TRƯỜNG ĐẠI HỌC ĐÀ LẠT
KHOA TOÁN - TIN HỌC

PHẠM TIẾN SƠN

TOÁN RỜI RẠC 1

(Bài Giảng Tóm Tắt)

-- Lưu hành nội bộ --

Đà Lạt 2008

Mục lục

MỞ ĐẦU

Toán học rời rạc là một bộ phận của Toán học nhằm nghiên cứu các đối tượng rời rạc: nghiên cứu các cấu trúc rời rạc khác nhau và các phương pháp giải các vấn đề có liên quan đến các cấu trúc này.

Thông tin lưu trữ và vận hành trong máy tính dưới dạng các tín hiệu rời rạc (các máy tính liên tục chỉ là các máy tính tương tự, chuyên dụng). Vì vậy công cụ dùng để biểu diễn thông tin trong máy và xử lý các thông tin này là Toán học rời rạc.

Ngoài ra, các phương pháp và kết quả của Toán học rời rạc có thể dùng để giải quyết trực tiếp nhiều vấn đề đặt ra của Tin học như *logic, hàm đại số logic, tổ hợp trên từ...* Toán học rời rạc chuẩn bị sẵn và cung cấp các công cụ, phương pháp luận để giải quyết nhiều vấn đề của Tin học. Có thể nói Toán học rời rạc là ngành Toán học cơ sở cho Tin học.

Mục đích của giáo trình nhằm cung cấp một số công cụ Toán học để bước đầu đi vào Tin học. Giáo trình được trình bày một cách dàn trải hơn là đi sâu vào một vấn đề cụ thể. Cuối mỗi phần có các bài tập nhằm củng cố những kiến thức đã học. Hy vọng rằng giáo trình này đáp ứng được phần nào yêu cầu học tập của các bạn sinh viên.

Đà Lạt, ngày 11 tháng 2 năm 2008
Phạm Tiến Sơn

Chương 1

TẬP HỢP VÀ ÁNH XẠ

1.1 Tập hợp

1.1.1 Khái niệm

Một khái niệm cơ bản của toán học hiện đại là khái niệm *tập hợp.*

Cũng giống như điểm, đoạn thẳng, mặt phẳng, ... trong hình học Euclid, khái niệm tập hợp không được định nghĩa mà chỉ được mô tả bằng những ví dụ. Chẳng hạn, tập hợp các sách trong thư viện, tập hợp các số thực, tập hợp các đa thức bậc hai, v.v...

Các vật tạo nên một tập hợp gọi là các *phần tử* của tập hợp ấy. Có hai cách xác định một tập hợp:

(a) *Liệt kê danh sách các phần tử của nó.* Chẳng hạn, tập hợp gồm các phần tử a, b, c, d thường được viết
$$\{a, b, c, d\}.$$

(b) *Nêu lên tính chất đặc trưng của các phần tử của tập hợp.* Chẳng hạn, tập hợp $\{1, 3\}$ có thể mô tả là tập hợp hai số tự nhiên lẻ nhỏ nhất hay tập hợp các nghiệm của phương trình bậc hai $x^2 - 4x + 3 = 0$.

Ký hiệu $x \in A$ (và đọc là x thuộc A) có nghĩa x là phần tử của tập hợp A. Khi x không phải là phần tử của tập hợp A ta viết $x \notin A$ (và đọc là x không thuộc A). Chẳng hạn, nếu gọi $\mathbb{N}$ là tập các số tự nhiên thì $7 \in \mathbb{N}$ nhưng $\frac{12}{5} \notin \mathbb{N}$.

Chú ý 1. (a) Để đơn giản, đôi khi ta chỉ dùng từ "tập" thay cho cụm từ "tập hợp".

(b) Ký hiệu $:=$ thường dùng để đưa vào định nghĩa, nó thay cho cụm từ "định nghĩa bởi". Chẳng hạn, $\mathbb{N} := \{0, 1, 2, \ldots\}$.

(c) Ta thường dùng ký hiệu | để diễn đạt ý "sao cho" (hoặc "trong đó"). Chẳng hạn, tập hợp tất cả các số tự nhiên chẵn có thể mô tả như sau:

$$\{n \in \mathbb{N} \mid n \text{ chia hết cho } 2\}.$$

Ví dụ 1.1.1. Một vài tập hợp số thường gặp:

(a) Tập hợp các số tự nhiên $\mathbb{N} := \{0, 1, 2, \ldots\}$.

(b) Tập hợp các số nguyên dương $\mathbb{P} := \{1, 2, \ldots\}$.

(c) Tập hợp các số nguyên $\mathbb{Z} := \{0, 1, -1, 2, -2, \ldots\}$.

(d) Tập hợp các số hữu tỉ $\mathbb{Q} := \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$.

(e) Tập hợp các số thực $\mathbb{R}$.

(f) Tập hợp các số phức $\mathbb{C} := \{a + \sqrt{-1}b \mid a, b \in \mathbb{R}\}$.

Một tập hợp không có phần tử nào cả gọi là tập hợp *trống* (hay *rỗng*) và được ký hiệu là $\emptyset$. Chẳng hạn tập hợp gồm các nghiệm số thực của phương trình bậc hai $x^2 + 1 = 0$ là một tập hợp trống.

Tập hợp B gọi là *tập hợp con* của tập hợp A nếu mọi phần tử của tập hợp B đều là phần tử của tập hợp A; trong trường hợp này ta ký hiệu $B \subseteq A$ hay $A \supseteq B$. Hiển nhiên $A \subseteq A$. Hơn nữa, để thuận tiện, ta thường coi tập hợp trống là một tập hợp con của tập bất kỳ, tức là $\emptyset \subseteq A$ với mọi tập hợp A. Hai tập hợp A và B gọi là *bằng nhau* nếu $B \subseteq A$ và $A \subseteq B$; khi đó ta viết $A = B$. Nếu $B \subseteq A$ nhưng $A \neq B$ ta nói B là *tập hợp con thực sự* của tập hợp A và viết $B \subsetneq A$.

Ví dụ 1.1.2. (a) Nếu

$$A := \{x \in \mathbb{R} \mid x^2 + x - 6 = 0\}, \quad B := \{2, -3\}$$

thì $A = B$.

(b) Ta có các bao hàm thức thực sự sau

$$\mathbb{P} \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}.$$

Một tập hợp mà phần tử của nó là những tập hợp thường được gọi là một họ các tập hợp, hoặc một hệ các tập hợp. Nói cách khác, "tập hợp", "họ", "hệ" là những thuật ngữ đồng nghĩa.

Để nêu lên danh sách các tập hợp của một họ tập hợp $\mathcal{A}$, ta hãy gọi mỗi tập hợp của $\mathcal{A}$ là A_i; ký hiệu i được gọi là *chỉ số* để đánh dấu tập hợp ấy, hai tập hợp khác nhau của họ

$\mathcal{A}$ được đánh dấu bởi hai chỉ số khác nhau. Nếu I là tập hợp tất cả các chỉ số đã dùng để đánh dấu các tập hợp của họ $\mathcal{A}$ thì ta có thể viết

$$\mathcal{A} := \{A_i \mid i \in I\},$$

hay

$$\mathcal{A} := \{A_i\}_{i \in I}.$$

Cũng có thể sử dụng phương pháp này để đánh dấu tất cả các phần tử của một tập hợp A tùy ý.

1.1.2 Các phép toán trên tập hợp

Cho trước các tập A và B ta có thể thành lập các tập mới bằng các phép toán sau:

Định nghĩa 1.1.1. *Hợp* của hai tập A và B là một tập hợp, ký hiệu $A \cup B$, gồm tất cả các phần tử hoặc thuộc A hoặc thuộc B (hoặc thuộc cả hai).

Giao của hai tập A và B là một tập hợp, ký hiệu $A \cap B$, gồm tất cả các phần tử vừa thuộc A vừa thuộc B.

Hiệu của tập hợp A với tập hợp B là một tập hợp, ký hiệu $A \setminus B$, gồm tất cả các phần tử thuộc A nhưng không thuộc B.

Hiệu đối xứng của hai tập hợp A và B là tập hợp

$$A \,\Delta\, B := (A \setminus B) \cup (B \setminus A).$$

Nhận xét 1. (a) Một cách tương tự, có thể định nghĩa hợp $\cup_{i \in I} A_i$ và giao $\cap_{i \in I} A_i$ của một họ tập hợp $\mathcal{A} := \{A_i \mid i \in I\}$.

(b) Ta luôn có $A \,\Delta\, B = B \,\Delta\, A$. Nhưng như ví dụ dưới đây chỉ ra, nói chung $A \setminus B \neq B \setminus A$.

Ví dụ 1.1.3. Giả sử $A := \{a, b, c, d\}$ và $B := \{c, d, e\}$. Khi đó

$$\begin{aligned} A \cup B &= \{a, b, c, d, e\}, \\ A \cap B &= \{c, d\}, \\ A \setminus B &= \{a, b\}, \\ B \setminus A &= \{e\}, \\ A \,\Delta\, B &= \{a, b, e\}. \end{aligned}$$

Ví dụ 1.1.4. Giả sử A (tương ứng, B) là tập nghiệm của phương trình $x^2 - 3x + 2 = 0$

(tương ứng, $x^2 - 4x + 3 = 0$). Ta có $A = \{1, 2\}, B = \{1, 3\}$ và

$$\begin{aligned} A \cup B &= \{1, 2, 3\}, \\ A \cap B &= \{1\}, \\ A \setminus B &= \{2\}, \\ B \setminus A &= \{3\}, \\ A \,\Delta\, B &= \{2, 3\}. \end{aligned}$$

Tập nghiệm của phương trình

$$(x^2 - 3x + 2)(x^2 - 4x + 3) = 0$$

là $A \cup B = \{1, 2, 3\}$. Tập nghiệm của hệ hai phương trình

$$\begin{aligned} x^2 - 3x + 2 &= 0, \\ x^2 - 4x + 3 &= 0, \end{aligned}$$

là $A \cap B = \{1\}$.

Ví dụ 1.1.5. Giả sử

$$A_i := \{i, i + 1, \ldots\}, \quad i \in \mathbb{N}.$$

Khi đó

$$\bigcup_{i \in \mathbb{N}} A_i = \mathbb{N} \quad \text{và} \quad \bigcap_{i \in \mathbb{N}} A_i = \emptyset.$$

Các phép toán hợp và giao trên các tập hợp có những tính chất sau:

Tính chất 1.1.2. Tính giao hoán

$$\begin{aligned} A \cup B &= B \cup A, \\ A \cap B &= B \cap A. \end{aligned}$$

Tính kết hợp

$$\begin{aligned} (A \cup B) \cup C &= A \cup (B \cup C), \\ (A \cap B) \cap C &= A \cap (B \cap C). \end{aligned}$$

Tính phân phối

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C). \end{aligned}$$

Chứng minh. Bài tập. □

Nếu các tập hợp A và B có giao bằng trống, tức là nếu $A \cap B = \emptyset$, thì các tập hợp này gọi là *không có phần tử chung*, hoặc là *rời nhau.*

Thường các tập hợp được xét tới trong cùng một vấn đề đều là các bộ phận của một tập hợp X cố định nào đó. Khi ấy, tập hợp X này gọi là "không gian". Hiệu $X \setminus A$ gọi là *phần bù* của tập A và ký hiệu là A^c. Hiển nhiên A và A^c là rời nhau, $A \setminus B = A \cap B^c$. Hơn nữa

Tính chất 1.1.3. (Công thức De Morgan) *Giả sử $\{A_i\}_{i\in I}$ là họ các tập hợp con của không gian X. Khi đó*

$$\begin{aligned}\left(\bigcup_{i\in I} A_i\right)^c &= \bigcap_{i\in I}(A_i)^c,\\ \left(\bigcap_{i\in I} A_i\right)^c &= \bigcup_{i\in I}(A_i)^c.\end{aligned}$$

Chứng minh. Bài tập. □

Định nghĩa 1.1.4. Họ các tập hợp $\mathcal{A} := \{A_i \mid i \in I\}$ gọi là *phủ* của tập X nếu $X = \cup_{i\in I} A_i$. Nếu ngoài ra $A_i \neq \emptyset$ với mọi $i \in I$ và $A_i \cap A_j = \emptyset$ với mọi $i, j \in I, i \neq j$, thì ta nói $\mathcal{A}$ là một *phân hoạch* của tập X.

Ví dụ 1.1.6. Đặt A_1 (tương ứng, A_2) là tập các số nguyên chẵn (tương ứng, lẻ). Khi đó $\{A_1, A_2\}$ là một phân hoạch của tập các số nguyên $\mathbb{Z}$.

1.1.3 Tích Descartes

Tích Descartes, hay vắn tắt *tích,* của các tập hợp $A_i, i \in I$, là một tập hợp, ký hiệu là

$$\prod_{i\in I} A_i,$$

được xác định như sau: tất cả các phần tử của nó có dạng $x := (x_i)_{i\in I}$ với $x_i \in A_i$. Khi đó, x_i gọi là *thành phần* (hay *tọa độ*) thứ i của x.

Tích của một số hữu hạn các tập hợp $A_i, i = 1, 2, \ldots, n$, thường được ký hiệu là

$$\prod_{i=1}^{n} A_i \quad \text{hoặc} \quad A_1 \times A_2 \times \cdots \times A_n.$$

Mỗi phần tử của tích này là một vector $(x_1, x_2, \ldots, x_n)$ với $x_i \in A_i, i = 1, 2, \ldots, n$. Nói cách khác

$$\prod_{i=1}^{n} A_i = \{(x_1, x_2, \ldots, x_n) \mid x_i \in A_i, i = 1, 2, \ldots, n\}.$$

Nếu $A_1 = A_2 = \cdots = A_n = A$ thì tích $A \times A \times \cdots \times A$ (A có mặt n lần) thường được ký hiệu là A^n.

Chú ý rằng, nói chung, $A \times B \neq B \times A$. Dĩ nhiên $A \times \emptyset = \emptyset$.

Ví dụ 1.1.7. Giả sử $A := \{1, 2\}, B = \{a, b, c\}$. Khi đó

$$\begin{aligned} A \times B &= \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}, \\ B \times A &= \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}, \\ A \times A &= \{(1,1),(1,2),(2,1),(2,2)\}. \end{aligned}$$

Bài tập

1. Giả sử $X := \{1, 2, \ldots, 10\}$. Đặt $A := \{1, 4, 7, 10\}, B := \{1, 2, 3, 4, 5\}$ và $C := \{2, 4, 6, 8\}$. Liệt kê các phần tử của mỗi tập hợp sau:

   (a) $A \cup B$.

   (b) $B \cup C$.

   (c) $A \cap B$.

   (d) $B \cap C$.

   (e) $A \setminus B$.

   (f) A^c.

   (g) $(B^c \cap (C \setminus A))$.

   (h) $(A \cap B)^c \cup C$.

   (i) $B \setminus A$.

   (j) $A \cap (B \cup C)$.

   (k) $((A \cap B) \setminus C)$.

   (l) $(A \cap B) \setminus (C \setminus B)$.

2. Giả sử $X := \{1, 2, 3\}$ và $Y := \{x, y\}$. Liệt kê các phần tử của mỗi tập hợp sau:

   (a) X^2.

   (b) $X \times Y$.

   (c) $Y \times X$.

   (d) Y^3.

3. Liệt kê tất cả các phân hoạch của các tập hợp sau:

   (a) $\{1\}$.

   (b) $\{1, 2\}$.

(c) $\{a, b, c\}$.

(d) $\{a, b, c, d\}$.

4. Xác định mối quan hệ giữa các cặp tập hợp sau:

   (a) $\{1, 2, 3\}$ và $\{1, 3, 2\}$.

   (b) $\{1, 2, 2, 3\}$ và $\{1, 2, 3\}$.

   (c) $\{1, 1, 3\}$ và $\{3, 3, 1\}$.

   (d) $\{x \in \mathbb{R} \mid x^2 + x = 2\}$ và $\{1, -2\}$.

   (e) $\{x \in \mathbb{R} \mid 0 < x \leq 2\}$ và $\{1, 2\}$.

5. Ký hiệu $\mathcal{P}(X)$ là tập hợp mà các phần tử của nó là các tập con của X. Liệt kê tất cả các phần tử của $\mathcal{P}(\{a, b\})$ và $\mathcal{P}(\{a, b, c\})$.

6. Giả sử X có 10 phần tử. Có bao nhiêu tập hợp con thực sự của tập hợp X? Tổng quát?

7. Giả sử X và Y là các tập hợp khác trống sao cho $X \times Y = Y \times X$. Các tập hợp X và Y phải thỏa những điều kiện gì?

8. Chứng minh hoặc cho phản ví dụ các quan hệ (A, B, C là những tập hợp con của tập hợp X) sau:

   (a) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

   (b) $(A \setminus B) \cap (B \setminus A) = \emptyset$.

   (c) $A \setminus (B \cup C) = (A \setminus B) \cup C$.

   (d) $(A \setminus B)^c = (B \setminus A)^c$.

   (e) $(A \cap B)^c \subseteq A$.

   (f) $(A \cap B) \cup (B \setminus A) = A$.

   (g) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

   (h) $(A \times B)^c = A^c \times B^c$.

9. Đẳng thức nào dưới đây là đúng?

   (a) $A \cap B = A$.

   (b) $A \cup B = A$.

   (c) $(A \cap B)^c = B^c$.

10. Tìm hiệu đối xứng của hai tập hợp $A := \{1, 2, 3\}$ và $B := \{2, 3, 4, 5\}$.

11. Giả sử C là một đường tròn và $\mathcal{A}$ là tập tất cả các đường kính của đường tròn C. Xác định $\cap_{A \in \mathcal{A}} A$.

12. Ký hiệu $\mathbb{P}$ là tập hợp tất cả các số nguyên lớn hơn 1. Với mỗi số tự nhiên $i \geq 2$, đặt

$$A_i := \{ik \mid k \geq 2, k \in \mathbb{P}\}.$$

Mô tả tập hợp $\mathbb{P} \setminus \bigcup_{i=2}^{\infty} A_i$.

13. Chứng minh các đẳng thức sau (giả sử các tập đu ợc xét đều là tập con của tập X nào đó):

$$\begin{aligned} A \cap (A_1 \cup A_2 \cup \cdots \cup A_n) &= (A \cap A_1) \cup (A \cap A_2) \cup \cdots \cup (A \cap A_n). \\ (A_1 \cap A_2 \cap \cdots \cap A_n)^c &= A_1^c \cup A_2^c \cup \cdots \cup A_n^c. \end{aligned}$$

1.2 Ánh xạ

1.2.1 Định nghĩa và tính chất

Một khái niệm cơ bản khác của toán học hiện đại là khái niệm *ánh xạ,* mở rộng khái niệm hàm số.

Định nghĩa 1.2.1. Cho X và Y là hai tập hợp bất kỳ. Một *ánh xạ* (hay hàm số) từ tập hợp X vào tập hợp Y là một tương ứng mỗi phần tử của X một phần tử xác định của Y.

Giả sử f là một ánh xạ từ tập hợp X vào tập hợp Y. Khi đó ta viết $f\colon X \to Y$; nếu $x \in X$ thì $f(x)$ chỉ phần tử của Y tương ứng với phần tử x đó và ta viết $x \mapsto f(x)$; phần tử $f(x)$ gọi là *ảnh* của phần tử x qua ánh xạ f, hay là giá trị của hàm f tại x. Tập hợp

$$\{(x, y) \in X \times Y \mid y = f(x)\}$$

gọi là *đồ thị của ánh xạ* f và ký hiệu là $\text{graph}(f)$.

Ví dụ 1.2.1. Tương ứng mỗi số thực x với một số thực x^3 cho ta một ánh xạ $f\colon \mathbb{R} \to \mathbb{R}, x \mapsto x^3$.

Cho trước một tập hợp $A \subseteq X$ thì tập hợp

$$f(A) := \{f(x) \mid x \in A\}$$

gọi là *ảnh* của tập hợp A qua ánh xạ f. Đặc biệt, tập hợp $f(X)$ gọi là *miền giá trị* của f.

Dễ dàng chứng minh rằng:

Tính chất 1.2.2. *Giả sử $f\colon X \to Y$ là một ánh xạ từ tập hợp X vào tập hợp Y. Khi đó*

(a) Nếu $A \subset B \subset X$ thì $f(A) \subset f(B)$.

(b) Nếu $A_i, i \in I$, là một họ các tập hợp con của tập hợp X thì

$$\begin{aligned} f\left(\bigcup_{i\in I} A_i\right) &= \bigcup_{i\in I} f\left(A_i\right), \\ f\left(\bigcap_{i\in I} A_i\right) &\subset \bigcap_{i\in I} f\left(A_i\right). \end{aligned}$$

Để ý rằng, nói chung đẳng thức sau

$$f\left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} f\left(A_i\right)$$

không đúng.

Định nghĩa 1.2.3. Giả sử $f\colon X \to Y$ là một ánh xạ từ tập hợp X vào tập hợp Y.

(a) Ánh xạ f gọi là *một-một* (hoặc *đơn ánh*) nếu với mọi $x, x' \in X$ mà $x \neq x'$ thì $f(x) \neq f(x')$.

(b) f gọi là *ánh xạ lên* (hoặc *toàn ánh*) nếu $f(X) = Y$.

(c) f gọi là *một-một lên* (hoặc *song ánh*) nếu f đồng thời là một-một và là lên; nói cách khác, với mỗi phần tử $y \in Y$ có duy nhất một phần tử $x \in X$ sao cho $f(x) = y$.

Ví dụ 1.2.2. (a) Ánh xạ

$$f\colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto \sin x,$$

là một-một nhưng không là ánh xạ lên.

(b) Ánh xạ[1]

$$g\colon \mathbb{R} \to \mathbb{N}, \quad x \mapsto [x],$$

là lên nhưng không là ánh xạ một-một.

(c) Ánh xạ

$$h\colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^3,$$

là một-một và lên.

Với một ánh xạ tùy ý $f\colon X \to Y$ và với một tập hợp $B \subseteq Y$, tập hợp

$$\{x \in X \mid f(x) \in B\}$$

gọi là *nghịch ảnh* của tập hợp B qua ánh xạ f và được ký hiệu là $f^{-1}(B)$. Rõ ràng $f^{-1}(Y) = X$ và $f^{-1}(\emptyset) = \emptyset$, nhưng có thể xảy ra rằng $\emptyset \neq B \subset Y$ và $f^{-1}(B) = \emptyset$.

[1] *Phần nguyên* của số thực x, ký hiệu $[x]$, là số nguyên lớn nhất không vượt quá x.

Nếu tập hợp $B \subset Y$ chỉ gồm có một phần tử y, tức là $B = \{y\}$, thì thay cho ký hiệu $f^{-1}(\{y\})$ ta thường ký hiệu vắn tắt là $f^{-1}(y)$.

Dễ dàng chứng minh rằng:

Tính chất 1.2.4. *Giả sử $f\colon X \to Y$ là một ánh xạ từ tập hợp X vào tập hợp Y. Khi đó*

(a) Nếu $B \subset C \subset Y$ thì $f^{-1}(B) \subset f^{-1}(C)$.

(b) Nếu $B_i, i \in I$, là một họ các tập hợp con của tập hợp Y thì

$$f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}\left(B_i\right),$$
$$f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}\left(B_i\right).$$

(c) Nếu B, C là hai tập hợp con của tập hợp Y thì

$$f^{-1}\left(B \setminus C\right) = f^{-1}\left(B\right) \setminus f^{-1}(C).$$

Đặc biệt

$$f^{-1}\left(Y \setminus B\right) = X \setminus f^{-1}(B).$$

(d) Với mọi tập hợp con $B \subset Y$ ta đều có

$$f[f^{-1}(B)] \subseteq B.$$

(e) Với mọi tập hợp con $A \subset X$ ta đều có

$$f^{-1}[f(A)] \supseteq A.$$

Để ý rằng các đẳng thức

$$f^{-1}[f(A)] = A \quad \text{và} \quad f[f^{-1}(B)] = B$$

nói chung không đúng.

1.2.2 Ánh xạ hạn chế

Giả sử $f\colon X \to Y$ là một ánh xạ từ tập hợp X vào tập hợp Y và giả sử Z là một tập hợp con của X. Ánh xạ

$$f|_Z\colon Z \to Y$$

xác định bởi

$$f|_Z(x) = f(x), \quad x \in Z,$$

được gọi là *hạn chế của f lên Z*, còn ánh xạ f được gọi là thác triển của $f|_Z$ lên X. Hiển nhiên

(a) Nếu f là một-một thì $f|_Z$ cũng là một-một .

(b) Với mọi tập hợp con B của Y ta đều có

$$(f|_Z)^{-1}(B) = f^{-1}(B) \cap Z.$$

1.2.3 Hợp của các ánh xạ

Giả sử X, Y và Z là ba tập hợp và ta có các ánh xạ

$$f\colon X \to Y, \quad g\colon Y \to Z.$$

Khi đó có thể thiết lập ánh xạ

$$g \circ f\colon X \to Z, \quad x \mapsto g[f(x)].$$

Ánh xạ $g \circ f$ được gọi là *hợp của các ánh xạ f và g.*

Ví dụ 1.2.3. Cho hai ánh xạ

$$\begin{aligned} f\colon \mathbb{R} &\to \mathbb{R}, \qquad x \mapsto x^2, \\ g\colon \mathbb{R} &\to \mathbb{R}, \qquad y \mapsto y - 1. \end{aligned}$$

Ta có ánh xạ hợp

$$g \circ f\colon \mathbb{R} \to \mathbb{R}, \qquad x \mapsto x^2 - 1.$$

Từ định nghĩa dễ dàng suy ra

Tính chất 1.2.5. *Cho hai ánh xạ*

$$f\colon X \to Y, \quad g\colon Y \to Z.$$

(a) Nếu f và g là một-một (tương ứng, lên, một-một lên) thì ánh xạ hợp $g \circ f$ cũng là một-một (tương ứng, lên, một-một lên).

(b) Với mọi tập hợp con A của X ta đều có

$$(g \circ f)(A) = g[f(A)].$$

(c) Với mọi tập hợp con C của Z ta đều có

$$(g \circ f)^{-1}(C) = f^{-1}[g^{-1}(C)].$$

1.2.4 Ánh xạ ngược

Giả sử

$$f\colon X \to Y$$

là ánh xạ một-một lên. Khi đó với mỗi phần tử $y \in Y$ tồn tại duy nhất một phần tử $x \in X$ sao cho $f(x) = y$, và bởi vậy $f^{-1}(y) = \{x\}$. Do đó ta có thể thiết lập một ánh xạ

$$g\colon Y \to X$$

xác định bởi công thức: với mọi $y \in Y$,

$$g(y) = x \quad \text{nếu} \quad f(x) = y.$$

Ánh xạ g gọi là *ánh xạ ngược* của f và ký hiệu là f^{-1}. Hiển nhiên $f^{-1}\colon Y \to X$ là ánh xạ một-một lên và $(f^{-1})^{-1} = f$.

Ví dụ 1.2.4. (a) Ánh xạ đồng nhất

$$id_X\colon X \to X, \quad x \mapsto x,$$

là ánh xạ một-một lên và $(id_X)^{-1} = id_X$.

(b) Ánh xạ một-một và lên

$$f\colon \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^3,$$

có ánh xạ ngược là

$$f^{-1}\colon \mathbb{R} \to \mathbb{R}, \quad y \mapsto y^{\frac{1}{3}}.$$

Từ định nghĩa dễ dàng suy ra

Tính chất 1.2.6. *(a) Giả sử $f\colon X \to Y$ là ánh xạ một-một lên. Khi đó*

$$f^{-1} \circ f = id_X, \quad f \circ f^{-1} = id_Y.$$

(b) Nếu $f\colon X \to Y, g\colon Y \to Z$ là những ánh xạ một-một lên, thì ánh xạ hợp $(g \circ f)\colon X \to Z$ cũng một-một lên và

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

1.2.5 Lực lượng của một tập hợp

Định nghĩa 1.2.7. (a) Hai tập hợp A và B gọi là *có cùng lực lượng* nếu tồn tại ánh xạ một-một và lên $f\colon A \to B$.

(b) Tập hợp trống, tập hợp $\{x_1, x_2, \ldots, x_n\}$ và các tập hợp cùng lực lượng với nó gọi là *tập hợp hữu hạn.*

(c) Tập hợp các số tự nhiên $\mathbb{N}$ và các tập hợp cùng lực lượng với nó gọi là *tập hợp đếm được.*

(d) Tập hợp các số thực $\mathbb{R}$ và các tập hợp cùng lực lượng với nó gọi là *tập hợp không đếm được.*

(e) Tập hợp A gọi là *không quá đếm được,* nếu A là một tập hợp hữu hạn (và có thể là trống), hoặc nếu A là một tập hợp đếm được.

Giả sử $A := \{x_1, x_2, \ldots, x_n\}$ là một tập hợp hữu hạn khác trống sao cho $x_i \neq x_j$ với mọi $i \neq j$. Khi đó ta nói tập hợp A có n *phần tử* và ký hiệu $\#A := n$. Tập hợp trống $\emptyset$ không có phần tử nào cả, vì vậy đặt $\#\emptyset := 0$. Nếu A là tập hợp khác trống và không phải tập hợp hữu hạn, đặt $\#A := +\infty$.

Bài tập

1. Giả sử $X := \{1, 2, 3\}, Y := \{a, b, c, d\}, Z := \{w, x, y, z\}$. Xét các ánh xạ $f\colon X \to Y$ và $g\colon Y \to Z$ cho bởi

$$f(1) = b, f(2) = c, f(3) = a,$$
$$g(a) = x, g(b) = x, g(c) = z, g(d) = w.$$

   Xác định ánh xạ hợp $f \circ g$.

2. Giả sử $f\colon X \to \mathbb{N}, x \mapsto x^2$, với $X := \{-5, -4, \ldots, 4, 5\}$. f là ánh xạ một-một? f là ánh xạ lên?

3. Có bao nhiêu ánh xạ từ tập $\{a, b\}$ vào tập $\{1, 2\}$. Những ánh xạ nào là một-một? Những ánh xạ nào là lên?

4. Giả sử $X := \{a, b, c\}$ và $f\colon X \to X$ cho bởi

$$f(a) = b, f(b) = a, f(c) = b.$$

   Định nghĩa dãy các ánh xạ $f^n\colon X \to X, n = 1, 2, \ldots,$ bởi $f^1 := f$ và $f^n := f^{n-1} \circ f$ với mọi $n \geq 2$. Hãy xác định các ánh xạ f^2, f^3, f^9, f^{789}.

5. Giả sử $X := \{0, 1, 2, 3, 4\}$ và ánh xạ $f\colon X \to X$ xác định bởi

$$f(x) := 4x \bmod 5.$$

   f là ánh xạ một-một? f là ánh xạ lên?

6. Giả sử m, n là các số nguyên dương. Giả sử $X := \{0, 1, 2, \ldots, m-1\}$. Xét ánh xạ $f\colon X \to X$ cho bởi

$$f(x) := nx \bmod m.$$

   Tìm những điều kiện của m và n để f là ánh xạ một-một và lên?

7. Cho các ánh xạ $f\colon X \to Y$ và $g\colon Y \to Z$. Chứng minh hoặc cho phản ví dụ các phát biểu sau:

   (a) Nếu g là một-một thì $g \circ f$ là một-một.

   (b) Nếu f và g là lên thì $g \circ f$ là lên.

   (c) Nếu f và g là một-một và lên thì $g \circ f$ là một-một và lên.

   (d) Nếu $g \circ f$ là một-một thì f là một-một.

   (e) Nếu $g \circ f$ là một-một thì g là một-một.

   (f) Nếu $g \circ f$ là lên thì f là lên.

   (g) Nếu $g \circ f$ là lên thì g là lên.

8. Giả sử $X := \{1, 2, 3\}$ và $Y := \{a, b, c, d\}$. Xét ánh xạ $f\colon X \to Y$ cho bởi

$$f(1) = a, f(2) = c, f(3) = c.$$

   Xác định các tập hợp sau: $f(\{1\}), f(\{1, 3\}), f^{-1}(\{a\})$ và $f^{-1}(\{a, c\})$.

9. Cho ánh xạ $f\colon X \to Y$. Chứng minh f là một-một nếu và chỉ nếu

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

   với mọi tập con A và B của X.

10. Cho ánh xạ $f\colon X \to Y$. Chứng minh rằng họ các tập hợp

$$\mathcal{A} := \{f^{-1}(\{y\}) \mid y \in Y\}$$

    là một phân hoạch của tập hợp X.

11. Cho ánh xạ $g\colon X \to Y$. Chứng minh rằng g là một-một nếu và chỉ nếu với mọi ánh xạ một-một $f\colon A \to X$ (A là tập hợp bất kỳ) thì ánh xạ hợp $g \circ f\colon A \to Y$ là một-một.

12. Cho ánh xạ $f\colon X \to Y$. Chứng minh rằng f là lên nếu và chỉ nếu với mọi ánh xạ lên $g\colon Y \to Z$ (Z là tập hợp bất kỳ) thì ánh xạ hợp $g \circ f\colon X \to Z$ là lên.

13. A là tập hợp con của tập hợp X. Định nghĩa *hàm đặc trưng* của tập hợp A (trong X) như sau:

$$\chi_A(x) := \begin{cases} 1 & \text{nếu } x \in A, \\ 0 & \text{nếu } x \notin A. \end{cases}$$

    (a) Chứng minh với mọi $x \in X$ ta có các quan hệ sau

$$\begin{aligned} \chi_{A\cap B}(x) &= \chi_A(x)\chi_B(x), \\ \chi_{A\cup B}(x) &= \chi_A(x) + \chi_B(x) - \chi_{A\cap B}(x), \\ \chi_{A^c}(x) &= 1 - \chi_A(x), \\ \chi_{A\setminus B}(x) &= \chi_A(x)[1 - \chi_B(x)]. \end{aligned}$$

(b) Chứng minh nếu $A \subseteq B$ thì $\chi_A(x) \leq \chi_B(x)$ với mọi $x \in X$.

