mệnh đề đúng.

Bảng chân trị:

P	Q	P ∨ Q
T	T	T
T	F	T
F	T	T
F	F	F

Qui tắc: Tuyển của 2 mệnh đề **chỉ sai** khi cả hai mệnh đề đều sai. Các trường hợp còn lại là đúng.

1.2.4. Phép XOR

Định nghĩa 5: Cho hai mệnh đề P và Q. Câu xác định "loại trừ P hoặc lọai trừ Q", nghĩa là "hoặc là P đúng hoặc Q đúng nhưng không đồng thời cả hai là đúng" là một mệnh đề mới được gọi là P XOR Q. Kí hiệu $P \oplus Q$.

Bảng chân trị:

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

1.2.5. Phép toán trên bit

Các máy tính dùng các bit để biểu diễn thông tin. Một bit có 2 giá trị khả dĩ là 0 và 1. Bit cũng có thể được dùng để biểu diễn chân trị. Thường người ta dùng bit 1 để biểu diễn chân trị đúng và bit 0 để biểu diễn chân trị sai. Các phép toán trên bit trong máy tính là các phép toán logic. Thông tin thường được biểu diễn bằng cách dùng các xâu bit. Ta có định nghĩa xâu bit như sau:

Định nghĩa 6: Một xâu bit (hoặc xâu nhị phân) là dãy có một hoặc nhiều bit. Chiều dài của xâu là số các bit trong xâu đó.

Ví dụ 6: 101011000 là một xâu bit có chiều dài là 9.

Có thể mở rộng các phép toán trên bit tới các xâu bit. Người ta định nghĩa các OR bit, AND bit và XOR bit đối với 2 xâu bit có cùng chiều dài là các xâu có các bit của chúng là các OR, AND, XOR của các bit tương ứng trong 2 xâu tương ứng. Chúng ta cũng dùng các kí hiệu $\wedge$, $\vee$, $\oplus$ để biểu diễn các phép tính OR bit, AND và XOR tương ứng.

Ví dụ 7: Tìm OR bit, AND bit và XOR bit đối với 2 xâu sau đây (mỗi xâu được tách thành 2 khối, mỗi khối có 5 bit cho dễ đọc)

01101	10110	
11000	11101	

11101	11111	OR bit
01000	10100	AND bit
10101	1011	XOR bit

1.2.6. Phép kéo theo (implication)

Định nghĩa 7: Cho P và Q là hai mệnh đề. Câu "Nếu P thì Q" là một mệnh đề mới được gọi là mệnh đề kéo theo của hai mệnh đề P,Q. Kí hiệu P → Q. P được gọi là giả thiết và Q được gọi là kết luận.

Ví dụ 8: Cho hai mệnh đề P và Q như sau :

P = " Tam giác T là đều"

Q = "Tam giác T có một góc bằng 60°"

Để xét chân trị của mệnh đề P → Q, ta có nhận xét sau :

- Nếu P đúng, nghĩa là tam giác T là đều thì rõ ràng rằng P → Q là đúng.
- Nếu P sai, nghĩa là tam giác T không đều và cũng không là cân thì dù

Q là đúng hay sai thì mệnh đề P → Q vẫn đúng.

Sau đây là bảng chân trị của của mệnh đề P →Q.

P	Q	P→Q
T	T	T
T	F	F
F	T	T
F	F	T

Qui tắc: Mệnh đề kéo theo **chỉ sai** khi giả thiết đúng và kết luận sai. Các trường hợp khác là đúng.

Từ mệnh đề P → Q, chúng ta có thể tạo ra các mệnh đề kéo theo khác như là mệnh đề Q → P và ¬Q → ¬P được gọi là mệnh đề đảo và mệnh đề phản đảo của mệnh đề P → Q.

Ví dụ 9: Tìm mệnh đề đảo và phản đảo của mệnh đề sau "Nếu tôi có nhiều tiền thì tôi mua xe hơi"

Mệnh đề đảo là:

" Nếu tôi mua xe hơi thì tôi có nhiều tiền"

Mệnh đề phản đảo là:

"Nếu tôi không mua xe hơi thì tôi không có nhiều tiền"

1.2.7. Phép tương đương (biconditional)

Định nghĩa 8: Cho P và Q là hai mệnh đề. Câu "P nếu và chỉ nếu Q" là một mệnh đề mới được gọi là P tương đương Q. Kí hiệu $P \leftrightarrow Q$. Mệnh đề tương đương đúng khi P và Q có cùng chân trị.

$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$ Đọc là : P nếu và chỉ nếu Q.

P là cần và đủ đối với Q Nếu P thì Q và ngược lại.

Bảng chân trị:

P	Q	P↔Q
T	T	T
T	F	F
F	T	F
F	F	T

1.3. Biểu thức mệnh đề (logical connectives)

1.3.1. Khái niệm

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.

Chính xác hơn ta có thể định nghĩa biểu thức mệnh đề bằng đệ qui như sau :

- Các mệnh đề sơ cấp là những biểu thức mệnh đề.
- Nếu A và B là 2 biểu thức mệnh đề thì $\neg A$, $A \vee B$, $A \wedge B$, $A \oplus B$,

$A \rightarrow B$, $A \leftrightarrow B$ là những biểu thức mệnh đề.

Chân trị của biểu thức mệnh đề là kết quả nhận được từ sự kết hợp giữa các phép toán và chân trị của các biến mệnh đề.

Ví dụ 10: Tìm chân trị của mệnh đề $\neg P \vee (Q \wedge R)$.

P	$\neg$ P	Q	R	$Q \wedge R$	$\neg P \vee (Q \wedge R)$
T	F	T	T	T	T
T	F	T	F	F	F
T	F	F	T	F	F
T	F	F	F	F	F
F	T	T	T	T	T
F	T	T	F	F	T
F	T	F	T	F	T
F	T	F	F	F	T

Do biểu thức mệnh đề là sự liên kết của nhiều mệnh đề bằng các phép toán nên chúng ta có thể phân tích để biểu diễn các biểu thức mệnh đề này bằng một cây mệnh đề.

Ví dụ 11: Xét câu phát biểu sau:

"Nếu Michelle thắng trong kỳ thi Olympic, mọi người sẽ khâm phục cô ấy, và cô ta sẽ trở nên giàu có. Nhưng, nếu cô ta không thắng thì cô ta sẽ mất tất cả."

Đây là một biểu thức mệnh đề và phép toán chính là phép hội và phép kéo theo. Có thể viết lại như sau:

"Nếu Michelle thắng trong kỳ thi Olympic, mọi người sẽ khâm phục cô ấy, và cô ta sẽ trở nên giàu có.

Nhưng, nếu cô ta không thắng thì cô ta sẽ mất tất cả."

Cả hai mệnh đề chính trong biểu thức mệnh đề này là mệnh đề phức hợp. Có thể định nghĩa các biến mệnh đề như sau:

P = "*Michelle thắng trong kỳ thi Olympic"*

Q = *"Mọi người sẽ khâm phục cô ấy"*

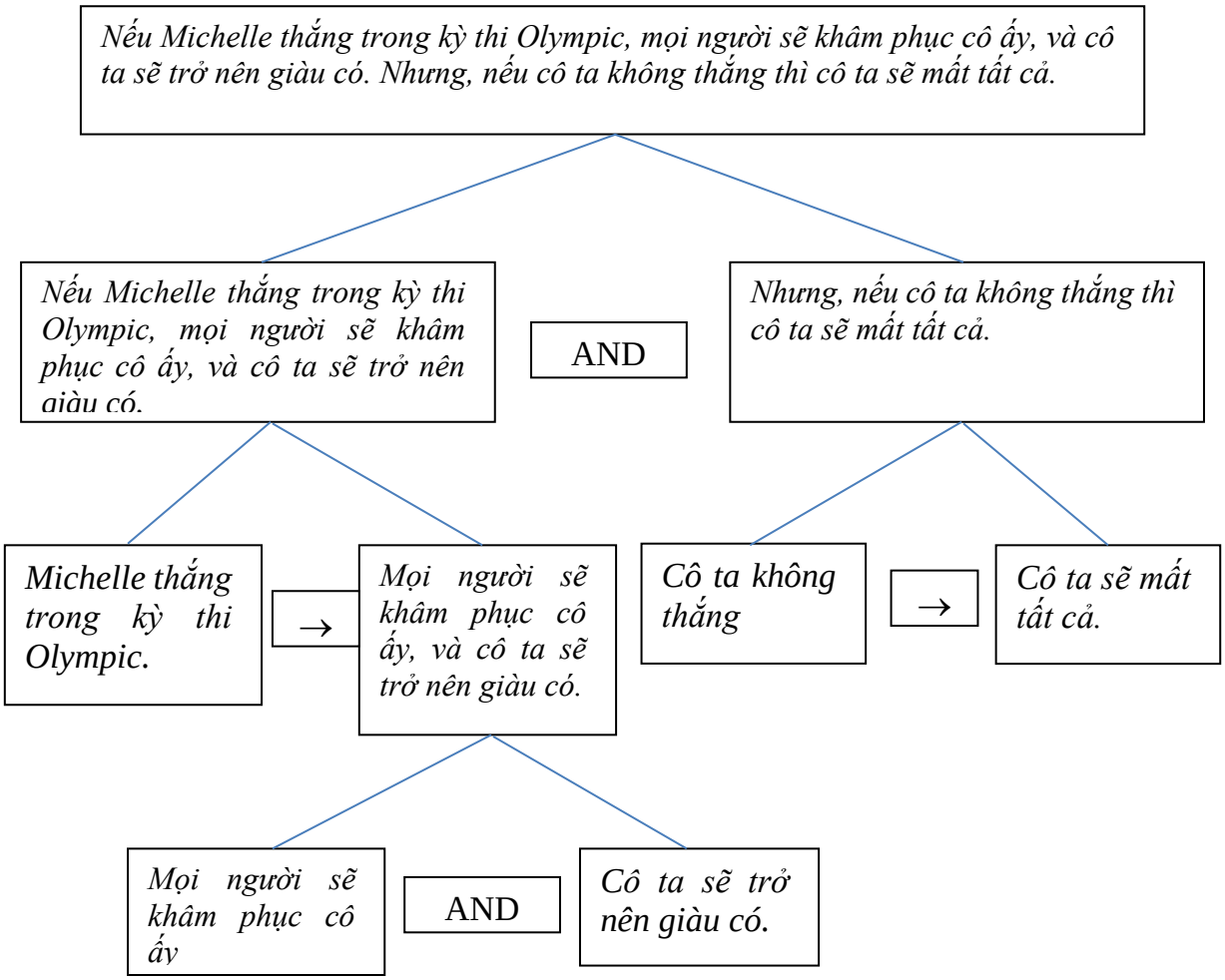
R = *"Cô ta sẽ trở nên giàu có"*

S = *"Cô ta sẽ mất tất cả"*

Biểu diễn câu phát biểu trên bằng các mệnh đề và các phép toán, ta có biểu thức mệnh đề sau :

$(P \rightarrow (Q \wedge R)) \wedge (\neg P \rightarrow S)$

Biểu diễn câu phát biểu trên thành một cây ngữ nghĩa như sau :



1.3.2. Định nghĩa Hằng đúng (tautologie)

Định nghĩa 9: Một hằng đúng là một mệnh đề có chân trị là đúng.

Một hằng đúng cũng là một biểu thức mệnh đề luôn có chân trị là đúng với mọi giá trị của biến mệnh đề.

Ví dụ 12: Xét chân trị của biểu thức mệnh đề $\neg P \vee P$

P	¬P	¬P ∨ P
T	F	T

F	T	T

Vậy ¬P∨P là một hằng đúng.

1.3.3. Định nghĩa Hằng sai (contradiction)

Định nghĩa 10: Một hằng sai là một mệnh đề có chân trị là sai.

Một hằng sai cũng là một biểu thức mệnh đề luôn có chân trị là sai với mọi giá trị của biến mệnh đề.

Ví dụ 13: Xét chân trị của biểu thức mệnh đề ¬P ∧ P

P	¬P	¬P ∧ P
T	F	F
F	T	F

Vậy ¬P∧P là một hằng sai.

1.3.4. Định nghĩa tiếp liên (contingency)

Định nghĩa 11: Một tiếp liên là một biểu thức mệnh đề không phải là hằng đúng và không phải là hằng sai.

Ví dụ 14: Tìm chân trị của biểu thức mệnh đề (P ∧ Q) ∨ ¬Q

P	Q	P ∧ Q	¬Q	(P ∧ Q) ∨ ¬Q
T	T	T	F	T
T	F	F	T	T
F	T	F	F	F
F	F	F	T	T

Vậy (P ∧ Q) ∨ ¬Q là một tiếp liên vì nó không phải là hằng đúng và cũng không phải là hằng sai.

1.3.5. Mệnh đề hệ quả

Định nghĩa 12: 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.

Kí hiệu F |→ G hay F ⇒ G

Ví dụ 15: Cho F = (P → Q) ∧ (Q → R) và G = P → R. Xét xem G có phải là hệ quả của F không?

Lập bảng chân trị cho F → G như sau:

P	Q	R	P → Q	Q → R	F	G	F → G
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Nhìn vào bảng chân trị ta thấy F → G là hằng đúng. Vậy G là mệnh đề hệ quả của F.

Nhận xét: Nếu G là hệ quả của F thì khi F là đúng thì bắt buộc G phải đúng. Ngược lại, nếu G là đúng thì chưa có kết luận gì về chân trị của F.

1.3.6. Tương đương logic (logically equivalent)

Định nghĩa 13: Mệnh đề P và mệnh đề Q được gọi là tương đương logic nếu P↔Q là hằng đúng.

Định nghĩa 14: Hai mệnh đề P và Q được gọi là tương đương logic nếu và chỉ nếu chúng có cùng chân trị.

Mệnh đề P và Q tương đương logic được kí hiệu là P ⇔ Q (hay P ≡ Q)

Ví dụ 16: Cho F = P∨(Q∧R) và G = (P∨Q) ∧ (P∨R)

Xét xem hai mệnh đề trên là có tương đương logic không ?

Lập bảng chân trị như sau:

P	Q	R	Q∧R	F	P∨Q	P∨R	G	F↔G
T	T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T	T
T	F	T	F	T	T	T	T	T
T	F	F	F	T	F	T	F	T
F	T	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F	T
F	F	T	F	F	F	T	F	T
F	F	F	F	F	F	F	F	T

Nhìn vào bảng chân trị, ta thấy F↔G là hằng đúng. Vậy F ⇔ G.

Ví dụ 17: Cho F = P → Q và G = ¬ (P∨Q)

Xét xem hai mệnh đề trên là có tương đương logic không ? Tương tự như *Ví dụ 16* ta dễ thấy F và G là tương đương nhau.

Sau đây là Bảng các tương đương logic thường dùng:

Đặt T= hằng đúng, F = hằng sai.

Tương đương logic	**Tên luật**
P ∨ T ⇔ T	Domination law (luật nuốt)
P ∧ F ⇔ F	‘’
P ∧ T ⇔ P	Identity law (luật đồng nhất)
P ∨ F ⇔ P	‘’
P ∨ P ⇔ P	Idempotent law (luật luỹ đẳng)
P ∧ P ⇔ P	‘’
¬¬P ⇔ P	Double negation law (luật phủ định kép)
P ∨ ¬P ⇔ T	Cancellation law (luật xoá bỏ)
P ∧ ¬P ⇔ F	
P ∨ Q ⇔ Q ∨ P	Commutative law (luật giao hoán)

$P \wedge Q \Leftrightarrow Q \wedge P$	‘’
$P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$	Associative law (luật kết hợp)
$P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$	‘’
$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	Distributive law (luật phân phối)
$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	‘’
$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	De Morgan’s law (luật De Morgan)
$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	‘’
$P \rightarrow Q \Leftrightarrow \neg P \vee Q$	Implication law (luật kéo theo)
$P \vee (P \wedge Q) \Leftrightarrow P$	
$P \wedge (P \vee Q) \Leftrightarrow P$	

Ngoài cách chứng minh biểu thức logic bằng cách lập bảng chân trị, ta có thể sử dụng các tương đương logic để chứng minh.

Ví dụ 18: Không lập bảng chân trị, sử dụng các tương đương logic để chứng minh rằng $(P \wedge Q) \rightarrow Q$ là hằng đúng.

Ta có, $(P \wedge Q) \rightarrow Q = \neg(P \wedge Q) \vee Q$ (luật kéo theo)

$= (\neg P \vee \neg Q) \vee Q$ (luật De Morgan)

$= \neg P \vee (\neg Q \vee Q)$ luật kết hợp)

$= \neg P \vee T$ (luật xoá bỏ) $= T$ (luật đồng nhất)

Ví dụ 19: Chứng minh rằng $\neg (Q \rightarrow P) \vee (P \wedge Q) = Q$

Biến đổi tương đương vế trái như sau :

$\neg (Q \rightarrow P) \vee (P \wedge Q) = \neg(\neg Q \vee P) \vee (P \wedge Q)$ (luật kéo theo)

$= (\neg\neg Q \wedge \neg P) \vee (P \wedge Q)$ (luật De Morgan)

$= (Q \wedge \neg P) \vee (P \wedge Q)$ (luật phủ định kép)

$= Q \wedge (\neg P \vee P)$ (luật giao hoán, phân phối)

$= Q \wedge T$ (luật xoá bỏ)

$= Q$ (luật đồng nhất)

Sau đây ta đưa ra một số ví dụ áp dụng trong lập trình.

Ví dụ 20: Áp dụng trong lập trình

Giả sử trong chương trình có câu lệnh sau :

while (NOT((A[i]<>0) AND NOT(A[i]>= 10))) do

Ta có thể viết lại câu lệnh này một cách đơn giản hơn bằng cách sử dụng công thức De Morgan.

While (A[i]=0) OR (A[i]>= 10) do

Ví dụ 21: Giả sử trong chương trình có câu lệnh sau :

While ((i<size) AND (A[i]>10)) OR ((i<size) AND (A[i]<0)) OR NOT ((A[i]<> 0) AND NOT (A[i]>=10)) do

Trước hết chúng ta sẽ áp dụng công thức De Morgan để biến đổi biểu thức sau cùng như sau :

While ((i<size) AND ((A[i]>10)) OR ((i<size) AND (A[i]<0)) OR ((A[i]=0) OR (A[i]>= 10)) do

Sau đó, chúng ta lại sử dụng công thức về tính phân phối của phép hội đối với phép tuyển để rút gọn biểu thức phía trước. Ta có câu lệnh sau cùng là:

While ((i<size) AND ((A[i]>10) OR (A[i]<0))) OR ((A[i]=0) OR (A[i]>= 10)) do

1.4. Các ứng dụng của logic (everday logical)

Ngày nay, logic mệnh đề được ứng dụng nhiều trong các lĩnh vực khác nhau như:

- Viết
- Nói
- Tìm kiếm trên mạng (search engines)
- Toán học
- Các chương trình máy tính (logic in programming).

Do đó, hiểu biết các qui tắc để sử dụng logic là rất hữu ích. Sau đây là một vài ví dụ để chỉ ra các ứng dụng đó.

Ví dụ 22: Logic trong tìm kiếm trên mạng

Đặt vấn đề: Bạn muốn tìm tài liệu trên mạng có liên quan đến hai từ "**disc golf**". Nếu bạn gõ vào ô tìm kiếm hai từ "**disc golf**" này, bạn sẽ tìm thấy các tài liệu về **disc** và các tài liệu về **golf** nhưng không tìm thấy các các tài liệu về "**disc golf**".

Cách giải quyết : Bạn chỉ cần gõ vào ô tìm kiếm là "**disc AND golf**"

Ví dụ 23: Logic trong lập trình (Logic in programming)

Bạn muốn đặt điều kiện là nếu 0<x<10 hay x=10 thì tăng x lên 1 đơn vị.

if (0<x<10 OR x=10) then x:= x + 1;

Dựa vào qui tắc logic, có thể viết lại câu lệnh như sau:

if ((x>0) AND (x <= 10)) then x:= x + 1;

Ví dụ 24: Logic trong cách nói ở gia đình

Mẹ của bé An nói rằng : "Nếu con ngoan thì con có thể được ăn kem hoặc ăn bánh bông lan". Bé An hiểu rằng nếu nó ngoan thì nó sẽ được ăn kem và ăn bánh bông lan. Tuy nhiên, mẹ của bé An tức giận vì thật sự bà ta chỉ cho phép nó được ăn một trong hai thứ mà thôi.

Cách giải quyết là mẹ của bé An phải nói như thế này : "Nếu con ngoan thì con sẽ được ăn hoặc là kem hoặc là bánh bông lan nhưng không được ăn cả hai".

Ví dụ 25: Logic trong tính toán

Bạn có 3 lần kiểm tra trong lớp học. Nếu bạn đạt được 2 lần điểm A, hoặc chỉ một lần điểm A nhưng không được có một lần nào rớt trong 3 lần kiểm tra đó thì bạn sẽ đạt điểm A cho toàn khóa học. Bạn là người không được siêng năng lắm, vậy thì bạn sẽ chọn cách nào để đạt điểm A cho toàn khóa học?

Bởi vì điều kiện là OR nên cách giải quyết là bạn có thể đạt 2 điểm A và rớt lần 3, hay là chỉ cần đạt một điểm A và không rớt lần nào. Bạn sẽ lựa chọn đạt một điểm A và không rớt lần nào.

*Ví dụ 26***:** Logic trong đời sống

Sau khi nướng 1 chiếc bánh cho 2 đứa cháu trai và 2 đứa cháu gái đến thăm, Dì Nellie lấy bánh ra khỏi lò nướng và để nguội. Sau đó, cô rời khỏi nhà để đến đóng cửa hàng ở gần đó. Lúc trở về thì có ai đó đã ăn 1/4 chiếc bánh và thậm chí còn đặt lại cái dĩa dơ bên phần bánh còn lại. Vì không còn ai đến nhà Dì ngày hôm đó trừ 4 đứa cháu nên Dì biết ngay là 1 trong 4 đứa đã ăn mà chưa được cho phép. Dì Nellie bèn hỏi 4 đứa thì được các câu trả lời như sau:

- Charles : Kelly đã ăn phần bánh
- Dawn : Con không ăn bánh
- Kelly : Tyler ăn bánh
- Tyler : Con không ăn, Kelly nói chơi khi bảo rằng con ăn bánh.

Nếu chỉ 1 trong 4 câu trả lời trên là đúng và chỉ 1 trong 4 đứa cháu là thủ phạm, hãy tìm ra người mà Dì Nellie phải phạt?

Cách giải quyết : Vì chỉ 1 trong 4 câu trả lời trên là đúng nên chúng ta có thể dùng phép vét cạn để tìm lời giải.

- Giả sử Charles nói đúng nghĩa là Kelly ăn bánh. Ba câu còn lại là sai. Dawn nói Con không ăn bánh là sai nghĩa là Dawn có ăn bánh. Vậy có đến 2 người ăn bánh, điều này mâu thuẩn giả thiết, giả sử không được chấp thuận.

- Giả sử Dawn nói đúng nghĩa là Dawn không ăn bánh và 3 câu còn lại là sai. Nhận thấy có mâu thuẩn giữa Kelly và Tyler. Bởi vì Kelly nói "Tyler ăn bánh" là sai nghĩa là Tyler không ăn. Trong khi đó, Tyler lại nói rằng "Con không ăn... " là sai, vậy thực tế là nó có ăn. Giả thuyết này là không chấp nhận được.

- Giả sử Kelly nói đúng nghĩa là Tyler ăn bánh và 3 câu còn lại là sai. Như vậy, cũng có 2 thủ phạm là Kelly và Dawn. Mâu thuẩn giả thiết.

- Giả sử sau cùng là Tyler nói đúng nghĩa là nó không ăn bánh và 3 câu còn lại là sai. Nhận thấy chỉ có một người ăn bánh chính là Dawn. Vậy giả thuyết này là hợp lý và thủ phạm chính là Dawn.

Ví dụ 27: Logic trong toán học

Tìm số tự nhiên a biết rằng trong 3 mệnh đề dưới đây có 2 mệnh đề là đúng và 1 mệnh đề là sai.

1) a + 51 là số chính phương 2) Chữ số tận cùng của a là 1 3) a - 38 là số chính phương

Cách giải quyết: Trước hết, chúng ta sẽ phải xác định xem 2 mệnh đề đúng và 1 mệnh đề sai là mệnh đề nào? Sau đó từ 2 mệnh đề đúng để tìm ra số tự nhiên a. Số chính phương là số nguyên dương khi lấy căn bậc hai. Do đó, số chính phương có các chữ số tận cùng là 0, 1, 4, 5, 6, 9.

- Nhận thấy giữa mệnh đề 1 và 2 có mâu thuẩn. Bởi vì, giả sử 2 mệnh đề này đồng thời là đúng thì a+51 có chữ số tận cùng là 2 nên không thể là số chính phương. Vậy trong 2 mệnh đề này phải có 1 mệnh đề là đúng và 1 là sai.
- Tương tự, nhận thấy giữa mệnh đề 2 và 3 cũng có mâu thuẩn. Bởi vì, giả sử mệnh đề này đồng thời là đúng thì a-38 có chữ số tận cùng là 3 nên không thể là số chính phương.

Vậy trong 3 mệnh đề trên thì mệnh đề 1 và 3 là đúng, còn mệnh đề 2 là sai.

Với $x > 0$ và $y > 0$. Đặt:

$a + 51 = x^2$ và $a - 38 = y^2$

Suy ra $89 = 1.89 = x^2 - y^2 = (x + y)(x - y)$

Từ đó ta có:

$x + y = 1$ (loại vì x, y là nguyên dương nên không thể có $x+y = 1$) và $x - y = 89$.

Hay $x + y = 89$ và $x - y = 1$

Giải hệ phuơng trình này ta được $x = 45$ và $y = 44$. Vậy $a = 1974$.

Trên đây là vài ví dụ đơn giản. Hy vọng rằng các ví dụ này cho chúng ta thấy được sự quan trọng của logic không chỉ trong toán học, khoa học máy tính mà còn trong cuộc sống hàng ngày.

CÂU HỎI VÀ BÀI TẬP

1. a) Nếu biết mệnh đề P→Q là sai, hãy cho biết chân trị của các mệnh đề sau:

$$P \wedge Q ; \quad \neg P \vee Q ; \quad Q \rightarrow P$$

b) Cho các biểu thức mệnh đề:

$$((P \wedge Q) \wedge R) \rightarrow (S \vee M)$$

$$(P \wedge (Q \wedge R)) \rightarrow (S \oplus M)$$

Xác định chân trị của các biến mệnh đề P, Q, R, S, M nếu các biểu thức mệnh đề trên là sai.

2. Nếu Q có chân trị là T, hãy xác định chân trị của các biến mệnh đề P, R, S nếu biểu thức mệnh đề sau cũng là đúng

$$(Q \rightarrow ((\neg P \vee R) \wedge \neg S)) \wedge (\neg S \rightarrow (\neg R \wedge Q))$$

3. Cho đoạn chương trình sau:

a) if n>5 then n:=n+2 ;

b) if ((n+2 = 8) or (n-3=6)) then n:= 2*n + 1;

c) if ((n-3=16) and (n div 5=1)) then n:= n + 3;

d) if ((n<>21) and (n-7=15)) then n:= n - 4 ;

e) if ((n div 5 = 2) or (n+1=20)) then n:=n+1 ;

Ban đầu biến nguyên n được gán trị là 7. Hãy xác định giá trị n trong các trường hợp sau:

- Sau mỗi câu lệnh (nghĩa là khi qua câu lệnh mới thì gán lại n = 7)
- Sau tất cả các lệnh (sử dụng kết quả của câu lệnh trước để tính toán cho câu sau).

4. Cho đoạn chương trình sau :

a) if (n-m = 5) then n:= n-2 ;

b) if ((2*m=n) and (n div 4 = 1)) then n:= 4*m - 3 ;

c) if ((n<8) or (m div 2=2)) then n:= 2*m else m:= 2*n ;

d) if ((n<20) and (n div 6 =1)) then m:= m-n-5 ;

e) if ((n= 2*m) or (n div 2= 5)) then m:= m+2 ;

f) if ((n div 3 = 3) and (m div 3 <>1)) then m:= n ;

g) if (m*n <> 35) then n:= 3*m+7 ;

Ban đầu biến nguyên n = 8 và m = 3. Hãy xác định giá trị của m, n trong các trường hợp sau:

- Sau mỗi câu lệnh (nghĩa là khi qua câu lệnh mới thì gán lại n = 8 và m = 3)
- Sau tất cả các lệnh (sử dụng kết quả của câu lệnh trước để tính toán cho câu sau)

5. Vòng lặp Repeat ... Until trong một đoạn chương trình Pascal như sau:

```
Repeat
    <lệnh>
Until ((x<>0) and (y>0)) or ( not ((w>0) and (t=3)));
```

Với mỗi cách gán giá trị biến như sau, hãy xác định trong trường hợp nào thì vòng lặp kết thúc.

a) x= 7, y= 2, w= 5, t= 3

b) x= 0, y= 2, w= -3, t= 3

c) x= 0, y= -1, w= 1, t= 3

d) x= 1, y= -1, w= 1, t= 3

6. Trong một phiên tòa xử án 3 bị can có liên quan đến vấn đề tài chánh, trước tòa cả 3 bị cáo đều tuyên thệ khai đúng sự thật và lời khai như sau:

Anh A: Chị B có tội và anh C vô tội

Chị B : Nếu anh A có tội thì anh C cũng có tội

Anh C: Tôi vô tội nhưng một trong hai người kia là có tội

Hãy xét xem ai là người có tội ?

7. Cho các mệnh đề được phát biểu như sau, hãy tìm số lớn nhất các mệnh đề đồng thời là đúng.

a) Quang là người khôn khéo

b) Quang không gặp may mắn

c) Quang gặp may mắn nhưng không khôn khéo

d) Nếu Quang là người khôn khéo thì nó không gặp may mắn

e) Quang là người khôn khéo khi và chỉ khi nó gặp may mắn

f) Hoặc Quang là người khôn khéo, hoặc nó gặp may mắn nhưng không đồng thời cả hai.

8. Cho a và b là hai số nguyên dương. Biết rằng, trong 4 mệnh đề sau đây có 3 mệnh đề đúng và 1 mệnh đề sai. Hãy tìm mọi cặp số (a, b) có thể có.

a) a+1 chia hết cho b

b) a = 2b + 5

c) a+b chia hết cho 3

d) a+7b là số nguyên tố

9. Không lập bảng chân trị, sử dụng các công thức tương đương logic, chứng minh rằng các biểu thức mệnh đề sau là hằng đúng

a) $(P \wedge Q) \rightarrow P$

b) $P \rightarrow (\neg P \rightarrow P)$

c) $P \rightarrow (Q \rightarrow (P \wedge Q))$

d) $\neg (P \vee \neg Q) \rightarrow \neg P$

e) $((P \rightarrow Q) \wedge (Q \rightarrow R)) \rightarrow (P \rightarrow R)$

10. Không lập bảng chân trị, sử dụng các công thức tương đương logic, xét xem biểu thức mệnh đề G có là hệ quả của F không ?

a) $F = P \wedge (Q \vee R)$ và $G = (P \wedge Q) \vee R$

b) $F = (P \rightarrow Q) \wedge (Q \rightarrow R)$ và $G = P \rightarrow (Q \rightarrow R)$

c) $F = P \wedge Q$ và $G = (\neg P \rightarrow Q) \vee (P \rightarrow \neg Q)$

11. Tương tự bài tập 9 và 10, chứng minh các tương đương logic sau đây:

a) $(P \vee Q) \wedge \neg (\neg P \wedge Q) \Leftrightarrow P$

b) $\neg(\neg((P \vee Q) \wedge R) \vee \neg Q) \Leftrightarrow Q \wedge R$

c) $((P \vee Q) \wedge (P \vee \neg Q)) \vee Q \Leftrightarrow P \vee Q$

d) $\neg(P \vee Q) \vee ((\neg P \wedge Q) \vee \neg Q) \Leftrightarrow \neg(Q \wedge P)$

e) $(P \rightarrow Q) \wedge (\neg Q \wedge (R \vee \neg Q)) \Leftrightarrow \neg (Q \vee P)$

f) $P \vee (P \wedge (P \vee Q) \Leftrightarrow P$

g) $P \vee Q \vee (\neg P \wedge \neg Q \wedge R) \Leftrightarrow P \vee Q \vee R$

h) $((\neg P \vee \neg Q) \rightarrow (P \wedge Q \wedge R) \Leftrightarrow P \wedge Q$

i) $P \wedge ((\neg Q \rightarrow (R \wedge R)) \vee \neg (Q \vee (R \wedge S) \vee (R \wedge \neg S))) \Leftrightarrow P$

j) $(P \vee Q \vee R) \wedge (P \vee S \vee \neg Q) \wedge (P \vee \neg S \vee R) \Leftrightarrow P \vee (R \wedge (S \vee \neg Q)$

II. SUY LUẬN TOÁN HỌC VÀ CÁC PHƯƠNG PHÁP CHỨNG MINH

Học xong mục này, sinh viên phải nắm bắt được các vấn đề sau:

- Khái niệm về suy luận toán học
- Các phương pháp chứng minh và biết vận dụng các phương pháp này để chứng minh một bài toán cụ thể.

2.1. Suy luận toán học

2.1.1. Khái niệm

Suy luận được xem là một trong những nền tảng xây dựng nên các ngành khoa học tự nhiên. Từ xưa đến nay, nhờ suy luận mà người ta có thể nhận thức được cái chưa biết từ những cái đã biết. Suy luận còn là cơ sở của sự sáng tạo. Từ các phán đoán, đưa đến các chứng minh để chấp nhận hay bác bỏ một vấn đề nào đó.

Suy luận toán học dựa trên nền tảng của các phép toán mệnh đề, chủ yếu là phép kéo theo. Để chứng minh một vấn đề nào đó, thông thường người ta phải xác định điểm ban đầu (có thể gọi là giả thiết) và điểm kết thúc (gọi là kết luận). Quá trình đi từ giả thiết đến kết luận gọi là quá trình chứng minh và quá trình này đươc thực hiện bằng cách nào đó thì gọi đó là phương pháp chứng minh.

Các phương pháp chứng minh là rất quan trọng vì không những chúng thường được sử dụng trong toán học mà còn được áp dụng nhiều trong tin học. Ví dụ, sự kiểm tra tính đúng đắn của một chương trình, của một hệ điều hành, xây dựng các luật suy diễn trong lĩnh vực trí tuệ nhân tạo... Do đó, chúng ta cần phải nắm vững các phương pháp chứng minh.

Tuy nhiên, có những phương pháp chứng minh đúng vì nó được dựa trên cơ sở của một mệnh đề đúng (hằng đúng) và có những phương pháp chứng minh sai. Các phương pháp chứng minh sai này là cố ý hoặc vô ý. Khi phương pháp chứng minh dựa trên một hằng sai thì sẽ mang lại kết quả sai nhưng người ta vẫn cho là đúng thì được gọi là cố ý. Đôi khi có những phương pháp chứng minh dựa trên một tiếp liên (có khi mệnh đề là đúng nhưng cũng có lúc sai) mà người ta tưởng lầm là hằng đúng nên cho là kết quả bao giờ cũng đúng thì trường hợp này gọi là vô ý (hay ngộ nhận).

Sau đây, chúng ta sẽ đi tìm hiểu các qui tắc suy luận.

2.1.2. Các qui tắc suy luận

Như đã giới thiệu ở trên, những suy luận có dùng các qui tắc suy diễn gọi là suy luận có cơ sở. Khi tất cả các suy luận có cơ sở là đúng thì sẽ dẫn đến một kết luận đúng. Một suy luận có cơ sở có thể dẫn đến một kết luận sai nếu một trong các mệnh đề đã dùng trong suy diễn là sai. Sau đây là bảng các qui tắc suy luận đúng.

Quy tắc	**Hằng đúng**	**Tên luật**
$\frac{P}{\therefore P \vee Q}$	$P \rightarrow (P \vee Q)$	Thêm vào tuyển
$\frac{P \wedge Q}{\therefore P}$	$(P \wedge Q) \rightarrow P$	Rút gọn
$\frac{P, P \rightarrow Q}{\therefore Q}$	$[P \wedge (P \rightarrow Q)] \rightarrow Q$	Modus Ponens
$\frac{\neg Q, P \rightarrow Q}{\therefore \neg P}$	$[\neg Q \wedge (P \rightarrow Q)] \rightarrow \neg P$	Modus Tollens
$\frac{P \rightarrow Q, Q \rightarrow R}{\therefore P \rightarrow R}$	$[(P \rightarrow Q) \wedge (Q \rightarrow R)] \rightarrow (P \rightarrow R)$	Tam đoạn luận giả định
$\frac{\neg P, P \vee Q}{\therefore Q}$	$[\neg P \wedge (P \vee Q)] \rightarrow Q$	Tam đoạn luận tuyển

Trong các phân số của qui tắc thì các giả thiết được viết trên tử số,

kết luận được viết dưới mẫu số. Kí hiệu ∴ có nghĩa là "vậy thì", "do đó",...

Ví dụ 1: Qui tắc suy luận nào là cơ sở của suy diễn sau :

"Nếu hôm nay trời mưa thì cô ta không đến, nếu cô ta không đến thì ngày mai cô ta đến. Vậy thì, nếu hôm nay trời mưa thì ngày mai cô ta đến."

Đây là suy diễn dựa trên qui tắc tam đoạn luận giả định.

"Nếu hôm nay tuyết rơi thì trường đại học đóng cửa. Hôm nay trường đại học không đóng cửa. Do đó, hôm nay đã không có tuyết rơi."

Đây là suy diễn dựa trên qui tắc Modus Tollens

"Alice giỏi toán. Do đó, Alice giỏi toán hoặc tin."

Đây là suy diễn dựa trên qui tắc cộng.

Ngụy biện

Các phương pháp chứng minh sai còn được gọi là ngụy biện. Ngụy biện giống như qui tắc suy luận nhưng không dựa trên một hằng đúng mà chỉ là một tiếp liên. Đây chính là sự khác nhau cơ bản giữa suy luận đúng và suy luận sai. Loại suy luận sai này được gọi là ***ngộ nhận kết luận.***

Ví dụ 2: Xét xem suy diễn sau là có cơ sở đúng không?

"Nếu bạn đã giải hết bài tập trong sách toán rời rạc này thì bạn nắm vững logic. Bạn nắm vững logic vậy thì bạn đã giải hết bài tập trong sách toán rời rạc 2 này".

Nhận thấy suy diễn này là dựa trên mệnh đề :

$$((P \rightarrow Q) \wedge Q) \rightarrow P$$

Trong đó:

P = "Bạn đã giải hết bài tập trong sách toán rời rạc"

Q = "Bạn nắm vững logic"

Mệnh đề $((P \rightarrow Q) \wedge Q) \rightarrow P$ không phải là hằng đúng vì nó sẽ sai khi P là F và Q là T. Do đó, suy diễn này không hoàn toàn có cơ sở đúng. Bởi vì, khi Q là T nghĩa là bạn đã nắm vững logic nhưng không chắc là bạn đã giải hết bài tập trong sách toán rời rạc này mà có thể giải sách khác (P là F).

2.2. Các phương pháp chứng minh

Như đã giới thiệu trong phần trên, mỗi bài toán cần chứng minh thông thường đều có hai phần chính là giả thiết và kết luận. Việc chỉ ra được cái nào là giả thiết, cái nào là kết luận sẽ giúp cho việc chứng minh dễ dàng hơn thông qua việc sử dụng phương pháp chứng minh thích hợp. Do đó, các phương pháp chứng minh trong dạng bài toán này là có liên quan đến mệnh đề kéo theo.

Vậy, trước khi tìm hiểu các phương pháp chứng minh, chúng ta hãy xem lại bảng chân trị của mệnh đề P kéo theo Q (với P là giả thiết và Q là kết luận). Các trường hợp để cho mệnh đề P kéo theo Q là đúng cũng chính là các phương pháp để chứng minh bài toán đúng.

Nhận thấy rằng, P→Q là đúng có 3 trường hợp. Các trường hợp này chính là các phương pháp chứng minh sẽ được trình bày dưới đây.

Trước khi đi vào các phương pháp chứng minh, có một khái niệm mà chúng ta cần tìm hiểu, đó là khái niệm về "**hàm mệnh đề**".

2.2.1. Hàm mệnh đề

Cho A là một tập hợp không rỗng sao cho ứng với mỗi x∈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∈A. Như vậy, khi nói ứng với mỗi x∈A, ta có một mệnh đề P(x), nghĩa là khi đó tính đúng sai của P(x) được hoàn toàn xác định phụ thuộc vào từng giá trị của x∈A.

Ví dụ 3: Cho hàm mệnh đề

P(x) = { x là số lẻ, x∈N}

Ta có : P(1) là mệnh đề đúng

P(2) là mệnh đề sai.

Tổng quát, với các tập hợp không rỗng A_1, A_2, ..., A_n, sao cho ứng với mỗi $x_1 \in A_1$, $x_2 \in A_2$, ..., $x_n \in A_n$, ta có một mệnh đề, ký hiệu $P(x_1, x_2, ..., x_n)$. Ta nói $P(x_1, x_2, ..., x_n)$ là một hàm mệnh đề theo n biến x.

Ví dụ 4: Cho hàm mệnh đề

P(x,y,z) = { 2x + y - z = 0, x, y, z∈Z}

Ta thấy P(x,y,z) là mệnh đề đúng khi x = 1, y = -1, z = 1, tức P(1,-1,1) đúng.

P(x,y,z) là mệnh đề sai khi x = 1, y = 1, z = 1, tức P(1,1,1) sai.

2.2.2. Chứng minh rỗng

Như đã biết mệnh đề P→Q chỉ sai khi P đúng và Q sai. Vậy, để chứng minh mệnh đề P→Q là đúng, người ta chỉ cần chứng minh rằng P là sai. Phương pháp chứng minh này được gọi là chứng minh rỗng.

Phương pháp chứng minh rỗng thường được sử dụng để chứng minh các trường hợp đặc biệt của định lý. Trường hợp tổng quát thì định lý này luôn đúng với mọi số n nguyên dương.

Ví dụ 5: Cho hàm mệnh đề P(n) = "Nếu n>1 thì n^2 >n " Chứng minh rằng P(1) là đúng.

Giải: Ta có P(1) = { Nếu 1 >1 thì 1^2 >1}

Nhận thấy rằng giả thiết 1>1 là sai, bất chấp kết luận 1^2 >1 là đúng hay sai thì P(1) là đúng.

2.2.3. Chứng minh tầm thường

Theo qui tắc đã nêu nếu Q đúng thì mệnh đề P→Q luôn đúng. Vậy, để chứng minh mệnh đề P→Q là đúng, người ta chỉ cần chứng minh rằng Q là đúng. Phương pháp chứng minh này được gọi là chứng minh tầm thường.

Phương pháp chứng minh tầm thường cũng được sử dụng để chứng minh các trường hợp đặc biệt của định lý. Trường hợp tổng quát thì định lý này luôn đúng với mọi số n nguyên dương.

Ví dụ 6: Cho hàm mệnh đề

P(n) = "Nếu a và b là 2 số nguyên dương và a ≥ b thì $a^n \geq b^n$". Chứng minh rằng P(0) là đúng.

Giải: Ta có $a^0 = b^0 = 1$. Do đó $a^0 \geq b^0$ là đúng.

Vậy P(0) là đúng bất chấp giả thiết a ≥ b là đúng hay sai.

2.2.4. Chứng minh trực tiếp

Theo qui tắc suy luận nếu P đúng và P→Q đúng thì Q phải đúng. Phương pháp chứng minh Q đúng dựa vào qui tắc này gọi là chứng minh trực tiếp.

Vậy để thực hiện phương pháp chứng minh trực tiếp, người ta giả sử rằng P là đúng, sau đó sử dụng các qui tắc suy luận hay các định lý để chỉ ra rằng Q là đúng và kết luận P→Q là đúng.

Ví dụ 7: Chứng minh rằng "Nếu n là số lẻ thì n^2 là số lẻ".

Giải: Giả sử rằng giả thiết của định lý này là đúng, tức là n là số lẻ.

Ta có n = 2k + 1 (k=0,1,2,...)

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

$= 2(2k^2 + 2k) + 1$ là lẻ. Vậy nếu n là số lẻ thì n^2 là số lẻ.

Ví dụ 8: Cho hàm mệnh đề P(n) = "Nếu n>1 thì n^2 >n". Chứng minh rằng P(n) là đúng với n là số nguyên dương.

Giải: Giả sử n > 1 là đúng, ta có : $n = 1 + k$ ($k \geq 1$) $\Rightarrow n^2 = (1 + k)^2$

$= 1 + 2k + k^2 = (1 + k) + k + k^2 > n$. Vậy nếu n > 1 thì $n^2 > n$.

2.2.5. Chứng minh gián tiếp

Vì mệnh đề P→Q ⇔ ¬Q → ¬P. Do đó, để chứng minh mệnh đề P→Q là đúng, người ta có thể chỉ ra rằng mệnh đề ¬Q → ¬P là đúng.

Ví dụ 9: Chứng minh định lý "Nếu 3n + 2 là số lẻ thì n là số lẻ".

Giải: Giả sử ngược lại kết luận của phép kéo theo là sai, tức n là chẵn.

Ta có n = 2k, (k∈N)

$\Rightarrow$ 3n + 2 = 3.2k + 2 = 2(3k + 1) là số chẵn

$\Rightarrow$ Nếu 3n + 2 là số lẻ thì n là số lẻ.

Nhận xét

• Có những bài toán có thể sử dụng phương pháp chứng minh trực tiếp hay gián tiếp đều được cả. Tuy nhiên, có những bài toán không thể sử dụng phương pháp chứng minh trực tiếp được hoặc sử dụng trực tiếp thì bài giải sẽ dài dòng phức tạp hơn là sử dụng chứng minh gián tiếp (hoặc ngược

lại). Khi chứng minh ta cần lựa chọn phương pháp chứng minh thích hợp với từng bài toán cụ thể.

• Để chứng minh mệnh đề có dạng : $(P_1 \vee P_2 \vee ... \vee P_n) \rightarrow Q$

Chúng ta có thể sử dụng mệnh đề tương đương:

$((P_1 \vee P_2 \vee ... \vee P_n) \rightarrow Q) \Leftrightarrow ((P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q) \wedge .... \wedge (P_n \rightarrow Q))$. Cách chứng minh này gọi là chứng minh từng trường hợp.

Ví dụ 10: Chứng minh rằng:

"Nếu n không chia hết cho 3 thì n^2 không chia hết cho 3".

Giải: Gọi P là mệnh đề "n không chia hết cho 3" và Q là mệnh đề "n^2 không chia hết cho 3". Khi đó, P tương đương với $P_1 \vee P_2$. Trong đó:

P_1 = "n mod 3 =1", P_2 = "n mod 3 =2"

Vậy, để chứng minh $P \rightarrow Q$ là đúng, tương đương với việc chứng minh $(P_1 \vee P_2) \rightarrow Q$ hay chứng minh $(P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q)$.

Giả sử P_1 là đúng. Ta có, n mod 3 = 1. Đặt n = 3k + 1 (k là số nguyên nào đó).

Suy ra:

$n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$ không chia hết cho 3.

Do đó, $P_1 \rightarrow Q$ là đúng.

Tương tự, giả sử P_2 là đúng. Ta có, n mod 3 = 2. Đặt n = 3k + 2 (k là số nguyên nào đó).

Suy ra $n^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$ không chia hết cho 3.

Do đó, $P_2 \rightarrow Q$ là đúng.

Do $P_1 \rightarrow Q$ là đúng và $P_2 \rightarrow Q$ là đúng, hay là $(P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q)$ đúng. Vậy $(P_1 \vee P_2) \rightarrow Q$.

2.2.6. Chứng minh phản chứng

Chứng minh phản chứng thường được sử dụng để chứng minh mệnh đề P là đúng. Trước hết, người ta giả sử ngược lại rằng P là sai hay $\neg P$ là đúng. Từ mệnh đề $\neg P$ là đúng dẫn đến kết luận Q sao cho $\neg P \rightarrow Q$ phải đúng.

Khi đó, người ta chỉ ra rằng Q là một mâu thuẩn, nghĩa là :

Q = R ∧¬R. (Sở dĩ có mâu thuẫn này là do ta giả sử P là sai). Vì ¬P→Q phải đúng và Q là F, suy ra rằng ¬P = F ⇒ P = T.

Phương pháp chứng minh phản chứng thường được sử dụng để chứng minh những vấn đề cơ bản và điều quan trọng trong kỹ thuật này là tìm ra được mâu thuẩn R∧¬R.

Ví dụ 11: "Chứng minh $\sqrt{2}$ là số vô tỉ".

Giải: Gọi P là mệnh đề "$\sqrt{2}$ là số vô tỉ". Giả sử ngược lại ¬P là đúng. Vậy, $\sqrt{2}$ là số hữu tỉ (vì tập số thực gồm 2 tập con là tập số vô tỉ và tập số hữu tỉ. Hai tập con này là rời nhau). Khi đó ∃a,b (a, b ∈ N) sao cho:

$\sqrt{2} = \frac{a}{b}$ ($\frac{a}{b}$ là phân số tối giản (mệnh đề R)). Suy ra $2b^2 = a^2 \Rightarrow a^2$ là số chẵn ⇒ a là số chẵn ⇒ đặt a = 2c, tương tự cũng chứng minh được b là số chẵn. Vậy a, b đều có ước chung là 2, nghĩa là phân số $\frac{a}{b}$ không tối giản (¬R). Điều này mâu thuẫn. Vậy $\sqrt{2}$ là số vô tỉ.

Ví dụ 12: Một trong những cách giải bài toán tồn tại là dùng lập luận phản chứng.

Cho 7 đoạn thẳng có độ dài lớn hơn 10 và nhỏ hơn 100. Chứng minh rằng luôn tìm được 3 đoạn để có thể ghép thành một tam giác.

Giải: Trước hết sắp xếp các đoạn đã cho theo thứ tự tăng dần của độ dài $a_1, a_2, ..., a_7$, và chứng minh rằng trong dãy đã xếp luôn tìm được 3 đoạn liên tiếp sao cho tổng của 2 đoạn đầu lớn hơn đoạn cuối (vì điều kiện để 3 đoạn có thể ghép thành một tam giác là tổng của 2 đoạn nhỏ hơn đoạn thứ ba).

Giả sử điều cần chứng minh là không xảy ra, nghĩa là đồng thời xảy ra các bất đẳng thức sau: bất đẳng thức sau:

$a_1 + a_2 \leq a_3$

$a_2 + a_3 \leq a_4$

$a_3 + a_4 \leq a_5$

$a_4 + a_5 \leq a_6$

$a_5 + a_6 \leq a_7$

Từ giả thiết a_1 , a_2 có giá trị lớn hơn 10, ta nhận được $a_3 > 20$. Từ $a_2 > 10$ và $a_3 > 20$ ta nhận được $a_4 > 30$. Tương tự ta suy ta được $a_5 > 50$, $a_6 > 80$, $a_7 > 140$.

Theo giả thiết các độ dài nhỏ hơn 100. Có mâu thuẩn này là do giả sử điều cần chứng minh không xảy ra.

Vậy, luôn tồn tại 3 đoạn liên tiếp sao cho tổng của 2 đoạn đầu lớn hơn đoạn cuối. Hay nói cách khác là 3 đoạn này có thể ghép thành một tam giác.

2.2.7. Chứng minh qui nạp

Giả sử cần tính tổng n số nguyên lẻ đầu tiên. Với n = 1, 2, 3, 4, 5 ta có :

n = 1: $1 = 1 = 1^2$

n = 2: $1 + 3 = 4 = 2^2$

n = 3: $1 + 3 + 5 = 9 = 3^2$

n = 4: $1 + 3 + 5 + 7 = 16 = 4^2$

n = 5: $1 + 3 + 5 + 7 + 9 = 25 = 5^2$

Từ các kết quả này ta dự đoán tổng n số nguyên lẻ đầu tiên là n^2. Tuy nhiên, chúng ta cần có phương pháp chứng minh dự đoán trên là đúng.

Qui nạp toán học là một kỹ thuật chứng minh rất quan trọng. Người ta dùng nó để chứng minh những kết quả đã có dựa trên sự suy luận nào đó như ví dụ trên. Tuy nhiên, qui nạp toán học chỉ dùng để chứng minh các kết quả nhận được bằng một cách nào đó chứ không là công cụ để phát hiện ra công thức.

a) Nguyên lý chứng minh qui nạp yếu :

Nhiều định lý phát biểu rằng P(n) là đúng ∀n nguyên dương, trong đó P(n) là hàm mệnh đề, ký hiệu ∀nP(n). Qui nạp toán học là một kỹ thuật chứng minh các định lý thuộc dạng trên. Nói cách khác qui nạp toán học

thường sử dụng để chứng minh các mệnh đề dạng ∀nP(n).

Nguyên lý chứng minh qui nạp yếu bao gồm 2 bước :

- Kiểm tra $P(x_0)$ là đúng với x_0 là giá trị đầu tiên của dãy số n
- Giả sử rằng P(k) là đúng khi n=k. Từ đó suy ra rằng P(k+1) là đúng.

Ta có cách viết của suy luận trên như sau:

$[P(x_0) \wedge (P(k) \rightarrow P(k+1))] \rightarrow \forall n P(n)$

Ví dụ 13: Chứng minh rằng $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ với n nguyên dương.

Giải: Đặt P(n) = $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Với n = 1, dễ nhận thấy P(1) đúng.

Giả sử P(k) đúng với k ≥ 1, nghĩa là $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

Ta chứng minh P(k+1) cũng đúng, nghĩa là $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$

Thật vậy, $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$

Khi sử dụng nguyên lý chứng minh qui nạp, không được bỏ qua bước kiểm tra $P(x_0)$ là đúng vì nếu chỉ có (P(n)→P(n+1)) là không đủ để kết luận rằng ∀nP(n) là đúng.

b) Nguyên lý chứng minh qui nạp mạnh:

Cho P(n) là một đẳng thức có chứa biến n, nếu P(0) là đúng và nếu $(P(x_0) \wedge P(x_0+1) \wedge \ldots \wedge P(k)) \rightarrow P(k+1)$ là đúng thì P(n) là mệnh đề đúng ∀n.

Chú ý rằng, để tạo ra giả thiết qui nạp với nguyên tắc qui nạp yếu, người ta chỉ giả thiết rằng P(k) là đúng tại n=k. Với nguyên tắc qui nạp mạnh, người ta chỉ ra rằng giả thiết đúng cho tất cả các mệnh đề $(P(x_0) \wedge P(x_0+1) \wedge \ldots \wedge P(k))$. *Đây chính là sự khác biệt cơ bản của 2 nguyên tắc qui nạp với giả thiết yếu và giả thiết mạnh.*

Ví dụ 14: Chứng minh rằng tích của 3 số liên tiếp luôn chia hết cho 6.

Giải: Đặt P(n) = "n.(n+1).(n+2) chia hết cho 6", n nguyên dương.

Ta có: P(1) = 1.2.3 chia hết cho 6 $\Rightarrow$ P(1) đúng.

P(2) = 2.3.4 chia hết cho 6 $\Rightarrow$ P(2) đúng.

P(3) = 3.4.5 chia hết cho 6 $\Rightarrow$ P(3) đúng.

Giả sử $\forall n \leq k$ ta có P(k) là đúng. Nghĩa là k(k+1)(k+2) chia hết cho 6.

Ta cần chứng minh P(k+1) đúng.

Thật vậy, (k+1)(k+2)(k+3) = k.(k+1).(k+2) + 3.(k+1).(k+2), mà k.(k+1).(k+2) chia hết cho 6 (P(k) đúng). Vậy P(k+1) đúng.

Ví dụ 15: Chứng minh rằng mọi bưu phí bằng hay lớn hơn 12 xu đều có thể tạo ra bằng các con tem 4 xu hay 5 xu.

Giải : Đặt P(n) = { n = 4 + ...+ 5+....}

Ta có : P(12) = { 12 = 4 + 4 + 4}

P(13) = { 13 = 4 + 4 + 5}

P(14) = { 14 = 4 + 5 + 5}

P(15) = { 15 = 5+ 5 + 5}

P(16) = { 16 = 4 + 4 + 4 + 4 }

P(17) = { 17 = 4 + 4 + 4 + 5 }

Giả sử n > 15 và P(n) là đúng. Nhận thấy rằng để tạo ra bưu phí (n+1) xu ta chỉ cần dùng con tem n-3 xu và cộng thêm một tem 4 xu.

CÂU HỎI VÀ BÀI TẬP

1. Quy tắc suy luận nào được dùng trong mỗi lập luận:

a) Những con kanguroo sống ở Australia là loài thú có túi. Do đó, kanguroo là loài thú có túi.

b) Hoặc hôm nay trời nóng trên 100 độ hoặc là sự ô nhiễm là nguy hại. Hôm nay nhiệt độ ngoài trời thấp hơn 100 độ. Do đó, ô nhiễm là nguy hại.

c) Steve sẽ làm việc ở một công ty tin học vào mùa hè này. Do đó, mùa hè này anh ta sẽ làm việc ở một công ty tin học hoặc là một kẻ lang

thang ngoài bể bơi.

d) Nếu tôi làm bài tập này cả đêm thì tôi có thể trả lời được tất cả bài tập. Nếu tôi trả lời được tất cả bài tập thì tôi sẽ hiểu được tài liệu này. Do đó, nếu tôi làm bài tập này cả đêm thì tôi sẽ hiểu được tài liệu này

2. Xác định xem các suy luận sau là có cơ sở không. Nếu một suy luận là có cơ sở thì nó dùng qui tắc suy luận nào. Nếu không hãy chỉ ra ngụy biện nào đã được sử dụng.

a) Nếu n là một số thực lớn hơn 1, khi đó $n^2 > 1$. Giả sử $n^2 > 1$. Khi đó $n > 1$.

b) Nếu n là một số thực và $n > 3$, khi đó $n^2 > 9$. Giả sử $n^2 \leq 9$. Khi đó, $n \leq 3$.

c) Một số nguyên dương hoặc là số chính phương hoặc có một số chẵn các ước nguyên dương. Giả sử, n là một số nguyên dương có một số lẻ các ước nguyên dương. Khi đó, n là số chính phương.

3. Chứng minh rằng bình phương của một số chẵn là một số chẵn bằng:

a) Chứng minh trực tiếp.

b) Chứng minh gián tiếp.

c) Chứng minh phản chứng .

4. Chứng minh rằng tích của 2 số hữu tỷ là một số hữu tỷ.

5. Chứng minh rằng một số nguyên không chia hết cho 5 thì bình phương của nó khi chia cho 5 sẽ dư 1 hoặc 4.

6. Chứng minh rằng nếu n là số nguyên dương khi đó n là lẻ nếu và chỉ nếu $5n + 6$ là lẻ.

7. Có 2 giả thiết

- Môn logic là khó hoặc không có nhiều sinh viên thích môn logic.
- Nếu môn toán là dễ thi logic là không khó.

Bằng cách chuyển các giả thiết trên thành các mệnh đề chứa các biến và các toán tử logic. Hãy xác định xem mỗi một trong các khẳng định sau là các kết luận có cơ sở của các giả thiết đã cho không ?

a) Môn toán là không dễ nếu nhiều sinh viên thích môn logic.

b) Không có nhiều sinh viên thích môn logic nếu môn toán là không dễ.

c) Môn toán là dễ hoặc môn logic là khó.

d) Môn logic là không khó hoặc môn toán là không dễ.

e) Nếu không có nhiều sinh viên thích môn logic khi đó hoặc là môn toán không dễ hoặc là logic không khó.

8. Dùng nguyên lý qui nạp yếu, chứng minh các đẳng thức :

a) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ với n nguyên dương.

b) $\sum_{i=1}^{n} i(i+1)(i+2) = \frac{n(n+1)(n+2)(n+3)}{4}$ với n nguyên dương.

c) $\sum i(i)!= (n+1)!- 1$

d) $\sum_{i=1}^{n} \frac{i}{i+1} = 1 - \frac{1}{(n+1)!}$ với n nguyên dương.

e) $\sum_{i=1}^{n} \frac{1}{(i+1)(i+2)} = \frac{n(n+3)}{4(n+1)(n+2)}$ với n nguyên dương.

f) $\sum_{i=1}^{n} i.2^i = 2 + (n-1).2^{n+1}$ với n nguyên dương.

g) $\sum_{i=1}^{n} 2.3^{i-1} = 3^n - 1$ với n nguyên dương.

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

9. Dùng nguyên lý qui nạp mạnh, chứng minh các bất đẳng thức sau:

a) $\forall n > 3 : 2^n < n!$

b) $\forall n > 4 : n^2 < 2^n$

c) $\forall n > 9 : n^2 < 2^n$

d) $\forall n >= 6 : 4n < n^2 - 7$

e) $\forall n > 10 : n - 2 < (n^2 - n)/12$

III. VỊ TỪ VÀ LƯỢNG TỪ

Học xong mục này, sinh viên phải nắm bắt được các vấn đề sau:

- Thế nào là vị từ, không gian của vị từ, trọng lượng của vị từ.
- Thế nào là lượng từ, lượng từ tồn tại, lượng từ với mọi.

- Cách biểu diễn một câu thông thường thành biểu thức logic.

3.1. Các định nghĩa

Trong toán học hay trong chương trình của máy tính, chúng ta thường gặp những câu có chứa các biến như sau : “x>3”, “x=y+3”, “x+y=z”...

Các câu này không đúng cũng không sai vì các biến chưa được gán cho những giá trị xác định. Trong chương này, chúng ta sẽ xem xét cách tạo ra những mệnh đề từ những câu như vậy.

3.1.1. Định nghĩa vị từ (predicate)

Định nghĩa 1: 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.

Ví dụ 1: Các câu có liên quan đến các biến như: “x>3”, “x + y = 5” rất thường gặp trong toán học và trong các chương trình của máy tính. Các câu này không đúng cũng không sai vì các biến chưa được cho những giá trị xác định.

Nói cách khác, vị từ có thể xem là một hàm mệnh đề có nhiều biến hoặc không có biến nào, nó có thể đúng hoặc sai tùy thuộc vào giá trị của biến và lập luận của vị từ.

Ví dụ 2: Câu {n là chẵn} là một vị từ. Nhưng, khi cho n là một số cụ thể là chẵn hay là lẻ ta được một mệnh đề:

Với n = 2 thì {2 là chẵn}là mệnh đề đúng.

Với n = 5 thì {5 là chẵn}là mệnh đề sai.

Vị từ {n là chẵn} có 2 phần. Phần thứ nhất là biến n là chủ ngữ của câu. Phần thứ hai “là chẵn” cũng được gọi là vị từ, nó cho biết tính chất mà chủ ngữ có thể có.

Ký hiệu: P(n) = {n là chẵn}

Tổng quát, người ta nói P(n) là giá trị của hàm mệnh đề P tại n. Một khi biến n được gán trị thì P(n) là một mệnh đề.

Ví dụ 3: Cho vị từ P(x) = {x>3}. Xác định chân trị của P(4) và P(2).

Giải: P(4) = {4>3} là mệnh đề đúng.

P(2) = {2>3} là mệnh đề sai.

3.1.2. Không gian của vị từ

Người ta có thể xem vị từ như là một hàm mệnh đề P, với mỗi phần tử x thuộc tập hợp E ta được một ảnh P(x)∈{0; 1}. Tập hợp E này được gọi là không gian của vị từ. Không gian này sẽ chỉ rõ các giá trị khả dĩ của biến x làm cho P(x) trở thành mệnh đề đúng hoặc sai.

3.1.3. Trọng lượng của vị từ

Chúng ta cũng thường gặp những câu có nhiều biến hơn. Vị từ xuất hiện cũng như một hàm nhiều biến, khi đó số biến được gọi là trọng lượng của vị từ.

Ví dụ 4: Vị từ P(a, b) = {a + b = 5} là một vị từ 2 biến trên không gian N. Ta nói P có trọng lượng 2.

Trong một vị từ $P(x_1, x_2, ..., x_n)$ có trọng lượng là n. Nếu gán giá trị xác định cho một biến trong nhiều biến thì ta được một vị từ mới $Q(x_1, x_2, ... x_n)$ có trọng lượng là (n-1). Qui luật này được áp dụng cho đến khi n=0 thì ta có một mệnh đề. Vậy, thực chất mệnh đề là một vị từ có trọng lượng là ∅.

Ví dụ 5: Cho vị từ P(x, y, z) = {x + y = z}.

Cho x = 0: Q(y, z) = P(0, y, z) = {0 + y = z}

y = 0: R(z) = Q(0, z) = P(0, 0, z) = {0 + 0 = z}

z = 1: T = P(0, 0, 1) = {0 + 0 = 1} là mệnh đề sai.

Câu có dạng $P(x_1, x_2, ..., x_n)$ được gọi là giá trị của hàm mệnh đề P tại $(x_1, x_2, ..., x_n)$ và P cũng được gọi là vị từ.

3.1.4. Phép toán vị từ

Phép toán vị từ sử dụng các phép toán logic mệnh đề và là sự mở rộng của phép toán mệnh đề để thể hiện rõ hơn các tri thức.

Ví dụ 6: Cần viết câu "Nếu hai người thích một người thì họ không thích nhau" dưới dạng logic vị từ.

Trước khi viết câu trên ta hãy tìm hiểu các câu đơn giản được viết như sau:

- "Nam thích Mai" được viết theo phép toán vị từ là: thích (Nam, Mai).
- "Đông thích Mai" được viết theo phép toán vị từ là: thích (Đông, Mai).

Tổng quát khẳng định trên được viết như sau:

Thích (X, Z) AND thích (Y, Z) → NOT thích (X, Y)

(Thích (X, Z) ∧ thích (Y, Z) → ¬ thích (X, Y)

Ví dụ 7: Cho vị từ "Quả bóng màu xanh". Phép toán vị từ cho phép mô tả theo quan hệ tri thức theo dạng: (quả bóng, xanh).

Cách thể hiện này thuận tiện đối với việc dùng biến và hàm trong xử lý tri thức. Trong lĩnh vực trí tuệ nhân tạo, để lập trình trên các vị từ người ta sử dụng ngôn ngữ Prolog. Đó là một ngôn ngữ cấp cao có đặc điểm gần với ngôn ngữ tự nhiên, do ông C.Cameraller (Đại học Marseilles, Pháp) và nhóm đồng sự cho ra đời năm 1973.

a) Hằng:

Là một giá trị xác định trong không gian của vị từ. các hằng được ký hiệu bởi các chữ thường dùng để đặt tên các đối tượng đặc biệt hay thuộc tính.

b) Biến:

Dùng để thể hiện các lớp tổng quát của các đối tượng hay các thuộc tính. Biến được viết bằng các ký hiệu bắt đầu là chữ in hoa. Vậy có thể dùng vị từ có biến để thể hiện các vị từ tương tự.

Ví dụ 8: Vị từ "Quả bóng màu xanh" có thể viết lại: "X màu Y".

Quả bóng xanh là các hằng được xác định trong không gian của vị từ. X, Y là biến.

c) Các vị từ:

Một sự kiện hay mệnh đề trong phép toán vị từ được chia hai thành phần: Vị từ và tham số. Tham số thể hiện một hay nhiều đối tượng của mệnh đề, còn vị từ dùng để khẳng định về đối tượng.

Ví dụ 9: Câu "X thích Y" có dạng *thích* (X, Y).

thích là vị từ cho biết quan hệ giữa các đối tượng trong ngoặc. Đối số hay còn gọi là các biến vị từ là các ký hiệu thay cho các đối tượng của bài toán.

d) Hàm:

Được thể hiện bằng ký hiệu, cho biết quan hệ hàm.

Ví dụ 10: Hoa là mẹ của Mai, Đông là cha của Cúc. Hoa và Đông là bạn của nhau. Ta có hàm được viết để thể hiện quan hệ này.

Hàm *mẹ*(Mai) = Hoa

Hàm *cha*(Cúc) = Đông

Và vị từ *bạn*(x, y) = "Người x là bạn của người y".

Các hàm sẽ được dùng trong vị tự *bạn* là *bạn* (*Mẹ* (Mai), *Cha* (Cúc)) với ý nghĩa mẹ của Mai là bạn của cha của Cúc.

3.2. Các lượng từ

Khi tất cả các biến trong một hàm mệnh đề đều được gán cho một giá trị xác định, ta được chân trị của hàm mệnh đề. Tuy nhiên, còn có một cách khác để biến các vị từ thành mệnh đề mà người ta gọi là sự lượng hóa (hay lượng từ).

3.2.1. Lượng từ tồn tại (∃)

Câu xác định "Tập hợp những biến x làm cho P(x) là đúng không là tập hợp rỗng" là một mệnh đề. Hay "Tồn tại ít nhất một phần tử x trong

không gian sao cho P(x) là đúng" là một mệnh đề được gọi là lượng từ tồn tại của P(x).

Ký hiệu: ∃x P(x).