(c) Chứng minh $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x)$ với mọi $x \in X$ nếu và chỉ nếu $A \cap B = \emptyset$.

(d) Tìm công thức liên quan đến ánh xạ $\chi_{A \,\Delta\, B}$.

14. Xét ánh xạ f từ $\mathcal{P}(X)$ vào tập hợp các hàm đặc trưng trong X định nghĩa bởi

$$f(A) := \chi_A.$$

Chứng minh f là một-một và lên.

15. Chứng minh tập hợp các số tự nhiên $\mathbb{N}$ và tập các số tự nhiên chẵn $2\mathbb{N}$ là cùng lực lượng.

16. Chứng minh tập hợp khác trống X không cùng lực lượng với $\mathcal{P}(X)$.

17. Giả sử $X := \{0, 1\}$. Liệt kê tất cả các chuỗi độ dài 2 trên X. Liệt kê tất cả các chuỗi độ dài ≤ 2 trên X.

18. Chuỗi s gọi là *chuỗi con* của chuỗi t nếu tồn tại các chuỗi u, v sao cho $t = usv$. Liệt kê tất cả các chuỗi con của chuỗi *babc*.

19. Chứng minh hoặc cho phản ví dụ các phát biểu sau đối với tất cả các số thực[2]:

(a) $\lceil x + 7 \rceil = \lceil x \rceil + 7$.

(b) $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$.

(c) $\lfloor x + y \rfloor = \lfloor x \rfloor + \lceil y \rceil$.

20. Giả sử n là số nguyên lẻ. Chứng minh các đẳng thức sau

$$\begin{aligned} \left\lfloor \frac{n^2}{4} \right\rfloor &= \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right), \\ \left\lceil \frac{n^2}{4} \right\rceil &= \frac{n^2+3}{4}. \end{aligned}$$

21. Chứng minh rằng

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

[2] $\lceil x \rceil$ là số nguyên nhỏ nhất lớn hơn hoặc bằng x; $\lfloor x \rfloor$ là số nguyên lớn nhất nhỏ hơn hoặc bằng x.

Chương 2

LOGIC VÀ CÁC PHƯƠNG PHÁP CHỨNG MINH

2.1 Mệnh đề

Một mệnh đề toán học có thể xem là một *khẳng định toán học chỉ có thể đúng hoặc sai,* không thể nhập nhằng, nghĩa là không thể vừa đúng vừa sai, cũng không thể vừa không đúng vừa không sai.

Ví dụ 2.1.1. Các phát biểu sau là các mệnh đề:

(a) Trái đất có dạng hình cầu.

(b) Việt Nam là nước có số dân đông nhất thế giới.

(c) $2 + 2 = 4$.

(d) 4 là một số dương và 3 là một số âm.

Ví dụ 2.1.2. Các phát biểu sau không phải là mệnh đề:

(a) Hôm nay trời mưa.

(b) Xin hãy giúp đỡ tôi.

(c) $x - y = y - x$.

(d) $x - 3 = 5$.

Ta thường dùng các ký tự in thường, chẳng hạn p, q và r để biểu diễn một mệnh đề. Để đơn giản, chúng ta cũng ký hiệu

$$p\colon 1+1=3$$

để định nghĩa p là mệnh đề $1+1=3$.

Định nghĩa 2.1.1. Giả sử p và q là các mệnh đề. *Hội* của p và q, ký hiệu là $p \wedge q$, là mệnh đề

$$p \quad \text{và} \quad q.$$

Tuyển của p và q, ký hiệu là $p \vee q$, là mệnh đề

$$p \quad \text{hoặc} \quad q.$$

Ví dụ 2.1.3. Giả sử

$$\begin{aligned} p\colon &\quad 1+1=3, \\ q\colon &\quad \text{một thập kỷ là 10 năm.} \end{aligned}$$

Khi đó hội của p và q là mệnh đề

$$p \wedge q\colon 1+1=3 \text{ và một thập kỷ là 10 năm,}$$

và tuyển của p và q là mệnh đề

$$p \vee q\colon 1+1=3 \text{ hoặc một thập kỷ là 10 năm.}$$

Định nghĩa 2.1.2. Giá trị của mệnh đề $p \wedge q$ được cho bởi *bảng chân trị*

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

trong đó ký hiệu T là đúng và F là sai.

Ví dụ 2.1.4. Giả sử

$$\begin{aligned} p\colon &\quad 1+1=3, \\ q\colon &\quad \text{Một thập kỷ là 10 năm.} \end{aligned}$$

Ta có p là sai và q là đúng. Vì vậy hội của p và q là mệnh đề sai.

Định nghĩa 2.1.3. Giá trị của mệnh đề $p \vee q$ được cho bởi *bảng chân trị*

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Ví dụ 2.1.5. Giả sử

$$p: \quad 1+1=3,$$
$$q: \quad \text{Một thập kỷ là 10 năm.}$$

Ta có p là sai và q là đúng. Vì vậy tuyển của p và q là mệnh đề đúng.

Định nghĩa 2.1.4. *Phủ định* của mệnh đề p, ký hiệu $\overline{p}$ hay p', là mệnh đề

không phải p.

Giá trị của mệnh đề $\overline{p}$ được cho bởi *bảng chân trị*

p	$\overline{p}$
T	F
F	T

Ví dụ 2.1.6. Giả sử

$$p: \quad \pi \text{ là số hữu tỉ.}$$

Ta có mệnh đề p là sai và do vậy phủ định của nó $\overline{p}$ là đúng.

Bài tập

1. Giá trị của các mệnh đề p, q và R tương ứng là F, T và F. Xác định giá trị của các mệnh đề sau:

   (a) $(\overline{p} \vee \overline{q}) \vee p$.

   (b) $(p \vee q) \wedge \overline{p}$.

   (c) $(p \wedge q) \wedge \overline{p}$.

   (d) $(p \wedge q) \vee (\overline{p} \vee q)$.

   (e) $\overline{(p \wedge q)} \vee (r \wedge \overline{p})$.

   (f) $(p \vee q) \wedge (\overline{p} \vee q) \wedge (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{q})$.

   (g) $\overline{(p \vee q)} \vee (\overline{q} \vee r)$.

2. Cho các mệnh đề sau

   $$p: 5 < 9, \quad q: 9 < 7 \text{ và } 5 < 7.$$

   Xác định tính đúng sai của các mệnh đề sau

   (a) $5 < 9$ và $9 < 7$.

   (b) Phủ định của mệnh đề ($5 < 9$ và $9 < 7$).

   (c) $5 < 9$ hoặc phủ định của mệnh đề ($9 < 7$ và $5 < 7$).

2.2 Mệnh đề có điều kiện và các mệnh đề tương đương

Định nghĩa 2.2.1. Giả sử p và q là hai mệnh đề. Khi đó phát biểu

$$\text{nếu } p \text{ thì } q$$

gọi là *mệnh đề có điều kiện* và ký hiệu là

$$p \to q.$$

Mệnh đề p gọi là *giả thiết* và mệnh đề q gọi là *kết luận* (hay *hệ quả*).

Định nghĩa 2.2.2. Bảng giá trị của mệnh đề có điều kiện $p \to q$ định nghĩa như sau:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Ví dụ 2.2.1. Giả sử

$$\begin{aligned} p&: \quad 1 > 2, \\ q&: \quad 3 < 7. \end{aligned}$$

Ta có p là sai và q là đúng. Do đó $p \to q$ là đúng và $q \to p$ là sai.

Định nghĩa 2.2.3. Giả sử p và q là hai mệnh đề. Khi đó phát biểu

$$p \text{ nếu và chỉ nếu } q$$

gọi là *mệnh đề nếu và chỉ nếu* và được ký hiệu là

$$p \leftrightarrow q.$$

Bảng giá trị của mệnh đề $p \leftrightarrow q$ được định nghĩa như sau:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Mệnh đề "p nếu và chỉ nếu q" còn được diễn đạt dạng "điều kiện cần và đủ để p là q".

Ví dụ 2.2.2. Câu

$$1 < 5 \text{ nếu và chỉ nếu } 2 < 8$$

có thể viết dưới dạng

$$p \leftrightarrow q,$$

trong đó

$$p\colon \quad 1 < 5, \quad q\colon \quad 2 < 8.$$

Ta có p và q là đúng. Do đó $p \leftrightarrow q$ là đúng.

Định nghĩa 2.2.4. Giả sử P và Q là hai mệnh đề được xây dựng từ các mệnh đề $p_1, p_2, \ldots, p_n$. Ta nói P *tương đương* Q và viết

$$P \equiv Q$$

nếu với mọi giá trị của $p_1, p_2, \ldots, p_n$ ta có P và Q hoặc đồng thời đúng, hoặc đồng thời sai.

Ví dụ 2.2.3. Ta có công thức De Morgan:

$$\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}, \quad \overline{p \wedge q} \equiv \overline{p} \vee \overline{q}.$$

Ví dụ 2.2.4. Ta có

$$\begin{aligned} \overline{p \to q} &\equiv p \wedge \overline{q}, \\ p \leftrightarrow q &\equiv (p \to q) \wedge (q \to p). \end{aligned}$$

Định nghĩa 2.2.5. Mệnh đề $\overline{q} \to \overline{p}$ gọi là *phản đảo* của mệnh đề $p \to q$.

Ví dụ 2.2.5. Giả sử

$$p\colon 1 < 4, \quad q\colon 5 > 8.$$

Khi đó

$$\begin{aligned} p \to q&\colon \quad \text{nếu } 1 < 4 \text{ thì } 5 > 8, \\ q \to p&\colon \quad \text{nếu } 5 > 8 \text{ thì } 1 < 4, \\ \overline{q} \to \overline{p}&\colon \quad \text{nếu 5 không lớn hơn 8 thì 1 không lớn hơn 4.} \end{aligned}$$

Ta có $p \to q$ là sai. Nên $q \to p$ là đúng và $\overline{q} \to \overline{p}$ là sai.

Định lý 2.2.6. *Mệnh đề $p \to q$ tương đương với mệnh đề phản đảo của nó. Tức là*

$$p \to q \equiv \overline{q} \to \overline{p}$$

Chứng minh. Chứng minh suy trực tiếp từ bảng chân trị của các mệnh đề $p \to q$ và $\overline{q} \to \overline{p}$. □

Bài tập

1. Xác định giá trị của các mệnh đề sau nếu giá trị của các mệnh đề p, q, r, s tương ứng là F, T, F, T :

   (a) $p \to q$.

   (b) $\overline{p} \to \overline{q}$.

   (c) $\overline{p \to q}$.

   (d) $(p \to q) \wedge (q \to r)$.

   (e) $(p \to q) \to r$.

   (f) $p \to (q \to r)$.

   (g) $(s \to (p \wedge \overline{r})) \wedge ((p \to (r \vee q)) \wedge s)$.

   (h) $((p \wedge \overline{q}) \to (q \wedge r)) \to (s \vee \overline{q})$.

2. Cho các mệnh đề

   $$p\colon 4 < 2, \quad q\colon 7 < 10, \quad r\colon 6 < 6.$$

   Viết các phát biểu dưới đây dạng ký hiệu

   (a) Nếu $4 < 2$ thì $7 < 10$.

   (b) Nếu ($4 < 2$ và $6 < 6$) thì $7 < 10$.

   (c) Nếu ($6 < 6$ và 7 không nhỏ hơn 10) không đúng thì $6 < 6$.

   (d) $7 < 10$ nếu và chỉ nếu ($4 < 2$ và 6 không nhỏ hơn 6).

3. Với các phát biểu dưới đây, hãy viết mỗi mệnh đề và phủ định của nó dạng ký hiệu. Tìm giá trị của mỗi mệnh đề.

   (a) Nếu $4 < 6$ thì $9 > 12$.

   (b) Nếu $4 > 6$ thì $9 > 12$.

   (c) $|1| < 3$ nếu $-3 < 1 < 3$.

   (d) $|4| < 3$ nếu $-3 < 4 < 3$.

4. $P \equiv Q$ là đúng hay sai nếu

   (a) $P = p, Q = p \vee q$.

   (b) $P = p \wedge q, Q = \overline{p} \vee \overline{q}$.

   (c) $P = p \to q, Q = \overline{p} \vee q$.

   (d) $P = p \wedge (\overline{q} \vee r), Q = p \vee (q \wedge \overline{r})$.

   (e) $P = p \wedge (q \vee r), Q = (p \vee q) \wedge (p \vee r)$.

   (f) $P = p \to q, Q = \overline{q} \to \overline{p}$.

   (g) $P = p \to q, Q = p \leftrightarrow q$.

(h) $P = (p \to q) \wedge (q \to r), Q = p \to r$.

(i) $P = (p \to q) \to r, Q = p \to (q \to r)$.

(k) $P = (s \to (p \wedge \overline{r})) \wedge ((p \to (r \vee q)) \wedge s), Q = p \vee t$.

5. Xét mệnh đề $p \oplus_1 q$ cho bởi bảng giá trị

p	q	$p \oplus_1 q$
T	T	T
T	F	F
F	T	F
F	F	T

Chứng minh rằng

$$p \oplus_1 q = q \oplus_1 p.$$

6. Xét mệnh đề $p \oplus_2 q$ cho bởi bảng giá trị

p	q	$p \oplus_2 q$
T	T	T
T	F	F
F	T	T
F	F	F

(a) Chứng minh rằng

$$(p \oplus_2 q) \wedge (q \oplus_2 p) \not\equiv p \leftrightarrow q.$$

(b) Chứng minh

$$(p \oplus_2 q) \wedge (q \oplus_2 p) \equiv p \leftrightarrow q$$

nếu ta thay $\oplus_2$ sao cho nếu p là sai và q là đúng thì $p \oplus_2 q$ là sai.

7. Chứng minh rằng

$$(p \to q) \equiv (\overline{p} \vee q).$$

2.3 Lượng hóa

Logic nghiên cứu các mệnh đề trong những tiết trước không đủ để diễn tả hầu hết các mệnh đề trong toán học cũng như khoa học máy tính. Chẳng hạn, xét:

p: n là một số nguyên lẻ.

Định nghĩa 2.3.1. Cho X là một tập hợp. $P(x)$ là một phát biểu liên quan đến biến $x \in X$. Ta nói P là *hàm mệnh đề* nếu với mỗi $x \in X$ thì $P(x)$ là một mệnh đề.

Ví dụ 2.3.1. Giả sử $\mathbb{P}$ là tập các số nguyên dương và với mỗi $n \in \mathbb{P}$ đặt

$$P(n)\colon n \text{ là một số nguyên lẻ.}$$

Khi đó P là hàm mệnh đề trên $\mathbb{P}$.

Định nghĩa 2.3.2. Giả sử P là hàm mệnh đề trên tập X. Phát biểu

$$\text{với mọi } x, P(x)$$

gọi là *lượng hóa phổ cập.* Ký hiệu $\forall$ nghĩa là "với mọi". Vì vậy phát biểu

$$\text{với mọi } x, P(x)$$

có thể viết lại

$$\forall x, P(x).$$

Ký hiệu $\forall$ gọi là *lượng hóa phổ cập.*

Phát biểu

$$\text{với mọi } x, P(x)$$

là đúng nếu $P(x)$ đúng với mọi $x \in X$. Phát biểu này là sai nếu có ít nhất một $x \in X$ sao cho $P(x)$ sai.

Phát biểu

$$\text{tồn tại } x, P(x)$$

gọi là *lượng hóa tồn tại.* Ký hiệu $\exists$ nghĩa là "tồn tại". Vì vậy phát biểu

$$\text{tồn tại } x, P(x)$$

có thể viết lại

$$\exists x, P(x).$$

Ký hiệu $\exists$ gọi là *lượng hóa tồn tại.*

Phát biểu

$$\text{tồn tại } x, P(x)$$

là đúng nếu $P(x)$ đúng với ít nhất một $x \in X$. Phát biểu này là sai nếu với mọi $x \in X$ đều có $P(x)$ sai.

Ví dụ 2.3.2. Phát biểu

$$\text{với mọi số thực } x \text{ thì } x^2 \geq 0$$

là lượng hóa phổ cập và là một khẳng định đúng.

Ví dụ 2.3.3. Phát biểu lượng hóa phổ cập

$$\text{với mọi số thực } x \text{ thì } x^2 - 1 > 0$$

là sai vì với $x = 1$ ta có

$$1^2 - 1 > 0$$

là mệnh đề sai.

Ví dụ 2.3.4. Phát biểu lượng hóa tồn tại

$$\text{tồn tại số nguyên } x \text{ để } x^2 - 4 = 0$$

là đúng vì ta có thể tìm được ít nhất một số nguyên x sao cho

$$x^2 - 4 = 0.$$

Chẳng hạn, với $x = 2$ ta có mệnh đề đúng:

$$2^2 - 4 = 0.$$

Ví dụ 2.3.5. Dễ dàng chứng minh phát biểu lượng hóa tồn tại sau là sai:

$$\text{tồn tại số thực } x \text{ để } \frac{1}{x^2 + 1} > 1.$$

Nhận xét 2. Giữa các lượng hóa phổ cập và tồn tại có liên hệ sau đây:

(a) Không $(\exists x)\ P(x) \Leftrightarrow (\forall x)$ không $P(x)$. Tức là phủ định của mệnh đề "có tồn tại một x sao cho $P(x)$" là "với mọi x đều không có $P(x)$".

(b) Không $(\forall x)\ P(x) \Leftrightarrow (\exists x)$ không $P(x)$. Tức là phủ định của mệnh đề "với mọi x đều có $P(x)$" là "có tồn tại một x sao cho không có $P(x)$".

Định lý 2.3.3. *Giả sử P là hàm mệnh đề. Khi đó cặp các mệnh đề (a) và (b) sau hoặc đồng thời đúng, hoặc đồng thời sai:*

(a) $\overline{\forall x, P(x)};\ \exists x, \overline{P(x)}$.

(b) $\overline{\exists x, P(x)};\ \forall x, \overline{P(x)}$.

Chứng minh. Bài tập. □

Bài tập

1. Giả sử $P(n)$ là hàm mệnh đề "n là ước số của 77". Kiểm tra tính đúng sai của
   (a) $P(11)$.
   (b) $P(1)$.
   (c) $P(3)$.
   (d) $P(n)$ với mọi số tự nhiên n.
   (e) Tồn tại số tự nhiên n sao cho $P(n)$.
2. Xác định giá trị của các phát biểu dưới đây (xét trên tập hợp các số thực $\mathbb{R}$):
   (a) $x^2 > x$ với mọi x.
   (b) Tồn tại x sao cho $x^2 > x$.
   (c) Với mọi x với $x > 1$ thì $x^2 > x$.
   (d) Tồn tại x với $x > 1$ sao cho $x^2 > x$.
   (e) Với mọi x với $x > 1$ thì $\frac{x}{x^2+1} < \frac{1}{3}$.
   (f) Tồn tại x với $x > 1$ thì $\frac{x}{x^2+1} < \frac{1}{3}$.
   (g) Với mọi x và với mọi y mà $x < y$ ta có $x^2 < y^2$.
   (h) Với mọi x, tồn tại y với $x < y$ ta có $x^2 < y^2$.
   (i) Tồn tại x sao cho với mọi y mà $x < y$ thì $x^2 < y^2$.
   (j) Tồn tại x, tồn tại y với $x < y$ sao cho $x^2 < y^2$.
3. Viết phủ định của các phát biểu trong bài tập trên.

2.4 Phương pháp chứng minh

Một *hệ thống toán học* gồm các *tiên đề, định nghĩa,* và các *thành phần không xác định.*

- Tiên đề được giả thiết là đúng.
- Định nghĩa được sử dụng để xây dựng các khái niệm mới từ các khái niệm đã có.
- Một số thành phần không được định nghĩa một cách tường minh mà được xác định bởi các tiên đề.

Từ hệ thống toán học ta có thể dẫn đến:

- *Định lý* là một mệnh đề đã được chứng minh là đúng.

- *Bổ đề* là một định lý không quan trọng lắm và được sử dụng để chứng minh một định lý khác.
- *Hệ quả* là một định lý được suy ra dễ dàng từ một định lý khác.
- *Chứng minh* là một lý luận chỉ ra tính đúng của một định lý.
- Logic là một công cụ để phân tích các chứng minh.

Ví dụ 2.4.1. Hình học Euclid là một hệ toán học. Một số tiên đề:

- Tồn tại một và chỉ một đường thẳng đi qua hai điểm phân biệt cho trước.
- Tồn tại một và chỉ một đường thẳng đi qua một điểm và song song với một đường thẳng (không chứa điểm) cho trước.

Điểm và *đường thẳng* là các thành phần không xác định và được định nghĩa ẩn trong các tiên đề.

Một số định nghĩa:

- Hai tam giác là *bằng nhau* nếu có thể sắp xếp các đỉnh thành những cặp sao cho các cạnh và các góc tương ứng là bằng nhau.
- Hai góc là *bù nhau* nếu tổng của chúng bằng 180^0.

Một số định lý:

- Nếu hai cạnh của một tam giác bằng nhau thì các góc đối diện bằng nhau.
- Nếu hai đường chéo của tứ giác cắt nhau tại các trung điểm của chúng thì tứ giác là hình bình hành.

Từ định lý thứ nhất suy ra hệ quả sau:

- Tam giác có ba cạnh bằng nhau thì có các góc bằng nhau.

Ví dụ 2.4.2. Tập các số thực $\mathbb{R}$ là một hệ toán học. Một số tiên đề:

- Với mọi $x, y \in \mathbb{R}$ ta có $xy = yx$.
- Tồn tại một tập con $P \subset \mathbb{R}$ sao cho
  (a) Nếu x, y thuộc P thì $x + y$ và xy thuộc P.

(b) Với mọi $x \in \mathbb{R}$ thì một và chỉ một trong các điều sau đúng:

$$x \in P, \quad x = 0, \quad -x \in P.$$

Phép toán nhân được định nghĩa ẩn trong tiên đề thứ nhất.

Một số định nghĩa:

- Các phần tử thuộc P gọi là *các số thực dương.*
- *Giá trị tuyệt đối* $|x|$ của số thực x được định nghĩa là x nếu x dương hoặc bằng 0 và bằng $-x$ nếu ngược lại.

Một số định lý:

- $x \cdot 0 = 0$ với mọi $x \in \mathbb{R}$.
- với mọi $x, y, z \in \mathbb{R}$ nếu $x \leq y$ và $y \leq z$ thì $x \leq z$.

Một ví dụ về bổ đề:

- nếu n là số nguyên dương thì hoặc $n - 1$ là số nguyên dương hoặc $n - 1 = 0$.

Định lý thường có dạng:

$$\text{Với mọi } x_1, x_2, \ldots, x_n, \text{nếu } p(x_1, x_2, \ldots, x_n) \text{ thì } q(x_1, x_2, \ldots, x_n). \tag{2.1}$$

Định nghĩa 2.4.1. *Chứng minh trực tiếp* của định lý (2.1) có dạng: Giả sử $p(x_1, x_2, \ldots, x_n)$ đúng; sử dụng $p(x_1, x_2, \ldots, x_n)$ cũng như các tiên đề, các định nghĩa, các định lý đã có để suy ra $q(x_1, x_2, \ldots, x_n)$ là đúng.

Ví dụ 2.4.3. Chứng minh trực tiếp khẳng định sau: *với mọi số thực* d, d_1, d_2 *và* x *ta có:*

$$\textit{nếu } d = \min\{d_1, d_2\} \textit{ và } x \leq d \textit{ thì } x \leq d_1 \textit{ và } x \leq d_2.$$

Định nghĩa 2.4.2. *Chứng minh phản chứng* (hay *chứng minh gián tiếp*) của định lý (2.1) có dạng: Giả sử $p(x_1, x_2, \ldots, x_n)$ đúng và $q(x_1, x_2, \ldots, x_n)$ sai; sử dụng $p, \overline{q}$ cũng như các tiên đề, các định nghĩa, các định lý đã có để suy ra một *mâu thuẫn.* Một mâu thuẫn là mệnh đề có dạng $r \wedge \overline{r}$ (r là mệnh đề nào đó).

Tính đúng của chứng minh phản chứng suy trực tiếp từ sự kiện sau (tại sao):

$$p \to q \quad \equiv \quad p \wedge \overline{q} \to r \wedge \overline{r}.$$

Ví dụ 2.4.4. Chứng minh bằng phản chứng khẳng định sau: *với mọi số thực x và y, nếu $x + y \geq 2$ thì hoặc $x \geq 1$ hoặc $y \geq 1$.*

Định nghĩa 2.4.3. Dãy các mệnh đề được viết dạng

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ p_n \\ \hline \therefore q \end{array}$$

hay $p_1, p_2, \ldots, p_n \ /\!\!\therefore q$ gọi là một *lý luận.* Các mệnh đề $p_1, p_2, \ldots, p_n$ gọi là các *giả thiết* và mệnh đề q gọi là *kết luận.* Lý luận là *hợp lệ* nếu p_1 và p_2 và $\cdots$ và p_n đồng thời đúng thì q cũng đúng; ngược lại lý luận gọi là *không hợp lệ* (hay *sai*).

Ví dụ 2.4.5. Chứng minh lý luận sau là hợp lệ:

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

Ví dụ 2.4.6. Lý luận sau không hợp lệ:

$$\begin{array}{l} \text{Nếu } 2 = 3 \text{ thì tôi ăn cái mũ này.} \\ \text{Tôi ăn cái mũ này.} \\ \hline \therefore 2 = 3 \end{array}$$

Bài tập

1. Cho một ví dụ về tiên đề, định nghĩa và định lý của hình học Euclid.

2. Cho một ví dụ về tiên đề, định nghĩa và định lý của hệ các số thực.

3. Giả sử ta đã có các định lý sau: với mọi $a, b, c \in \mathbb{R}$ thì $b + 0 = b$; $a(b + c) = ab + ac$; và nếu $a + b = a + c$ thì $b = c$. Hãy kiểm tra các bước chứng minh trực tiếp của khẳng định: "$x \cdot 0 = 0$ với mọi số thực x."

   Chứng minh. $(x \cdot 0) + 0 = x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$; do đó $x \cdot 0 = 0$. □

4. Giả sử đã có định lý sau: với mọi $a, b, c \in \mathbb{R}$, nếu $ab = ac$ và $a \neq 0$ thì $b = c$. Hãy kiểm tra các bước chứng minh bằng phản chứng của khẳng định: "nếu $x \cdot y = 0$ thì hoặc $x = 0$ hoặc $y = 0$."

   Chứng minh. Giả sử $x \cdot 0 = 0$ và $x \neq 0, y \neq 0$. Từ $xy = 0 = x \cdot 0$ và $n \neq 0$ ta có $y = 0$ mà là một mâu thuẫn. □

5. Chứng minh bằng phản chứng khẳng định sau: "nếu đặt 100 quả bóng vào trong 9 hộp thì có ít nhất một hộp chứa ít nhất 12 quả bóng".

6. Viết các lý luận sau dưới dạng ký hiệu và xác định tính đúng-sai:

   (a)

   Nếu tôi học tập chăm chỉ thì tôi sẽ đạt điểm tốt.
   Tôi học tập chăm chỉ.

   ∴ Tôi sẽ đạt điểm tốt.

   (b)

   Nếu tôi học tập chăm chỉ thì tôi sẽ đạt điểm tốt.
   Nếu tôi không giàu có thì tôi sẽ không đạt điểm tốt.

   ∴ Tôi giàu có

   (c)

   Tôi học tập chăm chỉ nếu và chỉ nếu tôi giàu có.
   Tôi giàu có.

   ∴ Tôi học tập chăm chỉ.

   (d)

   Nếu tôi học tập chăm chỉ hoặc tôi giàu có thì tôi sẽ đạt điểm tốt.
   Tôi sẽ đạt điểm tốt.

   ∴ Nếu tôi không học tập chăm chỉ thì tôi sẽ giàu có.

   (e)

   Nếu tôi học tập chăm chỉ thì hoặc tôi giàu có hoặc tôi sẽ đạt điểm tốt.
   Tôi không đạt điểm tốt và tôi không giàu có.

   ∴ Tôi không học tập chăm chỉ.

7. Giả sử

   p: Có 64K bộ nhớ thì tốt hơn không có bộ nhớ.
   q: Tôi sẽ mua bộ nhớ mới.
   r: Tôi sẽ mua một máy tính mới.

   Hãy viết các lý luận dưới đây dạng câu và xác định tính đúng-sai của các lý luận.

   (a)

$$\begin{array}{c} p \to r \\ \underline{p \to q} \\ \therefore p \to (r \wedge q) \end{array}$$

8. Chứng minh rằng nếu

$$p_1, p_2 / \therefore p$$

   và

$$p, p_3, \ldots, p_n / \therefore c$$

   là những lý luận hợp lệ thì lý luận sau cũng hợp lệ:

$$p_1, p_2, \ldots, p_n / \therefore c$$

9. Bình luận về lý luận sau

Có đĩa mềm thì tốt hơn không có gì.
Không có gì thì tốt hơn có một đĩa cứng.

$\therefore$ Có đĩa mềm thì tốt hơn có một đĩa cứng.

2.5 Quy nạp toán học

Định nghĩa 2.5.1. Giả sử với mỗi số nguyên dương n ta có một phát biểu $S(n)$ sao cho

Bước cơ bản: $S(1)$ đúng;

Bước quy nạp: nếu $S(i)$ đúng với mọi $i = 1, 2, \ldots, n$, thì $S(n+1)$ đúng.

Khi đó $S(n)$ đúng với mọi n nguyên dương.

Ví dụ 2.5.1. Ta có

$$n! \geq 2^{n-1} \quad \text{với } n = 1, 2, \ldots.$$

Thật vậy, khẳng định đúng với $n = 1$ vì

$$1! = 1 \geq 1 = 2^{1-1}.$$

Bây giờ giả sử rằng $n \geq 2$ và

$$i! \geq 2^{i-1} \quad \text{với } i = 1, 2, \ldots, n.$$

Khi đó

$$\begin{aligned} (n+1)! &= (n+1)(n!) \\ &\geq (n+1)2^{n-1} \\ &\geq 2 \cdot 2^{n-1} = 2^{(n+1)-1}. \end{aligned}$$

Theo nguyên lý quy nạp, $n! \geq 2^{n-1}$ với mọi n nguyên dương.

Cho X là một tập hợp. Ký hiệu $\mathcal{P}(X)$ (hoặc 2^X) là họ các tập hợp con (thực sự hoặc không) của X. Ta có

Định lý 2.5.2. *Nếu tập hợp hữu hạn X gồm n phần tử thì*

$$\#\mathcal{P}(X) = 2^n.$$

Chứng minh. Sử dụng quy nạp toán học. □

Bài tập

1. Dùng quy nạp toán học, chứng minh các đẳng thức sau với mọi n nguyên dương:

   (a) $1 + 3 + 5 + \cdots + (2n-1) = n^2$.

   (b) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$.

   (c) $1(1!) + 2(2!) + \cdots + n(n!) = (n+1)! - 1$.

   (d) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

   (e) $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n+1} n^2 = \frac{(-1)^{n+1} n(n+1)}{2}$.

   (f) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$.

   (g) $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$.

   (h) $\frac{1}{2^2-1} + \frac{1}{3^2-1} + \cdots + \frac{1}{(n+1)^2-1} = \frac{3}{4} - \frac{1}{2(n+1)} - \frac{1}{2(n+2)}$.

   (i) $\cos x + \cos 2x + \cdots + \cos nx = \frac{\cos[(x/2)(n+1)]\sin(nx/2)}{\sin(x/2)}$ nếu $\sin(x/2) \neq 0$.

   (j) $1\sin x + 2\sin 2x + \cdots + n\sin nx = \frac{\sin[(n+1)x]}{4\sin^2(x/2)} - \frac{(n+1)\cos\left(\frac{2n+1}{2}x\right)}{2\sin(x/2)}$ nếu $\sin(x/2) \neq 0$.

2. Dùng quy nạp toán học, chứng minh các bất đẳng thức sau

   (a) $\frac{1}{2n} \leq \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2\cdot 4\cdot 6\cdots(2n)}$, với $n = 1, 2, \cdots$.

   (b) $\frac{1}{\sqrt{n+1}} \geq \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2\cdot 4\cdot 6\cdots(2n)}$, với $n = 1, 2, \cdots$.

   (c) $2n + 1 \leq 2^n$ với $n = 3, 4, \ldots$.

   (d) $2^n \geq n^2$ với $n = 4, 5, \ldots$.

   (e) $(a_1 a_2 \ldots a_{2^n})^{1/2^n} \leq \frac{a_1 + a_2 + \cdots + a_{2^n}}{2^n}$ với $n = 1, 2, \ldots$, và các số không âm a_i.

   (f) $(1+x)^n \geq 1 + nx$ với $x \geq -1$ và $n = 1, 2, \ldots$.

3. Dùng quy nạp toán học, chứng minh các khẳng định sau:

   (a) $7^n - 1$ chia hết cho 6 với mọi $n = 1, 2, \ldots$.

   (b) $11^n - 6$ chia hết cho 5 với mọi $n = 1, 2, \ldots$.

   (c) $6 \cdot 7^n - 2 \cdot 3^n$ chia hết cho 4 với mọi $n = 1, 2, \ldots$.

   (d) $3^n + 7^n - 2$ chia hết cho 8 với mọi $n = 1, 2, \ldots$.

4. Dùng quy nạp toán học, chứng minh rằng n đường thẳng trong mặt phẳng chia mặt phẳng thành $(n^2 + n - 2)/2$ vùng. Giả sử hai đường thẳng bất kỳ không song song và không có ba đường thẳng cắt nhau tại một điểm.