3.3.2. Lượng từ với mọi (∀)

Câu xác định "Tập hợp những x làm cho P(x) đúng là tất cả tập hợp E" là một mệnh đề. Hay "P(x) đúng với mọi giá trị x trong không gian" cũng là một mệnh đề được gọi là lượng từ với mọi của P(x).

Ký hiệu: ∀xP(x).

Ví dụ 11: Cho vị từ P(x) = {số tự nhiên x là số chẵn}. Xét chân trị của hai mệnh đề ∀xP(x) và ∃xP(x).

Giải: ∀x P(x) = {tất cả số nguyên tự nhiên x là số chẵn} là mệnh đề sai. Vì khi x = 5 thì P(5) là sai.

∃x P(x) = {hiện hữu một số nguyên tự nhiên x là số chẵn} là mệnh đề đúng. Vì khi x = 10 thì P(10) là đúng.

Nhận xét: Cho P là một vị từ có không gian E. Nếu E = $\{e_1, e_2, ... e_n\}$, mệnh đề ∀xP(x) là đúng khi tất cả các mệnh đề $P(e_1)$, $P(e_2)$, ... $P(e_n)$ là đúng. Nghĩa là $\forall x\ P(x) \Leftrightarrow P(e_1) \wedge P(e_2) \wedge ... \wedge P(e_n)$.

Tương tự ∃xP(x) là đúng nếu có ít nhất một trong những mệnh đề $P(e_1)$, $P(e_2)$,..., $P(e_n)$ là đúng. Nghĩa là $\exists xP(x) \Leftrightarrow P(e_1) \vee P(e_2) \vee ... \vee P(e_n)$.

- Nếu không gian E là một tập rỗng thì ∀xP(x) và ∃xP(x) có chân trị như thế nào?

Ví dụ 12: Cho P(a,b) = {cặp số nguyên tương ứng thỏa a + b = 5}. Hãy xác định chân trị của các mệnh đề sau:

∀(a,b) P(a,b)	{Tất cả cặp số nguyên tương ứng (a,b) sao cho a+b =5}	F
∃(a,b) P(a,b)	{Có một cặp số nguyên tương ứng (a,b) sao cho a + b=5}	T
∃b∀a P(a,b)	{Có một cặp số nguyên tương ứng b sao cho cho mọi số nguyên a ta có a + b =5}	F
∀a ∃b P(a,b)	{Mọi số nguyên tương ứng a, có một số nguyên b sao	T

	cho a + b = 5}	
∃a ∀b P(a,b)	{Có một số nguyên a sao cho với mọi số nguyên b đề có a + b = 5 }	F

Định lý 1: Cho vị từ P(x, y) có trọng lượng là 2. Khi đó:

a) ∀a∀b P(a,b) ≡ ∀b∀a P(a, b)

b) ∃a∃b P(a,b) ≡ ∃b∃a P(a, b)

c) Nếu ∃a∀b P(a,b) là đúng thì ∀b∃a P(a,b) cũng đúng nhưng điều ngược lại chưa đúng. Nghĩa là : ∃a∀b P(a,b) → ∀b∃a P(a,b) là hằng đúng.

d) Nếu ∃b∀a P(a,b) là đúng thì ∀a∃b P(a,b) cũng đúng nhưng điều ngược lại chưa đúng. Nghĩa là: ∃b∀a P(a,b) → ∀a∃b P(a,b) là hằng đúng.

Định lý 2: Cho P(x) là vị từ có biến x. Khi đó:

1. ¬ (∀ x P(x)) và ∃ x (¬ P(x) là có cùng chân trị.
2. ¬ (∃ x P(x)) và ∀ x (¬ P(x) là có cùng chân trị.

Giải thích:

1. Phủ định với ∀xP(x) nói rằng tập hợp những x làm cho P(x) đúng không là tất cả tập hợp E. Vậy nói rằng hiện hữu ít nhất một phần tử x∈E mà ở chúng P(x) là sai hay nói rằng hiện hữu ít nhất một phần tử x ∈ E mà P(x) là đúng.

2. ¬(∃ x P(x)) nói rằng tập hợp những x mà ở đó P(x) là đúng là tập hợp rỗng. Nghĩa là, tập hợp những x mà ở đó P(x) là sai là tập hợp E hay không có phần tử nào làm P(x) đúng. Ta có ∀ x (¬ P(x)).

Ví dụ 13: Phủ định của "Mọi số nguyên n là chia chẵn cho 3" là "Tồn tại ít nhất một số nguyên n không chia chẵn cho 3".

- Phương pháp ứng dụng.

Để đạt được phủ định của một mệnh đề xây dựng bằng liên kết của những biến của vi từ với phương tiện định lượng, người ta thay thế những định lượng với mọi ∀ bởi tồn tại ∃, tồn tại ∃ bởi với với mọi ∀ và sau cùng thay thế vị từ bằng phủ định của vị từ đó.

Định lý 3: Cho P(x) và Q(x) là hai vị từ có cùng không gian. Khi đó:

1. $\forall x\ (P(x) \wedge Q(x)) \equiv (\forall x\ (P(x) \wedge \forall x\ (Q(x))$.
2. Nếu mệnh đề $\exists x\ (P(x) \wedge Q(x))$ là đúng thì ta có mệnh đề $(\exists x\ P(x)) \wedge (\exists xQ(x))$ cũng đúng. Điều ngược lại chưa chắc đúng.
3. $\exists x\ (P(x) \vee Q(x)) \equiv (\exists xP(x) \vee \exists xQ(x))$.
4. Nếu mệnh đề $\forall x\ (P(x) \vee Q(x))$ là đúng thì ta có mệnh đề $\forall xP(x) \vee \forall xQ(x)$ là đúng, nhưng điều ngược lại không luôn luôn đúng.

3.3. Dịch các câu thông thường thành biểu thức logic

Sau khi đã được giới thiệu về các lượng từ, chúng ta có thể biểu diễn được một tập hợp rộng lớn các câu thông thường thành các biểu thức logic. Việc làm này nhằm mục đích loại đi những điều chưa rõ ràng và người ta có thể sử dụng các câu suy luận này trong việc lập trình logic và trí tuệ nhân tạo.

Ví dụ 14: Biểu diễn câu "Mọi người đều có chính xác một người bạn tốt nhất" thành một biểu thức logic.

Giải: Giả sử B(x,y) là câu "y là bạn tốt của x". Để dịch câu trong ví dụ cần chú ý B(x,y) muốn nói rằng đối với mỗi cá nhân x có một cá nhân khác là y sao cho y là bạn tốt nhất của x, nếu z là một cá nhân khác y thì z không phải là bạn tốt nhất của x. Do đó, câu trên có thể dịch thành:

$$\forall x\ \exists y\ \forall z\ [B(x,y) \wedge ((z \neq y) \rightarrow \neg\ B(x, z))]$$

Ví dụ 15: Biểu diễn câu: "Nếu một người nào đó là phụ nữ và đã sinh con, thì người đó sẽ là mẹ của một người nào khác" thành một biểu thức logic:

Giải: Giả sử F(x) = "x là phụ nữ"

P(x) = "x đã sinh con"

M(x,y) = "x là mẹ của y"

Vì trong ví dụ áp dụng cho tất cả mọi người nên ta có thể viết nó thành biểu thức $\forall x\ (F(x) \wedge P(x)) \rightarrow \exists y\ M(x,y)$.

Ví dụ 16: Xét các câu sau. Hai câu đầu tiên là tiền đề và câu ba là kết luận.

Toàn bộ tập hợp 3 câu này được gọi là một suy lý.

"Tất cả sư tử Hà Đông đều hung dữ".

"Một số sư tử Hà Đông không uống cà phê". "Một số sinh vật hung dữ không uống cà phê".

Giải: Gọi P(x)= {x là sư tử Hà Đông}

Q(x)= {x hung dữ}

R(x)= {x uống cà phê}

Giả sử rằng không gian là tập hợp toàn bộ các sinh vật, ta có cách suy diễn sau:

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

$\exists x$ (P(x) $\wedge \neg$ R(x))

$\exists x$ (Q(x) $\wedge \neg$ R(x))

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

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

Phép phủ định các lượng từ được minh họa rõ hơn trong bảng chú thích sau:

CÂU HỎI VÀ BÀI TẬP

1. Cho 2 vị từ P(x) xác định như sau: P(x) = {x $\leq$ 3}

   Q(x) = {x+ 1 là số lẻ}

   Nếu không gian là tập số nguyên, hãy xác định chân trị của những mệnh đề sau:

a) P(1)	b) Q(1)	c) $\neg$ P(3)
d) Q(6)	e) P(7)$\wedge$Q(7)	f) P(3)$\wedge$Q(4)
g) P(4)	h) $\neg$ [P(-4)$\vee$Q(-3)]	i) $\neg$ P(-4) $\wedge\neg$ Q(-3)

2. Các vị từ P(x), Q(x) được cho như bài tập 1. R(x) = {x > 0}. Nếu không gian vẫn là tập số nguyên.

   a) Xác định chân trị của những mệnh đề sau:

   1. P(3)$\vee$ [Q(3)$\vee\neg$ R(3)] 2. $\neg$P(3) $\wedge$ [Q(3) $\vee$ Q(3) $\vee$ R(3)]

3. $P(2) \rightarrow [Q(2) \rightarrow R(2)]$ 4. $[P(2) \leftrightarrow Q(2)] \rightarrow R(2)$

5. $P(0) \rightarrow [\neg Q(1) \leftrightarrow R(1)]$ 6. $[P(-1) \leftrightarrow Q(-2)] \leftrightarrow R(-3)$

b) Xác định tất cả các giá trị x sao cho $[P(x) \wedge Q(x)] \wedge R(x)$ là một mệnh đề đúng.

c) Tìm 5 giá trị nguyên dương nhỏ nhất cảu x sao cho vị từ:

$P(x) \rightarrow [\neg Q(x) \wedge R(x)]$ là mệnh đề đúng.

3. Cho vị từ P(x) được xác định như sau: $P(x) = \{x^2 = 2x\}$ trên không gian là tập hợp số nguyên. Xác định giá trị đúng, sai của những mệnh đề:

a) P(0) b) P(1) c) P(2)

d) P(-2) e) $\exists x\, P(x)$ f) $\forall x\, P(x)$

4. Cho 2 vị từ 2 biến P(x,y) và Q(x,y) được xác định như sau:

$P(x,y) = \{x^2 \geq y\}$

$Q(x,y) = \{x+2 < y\}$

Nếu không gian là tập số thực, xác định chân trị của các mệnh đề

a) P(2,4) b) $Q(1,\pi)$

c) $P(-3,8) \wedge Q(1,3)$ d) $P(\overline{1}, \overline{1}) \vee \neg Q(-2,-3)$

e) $P(2,2) \rightarrow Q(1,1)$ f) $P(\overline{1,2}) \leftrightarrow \neg Q(1,2)$

5. Trong một chương trình Pascal, n là một biến nguyên và A là mảng chứa 20 giá trị nguyên A[1], A[2],..., A[20] được khai báo như sau:

for n:=1 to 20 do A[n]:=n*n- n;

Hãy viết dạng kí hiệu của những mệnh đề sau: nếu xem A[n] như vị từ một biến n trên không gian các số nguyên từ 1 đến 20:

a) Mọi phần tử của mảng đều không âm.

b) Số nguyên A[20] là phần tử lớn nhất trong mảng.

c) Tồn tại 2 phần tử trong mảng A mà phần tử sau gấp 2 lần phần tử trước.

d) Các phần tử trong mảng được xếp theo thứ tự tăng dần.

e) Mọi phần tử trong mảng đều khác nhau.

Chứng minh các mệnh đề trên.

6. Trên không gian là tập số nguyên, cho các vị từ sau:

P(x) = {x>0}

Q(x) = {x là số chẵn}

R(x) = {x là số chính phương}

S(x) = {x chia hết cho 4}

T(x) = {x chia hết cho 5}

a) Viết dạng ký hiệu của những mệnh đề sau:

1. Có ít nhất 1 số nguyên chẵn.
2. Tồn tại 1 số nguyên dương là số chẵn.
3. Nếu x chẵn, thì x không chia hết cho 5.
4. Không có số nguyên chẵn nào là chia hết cho 5.
5. Tồn tại 1 số nguyên chẵn chia hết cho 4.
6. Nếu x chẵn và x là số chính phương, thì x chia hết cho 4.

b) Xác định chân trị của mỗi mệnh đề a). Với mỗi mệnh đề sai, hãy cho một dẫn chứng cụ thể.

c) Viết thành lời các dạng ký hiệu sau:

1. $\forall x\ [R(x) \rightarrow P(x)]$
2. $\forall x\ [S(x) \rightarrow Q(x)]$
3. $\forall x\ [S(x) \rightarrow \neg T(x)]$
4. $\exists x\ [S(x) \wedge \neg R(x)]$
5. $\forall x\ [\neg R(x) \vee \neg Q(x) \vee S(x)]$

7. Cho các vị từ trên không gian là tập số thực như sau:

P(x) = {x ≥ 0}

Q(x) = {$x^2 \geq 0$}

R(x) = {x^2 - 3x -4 = 0}

S(x) = {x^2 - 3 > 0}

Xác định giá trị đúng, sai của những mệnh đề sau. Theo dẫn chứng hoặc giải thích cụ thể:

a) $\exists x\ [P(x) \wedge R(x)]$
b) $\forall x\ [P(x) \rightarrow Q(x)]$
c) $\forall x\ [Q(x) \rightarrow S(x)]$
d) $\forall x\ [R(x) \vee S(x)]$
e) $\forall x\ [R(x) \rightarrow P(x)]$

8. Cho 3 vị từ P(x), Q(x), R(x) được xác định như sau:

$P(x) = \{x^2 - 8x + 15 = 0\}$, Q(x) = {x là số lẻ}

R(x) = {x > 0}

Trên tập không gian là tất cả các số nguyên, hãy xác định giá trị đúng, sai của những mệnh đề sau. Cho dẫn chứng hoặc giải thích cụ thể:

a) $\forall x\ [P(x) \rightarrow Q(x)]$ b) $\forall x\ [Q(x) \rightarrow P(x)]$

c) $\exists x\ [P(x) \rightarrow Q(x)]$ d) $\exists x\ [Q(x) \rightarrow P(x)]$

e) $\exists x\ [R(x) \wedge P(x)]$ f) $\forall x\ [P(x) \rightarrow R(x)]$

g) $\exists x\ [R(x) \rightarrow P(x)]$ h) $\forall x\ [\neg Q(x) \rightarrow \neg P(x)]$

i) $\exists x\ [P(x) \rightarrow (Q(x) \wedge R(x))]$ j) $\forall x\ [(P(x) \vee Q(x) \rightarrow R(x)]$

9. Cho 3 vị từ P(x), Q(x), R(x) như sau:

$P(x) = \{x^2 - 7x + 10 = 0\}$

$Q(x) = \{x^2 - 2x - 3 = 0\}$

R(x) = {x < 0}

a) Xác định giá trị đúng, sai của những mệnh đề sau, cho dẫn chứng hoặc giải thích cụ thể, nếu không gian là tập số nguyên.

1. $\forall x\ [P(x) \rightarrow \neg R(x)]$ 2. $\forall x\ [Q(x) \rightarrow R(x)]$

3. $\exists x\ [Q(x) \rightarrow R(x)]$ 4. $\exists x\ [P(x) \rightarrow R(x)]$

b) Câu hỏi như phần a) nhưng không gian là tập $Z^{'}$

c) Câu hỏi như phần a) nhưng không gian chỉ gồm 2 số nguyên 2, 5.

10. Cho P(x) = {x học ở lớp hơn 5 giờ mỗi ngày trong tuần}

Không gian là tập hợp các sinh viên. Hãy diễn đạt các lượng từ sau thành câu thông thường.

a) $\exists x\ P(x)$ b) $\forall x\ P(x)$

c) $\exists x\ \neg P(x)$ d) $\forall x\ \neg P(x)$

11. Cho vị từ P(x,y) = {x đã học môn y} với không gian của x là tập hợp tất cả các sinh viên lớp bạn và không gian của y là tập hợp tất cả các môn tin học của học kỳ mà bạn đang học. Hãy diễn đạt các lượng từ sau thành

các câu thông thường:

a) $\exists x \exists y P(x,y)$ b) $\exists x \forall y P(x,y)$ c) $\forall x \exists y P(x,y)$

d) $\exists y \forall x P(x,y)$ e) $\forall y \exists x P(x,y)$ f) $\forall x \forall y P(x,y)$

12. Cho 2 vị từ:

P(x) = {x nói được Tiếng Anh} và Q(x) = {x biết ngôn ngữ C^{++}}

Cho không gian là tập hợp các sinh viên lớp bạn. Hãy diễn đạt các câu sau bằng cách dùng P(x), Q(x), các lượng từ và các phép toán logic.

a) Có một sinh viên ở lớp bạn nói được Tiếng Anh và biết C^{++}
b) Có một sinh viên ở lớp bạn nói được Tiếng Anh nhưng không biết C^{++}
c) Mọi sinh viên ở lớp bạn đều nói được Tiếng Anh hoặc biết C^{++}
d) Không có một sinh viên nào ở lớp bạn nói được Tiếng Anh hoặc biết C^{++}

13. Cho các vị từ:

P(x) = {x là sinh viên)

Q(x) = {x là kẻ ngu dốt}

R(x) = {x là kẻ vô tích sự}

Bằng cách dùng các lượng từ, các phép toán logic và với các vị từ P(x), Q(x), R(x). Hãy diễn đạt các câu sau với không gian là toàn thể sinh viên:

a) Không có sinh viên nào là kẻ ngu dốt.
b) Mọi kẻ ngu dốt đều là vô tích sự.
c) Không có sinh viên nào là vô tích sự.

Chương III
QUAN HỆ

MỤC TIÊU CỦA CHƯƠNG

Chương này có mục đích hệ thống hóa, củng cố những kiến thức mà người học đã biết ở mức độ nhất định ở trường phổ thông, đồng thời nâng cao, bổ sung một số nội dung mới mà người học cần phải có để có thể nghiên cứu tốt những nội dung chuyên ngành của tin học.

- Hiểu được khái niệm quan hệ tổng quát, quan hệ giữa hai tập hợp, đặc biệt quan hệ hai ngôi trên một tập hợp.

- Hiểu các khái niệm quan hệ tương đương, quan hệ thứ tự và vận dụng vào những vấn đề liên quan trong tin học, như cơ sở dữ liệu, mạng máy tính,…

TÀI LIỆU THAM KHẢO

1. Nguyễn Hữu Anh, 1999, Toán rời rạc, NXB Giáo dục
2. Đại học Cần Thơ, 2003, Bài giảng Toán rời rạc 1
3. Kenneth H. Rosen (Bùi Xuân Toại dịch), 2010, Toán rời rạc và những ứng dụng trong Tin học, NXB Lao động
4. Phạm Thế Long (chủ biên), Nguyễn Xuân Viên, Nguyễn Thiện Luân, Nguyễn Đức Hiếu, Nguyễn Văn Xuất, 2005, Toán rời rạc, NXB Đại học Sư phạm
5. Seymour Lipschutz, 1964, Set theory and related topics, Mc Hraw Hill.

I. KHÁI NIỆM QUAN HỆ

Quan hệ là một khái niệm quen thuộc trong cuộc sống hằng ngày, nói về sự liên hệ giữa sự vật, hiện tượng trong thế giới. Trong toán học, quan hệ là một khái niệm quan trọng, là sự trừu tượng hoá khái niệm quan hệ trong thực tế.

1.1. Quan hệ giữa hai tập hợp

Định nghĩa 1: Quan hệ R giữa tập hợp X và tập hợp Y là một tập con của tích Đề-các X×Y.

Ví dụ 1: Cho tập hợp X = {1; 2; 3} và tập hợp Y = {a; b; c; d}

thì R = {(1,b); (1,d); (2,a); (2,c); (3,a)} là một quan hệ giữa tập hợp X và tập hợp Y.

Ví dụ 2: Cho tập hợp môn học M ={Toán; Lập trình; Cơ sở dữ liệu} và tập hợp các điểm có thể nhận Đ = {0; 1; 2; 3; 4; 5; 6; 7; 8; 9; 10} thì R' = {(Toán,8); (Lập trình,9); (Cơ sở dữ liệu, 7)} là một quan hệ giữa M và Đ.

1.2. Quan hệ giữa n tập hợp

Định nghĩa 2: Cho n tập hợp X_1, X_2,…, X_n. Một tập con R của tích Đề-các $X_1 \times X_2 \times \ldots \times X_n$ gọi là quan hệ n ngôi giữa n tập hợp X_1, X_2,…, X_n.

Ví dụ 3: Cho tập hợp sinh viên S = {An; Mai; Lan}, tập hợp môn học M = {Toán; Lập trình; Cơ sở dữ liệu} và tập hợp điểm Đ = {0; 1; 2; 3; 4; 5; 6; 7; 8; 9; 10}thì một quan hệ R giữa 3 tập hợp trên là:

R = {(An, Toán, 8); (An, Lập trình,9); (Lan, Lập trình,9); (Mai, Cơ sở dữ liệu,7)}.

Quan hệ là cơ sở toán học để xây dựng lý thuyết về cơ sở dữ liệu quan hệ.

1.3. Quan hệ hai ngôi trên một tập hợp

Định nghĩa 3: Nếu R là quan hệ giữa tập hợp X và chính nó, ta nói R là quan hệ hai ngôi trên tập hợp X. Khi đó, nếu (a,b)$\in$ R ta nói a quan hệ R với b và thường kí hiệu a R b.

Từ nay về sau, nếu không nói gì thêm thì ta ngầm hiểu một quan hệ R trên X là quan hệ hai ngôi trên tập X.

Ví dụ 4: Cho tập hợp sinh viên S của một lớp học, trên S ta xác định quan hệ R_1 = {(x,y) ∈S×S| sinh viên x có quê cùng huyện với sinh viên y}, mà gọi ngắn gọn là quan hệ cùng quê.

Ví dụ 5: Cho tập hợp số tự nhiên N, trên N ta xác định quan hệ chia hết, kí hiệu $|_N$, a, b∈N, a|b ⇔ ∃k∈N, b = ka.

$|_N$ = {(a,b)∈N×N| a|b}.

Tương tự, ta có quan hệ chia hết trên trên tập hợp X, kí hiệu $|_X$, với X là tập hợp con bất kì của N.

Ví dụ 6: Cho tập số nguyên Z, trên Z ta xác định quan hệ đồng dư mô đun m (m nguyên dương), kí hiệu $\equiv_m$, x, y∈Z, x ≡ y (*mod m*) ⇔ x – y chia hết cho m.

$\equiv_m$ ={(x,y)∈Z×Z| x ≡ y(*mod m*).

Ví dụ 7: Cho M là tập hợp các máy tính trong một mạng. Trên M ta xác định quan hệ *Connected:*

Connected = {(m,n)∈M×M| máy m có kết nối "trực tiếp" với máy n}.

- Một quan hệ R trên X có thể được biểu diễn bằng một ma trận vuông M_R cấp |X|, trong đó M_R(x,y) = 1 nếu x R y và M_R(x,y) = 0 nếu x không quan hệ R với y.

Ví dụ 8: Cho X = {1; 2; 3; 4; 5; 6} thì ma trận M của quan hệ $|_X$ là:

$$M = \begin{array}{c|cccccc} x/y & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 1 & 0 & 1 \\ 3 & 0 & 0 & 1 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 1 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

CÂU HỎI VÀ BÀI TẬP

1. Quan hệ trên một tập hợp là gì?

2. Có bao nhiêu quan hệ trên một tập n phần tử ?
3. Giả sử $A_1 = \{0; 1; 2; 3; 4\}$, $A_2 = \{1; 3; 7; 12\}$, $A_3 = \{0; 1; 2; 4; 8; 16; 32\}$ và $A_4 = \{-3; -2; -1; 0; 1; 2; 3\}$

   a) Xét $R_1 = \{(x, y, z, t) \in A_1xA_2xA_3xA_4 | \ xyzt = 0\}$. Hãy tính $|R_1|$.

   b) Xét $R_2 = \{(x, y, z, t) \in A_1xA_2xA_3xA_4 | \ xyzt < 0\}$. Hãy tính $|R_2|$.
4. Cho A = {1; 2; 3}, B = {2; 4; 5}

   a) Tính |A x B|

   b) Tìm số quan hệ giữa A và B

   c) Tìm số quan hệ hai ngôi trên A

   d) Tìm số quan hệ giữa A và B chứa (1, 2) và (1, 5).

   e) Tìm số quan hệ giữa A và B chứa đúng 5 cặp có thứ tự (nghĩa là chứa các cặp dạng (a, b) sao cho $a \leq b$).

Bài tập trên máy tính

5. Cài đặt cấu trúc dữ liệu lưu trữ một quan hệ hai ngôi trên tập hợp hữu hạn, nhập dữ liệu cho quan hệ và in ra các cặp phần tử thuộc quan hệ.
6. Nghiên cứu các khái niệm bao đóng phản xạ, bao đóng đối xứng và bao đóng bắc cầu và xây dựng chương trình để tìm các loại bao đóng

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

Người ta thường xem xét bốn tính chất của quan hệ hai ngôi trên một tập hợp, đó là các tính chất phản xạ, đối xứng, phản xứng và bắc cầu.

2.1. Tính chất phản xạ (reflexive)

Định nghĩa 4: Quan hệ R trên tập hợp X được gọi là có tính chất phản xạ nếu $\forall x \in X$, x R x (hoặc $(x,x) \in X \times X$.

- Nhìn vào ma trận biểu diễn quan hệ, nếu $M_R(x,x) = 1$ $\forall x \in X$ thì quan hệ R có tính chất phản xạ.

Ví dụ 9: Quan hệ ở *Ví dụ 4, 5, 6, 7* ở mục 1.3 có tính chất phản xạ.

2.2. Tính chất đối xứng (symmetric)

Định nghĩa 5: Quan hệ R trên tập hợp X được gọi là có tính chất đối xứng nếu $\forall x, y \in X$ mà x R y thì y R x (hoặc mà $(x,y) \in X \times X$ thì $(y,x) \in X \times X$.

- Nhìn vào ma trận quan hệ, nếu quan hệ R có tính chất đối xứng thì ma trận quan hệ M_R đối xứng qua đường chéo chính, nghĩa là $M_R(x,y) = M_R(y,x)$, $\forall x, y \in X$.

Ví dụ 10: Các quan hệ cùng quê *Ví dụ 3, 4, 5* mục 1.3 có tính chất đối xứng.

2.3. Tính chất phản xứng (anti-symmetric)

Định nghĩa 6: Quan hệ R trên tập hợp X được gọi là có tính chất phản xứng nếu $\forall x, y \in X$ mà xRy và yRx thì x = y. Nói cách khác, nếu $x \neq y$ thì không thể đồng thời có x R y và yRx.

- Nhìn vào ma trận quan hệ, nếu quan hệ R có tính chất phản xứng thì $\forall x, y \in X$ mà $x \neq y$ thì $M_R(x,y) \neq M_R(y,x)$.

Ví dụ 11: Quan hệ chia hết trên N có tính chất phản xứng, vì:

Nếu $\exists a, b \in N$ mà a|b và b|a $\Rightarrow \exists k_1, k_2 \in N$, $b = k_1 a$ và $a = k_2 b \Rightarrow a = b$.

Ví dụ 12: Quan hệ đồng dư mô đun m trên Z không có tính chất phản xứng, vì $\exists 0, m \in Z$, $0 \neq m$ nhưng $m \equiv 0 (mod\ m)$.

2.4. Tính chất bắc cầu (transitive)

Định nghĩa 7: Quan hệ R trên tập hợp X gọi là có tính chất bắc cầu nếu $\forall x, y, z \in X$ mà xRy và yRz thì xRz.

Ví dụ 13: Các quan hệ ở *Ví dụ 4, 5, 6* ở mục 1.3 và *Ví dụ 11, 12* có tính chất bắc cầu.

CÂU HỎI VÀ BÀI TẬP

1. a) Có bao nhiêu quan hệ đối xứng trên một tập n phần tử?
   b) Có bao nhiêu quan hệ phản xạ trên một tập n phần tử?
   c) Có bao nhiêu quan hệ phản đối xứng trên một tập n phần tử?

2. a) Giải thích cách sử quan hệ n ngôi để biểu diễn thông tin về các sinh viên trong một trường đại học.

   b) Làm cách nào có thể sử dụng quan hệ 5 ngôi gồm tên sinh viên, địa chỉ sinh viên, số điện thoại, ngành học, và điểm trung bình để tạo nên quan hệ 3 ngôi chứa tên sinh viên, ngành học và điểm trung bình của họ?

3. Cho S là tập tất cả các xâu chữ cái tiếng Anh. Xác định xem các quan hệ dưới đây có là phản xạ, đối xứng, phản xứng, và bắc cầu không?

   a) R_1 = {(a, b)| a và b không có chữ cái nào giống nhau}

   b) R_2 = {(a, b)| a và b không cùng độ dài}

   c) R 3 = {(a, b)| a dài hơn b}

4. Xây dựng một quan hệ trên tập {1, 2, 3, 4}có các tính chất:

   a) Phản xạ, đối xứng, nhưng không bắc cầu

   b) Không phản xạ, đối xứng và bắc cầu

   c) Không phản xạ, phản xứng và không bắc cầu

   d) Phản xạ, không đối xứng, không phản xứng, bắc cầu

5. Chứng tỏ rằng tập con của một quan hệ của một quản hệ phản xứng cũng là quan hệ phản xứng.

6. Cho R là quan hệ phản xạ trên tập A. Chứng tỏ rằng $R \subseteq R^2$.

7. Cho R_1 và R_2 là các quan hệ phản xạ trên tập A. Hỏi $R_1 \cap R_2$ có là phản xạ không? $R_1 \cup R_2$ có là phản xạ không?

8. Cho R_1 và R_2 là các quan hệ đối xứng trên tập A. Hỏi $R_1 \cap R_2$ có là đối xứng không? $R_1 \cup R_2$ có là đối xứng không?

Bài tập trên máy tính

9. **Viết chương trình nhập vào một quan hệ trên một tập hợp và cho biết quan hệ thoả tính chất nào trong các tính chất phản xạ, đối xứng, phản xứng, bắc cầu?**

III. QUAN HỆ TƯƠNG ĐƯƠNG

3.1. Khái niệm

Định nghĩa 1: Quan hệ R trên tập hợp X được gọi là quan hệ tương đương nếu có ba tính chất:

i) Phản xạ

ii) Đối xứng

iii) Bắc cầu

Ví dụ 1: Quan hệ đồng dư mô đun *m* trên Z là quan hệ tương đương, vì:

+ Có tính chất phản xạ: $\forall x \in Z$, $x - x = 0$ chia hết cho *m* nên $x \equiv x (mod\ m)$.

+ Có tính chất đối xứng: $\forall x, y \in Z$ có $x \equiv y (mod\ m)$ thì $x - y$ chia hết cho $m \Rightarrow y - x$ chia hết cho $m \Rightarrow y \equiv x (mod\ m)$.

+ Có tính chất bắc cầu: $\forall x, y, z \in Z$ có $x \equiv y (mod\ m)$ và $y \equiv z (mod\ m)$ $\Rightarrow x - y$ chia hết cho *m* và $y - z$ chia hết cho $m \Rightarrow x - y + y - z = x - z$ chia hết cho $m \Rightarrow x \equiv z (mod\ m)$.

Ví dụ 2: Quan hệ chia hết trên N không phải quan hệ tương đương vì không có tính chất đối xứng, do $\exists 1,3 \in N$, 1chia hết 3 nhưng 3 không chia hết 1.

3.2. Lớp tương đương

Định nghĩa 2: Cho quan hệ tương đương R trên tập hợp X và $x \in X$. Lớp tương đương của phần tử x đối với quan hệ R, kí hiệu [x] (hoặc $\bar{x}$), là tập hợp gồm những phần tử của X có quan hệ R với x.

Ta có $[x] = \{y \in X \mid x\ R\ y\}$

- Chú ý, dễ nhận thấy luôn có $x \in [x]$.

Ví dụ 3: Quan hệ đồng dư mô đun 5 trên Z, có các lớp tương đương:

$[0] = \{0; \pm 1.5; \pm 2.5; \ldots; \pm k.5; \ldots\}$, $\forall k \in N$.

$[1] = \{1; 1 \pm 1.5; 1 \pm 2.5; \ldots; 1 \pm k.5; \ldots\}$, $\forall k \in N$.

$[2] = \{2; 2 \pm 1.5; 2 \pm 2.5; \ldots; 2 \pm k.5; \ldots\}$, $\forall k \in N$.

[3] = {3; 3±1.5; 3±2.5; …; 3±k.5; …}, $\forall k \in N$.

[4] = {4; 4±1.5; 4±2.5; …; 4±k.5; …}, $\forall k \in N$.

Ta kí hiệu Z_5 = {[0]; [1]; [2]; [3]; [4]} và gọi là tập hợp thương của Z trên quan hệ đồng dư mô đun 5 trên Z. Tổng quát, kí hiệu Z_m là tập thương của quan hệ đồng dư môn đun *m* trên Z.

Định lí 1: Cho R là quan hệ tương đương trên tập hợp X, $x, y \in X$. Khi đó:

i) $y \in [x] \Leftrightarrow [x] = [y]$.

ii) $[x] = [y]$ hoặc $[x] \cap [y] = \varnothing$.

Chứng minh:

i) Rõ ràng nếu $[x] = [y] \Rightarrow y \in [y] = [x]$

Nếu $y \in [x]$, lấy $z \in [x] \Rightarrow x \ R \ z$ và $x \ R \ y \Rightarrow x \ R \ z$ và $y \ R \ x \Rightarrow y \ R \ z \Rightarrow z \in [y] \Rightarrow [x] \subset [y]$.

Tương tự, cũng chứng minh được $[y] \subset [x]$. Vậy $[x] = [y]$.

ii) Giả sử $[x] \cap [y] \neq \varnothing \Rightarrow \exists z \in [x] \cap [y] \Rightarrow z \in [x]$ và $z \in [y] \Rightarrow [x] = [z]$ và $[y] = [z] \Rightarrow [x] = [y]$.

3.3. Sự phân hoạch tập hợp

Định nghĩa 3: Cho tập hợp $X \neq \varnothing$. Một sự phân hoạch tập hợp X là một sự phân chia X thành các tập con khác rỗng $B_1, B_2, \ldots, B_n$ thoả hai điều kiện:

1) $B_1 \cup B_2 \cup \ldots \cup B_n = X$

2) $B_i \cap B_j = \varnothing$, $\forall i \neq j$.

- *Nhận xét*: Mỗi sự phân hoạch tập hợp X tương ứng 1-1 với một quan hệ tương đương trên X sao cho mỗi lớp tương đương là một tập con của sự phân hoạch.

Ví dụ 4: Cho tập hợp X = {1; 2; 3; 4; 5; 6} có một phân hoạch là:

B_1 = {1; 3}, B_2 = {2; 4; 6}, B_3 = {5} và dễ nhận thấy sự phân hoạch này tương ứng với quan hệ tương đương R = {(1,1); (2,2); (3,3); (4,4); (5,5); (6,6); (1,3); (3,1); (2,4); (4,2); (2,6); (6,2); (4,6); (6,4)}.

CÂU HỎI VÀ BÀI TẬP

1. Quan hệ R được gọi là quan hệ vòng quanh nếu a R b và b R c kéo theo c R a. Chứng minh R là phản xạ và vòng quanh nếu và chỉ nếu nó là quan hệ tương đương.
2. Trong các quan hệ trên tập mọi người dưới đây, quan hệ nào là tương đương?
   a) {(x, y)| x và y sinh cùng ngày giờ}
   b) {(x, y)| x và y sinh cùng năm}
   c) {(x, y)| x và y ở cùng thành phố}
3. Chứng tỏ rằng {(x, y)| x – y ∈ Q} là một quan hệ tương đương trên tập các số thực. Xác định [1], [1/2], và [π].
4. Cho tập A = {1 ; 2 ; 3 ; 4}. Hãy xác định tất cả các phân hoạch của tập A thoả :
   a) Có một tập con có 3 phần tử và một tập con có một phần tử
   b) Có hai tập con, mỗi tập con có 2 phần tử
   c) Có ba tập con, trong đó có một tập con có 2 phần tử
5. Giả sử $P_1 = \{A_1, A_2,\ldots, A_m\}$ và $P_2 = \{B_1, B_2,\ldots, B_m\}$ là hai phân hoạch của tập S. Chứng tỏ rằng tập các tập con không rỗng dạng $A_i \cap B_j$ là một phân hoạch của S.

Bài tập trên máy tính

6. Viết chương trình nhập vào một quan hệ hai ngôi trên một tập hợp và cho biết quan hệ này có phải là quan hệ tương đương không ? Nếu quan hệ là tương đương hãy xuất ra các phần tử thuộc lớp tương đương của phần tử x (x là phần tử bất kỳ của tập hợp).

IV. QUAN HỆ THỨ TỰ - TẬP HỢP THỨ TỰ

4.1. Các khái niệm

a) Quan hệ thứ tự:

Định nghĩa 1: Quan hệ S trên tập hợp X được gọi là quan hệ thứ tự nếu S thoả ba tính chất:

i) Phản xạ

ii) Phản xứng

iii) Bắc cầu

Ví dụ 1: Quan hệ chia hết trên N là quan hệ thứ tự vì thoả tính chất phản xạ, phản xứng và bắc cầu.

Ví dụ 2: Cho E là một tập hợp bất kì. Trên P(E) xác định quan hệ tập con $\subset$. Dễ nhận thấy quan hệ $\subset$ có tính chất phản xạ, phản xứng, bắc cầu, nên $\subset$ là quan hệ thứ tự.

Ví dụ 3: Quan hệ đồng dư mô đun m trên Z không phải quan hệ thứ tự vì không có tính chất phản xứng.

b) Tập hợp thứ tự:

Định nghĩa 2: Một tập hợp X mà trên đó xác định một quan hệ thứ tự S gọi là một tập hợp thứ tự, kí hiệu (X, S).

Ví dụ 4: (N, |) là một tập hợp thứ tự. Các tập thứ tự (N, $\leq$), (N, $\geq$) với $\leq$, $\geq$ là các quan hệ so sánh thông thường cũng là các tập hợp thứ tự.

Định nghĩa 3: Tập hợp thứ tự (X, S) gọi là tập hợp thứ tự toàn phần nếu $\forall x, y \in X$ thì hoặc x S y, hoặc y S x.

Ví dụ 5: Tập hợp thứ tự (N, $\leq$), trong đó $\leq$ là quan hệ so sánh thông thường trên N là tập thứ tự toàn phần.

Định nghĩa 4: Tập thứ tự (X, S) không phải là tập thứ tự toàn phần gọi là tập thứ tự bộ phận. Nói cách khác, tập thứ tự (X, S) gọi là tập thứ tự bộ phận nếu $\exists x, y \in X$ mà x không quan hệ S với y và y không quan hệ S với x.

Ví dụ 6: Tập thứ tự (N, |) là tập thứ tự bộ phận vì $\exists 2, 3 \in N$ mà 2 không chia hết 3 và 3 không chia hết 2.

4.2. Phần tử tối đại, phần tử tối tiểu

Định nghĩa 5: Cho tập hợp thứ tự (X, S), phần tử $a \in X$ gọi là phần tử tối đại nếu $\forall x \in X$ mà a S x thì x = a.

Phần tử $b \in X$ gọi là phần tử tối tiểu nếu $\forall x \in X$ mà x S b thì x = b.

Ví dụ 7: Trên tập thứ tự $(P(E), \subset)$ thì E là phần tử tối đại, vì $\forall A \in P(E)$ nếu $E \subset A$ thì A = E; $\varnothing$ là phần tử tối tiểu vì nếu $A \subset \varnothing$ thì $A = \varnothing$.

Ví dụ 8: Cho X = {2; 3; 4; 5; 6; 7} thì tập thứ tự (X, |) dễ nhận thấy có các phần tử tối đại là 4, 5, 6, 7 và phần tử tối tiểu là 2, 3, 5.

- *Chú ý:* Một tập thứ tự có thể có nhiều phần tử tối đại và phần tử tối tiểu.

4.3. Phần tử lớn nhất, phần tử nhỏ nhất

Định nghĩa 6: Cho tập hợp thứ tự (X, S). Phần tử *m* gọi là phần tử lớn nhất nếu x S *m*, $\forall x \in X$. Phần tử *n* gọi là phần tử bé nhất nếu *n* S x, $\forall x \in X$.

Ví dụ 9: Trong *Ví dụ 7*, E là phần tử lớn nhất, $\varnothing$ là phần tử bé nhất. Trong *Ví dụ 8*, không có phần tử lớn nhất, cũng không có phần tử bé nhất.

- *Chú ý:*

+ Phần tử lớn nhất/bé nhất của một tập hợp thứ tự nếu có là duy nhất.

+ Một tập hợp thứ tự có thể không có phần tử lớn nhất/bé nhất.

+ Nếu một tập hợp thứ tự có duy nhất một phần tử tối đại thì nó cũng đồng thời là phần tử lớn nhất. Tương tự đối với phần tử tối tiểu.

4.4. Trội và bị trội

Định nghĩa 7: Cho tập hợp thứ tự (X, S) và $x, y \in X$. Phần tử y gọi là trội của phần tử x, hoặc x bị trội bởi x, nếu x S y.

Ví dụ 10: Trên tập hợp thứ tự (N, |) thì 4 trội 2, hoặc 2 bị trội bởi 4, vì 2|4.

- *Chú ý*: Một phần tử bất kì luôn trội và bị trội bởi chính nó.

4.5. Trội trực tiếp

Định nghĩa 8: Trên tập hợp thứ tự (X, S) và x, y∈X. Phần tử y gọi là trội trực tiếp x nếu:

+ y trội x, và

+ y ≠ x, và

+ không tồn tại z∈X, z ≠ x, z ≠ y mà z trội x và y trội z.

Ví dụ 11: Trên tập hợp thứ tự (N, |) thì 4 là trội trực tiếp của 2.

4.6. Cận trên, cận dưới

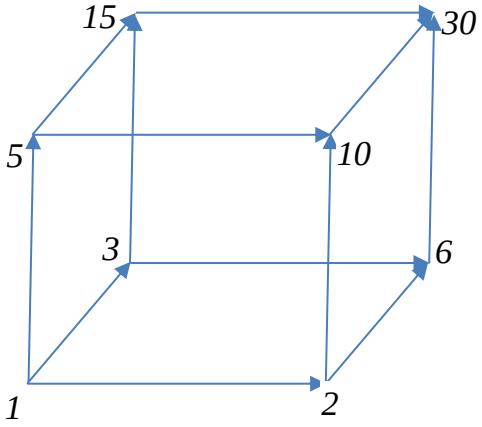
Định nghĩa 9: Cho tập hợp thứ tự (X, S) và A ⊂ X. Phần tử a ∈ X được gọi là một cận trên của A nếu a trội mọi phần tử x ∈ A. Phần tử b ∈ X được gọi là một cận dưới của A nếu b bị trội bởi mọi phần tử y ∈ A.

Ví dụ 12 : Trên tập hợp thứ tự (N, |) và A = {3 ; 6 ; 15}, các cận trên của A là 30, 60, 120,… các cận dưới của A là 1, 3.

4.7. Sơ đồ Hasse

Định nghĩa 10: Sơ đồ Hasse của tập hợp thứ tự (X, S) là một sự biểu diễn tập hợp thứ tự này trên mặt phẳng sao cho mỗi phần tử của X biểu diễn bằng một điểm trên mặt phẳng, và nếu phần tử y là trội trực tiếp phần tử x thì vẽ một cung từ điểm x đến điểm y.

Ví dụ 13: Gọi U_{30} là tập hợp các ước số dương của 30, nghĩa là U = {1; 2; 3; 5; 6; 10; 15; 30}. Sơ đồ Hasse của tập hợp thứ tự (U_{30},|) là:



CÂU HỎI VÀ BÀI TẬP

1. Cho E là tập hợp bất kỳ. Trên $\mathcal{P}(E)$ xác định quan hệ $\subset$ sao cho với A, B $\in \mathcal{P}(E)$, A $\subset$ B khi và chỉ khi A là tập con của B. hãy chứng minh quan hệ $\subset$ là quan hệ thứ tự.
2. Hãy vẽ sơ đồ Hasse cho tập hợp sắp thứ tự ($\mathcal{P}(E)$, $\subset$) trong đó E = {1; 2; 3; 4}.
3. Ký hiệu $Ư_n$ với n nguyên dương, là tập hợp các ước số nguyên dương của n.
    a) Chứng tỏ ($Ư_n$, |) là một tập hợp thứ tự.
    b) Vẽ sơ đồ Hasse của tập thứ tự ($Ư_{42}$, |), ($Ư_{210}$, |).
    c) Tìm phần tử lớn nhất, nhỏ nhất của các tập thứ tự ($Ư_{30}$, |), ($Ư_{210}$, |), ($Ư_{42}$, |), ($Ư_{105}$, |).
4. Có bao nhiêu quan hệ thứ tự dưới đây để cho x là phần tử tối tiểu?
    a) A = {x; y}
    b) A = {x; y; z}
5. Cho A = $\mathcal{P}(E)$ với thứ tự bao hàm và E = {1; 2; 3; 4; 5; 6; 7}. Xét B = {{1}; {2}; {2; 3}}. Hãy cho biết:
    a) Các chặn trên của B bao gồm 3, 4, 5 phần tử của E.
    b) Các chặn dưới của B.

Bài tập trên máy tính

6. Cho số nguyên n, hãy hiển thị tất cả các quan hệ trên tập có n phần tử.
7. Cho ma trận biểu diễn một quan hệ trên một tập hữu hạn. Hãy tim ma trận biểu diễn bao đóng phản xạ của quan hệ đó.
8. Cho ma trận biểu diễn một quan hệ trên một tập hữu hạn. Hãy tim ma trận biểu diễn bao đóng đối xứng của quan hệ đó.
9. Cho ma trận biểu diễn một quan hệ trên một tập hữu hạn. Hãy tim ma trận biểu diễn bao đóng bắc cầu của quan hệ đó.

Chương IV
PHƯƠNG PHÁP ĐẾM

MỤC TIÊU CỦA CHƯƠNG

Lý thuyết tổ hợp là một phần quan trọng của toán học rời rạc, chuyên nghiên cứu sự phân bố các phần tử vào các tập hợp. Thông thường các phần tử này là hữu hạn và việc phân bố chúng phải thoả mãn những điều kiện nhất định nào đó, tùy theo yêu cầu của bài toán cần nghiên cứu. Mỗi cách phân bố như vậy gọi là một cấu hình tổ hợp. Vấn đề này đã được nghiên cứu từ thế kỷ 17, khi những câu hỏi về tổ hợp được nêu ra trong những công trình nghiên cứu các trò chơi may rủi. Liệt kê, đếm các đối tượng có những tính chất nào đó là một phần quan trọng của lý thuyết tổ hợp. Chúng ta cần phải đếm các đối tượng để giải nhiều bài toán khác nhau. Hơn nữa các kỹ thuật đếm được dùng rất nhiều khi tính xác suất của các biến cố.

Sau khi học chương này, người học cần đạt được:

- Hiểu khái niệm chỉnh hợp, tổ hợp, hoán vị không lặp và lặp

- Hiểu các quy tắc cộng, quy tắc nhân và các nguyên lý bù trừ, nguyên lý Dirichlet

- Hiểu các phương pháp đếm nâng cao, biết lập hệ thức truy hồi và giải một số dạng phương trình truy hồi

- Có thể vận dụng kiến thức trên vào các bài toán đếm cụ thể

TÀI LIỆU THAM KHẢO

1. Đại học Cần Thơ, 2003, Bài giảng Toán rời rạc 1
2. Kenneth H. Rosen (Bùi Xuân Toại dịch), 2010, Toán rời rạc và những ứng dụng trong Tin học, NXB Lao động

3. Phạm Thế Long (chủ biên), Nguyễn Xuân Viên, Nguyễn Thiện Luân, Nguyễn Đức Hiếu, Nguyễn Văn Xuất, 2005, Toán rời rạc, NXB Đại học Sư phạm.

I. CÁC QUY TẮC ĐẾM

1.1. Quy tắc cộng

Quy tắc 1: Giả sử có k công việc $T_1, T_2, ..., T_k$. Các việc này có thể làm tương ứng bằng $n_1, n_2, ..., n_k$ cách và giả sử không có hai việc nào có thể làm đồng thời. Khi đó số cách làm một trong k việc đó là $n_1+n_2+ ... + n_k$.

Theo nghĩa tập hợp thì quy tắc cộng có thể phát biểu:

Cho k tập hợp $T_1, T_2, ..., T_k$ thoả điều kiện $T_i \cap T_j = \varnothing$, $\forall i \neq j$ thì:

$|T_1 \cup T_2 \cup ... \cup T_k| = |T_1|+|T_2|+ ...+|T_k|$.

Ví dụ 1: Một sinh viên có thể chọn bài thực hành máy tính từ một trong ba danh sách tương ứng có 23, 15 và 19 bài. Vì vậy, theo quy tắc cộng có 23 + 15 + 19 = 57 cách chọn bài thực hành.

Ví dụ 2: Giá trị của biến m bằng bao nhiêu sau khi đoạn chương trình sau được thực hiện?

```
m := 0;
for i1 := 1 to n1 do m := m+1;
for i2 :=1 to n2  do m := m+1;
.....
for ik := 1 to nk do m := m+1;
```

Giá trị khởi tạo của m bằng 0. Khối lệnh này gồm k vòng lặp khác nhau. Sau mỗi bước lặp của từng vòng lặp giá trị của k được tăng lên một đơn vị. Gọi T_i là việc thi hành vòng lặp thứ i. Có thể làm T_i bằng n_i cách vì vòng lặp thứ i có n_i bước lặp. Do các vòng lặp không thể thực hiện đồng thời nên theo quy tắc cộng, giá trị cuối cùng của m bằng số cách thực hiện một trong số các nhiệm vụ T_i, tức là $m = n_1+n_2+ ... + n_k$.

1.2. Quy tắc nhân

Quy tắc 2: Giả sử một nhiệm vụ nào đó được tách ra thành k việc T_1, T_2, ..., T_k. Nếu việc T_i có thể làm bằng n_i cách sau khi các việc T_1, T_2, ... T_{i-1} đã được làm, khi đó có $n_1.n_2....n_k$ cách thi hành nhiệm vụ đã cho.

Nguyên lý nhân thường được phát biểu bằng ngôn ngữ tập hợp như sau. Nếu A_1, A_2,..., A_k là các tập hợp hữu hạn, khi đó số phần tử của tích Đề-các của các tập này bằng tích của số các phần tử của mọi tập thành phần. Ta biết rằng việc chọn một phần tử của tích Đề-các A_1 x A_2 x...x A_k được tiến hành bằng cách chọn lần lượt một phần tử của A_1, một phần tử của A_2, ..., một phần tử của A_k. Theo quy tắc nhân ta có:

$$|A_1 \text{ x } A_2 \text{ x } ... \text{ x } A_k| = |A_1|.|A_2|...|A_k|.$$

Ví dụ 3: Người ta có thể ghi nhãn cho những chiếc ghế trong một giảng đường bằng một chữ cái và một số nguyên dương không vượt quá 100. Bằng cách như vậy, nhiều nhất có bao nhiêu chiếc ghế có thể được ghi nhãn khác nhau?

Thủ tục ghi nhãn cho một chiếc ghế gồm hai việc, gán một trong 26 chữ cái và sau đó gán một trong 100 số nguyên dương. Quy tắc nhân chỉ ra rằng có 26.100=2600 cách khác nhau để gán nhãn cho một chiếc ghế. Như vậy nhiều nhất ta có thể gán nhãn cho 2600 chiếc ghế.

Ví dụ 4: Có bao nhiêu xâu nhị phân có độ dài n?

Mỗi một trong n bit của xâu nhị phân có thể chọn bằng hai cách vì mỗi bit hoặc bằng 0 hoặc bằng 1. Bởi vậy theo quy tắc nhân có tổng cộng 2^n xâu nhị phân khác nhau có độ dài bằng n.

Ví dụ 5: Có thể tạo được bao nhiêu ánh xạ từ tập A có m phần tử vào tập B có n phần tử?

Theo định nghĩa, một ánh xạ xác định trên A có giá trị trên B là một phép tương ứng mỗi phần tử của A với một phần tử nào đó của B. Rõ ràng sau khi đã chọn được ảnh của i - 1 phần tử đầu, để chọn ảnh của phần tử thứ

i của A ta có n cách. Vì vậy theo quy tắc nhân, ta có n.n...n=n^m ánh xạ xác định trên A nhận giá trị trên B.

Ví dụ 6: Có bao nhiêu đơn ánh xác định trên tập A có m phần tử và nhận giá trị trên tập B có n phần tử?

Nếu m > n thì với mọi ánh xạ, ít nhất có hai phần tử của A có cùng một ảnh, điều đó có nghĩa là không có đơn ánh từ A đến B. Bây giờ giả sử m ≤ n và gọi các phần tử của A là $a_1,a_2,...,a_m$. Rõ ràng có n cách chọn ảnh cho phần tử a_1. Vì ánh xạ là đơn ánh nên ảnh của phần tử a_2 phải khác ảnh của a_1 nên chỉ có n - 1 cách chọn ảnh cho phần tử a_2. Nói chung, để chọn ảnh của a_k ta có n - k + 1 cách. Theo quy tắc nhân, ta có:

$$n(n-1)(n-2)...(n-m+1) = \frac{n!}{(n-m)!}$$ đơn ánh từ tập A đến tập B.

Ví dụ 7: Giá trị của biến k bằng bao nhiêu sau khi chương trình sau được thực hiện?

```
k := 0;
for i1 := 1 to n1 do
    for i2 := 1 to n2 do
    .....................
            for ik := 1 to nk do
                    k := k+1;
```

Giá trị khởi tạo của k bằng 0. Ta có k vòng lặp được lồng nhau. Gọi T_i là việc thi hành vòng lặp thứ i. Khi đó số lần đi qua vòng lặp bằng số cách làm các việc T_1, T_2, ..., T_k. Số cách thực hiện việc T_j là n_j (j=1, 2,..., k), vì vòng lặp thứ j được duyệt với mỗi giá trị nguyên i_j nằm giữa 1 và n_j. Theo quy tắc nhân vòng lặp lồng nhau này được duyệt qua $n_1.n_2....n_k$ lần. Vì vậy giá trị cuối cùng của k là $n_1.n_2....n_k$.

4.3. Các nguyên lý đếm

a) Nguyên lý bù trừ: Khi hai công việc có thể được làm đồng thời, ta không thể dùng quy tắc cộng để tính số cách thực hiện nhiệm vụ gồm cả hai việc.

Để tính đúng số cách thực hiện nhiệm vụ này ta cộng số cách làm mỗi một trong hai việc rồi trừ đi số cách làm đồng thời cả hai việc.

Ta có thể phát biểu nguyên lý đếm này bằng ngôn ngữ tập hợp. Cho A_1, A_2 là hai tập hữu hạn, khi đó:

$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

Từ đó với ba tập hợp hữu hạn A_1, A_2, A_3, ta có:

$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_1| + |A_1 \cap A_2 \cap A_3|$.

Bằng quy nạp, với k tập hữu hạn A_1, A_2, ..., A_k ta có:

$| A_1 \cup A_2 \cup ... \cup A_k| = N_1 - N_2 + N_3 - ... + (-1)^{k-1}N_k$,

trong đó N_m ($1 \le m \le k$) là tổng phần tử của tất cả các giao m tập lấy từ k tập đã cho, nghĩa là:

$$N_m = \sum_{1 \le i_1 < i_2 < ... < i_m \le k} | A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_m} |$$

Bây giờ ta đồng nhất tập A_m ($1 \le m \le k$) với tính chất A_m cho trên tập vũ trụ hữu hạn U nào đó và đếm xem có bao nhiêu phần tử của U sao cho không thỏa mãn bất kỳ một tính chất A_m nào. Gọi $\overline{N}$ là số cần đếm, N là số phần tử của U. Ta có:

$$\overline{N} = N - | A_1 \cup A_2 \cup ... \cup A_k| = N - N_1 + N_2 - ... + (-1)^k N_k,$$

trong đó N_m là tổng các phần tử của U thỏa mãn m tính chất lấy từ k tính chất đã cho. Công thức này được gọi là *nguyên lý bù trừ.* Nó cho phép tính $\overline{N}$ qua các N_m trong trường hợp các số này dễ tính toán hơn.

Ví dụ 8: Có n lá thư và n phong bì ghi sẵn địa chỉ. Bỏ ngẫu nhiên các lá thư vào các phong bì. Hỏi xác suất để xảy ra không một lá thư nào đúng địa chỉ.

Mỗi phong bì có n cách bỏ thư vào, nên có tất cả n! cách bỏ thư. Vấn đề còn lại là đếm số cách bỏ thư sao cho không lá thư nào đúng địa chỉ. Gọi U là tập hợp các cách bỏ thư và A_m là tính chất lá thư thứ m bỏ đúng địa chỉ. Khi đó theo công thức về nguyên lý bù trừ ta có:

$$\overline{N} = n! - N_1 + N_2 - ... + (-1)^n N_n,$$

trong đó N_m ($1 \le m \le n$) là số tất cả các cách bỏ thư sao cho có m lá thư đúng địa chỉ. Nhận xét rằng, N_m là tổng theo mọi cách lấy m lá thư từ n lá, với mỗi cách lấy m lá thư, có (n-m)! cách bỏ để m lá thư này đúng địa chỉ, ta nhận được:

$N_m = C_n^m (n - m)! = \frac{n!}{k!}$ và $\overline{N} = n!(1 - \frac{1}{1!} + \frac{1}{2!} - ... + (-1)^n \frac{1}{n!})$,

trong đó $C_n^m = \frac{n!}{m!(n-m)!}$ là tổ hợp chập m của tập n phần tử (số cách chọn m đối tượng trong n đối tượng được cho). Từ đó xác suất cần tìm là: $1 - \frac{1}{1!} + \frac{1}{2!} - ... + (-1)^n \frac{1}{n!}$. Một điều lý thú là xác suất này dần đến e^{-1} (nghĩa là còn $> \frac{1}{3}$) khi n khá lớn.

Số $\overline{N}$ trong bài toán này được gọi là số mất thứ tự và được ký hiệu là D_n.

Dưới đây là một vài giá trị của D_n, cho ta thấy D_n tăng nhanh như thế nào so với n:

N	2	3	4	5	6	7	8	9	10	11
D_n	1	2	9	44	265	1854	14833	133496	1334961	14684570

b) Nguyên lý Dirichlet:

Giả sử có một đàn chim bồ câu bay vào chuồng. Nếu số chim nhiều hơn số ngăn chuồng thì ít nhất trong một ngăn có nhiều hơn một con chim. Nguyên lý này dĩ nhiên là có thể áp dụng cho các đối tượng không phải là chim bồ câu và chuồng chim.

*Mệnh đề 1***:** Nếu có k+1 (hoặc nhiều hơn) đồ vật được đặt vào trong k hộp thì tồn tại một hộp có ít nhất hai đồ vật.

*Chứng minh***:** Giả sử không có hộp nào trong k hộp chứa nhiều hơn một đồ vật. Khi đó tổng số vật được chứa trong các hộp nhiều nhất là bằng k. Điều này trái giả thiết là có ít nhất k + 1 vật.

Nguyên lý này thường được gọi là nguyên lý Dirichlet, mang tên nhà toán học người Đức ở thế kỷ 19. Ông thường xuyên sử dụng nguyên lý này trong công việc của mình.

Ví dụ 9: Trong bất kỳ một nhóm 367 người thế nào cũng có ít nhất hai người có ngày sinh nhật giống nhau bởi vì chỉ có tất cả 366 ngày sinh nhật khác nhau.

Ví dụ 10: Trong kỳ thi học sinh giỏi, điểm bài thi được đánh giá bởi một số nguyên trong khoảng từ 0 đến 100. Hỏi rằng ít nhất có bao nhiêu học sinh dự thi để cho chắc chắn tìm được hai học sinh có kết quả thi như nhau?

Theo nguyên lý Dirichlet, số học sinh cần tìm là 102, vì ta có 101 kết quả điểm thi khác nhau.

Ví dụ 11: Trong số những người có mặt trên trái đất, phải tìm được hai người có hàm răng giống nhau. Nếu xem mỗi hàm răng gồm 32 cái như là một xâu nhị phân có chiều dài 32, trong đó răng còn ứng với bit 1 và răng mất ứng với bit 0, thì có tất cả $2^{32} = 4.294.967.296$ hàm răng khác nhau. Trong khi đó số người trên hành tinh này là vượt quá 5 tỉ, nên theo nguyên lý Dirichlet ta có điều cần tìm.

c) Nguyên lý Dirichlet tổng quát:

Mệnh đề 2: Nếu có N đồ vật được đặt vào trong k hộp thì sẽ tồn tại một hộp chứa ít nhất ⌈N/k⌉ đồ vật.

(Ở đây, ⌈x⌉ là giá trị của hàm trần tại số thực x, đó là số nguyên nhỏ nhất có giá trị lớn hơn hoặc bằng x. Khái niệm này đối ngẫu với ⌊x⌋ – giá trị của hàm sàn hay hàm phần nguyên tại x – là số nguyên lớn nhất có giá trị nhỏ hơn hoặc bằng x.)

Chứng minh: Giả sử mọi hộp đều chứa ít hơn ⌈N/k⌉ vật. Khi đó tổng số đồ vật là

$$\leq k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\,\frac{N}{k} = N.$$

Điều này mâu thuẫn với giả thiết là có N đồ vật cần xếp.

Ví dụ 12: Trong 100 người, có ít nhất 9 người sinh cùng một tháng.

Xếp những người sinh cùng tháng vào một nhóm. Có 12 tháng tất cả. Vậy theo nguyên lý Dirichlet, tồn tại một nhóm có ít nhất ⌈100/12⌉ = 9 người.

Ví dụ 13: Có năm loại học bổng khác nhau. Hỏi rằng phải có ít nhất bao nhiêu sinh viên để chắc chắn rằng có ít ra là 6 người cùng nhận học bổng như nhau.

Gọi N là số sinh viên, khi đó ⌈N/5⌉ = 6 khi và chỉ khi $5 < N/5 \leq 6$ hay $25 < N \leq 30$. Vậy số N cần tìm là 26.

Ví dụ 14: Số mã vùng cần thiết nhỏ nhất phải là bao nhiêu để đảm bảo 25 triệu máy điện thoại trong nước có số điện thoại khác nhau, mỗi số có 9 chữ số (giả sử số điện thoại có dạng 0XX - 8XXXXX với X nhận các giá trị từ 0 đến 9).

Có 10^7 = 10.000.000 số điện thoại khác nhau có dạng 0XX - 8XXXXX. Vì vậy theo nguyên lý Dirichlet tổng quát, trong số 25 triệu máy điện thoại ít nhất có ⌈25.000.000/10.000.000⌉ = 3 có cùng một số. Để đảm bảo mỗi máy có một số cần có ít nhất 3 mã vùng.

d) Một vài ứng dụng của nguyên lý Dirichlet:

Trong nhiều ứng dụng thú vị của nguyên lý Dirichlet, khái niệm đồ vật và hộp cần phải được lựa chọn một cách khôn khéo. Trong phần nay có vài ví dụ như vậy.

Ví dụ 15: Trong một phòng họp có n người, bao giờ cũng tìm được 2 người có số người quen trong số những người dự họp là như nhau.

Chứng minh: Số người quen của mỗi người trong phòng họp nhận các giá trị từ 0 đến $n - 1$. Rõ ràng trong phòng không thể đồng thời có người có số người quen là 0 (tức là không quen ai) và có người có số người quen là $n - 1$ (tức là quen tất cả). Vì vậy theo số lượng người quen, ta chỉ có thể phân n người ra thành $n - 1$ nhóm. Vậy theo nguyên lý Dirichlet tồn tai một nhóm

có ít nhất 2 người, tức là luôn tìm được ít nhất 2 người có số người quen là như nhau.

Ví dụ 16: Trong một tháng gồm 30 ngày, một đội bóng chuyền thi đấu mỗi ngày ít nhất 1 trận nhưng chơi không quá 45 trận. Chứng minh rằng tìm được một giai đoạn gồm một số ngày liên tục nào đó trong tháng sao cho trong giai đoạn đó đội chơi đúng 14 trận.

Chứng minh: Gọi a_j là số trận mà đội đã chơi từ ngày đầu tháng đến hết ngày j. Khi đó:

$$1 \le a_1 < a_2 < ... < a_{30} < 45$$

$$15 \le a_1+14 < a_2+14 < ... < a_{30}+14 < 59.$$

Sáu mươi số nguyên $a_1, a_2, ..., a_{30}, a_1+ 14, a_2 + 14, ..., a_{30}+14$ nằm giữa 1 và 59. Do đó theo nguyên lý Dirichlet có ít nhất 2 trong 60 số này bằng nhau. Vì vậy tồn tại i và j sao cho $a_i = a_j + 14$ (j < i). Điều này có nghĩa là từ ngày j + 1 đến hết ngày i đội đã chơi đúng 14 trận.

Ví dụ 17: Chứng tỏ rằng trong n + 1 số nguyên dương không vượt quá 2n, tồn tại ít nhất một số chia hết cho số khác.

Chứng minh: Ta viết mỗi số nguyên $a_1, a_2,..., a_{n+1}$ dưới dạng $a_j = 2^{k_j} q_j$ trong đó k_j là số nguyên không âm còn q_j là số dương lẻ nhỏ hơn 2n. Vì chỉ có n số nguyên dương lẻ nhỏ hơn 2n nên theo nguyên lý Dirichlet tồn tại i và j sao cho $q_i = q_j = q$. Khi đó $a_i = 2^{k_i} q$ và $aj = 2^{k_j} q$. Vì vậy, nếu $k_i \le k_j$ thì a_j chia hết cho a_i còn trong trường hợp ngược lại ta có a_i chia hết cho a_j.

Ví dụ 18: Giả sử trong một nhóm 6 người mỗi cặp hai hoặc là bạn hoặc là thù. Chứng tỏ rằng trong nhóm có ba người là bạn lẫn nhau hoặc có ba người là kẻ thù lẫn nhau.

Chứng minh: Gọi A là một trong 6 người. Trong số 5 người của nhóm hoặc là có ít nhất ba người là bạn của A hoặc có ít nhất ba người là kẻ thù của A, điều này suy ra từ nguyên lý Dirichlet tổng quát, vì ⌈5/2⌉ = 3. Trong trường hợp đầu ta gọi B, C, D là bạn của A. nếu trong ba người này có hai

người là bạn thì họ cùng với A lập thành một bộ ba người bạn lẫn nhau, ngược lại, tức là nếu trong ba người B, C, D không có ai là bạn ai cả thì chứng tỏ họ là bộ ba người thù lẫn nhau. Tương tự có thể chứng minh trong trường hợp có ít nhất ba người là kẻ thù của A.

II. CHỈNH HỢP – TỔ HỢP – HOÁN VỊ

2.1. Chỉnh hợp

a) Chỉnh hợp (không lặp) :

Định nghĩa 1: Một cách sắp xếp có thứ tự k phần tử (không lặp lại) của một tập hợp n phần tử gọi là một chỉnh hợp chập k của n phần tử.

Kí hiệu số chỉnh hợp chập k của n phần tử là A(k, n) hoặc A_n^k.

Ta có $A_n^k = \frac{n!}{(n-k)!} = n.(n-1)\ldots(n-k+1).$

b) Chỉnh hợp lặp :

Định nghĩa 2: Một cách sắp xếp có thứ tự k phần tử có thể lặp lại của một tập n phần tử được gọi là một chỉnh hợp lặp chập k từ tập n phần tử.

Nếu A là tập gồm n phần tử đó thì mỗi chỉnh hợp như thế là một phần tử của tập A^k. Kí hiệu số chỉnh hợp lặp chập k của n phần tử là $\bar{A}$(k, n) hoặc $\bar{A}_n^k$.

Ta có $\bar{A}_n^k = n^k$.

Thật vậy, mỗi chỉnh hợp lặp chập k từ tập n phần tử là một hàm từ tập k phần tử vào tập n phần tử. Vì vậy số chỉnh hợp lặp chập k từ tập n phần tử là n^k.

2.2. Tổ hợp

a) Tổ hợp (không lặp):

Định nghĩa 3: Một tổ hợp lặp chập k của một tập hợp là một cách chọn không có thứ tự k phần tử (không lặp lại) của tập hợp đã cho.

Như vậy một tổ hợp kiểu này là một dãy không kể thứ tự gồm k thành phần lấy từ tập n phần tử. Do đó k ≤ n.

Ký hiệu số tổ hợp chập k của n là C(k, n) hoặc C_n^k.

Ta có $C_n^k = \frac{n!}{k!(n-k)!}$.

b) Tổ hợp lặp:

Định nghĩa 4: Một tổ hợp lặp chập k của một tập hợp là một cách chọn không có thứ tự k phần tử có thể lặp lại của tập đã cho.