Chương 3

THUẬT TOÁN

3.1 Mở đầu

Có thể định nghĩa thuật toán theo nhiều cách khác nhau. Chúng ta sẽ không trình bày chặt chẽ về thuật toán như trong các giáo trình logic, mà sẽ hiểu khái niệm thuật toán theo cách thông thường nhất.

Có thể xem *thuật toán là một quy tắc để, với những dữ liệu ban đầu đã cho, tìm được lời giải của bài toán đang xét sau một khoảng thời gian hữu hạn.*

Để minh họa cách ghi một thuật toán, cũng như tìm hiểu những yêu cầu đề ra cho thuật toán, ta xét trên các ví dụ cụ thể sau đây.

3.1.1 Tìm số lớn nhất trong ba số

Thuật toán này tìm số lớn nhất trong ba số thực a, b và c.

Vào: a, b và c.
Ra: x là số lớn nhất trong ba số a, b, c.

Bước 1. Nếu $a > b$ thì đặt $x := a$; ngược lại, đặt $x := b$.

Bước 2. Nếu $c > x$ thì đặt $x := c$.

3.1.2 Tìm số lớn nhất trong dãy hữu hạn các số thực

Thuật toán này tìm số lớn nhất trong dãy hữu hạn các số thực $s_1, s_2, \ldots, s_n$.

Vào: dãy hữu hạn các số thực $s_1, s_2, \ldots, s_n$.
Ra: $x = \max\{s_i \mid i = 1, 2, \ldots, n\}$.

Bước 1. Đặt $x := s_1$.

Bước 2. Với $i := 2$ đến n thực hiện Bước 3.

Bước 3. Nếu $s_i > x$ thì gán $x := s_i$.

Trên đây ta đã ghi một thuật toán bằng ngôn ngữ thông thường. Trong trường hợp thuật toán được viết bằng ngôn ngữ của máy tính, ta có một *chương trình.*

Để kết thúc, chúng ta hãy thảo luận thêm một vài tính chất của các thuật toán.

Một *thuật toán* là một tập hợp các chỉ thị có những đặc trưng sau:

- *Tính chính xác.* Các bước được phát biểu một cách chính xác.
- *Tính duy nhất.* Các kết quả trung gian trong mỗi bước thực hiện được xác định một cách duy nhất và chỉ phụ thuộc vào dữ liệu đưa vào và các kết quả của bước trước.
- *Tính hữu hạn.* Thuật toán dừng sau hữu hạn bước.
- *Đầu vào.* Thuật toán có dữ liệu vào.
- *Đầu ra.* Thuật toán có dữ liệu ra.
- *Tính tổng quát.* Thuật toán thực hiện trên một tập các dữ liệu vào.

Ngoài những yếu tố kể trên, ta còn phải xét đến tính hiệu quả của thuật toán. Có rất nhiều thuật toán, về mặt lý thuyết là kết thúc sau hữu hạn bước, tuy nhiên thời gian "hữu hạn" đó vượt quá khả năng làm việc của chúng ta. Những thuật toán đó sẽ không được xét ở đây, vì chúng ta chỉ quan tâm những thuật toán có thể sử dụng thực sự trên máy tính.

Cũng do mục tiêu nói trên, ta còn phải chú ý đến độ phức tạp của các thuật toán. Độ phức tạp của một thuật toán có thể đo bằng không gian, tức là *dung lượng bộ nhớ* của máy tính cần thiết để thực hiện thuật toán, và bằng thời gian, tức là *thời gian máy tính làm việc.*

Bài tập

1. Viết thuật toán tìm giá trị nhỏ nhất của dãy

$$s_1, s_2, \ldots, s_n.$$

2. Viết thuật toán tìm vị trí đầu tiên của phần tử lớn nhất trong dãy

$$s_1, s_2, \ldots, s_n.$$

Chẳng hạn, vị trí đầu tiên của phần tử lớn nhất trong dãy

$$6.2, 8.9, 4.2, 8.9$$

là 2.

3. Viết thuật toán tìm vị trí sau cùng của phần tử lớn nhất trong dãy

$$s_1, s_2, \ldots, s_n.$$

Chẳng hạn, vị trí sau cùng của phần tử lớn nhất trong dãy

$$6.2, 8.9, 4.2, 8.9$$

là 4.

4. Viết thuật toán đảo ngược vị trí của dãy

$$s_1, s_2, \ldots, s_n.$$

5. Viết thuật toán cộng hai số nguyên dương.
6. Viết thuật toán nhân hai số nguyên dương.
7. Viết thuật toán kiểm tra tính đối xứng của ma trận vuông.
8. Viết thuật toán kiểm tra tính phản đối xứng của ma trận vuông.

3.2 Thuật toán Euclid

Phần này trình bày thuật toán Euclid tìm ước số chung lớn nhất của hai số nguyên. Ước số chung lớn nhất của hai số nguyên n và m (không đồng thời bằng không) là số nguyên dương lớn nhất và là ước số của m và n. Chẳng hạn, ước số chung lớn nhất của 4 và 6 là 2 và ước số chung lớn nhất của 3 và 8 là 1.

Nếu $a, b, q \in \mathbb{Z}, b \neq 0$, sao cho $a = bq$, ta nói *a chia hết cho b* và ký hiệu $b \mid a$; trong trường hợp này, ta nói q là *thương* và b là *ước số* của a. Nếu a không chia hết cho b, ta viết $b \nmid a$.

Ví dụ 3.2.1. Vì $21 = 3 \cdot 7$ nên $3 \mid 21$. Thương là 7.

Định nghĩa 3.2.1. Giả sử n và m là hai số nguyên không đồng thời bằng không. Số nguyên x gọi là *ước số chung* của m và n nếu x là ước số của m và n. Số nguyên

$$\text{USCLN}(m, n) := \max\{x \mid x \text{ là ước số chung của } m \text{ và } n\}$$

gọi là *ước số chung lớn nhất.*

Ví dụ 3.2.2. Các ước số nguyên dương của số 30 là

$$1, 2, 3, 5, 6, 10, 15, 30$$

và các ước số nguyên dương của số 105 là

$$1, 3, 5, 7, 15, 21, 35, 105;$$

do vậy các ước số chung dương của 30 và 105 là

$$1, 3, 5, 15.$$

Suy ra ước số chung lớn nhất của 30 và 105 là $\text{USCLN}(30, 105) = 15$.

Định lý 3.2.2. *Giả sử m, n và c là các số nguyên. Khi đó*

(a) Nếu c là ước số chung của m và n thì

$$c \mid (m + n).$$

(b) Nếu c là ước số chung của m và n thì

$$c \mid (m - n).$$

(c) Nếu $c \mid m$ thì $c \mid mn$.

Chứng minh. Bài tập. □

Tính chất 3.2.3. *Giả sử $a, b \in \mathbb{N}, b > 0$. Khi đó tồn tại các số nguyên q và r sao cho*

$$a = bq + r, \quad 0 \leq r < b, \quad q \geq 0.$$

Chứng minh. Bài tập. □

Ví dụ 3.2.3. Ta có

$$\begin{aligned} 22 &= 7 \times 3 + 1, \\ 24 &= 8 \times 3 + 0, \\ 103 &= 21 \times 4 + 19, \\ 0 &= 47 \times 0 + 0. \end{aligned}$$

Định lý 3.2.4. *Cho $a, b \in \mathbb{N}, b > 0$. Giả sử q và r là các số nguyên sao cho*

$$a = bq + r, \quad 0 \leq r < b, \quad q \geq 0.$$

Khi đó

$$\text{USCLN}(a, b) = \text{USCLN}(b, r).$$

Chứng minh. Bài tập. □

Ví dụ 3.2.4. Ta có

$$105 = 30 \times 3 + 15.$$

Suy ra

$$\text{USCLN}(105, 30) = \text{USCLN}(30, 15).$$

Lại có

$$30 = 15 \times 2 + 0.$$

Nên

$$\text{USCLN}(105, 30) = \text{USCLN}(30, 15) = \text{USCLN}(15, 0) = 15.$$

3.2.1 Thuật toán Euclid

Thuật toán này tìm ước số chung lớn nhất của hai số tự nhiên a và b, trong đó a, b không đồng thời bằng 0.

Vào: a, b là số tự nhiên không đồng thời bằng 0.
Ra: USCLN là ước số chung lớn nhất của a và b.

Bước 1. Nếu $a < b$ thì hoán đổi a và b.

Bước 2. Nếu $b = 0$ thì thực hiện USCLN $:= a$ và dừng.

Bước 3. Chia a cho b và nhận được $a = bq + r$ với $0 \leq r < b$.

Bước 4. Thực hiện $a := b, b := r$ và chuyển đến Bước 2.

Ví dụ 3.2.5. Ta sẽ áp dụng thuật toán Euclid để tính $\text{USCLN}(504, 396)$.

Đặt $a := 504, b := 396$. Vì $a > b$ nên ta chuyển đến Bước 2. Vì $b \neq 0$ nên chuyển đến Bước 3. Thực hiện Bước 3 ta có

$$504 = 396 \times 1 + 108.$$

Kế tiếp ta thực hiện Bước 4: đặt $a := 396, b := 108$ và chuyển đến Bước 2.

Vì $b \neq 0$ nên thực hiện Bước 3:

$$396 = 108 \times 3 + 72.$$

Thực hiện Bước 4: đặt $a := 108, b := 72$ và chuyển đến Bước 2.

Vì $b \neq 0$ nên thực hiện Bước 3:

$$108 = 72 \times 1 + 36.$$

Thực hiện Bước 4: đặt $a := 72, b := 36$ và chuyển đến Bước 2.

Vì $b \neq 0$ nên thực hiện Bước 3:

$$72 = 36 \times 2 + 0.$$

Thực hiện Bước 4: đặt $a := 36, b := 0$ và chuyển đến Bước 2.

Vì $b = 0$ nên áp dụng Bước 2 có USCLN $:= a = 36$ và thuật toán dừng. Vậy $\text{USCLN}(504, 396) = 36$.

Bài tập

1. Tìm các số nguyên q và r sao cho $a = bq + r$ với $0 \leq r < b$ và

   (a) $a := 45, b := 6$.

   (b) $a := 106, b := 12$.

   (c) $a := 66, b := 11$.

   (d) $a := 221, b := 17$.

   (e) $a := 0, b := 31$.

2. Dùng thuật toán Euclid để tìm ước số chung lớn nhất của cặp các số nguyên:

   $$(60, 90), (110, 273), (220, 1400), (315, 825), (20, 40).$$

3. Giả sử a, b, c là các số nguyên dương. Chứng minh nếu $a \mid b$ và $b \mid c$ thì $a \mid c$.

4. Giả sử a, b là các số nguyên dương. Chứng minh $\text{USCLN}(a, b) = \text{USCLN}(a, a + b)$.

5. Giả sử a, b là các số nguyên dương và p là số nguyên tố. Chứng minh nếu $p \mid ab$ thì hoặc $p \mid a$ hoặc $p \mid b$.

6. Tìm các số nguyên dương a, b, c sao cho $a \mid bc, a \nmid b$ và $a \nmid c$.

7. Giả sử $a > b \geq 0$. Chứng minh rằng

   $$\text{USCLN}(a, b) = \text{USCLN}(a - b, b).$$

8. Hãy viết một thuật toán tìm ước số chung lớn nhất của hai số nguyên không đồng thời bằng không sử dụng phép toán trừ thay cho phép toán chia.

3.3 Thuật toán đệ quy

Thuật toán đệ quy là một thuật toán gọi lại chính nó. Đệ quy là một công cụ hữu dụng và tự nhiên để giải quyết một lớp lớn các bài toán. Để giải những bài toán trong lớp này ta có thể sử dụng kỹ thuật *chia để trị*: Bài toán cần giải quyết được chia thành những bài toán con có dạng như bài toán ban đầu. Mỗi bài toán con lại được phân rã thêm. Quá trình phân rã cho đến khi nhận được những bài toán con với lời giải dễ dàng. Cuối cùng, tổ hợp các lời giải của các bài toán con ta được lời giải của bài toán ban đầu.

Ví dụ 3.3.1. n giai thừa của số tự nhiên n là số nguyên dương xác định bởi

$$n! := \begin{cases} 1 & \text{nếu } n = 0, \\ n(n-1)(n-2)\cdots 2 \cdot 1 & \text{nếu } n \geq 1. \end{cases}$$

Tức là nếu $n \geq 1$ thì $n!$ bằng tích của tất cả các số tự nhiên từ 1 đến n. Chẳng hạn,

$$\begin{aligned} 3! &= 3 \cdot 2 \cdot 1 = 6, \\ 6! &= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720. \end{aligned}$$

Từ định nghĩa suy ra

$$n! = n \cdot (n-1)!$$

với mọi $n \geq 1$. Vì vậy, bài toán ban đầu (tính $n!$) được phân rã thành các bài toán con (tính $(n-1)!$, tính $(n-2)!, \cdots$) cho đến bài toán con được giải dễ dàng là tính 0!. Cuối cùng, lời giải của các bài toán con được tổ hợp lại bằng phép nhân để nhận được lời giải bài toán ban đầu.

Thuật toán đệ quy dưới đây tính các giai thừa.

3.3.1 Tính n giai thừa

Thuật toán này tính $n!$.

Vào: n là số tự nhiên.
Ra: $n!$.

Bước 1. Nếu $n = 0$ thì xuất 1 và dừng.

Bước 2. Sử dụng thuật toán này để tính $(n-1)!$. Xuất $(n-1)!n$.

Định lý 3.3.1. *Thuật toán 3.3.1 tính giá trị của $n!$ với mọi $n \in \mathbb{N}$.*

Chứng minh. Chứng minh sử dụng quy nạp toán học. □

Kế tiếp ta trình bày thuật toán đệ quy tìm ước số chung lớn nhất của hai số tự nhiên không đồng thời bằng không.

Ta biết rằng nếu a là số nguyên không âm, b là số nguyên dương và

$$a = bq + r, \quad 0 \leq r < b,$$

thì

$$\text{USCLN}(a, b) = \text{USCLN}(b, r).$$

Điều này dễ dàng suy ra thuật toán đệ quy tìm ước số chung lớn nhất của hai số tự nhiên không đồng thời bằng không.

3.3.2 Tìm ước số chung lớn nhất

Thuật toán này tìm ước số chung lớn nhất của hai số tự nhiên a và b, trong đó a, b không đồng thời bằng 0.

Vào: a, b là số tự nhiên không đồng thời bằng 0.
Ra: x là ước số chung lớn nhất của a và b.

Bước 1. Nếu $a < b$ thì hoán đổi a và b.

Bước 2. Nếu $b = 0$ thì thực hiện $x := a$ và dừng.

Bước 3. Chia a cho b và nhận được $a = bq + r$ với $0 \leq r < b$.

Bước 4. Gọi thuật toán này để tính ước số chung lớn nhất của b và r. Lưu trữ giá trị này trong x.

Ví dụ cuối cùng là thuật toán đệ quy xác định bước đi của người máy.

Ví dụ 3.3.2. Một người máy có thể bước 1 hoặc 2 meter. Hãy tính số cách để người máy có thể bước n meter. Chẳng hạn:

Khoảng cách	Dãy các bước	Số cách để bước
1	1	1
2	1, 1, hoặc 2	2
3	1, 1, 1, hoặc 1, 2 hoặc 2, 1	3
4	1, 1, 1, 1, hoặc 1, 1, 2 hoặc 1, 2, 1, hoặc 2, 1, 1 hoặc 2, 2	5

Gọi f_n là số cách để người máy có thể bước n meter. Ta có

$$f_1 = 1, \quad f_2 = 2.$$

Hơn nữa, có thể chứng minh công thức truy hồi sau:

$$f_n = f_{n-1} + f_{n-2}, \quad n \geq 3.$$

3.3.3 Thuật toán xác định dãy Fibonacci

Thuật toán này tính hàm xác định bởi

$$f_n := \begin{cases} 1, & \text{nếu } n = 1 \\ 2, & \text{nếu } n = 2 \\ f_{n-1} + f_{n-2}, & \text{nếu } n > 2. \end{cases}$$

Vào: n là số tự nhiên.
Ra: f_n.

Bước 1. Nếu $n = 1$ hoặc $n = 2$ thì xuất n và dừng.

Bước 2. Tính f_{n-1} và f_{n-2} và xuất $f_{n-1} + f_{n-2}$.

Dãy

$$f_1, f_2, f_3, \ldots,$$

có các giá trị đầu tiên

$$1, 2, 3, 5, 8, 13, \ldots,$$

gọi là *dãy Fibonacci.*

Bài tập

1. (a) Sử dụng công thức

$$\begin{aligned} s_1 &= 1, \\ s_n &= s_{n-1} + n, \quad n \geq 2, \end{aligned}$$

hãy viết thuật toán dạng đệ quy tính tổng

$$s_n := 1 + 2 + 3 + \cdots + n.$$

(b) Sử dụng quy nạp toán học, chứng minh tính đúng của thuật toán trong câu (a).

2. (a) Sử dụng công thức

$$\begin{aligned} s_1 &= 2, \\ s_n &= s_{n-1} + 2n, \quad n \geq 2, \end{aligned}$$

hãy viết thuật toán dạng đệ quy tính tổng

$$s_n := 2 + 4 + 6 + \cdots + 2n.$$

(b) Sử dụng quy nạp toán học, chứng minh tính đúng của thuật toán trong câu (a).

3. (a) Một người máy có thể bước 1 meter, 2 meter hoặc 3 meter. Hãy viết thuật toán dạng đệ quy tính số cách người máy có thể bước n meter.

(b) Sử dụng quy nạp toán học, chứng minh tính đúng của thuật toán trong câu (a).

4. Hãy viết một thuật toán dạng đệ quy tìm ước số chung lớn nhất của hai số nguyên không đồng thời bằng không sử dụng phép toán trừ thay cho phép toán chia.

5. Viết thuật toán không đệ quy tính n giai thừa.

6. Một người máy có thể bước 1 hoặc 2 meter. Hãy viết thuật toán liệt kê tất cả các cách người máy có thể bước n meter.

7. Một người máy có thể bước 1, 2 hoặc 3 meter. Hãy viết thuật toán liệt kê tất cả các cách người máy có thể bước n meter.

8. Ký hiệu f_n là dãy Fibonacci. Sử dụng quy nạp toán học, chứng minh các quan hệ sau:

(a) $\sum_{k=1}^{n} f_k = f_{n+2} - 2, \quad n \geq 1.$

(b) $f_n^2 = f_{n-1} f_{n+1} + (-1)^n, \quad n \geq 2.$

(c) $f_{n+2}^2 - f_{n+1}^2 = f_n f_{n+3}, \quad n \geq 1.$

(d) $\sum_{k=1}^{n} f_k^2 = f_n f_{n+1} - 1, \quad n \geq 1.$

(e) f_n chẵn nếu và chỉ nếu $n + 1$ chia hết cho 3.

(f) với mọi $n \geq 5$ có

$$f_n > \left(\frac{3}{2}\right)^n.$$

(g) với mọi $n \geq 1$ có

$$f_n < 2^n.$$

(h) với mọi $n \geq 1$ có

$$\begin{aligned} \sum_{k=1}^{n} f_{2k-1} &= f_{2n} - 1, \\ \sum_{k=1}^{n} f_{2k} &= f_{2n+1} - 1. \end{aligned}$$

(i) Mọi số nguyên dương có thể viết dạng tổng của các số Fibonacci phân biệt và không có hai số nào là liên tiếp. Chứng minh cách viết này là duy nhất.

9. Giả sử có công thức đạo hàm của tích

$$\frac{d(fg)}{dx} = f\frac{dg}{dx} + g\frac{df}{dx}.$$

Dùng quy nạp toán học, chứng minh công thức

$$\frac{dx^n}{dx} = nx^{n-1}, \quad n \geq 1.$$

3.4 Độ phức tạp của thuật toán

Một chương trình máy tính, thậm chí dựa vào một thuật toán đúng, có thể không hữu dụng đối với một lớp các dữ liệu vào do thời gian cần thiết chạy chương trình hoặc không gian lưu trữ dữ liệu, các biến... quá lớn. *Phân tích thuật toán* đề cập đến quá trình ước lượng thời gian và không gian cần thiết để thực hiện thuật toán. *Độ phức tạp của thuật toán* ám chỉ đến số lượng thời gian và không gian đòi hỏi để thực hiện thuật toán.

Thời gian cần thiết để thực hiện một thuật toán là một hàm phụ thuộc dữ liệu đầu vào. Thường thì khó có thể xác định chính xác hàm này. Vì vậy, chúng ta sẽ sử dụng các tham số đặc trưng *kích thước* của dữ liệu đưa vào. Có ba khái niệm:

(a) *Thời gian trường hợp tốt nhất* là thời gian ít nhất để thực hiện thuật toán.

(b) *Thời gian trường hợp xấu nhất* là thời gian nhiều nhất để thực hiện thuật toán.

(c) *Thời gian trường hợp trung bình* là thời gian trung bình để thực hiện thuật toán.

Định nghĩa 3.4.1. Giả sử $f, g\colon \mathbb{N} \to \mathbb{R}$ là hai hàm số. Ta viết

$$f(n) = O(g(n))$$

và nói $f(n)$ có *bậc nhiều nhất* $g(n)$ nếu tồn tại hằng số dương C sao cho ngoài một tập hữu hạn các số tự nhiên ta luôn có

$$|f(n)| \leq C|g(n)|.$$

Khi đó ta nói $f(n)$ là *O-lớn* của $g(n)$.

Ví dụ 3.4.1. Ta có các quan hệ sau

$$\begin{aligned} 70n^2 + 5n + 1 &= O(n^2), \\ 2n + 3\ln n &= O(n), \\ 1 + 2 + \cdots + n &= O(n^2). \end{aligned}$$

Định lý 3.4.2. *Giả sử*

$$f(n) := a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0$$

là đa thức bậc k theo biến n. Khi đó

$$f(n) = O(n^k).$$

Chứng minh. Bài tập. □

Ví dụ 3.4.2. Vì $3n^4 - 7n^2 + 4n$ là đa thức bậc 4 theo biến n nên

$$3n^4 - 7n^2 + 4n = O(n^4).$$

Định nghĩa 3.4.3. Nếu một thuật toán đòi hỏi $t(n)$ đơn vị thời gian trong trường hợp tốt nhất (tương ứng, xấu nhất hoặc trung bình) với dữ liệu vào có kích thước n và

$$t(n) = O(g(n))$$

thì ta nói *thời gian trường hợp tốt nhất (tương ứng, xấu nhất hoặc trung bình) thực hiện thuật toán là $O(g(n))$.*

Giả sử $t(n) = O(g(n))$. Ta nói thuật toán *có độ phức tạp đa thức* hoặc *có thời gian đa thức* nếu $g(n)$ là đa thức theo biến n.

Ví dụ 3.4.3. Ký hiệu $t(n)$ là số lần câu lệnh $x := x + 1$ được thực hiện trong thuật toán sau:

Bước 1. Với $i := 1$ đến n thực hiện Bước 2.

Bước 2. Với $j := 1$ đến i thực hiện Bước 3.

Bước 3. $x := x + 1$.

Dễ thấy

$$t(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Suy ra

$$t(n) = O(n^2).$$

Ví dụ 3.4.4. Ký hiệu $t(n)$ là số lần câu lệnh $x := x + 1$ được thực hiện trong thuật toán sau:

Bước 1. Đặt $j := n$.

Bước 2. Nếu $j < 1$ thì dừng thuật toán.

Bước 3. Với $i := 1$ đến j thực hiện Bước 4.

Bước 4. Đặt $x := x + 1$.

Bước 5. Đặt $j := \lfloor j/2 \rfloor$.

Bước 6. Chuyển đến Bước 2.

Có thể chỉ ra

$$t(n) = O(n).$$

Ví dụ 3.4.5. Xét thuật toán tìm kiếm trong một dãy không được sắp thứ tự sau:

Vào: $s, s_1, s_2, \ldots, s_n$.
Ra: $j = 0$ nếu $s \neq s_i$ với mọi i; ngược lại, j là chỉ số nhỏ nhất sao cho $s = s_j$.

Bước 1. Với $i := 1$ đến n thực hiện Bước 2.

Bước 2. Nếu $s = s_i$ thì đặt $j := i$ và dừng thuật toán.

Bước 3. Đặt $j := 0$.

Có thể chứng minh thời gian trường hợp tốt nhất bằng $O(1)$, thời gian trường hợp xấu nhất bằng thời gian trường hợp trung bình và bằng $O(n)$.

Bài tập

1. Xác định ký hiệu O lớn đối với $f(n) + g(n)$ nếu

   (a) $f(n) := O(1), g(n) := O(n^2)$.
   (b) $f(n) := 6n^3 - 2n^2 + 4, g(n) := O(n \ln n)$.
   (c) $f(n) := O(n^{3/2}), g(n) := O(n^{5/2})$.

2. Xác định độ phức tạp tính toán với các thuật toán sau (xét số lần thực hiện câu lệnh $x := x + 1$):

   Bước 1. Với $i := 1$ đến $2n$ thực hiện $x := x + 1$.

3. Xác định độ phức tạp tính toán với các thuật toán sau (xét số lần thực hiện câu lệnh $x := x + 1$):

   Bước 1. $i := 1$.

   Bước 2. Nếu $i > 2n$ thì dừng.

   Bước 3. $x := x + 1$.

Bước 4. $i := i + 2$.

Bước 5. Chuyển đến Bước 2.

4. Xác định độ phức tạp tính toán với các thuật toán sau (xét số lần thực hiện câu lệnh $x := x + 1$):

   Bước 1. Với $i := 1$ đến n và với $j := 1$ đến n thực hiện $x := x + 1$.

5. Xác định độ phức tạp tính toán với các thuật toán sau (xét số lần thực hiện câu lệnh $x := x + 1$):

   Bước 1. Với $i := 1$ đến $2n$ và với $j := 1$ đến n thực hiện $x := x + 1$.

6. Xác định độ phức tạp tính toán với các thuật toán sau (xét số lần thực hiện câu lệnh $x := x + 1$):

   Bước 1. Với $i := 1$ đến $2n$ thực hiện Bước 2.

   Bước 2. Với $j := 1$ đến $\lfloor i/2 \rfloor$ thực hiện $x := x + 1$.

7. Xác định số phép toán so sánh và ký hiệu O lớn trong thuật toán sau

   Vào: $s_1, s_2, \ldots, s_n$.
   Ra: $M := \max_i s_i$ và $m := \min_i s_i$.

   Bước 1. $t := 2\lfloor n/2 \rfloor$.

   Bước 2. $i := 1$.

   Bước 3. Nếu $i > t - 1$ thì chuyển đến Bước 7.

   Bước 4. Nếu $s_i > s_{i+1}$ thì hoán đổi s_i và s_{i+1}.

   Bước 5. $i := i + 2$.

   Bước 6. Chuyển đến Bước 3.

   Bước 7. Nếu $n \leq t$ thì chuyển đến Bước 10.

   Bước 8. Nếu $s_{m-1} > s_n$ thì hoán đổi s_{m-1} và s_n.

   Bước 9. Nếu $s_n > s_m$ thì hoán đổi s_m và s_n.

   Bước 10. $m := s_1$.

   Bước 11. $M := s_2$.

   Bước 12. $i := 3$.

   Bước 13. Nếu $i > t - 1$ thì dừng.

   Bước 14. Nếu $s_i < m$ thì gán $m := s_i$.

   Bước 15. Nếu $s_{i+1} > M$ thì gán $M := s_{i+1}$.

   Bước 16. $i := i + 1$.

   Bước 17. Chuyển đến Bước 13.

8. Giả sử $a > 1$ và $f(n) := O(\log_a n)$. Chứng minh rằng $f(n) = O(\ln n)$.

9. Giả sử $g(n) > 0$ với mọi $n \in \mathbb{N}$. Chứng minh $f(n) = O(g(n))$ nếu và chỉ nếu tồn tại hằng số dương c sao cho
$$|f(n)| \leq cg(n)$$
với mọi $n \in \mathbb{N}$.

10. Chứng minh rằng nếu
$$f(n) = O(h(n)) \quad \text{và} \quad g(n) = O(h(n))$$
thì
$$f(n) + g(n) = O(h(n)) \quad \text{và} \quad cf(n) = O(h(n))$$
với mọi $c \in \mathbb{R}$.

11. Chứng minh $n! = O(n^n)$.

12. Chứng minh $2^n = O(n!)$.

13. Chứng minh $n \ln n = O(\ln(n!))$.

14. Chứng minh $\ln(n!) = O(n \ln n)$.

15. Tìm các hàm f và g sao cho
$$f(n) \neq O(g(n)) \quad \text{và} \quad g(n) \neq O(f(n)).$$

16. Tìm các hàm f, g, h và k sao cho
$$f(n) = O(g(n)), h(n) = O(k(n)), f(n) - h(n) \neq O(g(n) - k(n)).$$

17. Ta viết $f(n) = \Theta(g(n))$ nếu tồn tại các hằng số dương C_1, C_2 sao cho
$$C_1|g(n)| \leq |f(n)| \leq C_2|g(n)|$$
ngoài một tập hợp con hữu hạn của tập các số tự nhiên $\mathbb{N}$. Chứng minh rằng
   (a) $2n - 1 = \Theta(n)$.
   (b) $3n^2 - 1 = \Theta(n^2)$.
   (c) $(4n - 1)^2 = \Theta(n^2)$.
   (d) $(2n - 1)(7n + 1)/(n - 1) = \Theta(n)$.
   (e) Quan hệ $f(n) = \Theta(g(n))$ là quan hệ tương đương?

18. Ta viết $f \sim g$ nếu $f(n) = O(g(n))$. Quan hệ $\sim$ là quan hệ tương đương trên tập các số tự nhiên $\mathbb{N}$?

19. Sử dụng tích phân xác định, chứng minh bất đẳng thức sau

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \ln n.$$

Từ đó suy ra

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < O(\ln n).$$

20. Sử dụng tích phân xác định, chứng minh bất đẳng thức sau

$$1^m + 2^m + \cdots + n^m < \frac{(n+1)^{m+1}}{m+1},$$

trong đó m là số nguyên dương.

21. Chứng minh hoặc cho phản ví dụ các khẳng định sau:

(a) Nếu tồn tại giới hạn hữu hạn

$$\lim_{n\to\infty} \frac{f(n)}{g(n)}$$

thì $f(n) = O(g(n))$.

(b) Nếu $f(n) = O(g(n))$ thì tồn tại giới hạn hữu hạn

$$\lim_{n\to\infty} \frac{f(n)}{g(n)}.$$

(c) Nếu tồn tại giới hạn hữu hạn

$$\lim_{n\to\infty} \frac{f(n)}{g(n)}$$

thì $f(n) = \Theta(g(n))$.

(d) Nếu

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$$

thì $f(n) = \Theta(g(n))$.

(e) Nếu $f(n) = \Theta(g(n))$ thì tồn tại giới hạn hữu hạn

$$\lim_{n\to\infty} \frac{f(n)}{g(n)}.$$

3.5 Phân tích thuật toán Euclid

Phần này phân tích trường hợp xấu nhất của thuật toán Euclid tìm ước số chung lớn nhất của hai số tự nhiên a và b, trong đó a, b không đồng thời bằng 0. Trước hết ta nhắc lại thuật toán này:

Vào: a, b là số tự nhiên không đồng thời bằng 0.
Ra: USCLN là ước số chung lớn nhất của a và b.

Bước 1. Nếu $a < b$ thì hoán đổi a và b.

Bước 2. Nếu $b = 0$ thì thực hiện USCLN $:= a$ và dừng.

Bước 3. Chia a cho b và nhận được $a = bq + r$ với $0 \leq r < b$.

Bước 4. Thực hiện $a := b, b := r$ và chuyển đến Bước 2.

Ta định nghĩa thời gian để thực hiện thuật toán Euclid là số phép toán chia trong Bước 3. Trường hợp xấu nhất đối với thuật toán Euclid xảy ra khi số phép chia nhiều nhất. Nhắc lại rằng, dãy Fibonacci $\{f_n\}$ xác định bởi

$$f_1 := 1, \quad f_2 := 2; \quad f_n := f_{n-1} + f_{n-2},\ n \geq 3.$$

Ta có

Định lý 3.5.1. *Giả sử thuật toán Euclid đối với cặp các số tự nhiên a, b với $a > b$ cần n phép toán chia. Khi đó $a \geq f_{n+1}$ và $b > f_n$ trong đó $\{f_n\}$ là dãy Fibonacci.*

Chứng minh. Sử dụng quy nạp toán học. □

Định lý này dễ dàng suy ra

Định lý 3.5.2. *Giả sử thuật toán Euclid đối với cặp các số tự nhiên không đồng thời bằng không và thuộc khoảng $[0, m], m \geq 8$. Khi đó số phép chia cần thiết trong thuật toán Euclid không vượt quá*

$$\log_{3/2} \frac{2m}{3}.$$

Chứng minh. Bài tập. □

Vì hàm logarithm có cấp tăng chậm, kết quả trên chứng tỏ thuật toán Euclid rất hiệu quả thậm chí đối với các giá trị đầu vào rất lớn.

Bài tập

1. Có nhiều nhất bao nhiêu phép toán chia trong thuật toán Euclid đối với cặp các số thay đổi trong khoảng từ 0 đến 1000000?
2. Chứng minh có chính xác n phép toán chia trong thuật toán Euclid đối với cặp số $(f_n, f_{n+1}), n \geq 1$.
3. Chứng minh với mọi số nguyên $k > 1$ ta có số phép toán chia trong thuật toán Euclid đối với hai cặp số (a, b) và (ka, kb) là bằng nhau.
4. Chứng minh rằng USCLN$(f_n, f_{n+1}) = 1, n \geq 1$.

Chương 4

PHÉP ĐẾM

Toán tổ hợp nghiên cứu chủ yếu về cách sắp xếp các đối tượng. Đây là một bộ phận quan trọng của toán học rời rạc. Những vấn đề của tổ hợp được nghiên cứu từ Thế kỷ 17, liên quan trước tiên đến các trò chơi may rủi. Ngày nay toán tổ hợp được dùng rộng rãi trong tin học.

Mục đích của chương này là thiết lập một số phương pháp đếm các tập hợp gồm hữu hạn các phần tử mà không phải liệt kê các phần tử của chúng.

4.1 Các nguyên lý cơ bản của phép đếm

Nhắc lại: $\#S$ là số phần tử của tập hợp S. Do đó $\#S = \#T$ nếu hai tập S và T có cùng số các phần tử. Chú ý rằng

$$\#\emptyset = 0, \quad \#\{1, 2, \ldots, n\} = n \quad \text{với } n \in \mathbb{N}.$$

Chúng ta bắt đầu với một số nguyên lý đếm.

4.1.1 Nguyên lý tổng

Giả sử $A_1, A_2, \ldots, A_m$ là các sự kiện đôi một loại trừ nhau. Giả sử các sự kiện $A_1, A_2, \ldots, A_m$ có tương ứng $n_1, n_2, \ldots, n_m$ cách xảy ra. Khi đó sự kiện (hoặc A_1, hoặc A_2, ..., hoặc A_m) có $n_1 + n_2 + \cdots + n_m$ cách xảy ra.

Ví dụ 4.1.1. Lớp trưởng hoặc là một nữ sinh, hoặc là một nam sinh. Có bao nhiêu cách chọn lớp trưởng khác nhau nếu số học sinh nữ là 36 và số học sinh nam là 20?

Gọi A_1 (tương ứng, A_2) là sự kiện lớp trưởng là nữ sinh (tương ứng, nam sinh). Ta có 36 cách chọn lớp trưởng là nữ sinh và 20 cách chọn lớp trưởng là nam sinh. Theo nguyên lý tổng, sự kiện (A_1 hoặc A_2) có $(36 + 20) = 56$ cách chọn.

Ví dụ 4.1.2. Một sinh viên có thể chọn đúng một chuyên đề tự chọn thuộc một trong ba danh sách. Ba danh sách này gồm 3, 5 và 9 chuyên đề. Hỏi sinh viên đó có bao nhiêu cách lựa chọn?

Theo nguyên lý tổng, có $3 + 5 + 9 = 17$ cách.

Nhận xét 3. Có thể phát biểu nguyên lý tổng theo thuật ngữ của lý thuyết tập hợp như sau: Nếu các tập $T_1, T_2, \ldots, T_m$ đôi một rời nhau thì số các phần tử của tập $T_1 \cup T_2 \cup \cdots \cup T_m$ bằng tổng số các phần tử của các tập này; tức là

$$\#(T_1 \cup T_2 \cup \ldots \cup T_m) = \sum_{i=1}^{m} \#T_i.$$

4.1.2 Nguyên lý tích

Giả sử $A_1, A_2, \ldots, A_m$ là các sự kiện đôi một loại trừ nhau. Giả sử các sự kiện $A_1, A_2, \ldots, A_m$ có tương ứng $n_1, n_2, \ldots, n_m$ cách xảy ra. Khi đó sự kiện (A_1 và A_2 và ... và A_m) có $n_1 \times n_2 \times \cdots \times n_m$ cách xảy ra.

Ví dụ 4.1.3. Giả sử có hai mặt nạ, ba mũ. Hỏi có mấy cách hoá trang?

Dùng nguyên lý tích, có $3 \times 2 = 6$ cách hoá trang khác nhau. Cũng có thể dùng lý thuyết tập hợp như sau: Mỗi cách hoá trang là một cách chọn $x \in X$ và một cách chọn $y \in Y$. Do đó số cách hoá trang là số các cặp (x, y) thuộc $X \times Y$ và do đó bằng $\#X \times \#Y = 2 \times 3 = 6$.

Nhận xét 4. Nguyên lý này cũng thường được phát biểu dưới dạng tập hợp như sau: Giả sử các tập $T_1, T_2, \ldots, T_m$ có hữu hạn phần tử và đôi một rời nhau. Khi đó số phần tử của tập tích Descartes $T_1 \times T_2 \times \cdots \times T_m$ bằng

$$\#T_1 \times \#T_2 \times \cdots \times \#T_m.$$

Ví dụ 4.1.4. Có bao nhiêu chuỗi bit khác nhau có độ dài 8? Mỗi bit có hai cách chọn, hoặc 0 hoặc 1. Do đó theo nguyên lý tích, có $2^8 = 256$ chuỗi bit có độ dài 8.

Ví dụ 4.1.5. Có bao nhiêu bảng số xe khác nhau, nếu mỗi bảng gồm ba chữ cái và theo sau là ba con số (giả thiết bảng chữ cái gồm 26 ký tự)?

Mỗi chữ cái có 26 cách chọn; mỗi số có 10 cách chọn. Do đó theo nguyên lý tích, số các bảng số xe khác nhau là:

$$26 \times 26 \times 26 \times 10 \times 10 \times 10 = 17.576.000.$$

Ví dụ 4.1.6. Có bao nhiêu ánh xạ khác nhau từ tập X có m phần tử vào tập Y có n phần tử?

Mỗi ánh xạ là một bộ m cách chọn một trong n phần tử của Y cho mỗi một trong m phần tử của X. Theo nguyên lý tích, số ánh xạ này bằng

$$\underbrace{n \times n \times \cdots \times n}_{m \text{ lần}} = n^m.$$

Ví dụ 4.1.7. Có bao nhiêu ánh xạ một-một (đơn ánh) khác nhau từ tập X có m phần tử vào tập Y có n phần tử?

Nếu $m > n$: không có ánh xạ một-một từ X vào Y.

Giả sử $m \leq n$ và $X := \{a_1, a_2, \ldots, a_m\}$.

+ Với phần tử a_1 có n cách chọn phần tử tương ứng trong Y.

+ Vì ánh xạ là một-một, nên đối với a_2 chỉ còn $(n-1)$ cách chọn.

$\vdots$

+ Tương tự, a_m chỉ còn $(n-m+1)$ cách chọn.

Theo nguyên lý tích, số ánh xạ một-một khác nhau bằng

$$n(n-1)(n-2)\cdots(n-m+1).$$

Ví dụ 4.1.8. Đếm số tập con của một tập hữu hạn S.

Giả sử $S := \{a_1, a_2, \ldots, a_n\}$. Dễ dàng thiết lập một tương ứng một-một giữa tập con P của S với các chuỗi bit độ dài n : bit thứ i bằng 1 nếu và chỉ nếu $a_i \in P$. Mặt khác, số các chuỗi bit độ dài n là 2^n nên số các tập con của S là 2^n.

Ví dụ 4.1.9. Cho hai đoạn chương trình sau:

Chương trình 1:

$k := 0$;
for $i_1 := 1$ to n_1 do $k := k + 1$;
for $i_2 := 1$ to n_2 do $k := k + 1$;
...
for $i_m := 1$ to n_m do $k := k + 1$;

Chương trình 2:

$k := 0$;
for $i_1 := 1$ to n_1 do
  for $i_2 := 1$ to n_2 do
    ...
      for $i_m := 1$ to n_m do $k := k + 1$;

Hỏi k sẽ lấy giá trị bao nhiêu sau khi mỗi đoạn chương trình trên được thực hiện?

+ Chương trình 1: Cứ mỗi vòng lặp địa phương, k tăng lên một đơn vị.

Gọi A_i là số lần lặp của vòng lặp thứ i. A_i có n_i khả năng. Hơn nữa A_i và $A_j, i \neq j$, loại trừ nhau. Do đó theo nguyên lý tổng, số vòng lặp là $n_1 + n_2 + \cdots + n_m$.

+ Chương trình 2: Cứ mỗi vòng lặp toàn cục, k tăng lên một đơn vị. Mỗi vòng lặp toàn cục do m vòng lặp địa phương ghép lại. Theo nguyên lý tích số vòng lặp toàn cục bằng $n_1 \times n_2 \times \cdots \times n_m$.

Trong nhiều trường hợp ta cần phải phối hợp cả hai nguyên lý tổng và tích; chẳng hạn, xét ví dụ sau:

Ví dụ 4.1.10. Giả sử mỗi người sử dụng máy tính có một mật mã, gồm từ 6 đến 8 ký tự; mỗi ký tự là một chữ cái hoa hoặc là một con số. Mỗi mật mã nhất thiết phải chứa ít nhất một con số. Hỏi có bao nhiêu mật mã có thể có?

Gọi P là tổng số các mật mã có thể có và P_6, P_7, P_8 là số các mật mã có thể có với độ dài tương ứng bằng 6, 7, 8.

Theo nguyên lý tổng: $P = P_6 + P_7 + P_8$.

Việc tính trực tiếp P_6 là khó. Ta tính gián tiếp như sau:

+ Số các chuỗi có độ dài 6, gồm chữ và số, bao gồm cả trường hợp không có con số nào theo nguyên lý tích là $(26 + 10)^6 = 36^6$.

+ Số các chuỗi độ dài 6, không chứa con số nào là 26^6.

+ Do đó $P_6 = 36^6 - 26^6 = 1.867.866.560$.

Tương tự cho P_7 và P_8 :

$$\begin{aligned} P_7 &= 36^7 - 26^7 = 70.332.353.920, \\ P_8 &= 36^8 - 26^8 = 2.612.282.842.880. \end{aligned}$$

Cuối cùng

$$P = P_6 + P_7 + P_8 = 2.684.483.063.360.$$

Nhận xét 5. Khi các sự kiện A_1 và A_2 có thể xảy ra *đồng thời* ta không thể dùng nguyên lý tổng. Trường hợp này cần sửa đổi như sau: Nếu vẫn cộng $(n_1 + n_2)$ ta đã đếm thừa, vì có trường hợp đã đếm hai lần cùng một sự kiện (một lần trong A_1, một lần trong A_2). Trường hợp này chỉ xảy ra khi nó đồng thời có thể xảy ra A_1 và A_2. Vì vậy cần trừ đi số trường hợp dôi thừa này.

4.1.3 Nguyên lý bao hàm-loại trừ

Giả sử A_1 và A_2 là hai sự kiện bất kỳ. Nếu sự kiện A_1 có thể xảy ra n_1 cách, sự kiện A_2 có thể xảy ra n_2 cách, thì sự kiện (A_1 hoặc A_2) có thể xảy ra $[(n_1 + n_2)-$ số cách (A_1 và A_2)] cách.

Bằng thuật ngữ tập hợp, nguyên lý bao hàm-loại trừ trở thành:

$$\#(A_1 \cup A_2) = \#A_1 + \#A_2 - \#(A_1 \cap A_2).$$

Ví dụ 4.1.11. Có bao nhiêu chuỗi bit độ dài 8 hoặc bắt đầu bằng 1, hoặc kết thúc bằng 00? (Có thể có chuỗi vừa bắt đầu bằng 1, vừa kết thúc bằng 00).

Gọi P_1 là số các chuỗi bit độ dài 8 bắt đầu bằng 1. Như vậy, phần tử thứ nhất đã được chọn, chỉ còn lại 7 bit. Theo nguyên lý tích,

$$P_1 = 2^7 = 128.$$

Gọi P_2 là số các chuỗi bit độ dài 8 kết thúc bằng 00. Theo nguyên lý tích

$$P_2 = 2^6 = 64.$$

Gọi P_3 là số các chuỗi bit độ dài 8 bắt đầu bằng 1 và kết thúc bằng 00. Theo nguyên lý tích

$$P_3 = 2^5 = 32.$$

Áp dụng nguyên lý bao hàm-loại trừ ta có

$$P = P_1 + P_2 - P_3 = 160.$$

Nguyên lý bao hàm-loại trừ có thể mở rộng cho trường hợp m sự kiện, nhưng phức tạp hơn, ta sẽ đề cập ở phần sau.

Sự công nhận ba nguyên lý được đề cập trên đây như là xuất phát điểm của lý thuyết tổ hợp:

+ Tính đúng đắn của ba nguyên lý trên là "đúng hiển nhiên". Quan điểm của chúng ta là công nhận 3 nguyên lý trên, coi như xuất phát điểm của lý thuyết tổ hợp. Các kết quả khác sẽ lần lượt được suy ra trực tiếp hoặc gián tiếp từ ba nguyên lý này.

+ Nếu không thoả mãn, cũng có thể tìm cách chứng minh ba nguyên lý này, như vậy ta lại phải cần đến các công cụ khác, thực chất ta lại công nhận một điều gì khác là "đúng hiển nhiên" để rồi suy luận ra ba nguyên lý trên.

Bài tập

1. Có bao nhiêu chuỗi 8 bit bắt đầu bằng 1100?

2. Có bao nhiêu chuỗi 8 bit bắt đầu và kết thúc bằng 1?

3. Có bao nhiêu chuỗi 8 bit có đúng một bit bằng 1? Đúng hai bit bằng 1? Có ít nhất một bit bằng 1?

4. Có bao nhiêu chuỗi 8 bit đọc xuôi và đọc ngược đều giống như nhau?

5. Các ký tự $ABCDE$ được sử dụng để tạo thành các chuỗi độ dài 3.

   (a) Có bao nhiêu chuỗi được tạo ra nếu cho phép lặp?

   (b) Có bao nhiêu chuỗi được tạo ra nếu không cho phép lặp?

   (c) Có bao nhiêu chuỗi bắt đầu bằng A được tạo ra nếu cho phép lặp?

   (d) Có bao nhiêu chuỗi bắt đầu bằng A được tạo ra nếu không cho phép lặp?

   (e) Có bao nhiêu chuỗi không chứa ký tự A được tạo ra nếu cho phép lặp?

   (f) Có bao nhiêu chuỗi không chứa ký tự A được tạo ra nếu không cho phép lặp?

6. Trên tập $X := \{5, 6, \ldots, 200\}$:

   (a) Có bao nhiêu số chẵn, (tương ứng, lẻ)?

   (b) Có bao nhiêu số chia hết cho 5?

   (c) Có bao nhiêu số gồm những chữ số phân biệt?

   (d) Có bao nhiêu số không chứa chữ số 0?

   (e) Có bao nhiêu số lớn hơn 101 và không chứa chữ số 6?

   (f) Có bao nhiêu số có các chữ số được sắp theo thứ tự tăng thực sự?

   (g) Có bao nhiêu số có dạng xyz với $0 \neq x < y$ và $y > z$?

7. Giả sử có 5 sách tin học, 3 sách máy tính, 2 sách vật lý.

   (a) Có bao nhiêu cách sắp xếp chúng lên giá sách?

   (b) Có bao nhiêu cách sắp xếp sao cho 5 sách tin học ở phía trái, còn 2 sách vật lý ở bên phải?

   (c) Có bao nhiêu cách sắp chúng lên giá sao cho tất cả các sách theo cùng nhóm được sắp kề nhau?

   (d) Có bao nhiêu cách sắp chúng lên giá sao cho hai sách vật lý không kề nhau?

8. Có 10 bản bản sao (copy) của một cuốn sách và có một bản sao của 10 cuốn sách khác. Có bao nhiêu cách có thể chọn 10 cuốn sách?

9. Có bao nhiêu tập con có nhiều nhất n phần tử của tập gồm $(2n + 1)$ phần tử?

10. Áp dụng nguyên lý bao hàm-loại trừ để giải:

    (a) Có bao nhiêu chuỗi 8 bit hoặc bắt đầu bằng 100 hoặc có bit thứ tư bằng 1?

    (b) Có bao nhiêu chuỗi 8 bit hoặc bắt đầu bằng 1 hoặc kết thúc bằng 1?

    (c) Có bao nhiêu chuỗi 8 bit trong đó hoặc bit thứ hai, hoặc bit thứ tư bằng 1?

4.2 Hoán vị và tổ hợp

Định nghĩa 4.2.1. *Hoán vị* của n phần tử $x_1, x_2, \ldots, x_n$ là một sắp xếp có thứ tự n phần tử này.

Ví dụ 4.2.1. Có sáu hoán vị của ba phần tử. Nếu các phần tử được ký hiệu là A, B, C thì sáu hoán vị là

$$ABC, ACB, BAC, BCA, CAB, CBA.$$

Định lý 4.2.2. *Có $n!$ hoán vị của n phần tử.*

Chứng minh. Ta chứng minh theo quy nạp. Một hoán vị của n phần tử có thể được xây dựng theo n bước liên tiếp: Chọn phần tử đầu tiên, chọn phần tử thứ hai, ..., chọn phần tử cuối cùng. Phần tử đầu tiên có thể chọn n cách. Ngay khi phần tử đầu tiên được chọn, phần tử thứ hai có thể được chọn $n-1$ cách. Khi phần tử thứ hai đã được chọn, phần tử thứ ba có thể được chọn $n-2$ cách, và vân vân. Theo nguyên lý quy nạp và sau đó nguyên lý tích, tồn tại

$$n(n-1)(n-2)\cdots 2\cdot 1 = n!$$

hoán vị của n phần tử. □

Ví dụ 4.2.2. Có

$$10! = 10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1 = 3.628.800$$

hoán vị của 10 phần tử.

Ví dụ 4.2.3. Có bao nhiêu hoán vị của các ký tự $ABCDEF$ chứa chuỗi con DEF?

Có thể xem chuỗi con DEF như một ký tự. Theo Định lý 4.2.2 có $4! = 24$ hoán vị của các ký tự $ABCDEF$ chứa chuỗi con DEF.

Ví dụ 4.2.4. Có bao nhiêu hoán vị của các ký tự $ABCDEF$ chứa các ký tự DEF theo thứ tự bất kỳ?

Ta có thể giải bài toán qua hai bước: Chọn một thứ tự của các ký tự DEF; và xây dựng một hoán vị của ABC chứa thứ tự đã cho của các ký tự DEF. Theo Định lý 4.2.2, bước đầu tiên có $3! = 6$ cách; theo Ví dụ 4.2.3 bước thứ hai có $4! = 24$ cách. Theo nguyên lý tích, số các hoán vị của $ABCDEF$ chứa các ký tự DEF theo thứ tự bất kỳ là $6\cdot 24 = 144$.

Trong một số trường hợp ta muốn khảo sát một thứ tự của r phần tử được chọn từ n phần tử. Một thứ tự như thế gọi là "r-hoán vị".

Định nghĩa 4.2.3. *r-hoán vị* của n phần tử (phân biệt) $x_1, x_2, \ldots, x_n$ là một sắp xếp r-phần tử có thứ tự từ n phần tử này. Ký hiệu $P(n, r)$ là số các r-hoán vị của tập n phần tử phân biệt.

Ví dụ 4.2.5. Ta có một số 2-hoán vị của a, b, c là

$$ab, bc, ac.$$

Nếu $r = n$ trong Định nghĩa 4.2.3, chúng ta nhận được một thứ tự của tất cả n phần tử. Theo Định lý 4.2.2 thì $P(n, n) = n!$. Tổng quát ta có

Định lý 4.2.4. *Số các r-hoán vị của tập n phần tử phân biệt là*

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1), \quad r \leq n.$$

Chứng minh. Chúng ta đếm số các cách có thứ tự của r phần tử được chọn từ tập gồm n phần tử. Có n cách chọn phần tử đầu tiên. Kế tiếp, có $n-1$ cách chọn phần tử thứ hai, $n-2$ cách chọn phần tử thứ ba, ..., có $n-r+1$ cách chọn phần tử thứ r. Do đó theo nguyên lý tích, số các r-hoán vị của tập n phần tử phân biệt là

$$n(n-1)(n-2)\cdots(n-r+1).$$

□

Ví dụ 4.2.6. Theo Định lý 4.2.4, số các 2-hoán vị của $X = \{a, b, c\}$ là

$$P(3, 2) = 3 \cdot 2 = 6.$$

Sáu hoán vị này là

$$ab, ac, ba, bc, ca, cb.$$

Ví dụ 4.2.7. Có bao nhiêu cách chọn một chủ tịch, một phó chủ tịch, một thư ký và một thủ quỹ từ một nhóm gồm 10 người?

Chúng ta cần đếm số các cách có thứ tự của 4 người được chọn từ một nhóm gồm 10 người. Theo Định lý 4.2.4 số các cách chọn là

$$P(10, 4) = 10 \cdot 9 \cdot 8 \cdot 7 = 5040.$$

Chú ý rằng cũng có thể suy ra kết quả trực tiếp từ nguyên lý tích (tại sao?).

Ví dụ 4.2.8. Một người bán hàng rong cần đi qua 7 địa điểm khác nhau. Ông ta có thể đi theo thứ tự bất kỳ. Có bao nhiêu hành trình khác nhau?

Số các hành trình có thể có là số các hoán vị từ tập gồm 7 phần tử:

$$P(7, 7) = 7! = 5040.$$

Nếu chẳng hạn ông ta muốn tìm hành trình có độ dài ngắn nhất, ông ta cần tính toán và so sánh 5040 hành trình cả thảy!(?).

Ta có thể viết

$$\begin{aligned} P(n,r) &= n(n-1)(n-2)\cdots(n-r+1) \\ &= \frac{n(n-1)(n-2)\cdots(n-r+1)(n-r)\cdots 2\cdot 1}{(n-r)\cdots 2\cdot 1} \\ &= \frac{n!}{(n-r)!}. \end{aligned}$$

Định nghĩa 4.2.5. Xét tập X chứa n phần tử phân biệt. Một *r-tổ hợp* của tập X là một bộ r phần tử, không phân biệt thứ tự, lấy từ tập này. Số các r-tổ hợp của tập gồm n phần tử phân biệt ký hiệu là $C(n,r)$ hay $\binom{n}{r}$ và gọi $C(n,r)$ là *tổ hợp chập r của n phần tử*.

Chúng ta sẽ xác định công thức cho $C(n,r)$ bằng cách đếm số các r-hoán vị của tập gồm n phần tử theo hai cách. Thứ nhất, sử dụng công thức $P(n,r)$. Cách thứ hai là đếm số các r-hoán vị của tập gồm n phần tử có liên quan với $C(n,r)$. Từ đó sẽ suy ra kết quả.

Ta có thể xây dựng r-hoán vị của tập n phần tử phân biệt qua hai bước liên tiếp: Đầu tiên, chọn một r-tổ hợp của X (tập con r phần tử không phân biệt thứ tự) và sau đó sắp thứ tự nó. Chẳng hạn, để xây dựng một 2-hoán vị của $\{a,b,c,d\}$ ta có thể chọn 2-tổ hợp và sau đó sắp thứ tự nó. Theo nguyên lý tích, số các r-hoán vị bằng tích của số các r-tổ hợp và số các cách sắp thứ tự của r phần tử. Tức là

$$P(n,r) = C(n,r)r!.$$

Vậy

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

Do đó theo Định lý 4.2.4 ta có

Định lý 4.2.6. *Số các r-hoán vị của tập n phần tử phân biệt là*

$$C(n,r) = \frac{n!}{(n-r)!r!}, \quad r \le n.$$

Ví dụ 4.2.9. Có bao nhiêu cách chọn 5 người từ 10 người để lập thành một đội bóng (không phân biệt thứ tự)?

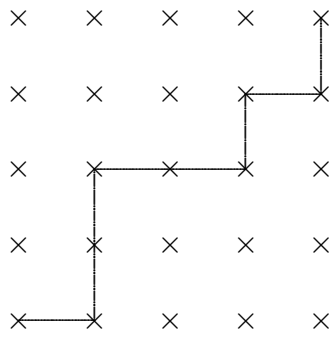
Câu trả lời là bằng số tổ hợp chập 5 của 10 phần tử

$$C(10,5) = \frac{10!}{5!5!} = 252.$$

Ví dụ 4.2.10. Có bao nhiêu cách chọn một hội đồng gồm hai người nữ và ba người nam từ một nhóm năm người nữ và sáu người nam?

Số cách chọn hai người nữ và ba người nam tương ứng là $C(5,2) = 10$ và $C(6,3) = 20$.

Hội đồng được xây dựng qua hai bước liên tiếp: Chọn người nữ; chọn người nam. Theo nguyên lý tích, tổng số các hội đồng là $10 \cdot 20 = 200$.



Hình 4.1:

Ví dụ 4.2.11. Có bao nhiêu chuỗi tám bit chứa chính xác bốn bit 1?

Một chuỗi tám bit chứa bốn bit 1 được xác định duy nhất ngay khi chúng ta biết các bit nào bằng 1. Nhưng điều này có thể thực hiện bởi $C(8, 4)$ cách.

Ví dụ 4.2.12. Có bao nhiêu hành trình từ góc dưới bên trái của một bàn cờ vuông kích thước $n \times n$ đến góc trên bên phải nếu chúng ta chỉ đi theo cách sang phải và lên trên? Một hành trình như vậy trên bàn cờ 4×4 được cho trong Hình 4.1.

Mỗi hành trình có thể được mô tả bởi một chuỗi độ dài $2n$ của n ký tự R và n ký tự U. Chẳng hạn, hành trình trong Hình 4.1 tương ứng chuỗi $RUURRURU$. Một chuỗi như vậy có thể nhận được bằng cách chọn n vị trí đối với R (không phân biệt thứ tự) trong số $2n$ vị trí cho phép của chuỗi và sau đó chèn n ký tự U vào những vị trí còn lại. Do đó số hành trình là $C(2n, n)$.

Bài tập

1. Có bao nhiêu hoán vị của a, b, c, d? Liệt kê các hoán vị này.
2. Có bao nhiêu 3-hoán vị của a, b, c, d? Liệt kê các hoán vị này.
3. Có bao nhiêu hoán vị, 5-hoán vị của 11 đối tượng khác nhau?
4. Có bao nhiêu cách chọn một chủ tịch, một phó chủ tịch và một thư ký từ một nhóm 11 người?
5. Có bao nhiêu cách chọn một chủ tịch, một phó chủ tịch, một kế toán và một thư ký từ một nhóm 12 người?
6. Có bao nhiêu chuỗi độ dài 5 có phân biệt thứ tự được tạo ra từ các ký tự A, B, C, D, E nếu:
   (a) Chứa chuỗi con ACE.
   (b) Chứa các ký tự ACE theo thứ tự tùy ý.

(c) Chứa các chuỗi con DB và AE.

(d) Chứa hoặc chuỗi con AE hoặc EA.

(e) Ký tự A xuất hiện trước ký tự D. Chẳng hạn $BCAED, BCADE$.

(f) Không chứa các chuỗi con AB, CD.

(g) Ký tự A xuất hiện trước ký tự C và C xuất hiện trước E.

7. Đặt $X := \{a, b, c, d\}$.

   (a) Tìm số các 3-tổ hợp của X. Liệt kê các tổ hợp này.

   (b) Tìm mối quan hệ giữa các 3-tổ hợp và 3-hoán vị của X.

8. Có bao nhiêu cách chọn một hội đồng gồm ba người từ nhóm 11 người?

9. Có bao nhiêu cách chọn một hội đồng gồm bốn người từ nhóm 12 người?

10. Một câu lạc bộ gồm sáu người nam và bảy người nữ.

    (a) Có bao nhiêu cách chọn một hội đồng gồm năm người?

    (b) Có bao nhiêu cách chọn một hội đồng gồm ba nam và bốn nữ?

    (c) Có bao nhiêu cách chọn một hội đồng gồm bốn người và ít nhất một nữ?

    (d) Có bao nhiêu cách chọn một hội đồng gồm bốn người với nhiều nhất một nam?

    (e) Có bao nhiêu cách chọn một hội đồng gồm bốn người có cả nam và nữ?

11. (a) Có bao nhiêu chuỗi 8 bit chứa chính xác ba bit 0?

    (b) Có bao nhiêu chuỗi 8 bit chứa ba bit 0 và 5 bit 1?

    (c) Có bao nhiêu chuỗi 8 bit chứa ít nhất hai bit 0?

12. Một cửa hàng có 50 máy tính trong đó có bốn bị hỏng.

    (a) Có bao nhiêu cách chọn bốn máy tính?

    (b) Có bao nhiêu cách chọn bốn máy tính không hỏng?

    (c) Có bao nhiêu cách chọn bốn máy tính trong đó có hai chiếc bị hỏng?

    (d) Có bao nhiêu cách chọn bốn máy tính trong đó có ít nhất một chiếc bị hỏng?

13. Xét một hành trình trên bàn cờ kích thước $m \times n$ từ góc trái bên dưới đến góc trên bên phải và theo hướng hoặc sang phải hoặc lên trên.

    (a) Số hành trình có thể là bao nhiêu?

    (b) Áp dụng để chứng minh đẳng thức

$$\sum_{k=0}^{n} C(k + m - 1, k) = C(m + n, m).$$

14. Chứng minh rằng số các chuỗi bit độ dài $n \geq 4$ chứa chính xác hai lần xuất hiện của chuỗi bit 10 là $C(n + 1, 5)$.

15. Chứng minh rằng số các chuỗi bit độ dài n chứa chính xác k bit 0 sao cho hai bit 0 không xuất hiện liên tiếp là $C(n-k+1,k)$.

16. Chứng minh rằng tích của k số nguyên liên tiếp chia hết cho $k!$.

17. Chứng minh rằng có $(2n-1)(2n-3)\cdot\ldots\cdot 3\cdot 1$ cách chọn n cặp từ $2n$ phần tử phân biệt.

18. Giả sử có n đối tượng trong đó có r đối tượng phân biệt và $n-r$ là đồng nhất. Chứng minh công thức
$$P(n,r) = r!C(n,r)$$
bằng cách đếm số có phân biệt thứ tự của n đối tượng theo hai cách:
+ Đầu tiên đếm số có phân biệt thứ tự các vị trí của r đối tượng phân biệt.
+ Đầu tiên đếm số có phân biệt thứ tự các vị trí của $n-r$ đối tượng đồng nhất.

4.3 Các thuật toán sinh ra hoán vị và tổ hợp

Nhóm nhạc rock của trường Đại học Đà Lạt có n bài hát cần ghi lên một đĩa CD. Các bài hát chiếm thời gian (tính bằng giây) tương ứng là
$$t_1, t_2, \ldots, t_n.$$
Đĩa CD có thể lưu trữ nhiều nhất là C giây. Vì đây là đĩa CD đầu tiên của nhóm, nên họ muốn ghi các bài hát với thời lượng càng nhiều càng tốt. Do đó bài toán là chọn một tập con $\{i_1, i_2, \ldots, i_k\}$ của $\{1,2,\ldots,n\}$ sao cho tổng
$$\sum_{j=1}^{k} t_{i_j} \tag{4.1}$$
không vượt quá C và lớn nhất có thể. Cách tiếp cận là kiểm tra tất cả các tập con của $\{1,2,\ldots,n\}$ và chọn một tập con sao cho tổng (4.1) lớn nhất có thể. Để thực hiện chúng ta cần một thuật toán tạo ra tất cả các tổ hợp của tập gồm n phần tử. Phần này trình bày các thuật toán sinh ra các hoán vị và tổ hợp.

Do có 2^n tập con của tập gồm n phần tử nên thời gian thực hiện của thuật toán kiểm tra tất cả các tập con ít nhất là $O(2^n)$. Những thuật toán như vậy là không hợp lý ngoại trừ với những giá trị n nhỏ. Tuy nhiên có những bài toán mà để giải nó không có cách nào tốt hơn là "liệt kê" tất cả các trường hợp.

Phương pháp liệt kê tất cả các tổ hợp và các hoán vị theo "thứ tự từ điển": Với hai từ đã cho, để xác định từ nào đứng trước trong từ điển, chúng ta so sánh các ký tự trong từ. Có hai khả năng:

(a) Mỗi ký tự trong từ ngắn hơn trùng với ký tự tương ứng trong từ dài hơn.

(b) Tại một vị trí nào đó, các ký tự trong hai từ khác nhau.

Nếu (a) đúng, từ ngắn hơn sẽ đứng trước. Chẳng hạn, "dog" đứng trước "doghouse" trong từ điển. Nếu (b) đúng chúng ta xác định vị trí bên trái nhất p mà tại đó các ký tự khác nhau. Thứ tự của các từ được xác định bởi thứ tự của các ký tự tại vị trí p. Chẳng hạn, "nha" đứng trước "nhanh" trong từ điển.

Để đơn giản ta sẽ định nghĩa thứ tự từ điển trên tập các ký hiệu là các số tự nhiên.

Định nghĩa 4.3.1. Giả sử $\alpha = s_1 s_2 \dots s_p$ và $\beta = t_1 t_2 \dots t_q$ là các chuỗi trên tập $\{1, 2, \dots, n\}$. Ta nói α *có thứ tự từ điển nhỏ hơn* β, ký hiệu $\alpha < \beta$, nếu hoặc

(a) $p < q$ và $s_i = t_i$ với $i = 1, 2, \dots, p$; hoặc

(b) Tồn tại i sao cho $s_i \neq t_i$, và với chỉ số i nhỏ nhất như vậy, ta có $s_i < t_i$.

Ví dụ 4.3.1. Trên tập $\{1, 2, 3, 4\}$ ta có $\alpha = 132 < \beta = 1324$. Trên tập $\{1, 2, 3, 4, 5, 6\}$ ta có $\alpha = 13246 < \beta = 1342$.

Đầu tiên ta xét bài toán liệt kê tất cả các r-tổ hợp của tập $\{1, 2, \dots, n\}$. Trong thuật toán, chúng ta sẽ liệt kê r-tổ hợp $\{x_1, x_2, \dots, x_r\}$ tương ứng chuỗi $s_1 s_2 \dots s_r$ trong đó $s_1 < s_2 < \cdots < s_r$ và $\{x_1, x_2, \dots, x_r\} = \{s_1, s_2, \dots, s_r\}$. Chẳng hạn, 3-tổ hợp $\{6, 2, 4\}$ sẽ tương ứng chuỗi 246.

Ta sẽ liệt kê các r-tổ hợp của tập $\{1, 2, \dots, n\}$ theo thứ tự từ điển. Do đó, các chuỗi được liệt kê đầu tiên và cuối cùng tương ứng là $12 \dots r$ và $(n - r + 1) \dots n$.

Ví dụ 4.3.2. Liệt kê tất cả 5-tổ hợp của $\{1, 2, 3, 4, 5, 6, 7\}$.