Như vậy một tổ hợp lặp kiểu này là một dãy không kể thứ tự gồm k thành phần lấy từ tập n phần tử. Do đó có thể là k có thể giá trị lớn hơn n.

Kí hiệu số tổ hợp lặp chập k của n phần tử là $\bar{C}$(k, n) hoặc $\bar{C}_n^k$.

Mệnh đề 3: Số tổ hợp lặp chập k từ tập n phần tử bằng C_{n+k-1}^k.

Chứng minh: Mỗi tổ hợp lặp chập k từ tập n phần tử có thể biểu diễn bằng một dãy n−1 thanh đứng và k ngôi sao. Ta dùng n − 1 thanh đứng để phân cách các ngăn. Ngăn thứ i chứa thêm một ngôi sao mỗi lần khi phần tử thứ i của tập xuất hiện trong tổ hợp. Chẳng hạn, tổ hợp lặp chập 6 của 4 phần tử được biểu thị bởi:

* * | * | | * * *

mô tả tổ hợp chứa đúng 2 phần tử thứ nhất, 1 phần tử thứ hai, không có phần tử thứ 3 và 3 phần tử thứ tư của tập hợp.

Mỗi dãy n − 1 thanh và k ngôi sao ứng với một xâu nhị phân độ dài n + k − 1 với k số 1. Do đó số các dãy n − 1 thanh đứng và k ngôi sao chính là số tổ hợp chập k từ tập n + k − 1 phần tử. Đó là điều cần chứng minh.

Ví dụ 19: Có bao nhiêu cách chọn 5 tờ giấy bạc từ một két đựng tiền gồm những tờ 1000đ, 2000đ, 5000đ, 10.000đ, 20.000đ, 50.000đ, 100.000đ. Giả sử thứ tự mà các tờ tiền được chọn là không quan trọng, các tờ tiền cùng loại là không phân biệt và mỗi loại có ít nhất 5 tờ.

Vì ta không kể tới thứ tự chọn tờ tiền và vì ta chọn đúng 5 lần, mỗi lần lấy một từ 1 trong 7 loại tiền nên mỗi cách chọn 5 tờ giấy bạc này chính là một tổ hợp lặp chập 5 từ 7 phần tử. Do đó số cần tìm là $C_{7+5-1}^5 = 462$.

Ví dụ 20: Phương trình $x_1 + x_2 + x_3 = 15$ có bao nhiêu nghiệm nguyên không âm?

Chúng ta nhận thấy mỗi nghiệm của phương trình ứng với một cách chọn 15 phần tử từ một tập có 3 loại, sao cho có x_1 phần tử loại 1, x_2 phần tử loại 2 và x_3 phần tử loại 3 được chọn. Vì vậy số nghiệm bằng số tổ hợp lặp chập 15 từ tập có 3 phần tử và bằng $C_{3+15-1}^{15} = 136$.

2.3. Hoán vị của tập hợp có các phần tử giống nhau

a) Hoán vị (không lặp):

Định nghĩa 5: Mỗi cách cách sắp xếp các phần tử của một tập có n phần tử là một hoán vị của n phần tử của tập này.

b) Hoán vị lặp:

Trong bài toán đếm, một số phần tử có thể giống nhau. Khi đó cần phải cẩn thận, tránh đếm chúng hơn một lần. Ta xét thí dụ sau.

Ví dụ 21: Có thể nhận được bao nhiêu xâu khác nhau bằng cách sắp xếp lại các chữ cái của từ SUCCESS?

Vì một số chữ cái của từ SUCCESS là như nhau nên câu trả lời không phải là số hoán vị của 7 chữ cái được. Từ này chứa 3 chữ S, 2 chữ C, 1 chữ U và 1 chữ E. Để xác định số xâu khác nhau có thể tạo ra được ta nhận thấy có C(7,3) cách chọn 3 chỗ cho 3 chữ S, còn lại 4 chỗ trống. Có C(4,2) cách chọn 2 chỗ cho 2 chữ C, còn lại 2 chỗ trống. Có thể đặt chữ U bằng C(2,1) cách và C(1,1) cách đặt chữ E vào xâu. Theo nguyên lý nhân, số các xâu khác nhau có thể tạo được là:

$$C_7^3 . C_4^2 . C_2^1 . C_1^1 = \frac{7!4!2!1!}{3!.4!.2!.2!.1!.1!.1!.0!} = \frac{7!}{3!.2!.1!.1!} = 420.$$

Mệnh đề 4: Số hoán vị của n phần tử trong đó có n_1 phần tử như nhau thuộc loại 1, n_2 phần tử như nhau thuộc loại 2, ..., và n_k phần tử như nhau thuộc loại k, bằng

$$\frac{n!}{n_1!.n_2!...n_k!}.$$

Chứng minh: Để xác định số hoán vị trước tiên chúng ta nhận thấy có $C_n^{n_1}$ cách giữ n_1 chỗ cho n_1 phần tử loại 1, còn lại n - n_1 chỗ trống. Sau đó có $C_{n-n_1}^{n_2}$ cách đặt n_2 phần tử loại 2 vào hoán vị, còn lại n - n_1 - n_2 chỗ trống. Tiếp tục đặt các phần tử loại 3, loại 4,..., loại k - 1vào chỗ trống trong hoán vị. Cuối cùng có $C_{n-n_1-...-n_{k-1}}^{n_k}$ cách đặt n_k phần tử loại k vào hoán vị. Theo quy tắc nhân tất cả các hoán vị có thể là: $C_n^{n_1}.C_{n-n_1}^{n_2}....C_{n-n_1-...-n_{k-1}}^{n_k} = \frac{n!}{n_1!.n_2!...n_k!}$.

*Ví dụ 22***:** Có bao nhiêu cách chia những xấp bài 5 quân cho mỗi một trong 4 người chơi từ một cỗ bài chuẩn 52 quân?

Người đầu tiên có thể nhận được 5 quân bài bằng C_{52}^5 cách. Người thứ hai có thể được chia 5 quân bài bằng C_{47}^5 cách, vì chỉ còn 47 quân bài. Người thứ ba có thể nhận được 5 quân bài bằng C_{42}^5 cách. Cuối cùng, người thứ tư nhận được 5 quân bài bằng C_{37}^5 cách. Vì vậy, theo nguyên lý nhân tổng cộng có

$$C_{52}^5.C_{47}^5.C_{42}^5.C_{37}^5 = \frac{52!}{5!.5!.5!.5!.32!}$$

cách chia cho 4 người mỗi người một xấp 5 quân bài.

Ví dụ trên là một bài toán điển hình về việc phân bố các đồ vật khác nhau vào các hộp khác nhau. Các đồ vật là 52 quân bài, còn 4 hộp là 4 người chơi và số còn lại để trên bàn. Số cách sắp xếp các đồ vật vào trong hộp được cho bởi mệnh đề sau

Mệnh đề 4: Số cách phân chia n đồ vật khác nhau vào trong k hộp khác nhau sao cho có n_i vật được đặt vào trong hộp thứ i, với i = 1, 2, ..., k bằng

$$\frac{n!}{n_1!.n_2!...n_k!.(n-n_1-...-n_k)!}.$$

2.4. Sinh các hoán vị và tổ hợp

*a) Sinh các hoán vị***:**

Có nhiều thuật toán đã được phát triển để sinh ra n! hoán vị của tập {1,2,...,n}. Ta sẽ mô tả một trong các phương pháp đó, phương pháp liệt kê các hoán vị của tập {1, 2,..., n} theo thứ tự từ điển. Khi đó, hoán vị $a_1a_2...a_n$ được gọi là đi trước hoán vị $b_1b_2...b_n$ nếu tồn tại k ($1 \le k \le n$), $a_1 = b_1$, $a_2 = b_2$,..., $a_{k-1} = b_{k-1}$ và $a_k < b_k$.

Thuật toán sinh các hoán vị của tập {1,2,...,n} dựa trên thủ tục xây dựng hoán vị kế tiếp, theo thứ tự từ điển, từ hoán vị cho trước $a_1\ a_2\ ...a_n$. Đầu tiên nếu $a_{n-1} < a_n$ thì rõ ràng đổi chỗ a_{n-1} và a_n cho nhau thì sẽ nhận được hoán vị mới đi liền sau hoán vị đã cho. Nếu tồn tại các số nguyên a_j và a_{j+1} sao cho $a_j < a_{j+1}$ và $a_{j+1} > a_{j+2} > ... > a_n$, tức là tìm cặp số nguyên liền kề đầu tiên tính từ bên phải sang bên trái của hoán vị mà số đầu nhỏ hơn số sau. Sau đó, để nhận được hoán vị liền sau ta đặt vào vị trí thứ j số nguyên nhỏ nhất trong các số lớn hơn a_j của tập $a_{j+1}, a_{j+2}, ..., a_n$, rồi liệt kê theo thứ tự tăng dần của các số còn lại của $a_j, a_{j+1}, a_{j+2}, ..., a_n$ vào các vị trí j+1, ..., n. Dễ thấy không có hoán vị nào đi sau hoán vị xuất phát và đi trước hoán vị vừa tạo ra.

Ví dụ 23: Tìm hoán vị liền sau theo thứ tự từ điển của hoán vị 4736521.

Cặp số nguyên đầu tiên tính từ phải qua trái có số trước nhỏ hơn số sau là $a_3 = 3$ và $a_4 = 6$. Số nhỏ nhất trong các số bên phải của số 3 mà lại lớn hơn 3 là số 5. Đặt số 5 vào vị trí thứ 3. Sau đó đặt các số 3, 6, 1, 2 theo thứ tự tăng dần vào bốn vị trí còn lại. Hoán vị liền sau hoán vị đã cho là 4751236.

procedure *Hoán vị liền sau ($a_1, a_2, ..., a_n$) (hoán vị của (1,2,...,n) khác(n, n–1, ..., 2, 1))*

begin

j := n – 1;

while *($a_j > a_{j+1}$)**do***

j := j – 1; {j là chỉ số lớn nhất mà $a_j < a_{j+1}$}

k := n;

while *($a_j > a_k$)**do***

k := k – 1; {a_k là số nguyên nhỏ nhất trong các số lớn hơn a_j và bên phải a_j}

đổi chỗ (a_j, a_k);

```
r := n;
s := j + 1;
while (r > s) do
begin
        đổi chỗ (a_r, a_s);
        r := r - 1 ; s := s + 1;
end;
{Điều này sẽ xếp phần đuôi của hoán vị ở sau vị trí thứ j theo
thứ tự tăng dần.}
```

end;

b) Sinh các tổ hợp:

Làm thế nào để tạo ra tất cả các tổ hợp các phần tử của một tập hữu hạn? Vì tổ hợp chính là một tập con, nên ta có thể dùng phép tương ứng 1-1 giữa các tập con của $\{a_1,a_2,...,a_n\}$ và xâu nhị phân độ dài n.

Ta thấy một xâu nhị phân độ dài n cũng là khai triển nhị phân của một số nguyên nằm giữa 0 và $2^n - 1$. Khi đó 2^n xâu nhị phân có thể liệt kê theo thứ tự tăng dần của số nguyên trong biểu diễn nhị phân của chúng. Chúng ta sẽ bắt đầu từ xâu nhị phân nhỏ nhất 00...00 (n số 0). Mỗi bước để tìm xâu liền sau ta tìm vị trí đầu tiên tính từ phải qua trái mà ở đó là số 0, sau đó thay tất cả số 1 ở bên phải số này bằng 0 và đặt số 1 vào chính vị trí này.

```
procedure Xâu nhị phân liền sau (b_{n-1}b_{n-2}...b_1b_0): xâu nhị phân
khác (11...11)
begin
        i := 0;
        while (b_i = 1)do
        begin
                b_i := 0;
                i := i + 1;
        end;
        b_i := 1;
end;
```

Tiếp theo chúng ta sẽ trình bày thuật toán tạo các tổ hợp chập k từ n phần tử {1,2,...,n}. Mỗi tổ hợp chập k có thể biểu diễn bằng một xâu tăng.

Khi đó có thể liệt kê các tổ hợp theo thứ tự từ điển. Có thể xây dựng tổ hợp liền sau tổ hợp $a_1a_2...a_k$ bằng cách sau. Trước hết, tìm phần tử đầu tiên a_i trong dãy đã cho kể từ phải qua trái sao cho $a_i \neq n - k + i$. Sau đó thay a_i bằng $a_i + 1$ và a_j bằng $a_i + j - i + 1$ với $j = i + 1, i + 2, ..., k$.

Ví dụ 24: Tìm tổ hợp chập 4 từ tập {1, 2, 3, 4, 5, 6} đi liền sau tổ hợp {1, 2, 5, 6}.

Ta thấy từ phải qua trái $a_2 = 2$ là số hạng đầu tiên của tổ hợp đã cho thỏa mãn điều kiện $a_i \neq 6 - 4 + i$. Để nhận được tổ hợp tiếp sau ta tăng a_i lên một đơn vị, tức $a_2 = 3$, sau đó đặt $a_3 = 3 + 1 = 4$ và $a_4 = 3 + 2 = 5$. Vậy tổ hợp liền sau tổ hợp đã cho là {1,3,4,5}. Thủ tục này được cho dưới dạng thuật toán như sau.

procedure *Tổ hợp liền sau ({a_1, a_2, ..., a_k}: tập con thực sự của tập {1, 2, ..., n} không bằng {n − k + 1, ..., n} với $a_1 < a_2 < ... < a_k$)*

begin

i := k;

while *($a_i = n - k + i$)* ***do***

i := i − 1;

a_i := a_i + 1;

for *j := i + 1* ***to*** *k* ***do***

a_j := a_i + j − I;

end*;*

III. ĐẾM NÂNG CAO

3.1. Hệ thức truy hồi

a) Khái niệm mở đầu và mô hình hóa bằng hệ thức truy hồi:

Đôi khi ta rất khó định nghĩa một đối tượng một cách tường minh. Nhưng có thể dễ dàng định nghĩa đối tượng này qua chính nó. Kỹ thuật này được gọi là đệ quy. Định nghĩa đệ quy của một dãy số định rõ giá trị của một hay nhiều hơn các số hạng đầu tiên và quy tắc xác định các số hạng tiếp theo từ các số hạng đi trước. Định nghĩa đệ quy có thể dùng để giải các bài toán đếm. Khi đó quy tắc tìm các số hạng từ các số hạng đi trước được gọi là các hệ thức truy hồi.

Định nghĩa 1: Hệ thức truy hồi (hay công thức truy hồi) đối với dãy số $\{a_n\}$ là công thức biểu diễn a_n qua một hay nhiều số hạng đi trước của dãy. Dãy số được gọi là lời giải hay nghiệm của hệ thức truy hồi nếu các số hạng của nó thỏa mãn hệ thức truy hồi này.

Ví dụ 1 (Lãi kép): Giả sử một người gửi 10.000 đô la vào tài khoản của mình tại một ngân hàng với lãi suất kép 11% mỗi năm. Sau 30 năm anh ta có bao nhiêu tiền trong tài khoản của mình?

Gọi P_n là tổng số tiền có trong tài khoản sau n năm. Vì số tiền có trong tài khoản sau n năm bằng số có sau n − 1 năm cộng lãi suất của năm thứ n, nên ta thấy dãy $\{P_n\}$ thoả mãn hệ thức truy hồi sau:

$$P_n = P_{n-1} + 0{,}11P_{n-1} = (1{,}11)P_{n-1}$$

với điều kiện đầu $P_0 = 10.000$ đô la. Từ đó suy ra $P_n = (1{,}11)^n.10.000$. Thay $n = 30$ cho ta $P_{30} = 228922{,}97$ đô la.

Ví dụ 2: Tìm hệ thức truy hồi và cho điều kiện đầu để tính số các xâu nhị phân độ dài n và không có hai số 0 liên tiếp. Có bao nhiêu xâu nhị phân như thế có độ dài bằng 5?

Gọi a_n là số các xâu nhị phân độ dài n và không có hai số 0 liên tiếp. Để nhận được hệ thức truy hồi cho $\{a_n\}$, ta thấy rằng theo quy tắc cộng, số các xâu nhị phân độ dài n và không có hai số 0 liên tiếp bằng số các xâu nhị phân như thế kết thúc bằng số 1 cộng với số các xâu như thế kết thúc bằng số 0. Giả sử $n \geq 3$.

Các xâu nhị phân độ dài n, không có hai số 0 liên tiếp kết thúc bằng số 1 chính là xâu nhị phân như thế, độ dài n − 1 và thêm số 1 vào cuối của chúng. Vậy chúng có tất cả là a_{n-1}. Các xâu nhị phân độ dài n, không có hai số 0 liên tiếp và kết thúc bằng số 0, cần phải có bit thứ n − 1 bằng 1, nếu không thì chúng có hai số 0 ở hai bit cuối cùng. Trong trường hợp này chúng có tất cả là a_{n-2}. Cuối cùng ta có được:

$$a_n = a_{n-1} + a_{n-2} \quad \text{với } n \geq 3.$$

Điều kiện đầu là $a_1 = 2$ và $a_2 = 3$. Khi đó $a_5 = a_4 + a_3 = a_3 + a_2 + a_3 = 2(a_2 + a_1) + a_2 = 13$.

b) Giải các hệ thức truy hồi:

Định nghĩa 2: Một hệ thức truy hồi tuyến tính thuần nhất bậc k với hệ số hằng số là hệ thức truy hồi có dạng:

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \ ... + c_ka_{n-k} ,$$

trong đó $c_1, c_2, ..., c_k$ là các số thực và $c_k \neq 0$.

Theo nguyên lý của quy nạp toán học thì dãy số thỏa mãn hệ thức truy hồi nêu trong định nghĩa được xác định duy nhất bằng hệ thức truy hồi này và k điều kiện đầu: $a_0 = c_0, a_1 = c_1, ..., a_{k-1} = c_{k-1}$.

Phương pháp cơ bản để giải hệ thức truy hồi tuyến tính thuần nhất là tìm nghiệm dưới dạng $a_n = r^n$, trong đó r là hằng số. Chú ý rằng $a_n = r^n$ là nghiệm của hệ thức truy hồi $a_n = c_1a_{n-1} + c_2a_{n-2} + \ ... + c_ka_{n-k}$ nếu và chỉ nếu $r^n = c_1r^{n-1} + c_2r^{n-2} + \ ... + c_kr^{n-k}$ hay $r^k - c_1r^{k-1} - c_2r^{k-2} - ... \ - c_{k-1}r - c_k = 0$.

Phương trình này được gọi là phương trình đặc trưng của hệ thức truy hồi, nghiệm của nó gọi là nghiệm đặc trưng của hệ thức truy hồi.

Mệnh đề 1: Cho $c_1, c_2, ..., c_k$ là các số thực. Giả sử rằng phương trình đặc trưng

$$r^k - c_1r^{k-1} - c_2r^{k-2} - ... \ - c_{k-1}r - c_k = 0$$

có k nghiệm phân biệt $r_1, r_2, ..., r_k$. Khi đó dãy $\{a_n\}$ là nghiệm của hệ thức truy hồi $a_n = c_1a_{n-1} + c_2a_{n-2} + ... + c_ka_{n-k}$ nếu và chỉ nếu $a_n = \alpha_1r_1^n + \alpha_2r_2^n + ... + \alpha_kr_k^n$, với n = 1, 2, ... trong đó $\alpha_1, \alpha_2, ..., \alpha_k$ là các hằng số.

Ví dụ 3: Tìm công thức hiển của các số Fibonacci.

Dãy các số Fibonacci thỏa mãn hệ thức $f_n = f_{n-1} + f_{n-2}$ và các điều kiện đầu $f_0 = 0$ và $f_1 = 1$. Các nghiệm đặc trưng là $r_1 = \frac{1+\sqrt{5}}{2}$ và $r_2 = \frac{1-\sqrt{5}}{2}$ Do đó các số Fibonacci được cho bởi công thức $f_n = \alpha_1(\frac{1+\sqrt{5}}{2})^n + \alpha_2(\frac{1-\sqrt{5}}{2})^n$. Các

điều kiện ban đầu $f_0 = 0 = \alpha_1 + \alpha_2$ và $f_1 = 1 = \alpha_1(\frac{1+\sqrt{5}}{2}) + \alpha_2(\frac{1-\sqrt{5}}{2})$. Từ hai phương trình này cho ta $\alpha_1 = \frac{1}{\sqrt{5}}$, $\alpha_2 = -\frac{1}{\sqrt{5}}$. Do đó các số Fibonacci được cho bởi công thức hiển sau:

$$f_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n.$$

Ví dụ 4: Hãy tìm nghiệm của hệ thức truy hồi $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ với điều kiện ban đầu $a_0 = 2$, $a_1 = 5$ và $a_2 = 15$.

Đa thức đặc trưng của hệ thức truy hồi này là $r^3 - 6r^2 + 11r - 6$. Các nghiệm đặc trưng là $r = 1$, $r = 2$, $r = 3$. Do vậy nghiệm của hệ thức truy hồi có dạng

$$a_n = \alpha_1 1^n + \alpha_2 2^n + \alpha_3 3^n.$$

Các điều kiện ban đầu $a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3$

$$a_1 = 5 = \alpha_1 + \alpha_2 2 + \alpha_3 3$$

$$a_2 = 15 = \alpha_1 + \alpha_2 4 + \alpha_3 9.$$

Giải hệ các phương trình này ta nhận được $\alpha_1 = 1$, $\alpha_2 = -1$, $\alpha_3 = 2$. Vì thế, nghiệm duy nhất của hệ thức truy hồi này và các điều kiện ban đầu đã cho là dãy $\{a_n\}$ với $a_n = 1 - 2^n + 2.3^n$.

3.2. Quan hệ chia để trị

a) Mở đầu:

Nhiều thuật toán đệ quy chia bài toán với các thông tin vào đã cho thành một hay nhiều bài toán nhỏ hơn. Sự phân chia này được áp dụng liên tiếp cho tới khi có thể tìm được lời giải của bài toán nhỏ một cách dễ dàng. Chẳng hạn, ta tiến hành việc tìm kiếm nhị phân bằng cách rút gọn việc tìm kiếm một phần tử trong một danh sách tới việc tìm phần tử đó trong một danh sách có độ dài giảm đi một nửa. Ta rút gọn liên tiếp như vậy cho tới khi còn lại một phần tử. Một ví dụ khác là thủ tục nhân các số nguyên. Thủ tục này rút gọn bài toán nhân hai số nguyên tới ba phép nhân hai số nguyên

với số bit giảm đi một nửa. Phép rút gọn này được dùng liên tiếp cho tới khi nhận được các số nguyên có một bit. Các thủ tục này gọi là các thuật toán chia để trị.

b) Hệ thức chia để trị:

Giả sử rằng một thuật toán phân chia một bài toán cỡ n thành a bài toán nhỏ, trong đó mỗi bài toán nhỏ có cỡ $\frac{n}{b}$ (để đơn giản giả sử rằng n chia hết cho b; trong thực tế các bài toán nhỏ thường có cỡ $[\frac{n}{b}]$ hoặc $]\frac{n}{b}[$). Giả sử rằng tổng các phép toán thêm vào khi thực hiện phân chia bài toán cỡ n thành các bài toán có cỡ nhỏ hơn là g(n). Khi đó, nếu f(n) là số các phép toán cần thiết để giải bài toán đã cho thì f thỏa mãn hệ thức truy hồi sau:

$f(n) = af(\frac{n}{b}) + g(n)$

Hệ thức này có tên là hệ thức truy hồi chia để trị.

Ví dụ 5: Thuật toán tìm kiếm nhị phân đưa bài toán tìm kiếm cỡ n về bài toán tìm kiếm phần tử này trong dãy tìm kiếm cỡ n/2, khi n chẵn. Khi thực hiện việc rút gọn cần hai phép so sánh. Vì thế, nếu f(n) là số phép so sánh cần phải làm khi tìm kiếm một phần tử trong danh sách tìm kiếm cỡ n ta có f(n) = f(n/2) + 2, nếu n là số chẵn.

Ví dụ 6: Có các thuật toán hiệu quả hơn thuật toán thông thường để nhân hai số nguyên. Ở đây ta sẽ có một trong các thuật toán như vậy. Đó là thuật toán nhân nhanh, có dùng kỹ thuật chia để trị. Trước tiên ta phân chia mỗi một trong hai số nguyên 2n bit thành hai khối mỗi khối n bit. Sau đó phép nhân hai số nguyên 2n bit ban đầu được thu về ba phép nhân các số nguyên n bit cộng với các phép dịch chuyển và các phép cộng.

Giả sử a và b là các số nguyên có các biểu diễn nhị phân độ dài 2n là:

$a = (a_{2n-1}\, a_{2n-2} \ldots a_1\, a_0)_2$ và $b = (b_{2n-1}\, b_{2n-2} \ldots b_1\, b_0)_2$.

Giả sử $a = 2^n A_1 + A_0$, $b = 2^n B_1 + B_0$, trong đó

$A_1 = (a_{2n-1}\ a_{2n-2} \ldots a_{n+1}\ a_n)_2$, $A_0 = (a_{n-1} \ldots a_1\ a_0)_2$

$B_1 = (b_{2n-1}\ b_{2n-2} \ldots b_{n+1}\ b_n)_2$, $B_0 = (b_{n-1} \ldots b_1\ b_0)_2$.

Thuật toán nhân nhanh các số nguyên dựa trên đẳng thức:

$ab = (2^{2n} + 2^n)A_1B_1 + 2^n(A_1 - A_0)(B_0 - B_1) + (2^n + 1)A_0B_0$.

Đẳng thức này chỉ ra rằng phép nhân hai số nguyên 2n bit có thể thực hiện bằng cách dùng ba phép nhân các số nguyên n bit và các phép cộng, trừ và phép dịch chuyển. Điều đó có nghĩa là nếu f(n) là tổng các phép toán nhị phân cần thiết để nhân hai số nguyên n bit thì

$f(2n) = 3f(n) + Cn$.

Ba phép nhân các số nguyên n bit cần 3f(n) phép toán nhị phân. Mỗi một trong các phép cộng, trừ hay dịch chuyển dùng một hằng số nhân với n lần các phép toán nhị phân và Cn là tổng các phép toán nhị phân được dùng khi làm các phép toán này.

Mệnh đề 2: Giả sử f là một hàm tăng thoả mãn hệ thức truy hồi $f(n) = af(\frac{n}{b}) + c$ với mọi n chia hết cho b, $a \geq 1$, b là số nguyên lớn hơn 1, còn c là số thực dương. Khi đó

$$f(n) = \begin{cases} O(n^{\log_b a}), a > 1 \\ O(\log n), a = 1 \end{cases}.$$

Mệnh đề 3: Giả sử f là hàm tăng thoả mãn hệ thức truy hồi $f(n) = af(\frac{n}{b}) + cn^d$ với mọi $n = b^k$, trong đó k là số nguyên dương, $a \geq 1$, b là số nguyên lớn hơn 1, còn c và d là các số thực dương. Khi đó

$$f(n) = \begin{cases} O(n^{\log_b a}), a > b^d \\ O(n^d \log n), a = b^d \\ O(n^d) \quad , a < b^d \end{cases}.$$

Ví dụ 7: Hãy ước lượng số phép toán nhị phân cần dùng khi nhân hai số nguyên n bit bằng thuật toán nhân nhanh.

Ví dụ 8: đã chỉ ra rằng f(n) = 3f(n/2) + Cn, khi n chẵn. Vì thế, từ *Mệnh đề 3* ta suy ra f(n) = O($n^{\log_2 3}$). Chú ý là $\log_2 3 \approx 1{,}6$. Vì thuật toán nhân thông thường dùng $O(n^2)$ phép toán nhị phân, thuật toán nhân nhanh sẽ thực sự tốt hơn thuật toán nhân thông thường khi các số nguyên là đủ lớn.

CÂU HỎI VÀ BÀI TẬP

1. Trong hình vuông có cạnh bằng 1 đặt 51 điểm bất kì phân biệt. Chứng minh rằng có ít nhất ba trong số 51 điểm đó nằm trong một hình tròn bán kính $\frac{1}{7}$.
2. Trong hình tròn có diện tích bằng 8 đặt 17 điểm bát kì phân biệt. Chứng minh rằng có ít nhất ba điểm tạo thành một tam giác có diện tích nhỏ hơn 1.
3. Trong mặt phẳng cho 2007 điểm. Biết rằng trong 3 điểm bất kì lấy từ các điểm đã cho luôn có hai điểm có khoảng cách nhỏ hơn 1. CMR có 1004 điểm nằm trong hình tròn bán kính 1.
4. Trên tờ giấy kẻ caro lấy 101 ô vuông bất kì. CMR trong 101 ô vuông đó có 26 ô vuông không chung cạnh hoặc chung đỉnh.
5. Trong tổng số 2504 sinh viên của một khoa công nghệ thông tin, có 1876 theo học môn ngôn ngữ lập trình Pascal, 999 học môn ngôn ngữ Fortran và 345 học ngôn ngữ C. Ngoài ra còn biết 876 sinh viên học cả Pascal và Fortran, 232 học cả Fortran và C, 290 học cả Pascal và C. Nếu 189 sinh viên học cả 3 môn Pascal, Fortran và C thì trong trường hợp đó có bao nhiêu sinh viên không học môn nào trong 3 môn ngôn ngữ lập trình kể trên.
6. Một cuộc họp gồm 12 người tham dự để bàn về 3 vấn đề. Có 8 người phát biểu về vấn đề I, 5 người phát biểu về vấn đề II và 7 người phát biểu về vấn đề III. Ngoài ra, có đúng 1 người không phát biểu vấn đề nào. Hỏi nhiều lắm là có bao nhiêu người phát biểu cả 3 vấn đề.
7. Chỉ ra rằng có ít nhất 4 người trong số 25 triệu người có cùng tên họ viết tắt bằng 3 chữ cái sinh cùng ngày trong năm (không nhất thiết trong cùng một năm).

8. Một tay đô vật tham gia thi đấu giành chức vô địch trong 75 giờ. Mỗi giờ anh ta có ít nhất một trận đấu, nhưng toàn bộ anh ta có không quá 125 trận. Chứng tỏ rằng có những giờ liên tiếp anh ta đã đấu đúng 24 trận.

9. Cho n là số nguyên dương bất kỳ. Chứng minh rằng luôn lấy ra được từ n số đã cho một số số hạng thích hợp sao cho tổng của chúng chia hết cho n.

10. Trong một cuộc lấy ý kiến về 7 vấn đề, người được hỏi ghi vào một phiếu trả lời sẵn bằng cách để nguyên hoặc phủ định các câu trả lời tương ứng với 7 vấn đề đã nêu.

Chứng minh rằng với 1153 người được hỏi luôn tìm được 10 người trả lời giống hệt nhau.

11. Có 17 nhà bác học viết thư cho nhau trao đổi 3 vấn đề. Chứng minh rằng luôn tìm được 3 người cùng trao đổi một vấn đề.

12. Trong kỳ thi kết thúc học phần toán học rời rạc có 10 câu hỏi. Có bao nhiêu cách gán điểm cho các câu hỏi nếu tổng số điểm bằng 100 và mỗi câu ít nhất được 5 điểm.

13. Phương trình $x_1 + x_2 + x_3 + x_4 + x_5 = 21$ có bao nhiêu nghiệm nguyên không âm?

14. Có bao nhiêu xâu khác nhau có thể lập được từ các chữ cái trong từ *MISSISSIPI*, yêu cầu phải dùng tất cả các chữ?

15. Một giáo sư cất bộ sưu tập gồm 40 số báo toán học vào 4 chiếc ngăn tủ, mỗi ngăn đựng 10 số. Có bao nhiêu cách có thể cất các tờ báo vào các ngăn nếu:

a) Mỗi ngăn được đánh số sao cho có thể phân biệt được;

b) Các ngăn là giống hệt nhau?

16. Tìm hệ thức truy hồi cho số mất thứ tự D_n.

17. Tìm hệ thức truy hồi cho số các xâu nhị phân chứa xâu 01.

18. Tìm hệ thức truy hồi cho số cách đi lên n bậc thang nếu một người có thể bước một, hai hoặc ba bậc một lần.

19. Tìm hệ thức truy hồi mà R_n thoả mãn, trong đó R_n là số miền của mặt phẳng bị phân chia bởi n đường thẳng nếu không có hai đường nào song song và không có 3 đường nào cùng đi qua một điểm.

Tính R_n bằng phương pháp lặp.

20. Tìm nghiệm của hệ thức truy hồi $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$ với $a_0 = 7$, $a_1 = -4$, $a_2 = 8$.

Chương V
ĐẠI SỐ BOOLE

MỤC TIÊU CỦA CHƯƠNG

Đại số Boole được ứng dụng phổ biến trong khoa học máy tính với tư cách là một công cụ để giải quyết nhiều vấn đề của tin học. Đại số Boole là một cấu trúc đại số trừu tượng hoá các phép toán trong logic và trong tập hợp, như các phép toán tuyển, hội, phủ định trong logic hoặc phép hợp, giao, phần bù trong tập hợp.

Chương này, người học cần nắm những kiến và kỹ năng cơ bản sau:

- Hiểu khái niệm dàn, dàn bị bù, dàn phân phối; mối quan hệ giữa tập hợp thứ tự và dàn; biết chứng minh một tập hợp thứ tự cụ thể có phải là dàn hay không.
- Hiểu khái niệm đại số Boole bằng hai tiếp cận khác nhau, một tiếp cận từ khái niệm dàn và một tiếp cận bằng cách định nghĩa trực tiếp. Người học biết cách chứng minh một tập hợp là một đại số Boole từ cả hai tiếp cận, và mối liên hệ giữa đại số Boole và tập thứ tự.
- Hiểu các khái niệm liên quan đến đại số Boole, như nguyên tử, đẳng cấu đại số Boole, đặc biệt các khái niệm trên một đại số Boole đặc biệt là đại số Boole của các hàm Boole.
- Hiểu phương trình và hệ phương trình Boole và ứng dụng của nó để tìm phủ tối tiểu trong một hệ phủ cụ thể.
- Biết các phương pháp để tối tiểu hàm Boole là phương pháp bảng Karnaugh, phương pháp thoả thuận và phương pháp Quin-McCluskey.

TÀI LIỆU THAM KHẢO

1. Đại học Cần Thơ, 2003, Bài giảng Toán rời rạc 2

2. Phạm Thế Long (chủ biên), Nguyễn Xuân Viên, Nguyễn Thiện Luân, Nguyễn Đức Hiếu, Nguyễn Văn Xuất, 2005, Toán rời rạc, NXB Đại học Sư phạm
3. Kenneth H. Rosen (Bùi Xuân Toại dịch), 2010, Toán rời rạc và những ứng dụng trong Tin học, NXB Lao động.