Chuỗi đầu tiên là 12345, theo sau là 12346 và 12347. Chuỗi kế tiếp là 12356 và sau đó 12357. Chuỗi cuối cùng là 34567.

Ví dụ 4.3.3. Tìm chuỗi tiếp theo 13467 khi chúng ta liệt kê 5-tổ hợp của tập hợp $X := \{1, 2, 3, 4, 5, 6, 7\}$.

Không có chuỗi nào bắt đầu với 134 và các biểu diễn của một tổ hợp 5 phần tử của X phải lớn hơn 13467. Do đó chuỗi tiếp theo 13467 phải bắt đầu là 135. Vì 13567 là chuỗi nhỏ nhất bắt đầu bằng 135 và là một tổ hợp của 5 phần tử của X nên 13567 là tổ hợp phải tìm.

Ví dụ 4.3.4. Tìm chuỗi tiếp theo 2367 khi chúng ta liệt kê 4-tổ hợp của tập hợp $X := \{1, 2, 3, 4, 5, 6, 7\}$.

Không có chuỗi nào bắt đầu với 23 và các biểu diễn của một tổ hợp 4 phần tử của X phải lớn hơn 2367. Do đó chuỗi tiếp theo 2367 phải bắt đầu là 24. Vì 2456 là chuỗi nhỏ nhất bắt đầu bằng 24 và là một tổ hợp của 5 phần tử của X nên 2456 là tổ hợp phải tìm.

Xét chuỗi $\alpha = s_1 s_2 \dots s_r$ biểu diễn tổ hợp $\{x_1, x_2, \dots, x_r\}$. Để tìm chuỗi kế tiếp $\beta = t_1 t_2 \dots t_r$ ta tìm phần tử bên phải nhất s_m mà không phải là giá trị cực đại của nó tại đó. (s_r có thể lấy giá trị cực đại n, s_{r-1} có thể lấy giá trị cực đại $n-1, \dots$). Khi đó

$$t_i = s_i, \quad \text{với } i = 1, 2, \dots, m-1.$$

Phần tử t_m bằng $s_m + 1$. Những phần tử còn lại của chuỗi β xác định bởi

$$t_{m+1} = s_m + 2, \quad t_{m+2} = s_m + 3, \dots .$$

Thuật toán sinh các tổ hợp

Bước 1. [Khởi tạo chuỗi] Đặt $s_i = i, i = 1, 2 \dots, r$.

Bước 2. [Xuất tổ hợp đầu tiên] Xuất chuỗi $s = s_1 s_2 \dots s_r$.

Bước 3. [Lặp] Với mỗi $i = 2, 3, \dots, C(n, r)$ thực hiện các bước sau:

3.1. Tìm phần tử bên phải nhất không phải là giá trị cực đại của nó.

3.2. (Giá trị cực đại của s_k được định nghĩa là $n - r + k$).

3.3. Đặt $s_m = s_m + 1$.

3.4. Với mỗi $j = m+1, \dots, r$, đặt $s_j = s_{j-1} + 1$.

3.5. Xuất s.

Ví dụ 4.3.5. Xét tập $\{1, 2, 3, 4, 5, 6, 7\}$. Giả sử

$$s_1 = 2, s_2 = 3, s_3 = 4, s_4 = 6, s_5 = 7.$$

Ta có s_3 là phần tử bên phải nhất không phải là giá trị cực đại của nó tại đó. Áp dụng thuật toán trên, ta có chuỗi tiếp theo 23467 là 23567.

Ví dụ 4.3.6. Thuật toán tạo 4-tổ hợp của $\{1, 2, 3, 4, 5, 6\}$ cho ta

$$1234, 1235, 1236, 1246, 1256, 1345, 1346,$$

$$1356, 1456, 2345, 2346, 2356, 3456.$$

Tương tự thuật toán sinh các tổ hợp, thuật toán sinh các hoán vị sẽ liệt kê theo thứ tự từ điển.

Ví dụ 4.3.7. Để xây dựng hoán vị của tập $\{1, 2, 3, 4, 5, 6\}$ sau hoán vị 163542, chúng ta cần cố định các chữ số bên trái nhiều nhất có thể.

Tồn tại hoán vị tiếp theo hoán vị 1635__? Vì hoán vị có dạng 1635__ khác hoán vị đã cho là 163524 và 163524 nhỏ hơn 163542 nên hoán vị sau 163542 không thể có dạng 1635__.

Tồn tại hoán vị tiếp theo hoán vị 163__? Ba chữ số cuối cùng phải là một hoán vị của $\{2, 4, 5\}$. Vì 542 là hoán vị lớn nhất của $\{2, 4, 5\}$ nên hoán vị bất kỳ với ba chữ số bắt đầu 163 nhỏ hơn hoán vị 63542. Vậy hoán vị sau hoán vị đã cho không thể có dạng 163__.

Hoán vị tiếp theo của 163542 không thể bắt đầu là 1635 hay 163 do hoặc các chữ số còn lại trong hoán vị đã cho (42 và 542, tương ứng) là *giảm*. Do đó, bắt đầu từ bên phải, chúng ta cần tìm chữ số đầu tiên d mà lân cận bên phải của nó là r thoả mãn $d < r$. Trong trường hợp trên, chữ số thứ ba: 3 có tính chất này. Vậy hoán vị tiếp theo hoán vị đã cho sẽ bắt đầu là 16. Chữ số tiếp theo không thể nhỏ hơn 3. Vì ta muốn hoán vị tiếp theo nhỏ nhất, nên chữ số kế tiếp là 4. Do đó hoán vị tiếp theo bắt đầu với 164. Các chữ số còn lại: 235 cần tăng với giá trị nhỏ nhất. Vậy hoán vị tiếp theo hoán vị đã cho là 164235.

Nhận xét rằng để tạo tất cả các hoán vị của tập $\{1, 2, \ldots, n\}$ chúng ta có thể bắt đầu với hoán vị $12 \ldots n$ và lặp lại phương pháp của Ví dụ 4.3.7 để tạo hoán vị kế tiếp. Thuật toán kết thúc khi tạo ra hoán vị $n(n-1) \ldots 21$.

Ví dụ 4.3.8. Áp dụng phương pháp của Ví dụ 4.3.7, ta có thể liệt kê tất cả các hoán vị của $\{1, 2, 3, 4\}$ theo thứ tự từ điển như sau:

1234,	1243,	1324,	1342,	1423,	1432,	2134,	2143,
2314,	2341,	2413,	2431,	3124,	3142,	3214,	3241,
3412,	3421,	4123,	4132,	4213,	4231,	4312,	4321.

Thuật toán sinh các hoán vị

Bước 1. [Khởi tạo chuỗi] Đặt $s_i = i, i = 1, 2 \ldots, n$.

Bước 2. [Xuất hoán vị đầu tiên] Xuất chuỗi $s = s_1 s_2 \ldots s_n$.

Bước 3. [Lặp] Với mỗi $i = 2, 3, \ldots, n!$ thực hiện các bước sau:

3.1. Tìm chỉ số lớn nhất m thoả mãn $s_m < s_{m+1}$.

3.2. Tìm chỉ số lớn nhất k thoả mãn $s_k > s_m$.

3.3. Hoán vị hai phần tử s_m và s_k.

3.4. Đảo ngược thứ tự của các phần tử $s_{m+1}, \ldots, s_n$.

3.5. Xuất s.

Ví dụ 4.3.9. Áp dụng thuật toán trên tìm hoán vị tiếp theo 163542: Giả sử

$$s_1 = 1, s_2 = 6, s_3 = 3, s_4 = 5, s_5 = 4, s_6 = 2.$$

Chỉ số m lớn nhất thoả $s_m < s_{m+1}$ là 3. Chỉ số k lớn nhất thoả $s_k > s_m$ là 5. Hoán vị s_m và s_k ta có $s_3 = 4, s_5 = 3$. Đảo ngược thứ tự các phần tử s_4, s_5, s_6 ta nhận được hoán vị tiếp theo là 164235.

Bài tập

1. Tìm r-tổ hợp sinh ra bởi thuật toán sinh tổ hợp với $n = 7$ sau khi r-tổ hợp được cho: 1356, 12367, 14567.

2. Tìm hoán vị sinh ra bởi thuật toán sinh hoán vị sau hoán vị được cho: 12354, 625431, 12876543.

3. Tìm tất cả r-tổ hợp từ tập n phần tử nếu

   (a) $n = 6, r = 3$.

   (b) $n = 6, r = 2$.

   (c) $n = 7, r = 5$.

4. Tìm các hoán vị của tập hai, ba phần tử.

5. Viết thuật toán đệ quy sinh ra tất cả các r-tổ hợp của tập $\{s_1, s_2, \ldots, s_n\}$. Chia bài toán thành hai bài toán con:

   + Liệt kê các r-tổ hợp chứa s_1.

   + Liệt kê các r-tổ hợp không chứa s_1.

6. Viết thuật toán đệ quy sinh ra tất cả các hoán vị của tập $\{s_1, s_2, \ldots, s_n\}$. Chia bài toán thành n bài toán con:

   + Liệt kê các hoán vị bắt đầu với s_1.

   + Liệt kê các hoán vị bắt đầu với s_2.

   $\vdots$

   + Liệt kê các hoán vị bắt đầu với s_n.

4.4 Hoán vị và tổ hợp suy rộng

Trong các mục trước, chúng ta đã nghiên cứu các hoán vị và tổ hợp không cho phép lặp lại các phần tử. Phần này tìm hiểu các hoán vị của các dãy chứa những phần tử lặp lại và các phép chọn không phân biệt thứ tự có lặp lại. Trước hết ta xét ví dụ sau.

Ví dụ 4.4.1. Trong nhiều vấn đề đếm, các phần tử có thể lặp lại; chẳng hạn có bao nhiêu xâu khác nhau có độ dài n từ bảng 26 chữ cái?

Hiển nhiên ở đây, có thể coi các chữ cái được rút ra có hoàn lại. Một xâu độ dài n gồm n chữ cái. Mỗi chữ cái có 26 cách chọn lựa. Theo nguyên lý tích, số xâu có thể là

$$\underbrace{26 \times 26 \times \cdots \times 26}_{n \text{ lần}} = 26^n.$$

Định lý 4.4.1. *Số các r-hoán vị có lặp lại của tập n phần tử bằng n^r.*

Chứng minh. Có n cách chọn cho mỗi vị trí trong r-hoán vị (vì có lặp lại). Áp dụng nguyên lý tích, số các r-hoán vị có lặp lại bằng n^r. □

Ví dụ 4.4.2. Xét chuỗi $SUCCESS$. Có bao nhiêu chuỗi khác nhau có thể có khi sắp xếp lại các ký tự của chuỗi này?

Trước hết chú ý rằng trong chuỗi $SUCCESS$ độ dài 7 có ba ký tự S, hai ký tự C, một ký tự U và một ký tự E. Ba ký tự S (tương ứng, hai ký tự C) là không phân biệt, nên hoán vị chúng không tạo ra chuỗi mới.

Có tất cả 7! chuỗi là hoán vị của chuỗi $SUCCESS$. Ba ký tự S hoán vị tạo ra 3! chuỗi; hai ký tự C hoán vị tạo ra 2! chuỗi; một ký tự U hoán vị tạo ra 1! chuỗi; và một ký tự E hoán vị tạo ra 1! chuỗi. Vậy số chuỗi thật sự khác nhau là

$$\frac{7!}{3!2!1!1!}.$$

Ví dụ 4.4.3. Xét chuỗi $MISSISSIPPI$. Có bao nhiêu chuỗi khác nhau có thể có khi sắp xếp lại các ký tự của chuỗi này?

Xét bài toán điền vào 11 chỗ trống

$$\_\ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \_,$$

với các ký tự đã cho. Có $C(11,2)$ cách chọn các vị trí đối với P. Khi đã chọn xong P, ta có $C(9,4)$ cách chọn các vị trí đối với S. Khi đã chọn S, có $C(5,4)$ cách chọn các vị trí đối với I. Cuối cùng chỉ còn một cách chọn M. Theo nguyên lý tích, số các cách để điền các ký tự là

$$\begin{aligned} C(11,2)C(9,4)C(5,4) &= \frac{11!}{2!9!}\frac{9!}{4!5!}\frac{5!}{4!1!} \\ &= \frac{11!}{2!4!4!1!} \\ &= 34.650. \end{aligned}$$

Tổng quát ta có

Định lý 4.4.2. *Giả sử dãy n phần tử S có n_1 đối tượng loại 1, n_2 đối tượng loại 2, ..., và n_t đối tượng loại t. Khi đó số các cách chọn dãy S là*

$$\frac{n!}{n_1!n_2!\ldots n_t!}.$$

Chứng minh. Ta gán các vị trí đối với mỗi dãy độ dài n các đối tượng để tạo ra một thứ tự trong S. Có $C(n,n_1)$ cách chọn các vị trí đối với các đối tượng loại 1. Khi đã chọn xong

các đối tượng này, ta có $C(n-n_1, n_2)$ cách chọn các vị trí đối với các đối tượng loại 2, và vân vân. Theo nguyên lý tích, số các cách để thực hiện là

$$C(n, n_1)C(n-n_1, n_2)\cdots C(n-n_1-n_2-\cdots-n_{t-1}, n_t)$$

và do đó có điều cần chứng minh. □

Kế tiếp chúng ta khảo sát bài toán đếm các phép chọn không phân biệt thứ tự có lặp lại.

Ví dụ 4.4.4. Xét ba loại sách: sách máy tính, sách vật lý và sách lịch sử. Giả sử thư viện có ít nhất sáu cuốn sách mỗi loại. Có bao nhiêu cách có thể chọn sáu cuốn sách?

Bài toán là lấy sáu phần tử không phân biệt thứ tự từ tập {máy tính, vật lý, lịch sử} cho phép lặp lại. Một phép chọn được xác định duy nhất bởi số mỗi kiểu sách được chọn. Ký hiệu

Máy tính	Vật lý	Lịch sử
× × × |	× × |	×

có nghĩa là phép chọn ba cuốn sách máy tính, hai sách vật lý và một sách lịch sử. Nhận xét rằng mỗi thứ tự của sáu ký hiệu × và hai ký hiệu | tương ứng một phép chọn. Do đó bài toán là đếm số các thứ tự. Vậy có thể thực hiện bằng $C(8, 2) = 28$ cách.

Định lý 4.4.3. *Nếu X là tập gồm t phần tử thì số phép chọn k phần tử không phân biệt thứ tự từ X cho phép lặp là*

$$C(k+t-1, t-1) = C(k+t-1, k).$$

Chứng minh. Đặt $X := \{a_1, a_2, \ldots, a_t\}$. Xét $k+t-1$ khoảng trắng

_ _ _ · · · _ _

gồm k ký hiệu × và $t-1$ ký hiệu |. Mỗi vị trí của ký hiệu này trên các khoảng trắng xác định một phép chọn. n_1 ký hiệu × đến ký hiệu | đầu tiên tương ứng phép chọn n_1 phần tử a_1; n_2 ký hiệu × đến ký hiệu | thứ hai tương ứng phép chọn n_2 phần tử a_2; và vân vân. Ta có $C(k+t-1, t-1)$ cách chọn các vị trí cho | nên có $C(k+t-1, t-1)$ cách chọn. Giá trị này bằng $C(k+t-1, k)$, số cách chọn các vị trí của ×; do đó có

$$C(k+t-1, t-1) = C(k+t-1, k)$$

cách chọn k phần tử không phân biệt thứ tự từ tập X cho phép lặp lại. □

Ví dụ 4.4.5. Có các hộp chứa các quả bóng màu đỏ, xanh và vàng. Mỗi hộp chứa ít nhất tám quả bóng. Có bao nhiêu cách chọn tám quả bóng? Có bao nhiêu cách chọn tám quả bóng, mỗi màu ít nhất một quả bóng?

(a) Theo Định lý 4.4.3, số cách chọn tám quả bóng là

$$C(8+3-1, 3-1) = C(10, 2) = 45.$$

(b) Đầu tiên chọn một quả bóng mỗi màu; sau đó chọn thêm năm quả bóng. Theo Định lý 4.4.3 ta có

$$C(5+3-1,3-1) = C(7,2) = 21$$

cách.

Ví dụ 4.4.6. (a) Có bao nhiêu nghiệm nguyên không âm của phương trình

$$x_1 + x_2 + x_3 + x_4 = 29? \tag{4.2}$$

Mỗi nghiệm của phương trình (4.2) tương đương với phép chọn 29 phần tử x_i có kiểu i với $i := 1, 2, 3, 4$. Theo Định lý 4.4.3, số phép chọn là

$$C(29+4-1,4-1) = C(32,3) = 4960.$$

(b) Có bao nhiêu nghiệm nguyên của phương trình (4.2) thoả mãn

$$x_1 > 0, \quad x_2 > 1, \quad x_3 > 2, \quad x_4 \geq 0?$$

Mỗi nghiệm của (4.2) thoả điều kiện đã cho tương đương với phép chọn 29 phần tử x_i có kiểu $i, i = 1, 2, 3, 4$, sao cho cần ít nhất một phần tử có kiểu 1, ít nhất hai phần tử có kiểu 2, ít nhất ba phần tử có kiểu 3. Đầu tiên chọn một phần tử có kiểu 1, hai phần tử có kiểu 2 và ba phần tử có kiểu 3. Sau đó chọn thêm 23 phần tử còn lại. Theo Định lý 4.4.3 số phép chọn là

$$C(23+4-1,4-1) = C(26,3) = 2600.$$

Chúng ta kết thúc phần này với việc mở rộng nguyên lý bao hàm-loại trừ.

Xét trường hợp có ba sự kiện A, B, C. Ta cần tính $\#(A \cup B \cup C)$. Nhận xét là

(a) Nếu lấy $\#A + \#B + \#C$: có phần được tính một lần, hai lần và ba lần (Hình 4.2(a));

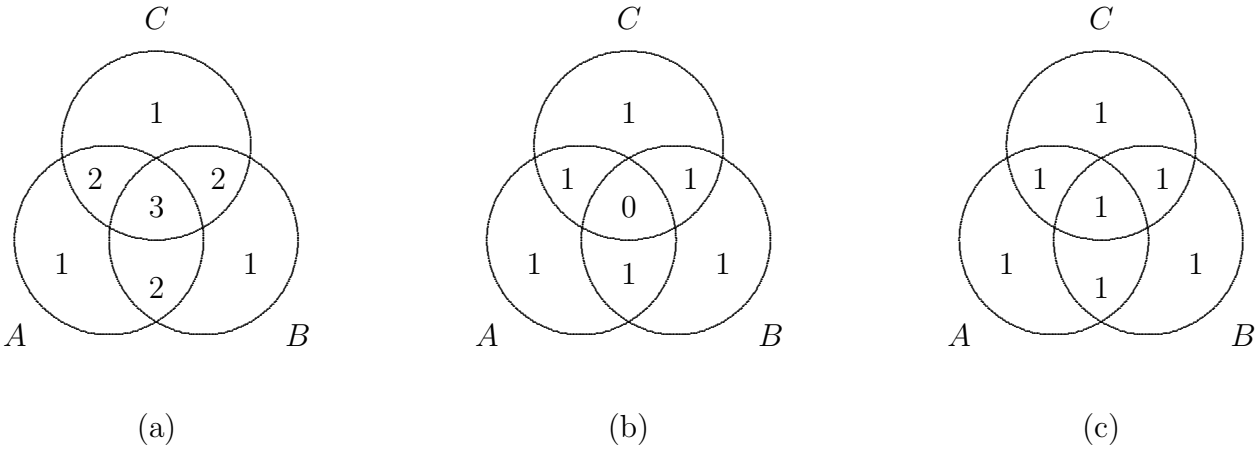
(b) Nếu lấy $\#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C)$: có phần không được tính lần nào (Hình 4.2(b));

(c) Nếu lấy $\#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C)$: mỗi phần được tính đúng một lần (Hình 4.2(c)).

Vậy

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

Tổng quát ta có



Hình 4.2:

Định lý 4.4.4. *Giả sử có m sự kiện $A_1, A_2, \dots A_m$. Khi đó*

$$\begin{aligned}\#(A_1 \cup A_2 \cup \cdots \cup A_m) &= \sum_{i=1}^{m} \#A_i - \sum_{1\le i<j\le m} \#(A_i \cap A_j) + \sum_{1\le i<j<k\le m} \#(A_i \cap A_j \cap A_k) \\ &\quad + \cdots + (-1)^{m+1} \#(A_1 \cap A_2 \cap \cdots \cap A_m).\end{aligned}$$

Chứng minh. Ta sẽ chứng minh rằng lấy một phần tử a bất kỳ thuộc tập $A_1 \cup A_2 \cup \cdots \cup A_m$ thì a cũng được kể đến đúng một lần ở vế phải.

Giả sử a thuộc đúng r tập, chẳng hạn trong $A_1 \cap A_2 \cap \cdots \cap A_r, r \le m$. Phần tử này đã được tính

+ $C(r,1)$ lần trong $\sum_{i=1}^{m} \#A_i$;

+ $C(r,2)$ lần trong $\sum_{i=1}^{m} \#(A_i \cap A_j)$;

...

+ $C(r,m)$ lần trong $\sum_{i=1}^{m} \#(A_{i_1} \cap A_{i_2} \cap \cdots A_{i_m})$.

Vậy nó đã được tính tổng cộng số lần là

$$C(r,1) - C(r,2) + C(r,3) - \cdots + (-1)^{m+1} C(r,r).$$

Nhưng

$$C(r,0) - C(r,1) + C(r,2) - \cdots + (-1)^{r} C(r,r) = 0$$

và $C(r,0) = 1$. Vậy phần tử a đã được tính

$$C(r,1) - C(r,2) + C(r,3) - \cdots + (-1)^{r+1} C(r,r) = 1$$

lần. □

Ví dụ 4.4.7. Có bao nhiêu nghiệm nguyên không âm của phương trình

$$x_1 + x_2 + x_3 = 11 \tag{4.3}$$

với điều kiện $x_1 \leq 3, x_2 \leq 4$ và $x_3 \leq 6$?

Tương tự như Ví dụ 4.4.6, ta có

+ Tổng số nghiệm nguyên không âm của phương trình (4.3) là

$$C(11 + 3 - 1, 11) = C(13, 11) = 78.$$

+ Số nghiệm với điều kiện $x_1 \geq 4$ là

$$C(7 + 3 - 1, 7) = C(9, 7) = 36.$$

+ Số nghiệm với điều kiện $x_2 \geq 5$ là

$$C(6 + 3 - 1, 6) = C(8, 6) = 28.$$

+ Số nghiệm với điều kiện $x_3 \geq 7$ là

$$C(4 + 3 - 1, 4) = C(6, 4) = 15.$$

+ Số nghiệm với điều kiện $x_1 \geq 4, x_2 \geq 5$ là

$$C(2 + 3 - 1, 2) = C(4, 2) = 6.$$

+ Số nghiệm với điều kiện $x_1 \geq 4, x_3 \geq 7$ là

$$C(0 + 3 - 1, 0) = C(2, 0) = 1.$$

+ Số nghiệm với điều kiện $x_2 \geq 5, x_3 \geq 7$ bằng 0.

+ Số nghiệm với điều kiện $x_1 \geq 4, x_2 \geq 4, x_3 \geq 7$ bằng 0.

Theo Định lý 4.4.4, số nghiệm đòi hỏi là

$$78 - 36 - 28 - 15 + 6 + 1 + 0 - 0 = 6.$$

Định lý 4.4.5. *Giả sử m, n là các số nguyên dương khác nhau, $m \leq n$. Khi đó có*

$$n^m - C(n, 1)(n - 1)^m + C(n, 2)(n - 2)^m - \cdots + (-1)^{n-1} C(n, n - 1)1^m$$

ánh xạ lên khác nhau từ tập m phần tử đến tập có n phần tử.

Chứng minh. Bài tập. □

Ví dụ 4.4.8. Giả sử có năm công việc và bốn người xin việc. Có bao nhiêu cách phân công việc khác nhau nếu mỗi người phải được phân công ít nhất một công việc?

Mỗi phương pháp phân công tương ứng một ánh xạ lên từ tập các công việc đến tập người. Theo giả thiết, mỗi người đều được phân công ít nhất một công việc, các ánh xạ là lên. Áp dụng Định lý 4.4.5 với $m = 5, n = 4$ ta có số cách phân công công việc bằng số các ánh xạ lên khác nhau và bằng

$$4^5 - C(4, 1)3^5 + C(4, 2)2^5 - C(4, 3)1^5 = 1024 - 972 + 192 - 4 = 240.$$

Bài tập

1. Có bao nhiêu chuỗi khác nhau có thể có khi sắp xếp lại các ký tự của các chuỗi sau:
   (a) $GUIDE$.
   (b) $SCHOOL$.
   (c) $SALEPERSONS$.

2. Có bao nhiêu cách chia 10 cuốn sách cho ba sinh viên sao cho sinh viên thứ nhất có năm cuốn, sinh viên thứ hai có ba cuốn và sinh viên thứ ba có hai cuốn?

3. Giả sử có các hộp chứa các quả bóng màu xanh, đỏ và vàng. Mỗi hộp chứa ít nhất 10 quả.
   (a) Có bao nhiêu cách chọn 10 quả bóng?
   (b) Có bao nhiêu cách chọn 10 quả bóng với ít nhất một quả màu đỏ?
   (c) Có bao nhiêu cách chọn 10 quả bóng với ít nhất một quả màu đỏ, ít nhất hai quả màu xanh và ít nhất ba quả màu vàng?
   (d) Có bao nhiêu cách chọn 10 quả bóng với đúng một quả màu đỏ?
   (e) Có bao nhiêu cách chọn 10 quả bóng với đúng một quả màu đỏ và ít nhất một quả màu xanh?

4. Tìm số nghiệm nguyên của phương trình
   $$x_1 + x_2 + x_3 = 15$$
   nếu
   (a) $x_1 \geq 0, x_2 \geq 0, x_3 \geq 0$.
   (b) $x_1 = 1, x_2 \geq 0, x_3 \geq 0$.
   (c) $6 \geq x_1 \geq 0, x_2 \geq 0, x_3 \geq 0$.
   (d) $x_1 \geq 1, x_2 \geq 1, x_3 \geq 1$.
   (e) $x_1 \geq 0, x_2 > 0, x_3 = 1$.
   (f) $6 > x_1 \geq 0, 9 > x_2 \geq 1, x_3 \geq 0$.

5. Tìm số nghiệm nguyên của phương trình
   $$x_1 + x_2 + x_3 + x_4 = 15$$
   nếu $0 \leq x_1 \leq 4, 0 \leq x_2 \leq 5, 0 \leq x_3 \leq 9$.

6. Có bao nhiêu số nguyên trong tập $\{1, 2, \ldots, 1000000\}$ có tổng các chữ số bằng 15?

7. Có bao nhiêu số nguyên trong tập $\{1, 2, \ldots, 1000000\}$ có tổng các chữ số bằng 20?

8. Có bao nhiêu cách chọn ba đội: một đội bốn người, hai đội hai người từ một nhóm tám người?

9. Một túi sách chứa 20 quả bóng: sáu đỏ, sáu xanh và tám tím.

   (a) Có bao nhiêu cách chọn năm quả bóng nếu các quả bóng được xem là phân biệt?

   (b) Có bao nhiêu cách chọn năm quả bóng nếu các quả bóng cùng màu được xem là đồng nhất?

10. Chứng minh rằng $(n!)^k$ chia hết $(kn)!$.

11. Chứng minh rằng
$$\sum_{i=k-1}^{n+k-2} C(i, k-1) = C(n+k-1, k-1).$$

12. Viết thuật toán tìm tất cả các nghiệm nguyên không âm của phương trình
$$x_1 + x_2 + x_3 = n \qquad (n \in \mathbb{N}).$$

4.5 Hệ số của nhị thức và các đồng nhất thức

Định lý 4.5.1. (Định lý nhị thức) *Nếu a và b là các số thực và n là số tự nhiên thì*
$$(a+b)^n = \sum_{k=0}^{n} C(n,k) a^{n-k} b^k.$$

Chứng minh. Khi khai triển $(a+b)^n$ các từ có dạng $a^{n-k}b^k, k = 0, 1, \ldots, n$. Để có một thành phần $a^{n-k}b^k$ cần có đúng $n-k$ chữ a trong tổng số n vị trí (và kéo theo có đúng k chữ b). Điều này có thể thực hiện bằng $C(n,k)$ cách. Do đó $a^{n-k}b^k$ xuất hiện $C(n,k)$ lần. Suy ra
$$(a+b)^n = C(n,0)a^n b^0 + C(n,1)a^{n-1}b^1 + \cdots + C(n,n)a^0 b^n.$$
□

Chính vì lý do trên mà $C(n,r)$ được gọi là *hệ số nhị thức*.

Ví dụ 4.5.1. Tìm hệ số của a^5b^4 trong khai triển của $(a+b)^9$.

Theo Định lý nhị thức, hệ số của a^5b^4 trong khai triển $(a+b)^9$ là
$$C(9,4) = \frac{9!}{4!5!} = 126.$$

Ví dụ 4.5.2. Chứng minh rằng

$$\sum_{k=0}^{n}(-1)^k C(n,k) = 0.$$

Ta có

$$0 = [1+(-1)]^n = \sum_{k=0}^{n} C(n,k)1^{n-k}(-1)^k = \sum_{k=0}^{n}(-1)^k C(n,k).$$

Ví dụ 4.5.3. Sử dụng Định lý nhị thức ta có

$$2^n = (1+1)^n = \sum_{k=0}^{n} C(n,k).$$

Định lý 4.5.2. (Đẳng thức Pascal)

$$C(n+1,k) = C(n,k-1) + C(n,k)$$

với $1 \le k \le n$.

Chứng minh. Giả sử X là tập gồm n phần tử. Chọn $a \notin X$. Ta có $C(n+1,k)$ là số các tập con k phần tử của tập $Y := X \cup \{a\}$. Mỗi tập con k phần tử của Y có thể chia thành hai lớp:

+ Các tập con của Y không chứa a.

+ Các tập con của Y chứa a.

Các tập con thuộc nhóm thứ nhất là các tập con của X gồm k phần tử và do đó có $C(n,k)$ tập con như vậy.

Các tập con thuộc nhóm thứ hai là các tập là hợp của tập con $(k-1)$ phần tử của X với tập gồm một phần tử a và do đó có $C(n,k-1)$ tập con như vậy. Suy ra

$$C(n+1,k) = C(n,k-1) + C(n,k).$$

□

Ví dụ 4.5.4. Chứng minh đẳng thức

$$\sum_{i=k}^{n} C(i,k) = C(n+1,k+1).$$

Theo Định lý 4.5.2

$$C(i,k) = C(i+1,k+1) - C(i,k+1), \quad i \ge k.$$

Vậy

$$\begin{aligned}\sum_{i=k}^{n} C(i,k) &= \sum_{i=k}^{n} C(i+1,k+1) - \sum_{i=k}^{n} C(i,k+1) \\ &= C(n+1,k+1).\end{aligned}$$

Ví dụ 4.5.5. Từ đẳng thức (4.5.4) ta có

$$\begin{aligned}1+2+\cdots+n &= C(1,1)+C(2,1)+\cdots+C(n,1) \\ &= C(n+1,2) \\ &= \frac{(n+1)n}{2}.\end{aligned}$$

Định lý 4.5.3. (Đẳng thức Vandermonde)

$$C(m+n,r) = \sum_{k=0}^{r} C(m,k)C(n,r-k)$$

với $r \leq \min(m,n)$.

Chứng minh. Giả sử các tập T_1, T_2 tương ứng gồm m, n phần tử phân biệt. Lấy tập S gồm r phần tử từ hai tập này. Số các tập S như vậy bằng $C(m+n,r)$.

Mặt khác, tập S có thể gồm

$+$ k phần tử thuộc tập T_1. Số các tập con như vậy bằng $C(m,k)$;

$+$ $(r-k)$ phần tử thuộc tập T_2. Số các tập con như vậy bằng $C(n,r-k)$;

với $0 \leq k \leq r$.

Theo nguyên lý tích, sau đó nguyên lý tổng ta có điều cần chứng minh. □

Bài tập

1. Sử dụng Định lý nhị thức khai triển các biểu thức
   (a) $(x+y)^4$.
   (b) $(2c-3d)^5$.
2. Tìm hệ số của số hạng khi biểu thức được khai triển:
   (a) $x^4y^7; (x+y)^{11}$.
   (b) $x^2y^3z^5; (x+y+z)^{10}$.
   (c) $a^2x^3; (a+x+c)^2(a+x+d)^3$.

(d) $a^3x^4; (a + \sqrt{ax} + x)^2(a + x)^5$.

(e) $a^2x^3; (a + ax + x)(a + x)^4$.

3. Tìm số các số hạng khi khai triển biểu thức

   (a) $(x + y + z)^{10}$.

   (b) $(w + x + y + z)^{12}$.

   (c) $(x + y + z)^{10}(w + x + y + z)^2$.

4. (a) Chứng minh rằng $C(n, k) < C(n, k + 1)$ nếu và chỉ nếu $k < (n - 1)/2$.

   (b) Suy ra $\max\{C(n, k) \mid k = 0, 1, \ldots, n\} = C(n, [n/2])$.

5. Chứng minh Định lý nhị thức bằng quy nạp toán học.

6. Sử dụng lý luận tổ hợp chứng minh rằng

$$C(n, k) = C(n, n - k).$$

7. Tính tổng

$$\sum_{k=1}^{n-1} k(k + 1).$$

8. Tính tổng

$$\sum_{k=1}^{n} k^2.$$

9. Dùng Định lý nhị thức chứng minh

$$\sum_{k=0}^{n} 2^k C(n, k) = 3^n.$$

10. Giả sử n chẵn. Chứng minh rằng

$$\sum_{k=0}^{n/2} C(n, 2k) = 2^{n-1} = \sum_{k=1}^{n/2} C(n, 2k - 1).$$

11. Chứng minh rằng

$$(a + b + c)^n = \sum_{0 \le i+j \le n} \frac{n!}{i!j!(n - i - j)!} a^i b^j c^{n-i-j}.$$

12. Chứng minh rằng

$$3^n = \sum_{0 \le i+j \le n} \frac{n!}{i!j!(n - i - j)!}.$$

13. Dùng lý luận tổ hợp chứng minh rằng

$$\sum_{k=0}^{n} C(n,k)^2 = C(2n,n).$$

14. (a) Chứng minh rằng

$$n(1+x)^{n-1} = \sum_{k=1}^{n} C(n,k)kx^{k-1}.$$

(b) Từ đó suy ra

$$n2^{n-1} = \sum_{k=1}^{n} kC(n,k).$$

4.6 Nguyên lý chuồng chim bồ câu

Nguyên lý chuồng chim bồ câu (còn gọi là *nguyên lý Dirichlet*) thường dùng nhằm trả lời câu hỏi: Có tồn tại một phần tử thoả tính chất cho trước? Khi áp dụng thành công, nguyên lý này chỉ ra rằng đối tượng tồn tại; tuy nhiên không chỉ ra cách tìm nó như thế nào và có bao nhiêu phần tử tồn tại.

Dạng đầu tiên của nguyên lý chuồng chim bồ câu khẳng định rằng nếu có n vật cần xếp vào k hộp và $n > k$ thì có ít nhất có một hộp chứa hai hoặc nhiều hơn hai vật. Lý do khẳng định này đúng có thể chứng minh bằng phản chứng: Nếu kết luận là sai, mỗi hộp chứa nhiều nhất một vật và do đó trong trường hợp này có nhiều nhất k vật. Nhưng có n vật nên $n \leq k$ vô lý.

4.6.1 Nguyên lý chuồng chim bồ câu (dạng thứ nhất)

Nếu có n vật cần xếp vào k hộp và $n > k$ thì tồn tại ít nhất một hộp có chứa hai hoặc nhiều hơn hai vật.

Chú ý rằng, nguyên lý chuồng chim bồ câu không chỉ ra hộp nào chứa hơn hai vật. Nó chỉ khẳng định sự *tồn tại* của một hộp với ít nhất hai vật trong đó.

Ví dụ 4.6.1. Số các học viên của một lớp học ít nhất là bao nhiêu để có ít nhất hai học viên có số điểm như nhau trong kỳ thi môn Toán học rời rạc, nếu dự định thang điểm là 0-10?

Có 11 thang điểm. Theo nguyên lý chuồng chim bồ câu, cần có ít nhất $11 + 1 = 12$ học viên.

Ví dụ 4.6.2. Chứng minh rằng với $n+1$ số nguyên dương khác nhau không vượt quá $2n$ thì phải có hai số chia hết cho nhau.

Giả sử $n+1$ số nguyên dương là $a_1, a_2, \ldots, a_{n+1}$, với $0 < a_i \leq 2n$. Ta có thể viết

$$a_i = 2^{k_i} q_i, \qquad i = 1, 2, \ldots, n+1,$$

trong đó k_i là số nguyên không âm và q_i là số nguyên lẻ không âm và không vượt quá $2n$. Ví dụ $1 = 2^0, 14 = 2^1 \times 7, 40 = 2^3 \times 5, \ldots$.

Vì chỉ có n số lẻ không vượt quá $2n$ nên trong $n+1$ số lẻ $q_1, q_2, \ldots, q_{n+1}$ phải có ít nhất hai số bằng nhau, chẳng hạn $q_i = q_j = q$ với $i \neq j$.

Khi đó

$$a_i = 2^{k_i} q_i = 2^{k_i} q, \qquad a_j = 2^{k_j} q_j = 2^{k_j} q,$$

với $k_i \neq k_j$. Suy ra $a_i \mid a_j$ nếu $k_i > k_j$ và $a_j \mid a_i$ nếu $k_j > k_i$.

Kết quả trên là tốt nhất theo nghĩa nếu ta giảm nhẹ giả thiết đi bằng cách thay n cho $n+1$ thì kết quả không còn đúng nữa. Thật vậy chỉ cần lấy tập các số

$$\{n+1, n+2, \ldots, 2n\}.$$

Ví dụ 4.6.3. Chứng minh rằng trong mọi dãy gồm n^2+1 số thực phân biệt đều chứa một dãy con độ dài $n+1$ hoặc tăng thực sự, hoặc giảm thực sự.

Giả sử n^2+1 số thực phân biệt là $a_1, a_2, \ldots, a_{n^2+1}$. Với mỗi số a_i ta gán cho nó cặp số (k_i, d_i) như sau:

+ k_i là độ dài của dãy con tăng dài nhất xuất phát từ a_i.

+ d_i là độ dài của dãy con giảm dài nhất xuất phát từ a_i.

Bằng phản chứng giả sử không có dãy con nào có độ dài $n+1$ lại tăng thực sự hoặc giảm thực sự. Khi đó $k_i, d_i \leq n, i = 1, 2, \ldots, n^2+1$.

Nhận xét rằng có n^2 cặp (k_i, d_i) khác nhau với $k_i, d_i \leq n$. Nên tồn tại các chỉ số s, t sao cho $(k_s, d_s) = (k_t, d_t)$.

Nhưng các số lấy là phân biệt, nên $a_s \neq a_t$. Không mất tính tổng quát giả sử $a_s < a_t$. Bây giờ thêm a_s vào dãy con xuất phát từ a_t để được một dãy con mới tăng có độ dài $1 + k_t = 1 + k_s$ trái với giả thiết k_s là độ dài của dãy con tăng dài nhất.

4.6.2 Nguyên lý chuồng chim bồ câu (dạng thứ hai)

Nếu f là ánh xạ từ tập hữu hạn X đến tập hữu hạn Y và $\#X > \#Y$ thì tồn tại $x_1, x_2 \in X, x_1 \neq x_2$, sao cho $f(x_1) = f(x_2)$.

Thật vậy, đặt X là tập các vật và Y là tập các hộp. Gán mỗi vật x với một hộp $f(x)$. Theo nguyên lý chuồng chim bồ câu dạng thứ nhất, có ít nhất hai vật khác nhau $x_1, x_2 \in X$ được gán cùng một hộp; tức là $f(x_1) = f(x_2)$.

Ví dụ 4.6.4. Nếu 20 bộ vi xử lý được nối với nhau thì có ít nhất hai bộ vi xử lý được nối trực tiếp tới cùng số các bộ vi xử lý.

Ký hiệu các bộ vi xử lý là $1, 2, \ldots, 20$. Đặt a_i là số các bộ vi xử lý được nối trực tiếp với bộ vi xử lý i. Chúng ta cần chứng minh rằng $a_i = a_j$ với $i \neq j$ nào đó. Miền xác định và miền giá trị của bài toán tương ứng là $X := \{1, 2, \ldots, 20\}$ và $\{0, 1, \ldots, 19\}$. Tuy nhiên số phần tử của hai tập hợp này bằng nhau, nên không thể áp dụng trực tiếp nguyên lý chuồng chim bồ câu dạng hai.

Chú ý rằng ta không thể có $a_i = 0$ và $a_j = 19$ với i, j nào đó, vì nếu ngược lại ta có một bộ vi xử lý (thứ i) không được nối với bất cứ bộ vi xử lý nào trong khi lại có một bộ vi xử lý (thứ j) được nối với tất cả các bộ vi xử lý khác (kể các bộ vi xử lý thứ i). Do đó Y là tập con của tập $\{0, 1, \ldots, 18\}$ hoặc $\{1, 2, \ldots, 19\}$. Vậy $\#Y < 20 = \#X$. Theo nguyên lý chuồng chim bồ câu dạng hai ta có $a_i = a_j$ với $i \neq j$ nào đó.

Ví dụ 4.6.5. Chứng minh rằng nếu chọn 151 giáo trình máy tính phân biệt được đánh số thứ tự từ 1 đến 300 thì có ít nhất hai giáo trình có số thứ tự liên tiếp.

Giả sử các giáo trình được đánh số là

$$c_1, c_2, \ldots, c_{151}. \tag{4.4}$$

Các số này cùng với

$$c_1 + 1, c_2 + 1, \ldots, c_{151} + 1 \tag{4.5}$$

tạo thành 302 số thay đổi từ 1 đến 301. Theo nguyên lý chuồng chim bồ câu dạng thứ hai có ít nhất hai giá trị bằng nhau. Các số trong (4.4) là phân biệt và do đó các số trong (4.5) cũng khác nhau. Vì vậy phải có một số trong dãy (4.4) bằng một số trong dãy (4.5). Do đó

$$c_i = c_j + 1$$

(hiển nhiên $i \neq j$) và ta có hai giáo trình c_i và c_j được đánh số liên tiếp.

Ví dụ 4.6.6. Bản kê tài khoản gồm 80 khoản mục, mỗi khoản mục được đánh dấu "hợp lệ" hoặc "không hợp lệ". Có 45 khoản mục hợp lệ. Chứng minh rằng có ít nhất hai khoản mục hợp lệ trong danh sách cách nhau chính xác chín khoản mục. (Chẳng hạn các khoản mục tại các vị trí 13 và 22 hoặc tại vị trí 69 và 78 cách nhau đúng 9 khoản mục).

Ký hiệu a_i là vị trí của khoản mục hợp lệ thứ i. Ta cần chỉ ra $a_i - a_j = 9$ với i, j nào đó. Xét các số

$$a_1, a_2, \ldots, a_{45} \tag{4.6}$$

và

$$a_1 + 9, a_2 + 9, \ldots, a_{45} + 9. \tag{4.7}$$

90 số trong (4.6) và (4.7) lấy các giá trị từ 1 đến 89. Do đó theo nguyên lý chuồng chim bồ câu dạng thứ hai, có ít nhất hai số trùng nhau. Hiển nhiên không thể có hai số trong dãy (4.6) hoặc (4.7) bằng nhau; nên tồn tại một số trong dãy (4.6) bằng một số trong dãy (4.7). Vậy $a_i - a_j = 9$ với i, j nào đó.

4.6.3 Nguyên lý chuồng chim bồ câu (dạng thứ ba)

Cho f là ánh xạ từ tập hữu hạn X đến tập hữu hạn Y. Giả sử $n := \#X, m := \#Y, k := \lceil n/m \rceil$. Khi đó tồn tại ít nhất k giá trị $a_1, a_2, \ldots, a_k$ sao cho

$$f(a_1) = f(a_2) = \cdots = f(a_k).$$

Chứng minh. Đặt $Y := \{y_1, y_2, \ldots, y_m\}$. Giả sử khẳng định là sai. Khi đó tồn tại nhiều nhất $k-1$ giá trị $x \in X$ với $f(x) = y_1$; tồn tại nhiều nhất $k-1$ giá trị $x \in X$ với $f(x) = y_2; \ldots;$ tồn tại nhiều nhất $k-1$ giá trị $x \in X$ với $f(x) = y_m$. Do đó tồn tại nhiều nhất $m(k-1)$ phần tử trong miền xác định của f. Nhưng

$$m(k-1) < m\frac{n}{m} = n,$$

vô lý. Do đó tồn tại ít nhất k giá trị $a_1, a_2, \ldots, a_k \in X$ sao cho

$$f(a_1) = f(a_2) = \cdots = f(a_k).$$

□

Ví dụ 4.6.7. Một đặc trưng hữu ích của các ảnh đen trắng là độ sáng trung bình của ảnh. Ta nói rằng hai ảnh là *tương tự* nếu độ sáng trung bình của chúng khác nhau không vượt quá một ngưỡng nào đó. Chứng minh rằng trong số sáu ảnh, hoặc có ba ảnh đồng thời tương tự, hoặc có ba ảnh đồng thời không tương tự.

Ký hiệu các ảnh là $P_1, P_2, \ldots, P_6$. Mỗi cặp $(P_1, P_i), i = 2, 3, \ldots, 6$, có giá trị "tương tự" hoặc "không tương tự". Theo nguyên lý chuồng chim bồ câu dạng thứ ba, tồn tại ít nhất $\lceil 5/2 \rceil = 3$ cặp với cùng giá trị; tức là tồn tại các cặp

$$(P_1, P_i), (P_1, P_j), (P_1, P_k)$$

hoặc tương tự, hoặc không tương tự. Giả sử mỗi cặp là tương tự (trong trường hợp ngược lại, xem Bài tập 5). Nếu một trong các cặp

$$(P_i, P_j), (P_i, P_k), (P_j, P_k) \tag{4.8}$$

là tương tự, thì hai hình ảnh này cùng với P_1 đôi một tương tự và do đó ta có ba hình tương tự. Ngược lại, nếu các cặp trong (4.8) không tương tự thì ta có ba ảnh tương ứng không tương tự.

Ví dụ 4.6.8. Số học viên tối thiểu là bao nhiêu để đảm bảo ít nhất có 6 người cùng thang điểm, nếu giáo viên cho điểm theo thang điểm A, B, C, D, F?

Ta có N là số nhỏ nhất thoả $\lceil N/5 \rceil = 6$. Suy ra $N = 5 \times 5 + 1 = 26$ học viên.

Ví dụ 4.6.9. Giả sử nhóm có sáu người; cứ lấy một cặp bất kỳ, thì hai người này hoặc là bạn, hoặc là thù. Chứng minh rằng sẽ có các bộ ba hoặc đều là bạn của nhau, hoặc đều là thù của nhau.

Lấy x là người bất kỳ trong nhóm; năm người còn lại lập thành nhóm riêng. Ta tạo hai hộp B và T. Năm người này sẽ được phân loại (theo quan hệ với x) :

(a) hoặc là bạn của x : tương ứng người trong hộp B;

(b) hoặc là thù của x : tương ứng người trong hộp T.

Theo nguyên lý chuồng chim bồ câu dạng thứ ba, sẽ có một hộp có ít nhất $\lceil 5/2 \rceil = 3$ người. Giả sử đó là hộp B với ba người y, z, u.

Nếu tồn tại cặp trong nhóm ba người này là bạn của nhau, chẳng hạn y và z, khi đó $\{x, y, z\}$ là bộ ba cần tìm. Ngược lại, tức là y, z, u mỗi cặp đôi một là thù của nhau, khi đó $\{y, z, u\}$ là bộ ba cần tìm.

Các trường hợp còn lại chứng minh tương tự.

Bài tập

1. Có thể nối năm máy tính với nhau sao cho có chính xác hai máy tính được nối trực tiếp đến cùng một số máy? Giải thích.

2. Bản kê tài khoản gồm 115 khoản mục, mỗi khoản mục được đánh dấu "hợp lệ" hoặc "không hợp lệ". Có 60 khoản mục hợp lệ. Chứng minh rằng có ít nhất hai khoản mục hợp lệ trong danh sách cách nhau chính xác bốn khoản mục.

3. Bản kê tài khoản gồm 100 khoản mục, mỗi khoản mục được đánh dấu "hợp lệ" hoặc "không hợp lệ". Có 55 khoản mục hợp lệ. Chứng minh rằng có ít nhất hai khoản mục hợp lệ trong danh sách cách nhau chính xác chín khoản mục.

4. Bản kê tài khoản gồm 80 khoản mục, mỗi khoản mục được đánh dấu "hợp lệ" hoặc "không hợp lệ". Có 50 khoản mục hợp lệ. Chứng minh rằng có ít nhất hai khoản mục trong danh sách cách nhau chính xác hoặc ba hoặc sáu khoản mục.

5. Hoàn chỉnh Ví dụ 4.6.7 bằng cách chỉ ra rằng nếu các cặp $(P_1, P_i), (P_1, P_j), (P_1, P_k)$ là không tương tự thì tồn tại ba ảnh đôi một tương tự hoặc đôi một không tương tự.

6. Kết luận của Ví dụ 4.6.7 như thế nào nếu:

(a) Có ít hơn sáu ảnh?

(b) Có hơn sáu ảnh?

7. Giả sử X gồm $(n+2)$ phần tử là tập con của $\{1, 2, \ldots, 2n+1\}$ và $m := \max X$. Với mỗi $k \in X \setminus \{m\}$ đặt

$$a_k := \begin{cases} k & \text{nếu } k \le \frac{m}{2}, \\ m-k & \text{nếu } k > \frac{m}{2}. \end{cases}$$

(a) Chứng minh miền giá trị của a chứa trong $\{1, 2, \ldots, n\}$.

(b) Suy ra tồn tại $i \neq j$ sao cho $a_i = a_j$.

(c) Chứng minh tồn tại hai phần tử phân biệt $i, j \in X$ sao cho $m = i + j$.

(d) Cho ví dụ tập X gồm $(n+1)$ phần tử là tập con của $\{1, 2, \ldots, 2n+1\}$ có tính chất: Không tồn tại $i, j \in X$ sao cho $i + j \in X$.

8. Xét một nhóm 10 người với các tuổi (được tính là số nguyên) là $a_1, a_2, \ldots, a_{10}$. Đặt $r_i := a_i \bmod 16$ và

$$s_i := \begin{cases} r_i & \text{nếu } r_i \le 8, \\ 16 - r_i & \text{nếu } r_i > 8. \end{cases}$$

(a) Chứng minh rằng $0 \le s_i \le 8$ với mọi $i := 1, 2, \ldots, 10$.

(b) Chứng minh tồn tại $j \neq k$ sao cho $s_j \neq s_k$.

(c) Chứng minh rằng nếu ($s_j = r_j$ và $s_k = r_k$) hoặc ($s_j = 16 - r_j$ và $s_k = 16 - r_k$) thì 16 chia hết $a_j - a_k$.

(d) Chứng minh nếu các điều kiện trong (c) sai thì 16 chia hết $a_j + a_k$.

9. Chứng minh rằng trong khai triển thập phân của thương của hai số nguyên, khối các chữ số cuối cùng là lặp lại. Ví dụ

$$1/6 = 0.1\underline{6}66\ldots, \qquad 217/660 = 0.32\underline{87}8787\ldots.$$

10. Mười sáu cầu thủ bóng rổ mặc áo mang các số từ 1 đến 12 đứng thành vòng tròn trên sàn đấu theo thứ tự tuỳ ý. Chứng minh rằng tồn tại ba cầu thủ liên tiếp có tổng các số ít nhất 26.

11. Giả sử f là ánh xạ một-một lên từ $X := \{1, 2, \ldots, n\}$ lên X. Ký hiệu f^k là ánh xạ hợp k lần của f :

$$f^k := \underbrace{f \circ f \circ \cdots \circ f}_{k \text{ lần}}.$$

Chứng minh rằng tồn tại các số nguyên phân biệt $i \neq j$ sao cho $f^i(x) \neq f^j(x)$ với mọi $x \in X$. Chứng minh rằng tồn tại số nguyên k sao cho $f^k(x) = x$ với mọi $x \in X$.

12. Một hình chữ nhật kích thước 3×7 được chia thành 21 hình vuông; mỗi hình vuông được tô màu đen hoặc trắng. Chứng minh rằng bàn cờ chứa một hình chữ nhật không tầm thường (không có kích thước $1 \times k$ hoặc $k \times 1$) sao cho bốn hình vuông ở mỗi góc hoặc tất cả tô màu đen hoặc tất cả tô màu trắng.

13. Chứng minh rằng nếu p bit 1 và q bit 0 được đặt xung quanh một vòng tròn theo thứ tự tuỳ ý, trong đó p, q, k là các số nguyên thoả $p \geq kq$ thì tồn tại k bit 1 đứng liên tiếp.

14. Viết thuật toán tìm độ dài của dãy con đơn điệu tăng dài nhất của một dãy số cho trước.

Chương 5

QUAN HỆ

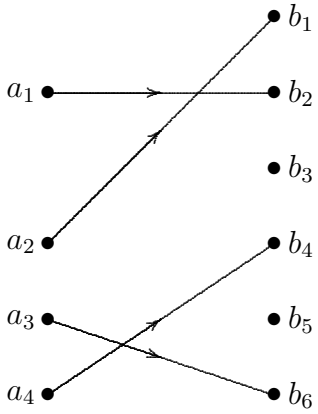
Như đã biết, tất cả các đối tượng trong thế giới xung quanh ta đều có những mối quan hệ nhất định với nhau. Rõ ràng không có một đối tượng nào có thể tồn tại tách rời (không liên quan) với thế giới bên ngoài. Mặt khác, mỗi đối tượng lại chứa đựng rất nhiều mối quan hệ nội tại của bản thân nó. Xét một nhóm sinh viên trong cùng một lớp, ta có thể nói rằng hai sinh viên có quan hệ với nhau nếu họ có cùng quê. Xét một tập hợp các số nguyên $\{1, 2, \ldots, 15\}$, ta có thể nói rằng ba phần tử nào đó của tập hợp này có quan hệ với nhau nếu tổng của chúng chia hết cho 4. Nói một cách khác, các phần tử hay các đối tượng có quan hệ chặt chẽ với nhau, nhưng mối quan hệ được hiểu như thế nào là phụ thuộc vào định nghĩa của chúng ta. *Mô hình cơ sở dữ liệu quan hệ*, được đưa ra bởi E. F. Codd vào năm 1970, dựa trên khái niệm của quan hệ n ngôi là một trong những ứng dụng của quan hệ trong Tin học.

Trong chương này, chúng ta sẽ nghiên cứu các mối quan hệ trên cơ sở lý thuyết tập hợp. Trước hết ta nghiên cứu các quan hệ hai ngôi trên hai tập hợp và trên cùng một tập hợp, cùng với các tính chất của các quan hệ đó. Tiếp theo, chúng ta sẽ xét đến quan hệ thứ tự, quan hệ tương đương và các mối liên quan.

5.1 Quan hệ hai ngôi

Định nghĩa 5.1.1. *Quan hệ hai ngôi* R từ tập S lên tập T là một tập hợp con của $S \times T$. Tập S được gọi là *miền xác định* còn T là *đối miền xác định*. Nếu $S \equiv T$ ta nói R là quan hệ hai ngôi trên S.

Ví dụ 5.1.1. Giả sử S là danh sách các sinh viên của trường đại học. T là danh sách các chứng chỉ học. Tập $R \subset S \times T$ gồm các cặp (a, b), trong đó a là sinh viên còn b là chứng chỉ mà sinh viên ghi danh học. Với mỗi $a \in S$, tập $\{b \in T \mid (a, b) \in R\}$ là danh sách các chứng chỉ mà sinh viên a theo học. Tập $\{a \mid (a, b) \in R\}$ là danh sách các sinh viên theo học



Hình 5.1:

chứng chỉ b.

Ví dụ 5.1.2. Giả sử P là tập các chương trình được thực hiện trên máy tính và một đơn vị C các chương trình có sẵn cho phép để sử dụng. Ta đặt một quan hệ R từ C lên P như sau: $(c, p) \in R$ nếu chương trình p sử dụng thủ tục c.

Ví dụ 5.1.3. Cho

$$S := \{a_1, a_2, a_3, a_4\}$$

là tập các sinh viên tốt nghiệp còn

$$T := \{b_1, b_2, b_3, b_4, b_5, b_6\}$$

là tập các cơ quan cần nhận sinh viên tốt nghiệp. Quan hệ

$$R := \{(a_1, b_2), (a_2, b_1), (a_3, b_6), (a_4, b_4)\}$$

từ S lên T mô tả các cặp sắp xếp nơi công tác cho mỗi sinh viên.

Trong chương này, ngoại trừ những trường hợp ngoại lệ mà sẽ nói rõ, ta sẽ luôn luôn giả thiết rằng các quan hệ được xét trên các *tập hữu hạn*. Khi đó có thể mô tả quan hệ R từ S lên T bằng phương pháp *đồ thị* như sau: các đỉnh của đồ thị biểu thị các phần tử của S và T, còn các cung là các đường có hướng nối các cặp $(a, b) \in R$ (có khi người ta viết tắt dưới dạng aRb); chẳng hạn quan hệ trong Ví dụ 5.1.3 có đồ thị trong Hình 5.1.

Ngoài ra, người ta cũng thường dùng ma trận cấp $m \times n$ để biểu thị mối quan hệ R từ $S = \{a_1, a_2, \ldots, a_m\}$ lên $T = \{b_1, b_2, \ldots, b_n\}$, trong đó $m := \#S, n := \#T$. Phần tử m_{ij} của ma trận được xác định như sau

$$m_{ij} := \begin{cases} 1 & \text{nếu } (a_i, b_j) \in R, \\ 0 & \text{nếu ngược lại.} \end{cases}$$

Ví dụ 5.1.4. Ma trận biểu diễn quan hệ R trong Ví dụ 5.1.3 là

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{array} \begin{array}{c} \begin{array}{cccccc} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array}.$$

Bản thân các quan hệ lại liên quan với nhau tạo nên các quan hệ mới. Chẳng hạn, hợp giữa các quan hệ là một hình thức tạo nên các quan hệ mới.

Định nghĩa 5.1.2. Giả sử R_1 là quan hệ từ S_1 lên S_2; R_2 là quan hệ từ S_2 lên S_3. *Hợp của hai quan hệ* R_1 và R_2 là một quan hệ từ S_1 lên S_3 xác định bởi

$$R_2 \circ R_1 := \{(x, z) \in S_1 \times S_3 \mid \text{ tồn tại } y \in S_2 \text{ để } (x, y) \in R_1, (y, z) \in R_2\}.$$

Ví dụ 5.1.5. Giả sử T là tập các chứng chỉ, U là tập các khoa. Xét quan hệ R như trong Ví dụ 5.1.1. Quan hệ $R' \subset S \times U$ gồm các cặp (b, c) sao cho chứng chỉ $b \in T$ là bắt buộc ghi danh học khoa U. Thế thì $R' \circ R$ là tập các cặp (a, c) sao cho tồn tại chứng chỉ bắt buộc mà sinh viên a phải học khi ghi danh vào khoa c. Chú ý rằng trong trường hợp này $R \circ R'$ là không có nghĩa!

Tính chất 5.1.3. *Hợp các quan hệ có các tính chất sau:*

(a) Tính kết hợp

$$R_3 \circ (R_2 \circ R_1) = (R_3 \circ R_2) \circ R_1.$$

(b) Tính phân bố

$$\begin{aligned} R_3 \circ (R_1 \cup R_2) &= (R_3 \circ R_1) \cup (R_3 \circ R_2), \\ (R_2 \cup R_3) \circ R_1 &= (R_2 \circ R_1) \cup (R_3 \circ R_1). \end{aligned}$$

(c) Nếu $R_1 \subset R_2$ và $R_3 \subset R_4$ thì

$$\begin{aligned} R_1 \cup R_3 &\subset R_2 \cup R_4, \\ R_1 \cap R_3 &\subset R_2 \cap R_4. \end{aligned}$$

(d) Nếu $R_1 \subset R_2$ và $R_3 \subset R_4$ thì

$$R_3 \circ R_1 \subset R_4 \circ R_2.$$

Chứng minh. Bài tập. □

Ví dụ 5.1.6. Đặt $S_1 := \{1,2,3,4,5\}, S_2 := \{a,b,c\}$ và $S_3 := [e,f,g,h\}$. Xét các quan hệ từ S_1 lên S_2 và từ S_2 lên S_3 xác định tương ứng bởi

$$R_1 := \{(1,a),(2,a),(2,c),(3,a),(3,b),(4,a),(4,b),(4,c),(5,b)\},$$
$$R_2 := \{(a,e),(a,g),(b,f),(b,g),(b,h),(c,e),(c,g),(c,h)\}.$$

Khi đó

$$R_2 \circ R_1 = \{(1,e),(1,g),(2,e),(2,g),(2,h),(3,e),(3,f),(3,g),(3,h),$$
$$(4,e),(4,f),(4,g),(4,h),(5,f),(5,g),(5,h)\},$$

và các ma trận A_1, A_2 và A tương ứng các quan hệ R_1, R_2 và $R_2 \circ R_1$ là

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

So sánh A và ma trận tích của A_1 và A_2

$$A_1A_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 0 & 2 & 1 \\ 1 & 1 & 2 & 1 \\ 2 & 1 & 3 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

ta thấy số 1 trong ma trận A tương ứng với phần tử khác 0 trong ma trận A_1A_2! Điều này sẽ được giải thích trong phần sau.

Định nghĩa 5.1.4. Giả sử R là quan hệ từ S lên T. *Quan hệ ngược* của R, ký hiệu R^{-1}, là một quan hệ từ T lên S xác định bởi

$$R^{-1} := \{(x,y) \in T \times S \mid (y,x) \in R\}.$$

Tính chất 5.1.5. *Giả sử R là quan hệ trên S. Khi đó*

(a) $R = R^{-1}$ nếu và chỉ nếu R đối xứng, tức là

$$R = R^{-1} \Leftrightarrow xRy \text{ suy ra } yRx.$$

(b) $R \cap R^{-1} \subset E := \{(x,x) \mid x \in S\}$ nếu và chỉ nếu R phản đối xứng, tức là

$$R \cap R^{-1} \subset E \Leftrightarrow xRy \text{ và } yRx \text{ thì } x = y.$$

Chứng minh. (a) Hiển nhiên theo định nghĩa.

(b) Giả sử R phản đối xứng, và $(x,y) \in R \cap R^{-1}$. Khi đó xRy và yRx. Suy ra xRx. Hay $(x,x) \in E$.

Ngược lại giả sử $R \cap R^{-1} \subset E, xRy$ và yRx. Thì $(x,y) \in R \cap R^{-1} \subset E$. Do đó $(x,y) \in E$. □

Bài tập

1. Đặt $S := \{0, 1, 2\}$. Mỗi phát biểu sau xác định một quan hệ R trên S bởi mRn nếu khẳng định là đúng đối với $m, n \in S$. Viết mỗi quan hệ như một tập các cặp có thứ tự.

(a)	$m \leq n$.	(d)	$mn = 0$.	(g)	$m^2 + n^2 = 2$.
(b)	$m < n$.	(e)	$mn = m$.	(h)	$m^2 + n^2 = 3$.
(c)	$m = n$.	(f)	$m + n \in S$.	(i)	$m = \max\{n, 1\}$.

   Các quan hệ nào là đối xứng? phản đối xứng? Viết ma trận và vẽ các đồ thị tương ứng.

2. Các quan hệ hai ngôi sau xác định trên $\mathbb{N}$.

   (a) Viết quan hệ hai ngôi R_1 xác định bởi $m + n = 5$ dạng các cặp thứ tự.

   (b) Như trên với R_2 xác định bởi $\max\{m, n\} = 2$.

   (c) Quan hệ hai ngôi R_3 xác định bởi $\min\{m, n\} = 2$ gồm vô hạn các cặp thứ tự. Hãy viết năm cặp trong đó.

3. Nếu A là ma trận của quan hệ R từ S lên T (giả thiết S và T là các tập hữu hạn). Tìm ma trận của quan hệ ngược R^{-1}.

4. Giả sử R là quan hệ hai ngôi trên tập S. Chứng minh rằng R là đối xứng nếu và chỉ nếu $R = R^{-1}$.

5. Giả sử R_1, R_2 là các quan hệ từ S lên T.

   (a) Chứng minh rằng $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$.

   (b) Chứng minh rằng $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$.

   (c) Chứng minh rằng nếu $R_1 \subseteq R_2$ thì $R_1^{-1} \subseteq R_2^{-1}$.

6. Giả sử G là đồ thị của quan hệ R trên tập hữu hạn S. Mô tả đồ thị của quan hệ R^{-1}.

7. Trên tập $S := \{1, 2, 3, 4\}$ xét các quan hệ hai ngôi sau:

   $$\begin{aligned} R_1 &:= \{(1,1), (1,2), (3,4), (4,2)\}, \\ R_2 &:= \{(1,1), (2,1), (3,1), (4,4), (2,2)\}. \end{aligned}$$

   Liệt kê các phần tử của $R_1 \circ R_2$ và $R_2 \circ R_1$.

8. Khảo sát các quan hệ R_1 và R_2 từ S lên T và các quan hệ R_3 và R_4 từ T lên U.

   (a) Chứng minh rằng $(R_3 \cup R_4) \circ R_1 = R_3 \circ R_1 \cup R_4 \circ R_1$.

   (b) Chứng minh rằng $R_3 \circ (R_1 \cap R_2) \subseteq R_3 \circ R_1 \cap R_3 \circ R_2$ và đẳng thức không nhất thiết đúng.

   (c) Các quan hệ $(R_3 \cap R_4) \circ R_1$ và $R_3 \circ R_1 \cap R_4 \circ R_1$ có liên hệ như thế nào?

5.2 Quan hệ và ma trận

Như Ví dụ 5.1.6 chỉ ra, ma trận của quan hệ $R_2 \circ R_1$ không phải là tích A_1A_2 của các ma trận R_1 và R_2. Tuy nhiên chúng có mối liên hệ: phần tử bằng 1 trong A tương ứng một-một với phần tử khác không trong A_1A_2.

Xét $\mathbb{B} := \{0, 1\}$ và hai *phép toán Boole* $\wedge, \vee$ định nghĩa như sau:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

Ta có

Tính chất 5.2.1. *Với mọi $x, y \in \mathbb{B}$ ta có*

$$x \vee y = \max\{x, y\}, \quad x \wedge y = \min\{x, y\}.$$

Chứng minh. Bài tập. □

Định nghĩa 5.2.2. (a) A được gọi là *ma trận Boole* nếu các phần tử của nó thuộc $\mathbb{B}$.