I. DÀN

1.1. Cận trên đúng, cận dưới đúng

Định nghĩa 1: Cho (X, S) là một tập hợp thứ tự, A là một tập con bất kì của X. Phần tử m $\in$ X được gọi là một cận trên của A nếu m trội mọi phần tử của A.

Định nghĩa 2: Cho (X, S) là một tập hợp thứ tự, B là một tập con bất kì của X. Phần tử n $\in$ X được gọi là cận dưới của B nếu n bị trội bởi mọi phần tử của B.

Định nghĩa 3: Cho (X, S) là một tập hợp thứ tự, A là một tập con bất kì của X. Phần tử $a \in X$ được gọi là cận trên đúng của A nếu a là phần tử bé nhất trong tập hợp tất cả cận trên của A. Khí đó kí hiệu $a = sup(A)$.

Định nghĩa 4: Cho (X, S) là một tập hợp thứ tự, B là một tập con bất kì của X. Phần tử $b \in X$ được gọi là cận dưới đúng của B nếu b là phần tử lớn nhất trong tập hợp tất cả các cận dưới của B. Khi đó kí hiệu $b = inf(B)$.

Chú ý:

+ Khái niệm lớn nhất, bé nhất theo nghĩa của quan hệ thứ tự S trên X.

+ Trên một tập thứ tự có thể không tồn tại cận trên đúng và cận dưới đúng của một tập con bất kì.

Ví dụ 1: Cho E = {1; 2; 3; 4}, trên tập thứ tự $(P(E), \subset)$ cho A = {{1}; {1; 2; 4}; {1; 4}} thì:

+ Tập tất cả cận trên của A là X= {{1; 2; 4}; {1; 2; 3; 4}}, phần tử bé nhất trong X là {1; 2; 4}. Vậy $sup(A)$ = {1; 2; 4}.

+ Tập hợp tất cả cận dưới của A là Y = {∅; {1}}, phần tử lớn nhất trong Y là {1}. Vậy *inf*(A) = {1}.

Ví dụ 2: Cho tập thứ tự (N, |) và B = {2; 3; 4; 5} thì:

+ Tập hợp tất cả cận trên của B là X = {60; 120;…}, phần tử bé nhất của X là 60. Vậy *sup*(B) = 60.

+ Tập hợp tất cả cận dưới của B là Y = {1}, phần tử lớn nhất của Y là 1. Vậy *inf*(B) = 1.

Ví dụ 3: Cho X = {2; 3; 4; 5}, xét tập hợp thứ tự (X, |) và A = {3;,4}. Dễ nhận thấy A không tồn tại cận trên và cận dưới nào, nên A không có cận trên đúng và cận dưới đúng.

1.2. Khái niệm dàn(Lattic)

Định nghĩa 5: Một tập hợp thứ tự (X, S) đươi gọi là một dàn nếu mọi phần tử x, y∈X đều tồn tại *sup*({x,y}) và *inf*({x,y}).

Ta còn kí hiệu: *sup*({x,y}) = x∨y và *inf*({x,y})= x∧y (đọc x tuyển y và x hội y).

Kí hiệu *sup*(X) = 1 và *inf*(X) = 0.

Ví dụ 4: Tập hợp thứ tự (U_{30},|) có ∀a, b∈ U_{30}, *sup*({a,b}) = BCNN(a,b)∈ U_{30} và *inf*({a,b}) = UCLN(a,b)∈ U_{30}. Do đó (U_{30},|) là một dàn.

Ví dụ 5: Tập hợp thứ tự (P(E),⊂) cũng là một dàn, vì A, B∈P(E) ta có *sup*({A,B}) = A∪B và *inf*({A,B}) = A∩B.

1.3. Dàn bị bù và dàn phân phối

Định nghĩa 6: Dàn (X, S) gọi là dàn bị bù nếu ∀x∈X, ∃x'∈X sao cho *sup*(x, x') = 1 và *inf*(x,x') = 0.

Định nghĩa 7: Dàn (X, S) gọi là dàn phân phối nếu ∀x, y, z∈X thoả:

x∨(y∧z) = (x∨y) ∧ (x∨z)

và x∧ (y∨z) = (x∧y) ∨ (x∧z)

Ví dụ 6: Dàn $(U_{30},|)$ là dàn phân phối, vì $\forall a, b, c \in U_{30}$, $a \vee (b \wedge c) = BCNN(a, UCLN(b,c)) = UCLN(BCNN(a,b), UCLN(a,c)) = (a \vee b) \wedge (a \vee c)$. Tương tự cũng chứng minh được $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Ví dụ 7: Dàn $(P(E),\subset)$ là dàn phân phối, vì $\forall A, B, C \in P(E)$, $A \vee (B \wedge C) = A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (tính chất của tập hợp). Tương tự cũng chứng minh được $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$.

II. ĐẠI SỐ BOOLE

2.1. Khái niệm đại số Boole

Có thể định nghĩa khái niệm đại số Boole bằng hai cách, cách thứ nhất phát triển từ khái niệm dàn và cách thứ hai định nghĩa trực tiếp.

Định nghĩa 1: Một dàn (X, S) có nhiều hơn một phần tử gọi là đại số Boole nếu (X, S) là dàn bị bù và dàn phân phối.

Ví dụ 1: Dàn $(U_{30},|)$ là một đại số Boole, vì theo chứng minh trên nó là dàn bị bù và dàn phân phối.

Ví dụ 2: Tương tự, dàn $(P(E),\subset)$ với $E \neq \varnothing$ là đại số Boole.

Định nghĩa 2: Một tập hợp X có không ít hơn hai phần tử và trên đó có hai phép toán hai ngôi $\vee$ và $\wedge$ và phép toán một ngôi - được gọi là một đại số Boole nếu thoả mãn các tính chất sau:

i) Tính kết hợp: $\forall x, y, z \in X$:

$$x \vee (y \vee z) = (x \vee y) \vee z$$

và $$x \wedge (y \wedge z) = (x \wedge y) \wedge z$$

ii) Tính giao hoán: $\forall x, y \in X$:

$$x \vee y = y \vee x$$

và $$x \wedge y = y \wedge x$$

iii) Tính phân phối: $\forall x, y, z \in X$:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

và $$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

iv) Phần tử trung hoà: Tồn tại hai phần tử trung hoà 0, $1 \in X$ sao cho $\forall x \in X$ ta có:

$x \vee 0 = x$

và $x \wedge 1 = x$

v) Phần tử bù: $\forall x \in X$, tồn tại $\bar{x} \in X$ sao cho:

$x \vee \bar{x} = 1$

và $x \wedge \bar{x} = 0$

Ví dụ 3: Cho B = {0; 1}. Trên B^n (n nguyên dương) xác định phép toán $\vee$, $\wedge$ như sau:

$x, y \in B^n$, $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$

$x \vee y = (\max(x_1,y_1), \max(x_2,y_2), \ldots, \max(x_n,y_n))$

và $x \wedge y = (\min(x_1,y_1), \min(x_2,y_2), \ldots, \min(x_n,y_n))$

Ta chứng tỏ $(B^n, \vee, \wedge)$ thoả mãn 5 tính chất của *Định nghĩa 2*:

+ Tính giao hoán (dễ dàng nhận thấy).

+ Tính kết hợp: do tính kết hợp của max và min.

+ Tính phân phối: $x, y, z \in B^n$, $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$, $z = (z_1, z_2, \ldots, z_n)$ ta có:

$x \vee (y \wedge z) = (\max(x_1, \min(y_1,z_1)), \max(x_2, \min(y_2,z_2)), \ldots, \max(x_n, \min(y_n,z_n))) = (\min(\max(x_1,y_1), \max(x_1,z_1)), \min(\max(x_2,y_2), \max(x_2,z_2)), \ldots, \min(\max(x_n,y_n), \max(x_n,z_n))) = (x \vee y) \wedge (x \vee z)$.

Tương tự, cũng chứng minh được $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

+ Phần tử trung hoà: $0 = (0, 0, \ldots, 0)$ và $1 = (1, 1, \ldots, 1)$ vì:

$0 \vee x = (\max(0,y_1), \max(0,y_2), \ldots, \max(0,y_n)) = (x_1, x_2, \ldots, x_n) = x$

$1 \wedge x = (\min(1,y_1), \min(1,y_2), \ldots, \min(1,y_n)) = (x_1, x_2, \ldots, x_n) = x$.

+ Phần tử bù: $\forall x \in B^n$, $\bar{x} = (1-x_1, 1-x_2, \ldots, 1-x_n)$, vì:

$x \vee \bar{x} = (\max(x_1,1-x_1), \max(x_2,1-x_2), \ldots, \max(x_n,1-x_n)) = (1, 1, \ldots, 1) = 1$

$x \wedge \bar{x} = (\min(x_1,1-x_1), \min(x_2,1-x_2), \ldots, \min(x_n,1-x_n)) = (0, 0,\ldots, 0) = 0$.

Ví dụ 4: Tập hợp U_{30}, U_{210} với phép tuyển là bội chung nhỏ nhất, phép hội là ước chung lớn nhất và phần tử bù của a là 30/a hoặc 210/a cũng là những đại số Boole (tự chứng minh).

2.2. Tính chất của đại số Boole

Cho đại số Boole $(X, \vee, \wedge)$.

a) Phần tử bù của phần tử $x \in X$ là duy nhất.

b) Qui tắc De Morgan: $\forall x, y \in X$ thì:

$$\overline{x \vee y} = \bar{x} \wedge \bar{y} \text{ và } \overline{x \wedge y} = \bar{x} \vee \bar{y}$$

Chứng minh: Để chứng minh $\overline{x \vee y} = \bar{x} \wedge \bar{y}$ ta cần chứng minh:

$(x \vee y) \vee (\bar{x} \wedge \bar{y}) = 1$ và $(x \vee y) \wedge (\bar{x} \wedge \bar{y}) = 0$.

Thật vậy, $(x \vee y) \vee (\bar{x} \wedge \bar{y}) = x \vee (y \vee \bar{x}) = (x \vee \bar{x}) \vee y = 1$

Và $(x \vee y) \wedge (\bar{x} \wedge \bar{y}) = (x \wedge \bar{x}) \vee (y \wedge \bar{x}) \wedge \bar{y} = (y \wedge \bar{x}) \wedge \bar{y} = 0$.

Tương tự, cũng chứng minh được $(x \vee y) \wedge (\bar{x} \wedge \bar{y}) = 0$.

c) Luật nuốt: $\forall x, y \in X$ thì:

$$x \vee (x \wedge y) = x$$

và $x \wedge (x \vee y) = x$

Chứng minh: $x \vee (x \wedge y) = (x \wedge 1) \vee (x \wedge y) = x \wedge (1 \vee y) = x \wedge 1 = x$.

Hoàn toàn tương tự, cũng chứng minh được $x \wedge (x \vee y) = x$.

d) Trong đại số Boole X, định nghĩa quan hệ $<$ như sau:

$$x < y \Leftrightarrow x \wedge y = x$$

Khi đó $<$ là một quan hệ thứ tự trên X sao cho X là một dàn bù đối với quan hệ thứ tự này. Hơn nữa, $\forall x, y \in X$ ta có:

$$sup(\{x, y\}) = x \vee y \text{ và } inf(\{x, y\}) = x \wedge y.$$

Chứng minh: Trước hết ta kiểm tra $<$ là một quan hệ thứ tự trên X. $\forall x \in X$ ta có:

$x \wedge x = (x \wedge x) \vee 0 = (x \wedge x) \vee (x \wedge \bar{x}) = x \wedge (x \vee \bar{x}) = x \wedge 1 = x.$

Nghĩa là $x < x$. Do đó $<$ có tính phản xạ.

Mặt khác, với $\forall x, y \in X$ sao cho $x < y$ và $y < x$ ta có:

$x \wedge y = x$ và $y \wedge x = y \Rightarrow x = y$. Vậy $<$ có tính phản xứng.

$\forall x, y, z \in X$ sao cho $x < y$ và $y < z$ ta có:

$x \wedge y = x$ và $y \wedge z = y$, suy ra $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$.

Nghĩa $x < z$. Do đó $<$ có tính bắc cầu. Vậy $<$ là quan hệ thứ tự trên X.

Định nghĩa 3: Phần tử *a* của đại số Boole $(X, \vee, \wedge)$ được gọi là một nguyên tử nếu *a* trội trực tiếp phần tử 0.

Ví dụ 5: Đại số Boole $(U_{30}, |)$ có các nguyên tử là 2, 3, 5.

Đại số Boole $(P(E), \subset)$ với $E = \{a; b; c\}$ có 3 nguyên tử là {a}, {b}, {c}.

Đại số Boole B^n có n nguyên tử là $e_1=(1,0,\ldots,0)$, $e_2 = (0,1,0\ldots,0),\ldots,$ $e_n = (0,0,\ldots,0,1)$.

Định nghĩa 4: Một đẳng cấu giữa hai đại số Boole X và Y là một song ánh $\varphi : X \to Y$ sao cho với mọi $x, y \in X$ ta có:

$$\varphi(x \vee y) = \varphi(x) \vee \varphi(y)$$

và $$\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$$

Ví dụ 6: Giữa các đại số Boole U_{30} và $P(\{1, 2, 3\})$ như định nghĩa trước, tồn tại đẳng cấu đại số Boole φ: $U_{30} \to P(\{1, 2, 3\})$ xác định như sau:

$1 \to \varnothing$

$2 \to \{1\}$

$3 \to \{2\}$

$5 \to \{3\}$

$6 \to \{1; 2\}$

$10 \to \{1; 3\}$

$15 \rightarrow \{2; 5\}$

$30 \rightarrow \{1; 2; 3\}$

Mệnh đề 1: Nếu $\varphi : X \rightarrow Y$ là một đẳng cấu đại số Boole thì φ cũng là đẳng cấu tập hợp có thứ tự trên X và Y, nghĩa là φ bảo tồn quan hệ thứ tự xác định bởi tính chất d). Đặc biệt, nếu 0, 1 là phần tử trung hoà của X thì $\varphi(0)$, $\varphi(1)$ là phần tử trung hoà của Y.

Chứng minh: Giả sử x, y là hai phần tử trung hoà trong X sao cho $x < y$. Khi ấy ta có:

$x \wedge y = x \Rightarrow \varphi(x) \wedge \varphi(y) = \varphi(x) \Rightarrow \varphi(x) < \varphi(y)$.

Do 0 và 1 là phần tử bé nhất và lớn nhất của X, nên $\varphi(0)$ và $\varphi(1)$ cũng là phần tử bé nhất và lớn nhất trong Y, nghĩa là chúng là các phần tử trung hoà của Y.

Định lý 1: Một đại số Boole hữu hạn X luôn đẳng cấu với đại số Boole B^n, trong đó n là một số nguyên dương, và nếu X có 2^n phần tử thì có n nguyên tử.

Chứng minh: Giả sử tập các nguyên tử của đại số Boole X là $\{a_1, a_2, \ldots, a_n\}$ và mỗi $x \in X$, $x \neq 0$ được phân tích thành tuyển các nguyên tử bị trội bởi x.

Đại số Boole B^n có 2^n phần tử. Ta lập ánh xạ φ: $X \rightarrow B^n$ như sau:

$0 \rightarrow (0, 0, \ldots, 0)$

$x \rightarrow (b_1, b_2, \ldots, b_n)$, trong đó:

$b_i = 1$ nếu a_i xuất hiện trong sự phân tích của x

$b_i = 0$ nếu a_i không xuất hiện trong sự phân tích của x.

Dễ nhận thấy φ là song ánh, do đó số phần tử của X cũng là 2^n.

Do trong B^n có nguyên tử là $a_1 = (1, 0, \ldots, 0)$, $a_2 = (0, 1, 0, \ldots, 0)$, …, $a_n = (0, 0, \ldots, 0, 1)$ nên X cũng có n nguyên tử.

Hệ quả 1: Số phần tử của một đại số Boole hữu hạn là một luỹ thừa của 2.

Hệ quả 2: Hai đại số Boole hữu hạn có cùng số phần tử thì đẳng cấu với nhau.

Định nghĩa 5: Trong đại số Boole X, một trội trực tiếp của phần tử bé nhất được gọi là một nguyên tử của X.

Ví dụ 7: Trong đại số Boole U_{30} tập các nguyên tử là {2; 3; 5}, còn trong đại số Boole P({1; 2; 3}) thì tập các nguyên tử là {{1}; {2}; {3}}.

Mệnh đề 2: Giả sử X là một đại số Boole hữu hạn với phần tử bé nhất là 0. Khi đó mọi $x \in X, x \neq 0$ đều có thể viết dưới dạng:

$$x = a_1 \vee a_2 \vee \ldots \vee a_n$$

trong đó $\{ a_1; a_2; \ldots ; a_n\}$ là tập hợp các nguyên tử bị trội bởi x.

Ví dụ 8: Trong đại số Boole U_{30}, $15 \in U_{30}$ có tập nguyên tử bị trội bởi 15 là {3; 5}, do đó $15 = 3 \vee 5 = BCNN(3, 5)$.

Trong P({1; 2; 3; 4}) $\{1; 3; 4\} \in P(\{1; 2; 3; 4\})$ có tập nguyên tử bị trội bởi {1; 3; 4} là {{1}; {3}; {4}}, nên $\{1; 3; 4\} = \{1\} \vee \{3\} \vee \{4\} = \{1\} \cup \{3\} \cup \{4\}$.

2.3. Hàm Boole và đại số Boole của các hàm Boole

a) Hàm Boole n biến:

Định nghĩa 6: Cho B^n và B là hai đại số Boole. Một ánh xạ $f: B^n \rightarrow B$ gọi là một hàm Boole n biến.

Để thuận tiện ta kí hiệu f_i bằng một xâu nhị phân 2^n bit $(b_1, b_2, \ldots, b_{2^n})$ có giá trị thập phân bằng i theo qui tắc:

$f_i(0,0,\ldots 0) = b_1$

$f_i(0,0,\ldots 1) = b_2$

.....

$f_i(1,1,\ldots 1) = b_{2^n}$

Ta kí hiệu F_n là tập hợp các hàm Boole n biến, như đã biết do |B| = 2, $|B^n|=2^n$ nên $|F_n| = 2^{2^n}$ và $F_n = \{f_0, f_1, \ldots, f_{2^{2^n}-1}\}$.

Ví dụ 9: Tập hợp các hàm Boole F_2 có thể biểu diễn như bảng sau:

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

b) Đại số Boole của các hàm Boole n biến:

Trên tập hợp F_n ta xác định các phép toán $\vee$, $\wedge$ và lấy phần tử bù như sau: $\forall f, g \in F_n$ thì:

$h = f \vee g \in F_n \Leftrightarrow \forall x \in B^n$, $h(x) = (f \vee g)(x) = f(x) \vee g(x)$

$k = f \wedge g \in F_n \Leftrightarrow \forall x \in B^n$, $h(x) = (f \wedge g)(x) = f(x) \wedge g(x)$

$\bar{f} \in F_n \Leftrightarrow \forall x \in B^n$, $\bar{f}(x) = 1 - f(x)$.

Từ tính chất của ánh xạ, dễ dàng chứng minh được F_n với các phép toán $\vee$, $\wedge$ và lấy phần tử bù như ở trên là một đại số Boole, ta gọi là đại số Boole của các hàm Boole n biến.

2.4. Dạng chuẩn của hàm Boole

a) Dạng tuyển chuẩn:

Định nghĩa 7: Trong đại số Boole F_n hàm Boole *f* tương ứng với xâu nhị phân 2^n bit chỉ có một bit 1 gọi là từ tối tiểu.

Ta nhận thấy, mỗi từ tối tiểu trong đại số Boole F_n chính là một nguyên tử trong đại số Boole tổng quát.

Ví dụ 10: Trong đại số Boole F_2 có 4 từ tối tiểu là:

$f_1 = (0, 0, 0, 1)$

$f_2 = (0, 0, 1, 0)$

$f_4 = (0, 1, 0, 0)$

$f_5 = (1, 0, 0, 0)$

Hệ quả 3: Mỗi hàm Boole f ($f \neq 0$) của đại số Boole F_n có thể được biểu diễn bằng tuyển tập từ tối tiểu bị trội bởi f, nghĩa là nếu $\{m_1, m_2, \ldots, m_k\}$ là tập các từ tối tiểu bị trội bởi f thì $f = m_1 \vee m_2 \vee \ldots \vee m_k$.

Ví dụ 11: Trong đại số Boole F_2, $f_6 = (0, 1, 1, 0)$ có tập từ tối tiểu bị trội bởi f_6 là $\{f_4; f_2\}$ nên $f_6 = f_2 \vee f_4$.

Định nghĩa 8: Trong đại số Boole F_n, mỗi hàm Boole biểu diễn bằng xâu nhị phân 2^n bit tương ứng với mỗi biến Boole hoặc bù của nó gọi là các *literal* và kí hiệu là $x_1, x_2, \ldots, x_n, \bar{x}_1, \bar{x}_2, \ldots, \overline{x}_n$.

Ví dụ 12: Trong đại số Boole F_2 có 4 từ *literal* là $f_3 = (0, 0, 1, 1) = x_1$, $f_5 = (1, 0, 0, 1) = x_2$, $f_{12} = (1, 1, 0, 0) = \overline{x}_1$, $f_6 = (0, 1, 1, 0) = \overline{x}_2$,

Định lý 2: Trong đại số Boole F_n, mỗi từ tối tiểu được biểu diễn bằng một tích của n *literal*.

Chứng minh: Nếu m là một từ tối tiểu trong F_n, theo định nghĩa tồn tại duy nhất phần tử $a = (a_1, a_2, \ldots, a_n)$ sao cho $m(a) = m(a_1, a_2, \ldots, a_n) = 1$. Khi đó ta cần chứng tỏ m được viết dưới dạng tích của các *literal*: $m = l_1.l_2 \ldots l_n$, trong đó:

$l_i = x_i$ nếu $a_i = 1$

$l_i = \overline{x}_i$ nếu $a_i = 0$ ($i = 1, 2, \ldots, n$)

Thật vật với $\forall b = (b_1, b_2, \ldots, b_n) \in B^n$, thì:

$m(b) = 1$ khi $b = a$ và $m(b) = 0$ khi $b \neq a$.

Ta xét hai trường hợp:

- Nếu mọi bit của a đều bằng 1. Khi đó $l_i(b) = x_i(b) = b_i$. Nên nếu $l_1.l_2 \ldots l_n(b) = l_1(b).l_2(b) \ldots l_n(b) = 1 \Rightarrow l_i(b) = 1 \Rightarrow b_i = 1, \forall i = 1, 2, \ldots, n \Rightarrow b = a \Rightarrow m = l_1.l_2 \ldots l_n$.

- Nếu tồn tại bit $a_i = 0$. Khi đó $l_i(b) = \overline{x}_i(b) = \bar{b}_i$. Nên nếu $l_1.l_2 \ldots l_n(b) = l_1(b).l_2(b) \ldots l_n(b) = 0 \Rightarrow \exists i: l_i(b) = 0 \Rightarrow \bar{b}_i = 0 \Rightarrow b_i = 1 \Rightarrow a_i \neq b_i \Rightarrow a \neq b \Rightarrow m(b) = 0 \Rightarrow m = l_1.l_2 \ldots l_n$.

Qui tắc viết dạng tuyển chuẩn tắc của hàm Boole f

Bước 1: Lập bảng chân trị của hàm f.

Bước 2: Mỗi a = (a_1, a_2, …, a_n) mà f(a) = 1 thì:

- Viết tích của các biến
- Đặt dấu bù lên biến mà bit tương ứng của nó bằng 0.

Bước 3: Viết f bằng tuyển (tổng) các tích vừa tìm.

Ví dụ 13: Hàm Boole f trong F_3 cho bởi bảng chân trị sau:

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Theo qui tắc trên dạng tuyển chuẩn của *f* là:

$$f = \overline{x_1}x_2x_3 \vee x_1\bar{x}_2x_3 \vee x_1x_2\bar{x}_3 \vee x_1x_2x_3$$

b) Dạng hội chuẩn tắc:

Định nghĩa 9: Hàm Boole *f* trong đại số Boole F_n được gọi là một từ tối đại khi và chỉ khi xâu nhị phân tương ứng với nó chỉ có một bit 0.

Ví dụ 14: Trong F3 có các từ tối đại như sau:

B^3	F	$\bar{f}$	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
000	0	1	0	1	1	1	1	1	1	1
001	0	1	1	0	1	1	1	1	1	1
010	0	1	1	1	0	1	1	1	1	1
011	1	0	1	1	1	0	1	1	1	1
100	0	1	1	1	1	1	0	1	1	1
101	1	0	1	1	1	1	1	0	1	1
110	1	0	1	1	1	1	1	1	0	1
110	1	0	1	1	1	1	1	1	1	0

Qui tắc viết hàm Boole dưới dạng hội chuẩn tắc:

Bước 1: Lập bảng chân trị của f.

Bước 2: Mỗi a = (a_1, a_2, …, a_n) mà f(a) = 0 thì:

- Viết tuyển (tổng) của các biến
- Đặt dấu bù lên biến mà bit tương ứng của nó bằng 1.

Bước 3: Viết *f* bằng tích (hội) các tổng vừa tìm được.

Ví dụ 15: Hàm *f* biểu diễn ở bảng có dạng hội chuẩn tắc là:

$f = M_1.M_2.M_3.M_5 =$

$(x_1 \vee x_2 \vee x_3).(x_1 \vee x_2 \bar{x}_3).(x_1 \vee \bar{x}_2 \vee x_3).(\bar{x}_1 \vee x_2 \vee x_3)$

Nhận xét: Do tính chất đối ngẫu của $\vee$ và $\wedge$ nên có thể viết hội chuẩn tắc của *f* theo hai bước:

Bước 1: Xác định tuyển chuẩn tắc của $\bar{f}$.

Bước 2: Dùng luật De Morgan để xác định $f = \bar{\bar{f}}$.

Ví dụ 16: Hàm *f* trong *Ví dụ 14* được viết dạng hội chuẩn tắc như sau:

$\bar{f} = \bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2x_3 \vee \bar{x}_1x_2\bar{x}_3 \vee x_1\bar{x}_2\bar{x}_3$

$f = \bar{\bar{f}} = \overline{\bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2x_3 \vee \bar{x}_1x_2\bar{x}_3 \vee x_1\bar{x}_2\bar{x}_3}$

$f = (x_1 \vee x_2 \vee x_3).(x_1 \vee x_2 \vee \bar{x}_3).(x_1 \vee \bar{x}_2 \vee x_3).(\bar{x}_1 \vee x_2 \vee x_3).$

2.5. Hệ phương trình Boole

a) Phương trình Boole và hệ phương trình Boole:

Định nghĩa 10: Phương trình Boole là phương trình có dạng:

G(x, y, z, …) = D(x, y, z, …) *(I)*

trong đó G(x, y, z, …) và D(x, y, z, …) là các biểu thức Boole, x, y, z, … gọi là các biến Boole.

Một nghiệm của phương trình Boole (I) là một bộ giá trị (b_1, b_2, b_3, …) thuộc B^n tương ứng với x, y, z, … sao cho khi thế vào thì (I) là đẳng thức đúng.

Định nghĩa 11: Hệ phương trình Boole là hệ có dạng:

$$\begin{cases} G_1(x,y,z,\ldots) = D_1(x,y,z,\ldots) \\ G_2(x,y,z,\ldots) = D_2(x,y,z,\ldots) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ G_m(x,y,z,\ldots) = D_m(x,y,z,\ldots) \end{cases} (II)$$

Trong đó mỗi $G_i(x,y,z,\ldots) = D_i(x,y,z,\ldots)$, *i = 1, 2, …, m*, là một phương trình Boole.

Một nghiệm của hệ *(II)* là bộ giá trị (b_1, b_2, b_3, …) tương ứng với x, y, z, … là nghiệm của mọi phương trình của hệ *(II)*.

Ví dụ 17: Hệ phương trình Boole:

$$\begin{cases} xy \vee \bar{x}z = x \vee y \\ x \vee y \vee z = xy \end{cases}$$

có nghiệm (x = 1; y = 1; z = 1) vì:

$$\begin{cases} 1.1 \vee \bar{1}.1 = 1 \vee 1 \\ 1 \vee 1 \vee 1 = 1.1 \end{cases} \Leftrightarrow \begin{cases} 1 = 1 \\ 1 = 1 \end{cases}$$

b) Phương pháp giải hệ phương trình Boole:

Để tìm tập nghiệm của hệ phương trình Boole, ta tuần tự thực hiện các bước sau:

Bước 1: Biến đổi hai vế của mỗi phương trình của hệ về dạng tuyển (sử dụng tính chất của đại số Boole).

Bước 2: Biến đổi mỗi phương trình của hệ về dạng:

$F_i(x, y, z, \ldots) = 1$

Bằng cách sử dụng công thức: $G = D \Leftrightarrow G.D \vee \bar{G}.\bar{D} = 1$.

Khi đó hệ *(II)* trở thành:

$$\begin{cases} F_1(x,y,z,\ldots) = 1 \\ F_2(x,y,z,\ldots) = 1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ F_m(x,y,z,\ldots) = 1 \end{cases} (III)$$

Bước 3: Hệ *(III)* tương đương với phương trình:

$F_1(x, y, z,\ldots).F_2(x, y, z, \ldots)\ldots.F_m(x, y, z, \ldots) = 1$ *(IV)*

Bước 4: Rút gọn biểu thức vế trái của phương trình*(IV)*, phương trình Boole có dạng:

$A_1(x, y, z,\ldots).A_2(x, y, z,\ldots)\ldots A_k(x, y, z,\ldots) = 1$ *(V)*

Trong đó mỗi A_i là một đơn thức.

Bước 5: Từ phương trình*(V)*rút ra:

$$\begin{bmatrix} A_1(x,y,z\ldots)=1 \\ A_2(x,y,z,\ldots)=1 \\ \ldots\ldots\ldots\ldots\ldots\ldots.. \\ A_k(x,y,z,\ldots)=1 \end{bmatrix}$$

Từ đó kết luận tập nghiệm của phương trình.

Ví dụ 18: Giải hệ phương trình:

$$\begin{cases} xy\vee\bar{x}z = x\vee y \\ x\vee y\vee z = xy \end{cases} \Leftrightarrow \begin{cases} [(xy\vee\bar{x}z).(x\vee y)]\vee[\overline{xy\vee\bar{x}z}.\overline{x\vee y}] = 1 \\ [(x\vee y\vee z)xy]\vee[\overline{x\vee y\vee z}.\overline{xy}] = 1 \end{cases} \Leftrightarrow$$

$$\begin{cases} [xy\vee\bar{x}yz]\vee[(\bar{x}\vee\bar{y}).(x\vee\bar{z}).(\bar{x}.\bar{y})] = 1 \\ [xy]\vee[\bar{x}.\bar{y}.\bar{z}.(\bar{x}\vee\bar{y})] = 1 \end{cases} \Leftrightarrow \begin{cases} [xy\vee\bar{x}yz]\vee\bar{x}.\bar{y}.\bar{z} = 1 \\ [xy]\vee[\bar{x}.\bar{y}.\bar{z}] = 1 \end{cases}$$

$$\Leftrightarrow \begin{cases} [xy\vee\bar{x}yz]\vee\bar{x}.\bar{y}.\bar{z} = 1 \\ [xy]\vee[\bar{x}.\bar{y}.\bar{z}] = 1 \end{cases} \Leftrightarrow (xy\vee\bar{x}yz\vee\bar{x}.\bar{y}.\bar{z}).(xy\vee\bar{x}.\bar{y}.\bar{z})=1$$

$$\Leftrightarrow xy\vee\bar{x}.\bar{y}.\bar{z} = 1 \Leftrightarrow \begin{bmatrix} xy = 1 \\ \bar{x}.\bar{y}.\bar{z} = 1 \end{bmatrix} \Leftrightarrow \begin{bmatrix} x = y = 1, z\ tuỳ\ ý \\ x = y = z = 0 \end{bmatrix}$$

c) Ứng dụng tìm phủ tối tiểu:

Người ta có thể sử dụng hệ phương trình Boole để tìm phủ tối tiểu cho một phủ.

Theo nghĩa tập hợp, một phủ của tập hợp E hữu hạn, E = {x_1; x_2; …, x_n}là một tập hợp các tập con {A_1; A_2; …; A_k}sao cho $A_i \subset$E và $\bigcup_{i=1}^{k} A_i$ = E.

Ta lập hệ phương trình Boole như sau: Đặt các biến Boole c_1, c_2,…, c_k tương ứng với các tập con A_1; A_2; …; A_k. Với mỗi phần tử $x_i \in$E, nếu $x_i \in A_{i_j}$ với *j = 1, 2, ..., h* thì lập phương trình Boole $c_{i_1} \vee c_{i_2} \vee \ldots \vee c_{i_h} = 1$.

Giải hệ phương trình Boole được thành lập như trên, nếu hệ có một nghiệm $(c_{i_1} = 1, c_{i_2} = 1, \ldots, c_{i_l=1})$ thì tương ứng ta có một phủ tối tiểu $\{A_{i_1}; A_{i_2}; \ldots; A_{i_l}\}$.

Ví dụ 19: Cho tập hợp E = {1; 2; 3; 4; 5; 6; 7; 8} và hệ phủ của E là A_1 = {1; 3; 5}, A_2 = {1; 2; 7}; A_3 = {2; 3; 5}; A_4 = {2; 4; 6; 8}; A_5 = {1;2; 4;7}. Việc tìm phủ tối tiểu cho hệ phủ trên như sau:

Ta lập bảng như sau:

	c_1	c_2	c_3	c_4	c_5
	A_1	A_2	A_3	A_4	A_5
1	x	x			x
2		x	x	x	x
3	x		x		
4				x	x
5	x		x		
6				x	
7		x			X
8				x	

Từ bảng trên lập hệ phương trình Boole:

$$\begin{cases} c_1 \vee c_2 \vee c_5 = 1 \\ c_2 \vee c_3 \vee c_4 \vee c_5 = 1 \\ c_1 \vee c_3 = 1 \\ c_4 \vee c_5 = 1 \\ c_1 \vee c_3 = 1 \\ c_4 = 1 \\ c_2 \vee c_5 = 1 \\ c_4 = 1 \end{cases} \Leftrightarrow$$

$$(c_1 \vee c_2 \vee c_5)(c_2 \vee c_3 \vee c_4 \vee c_5)(c_1 \vee c_3)(c_4 \vee c_5)(c_1 \vee c_3)c_4(c_2 \vee c_5)c_4 = 1$$

$$\Leftrightarrow (c_1 \vee c_3)(c_2 \vee c_5)c_4 = 1$$

$$\Leftrightarrow (c_1 \vee c_3)(\, c_2c_4 \vee c_4c_5) = 1$$

$$\Leftrightarrow c_1c_2c_4 \vee\, c_1c_4c_5 \vee c_2c_3c_4 \vee c_3c_4c_5 = 1$$

$$\Leftrightarrow \begin{bmatrix} c_1 = c_2 = c_4 = 1 \\ c_3 = c_4 = c_5 = 1 \\ c_1 = c_4 = c_5 = 1 \\ c_2 = c_3 = c_4 = 1 \end{bmatrix}$$

Vậy các phủ tối tiểu là $\{A_1; A_2; A_4\}$ và $\{A_3; A_4; A_5\}$, $\{A_1; A_4; A_5\}$, $\{A_2; A_3; A_4\}$.