(b) *Tích hai ma trận Boole* A_1 và A_2 cấp $m \times n$ và $n \times p$ tương ứng là ma trận Boole cấp $m \times p$, kí hiệu $A_1 * A_2$, xác định bởi

$$(A_1 * A_2)[i, j] := \vee_{k=1}^{n}(A_1[i, k] \wedge A_2[k, j]), \quad i = 1, 2, \ldots, m, j = 1, 2, \ldots, p.$$

(c) *Hội hai ma trận Boole* A_1 và A_2 cấp $m \times n$ là ma trận Boole cấp $m \times n$, kí hiệu $A_1 \wedge A_2$, có các phần tử là

$$(A_1 \wedge A_2)[i, j] := A_1[i, j] \wedge A_2[i, j], \quad i = 1, 2, \ldots, m, j = 1, 2, \ldots, n.$$

(d) *Tuyển hai ma trận Boole* A_1 và A_2 cấp $m \times n$ là ma trận Boole cấp $m \times n$, kí hiệu $A_1 \vee A_2$, có các phần tử là

$$(A_1 \vee A_2)[i, j] := A_1[i, j] \vee A_2[i, j], \quad i = 1, 2, \ldots, m, j = 1, 2, \ldots, n.$$

Ví dụ 5.2.1. Trong Ví dụ 5.1.6 thì $A = A_1 * A_2$.

Định lý 5.2.3. *Nếu A_1 và A_2 là các ma trận tương ứng quan hệ R_1 từ A lên B và R_2 từ B lên C thì $A_1 * A_2$ là ma trận của quan hệ hợp $R_2 \circ R_1$.*

Chứng minh. Ta có

$$\begin{aligned}(A_1 * A_2)[i, j] = 0 &\Leftrightarrow A_1[i, k] \wedge A_2[k, j] = 0, \forall k = 1, 2, \ldots, n, \\ &\Leftrightarrow A_1[i, k] = A_2[k, j] = 0, \forall k = 1, 2, \ldots, n.\end{aligned}$$

□

Ví dụ 5.2.2. Giả sử R là quan hệ trên $\{1,2,3\}$ với ma trận

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Quan hệ $R^2 := R \circ R$ có ma trận

$$A * A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Và quan hệ $R^3 := R^2 \circ R$ có ma trận

$$A * A * A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = A.$$

Suy ra $R = R^3$. Hơn nữa với mọi $n \geq 1$ ta có

$$R^{n+2} = R^{(n-1)+3} = R^{n-1} \circ R^3 = R^{n-1} \circ R = R^n!$$

Ví dụ 5.2.3. Giả sử R_1 và R_2 là các quan hệ trên $\{1,2\}$ có các ma trận Boole tương ứng

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Do

$$A_1 * A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = A_2 * A_1,$$

nên $(2,2) \in R_2 \circ R_1$ nhưng $(2,2) \notin R_1 \circ R_2$. Suy ra $R_1 \circ R_2 \neq R_2 \circ R_1$.

Định lý 5.2.4. *Tập $\mathcal{P}(S \times S)$, tất cả các quan hệ trên S, với phép toán hợp là nửa nhóm, tức là có các tính chất sau: phép toán hợp có tính kết hợp và $\mathcal{P}(S \times S)$ chứa phần tử đơn vị.*

Chứng minh. Thật vậy, phép hợp có tính chất kết hợp do Tính chất 5.1.3(a); và đơn vị là quan hệ "đồng nhất":

$$E := \{(x,x) \in S \mid x \in S\}.$$

□

Định lý sau chỉ ra việc nghiên cứu quan hệ chuyển về nghiên cứu các ma trận của chúng.

Định lý 5.2.5. *Giả sử S là tập n phần tử. Khi đó tồn tại ánh xạ một-một lên giữa tập $\mathcal{P}(S \times S)$ các quan hệ trên S và tập các ma trận Boole cấp $n \times n$. Ánh xạ này bảo toàn các phép toán nửa nhóm: nếu R_1, R_2 và R là các quan hệ với các ma trận Boole A_1, A_2 và A tương ứng, thì*

$$R_2 \circ R_1 = R \Leftrightarrow A_1 * A_2 = A.$$

Chứng minh. Hiển nhiên theo các kết quả trên. □

Định nghĩa 5.2.6. Quan hệ hai ngôi R trên S được gọi là

(a) *Phản xạ* nếu xRx với mọi $x \in S$;

(b) *Bắc cầu* nếu xRy và yRz thì xRz.

Ví dụ 5.2.4. Xét các quan hệ R_1, R_2, R_3 và E trên $S := \{1, 2, 3, 4\}$ tương ứng với các ma trận

$$A_1 := \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad A_2 := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

$$A_3 := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad I_4 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(a) R_1 là quan hệ được xác định bởi mR_1n nếu $m \leq n$. Quan hệ R_1 là phản xạ và bắc cầu.

(b) R_2 là quan hệ được xác định bởi mR_2n nếu $|m - n| \leq 1$. Quan hệ R_2 là phản xạ, đối xứng nhưng không bắc cầu.

(c) R_3 là quan hệ được xác định bởi mR_3n nếu và chỉ nếu $m = n \pmod 3$. Ta có R_3 là quan hệ phản xạ, đối xứng và bắc cầu.

(d) Quan hệ $E := \{(m, n) \in S \times S \mid m = n\}$ trên S là phản xạ, đối xứng và bắc cầu.

Ví dụ 5.2.5. (a) Quan hệ R trên $\mathbb{Z}$ định nghĩa bởi

$$mRn \quad \text{nếu và chỉ nếu} \quad m + n = 0 \pmod 3$$

là đối xứng, không phản xạ do $(1, 1) \notin R$ và không bắc cầu do $(4, 2), (2, 1) \in R$ nhưng $(4, 1) \notin R$.

(b) Với $m, n \in \mathbb{Z}$ định nghĩa mRn nếu $m - n$ lẻ. Quan hệ là đối xứng nhưng không phản xạ và không bắc cầu.

Tính chất 5.2.7. *Giả sử R là quan hệ trên tập A. Khi đó*

(a) R phản xạ nếu và chỉ nếu $E \subset R$.

(b) R bắc cầu nếu và chỉ nếu $R^2 \subset R$.

Chứng minh. (a) Hiển nhiên.

(b) Giả sử R là bắc cầu và $(x,z) \in R^2$. Khi đó tồn tại $y \in A$ sao cho $(x,y),(y,z) \in R$. Vì R bắc cầu nên $(x,z) \in R$. Ngược lại, giả sử $R^2 \subset R$. Xét $(x,y),(y,z) \in R$. Thì $(x,z) \in R^2$. Vậy $(x,z) \in R$. □

Giả sử A_1, A_2 là hai ma trận Boole cùng cấp $m \times n$. Ký hiệu $A_1 \leq A_2$ nghĩa là

$$A_1[i,j] \leq A_2[i,j]$$

với mọi $i = 1,2,\ldots,m, j = 1,2,\ldots,n$.

Tính chất 5.2.8. *Giả sử R_1, R_2 là hai quan hệ từ S lên T tương ứng các ma trận A_1, A_2. Ta có*

(a) $R_1 \subseteq R_2$ nếu và chỉ nếu $A_1 \leq A_2$.

(b) $R_1 \cup R_2$ có ma trận Boole $A_1 \vee A_2$.

(c) $R_1 \cap R_2$ có ma trận Boole $A_1 \wedge A_2$.

Chứng minh. Bài tập. □

Hệ quả 5.2.9. *Giả sử R là quan hệ trên tập S tương ứng ma trận Boole $A := (a_{ij})_{n\times n}, n = \#S$. Khi đó*

(a) $R^2 \subseteq R$ nếu và chỉ nếu $A * A \leq A$.

(b) R phản xạ nếu và chỉ nếu $a_{ii} = 1, i = 1,2,\ldots,n$.

(c) R đối xứng nếu và chỉ nếu $A = A^t$.

(d) R phản đối xứng nếu và chỉ nếu $A \wedge A^t \leq I_n$.

(e) R bắc cầu nếu và chỉ nếu $A * A \leq A$.

Chứng minh. Bài tập. □

Bài tập

1. Với mỗi ma trận Boole sau, xét quan hệ tương ứng R trên $\{1,2,3\}$. Tìm ma trận Boole của R^2 và xác định quan hệ nào là bắc cầu.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

   Vẽ đồ thị của các quan hệ trên.

2. Giả sử $S := \{1,2,3\}, T := \{a,b,c,d\}$ và R_1, R_2 là các quan hệ từ S lên T với các ma trận Boole

$$A_1 := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \qquad A_2 := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

   (a) Tìm các ma trận Boole của R_1^{-1}, R_2^{-1}.

   (b) Tìm các ma trận Boole của $R_1^{-1} \circ (R_1 \cap R_2), (R_1^{-1} \circ R_1) \cap (R_1^{-1} \circ R_2)$.

   (c) Tìm các ma trận Boole của $(R_1^{-1} \cup R_2^{-1}) \circ R_2, (R_1^{-1} \circ R_2) \cup (R_2^{-1} \circ R_2)$.

   (d) So sánh các câu trả lời trong phần (b) và (c) với các khẳng định trong Bài tập 10.

3. Giả sử $S := \{1,2,3\}$ và $R := \{(1,1),(1,2),(1,3),(3,2)\}$.

   (a) Tìm các ma trận của $R, R \circ R^{-1}$ và $R^{-1} \circ R$.

   (b) Vẽ các đồ thị của các quan hệ trong phần (a).

   (c) Chứng minh rằng R là bắc cầu (tức là $R^2 \subseteq R$), nhưng $R^2 \neq R$.

   (d) $R \cup R^{-1}$ là quan hệ bắc cầu? Giải thích.

   (e) Tìm R^n với $n = 2, 3, \ldots$.

4. Giả sử $S := \{1,2,3\}$ và $R := \{(2,1),(2,3),(3,2)\}$.

   (a) Tìm các ma trận của R, R^{-1} và $R \circ R^2$.

   (b) Vẽ các đồ thị của các quan hệ trong phần (a).

   (c) R là bắc cầu?

   (d) R^2 là bắc cầu?

   (e) $R \cup R^2$ là bắc cầu?

5. Giả sử R là quan hệ trên $S := \{1,2,3\}$ với ma trận Boole

$$A := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

   (a) Tìm ma trận Boole của $R^n, n \in \mathbb{N}$.

   (b) R là phản xạ? Đối xứng? Bắc cầu?

6. Lặp lại Bài tập 5 với

$$A := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

7. Giả sử P là tập tất cả các người và khảo sát quan hệ R, trong đó pRq nếu p "thích" q.

(a) Mô tả các quan hệ $R \cap R^{-1}$, $R \cup R^{-1}$, và R^2.

(b) R là phản xạ? Đối xứng? Bắc cầu?

8. Cho ví dụ quan hệ mà

   (a) Phản đối xứng, bắc cầu nhưng không phản xạ.

   (b) Đối xứng nhưng không phản xạ hay bắc cầu.

9. Với ánh xạ $f\colon S \to T$ ta định nghĩa quan hệ

$$R_f := \{(x, y) \in S \times T | y = f(x)\}.$$

   Xét các ánh xạ $f, g\colon \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ xác định bởi $f(m) := \max\{2, 4 - m\}$ và $g(m) := 5 - m$.

   (a) Tìm các ma trận Boole A_f, A_g của các quan hệ R_f và R_g tương ứng với các ánh xạ f, g.

   (b) Tìm các ma trận Boole của R_f, R_g, và $R_{f\circ g}$ và so sánh.

   (c) Tìm các ma trận Boole của R_f^{-1}, R_g^{-1}. Các quan hệ này tương ứng với các ánh xạ nào?

10. Khảo sát các quan hệ R_1 và R_2 trên tập S. Chứng minh hoặc cho phản ví dụ:

    (a) Nếu R_1 và R_2 phản xạ thì $R_2 \circ R_1$ phản xạ.

    (b) Nếu R_1 và R_2 đối xứng thì $R_2 \circ R_1$ đối xứng.

    (c) Nếu R_1 và R_2 bắc cầu thì $R_2 \circ R_1$ bắc cầu.

11. Giả sử R_1, R_2 là các quan hệ hai ngôi trên tập S.

    (a) Chứng minh rằng $R_1 \cap R_2$ là phản xạ nếu R_1 và R_2 là phản xạ.

    (b) Chứng minh rằng $R_1 \cap R_2$ là đối xứng nếu R_1 và R_2 là đối xứng.

    (c) Chứng minh rằng $R_1 \cap R_2$ là bắc cầu nếu R_1 và R_2 là bắc cầu.

12. Giả sử R_1, R_2 là các quan hệ hai ngôi trên tập S.

    (a) $R_1 \cup R_2$ là phản xạ nếu R_1 và R_2 là phản xạ?

    (b) $R_1 \cup R_2$ là đối xứng nếu R_1 và R_2 là đối xứng?

    (c) $R_1 \cup R_2$ là bắc cầu nếu R_1 và R_2 là bắc cầu?

13. Giả sử R là quan hệ từ $S := \{1, 2, 3, 4\}$ lên $T := \{a, b, c\}$ với ma trận Boole

$$A := \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array}.$$

(a) Chứng minh rằng $R^{-1} \circ R$ là quan hệ đối xứng trên S.

(b) Chứng minh rằng $R \circ R^{-1}$ là quan hệ đối xứng trên S.

(c) Các quan hệ $R \circ R^{-1}, R^{-1} \circ R$ là phản xạ? Bắc cầu?

14. Giả sử R là quan hệ từ S lên T.

(a) Chứng minh rằng $R^{-1} \circ R$ là quan hệ đối xứng trên S. (Không sử dụng ma trận Boole do S hoặc T có thể không hữu hạn).

(b) Suy ra $R \circ R^{-1}$ là đối xứng trên T.

(c) Khi nào thì $R^{-1} \circ R$ là phản xạ?

15. Giả sử R_1 là quan hệ từ S lên T, R_2 là quan hệ từ T lên U, trong đó S, T, U là các tập hữu hạn. Dựa vào ma trận Boole biểu diễn quan hệ, chứng minh rằng

$$(R_2 \circ R_1)^{-1} = R_1^{-1} \circ R_2^{-1}.$$

16. Giả sử R_1, R_2 là các quan hệ từ $S := \{1, 2, \ldots, m\}$ lên $T := \{1, 2, \ldots, n\}$, tương ứng với các ma trận A_1, A_2. Chứng minh rằng $R_1 \subseteq R_2$ nếu và chỉ nếu $A_1 \leq A_2$.

17. Sử dụng tính kết hợp của các quan hệ, chứng minh rằng tích Boole là một phép toán có tính kết hợp.

18. Giả sử S là tập khác trống. $\mathcal{P}(S \times S)$ là một nhóm với phần tử ngược R^{-1}? Giải thích.

19. Giả sử R là quan hệ trên S và $R^* := \cup_{n \geq 0} R^n$ là *bao đóng truyền ứng* của R. Chứng minh rằng R^* là phản xạ và bắc cầu. Hơn nữa, nếu $R \subset R'$, trong đó R' là bắc cầu và đối xứng, thì $R^* \subset R'$.

5.3 Quan hệ thứ tự

Định nghĩa 5.3.1. Quan hệ hai ngôi R trên tập S được gọi là *quan hệ thứ tự* (hay rõ hơn, *quan hệ thứ tự bộ phận*) nếu nó có các tính chất: phản xạ, phản đối xứng và bắc cầu. Khi đó thay cho cách viết aRb, người ta thường viết $a \leq b$ hoặc $b \geq a$ và nói rằng a *đi trước* b, hoặc b *đi sau* a. Như vậy

(a) $a \leq a$ với mọi $a \in S$.

(b) Nếu $a \leq b$ và $b \leq a$ thì $a = b$.

(c) Nếu $a \leq b$ và $b \leq c$ thì $a \leq c$.

Nếu $a \leq b$ và $a \neq b$ ta ký hiệu $a < b$ hoặc $b > a$ và nói rằng a *thực sự đi trước* b hoặc b *thực sự đi sau* a.

Kí hiệu $(S, \leq)$ có nghĩa $\leq$ là quan hệ thứ tự trên tập S; và $(S, \leq)$ được gọi là tập có *thứ tự bộ phận*.

Nhận xét rằng với hai phần tử $a, b \in S$ thì không nhất thiết phải có $a \leq b$ hoặc $b \leq a$. Nếu hoặc $a \leq b$ hoặc $b \leq a$ thì các phần tử a và b gọi là *so sánh được với nhau*. Nếu $A \subset S$ và hai phần tử bất kỳ của A là so sánh được với nhau thì A gọi là *tập con sắp thẳng* của S.

Ví dụ 5.3.1. Xét trường số phức $\mathbb{C}$ và quan hệ $x \leq y$, trong đó $x = a + ib$ và $y = c + id, i = \sqrt{-1}$, nếu $a \leq c$ và $b \leq d$. Hiển nhiên $\leq$ là quan hệ thứ tự. Đặt

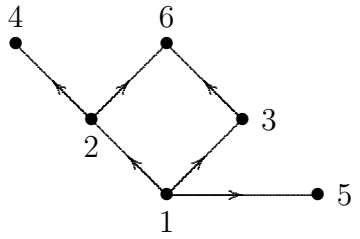
$$A := \{x \in \mathbb{C} \mid x = a + i0, a \in \mathbb{R}\}.$$

Với quan hệ $\leq$ tập A là tập con sắp thẳng của $\mathbb{C}$. Ta có $2 + i3 < 2 + i5$. Nhưng $2 + i3$ không so sánh được với $1 + i5$.

Định nghĩa 5.3.2. (a) Giả sử $\leq$ là quan hệ thứ tự trên tập S. Ta nói rằng t *phủ* s nếu $s < t$ và không tồn tại $u \in S$ sao cho $s < u < t$.

(b) Lược đồ *Hasse* của $(S, \leq)$ là một *đồ thị có hướng* gồm các đỉnh là các phần tử của S và nếu t phủ s thì có một cung nối từ s đến t.

Ví dụ 5.3.2. (a) Đặt $S := \{1, 2, 3, 4, 5, 6\}$. Ta viết $m|n$ nếu n là bội nguyên của m. Khi đó $(S, |)$ là tập được sắp thứ tự bộ phận. Ta có lược đồ Hasse trong Hình 5.2.



Hình 5.2:

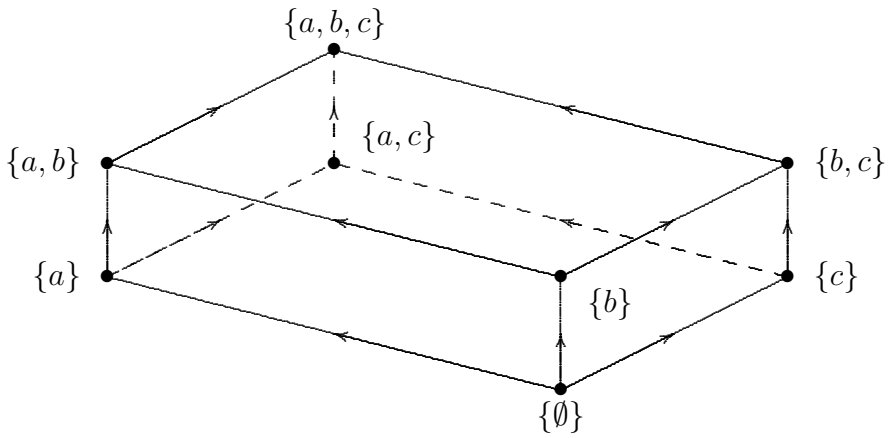
(b) Trên $S := \mathcal{P}(\{a, b, c\})$ xét quan hệ bao hàm $\subset$. Khi đó $(S, \subset)$ là tập được sắp thứ tự bộ phận và có lược đồ Hasse trong Hình 5.3.

(c) Lược đồ trong Hình 5.4 không phải là lược đồ Hasse (tại sao?):

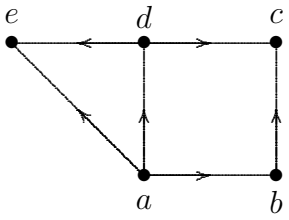
(d) Các lược đồ trong Hình 5.5 là lược đồ Hasse của các tập được sắp thứ tự bộ phận (được suy trực tiếp từ đồ thị).

Nói chung với lược đồ Hasse của tập được sắp thứ tự bộ phận, ta có $s \leq t$ nếu và chỉ nếu hoặc $s = t$ hoặc có một đường đi định hướng từ s đến t.

Giả sử $(S, \leq)$ là tập được sắp thứ tự bộ phận và $A \subset S, A \neq \emptyset$.



Hình 5.3:



Hình 5.4:

Định nghĩa 5.3.3. (a) Phần tử $x \in S$ được gọi là *cận trên* của A nếu $a \leq x$ với mọi $a \in A$; khi đó A được gọi là *bị chặn trên*. Nếu x là cận trên của A và $x \in A$ thì x được gọi là *phần tử lớn nhất* của A, ký hiệu

$$\max A := \max\{a \mid a \in A\}.$$

(b) Phần tử $y \in S$ được gọi là *cận dưới* của A nếu $y \leq a$ với mọi $a \in A$; khi đó A được gọi là *bị chặn dưới*. Nếu y là cận dưới của A và $y \in A$ thì y được gọi là *phần tử nhỏ nhất* của A, ký hiệu

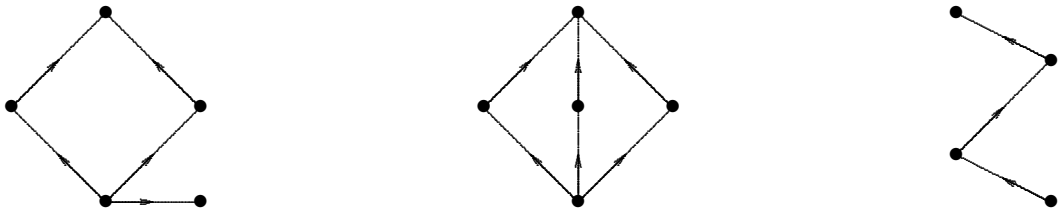
$$\min A := \min\{a \mid a \in A\}.$$

(c) Ký hiệu A^s là tập hợp tất cả các cận trên của A. Nếu $A^s \neq \emptyset$ (tức là nếu A bị chặn trên) và nếu A^s có phần tử nhỏ nhất x^* thì x^* được gọi là *cận trên nhỏ nhất* hoặc *cận trên đúng* của A, ký hiệu

$$\sup A := \sup\{a \mid a \in A\}.$$

(d) Ký hiệu A^i là tập hợp tất cả các cận dưới của A. Nếu $A^i \neq \emptyset$ (tức là nếu A bị chặn dưới) và nếu A^i có phần tử lớn nhất y^* thì y^* được gọi là *cận dưới lớn nhất* hoặc *cận dưới đúng* của A, ký hiệu

$$\inf A := \inf\{a \mid a \in A\}.$$



Hình 5.5:

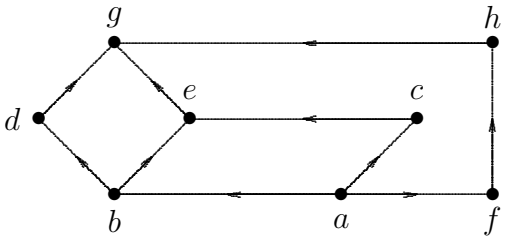
Ví dụ 5.3.3. Xét tập được sắp thứ tự bộ phận trong Ví dụ 5.3.2(a). Tập S không có phần tử lớn nhất; 1 là phần tử nhỏ nhất.

Nhận xét 6. (a) Phần tử lớn nhất (nhỏ nhất) của A, nếu tồn tại, là duy nhất.

(b) Nếu tồn tại $x = \max A$ (tương ứng $y = \min A$) thì $x = \sup A$ (tương ứng $y = \inf A$). Điều ngược lại không đúng (cho ví dụ).

Ví dụ 5.3.4. (a) Trong tập được sắp thứ tự bộ phận $(\{1, 2, 3, 4, 5, 6\}, |)$ tập con $\{2, 3\}$ có đúng một cận trên là 6, và do đó $\sup\{2, 3\} = 6$. Tương tự $\inf\{2, 3\} = 1$. Tập con $\{4, 6\}$ không có cận trên; $\inf\{4, 6\} = 2$. Tập con $\{3, 6\}$ có cận trên 6 và hai cận dưới là 1 và 3; do đó $\sup\{3, 6\} = 6$ và $\inf\{3, 6\} = 3$. Vậy các cận trên đúng và cận dưới đúng của A chưa chắc tồn tại, và nếu chúng tồn tại chưa chắc chúng thuộc tập con A.

(b) Xét tập con được sắp thứ tự bộ phận có lược đồ Hasse trong Hình 5.6. Ta có $\sup\{d, f\} = g$ và $\inf\{b, d, e, f\} = a$. Nhưng $\sup\{b, c\}$ và $\inf\{d, e, f\}$ không tồn tại.



Hình 5.6:

Định nghĩa 5.3.4. Tập được sắp thứ tự bộ phận $(S, \leq)$ được gọi là *lattice* (dàn) nếu tồn tại $\sup\{x, y\}$ và $\inf\{x, y\}$ với mọi $x, y \in S$. Khi đó ta định nghĩa hai phép toán

$$x \vee y := \sup\{x, y\}, \quad x \wedge y := \inf\{x, y\}.$$

Hiển nhiên $\vee$ và $\wedge$ là các phép toán hai ngôi trên S. Hơn nữa

$$x \wedge y = x \Leftrightarrow x \leq y \Leftrightarrow x \vee y = y.$$

Bằng quy nạp, chúng ta có thể chứng minh mọi tập con A hữu hạn phần tử của lattice L luôn tồn tại $\sup A, \inf A$.

Ví dụ 5.3.5. (a) Tập được sắp thứ tự trong Ví dụ 5.3.2(b) là lattice.

(b) Tập được sắp thứ tự trong Ví dụ 5.3.2(a) không là lattice do tập $\{3, 4\}$ không có cận trên trong S.

Từ định nghĩa của các phép toán $\wedge$ và $\vee$ ta có các đẳng thức sau:

$$\begin{array}{lcllcl} x \wedge x & = & x, & x \vee x & = & x, \\ x \wedge y & = & y \wedge x, & x \vee y & = & y \vee x, \\ (x \wedge y) \wedge z & = & x \wedge (y \wedge z), & (x \vee y) \vee z & = & x \vee (y \vee z). \end{array}$$

Bài tập

1. Vẽ lược đồ Hasse của các tập được sắp thứ tự bộ phận sau:

   (a) $(\{1, 2, 3, 4, 6, 8, 12, 24\}, |)$, trong đó $m|n$ nghĩa là n chia hết cho m.

   (b) Tập các tập con của $\{3, 7\}$ với quan hệ $\subseteq$.

2. Tìm các tập con thực sự cực đại của tập $\{a, b, c\}$. Tức là tìm các phần tử cực đại của tập con được sắp thứ tự bộ phận của $\mathcal{P}(\{a, b, c\})$ là những tập con thực sự của $\{a, b, c\}$.

3. Trên $\mathbb{R} \times \mathbb{R}$ xét các quan hệ $<, \prec, \preceq$ xác định bởi

   $$\begin{array}{l} (x, y) < (z, w) \text{ nếu } x^2 + y^2 < z^2 + w^2, \\ (x, y) \prec (z, w) \text{ nếu } (x, y) < (z, w) \text{ hoặc } (x, y) = (z, w), \\ (x, y) \preceq (z, w) \text{ nếu } x^2 + y^2 \leq z^2 + w^2. \end{array}$$

   (a) Quan hệ nào là quan hệ thứ tự bộ phận?

   (b) Vẽ một phần của $\{(x, y) \mid (x, y) \prec (3, 4)\}$ trong $\mathbb{R}^2$.

   (c) Vẽ một phần của $\{(x, y) \mid (x, y) \preceq (3, 4)\}$ trong $\mathbb{R}^2$.

4. Giả sử $\mathcal{E}(\mathbb{N})$ là tập tất cả các tập con hữu hạn của $\mathbb{N}$ mà có một số chẵn phần tử, với quan hệ thứ tự bộ phận $\subseteq$.

   (a) Đặt $A := \{1, 2\}$ và $B := \{1, 3\}$. Tìm bốn cận trên của $\{A, B\}$.

   (b) $\{A, B\}$ có cận trên nhỏ nhất trong $\mathcal{E}(\mathbb{N})$? Giải thích.

   (c) $\mathcal{E}(\mathbb{N})$ là lattice?

5. Mọi tập con được sắp thứ tự bộ phận của một lattice là một lattice? Giải thích.

6. Bảng trong hình sau cho quan hệ thứ tự bộ phận. Nó cho giá trị $x \vee y$ đối với lattice $(L, \leq)$. Chẳng hạn $b \vee c = d$.

$\vee$	a	b	c	d	e	f
a		e	a	e	e	a
b			d	d	e	b
c				d	e	c
d					e	d
e						e
f						

   (a) Viết các chỗ trống còn lại của bảng.

   (b) Tìm các phần tử lớn nhất và nhỏ nhất của L.

   (c) Chứng minh rằng $f \leq c \leq d \leq e$.

   (d) Vẽ lược đồ Hasse của L.

7. Xét $\mathbb{R}$ với thứ tự $\leq$ thông thường.

   (a) $\mathbb{R}$ là lattice? Nếu đúng thì ý nghĩa của $a \vee b, a \wedge b$ trong $\mathbb{R}$.

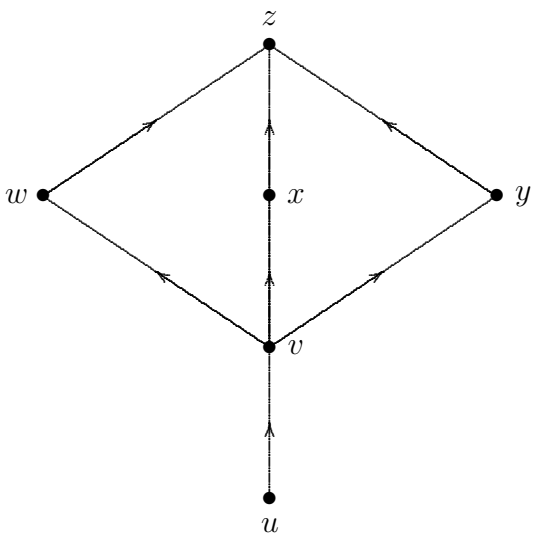
   (b) Tìm ví dụ của tập con khác trống của $\mathbb{R}$ mà không có cận trên nhỏ nhất.

   (c) Tìm $\sup\{x \in \mathbb{R} \mid x < 73\}$, $\sup\{x \in \mathbb{R} \mid x \leq 73\}$, $\sup\{x \in \mathbb{R} \mid x^2 \leq 73\}$, $\inf\{x \in \mathbb{R} \mid x^2 < 73\}$.

8. (a) Dùng quy nạp, chứng minh rằng mọi tập được sắp thứ tự bộ phận hữu hạn có phần tử nhỏ nhất.

   (b) Cho ví dụ tập được sắp thứ tự bộ phận có phần tử lớn nhất nhưng không có phần tử nhỏ nhất.

9. Khảo sát tập được sắp thứ tự bộ phận C có lược đồ Hasse sau:



Chứng minh các bất đẳng thức:

$$w \vee (x \wedge y) \neq (w \vee x) \wedge (w \vee y),$$
$$w \wedge (x \vee y) \neq (w \wedge x) \vee (w \wedge y).$$

Từ đó suy ra lattice C không thoả mãn luật phân phối.

10. (a) Chứng minh rằng nếu $\preceq$ là một thứ tự bộ phận trên S thì quan hệ ngược $\succeq$ cũng là thứ tự bộ phận trên S.

    (b) Chứng minh rằng nếu $\prec$ là quan hệ trên S thoả tính chất (T) và $s \prec s$ sai với mọi $s \in S$ thì quan hệ $\preceq$ xác định bởi

    $$x \preceq y \text{ nếu và chỉ nếu } x \prec y \text{ hoặc } x = y,$$

    là quan hệ thứ tự bộ phận.

11. Giả sử R là quan hệ phản đối xứng và bắc cầu trên tập S.

    (a) Chứng minh rằng $R \cup E$ là thứ tự bộ phận trên S.

    (b) $R \setminus E$ là thứ tự bộ phận trên S?

12. Giả sử Σ là một bảng các ký tự và Σ^* là tập các chuỗi ký tự. Xét quan hệ $\preceq$ trên Σ^* như sau. Với mỗi $x, y \in \Sigma^*$ ký hiệu $x \preceq y$ nếu x là một đoạn khởi đầu của y, tức là tồn tại $z \in \Sigma^*$ sao cho $xz = y$. Ký hiệu $\text{length}(w), w \in \Sigma^*$, là độ dài của chuỗi w.

    (a) Chứng minh rằng $\preceq$ có tính phản xạ, phản đối xứng và bắc cầu.

    (b) Chứng minh rằng nếu x phủ y thì $\text{length}(x) = 1 + \text{length}(y)$.

13. Giả sử Σ là một bảng các ký tự. Ký hiệu $w_1 \preceq w_2, w_1, w_2 \in \Sigma^*$, nghĩa là $\text{length}(w_1) \leq \text{length}(w_2)$. Quan hệ $\preceq$ là quan hệ thứ tự bộ phận trên Σ^*? Tại sao?

14. Giả sử Σ là một bảng các ký tự.

    (a) Với mỗi $x, y \in \Sigma^*$, định nghĩa $x \preceq y$ nếu tồn tại $v, v' \in \Sigma^*$ sao cho $y = vxv'$. Quan hệ $\preceq$ là thứ tự bộ phận trên Σ^*? Giải thích.

    (b) Trả lời câu hỏi trên nếu hạn chế $x, y \in \Sigma$.

15. Ký hiệu Σ^* là tập tất cả các chuỗi ký tự trên bảng chữ cái $\Sigma := \{a, b\}$. Xét quan hệ hai ngôi $\preceq$ trên $\mathcal{P}(\Sigma^*)$ bởi $A \preceq B$ nếu và chỉ nếu $A^* \subseteq B^*$. Ký hiệu (R), (S), (AS) và (T) là các tính chất phản xạ, đối xứng, phản đối xứng và bắc cầu.

    (a) Các tính chất nào trong số (R), (S), (AS), (T) mà quan hệ $\preceq$ thoả?