2.6. Tối tiểu hàm Boole

Tối tiểu một hàm Boole *f* nghĩa là biến đổi tương đương hàm Boole *f* về dạng một tuyển gồm các đơn thức tối giản (đơn thức tối đại bị trội bởi f).

Nói chung quá trình tối tiểu hàm Boole có hai giai đoạn:

Giai đoạn 1: Đi tìm tập hợp các đơn thức tối giản bị trội bởi f.

Giai đoạn 2: Đi tìm phủ tối tiểu của tập hợp các đơn thức tối giản tìm được ở *Giai đoạn 1*.

Có 3 phương pháp phổ biến để tối tiểu hàm Boole:

- Phương pháp lập bảng Karnaugh
- Phương pháp thoả thuận (consensus)
- Phương pháp Quine – Mc Cluskey

Mỗi phương pháp đều có những ưu điểm và nhược điểm. Sau đây ta nghiên cứu cụ thể từng phương pháp:

a) Phương pháp bảng Karnaugh:

Để làm giảm số các số hạng trong một biểu thức Boole biểu diễn một mạch, ta cần phải tìm các số hạng để tổ hợp lại. Có một phương pháp đồ thị, gọi là bản đồ Karnaugh, được dùng để tìm các số hạng tổ hợp được đối với các hàm Boole có số biến tương đối nhỏ. Phương pháp mà ta mô tả dưới đây đã được Maurice Karnaugh đưa ra vào năm 1953. Phương pháp này dựa trên một công trình trước đó của E.W. Veitch. Các bản đồ Karnaugh cho ta một phương pháp trực quan để rút gọn các khai triển tổng các tích, nhưng chúng không thích hợp với việc cơ khí hoá quá trình này. Trước hết, ta sẽ minh hoạ cách dùng các bản đồ Karnaugh để rút gọn biểu thức của các hàm Boole hai biến.

Có bốn hội sơ cấp khác nhau trong khai triển tổng các tích của một hàm Boole có hai biến x và y. Một bản đồ Karnaugh đối với một hàm Boole hai biến này gồm bốn ô vuông, trong đó hình vuông biểu diễn hội sơ cấp có mặt trong khai triển được ghi số 1. Các hình ô được gọi là kề nhau nếu các hội sơ cấp mà chúng biểu diễn chỉ khác nhau một biến.

	y	$\bar{y}$
X	xy	x$\bar{y}$
$\bar{x}$	$\bar{x}y$	$\bar{x}\bar{y}$

Ví dụ 20: Tìm các bản đồ Karnaugh cho các biểu thức và rút gọn chúng:

a) $xy + \bar{x}y$ b) $x\bar{y} + \bar{x}y$ c) $x\bar{y} + \bar{x}y + \bar{x}\bar{y}$

Ta ghi số 1 vào ô vuông khi hội sơ cấp được biểu diễn bởi ô đó có mặt trong khai triển tổng các tích. Ba bản đồ Karnaugh được cho trên hình sau.

a)

	y	$\bar{y}$
X	1	0
$\bar{x}$	1	0

Hàm rút gọn là y = $xy + \bar{x}y$

b)

	y	$\bar{y}$
X	0	1
$\bar{x}$	1	0

Hàm này không rút gọn được nữa.

Để rút gọn khai triển tổng các tích ba biến, ta sẽ dùng bản đồ Karnaugh để nhận dạng các hội sơ cấp có thể tổ hợp lại. Các khối gồm hai ô kề nhau biểu diễn cặp các hội sơ cấp có thể được tổ hợp lại thành một tích của hai biến; các khối 2 x 2 và 4 x 1 biểu diễn các hội sơ cấp có thể tổ hợp lại thành một biến duy nhất; còn khối gồm tất cả tám ô biểu diễn một tích không có một biến nào, cụ thể đây là biểu thức 1.

Ví dụ 21: Dùng các bản đồ Karnaugh ba biến để rút gọn các khai triển tổng các tích sau:

a) $xy\bar{z} + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z,$

b) $x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z},$

c) $xyz + xy\bar{z} + x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}y\bar{z} + \bar{x}\bar{y}z$

Bản đồ Karnaugh cho những khai triển tổng các tích này được cho trong hình sau:

	Yz	$\bar{y}z$	$\bar{y}\bar{z}$	y$\bar{z}$
x	Xyz	x$\bar{y}z$	x$\bar{y}\bar{z}$	xy$\bar{z}$
$\bar{x}$	$\bar{x}yz$	$\bar{x}\bar{y}z$	$\bar{x}\bar{y}\bar{z}$	$\bar{x}$y$\bar{z}$

a)

	Yz	$\bar{y}z$	$\bar{y}\bar{z}$	y$\bar{z}$
x	0	0	1	1
$\bar{x}$	1	0	1	0

Hàm rút gọn là xyz + $\bar{y}\bar{z}$ + x$\bar{z}$

b)

	Yz	$\bar{y}z$	$\bar{y}\bar{z}$	y$\bar{z}$
x	0	1	1	0
$\bar{x}$	1	1	1	0

Hàm rút gọn là $\bar{y}$ + $\bar{x}z$

Bản đồ Karnaugh bốn biến là một hình vuông được chia làm 16 ô. Các ô này biểu diễn 16 hội sơ cấp có được. Một trong những cách lập bản đồ Karnaugh bốn biến được cho trong hình dưới đây.

	Yz	y$\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
Wx	wxyz	wxy$\bar{z}$	wx$\bar{y}\bar{z}$	wx$\bar{y}z$
$\bar{wx}$	$w\bar{x}yz$	$w\bar{x}y\bar{z}$	$w\bar{x}\bar{y}\bar{z}$	$w\bar{x}\bar{y}z$
$\bar{w}\bar{x}$	$\bar{w}\bar{x}yz$	$\bar{w}\bar{x}y\bar{z}$	$\bar{w}\bar{x}\bar{y}\bar{z}$	$\bar{w}\bar{x}\bar{y}z$
$\bar{w}x$	$\bar{w}xyz$	$\bar{w}xy\bar{z}$	$\bar{w}x\bar{y}\bar{z}$	$\bar{w}x\bar{y}z$

Hai ô được gọi là kề nhau nếu các hội sơ cấp mà chúng biểu diễn chỉ khác nhau một biến. Do đó, mỗi một ô kề với bốn ô khác. Sự rút gọn một khai triển tổng các tích bốn biến được thực hiện bằng cách nhận dạng các khối gồm 2, 4, 8 hoặc 16 ô biểu diễn các hội sơ cấp có thể tổ hợp lại được. Mỗi ô biểu diễn một hội sơ cấp hoặc được dùng để lập một tích có ít biến hơn hoặc được đưa vào trong khai triển. Cũng như trong trường hợp bản đồ Karnaugh hai và ba biến, mục tiêu là cần phải nhận dạng các khối lớn nhất có chứa các số 1 bằng cách dùng một số ít nhất các khối, mà trước hết là các khối lớn nhất.

Ví dụ 22: Rút gọn hàm Boole sau:
wxyz + wxy$\bar{z}$ + wx$\bar{y}\bar{z}$ + $w\bar{x}yz$ + $w\bar{x}\bar{y}z$ + $w\bar{x}\bar{y}\bar{z}$ +$\bar{w}x\bar{y}z$ + $\bar{w}\bar{x}yz$ + $\bar{w}\bar{x}y\bar{z}$

	yz	y$\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
Wx	1	1	1	0
$\bar{wx}$	1	0	1	1
$\bar{w}\bar{x}$	1	1	0	0
$\bar{w}x$	0	0	0	1

Hàm rút gọn là wyz + wx$\bar{z}$ + $\bar{wx}\,\bar{y}$ + $\bar{w}\bar{x}$ + $\bar{w}x\bar{y}z$

b) Phương pháp thoả thuận:

Thoả thuận: Hai đơn thức dạng xm và $\bar{x}n$ gọi là có đơn thức thoả thuận mn, kí hiệu *con*(xm, $\bar{x}n$) = mn.

Chú ý: Trong m và n lần lượt chứa 2 biến bù nhau thì thoả thuận bằng 0.

Bước 1: Biến đổi hàm Boole f về dạng tuyển (mỗi đơn thức không cần đủ các biến)

Bước 2: Gọi L là tập các đơn thức của f

Bước 3: Với mỗi biến x của hàm f, thực hiện:

- Tính A gồm các đơn thức của L chứa x
- Tính B gồm các đơn thức của L chứa $\bar{x}$
- Tính thoả thuận mỗi đơn thức trong A với mỗi đơn thức trong B.

Nếu đơn thức thoả thuận khác 0 và chưa thuộc L thì thêm vào L

- Xoá những đơn thức bị trội bởi một đơn thức khác trong L

Bước 4: Tìm phủ tối tiểu tập các đơn thức của L

Bước 5: Tuyển các đơn thức thuộc phủ tối tiểu là một đa thức rút gọn.

Ví dụ 23: Rút gọn hàm Boole f = $xz\bar{t} + \bar{x}\bar{t}v + \bar{y}zv + \bar{t}\bar{v} + yztv$

Giải: Ta có tập biến V = {x, y, z, t, v}

L = { $xz\bar{t}$, $\bar{x}\bar{t}v$, $\bar{y}zv$, $\bar{t}\bar{v}$, $yztv$ }

Với x = x :

A = { $xz\bar{t}$}, B = {$\bar{x}\bar{t}v$ }

con($xz\bar{t}$, $\bar{x}\bar{t}v$) = $z\bar{t}v$

L = { $xz\bar{t}$, $\bar{x}\bar{t}v$, $\bar{y}zv$, $\bar{t}\bar{v}$, $yztv$, $z\bar{t}v$ }

Với x = y :

A = { $yztv$}, B = {$\bar{y}zv$ }

con($yztv$, $\bar{y}zv$) = ztv

L = { $xz\bar{t}$, $\bar{x}\bar{t}v$, $\bar{y}zv$, $\bar{t}\bar{v}$, $yztv$, $z\bar{t}v$, ztv } rút gọn được L = { $xz\bar{t}$, $\bar{x}\bar{t}v$, $\bar{y}zv$, $\bar{t}\bar{v}$, $z\bar{t}v$, ztv }

Với x = z: không có thoả thuận

Với x = t:

A = { ztv }, B = { $xz\bar{t}$, $\bar{x}\bar{t}v$, $\bar{t}\bar{v}$, $z\bar{t}v$ }

con(ztv, $xz\bar{t}$) = xzv

con(ztv, $\bar{x}\bar{t}v$) = $\bar{x}zv$

con(ztv, $\bar{t}\bar{v}$) = 0

con(ztv, z$\bar{t}v$) = zv

L = { $xz\bar{t}$, $\bar{x}\bar{t}v$, $\bar{y}zv$, $\bar{t}\bar{v}$, $z\bar{t}v$, ztv, zv } rút gọn được L = { $xz\bar{t}$, $\bar{x}\bar{t}v$, $\bar{t}\bar{v}$, zv }.

Với x = v :

A = {$\bar{x}\bar{t}v$, zv }, B = { $\bar{t}\bar{v}$}

con ($\bar{x}\bar{t}v$, $\bar{t}\bar{v}$) = $\bar{x}\bar{t}$

con (zv, $\bar{t}\bar{v}$) = $z\bar{t}$

L = {$xz\bar{t}$, $\bar{x}\bar{t}v$, $\bar{t}\bar{v}$, zv, $\bar{x}\bar{t}$, $z\bar{t}$ }rút gọn được L = {$\bar{t}\bar{v}$, zv, $\bar{x}\bar{t}$, $z\bar{t}$}

Như vậy tập các đơn thức rút gọn là {$\bar{t}\bar{v}$, zv, $\bar{x}\bar{t}$, $z\bar{t}$}.

Lập hệ phương trình Boole để tìm phủ tối tiểu:

	$\bar{t}\bar{v}$(c_1)	zv(c_2)	$\bar{x}\bar{t}$(c_3)	$z\bar{t}$(c_4)
$xz\bar{t}$				+
$\bar{x}\bar{t}v$			+	
zv		+		
$\bar{t}\bar{v}$	+			
$yztv$		+		

Giải hệ phương trình Boole :

$$\begin{cases} c_4 = 1 \\ c_3 = 1 \\ c_2 = 1 \\ c_1 = 1 \end{cases} \Leftrightarrow c_1 = c_2 = c_3 = c_4 = 1$$

Do đó tập phủ tối tiểu là $\{\bar{t}\bar{v}, zv, \bar{x}\bar{t}, z\bar{t}\}$

Do đó hàm tối tiểu tìm được là f = $\bar{t}\bar{v} = zv + \bar{x}\bar{t} + \bar{x}\bar{t} + z\bar{t}$.

c) Phương pháp Quine – Mc Cluskey:

Ta đã thấy rằng các bản đồ Karnaugh có thể được dùng để tạo biểu thức cực tiểu của các hàm Boole như tổng của các tích Boole. Tuy nhiên, các bản đồ Karnaugh sẽ rất khó dùng khi số biến lớn hơn bốn. Hơn nữa, việc dùng các bản đồ Karnaugh lại dựa trên việc rà soát trực quan để nhận dạng các số hạng cần được nhóm lại. Vì những nguyên nhân đó, cần phải có một thủ tục rút gọn những khai triển tổng các tích có thể cơ khí hoá được. Phương pháp Quine-McCluskey là một thủ tục như vậy. Nó có thể được dùng cho các hàm Boole có số biến bất kỳ. Phương pháp này được W.V. Quine và E.J. McCluskey phát triển vào những năm 1950. Về cơ bản, phương pháp Quine-McCluskey có hai phần. Phần đầu là tìm các số hạng là ứng viên để đưa vào khai triển cực tiểu như một tổng các tích Boole mà ta gọi là các nguyên nhân nguyên tố. Phần thứ hai là xác định xem trong số các ứng viên đó, các số hạng nào là thực sự dùng được.

Phương pháp Quine-McCluskey tìm dạng tổng chuẩn tắc thu gọn:

Giả sử *F* là một hàm Boole n biến $x_1, x_2, \ldots, x_n$. Mỗi hội sơ cấp của n biến đó được biểu diễn bằng một dãy n ký hiệu trong bảng {0, 1, −} theo quy ước: ký tự thứ i là 1 hay 0 nếu x_i có mặt trong hội sơ cấp là bình thường hay với dấu phủ định, còn nếu x_i không có mặt thì ký tự này là −. Chẳng hạn, hội sơ cấp của 6 biến $x_1, \ldots, x_6$ là $\overline{x_1}x_3x_4\overline{x_6}$ được biểu diễn bởi 0−11−0. Hai hội sơ cấp được gọi là kề nhau nếu các biểu diễn nói trên của chúng chỉ khác nhau ở một vị trí 0, 1. Rõ ràng các hội sơ cấp chỉ có thể dán được với nhau bằng phép dán $Ax + A\bar{x} = A$ nếu chúng là kề nhau.

Thuật toán được tiến hành như sau: Lập một bảng gồm nhiều cột để ghi các kết quả dán. Sau đó lần lượt thực hiện các bước sau:

Bước 1: Viết vào cột thứ nhất các biểu diễn của các nguyên nhân hạng n của hàm Boole *F*. Các biểu diễn được chia thành từng nhóm, các biểu diễn trong mỗi nhóm có số các ký hiệu 1 bằng nhau và các nhóm xếp theo thứ tự số các ký hiệu 1 tăng dần.

Bước 2: Lần lượt thực hiện tất cả các phép dán các biểu diễn trong nhóm i với các biểu diễn trong nhóm i+1 (i=1, 2, …). Biểu diễn nào tham gia ít nhất một phép dán sẽ được ghi nhận một dấu * bên cạnh. Kết quả dán được ghi vào cột tiếp theo.

Bước 3: Lặp lại Bước 2 cho cột kế tiếp cho đến khi không thu thêm được cột nào mới. Khi đó tất cả các biểu diễn không có dấu * sẽ cho ta tất cả các nguyên nhân nguyên tố của *F*.

Ví dụ 23: Tìm dạng tổng chuẩn tắc thu gọn của các hàm Boole:

a) $F_1 = \overline{w}\overline{x}\overline{y}z + \overline{w}x\overline{y}z + \overline{w}\overline{x}yz + \overline{w}xyz + w\overline{x}yz + wxyz$,

b) $F_2 = \overline{w}\overline{x}y\overline{z} + \overline{w}\overline{x}yz + \overline{w}x\overline{y}z + wx\overline{y}\overline{z} + wx\overline{y}z + wxy\overline{z} + wxyz$.

0 0 0 1 *	0 − 0 1 *	0 − − 1		0 0 1 0 *	0 0 1 −	1 1 − −
0 1 0 1 *	0 0 − 1 *	− 0 − 1		0 0 1 1 *	− 0 1 1	
0 0 1 1 *	− 0 0 1 *	− − 1 1		1 1 0 0 *	1 1 0 − *	
1 0 0 1 *	− 0 1 1 *			1 0 1 1 *	1 1 − 0 *	
1 0 1 1 *	1 0 − 1 *			1 1 0 1 *	1 − 1 1	
0 1 1 1 *	0 1 − 1 *			1 1 1 0 *	1 1 − 1 *	
1 1 1 1 *	0 − 1 1 *			1 1 1 1 *	1 1 1 − *	
	1 − 1 1 *					
	− 1 1 1 *					

Từ các bảng trên ta có dạng tổng chuẩn tắc thu gọn của F_1 và F_2 là:

$F_1 = \overline{w}z + \overline{x}z + yz$,

$F_2 = \overline{w}\overline{x}y + \overline{x}yz + wyz + wx$.

Phương pháp Quine-McCluskey tìm dạng tổng chuẩn tắc tối thiểu:

Sau khi tìm được dạng tổng chuẩn tắc thu gọn của hàm Boole *F*, nghĩa là tìm được tất cả các nguyên nhân nguyên tố của nó, ta tiếp tục phương

pháp Quine-McCluskey tìm dạng tổng chuẩn tắc tối thiểu (cực tiểu) của *F* như sau.

Lập một bảng chữ nhật, mỗi cột ứng với một cấu tạo đơn vị của *F* (mỗi cấu tạo đơn vị là một hội sơ cấp hạng n trong dạng tổng chuẩn tắc hoàn toàn của *F*) và mỗi dòng ứng với một nguyên nhân nguyên tố của *F*. Tại ô (i, j), ta đánh dấu cộng (+) nếu nguyên nhân nguyên tố ở dòng i là một phần con của cấu tạo đơn vị ở cột j. Ta cũng nói rằng khi đó nguyên nhân nguyên tố i là phủ cấu tạo đơn vị j. Một hệ S các nguyên nhân nguyên tố của *F* được gọi là phủ hàm *F* nếu mọi cấu tạo đơn vị của *F* đều được phủ ít nhất bởi một thành viên của hệ. Dễ thấy rằng nếu hệ S là phủ hàm *F* thì nó là đầy đủ, nghĩa là tổng của các thành viên trong S là bằng *F*.

Một nguyên nhân nguyên tố được gọi là cốt yếu nếu thiếu nó thì một hệ các nguyên nhân nguyên tố không thể phủ hàm *F*. Các nguyên nhân nguyên tố cốt yếu được tìm như sau: tại những cột chỉ có duy nhất một dấu +, xem dấu + đó thuộc dòng nào thì dòng đó ứng với một nguyên nhân nguyên tố cốt yếu.

Việc lựa chọn các nguyên nhân nguyên tố trên bảng đã đánh dấu, để được một dạng tổng chuẩn tắc tối thiểu, có thể tiến hành theo các bước sau.

Bước 1: Phát hiện tất cả các nguyên nhân nguyên tố cốt yếu.

Bước 2: Xoá tất cả các cột được phủ bởi các nguyên nhân nguyên tố cốt yếu.

Bước 3: Trong bảng còn lại, xoá nốt những dòng không còn dấu + và sau đó nếu có hai cột giống nhau thì xoá bớt một cột.

Bước 4: Sau các bước trên, tìm một hệ S các nguyên nhân nguyên tố với số biến ít nhất phủ các cột còn lại.

Tổng của các nguyên nhân nguyên tố cốt yếu và các nguyên nhân nguyên tố trong hệ S sẽ là dạng tổng chuẩn tắc tối thiểu của hàm *F*.

Các bước 1, 2, 3 có tác dụng rút gọn bảng trước khi lựa chọn. Độ phức tạp chủ yếu nằm ở Bước 4. Tình huống tốt nhất là mọi nguyên nhân nguyên tố đều là cốt yếu. Trường hợp này không phải lựa chọn gì và hàm *F* có duy

nhất một dạng tổng chuẩn tắc tối thiểu cũng chính là dạng tổng chuẩn tắc thu gọn. Tình huống xấu nhất là không có nguyên nhân nguyên tố nào là cốt yếu. Trường hợp này ta phải lựa chọn toàn bộ bảng.

Ta cũng có thể tìm dạng chuẩn tắc tối tiểu bằng cách giải hệ phương trình tìm phủ tối tiểu của tập các nguyên nhân nguyên tố.

Ví dụ 24: Tìm dạng tổng chuẩn tắc tối thiểu của các hàm Boole cho trong *Ví dụ 23*.

	$\bar{w}\bar{x}\bar{y}z$	$\bar{w}x\bar{y}z$	$\bar{w}\bar{x}yz$	$w\bar{x}\bar{y}z$	$\bar{w}xyz$	$w\bar{x}yz$	$wxyz$
$\bar{w}z$	+	+	+				
$\bar{x}z$	+		+	+	+		
yz			+		+	+	+

Các nguyên nhân nguyên tố đều là cốt yếu nên dạng tổng chuẩn tắc tối thiểu của F_1 là:

$$F_1 = \bar{w}z + \bar{x}z + yz$$

	$\bar{w}\bar{x}y\bar{z}$	$\bar{w}\bar{x}yz$	$\bar{w}xyz$	$wx\bar{y}\bar{z}$	$wx\bar{y}z$	$wxy\bar{z}$	$wxyz$
wx				+	+	+	+
$\bar{w}\bar{x}y$	+	+					
$\bar{x}yz$		+	+				
wyz			+				+

Các nguyên nhân nguyên tố cốt yếu nằm ở dòng 1 và 2. Sau khi rút gọn, bảng còn dòng 3, 4 và một cột 3. Việc chọn S khá đơn giản: có thể chọn một trong hai nguyên nhân nguyên tố còn lại. Vì vậy ta được hai dạng tổng chuẩn tắc tối thiểu là:

$$F_2 = wx + \bar{w}\bar{x}y + \bar{x}yz,$$
$$F_2 = wx + \bar{w}\bar{x}y + wyz.$$

CÂU HỎI VÀ BÀI TẬP

1. Cho S là tập hợp các ước nguyên dương của 70, với các phép toán $\wedge$, $\vee$ và – được định nghĩa trên S như sau:

$$a \wedge b = UCLN(a, b),\ a \vee b = BCNN(a, b),\ \bar{a} = 70/a.$$

Chứng tỏ rằng S cùng với các phép toán $\wedge$, $\vee$ và $-$ lập thành một đại số Boole.

2. Chứng minh rằng:

a) $(a \vee b) \wedge (a \vee \bar{b}) = a$;

b) $(a \wedge b) \vee (\bar{a} \wedge c) = (a \vee c) \wedge (\bar{a} \vee b)$.

3. Cho các hàm Boole F_1, F_2, F_3 xác định bởi bảng sau:

x	y	z	F_1	F_2	F_3
0	0	0	1	1	0
0	0	1	1	0	1
0	1	0	0	1	1
0	1	1	1	1	0
1	0	0	1	0	1
1	0	1	0	0	1
1	1	0	0	1	1
1	1	1	1	1	1

Vẽ mạch thực hiện các hàm Boole này.

4. Hãy dùng các cổng NAND để xây dựng các mạch với các đầu ra như sau:

a) $\bar{x}$ b) xy c) $x+y$ d) $x \oplus y$.

5. Hãy dùng các cổng NOR để xây dựng các mạch với các đầu ra được cho trong Bài tập 4.

6. Hãy dùng các cổng NAND để dựng mạch cộng bán phần.

7. Hãy dùng các cổng NOR để dựng mạch cộng bán phần.

8. Dùng các bản đồ Karnaugh, tìm dạng tổng chuẩn tắc tối thiểu (khai triển cực tiểu) của các hàm Boole ba biến sau:

a) $F = \bar{x}yz + \bar{\bar{x}}yz$.

b) $F = xyz + xy\bar{z} + + \bar{x}yz + \bar{x}y\bar{z}$.

c) $F = xy\bar{z} + +x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z$.

d) $F = xyz + x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z}$.

9. Dùng các bản đồ Karnaugh, tìm dạng tổng chuẩn tắc tối thiểu của các hàm Boole bốn biến sau:

a) $F = wxyz + wx\bar{y}z + wx\bar{y}\bar{z} + w\bar{x}yz + w\bar{x}\bar{y}z$.

b) $F = wxy\bar{z} + wx\bar{y}z + w\bar{x}yz + w\bar{x}\bar{y}z + w\bar{x}y\bar{z} + w\bar{x}\bar{y}\bar{z}$.

c) $F = wxyz + wxy\bar{z} + wx\bar{y}z + w\bar{x}yz + w\bar{x}y\bar{z} + w\bar{x}\bar{y}z + \bar{w}xyz + \bar{w}x\bar{y}z + \bar{w}\bar{x}yz$.

d)

$F = wxyz + wxy\bar{z} + wx\bar{y}z + w\bar{x}yz + w\bar{x}y\bar{z} + w\bar{x}\bar{y}z + \bar{w}xyz + \bar{w}x\bar{y}z + \bar{w}\bar{x}yz$.

F= 1111 + 1110 + 1101 + 1011 + 1010 + 0111 + 0011 + 0010 + 0001

10. Dùng phương pháp Quine-McCluskey, thoả thuận tìm dạng tổng chuẩn tắc tối thiểu của các hàm Boole ba biến cho trong Bài tập 8 và hãy vẽ mạch thực hiện các dạng tối thiểu tìm được.

11. Dùng phương pháp Quine-McCluskey tìm dạng tổng chuẩn tắc tối thiểu của các hàm Boole bốn biến cho trong Bài tập 9 và hãy vẽ mạch thực hiện các dạng tối thiểu tìm được.

12. Dùng phương pháp thoả thuận để rút gọn các hàm Boole sau :

a) $\bar{z}(x\bar{y} \vee yt) \vee y(x\bar{z} \vee \bar{x}z)$

= $\bar{z}(x\bar{y} \vee yt) \vee y(x\bar{z} \vee \bar{x}z)$

= xyz + zyt + xyz+xyz

L = { xyz, zyt, xyz, xyz }

+ Với x =x:

A = { xyz , xyz }, B = { xyz}

Con (xyz, xyz) = 0

Con (xyz, xyz) = 0

+ Với x =y:

A = { zyt, xyz , xyz }, B ={ xyz }

Con(zyt, xyz) = xzt

Con(xyz, xyz) = xz

Con(xyz, xyz) = 0

L = { xyz, zyt, xyz, xyz , xz } rút gọn L = {zyt, xyz , xz }

+ Với x = z:

A = { xyz }, B= {zyt, xz }

con(xyz, zyt) = xyt

con(xyz, xz) =0

L = {zyt, xyz , xz , xyt }

+ Với x=t: không có thỏa thuận

Vậy tập đơn thức tối giản là: {zyt, xyz , xz , xyt }

Tìm phủ tối thiểu:

	Zyt(c1)	Xyz(c2)	Xz(c3)	Xyt(c4)
xyz			+	
Yzt	+			
xyz			+	
xyz		+		

C1=c2=c3=1

b) $xyzt \vee \bar{x}\bar{y} \vee x\bar{z}t \vee y\bar{z}\bar{t}$

c) $\bar{y}(xt \vee \bar{z}\bar{t}) \vee y(\bar{z}\bar{t} \vee xzt) \vee \bar{x}zt$

d) $xyzt \vee x\bar{y} \vee x\bar{z} \vee yz \vee xy(\bar{z} \vee \bar{t})$

e) $(x \vee t)(x \vee z)(y \vee t)(y \vee z)$

f) $yt(x \vee \bar{z}) \vee \bar{x}(\bar{z}\bar{t} \vee yt) \vee \bar{x}\bar{y}\bar{z}t$

13. Hãy giải thích làm thế nào có thể dùng các bản đồ Karnaugh để rút gọn dạng tích chuẩn tắc (tích các tổng) hoàn toàn của một hàm Boole ba biến. (Gợi ý: Đánh dấu bằng số 0 tất cả các tuyển sơ cấp trong biểu diễn và tổ hợp các khối của các tuyển sơ cấp.)

14. Dùng phương pháp ở Bài tập 12, hãy rút gọn dạng tích chuẩn tắc hoàn toàn:

$$F = (x + y + z)(x + y + \bar{z})(x + \bar{y} + z)(\bar{x} + y + z).$$

15.Tìm công thức của hàm Boole f dưới đây. Cho biết số cổng thiết kế các mạng tối ưu tổng hợp f

a) f là hàm Boole 3 biến và lấy giá trị 1 khi và chỉ khi có đúng 2 biến lấy giá trị 1.

b) f là hàm Boole 3 biến và lấy giá trị 1 khi và chỉ khi có ít nhất 2 biến lấy giá trị 1.

Chương VI

LÝ THUYẾT SỐ

MỤC TIÊU CỦA CHƯƠNG

Học xong chương này, sinh viên phải nắm được các vấn đề sau:

- Các vấn đề chia trên số nguyên; số nguyên tố và các tính chất của nó
- Ước số chung lớn nhất và bội số chung nhỏ nhất và các giải thuật
- Vận dụng lý thuyết đồng dư và các ứng dụng của lý thuyết số vào lý thuyết mật mã

TÀI LIỆU THAM KHẢO

1. Kenneth H.Rosen (Bùi Xuân Toại dịch), 2010, *Toán rời rạc và những ứng dụng trong tin học*, NXB Lao động, (chương 2, trang 155 - 266).

I. SỐ NGUYÊN VÀ PHÉP CHIA

1.1. Phép chia

Định nghĩa 1: Nếu a và b là hai số nguyên với $a \neq 0$, ta nói b chia hết cho a nếu có một số nguyên c sao cho $b = ac$. Khi b chia hết cho a ta cũng nói a là một thừa số (ước) của b và b là bội của a. Kí hiệu a|b chỉ b chia hết cho a.

Ví dụ 1: Xác định xem 3|7 và 3|12 có đúng không?

Ví dụ 2: Cho a và d là hai số nguyên dương. Có bao nhiêu số nguyên dương không lớn hơn n chia hết cho d ?

Giải : Các số nguyên dương chia hết cho d có dạng dk, trong đó k là số nguyên dương. Do đó số các số nguyên dương chia hết cho d không lớn hơn n bằng số các số nguyên k với $0 < kd \leq n$ hay $0 < k \leq n/d$. Vậy có $\lfloor n/d \rfloor$ số nguyên dương không vượt quá n chia hết cho d.

Một số tính chất của tính chất chia hết của số nguyên :

Định lí 1 : Cho a, b và c là các số nguyên. Khi đó :

1. Nếu a|b và a|c thì a| (b+c);
2. Nếu a|b thì a|bc với mọi số nguyên c;
3. Nếu a|b và b|c thì a|c.

Dễ dàng chứng mính được những tính chất này.

Mọi số nguyên lớn hơn 1 đều chia hết ít nhất cho hai số nguyên là 1 và chính nó.

Định nghĩa 2: Số nguyên dương lớn hơn 1 chỉ có đúng hai thừa số nguyên dương là 1 và chính nó gọi là số nguyên tố.

Ví dụ 3 : Số nguyên 7 là số nguyên tố, vì chí có hai thừa số dương là 1 và 7.

Định lý 2 (Định lý cơ bản của số học): Mọi số nguyên dương lớn hơn 1 đều có thể viết dưới dạng tích của các số nguyên tố một cách duy nhất, trong đó các số nguyên tố được sắp xếp theo thứ tự tăng dần.

Ví dụ 4: Các số 100, 641 và 999 được phân tích ra thừ số nguyên tố như sau :

100 = 2.2.5.5

641 = 641

999 = 3.3.3.37

Định lý 3: Nếu n là một hợp số dương lớn hơn 1, thì n có ước số nguyên tố không lớn hơn $\sqrt{n}$.

Chứng minh : Nếu n là hợp số, nó sẽ có một thừa số a với 1 < a < n. Vì vậy n = ab, trong đó a, b đều là số nguyên dương lớn hơn 1. Rõ ràng hoặc a ≤ $\sqrt{n}$, hoặc b ≤ $\sqrt{n}$.

Ví dụ 5: Chứng minh rằng 101 là số nguyên tố.

Số nguyên tố đóng vai trò đặc biệt quan trọng việc mật mã hoá. Từ lâu chúng ta đã biết số các số nguyên tô là vô hạn, nhưng làm thế nào để liệt kê tập hợp các số nguyên tố, nhưng chưa có kết quả. Khoảng 300 năm trước đây, số nguyên tố lớn nhất được biết tới là một số nguyên có dạng đặc biệt $2^p - 1$, trong đó p cũng là số nguyên tố.. Những số nguyên tố dạng này được gọi là số nguyên tố Mersenne, theo tên tu sĩ người Pháp Marin Mersenne. Từ

khi có máy tính điện tử ra đời và phát triển mạnh mẽ, người ta đã tìm ra được những số tố Mersenne rất lớn.

1.2. Thuật toán chia

Định lý 4 (Thuật toán chia): Cho a là một số nguyên và d là một số nguyên dương. Khi đó tồn tại hai số nguyên duy nhất q và r sao cho a = dq + r, với $0 \leq r < d$.

Định nghĩa 3: Trong đẳng thức ở thuật toán chia, d gọi là *số chia*, a là *số bị chia*, q là *thương số*, r là *số dư*.

Ví dụ 6: Xác định thương số và số dư khi chia 101 cho 11.

Giải : Ta có : 101 = 11.9 + 2. Do đó thương số là 9, số dư là 2.

Ví dụ 7: Xác định thương số và số dư khi chia (-11) cho 3.

Giải : Ta có -11 = 3.(-4) + 1. Do đó thương số là -4, số dư là 1.

1.3. Ước số chung lớn nhất, bội số chung nhỏ nhất

Định nghĩa 4: Cho a và b là hai số nguyên khác 0. Số nguyên d lớn nhất sao cho d|a và d|b gọi là ước số chung lớn nhất của a và b và kí hiệu ƯCLN(a,b).

Ví dụ 8: Tìm ƯCLN(24, 36).

Các ước số chung của 24 và 36 là 1, 2, 3, 4, 6, 12. Do đó ƯCLN(24, 26)=12.

Định nghĩa 5: Hai số nguyên a và b gọi là *hai số nguyên tố cùng nhau* nếu ƯCLN(a, b) = 1.

Ví dụ 9: 17 và 18 là hai số nguyên tô cùng nhau, vì ƯCLN(17, 18) = 1.

Định nghĩa 6: Các số nguyên $a_1, a_2, \ldots, a_n$ được gọi là đôi một nguyên tố cùng nhau nếu ƯCLN(a_i, a_j) = 1 với mọi $1 \leq i, j \leq n, i \neq j$.

Ví dụ 10: Xác định xem các số nguyên 10, 17, 21 có đôi một nguyên tố cùng nhau không ? Tương tự như vậy với các số nguyên 10, 19, 24 ?

Giải: Ta có ƯCLN(10, 17) = 1, ƯCLN(10, 21) = 1, ƯCLN(17, 21) = 1. Vậy 10, 17, 21 có đôi một nguyên tố cùng nhau.

Nhưng, do ƯCLN(10, 24) = 2, nên 10, 19, 24 không đôi một nguyên

tô cùng nhau.

Một cách khác để tìm ƯCLN của hai số nguyên là dùng phép phân tích thừa số nguyên tố. Giả sử a và b là hai số nguyên khác 0, được phân tích ra thừa số nguyên tô như sau :

$a = p_1^{a_1}.p_2^{a_2} \dots p_n^{a_n}$ và b= $p_1^{b_1}.p_2^{b_2} \dots p_n^{b_n}$, trong đó các số mũ là số nguyên không âm. Khi đó :

ƯCLN(a, b) = $p_1^{\min(a_1,b_1)}.p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)}$

Định lý 5: Nếu a và b là hai số nguyên dương, sẽ tồn tại các số nguyên s và t sao cho ƯCLN(a, b) = sa + tb.

Ví dụ 11: Biểu diễn ƯCLN(252, 198) = 18 dưới dạng tổ hợp tuyến tính của 252 và 198.

Giải: Sử dụng thuật toán Euclid:

252 = 1.198 + 54

198 = 3.54 + 36

54 = 1.36 + 18

36 = 2.18

Do đó 18 = 54 – 1.36 = 54 -1.(198 – 3.54) = -1.198 + 4.54

= -1.198 + 4.(252 – 1.198) = 4.252 -5.198

Định nghĩa 7: Bội chung nhỏ nhất của hai số nguyên a và b là số nguyên dương nhỏ nhất chia hết cho cả a lẫn b, và được kí hiệu BCNN(a,b).

Tương tự cách tìm ƯCLN của hai số nguyên a và b như trên, BCNN của chúng là:

BCNN(a, b) = $p_1^{\max(a_1,b_1)}.p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}$

Ví dụ 12: Xác định BCNN của $2^3.3^5.7^2$ và $2^4.3^3$

Giải : BCNN($2^3.3^5.7^2$, $2^4.3^3$) = BCNN($2^3.3^5.7^2$, $2^4.3^3.7^0$)

= $2^{\max(3,4)}.3^{\max(5,3)}.7^{\max(2,0)} = 2^4.3^5.7^2$

Ngoài ra, có thể tìm BCNN của hai số nguyên dựa vào định lý sau :

Định lý 6 : Cho a và b là hai số nguyên dương. Khi đó :

ab = ƯCLN(a, b). BCNN(a, b)

II. SỐ HỌC MÔ ĐUN

2.1. Khái niệm và tính chất

Định nghĩa 8: Cho a là một số nguyên và m là một số nguyên dương. Ta ký hiệu **a mod m** là số dư khi chia a cho m.

Như vậy, nếu a = qm + r, 0 ≤ r <m, thì a mod m = r.

Ví dụ 13: 17 mod 5 = 2, -133 mod 9 = 2, 2014 mod 101 = 95

Định nghĩa 9: Nếu a và b là hai số nguyên và m là một số nguyên dương. Khi đó a được gọi là đồng dư với b theo mô đun m nếu a – b chia hết cho m. Kí hiệu $a \equiv b(mod\ m)$.

Ví dụ 14: Xác định xem 17 có đồng dư với 5 theo mô đun 6 không? Tương tư như vậy đối với 24 và 14?

Giải: Ví 17 – 5 = 12 chia hết cho 6, nên 17 ≡ 5 (mod 6). Tuy nhiên 24 không đồng dư với 14 theo mô đun 6 (?).

Định lý 7: Cho m là một số nguyên dương. Các số nguyên a và b đồng dư theo mô đun m nếu và chỉ nếu tồn tại một số nguyên k sao cho a = b + km.

Chứng minh: Nếu a ≡ b(mod m) thì a – b chia hết cho m. Suy ra tồn tại số nguyên k sao cho a – b = km, hay a = b + km.

Ngược lại, nếu tồn tại số nguyên k sao cho a = b + km thì a – b = km. Suy ra a – b chia hết cho m, hay a ≡ b(mod m).

Định lý 8: Cho m là một số nguyên dương. Nếu a ≡ b(mod m) và c ≡ d(mod m) thì:

a + c ≡ b + d(mod m) và ac ≡ bd(mod m)

Chứng minh: Vì a ≡ b(mod m) và c ≡ d(mod m) nên tồn tại hai số nguyên s và t sao cho a = b + sm và c = d + tm. Từ đó:

a + c = (b + sm) + (d + tm) = (b + d) + (s + t)m. Vậy a + c ≡ (b + d) (mod m)

Tương tự, ac = (b + sm).(d + tm) = bd + (bt + sd + stm)m, nên ac ≡ bd

(mod m).

2.2. Biểu diễn số nguyên

Định lý 9: Cho b là số nguyên dương lớn hơn 1. Có thể biểu diễn một số n nguyên dương một cách duy nhất dưới dạng:

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

trong đó k là số nguyên không âm, $a_0, a_1, a_2, \ldots, a_k$ là các số nguyên không âm nhỏ hơn b và $a_k \neq 0$.

Biểu diễn của số n trong Định lý 8 gọi là khai triển cớ số b của n và ký hiệu $n = (a_k\, a_{k-1} \ldots a_1 a_0)_b$. Đặc biệt, khi b = 2 ta gọi là khai triển nhị phân của số nguyên.

Ví dụ 15: Tìm khai triển thập phân của số nguyên có khai triển nhị phân là $(101011111)_2$.

Giải: $(101011111)_2 = 2^8 + 2^6 + 2^4 + 2^3 + 2^2 + 2 + 1 = 351$.

Ví dụ 16: Tìm khai triển thập phân của khai triển thập lục phân $(2AEOB)_{16}$.

Thuật toán khai triển cơ số b của số n nguyên dương

```
Procedure Khai_triển_cơ_số_b(n: nguyên dương);
begin
    q:= n;
    k:= 0;
    while (q≠0)
    begin
        a_k:= q mod b;
        q:= ⌊q/b⌋;
        k:= k + 1;
    end;
end;  {n = (a_k a_{k-1} …a_1 a_0)_b }
```

2.3. Phương trình và hệ phương trình đồng dư

Định nghĩa 10: Phương trình dạng $ax \equiv b \pmod m$, trong đó m là số nguyên

dương, a và b là các số nguyên, x là biến gọi là phương trình đồng dư tuyến tính.

Định lý 10: Nếu a và m là các số nguyên tố cùng nhau (m>1), thì sẽ tồn tại và duy nhất số đảo $\bar{a}$ của a theo mô đun m, nghĩa là:

$a\bar{a}$ = 1(mod m)

Chứng minh: Vì ƯCLN(a, m) =1 nên theo *Định lý 5* tồn tại các số nguyên s và t sao cho: sa + tm = 1. Do đó sa + tm ≡ 1(mod m), vì vậy sa ≡ 1 (mod m), tức là $\bar{a}$ = s.

Ví dụ 17 : Tìm đảo của 3 theo mô đun 7.

Giải : Vì ƯCLN(3, 7) =1, nên tồn tại đảo của 3 theo mô đun 7.

7 = 2.3 + 1

Suy ra 1 = 1.7 -2.3, nghĩa là -2.3 ≡ 1(mod 7). Vậy -2 là đảo của 3 theo mô đun 7.

Ví dụ 18: Tìm nghiệm của phương trình đồng dư 3x ≡ 4(mod 7)

Giải : Trong *Ví dụ 17* ta đã biết -2 là một đảo của 3 theo mô đun 7, nên

-2.3x ≡ -2.4 (mod 7). Mà -6 ≡ 1(mod 7) và -8 ≡ 6(mod 7), nên x ≡ 6(mod7).

Định nghĩa 11 (Hệ phương trình đồng dư tuyến tính): Hệ phương trình đồng dư tuyến tính là hệ phương trình có dạng :

$$\begin{cases} a_1x \equiv b_1(mod\ m_1) \\ a_2x \equiv b_2(mod\ m_2) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_nx \equiv b_n(mod m_n) \end{cases}$$

Định lý 11 (Định lý số dư Trung hoa): Cho m_1, m_2,…, m_n là các số nguyên dương nguyên tố cùng nhau từng đôi một. Khi đó hệ phương trình :

$$\begin{cases} x \equiv b_1(mod\ m_1) \\ x \equiv b_2(mod\ m_2) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ x \equiv b_n(mod m_n) \end{cases}$$

có một nghiệm duy nhất theo mô đun m = m_1. m_2….. m_n.

Ví dụ 19: Tìm nghiệm của hệ phương trình đồng dư :

$$\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \\ x \equiv 2(mod\ 7) \end{cases}$$

Giải: Ta thấy 3, 5, 7 nguyên tố cùng nhau từng đôi một, nên theo *Định lý 11* hệ có nghiệm duy nhất.

Đặt m = 3.5.7 = 105, M_1 = m/3 = 35, M_2 = m/5 = 21, M_3 = m.7 = 15.

Ta thấy y_1 = 2 là đảo của M_1 theo mô đun 3, vì 35 ≡ 1(mod 3), y_2 = 1 là đảo của M_2, vì 21 ≡ 1(mod 5), và y_3 = 1 là đảo của M_3, vì 15 ≡ 1(mod 7).

Do đó X = $b_1M_1y_1 + b_2M_2y_2 + b_3M_3y_3$ = 2.35.2 + 3.21.1 + 2.15.1 = 233

= 23 (mod 105), nên x = 23.

Định lý 12 (Định lý nhỏ Fermat): Nếu p là số nguyên tố và a là một số nguyên không chia hết cho p, thì :

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

Ngoài ra, với mọi số a chúng ta đều có $a^p \equiv a(mod\ p)$.

III. ỨNG DỤNG CỦA LÝ THUYẾT SỐ

3.1. Mã hoá Caesar

Lý thuyết số có nhiều ứng dụng trong toán học rời rạc cũng như trong tin học. Một trong các ứng dụng của phép đồng dư liên quan đến mật mã học, một lĩnh vực nghiên cứu các thông điệp bí mật. Một trong những người sử dụng mật mã sớm nhất là Julius Caesar. Ông đã làm cho các bức thư trở thành bí mật bằng cách dịch chuyển các chữ cái ba vị trí về phía dưới trong bảng chữ cái (và chuyển ba chữ cái cuối cùng trong bảng chữ cái thành ba chữ cái đầu tiên). Ví dụ, chữ B chuyển thành chữ E, chữ X thành chữ A

Ví dụ 20: Dùng mật mã Caesar chuyển thông điệp ″MEET YOU IN THE PARK″ thành thông điệp bí mật.

Giải: Trước hết thay các chữ cái trong thông điệp bằng các con số theo vị trí của nó trong bảng chữ cái, chẳng hạn thay A bằng 0, K bằng 10 và Z

bằng 25, ta có :

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

Bây giờ thay các số p đó bằng f(p) = (p + 3) mod 26, ta có :

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13

Đổi lại thành chữ cái, ta được thông điệp bí mật ″PHHW BRX LQ WKH SDUN″.

Để phục hồi thông điệp đã được mật mã hoá theo mã Caesar thành thông điệp gốc, ta dùng hàm đảo của f là $f^{-1}(p) = (p – 3) \bmod 26$.

Ta có thể tổng quát hoá mật mã Caesar bằng cách dịch chuyển k vị trí sao cho $f(p) = (p + k) \bmod 26$ và $f^{-1}(p) = (p – k) \bmod 26$.

3.2. Mã hoá công khai

Năm 1976 tại viện MIT, ba nhà nghiên cứu Ron Rivest, Adi Shamir, và Len Adleman đã giới thiệu hệ thống mã hoá công khai gọi là hệ thống RSA. Hệ thống RSA dựa trên cơ sở mã hoá mô đun theo mô đun của tích hai số nguyên tố lớn. Mỗi người có một khoá mã gồm một mô đun n = pq, với p và q là các số nguyên tố lớn, và một số e nguyên tố cùng nhau với (p- 1)(q – 1). Để tạo ra một khoá dùng được, bạn phải tìm hai số nguyên tố lớn. Tuy nhiên, việc nhân hai số nguyên tố n = pq với xấp xỉ 400 con số, không thể thực hiện được trong một khoảng thời gian thực tế. Vì vậy, việc giải mã không thể thực hiện nhanh nếu không có một khoá giải mã riêng.

3.2.1. Mã hoá RSA

Trong phương pháp mã hoá RSA, thông điệp được diễn dịch thành những dãy số nguyên. Quá trình mã hoá được thực hiện bằng cách chuyển đổi số nguyên M biểu diễn cho văn bản thông thường (thông điệp gốc) thành số nguyên C biểu diễn cho văn bản mật mã, nhờ sử dụng hàm $C = M^e \bmod n$.

Ví dụ 21: Thực hiện mã hoá thông điệp « STOP » bằng hệ thống mật mã hoá RSA với p = 43 và q = 59 để cho n = 43.59 = 2537, và với e = 13 (ƯCLN(13, (43-1).(59-1)) =1).

Giải : Ta diễn dịch các chữ cái trong ″STOP″ thành các con số tương đương của chúng, rồi nhóm các con số đó thành các khối bốn con số là 1819

1415

Chúng ta mã hoá từng khối bằng cách ánh xạ $C = M^{13} \bmod 2537$.

Cụ thể, $1819^{13} \bmod 2537 = 2081$ và $1415^{13} \bmod 2537 = 2182$. Do đó, thông điệp mã hoá là 2081 2182.

3.2.2. Giải mã RSA

Ta có thể phục hồi thành thông điệp văn bản thông thường khi biết khoá giải mã d là số đảo mô đun e của (p – 1)(q – 1).

Nếu $de \equiv 1 \pmod{(p-1)(q-1)}$ thì tồn tại số nguyên k để $de = 1 + k(p-1)(q-1)$. Do đó $C^d = (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$.

Nói chung ƯCLN(M, p) = ƯCLN(M, q) = 1, nên theo Định lý nhỏ Fermat ta có: $M^{p-1} \equiv 1 \pmod p$ và $M^{q-1} \equiv 1 \pmod q$. Từ đó suy ra:

$C^d = M.(M^{p-1})^{k(q-1)} = M.1 \equiv 1 \pmod p$

$C^d = M.(M^{q-1})^{k(p-1)} = M.1 \equiv 1 \pmod q$

Vì ƯCLN(p, q) = 1, nên theo Định lý số dư Trung hoa ta có:

$C^d \equiv M \pmod{pq} \equiv M \pmod n$.

Ví dụ 22: Giả sử ta nhận được mật mã 0981 0461. Hãy giải mã thông điệp này nếu nó được mã hoá bằng mật mã RSA của *Ví dụ 21*.

Chọn d = 937 là số đảo mô đun 13 của 42.58 = 2436. Để giải mã một khối C ta phải tính:

$P = C^{937} \bmod 2537$

Với C = 0981, ta có $P = 0981^{937} \bmod 2537 = 0704$, và với C = 0461, ta có $P = 0461^{937} \bmod 2537 = 1115$. Do đó, phiên bản số của thông điệp gốc là 0704 1115, và tương ứng thông điệp văn bản gốc là HELP.

CÂU HỎI VÀ BÀI TẬP

1. Chứng minh rằng nếu a | b và b | a, đồng thời a và b là các số nguyên thì a = b hoặc a = -b.

2. Chứng minh rằng nếu a, b, c và d là các số nguyên và a | c và b | d thì ab | cd.
3. Các số sau có phải là số nguyên tố không ?
   a) 19 b) 27 c) 93 d) 101 e) 107 f) 113
4. 100! tận cùng bằng bao nhiêu số 0 ?
5. Tìm các số nguyên dương nhỏ hơn 12 là nguyên tố cùng nhau với 12.
6. Một số nguyên dương gọi là **hoàn hảo** nếu nó bằng tổng các ước số dương của nó (trừ bản thân chính nó).
   a) Chứng mính rằng 6 và 28 là các số hoàn hảo.
   b) Chứng mính $2^{p-1}(2^p - 1)$ là số hoàn hảo khi $2^p - 1$ là số nguyên tố.
7. Cho m là số nguyên dương. Chứng minh rằng a ≡ b (mod m) khi và chỉ khi a mod m = b mod m.
8. Kí hiệu hàm Euler ϕ(n) với n là số nguyên dương là số các số nguyên dương nhỏ hơn hoặc bằng n và nguyên tố cùng nhau với n. Tìm:
   a) ϕ(4) b) ϕ(10) c) ϕ(13)
9. Cho n là số nguyên dương. Chứng minh rằng n là số nguyên tố nếu và chỉ nếu ϕ(n) = n – 1.
10. Nếu tích của hai số nguyên là $2^7 3^8 5^3 7^{12}$ và ƯCLN của chúng là $2^3 3^4 5$, thì BCNN của chúng là bao nhiêu?
11. Chứng minh rằng nếu a ≡ b(mod m) và c ≡ d(mod m) , trong đó a, b, c, d là các số nguyên và m ≥ 2 thì a – c ≡ b – d(mod m).
12. Chứng minh rằng nếu a, b, m là các số nguyên sao cho m ≥ 2 và a ≡ b(mod m) thì ƯCLN(a,m) = ƯCLN(b,m).
13. Chứng minh rằng nếu a, b, k, và m là các số nguyên dương sao cho k ≥ 1, m ≥ 2, và a ≡ b(mod m) thì $a^k \equiv b^k$(mod m) với mọi k là số nguyên dương.
14. Ô nhớ nào sẽ được gắn bởi hàm băm h(k) = k mod 101 cho hồ sơ của sinh viên có số thẻ bảo hiểm xã hội là :
   a) 104578690 b) 432222187 c) 372201919 d) 501338753

15. Một bãi đỗ xe có 31 chỗ dành cho khách, được đánh số từ 0 đến 31. Xe của khách được gán cho chỗ đó bằng cách dùng hàm băm h(k) = k mod 31, trong đó k là một số tạo bởi 3 chữ số đầu tiên trên biển đăng ký xe của khách.

a) Xác định chỗ đỗ của xe, nếu biết 3 chữ số đầu tiên trên biển đăng ký của nó là 317, 918, 007, 100, 111, 310.

b) Mô tả thủ tục mà khách phải thực hiện theo để tìm một chỗ đỗ còn trống, khi chỗ đỗ theo quy định của họ đã bị chiếm.

16. Dùng thuật toán Euclid để tìm:

a) ƯCLN(1, 5) b) ƯCLN(100, 101) c) ƯCLN(123, 277)

d) ƯCLN(1529, 14039) e) ƯCLN(1529, 14038)

17. Biểu diễn ƯCLN của các cặp số nguyên sau đây dưới dạng tổ hợp tuyến tính của các số nguyên đó:

a) 10, 11 b) 21, 44 c) 36, 48

d)34, 55 e) 117, 213 f) 0, 223

18. Chứng tỏ 15 là một đảo của 7 mô đun 26

19. Chứng tỏ 937 là một đảo của 13 mô đun 2436

20. Giải các phương trình đồng dư:

a) $4x \equiv 5 (\text{mod } 9)$ b) $2x \equiv 7 (\text{mod } 9)$

21. Chứng minh rằng nếu p là số nguyên tố thì $x^2 \equiv 1 (\text{mod } p)$ có lời giải duy nhất là cặp số nguyên x sao cho $x \equiv 1 (\text{mod } p)$ và $x \equiv -1 (\text{mod } p)$.

22. Cho $m_1, m_2, \ldots, m_n$ là những số nguyên không nhỏ hơn 2 và nguyên tố cùng nhau từng đôi một. Chứng mính rằng nếu $a \equiv b (\text{mod } m_i)$ đối với i = 1, 2,…, n, thì $a \equiv b (\text{mod } m)$, với $m = m_1 . m_2 \ldots . m_n$.

23. Chứng minh rằng :

a) $2^{340} \equiv 1 (\text{mod } 11)$ b) $2^{340} \equiv 1 (\text{mod } 31)$

HƯỚNG DẪN GIẢI BÀI TẬP

BÀI TẬP CHƯƠNG I

Bài tập về tập hợp

4. $x \in A \Rightarrow x \notin B \Rightarrow x \in B_C$

8. Nếu $A \cap B = \varnothing \Rightarrow B \subset A_C \Rightarrow B \cap A_C = B$

10. (E-A)-(E-B) với E là tập vũ trụ

Với $x \in (E-A)-(E-B) \Rightarrow x \in (E-A)$ và $x \notin (E-B) \Rightarrow (x \in E$ và $x \notin A)$ và $(x \in B)$

$\Rightarrow x \in B$ và $x \notin A$

13.

$A^C = \{(6,0.8); (2,0.1); (7,0.5);(4,0.7); (9,0.8)\}$

$B^C = \{(6,1.0); (2,0.0); (7,0.5); (4,0.4); (9,0.9)\}$

14.

a) Tương tự câu 13.

b) $A \cap B = \{(0,1/2); (1,1/3); (2,1/4); (3,1/5);(4,1/6);(5,1/7)\}$

$\cap\{(0,1);(1,1/2);(2,1/3);(3,1/4);(4,1/5);(5,1/6)\}$

$= \{(0,1/2);(1,1/3);(2,1/4);(3,1/5);(4,1/6);(5,1/7)\}$

16. Chứng tỏ rằng tồn tại $x \in X$ có $\mu(x)<1$.

Bài tập về ánh xạ

1. 3) là ánh xạ
2. a) f là đơn ánh, f(R) = R

   b) f là đơn ánh, f(Q) = Q

   c) f là đơn ánh, f(Z) = Z

   d) f là đơn ánh, $f(R) = R^+$
3. Tương tự câu 2.
4. $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$

   $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$
5. a) $f \circ g(x) = f(g(x)) = f(3x) = 3x - 1$.

   $g \circ f(x) = g(x-1) = 3(x-1)$

b) Tương tự a)

9. a) Giả sử f không đơn ánh $\Rightarrow \exists x_1 \neq x_2 \in A$, mà $f(x_1) = f(x_2)$ khi đó $g(f(x_1)) = g(f(x_2))$. Chứng tỏ $g \circ f$ không phải đơn ánh.

b) c), d) chứng minh tương tự như a)

BÀI TẬP CHƯƠNG II

Bài tập về đại số mệnh đề

6. Anh C vô tội, anh A vô tội, chị B có tội.
7. Có 5 mệnh đề đồng thời cùng đúng là a), c), d) e), f)
8. Trước hết tìm mệnh đề sai trong 4 mệnh đề. Mệnh đề a+1 chia hết cho 3 là sai. $a = 2b + 5 \Rightarrow a+1 = 2b + 6$ chia hết cho $b \Rightarrow 6$ chia hết cho $b \Rightarrow b$ có thể là 1, 2, 3, hoặc 6. Do $a + 7b$ là nguyên tố, thế vào chỉ có b=2, b=6 là đúng.
9. c) $P \rightarrow (Q \rightarrow (P \wedge Q)) \Leftrightarrow \neg P \vee (\neg Q \vee (P \wedge Q)) \Leftrightarrow \neg P \vee (\neg Q \vee P) \Leftrightarrow (\neg P \vee P) \vee \neg Q \Leftrightarrow T \vee \neg Q \Leftrightarrow T$.

   Các câu khác biến đổi tương tự.

11. j) $(P \vee Q \vee R) \wedge (P \vee S \vee \neg Q) \wedge (P \vee \neg S \vee R) \Leftrightarrow P \vee [(Q \vee R) \wedge (S \vee \neg Q) \wedge (\neg S \vee R)]$

$\Leftrightarrow P \vee [(S \vee \neg Q) \wedge ((Q \vee R) \wedge (\neg S \vee R))]$

$\Leftrightarrow P \vee [(S \vee \neg Q) \wedge (R \vee (Q \vee \neg S))] \Leftrightarrow P \vee [R \vee (S \vee \neg Q)]$

Bài tập về suy luận toán học và các phương pháp chứng minh

2. a) Không có cơ sở

b) Có cơ sở

c) Không có cơ sở

7. Gọi P =“Môn logic là khó”, Q = “Không có nhiều sinh viên thích môn logic”, R = “Môn toán là dễ”. Giả thiết $P \vee Q \Leftrightarrow \neg Q \rightarrow P$ và $R \rightarrow \neg P \Leftrightarrow P \rightarrow \neg R$

a) $\neg Q \rightarrow \neg R$ đúng.

b) $\neg R \rightarrow Q$ đúng.

c) $R \vee P$ không đúng.

d) $\neg P \vee \neg R$ đúng.

9. a) Gọi P(n) = "$2^n < n!$"

Với n = 4 thì $2^4 = 16 < 4! = 24$ (đúng)

Giả sử $\forall n \leq k$ có P(n) đúng, nghĩa là $2^n < n!$. Ta cần chứng minh P(k+1) đúng.

Thật vậy $2^{k+1} = 2.2^k < 2.k! < (k+1).k! < (k+1)!$. Vậy P(k+1) đúng.

Tương tự cho các câu b), c), d), e).

Bài tập về vị từ, lượng từ

5. a) $\forall n \in N, (0 < n < 21) \wedge (A[n] \geq 0)$.

b) $\forall n \in N, (0 < n < 20) \wedge (A[20] \geq A[n])$

c) $\exists n, m \in N, (0 < n < m < 21) \wedge (A[m] = 2A[n])$

d) $\forall n, m \in N, (0 < n < m < 21) \wedge (A[n] \leq A[m])$

e) $\forall n, m \in N, (0 < n < m < 21) \wedge (A[n] \neq A[m])$

BÀI TẬP CHƯƠNG III

Bài tập về khái niệm của quan hệ

2. $2^{\frac{n(n+1)}{2}}$

3. a) A ={(x, y, z, t)|x=0}, B = {(x, y, z, t)|z=0}, C={(x, y, z, t)|t=0}.

$|A| = 4.7.7$, $|B| = 5.4.7$, $|C| = 5.4.7$

$|A \cap B| = 4.7$, $|A \cap C| = 4.7$, $|B \cap C| = 5.4$, $|A \cap B \cap C| = 4$

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

b) Tương tự câu a).

4. a) $|A \times B| = 9$

b) 2^9

c) 2^9

d) 2^7

Bài tập về tính chất của quan hệ

3. a) Đối xứng, không phản xạ, không bắc cầu, không phản xứng

b) Đối xứng, không phản xạ, không bắc cầu, không phản xứng

c) Không đối xứng, không phản xứng, không phản xạ, bắc cầu.

4. a) {(1,1); (2,2); (3,3);(4,4); (1,3);(3,1); (2,3);(3,2)}

b) {(1,1);(4,4); (1,3);(3,1)}

c) {(1,1);(4,4); (1,3);(3,2);(1,2)}

d) {(1,1);(2,2); (3,3);(4,4);(1,2);(3,4);(4,3)}

Bài tập về quan hệ tương đương

3. Có tính phản xạ vì $x - x = 0 \in Q$, có tính đối xứng vì $x-y \in Q \Rightarrow y-x \in Q$, có tính bắc cầu vì $x-y \in Q$ và $y-z \in Q$ thì $x-y+y-z \in Q$.

$[1] = \{x | x \in Q\}$, $[1/2] = \{x | x \in Q\}$, $[\pi] = \{\pi\}$.

4. a) $A_1 = \{1;2;3\}$, $A_2 = \{4\}$

$B_1 = \{1;2;4\}$, $B_2 = \{3\}$

$C_1 = \{2;3;4\}$, $C_2 = \{1\}$

$D_1 = \{1;3;4\}$, $D_2 = \{2\}$

Câu b), c) tương tự.

5. Chứng minh $\cup_{i,j}(A_i \cap B_j) = (\cup A_i) \cap (\cup B_j) = S \cap S = S$ và $(A_i \cap B_j) \cap (A_k \cap B_l) = \varnothing \Leftrightarrow i \neq k$ hoặc $j \neq l$.

Bài tập về quan hệ thứ tự và tập thứ tự

4. a) $S_1 = \{(x,x);(y,y)\}$, $S_2 = \{(x,x);(y,y);(x,y)\}$

b) $S_1 = \{(x,x) ;(y,y) ;(z,z)\}$, $S_2 = \{(x,x) ;(y,y) ;(z,z) ;(x,y)\}$

$S_3 = \{(x,x) ;(y,y) ;(z,z) ;(x,z)\}$; $S_4 = \{(x,x) ;(y,y) ;(z,z) ;(y,z)\}$

$S_5 = \{(x,x) ;(y,y) ;(z,z) ;(z,y)\}$;

$S_6 = \{(x,x) ;(y,y) ;(z,z) ;(x,z) ;(x,y)\}$

$S_7 = \{(x,x) ;(y,y) ;(z,z) ;(x,y) ;(y,z) ;(x,z)\}$

$S_8 = \{(x,x) ;(y,y) ;(z,z) ;(x,z) ;(z,y) ;(x,y)\}$

5. a) Chặn trên của B là {1;2 ;3}, {1;2 ;3 ;4}, {1 ;2 ;3 ;5}, {1;2 ;3 ;6}, {1 ;2 ;3 ;7},…

b) Chặn dưới của B là $\varnothing$.

BÀI TẬP CHƯƠNG IV

1. Chia hình vuông thành 25 hình vuông con nội tiếp hình tròn bán hính 1/7. Áp dụng nguyên lý Dirichlet để chứng minh cho 51 điểm chứa trong 25 hình tròn.

2. Chia hình tròn thành 8 hình quạt bằng nhau. Áp dụng nguyên lý Dirichlet để chứng minh cho 17 điểm chứa trong 8 quạt có diện tích 1.

3. Lấy điểm A trong 2007 điểm đó và xét (C) = (A, 1).

+) Nếu các điểm đều thuộc (C) thì ta có đpcm.

+) Nếu có B sao cho AB ≥ 1 thì xét (C') = (B, 1). Khi đó với mọi C trong 2005 điểm còn lại luôn xảy ra một trong các khả năng sau: $\begin{bmatrix} BC<1 \\ AC<1 \end{bmatrix}$ (vì AB ≥ 1) $\Rightarrow \begin{bmatrix} C\in(C') \\ C\in(C) \end{bmatrix}$. Từ 2005 điểm này sẽ có ít nhất 1003 điểm cùng thuộc (C) hoặc (C').

5. A = {SV học môn ngôn ngữ lập trình}

B = {SV học ngôn ngữ Fortran}

C = {SV học ngôn ngữ C}

Tính |A∩B|, |A∩C|, |B∩C|, |A∩B∩C|, rồi áp dụng nguyên lý bù trừ.

6. A = {người phát biểu vấn đề I}

B = {người phát biểu vấn đề II}

C = {người phát biểu vấn đề III}

|A∩B| <6, |A∩C| <8, |B∩C| <6, |A∩B∩C| = |A∪B∪C|-

(|A|+|B|+|C|)+(|A∩B|+|A∩C|+|B∩C|) <11 –(6+8+6)+(8+5+7) =5.

9. Giả sử n số nguyên dương là $a_1, a_2,..., a_n$. Đặt $s_1 = a_1$, $s_2=a_1+a_2$, $s3=a_1+a_2+a_3,..., s_n = a_1+a_2+a_3+...+a_n$. Khi chia s_i cho n sẽ có số dư là 0, 1,..., n-1. Nếu s_i chia n có số dư bằng 0 thì $a_1+a_2+...a_i$ chia hết cho n, ngược lại tồn tại hai số s_i, s_k (i<k) chia cho n có cùng số dư, khi đó s_k-s_i chia hết cho n.

17. $a_2 = 1$, $a_3 = 4$, $a_n = a_{n-1}+2^{n-1}-1$

18. $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_n = a_{n-3}+3$

BÀI TẬP CHƯƠNG V

1. Sử dụng *Định nghĩa 2* về đại số Boole.

2. a) Sử dụng tính chất phân phối giữa tuyển và hội.

b) (a∧b) ∨($\bar{a}$∧c) = (a∨($\bar{a}$∧c)) ∧(b∨($\bar{a}$∧c)) = (a∨c) ∧(b∨($\bar{a}$∧c)) = (a∨c) ∧ ($\bar{a}$∨b)

15. a) Lập bảng chân trị:

X	y	z	F(x, y, z)
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Từ đó xác định được hàm F. Tối tiểu hàm Boole sẽ xác định số cổng thiết kế mạng tối ưu.

b) Tương tự câu a).

TÀI LIỆU THAM KHẢO

1. Nguyễn Hữu Anh, 1999, Toán rời rạc, NXB Giáo dục
2. Đại học Cần Thơ, 2003, Bài giảng Toán rời rạc 1, 2, 3
3. Đỗ Đức Giáo, 1999, Toán rời rạc, NXB Đại học Quốc gia HN
4. Phạm Thế Long (chủ biên), Nguyễn Xuân Viên, Nguyễn Thiện Luân, Nguyễn Đức Hiếu, Nguyễn Văn Xuất, 2005, Toán rời rạc, NXB Đại học Sư phạm
5. Nguyễn Đức Nghĩa, 1997, Toán rời rạc, NXB Giáo dục
6. Kenneth H. Rosen (Bùi Xuân Toại dịch), 2010, Toán rời rạc và những ứng dụng trong Tin học, NXB Lao động
7. Seymour Lipschutz, 1964, Set theory and related topics, Mc Hraw Hill.