    (b) $\preceq$ là thứ tự bộ phận?

16. Giả sử x, y, z là các chuỗi trên bảng ký tự khác trống Σ nào đó. Quan hệ hai ngôi $P(x, y)$ sau có tính chất gì:

    $$P(x, y) \Leftrightarrow (\exists z)(\text{concat}(x, z) = y),$$

    trong đó $\text{concat}(x, z)$ là chuỗi nhận được bằng cách nối chuỗi z sau chuỗi x. Chẳng hạn, nếu $x =$ "ANH", $z =$ " EM.", thì $\text{concat}(x, z) =$ "ANH EM.".

17. Ký hiệu $\mathcal{J}(\mathbb{N})$ là họ tất cả các tập con hữu hạn của $\mathbb{N}$. Khi đó $(\mathcal{J}(\mathbb{N}), \subseteq)$ là một tập được sắp thứ tự bộ phận.

    (a) $\mathcal{J}(\mathbb{N})$ có phần tử lớn nhất? Nếu có, hãy tìm. Nếu không, giải thích.

    (b) $\mathcal{J}(\mathbb{N})$ có phần tử nhỏ nhất? Nếu có, hãy tìm. Nếu không, giải thích.

    (c) Giả sử $A, B \in \mathcal{J}(\mathbb{N})$, $\{A, B\}$ có cận trên nhỏ nhất trong $\mathcal{J}(\mathbb{N})$? Nếu có, hãy tìm. Nếu không, cho ví dụ.

    (d) Giả sử $A, B \in \mathcal{J}(\mathbb{N})$, $\{A, B\}$ có cận dưới lớn nhất trong $\mathcal{J}(\mathbb{N})$? Nếu có, hãy tìm. Nếu không, cho ví dụ.

    (e) $\mathcal{J}(\mathbb{N})$ là lattice? Giải thích.

18. Lặp lại bài tập trên, nếu thay $\mathcal{J}(\mathbb{N})$ là họ các tập con vô hạn của $\mathbb{N}$.

19. Giả sử x, y, z là các chuỗi. Ý nghĩa của biểu thức sau

$$Q(x, y) \Leftrightarrow (\exists z)(\text{concat}(z, x) = y)?$$

20. Giả sử $(A, \leq)$ là tập được sắp thứ tự bộ phận. Xét quan hệ $\geq$ trên $A : a \geq b$ nếu và chỉ nếu $b \leq a$. Chứng minh rằng $(A, \geq)$ cũng là một tập được sắp thứ tự.

21. Giả sử Σ^* là tập các dãy hữu hạn phần tử của tập Σ bao gồm cả tập trống. Chỉ ra $(\Sigma^*, \leq)$ có phải là tập được sắp thứ tự bộ phận nếu

    (a) $w \leq w'$ nếu và chỉ nếu $l(w) \leq l(w')$, trong đó $l(w)$ là độ dài của chuỗi w.

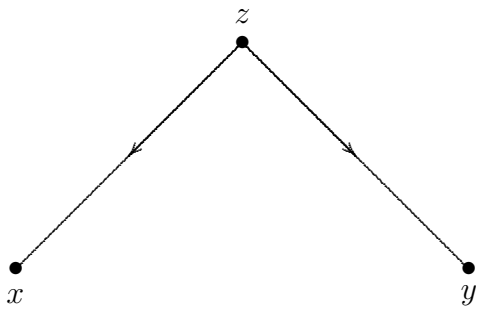
    (b) $w \leq w'$ nếu và chỉ nếu tồn tại các chuỗi $w_1, w_2 \in \Sigma^*$ sao cho $w_1 w' w_2 = w$.

22. (a) Khảo sát các phần tử x, y, z trong một tập được sắp thứ tự bộ phận. Chứng minh rằng nếu $\sup\{x, y\} = a$ và $\inf\{a, z\} = b$, thì $\sup\{x, y, z\} = b$.

    (b) Chứng minh rằng mọi tập con hữu hạn của một lattice có cận trên nhỏ nhất.

    (c) Chứng minh rằng nếu x, y, z là các phần tử của một lattice, thì $(x \vee y) \vee z = x \vee (y \vee z)$.

23. Giả sử Left là quan hệ hai ngôi trên tập các node của cây nhị phân T xác định như sau: Left(x,y) nếu và chỉ nếu x và y có chung một tổ tiên z sao cho x là node trên cây con bên trái từ z; và y là node trên cây con bên phải từ z.



    Chứng minh rằng Left(x, y) và Left(y, w) suy ra Left(x, w).

24. Giả sử $(a_1, \ldots, a_n)$ là dãy gồm n phần tử của tập hữu hạn A; R là một thứ tự bộ phận trên A. Ta nói rằng $(a_1, \ldots, a_n)$ là *sắp xếp tô pô* của A đối với R nếu với mọi $a_i, a_j \in A, (a_i, a_j) \in R$ suy ra $i < j$.

    (a) Chứng minh rằng nếu R là thứ tự bộ phận trên A, thì tồn tại các phần tử $x, y \in A$ sao cho không có $z \in A$ thoả $(z, x) \in R$ và $(y, z) \in R$. (x, y gọi là các phần tử nhỏ nhất và lớn nhất tương ứng).

    (b) Chứng minh rằng nếu R là thứ tự bộ phận trên A, thì A có thể sắp xếp tô pô đối với R.

25. Giả sử $(A, \geq)$ nhận được từ $(A, \leq)$ như trong Bài tập 19. Chứng minh rằng b là cận dưới lớn nhất đối với $(a_i | i \in I)$ trong $(A, \leq)$ nếu b là cận trên nhỏ nhất đối với $(a_i | i \in I)$ trong $(A, \geq)$.

5.4 Quan hệ tương đương

Trong mục này chúng ta sẽ nghiên cứu các quan hệ tương đương: là quan hệ mà nhóm các phần tử có cùng một đặc trưng hay tính chất.

Định nghĩa 5.4.1. Quan hệ R trên S được gọi là *quan hệ tương đương* nếu nó có các tính chất: phản xạ, đối xứng và bắc cầu. Khi đó thay cho cách viết aRb, ta thường viết $a \sim b$ hoặc $a \equiv b$.

Ví dụ 5.4.1. (a) Giả sử p là số tự nhiên lớn hơn 2. Trên tập các số tự nhiên $\mathbb{N}$, quan hệ sau là quan hệ tương đương:

$$mRn \Leftrightarrow m - n \vdots p \Leftrightarrow m = n \pmod{p}, \ \forall\, m, n \in \mathbb{N}.$$

(b) Giả sử S là tập các tam giác trong mặt phẳng. Xét quan hệ R trên S: $T_1 R T_2$ nếu và chỉ nếu tồn tại ánh xạ một-một từ tam giác T_1 lên tam giác T_2 sao cho các góc tương ứng bằng nhau. Thì R là quan hệ tương đương.

(c) Hai ma trận vuông cấp n : A và B được gọi là *tương đương,* kí hiệu $A \sim B$, nếu tồn tại các ma trận vuông cấp n khả nghịch P, Q sao cho $B = PAQ$. Khi đó "$\sim$" là quan hệ tương đương.

(d) Xét $\mathcal{P}(S)$ các tập con của tập S. Với $A, B \in \mathcal{P}(S)$, ta định nghĩa $A \sim B$ nếu *hiệu đối xứng* của chúng $A \oplus B := (A \setminus B) \cup (B \setminus A)$ là một tập hữu hạn. Thì "$\sim$" là quan hệ tương đương.

Giả sử $\sim$ là quan hệ tương đương trên tập S. Tập hợp

$$[s] := \{t \in S \mid s \sim t\}$$

được gọi là *lớp tương đương* của s, và

$$[S] := \{[s] \mid s \in S\}$$

là tập các lớp tương đương.

Ví dụ 5.4.2. Giả sử $\sim$ là quan hệ tương đương trong Ví dụ 5.4.1(a) thì

$$[m] = \{n \in \mathbb{Z} \mid m = n \pmod{p}\}.$$

Do đó với $p = 3$ ta có ba lớp tương đương: [0], [1] và [2].

Bổ đề 5.4.2. *Giả sử $\sim$ là quan hệ tương đương trên S; và $s, t \in S$. Các khẳng định sau là tương đương*

(a) $s \sim t$;

(b) $[s] = [t]$;

(c) $[s] \cap [t] \neq \emptyset$.

Chứng minh. (a) $\Rightarrow$ (b) Giả sử $s \sim t$ và xét $s' \in [s]$. Thì $s \sim s'$. Ta có $t \sim s$ (đối xứng). Suy ra $t \sim s'$ (bắc cầu). Do đó $s' \in [t]$. Vậy $[s] \subseteq [t]$. Tương tự cũng có $[t] \subseteq [s]$.

(b) $\Rightarrow$ (c) Hiển nhiên.

(c) $\Rightarrow$ (a) Lấy $u \in [s] \cap [t]$. Thì $s \sim u$ và $u \sim t$. Vậy $s \sim t$. $\square$

Nhắc lại rằng *phân hoạch* của tập A là một họ các tập con $A_1, A_2, \ldots, A_k$ của A sao cho

(a) $\bigcup_{i=1}^{k} A_i = A$; và

(b) $A_i \cap A_j = \emptyset$ với mọi $i, j = 1, 2, \ldots, k, i \neq j$.

Ví dụ 5.4.3. Họ

$$\Sigma := \{\{1, 2, 4\}, \{3, 5, 7\}, \{6, 8\}\}$$

là một phân hoạch của tập $A := \{1, 2, \ldots, 8\}$.

Định lý sau cho chúng ta mối quan hệ giữa phân hoạch và quan hệ tương đương.

Định lý 5.4.3. *(a) Nếu $\sim$ là quan hệ tương đương trên tập khác trống S thì $[S]$ là một phân hoạch của tập S.*

(b) Ngược lại, nếu $\{A_i \mid i \in I\}$ là một phân hoạch của tập S thì các tập A_i là các lớp tương đương ứng với quan hệ tương đương nào đó trên S.

Chứng minh. (a) Ta cần chứng tỏ

(i) $\bigcup_{s\in S}[s] = S$.

(ii) Với mọi $s, t \in S$ ta có hoặc $[s] = [t]$ hoặc $[s] \cap [t] = \emptyset$.

Thật vậy, hiển nhiên rằng $\bigcup_{s\in S}[s] \subset S$. Lấy $s_0 \in S$ ta có $s_0 \in [s_0]$. Do đó $S \subset \bigcup_{s\in S}[s]$. Vậy (i) đúng.

Khẳng định (ii) suy từ Bổ đề 5.4.2.

(b) Giả sử $\{A_i \mid i \in I\}$ là một phân hoạch của S. Trên S xét quan hệ $\sim$:

$$s \sim t \;\Leftrightarrow\; \text{tồn tại } i \in I \text{ sao cho } s, t \in A_i.$$

Dễ dàng kiểm tra " $\sim$" là quan hệ tương đương. □

Ví dụ 5.4.4. (a) Giả sử $\mathcal{J}$ là họ các tập nào đó và với mỗi $S, T \in \mathcal{J}$ ta định nghĩa $S \sim T$ nếu tồn tại ánh xạ một-một từ S lên T. Thì ' $\sim$' là quan hệ tương đương trên $\mathcal{J}$. Hiển nhiên rằng nếu S là tập hữu hạn, thì $[S]$ gồm tất cả các tập con của $\mathcal{J}$ có cùng số phần tử với tập S. Nếu S là tập đếm được thì $[S]$ gồm tất cả các tập con đếm được (của $\mathcal{J}$).

(b) Trên $\mathbb{N} \times \mathbb{N}$ ta định nghĩa

$$(m, n) \sim (j, k) \quad \text{nếu } m^2 + n^2 = j^2 + k^2.$$

Hiển nhiên $\sim$ là quan hệ tương đương. Bằng cách xét ánh xạ

$$f\colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \quad (m, n) \mapsto m^2 + n^2,$$

thì các lớp tương đương chính là các tập con khác trống $f^{-1}(u), u \in \mathbb{N}$.

Định lý 5.4.4. *(a) Giả sử $S \neq \emptyset$ và ánh xạ $f\colon S \longrightarrow T$. Ta định nghĩa $s \sim t$ $(s, t \in S)$ nếu $f(s) = f(t)$. Thì $\sim$ là quan hệ tương đương trên S và các lớp tương đương là các tập khác trống $f^{-1}(u)$, trong đó $u \in T$.*

(b) Mỗi quan hệ tương đương trên S được xác định bởi một ánh xạ f thích hợp như trong phần (a).

Chứng minh. (a) Chúng ta kiểm tra $\sim$ là quan hệ tương đương:

[Phản xạ]. Ta có $f(s) = f(s)$. Vậy $s \sim s$ với mọi $s \in S$.

[Đối xứng]. $f(s_1) = f(s_2) \;\Leftrightarrow\; f(s_2) = f(s_1)$. Vậy quan hệ $s_1 \sim s_2$ suy ra $s_2 \sim s_1$.

[Bắc cầu]. Nếu $f(s_1) = f(s_2)$ và $f(s_2) = f(s_3)$ thì $f(s_1) = f(s_3)$.

(b) Xét ánh xạ tự nhiên

$$f\colon S \longrightarrow [S], \qquad s \mapsto [s].$$

Dễ dàng kiểm tra f thỏa các điều kiện đòi hỏi. □

Bài tập

1. Ký hiệu (R), (S), (AS) và (T) là các tính chất phản xạ, đối xứng, phản đối xứng và bắc cầu. Tìm các ma trận của các quan hệ trên $S := \{0, 1, 2, 3\}$ và kiểm tra các tính chất (R), (S), (AS) và (T), nếu

   (a) mR_1n nếu $m + n = 3$.

   (b) mR_2n nếu $m = n \pmod 2$.

   (c) mR_3n nếu $m \leq n$.

   (d) mR_4n nếu $m + n \leq 4$.

   (e) mR_5n nếu $\max\{m, n\} = 3$.

   Các quan hệ nào là thứ tự bộ phận, quan hệ tương đương?

2. Các quan hệ sau trên $\mathbb{Z}$, quan hệ nào là tương đương, khi đó liệt kê các lớp tương đương.

   (a) $n \equiv m \pmod 4$.
   (b) $mn = 0$.
   (c) $mn > 0$.
   (d) $n \leq m$.

3. Xét quan hệ R trên $\mathbb{Z}$ xác định bởi mRn nếu và chỉ nếu $m^3 - n^3 \equiv 0 \pmod 5$.

   (a) R thoả các tính chất nào trong số (R), (S), (AS), (T).

   (b) R là quan hệ tương đương? thứ tự bộ phận?

4. Đặt $\Sigma := \{a, b, c, d, e, f, g\}$. Viết ma trận tương ứng quan hệ trên Σ xác định bởi phân hoạch $\{\{a, d\}, \{c, e, f\}, \{b, g\}\}$.

5. (a) Cho tập khác trống S. Khảo sát quan hệ trống $\emptyset \subset S \times S$ trên S. Các tính chất nào trong số (R), (S), (AS), (T) mà quan hệ $\emptyset$ thoả?

   (b) Như trên đối với quan hệ $U := S \times S$ trên S.

6. (a) Chứng minh rằng giao của hai quan hệ tương đương là quan hệ tương đương.

   (b) Hợp hai quan hệ tương đương là quan hệ tương đương?

7. Giả sử S là tập các tập con vô hạn của $\mathbb{N}$. Với A, B trong S, xét quan hệ

   $$A \sim B \Leftrightarrow A \cap B \text{ là tập hữu hạn.}$$

   Đây là quan hệ tương đương?

8. Chứng minh rằng quan hệ R trên tập S là quan hệ tương đương, nếu và chỉ nếu thoả mãn ba điều kiện

   (a) $E := \{(x, x) \in S \times S\} \subset R$,

   (b) $R = R^{-1}$,

   (c) $R \circ R \subset R$.

9. Ta nói một họ các tập con khác trống rời nhau của tập S là một phân hoạch của tập S nếu hợp của các tập này bằng S. Chứng minh rằng các lớp tương đương của một quan hệ trên S lập thành phân hoạch của tập S. Ngược lại, giả sử $(A_i|i \in I)$ các tập con của S sao cho $A_i \cap A_j = \emptyset, i \neq j$, và $\cup(A_i|i \in I) = S$. Xét quan hệ $\sim_S$ trên S : $a \sim_S b$ nếu và chỉ nếu tồn tại chỉ số $i \in I$ sao cho $a, b \in A_i$.

   (a) Chứng minh rằng $\sim_S$ là quan hệ tương đương.

   (b) Chứng minh rằng các lớp tương đương của $\sim_S$ là các *khối* A_i của phân hoạch $(A_i|i \in I)$.

10. Giả sử F là tập tất cả các hàm từ $\mathbb{N}$ lên $\mathbb{N}$. Với $f, g \in F$, xét quan hệ $f \sim g$ nếu $f(n) = g(n)$ ngoài một tập con hữu hạn của tập các số tự nhiên $\mathbb{N}$.

    (a) Chứng minh rằng $\sim$ là quan hệ tương đương.

    (b) Ký hiệu lớp tương đương của f bởi $[f]$. Ta nói, $[f] \leq [g]$ nếu $f(n) \leq g(n)$ ngoài một tập con hữu hạn của tập các số tự nhiên $\mathbb{N}$.

    (c) Ký hiệu $[k]$ là lớp tương đương của $f(n) = k$ với mọi $n \in \mathbb{N}$. Chứng minh rằng tồn tại vô hạn các phần tử $[f_1], [f_2], \ldots, [f_m], \ldots$, sao cho

$$[k] \leq [f_1] \leq [f_2] \leq \cdots \leq [f_m] \leq \cdots \leq [k+1].$$

11. Các quan hệ sau, quan hệ nào là quan hệ tương đương?

    (a) $L_1||L_2$, đối với các đường thẳng trong mặt phẳng, nếu L_1 và L_2 là trùng nhau hoặc song song.

    (b) $L_1 \perp L_2$, đối với các đường thẳng trong mặt phẳng, nếu L_1 và L_2 vuông góc.

    (c) $p_1 \sim p_2$, đối với người Việt Nam, nếu p_1 và p_2 sống trong cùng một thành phố.

    (d) $p_1 \sim p_2$, đối với người, nếu p_1 và p_2 có chung cha mẹ.

    (e) $p_1 \sim p_2$, đối với người, nếu p_1 và p_2 có chung mẹ.

12. (a) Liệt kê tất cả các lớp tương đương của $\mathbb{Z}$ đối với quan hệ tương đương đồng dư modulo cho 4.

    (b) Có bao nhiêu lớp tương đương khác nhau của $\mathbb{Z}$ tương ứng với quan hệ tương đương đồng dư modulo cho 73.

13. Giả sử S là tập hợp. Quan hệ $=$ là quan hệ tương đương?

14. Các ma trận A và B trong $\mathrm{Mat}(n, n)$ là *đồng dạng* (similar) nếu tồn tại ma trận khả nghịch P sao cho $B = PAP^{-1}$; khi đó ta ký hiệu $A \approx B$. Chứng minh rằng $\approx$ là quan hệ tương đương trên $\mathrm{Mat}(n, n)$.

15. Giả sử S là tập tất cả các dãy $(s_n) \subset \mathbb{R}$, và định nghĩa $(s_n) \approx (t_n)$ nếu $\{n \in \mathbb{N} \mid s_n \neq t_n\}$ là tập hữu hạn. Chứng minh rằng $\approx$ là quan hệ tương đương trên S.

16. Quan hệ "quen biết" là quan hệ tương đương?

17. Giả sử S là tập hợp và G là nhóm các hàm một-một lên $f\colon S \to S$, tức là,

    (a) hàm đồng nhất 1_S thuộc G;

    (b) nếu $f, g \in G$ thì $f \circ g \in G$;

    (c) nếu $f \in G$ thì $f^{-1} \in G$.

    Với $x, y \in S$, định nghĩa $x \sim y$ nếu tồn tại $f \in G$ sao cho $f(x) = y$. Chứng minh rằng $\sim$ là quan hệ tương đương trên S.

18. Trên $\mathbb{Z}$ xét quan hệ $\approx$ định nghĩa bởi $m \approx n$ nếu $m^2 = n^2$.

    (a) Chứng minh rằng $\approx$ là quan hệ tương đương trên $\mathbb{Z}$.

    (b) Mô tả các lớp tương đương đối với $\approx$. Có bao nhiêu lớp tương đương?

19. Trên $\mathbb{N}$ xét quan hệ $\sim$ định nghĩa bởi $m \sim n$ nếu $m^2 - n^2$ là bội của 3.

    (a) Chứng minh rằng $\sim$ là quan hệ tương đương trên $\mathbb{N}$.

    (b) Liệt kê bốn phần tử trong lớp tương đương [0].

    (c) Liệt kê bốn phần tử trong lớp tương đương [1].

    (d) Có lớp tương đương nào khác?

20. Khảo sát tập $\mathcal{P}(S)$ các tập con của tập S. Với $A, B \in \mathcal{P}(S)$, ký hiệu $A \sim B$ nếu hiệu đối xứng $A \oplus B := (A \setminus B) \cup (B \setminus A)$ là tập hữu hạn. Chứng minh rằng $\sim$ là quan hệ tương đương trên $\mathcal{P}(S)$.

    (a) Mô tả các tập trong lớp tương đương chứa tập trống $\emptyset$.

    (b) Mô tả các tập trong lớp tương đương chứa S.

21. Trên $\mathbb{N} \times \mathbb{N}$ định nghĩa $(m, n) \sim (k, l)$ nếu $m + l = n + k$.

    (a) Chứng minh rằng $\sim$ là quan hệ tương đương trên $\mathbb{N} \times \mathbb{N}$.

    (b) Vẽ một phần của $\mathbb{N} \times \mathbb{N}$ để chỉ ra các lớp tương đương.

22. Định nghĩa $m \equiv n \pmod{p}$ vẫn có nghĩa khi $p = 1$ hoặc $p = 0$.

    (a) Mô tả quan hệ tương đương này đối với $p = 1$ và các lớp tương đương tương ứng trong $\mathbb{Z}$.

    (b) Như trên với $p = 0$.

23. Giả sử P là tập tất cả các chương trình máy tính và hai chương trình p_1 và p_2 là tương đương nếu chúng cho cùng một kết quả với cùng dữ liệu ban đầu. Đây là quan hệ tương đương? Tại sao?

24. Giả sử Σ là bảng chữ cái, và với $x, y \in \Sigma^*$, ký hiệu $x \sim y$ nếu $\text{length}(x) = \text{length}(y)$. Chứng minh rằng $\sim$ là quan hệ tương đương và mô tả các lớp tương đương.

25. Khảo sát $\mathbb{P} \times \mathbb{P}$ và định nghĩa $(m, n) \sim (p, q)$ nếu $mq = np$.

    (a) Chứng minh rằng $\sim$ là quan hệ tương đương trên $\mathbb{P} \times \mathbb{P}$.

    (b) Chứng minh rằng $\sim$ là quan hệ tương đương tương ứng với hàm $\mathbb{P} \times \mathbb{P} \to \mathbb{Q}$ cho bởi $f((m, n)) = m/n$.

26. Có bao nhiêu quan hệ tương đương trên tập $\{0, 1, 2, 3\}$?

27. Trên $\mathbb{Z}$ xét quan hệ $\approx$ định nghĩa bởi $m \approx n$ nếu $m^2 = n^2$.

    (a) Sai (vì sao) nếu định nghĩa $\leq$ trên $[\mathbb{Z}]$ bởi $[m] \leq [n]$ nếu và chỉ nếu $m \leq n$?

    (b) Sai (vì sao) nếu định nghĩa hàm $f : [\mathbb{Z}] \to \mathbb{Z}, f([m]) = m^2 + m + 1$?

    (c) Như trên, với $g([m]) = m^4 + m^2 + 1$.

    (d) Sai (vì sao) nếu định nghĩa trên $\mathbb{Z}$, $[m] \oplus [n] = [m + n]$?

5.5 Bao đóng của quan hệ

Đôi khi chúng ta muốn xây dựng một quan hệ mới từ một quan hệ đã có. Chẳng hạn, ta có hai quan hệ tương đương R_1 và R_2 trên S và chúng ta muốn tìm quan hệ nhỏ nhất chứa cả R_1 và R_2. Quan hệ này có thể không phải là quan hệ tương đương. Điều này xảy ra do $R_1 \cup R_2$ có thể không phải là bắc cầu. Vậy quan hệ bắc cầu nhỏ nhất chứa $R_1 \cup R_2$ là gì? Trong phần này chúng ta sẽ trả lời câu hỏi này.

Giả sử R là quan hệ trên S. Kí hiệu $r(R), s(R)$ và $t(R)$ là các quan hệ phản xạ, đối xứng và bắc cầu nhỏ nhất chứa R. Các quan hệ này được gọi tương ứng là các *bao đóng* phản xạ, đối xứng và bắc cầu của quan hệ R.

Mệnh đề 5.5.1. *(a) $R = r(R)$ nếu và chỉ nếu R phản xạ.*

(b) $R = s(R)$ nếu và chỉ nếu R đối xứng.

(c) $R = t(R)$ nếu và chỉ nếu R bắc cầu.

Hơn nữa

$$r(r(R)) = r(R), \quad s(s(R)) = s(R), \quad t(t(R)) = t(R).$$

Chứng minh. Suy từ định nghĩa. □

Ví dụ 5.5.1. Xét quan hệ R trên $\{1, 2, 3, 4\}$ tương ứng ma trận Boole:

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

(a) Quan hệ R không phản xạ. Ma trận Boole $r(A)$ của quan hệ $r(R)$ nhận được từ ma trận A với tất cả các phần tử trên đường chéo bằng một và đồ thị của $r(R)$ suy từ đồ thị của R bằng cách thêm các khuyên tại các đỉnh:

$$r(A) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

(b) Quan hệ R không đối xứng. Đồ thị của quan hệ $s(R)$ suy từ đồ thị của quan hệ R bằng cách thêm (nếu chưa có) các cung (j, i) nếu tồn tại cung (i, j). Ma trận Boole $s(A)$ có dạng

$$s(A) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

(c) Quan hệ R không bắt cầu. Ma trận Boole $t(A)$ có dạng

$$t(A) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Định lý 5.5.2. *Nếu R và $E := \{(x, x) \mid x \in S\}$ là các quan hệ trên S thì*

(a) $r(R) = R \cup E$.

(b) $s(R) = R \cup R^{-1}$.

(c) $t(R) = \bigcup_{i=1}^{\infty} R^i$.

Chứng minh. (a) Ta biết rằng quan hệ là phản xạ nếu và chỉ nếu nó chứa E. Do đó $R \cup E$ là phản xạ và do mọi quan hệ phản xạ chứa R phải chứa $R \cup E$ nên $r(R) = R \cup E$.

(b) Nhắc lại rằng R_1 là đối xứng nếu và chỉ nếu $R_1^{-1} = R_1$. Nếu $(x, y) \in R \cup R^{-1}$ thì $(y, x) \in R^{-1} \cup R = R \cup R^{-1}$. Do đó $R \cup R^{-1}$ là quan hệ đối xứng.

Xét R_1 là quan hệ đối xứng chứa R. Nếu $(x, y) \in R^{-1}$ thì $(y, x) \in R \subset R_1$, và do R_1 đối xứng nên $(x, y) \in R_1$. Suy ra $R^{-1} \subset R_1$. Vậy $R \cup R^{-1} \subset R_1$.

(c) Đầu tiên ta chứng minh hợp $U := \bigcup_{i=1}^{\infty} R^i$ là bắc cầu. Thật vậy lấy $x, y, z \in S$ sao cho $(x, y) \in U, (y, z) \in U$. Khi đó tồn tại $i, j \in \mathbb{N}$ sao cho $(x, y) \in R^i$ và $(y, z) \in R^j$. Do đó

$$(x, z) \in R^{i+j} \subset U.$$

Vậy U là quan hệ bắc cầu. Bây giờ lấy R_1 là quan hệ bắc cầu chứa R. Ta chứng minh quy nạp theo $k : R^k \subset R_1$.

Với $k = 1$ là hiển nhiên. Giả sử đúng đến k. Ta có

$$R^{k+1} = R^k \circ R \subset R_1 \circ R_1 \subset R_1$$

(bao hàm thức cuối có được do R_1 bắc cầu).

Vậy với mọi $k > 1$ ta có

$$R^k \subset R_1.$$

Hay $U \subset R_1$. □

Ví dụ 5.5.2. (a) Giả sử R là quan hệ trên tập S có n phần tử và A là ma trận Boole của R. Như trong Định lý 5.5.3 dưới đây chỉ ra:

$$t(R) = \bigcup_{i=1}^{n} R^i.$$

Dựa vào các kết quả trước ta có

$$t(A) = A \vee A^2 \vee \ldots \vee A^n, \quad s(A) = A \vee A^t, \quad r(A) = A \vee I_n.$$

Trong đó I_n là ma trận đơn vị cấp n. Từ các ma trận này chúng ta dễ dàng xác định các quan hệ $t(R), s(R)$ và $r(R)$.

(b)Xét quan hệ R trong Ví dụ 5.5.1, dễ dàng kiểm tra lại các đẳng thức trên.

Định lý 5.5.3. *Nếu R là quan hệ trên S có n phần tử, thì*

$$t(R) = \bigcup_{i=1}^{n} R^i.$$

Chứng minh. Chỉ cần chứng minh $t(R) \subset \bigcup_{i=1}^{n} R^i$. Lấy $(x, y) \in t(R)$. Gọi m là số nguyên dương nhỏ nhất sao cho $(x, y) \in R^m$. Chỉ cần xét trường hợp $m > 2$. Khi đó tồn tại dãy các phần tử trong S

$$x_1, x_2, \ldots, x_{m-1}, x_m = y,$$

sao cho

$$xRx_1, x_1Rx_2, \ldots, x_{m-1}Rx_m.$$

Nếu $m > n$ thì tồn tại i, j $(i < j)$ sao cho $x_i = x_j$ thì ta có thể bỏ qua $x_i, x_{i+1}, \ldots, x_{j-1}$ và được một xích ngắn hơn:

$$xRx_1, \ldots, x_{i-1}Rx_j, \ldots, x_{m-1}Ry.$$

Mâu thuẫn vì m nhỏ nhất. □

Chúng ta đã xét các bao đóng trên quan hệ R, bây giờ ta sẽ lấy một quan hệ mới có dạng là tổ hợp của bao đóng.

Ví dụ 5.5.3. Xét R trong Ví dụ 5.5.1. Ma trận Boole của $s(r(R))$ là

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Đó cũng là ma trận Boole $r(s(A))$ của quan hệ $r(s(R))$ và vì vậy $s(r(R)) = r(s(R))$. Hơn nữa quan hệ $trs(R) = tsr(R)$ là quan hệ tương đương với ma trận Boole

$$tsr(A) = trs(A) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Ví dụ 5.5.4. Xét quan hệ R trên $\{1, 2, 3\}$ có ma trận Boole

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Vì $A * A = A$ nên R là bắc cầu. Ma trận tương ứng quan hệ $s(R)$ có dạng

$$s(A) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Dễ thấy rằng quan hệ $s(R)$ không bắc cầu!

Ví dụ này chứng tỏ bao đóng đối xứng của bao đóng bắc cầu chưa chắc là quan hệ bắc cầu. Nói một cách khác các phép lấy bao đóng có thể phá hủy tính phản xạ, đối xứng hay bắc cầu.

Bổ đề 5.5.4. *(a) Nếu R phản xạ thì $s(R)$ và $t(R)$ cũng phản xạ.*

(b) Nếu R đối xứng thì $r(R)$ và $t(R)$ cũng đối xứng.

(c) Nếu R bắc cầu thì $r(R)$ cũng bắc cầu.

Chứng minh. (a) Hiển nhiên vì nếu $E \subseteq R$ thì $E \subseteq s(R)$ và $E \subseteq t(R)$.

(b) Bài tập.

(c) Giả sử R bắc cầu và $(x, y), (y, z) \in r(R) = R \cup E$.

+ Nếu $(x,y) \in E$ thì $x = y$ và do đó $(x,z) = (y,z) \in R \cup E$.

+ Nếu $(y,z) \in E$ thì $y = z$ và do đó $(x,z) = (x,y) \in R \cup E$.

+ Nếu $(x,y) \notin E$ và $(y,z) \notin E$ thì $(x,y), (y,z) \in R$, do đó $(x,z) \in R \subseteq R \cup E$.

Vậy ta luôn luôn có $(x,z) \in R \cup E$. □

Định lý 5.5.5. *Giả sử R là quan hệ trên S thì $tsr(R)$ là quan hệ tương đương nhỏ nhất chứa R.*

Chứng minh. + Từ $r(R)$ phản xạ và Bổ đề 5.5.4(a), suy ra $tsr(R)$ phản xạ.

+ Từ $sr(R)$ đối xứng và Bổ đề 5.5.4(b), suy ra $tsr(R)$ đối xứng.

+ Hiển nhiên $tsr(R)$ bắc cầu.

Vậy $tsr(R)$ là quan hệ tương đương. Lấy R_1 là quan hệ tương đương chứa R. Thì

$$r(R) \subseteq r(R_1) = R_1.$$

Do đó

$$sr(R) \subseteq s(R_1) = R_1.$$

Suy ra

$$tsr(R) \subseteq t(R_1) = R_1.$$

Nói cách khác $tsr(R)$ là quan hệ tương đương nhỏ nhất chứa R. □

Ví dụ 5.5.5. Giả sử R là quan hệ trên $\{1,2,3\}$ trong Ví dụ 5.5.4. Ta có

$$r(A) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad s(r(A)) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad t(s(r(A))) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Vậy $trs(R) = \{1,2,3\} \times \{1,2,3\}$.

Bài tập

1. Xét quan hệ R trên tập $S := \{1,2,3\}$ tương ứng ma trận Boole

$$A := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Tìm các ma trận Boole của $r(R), s(R), rs(R), sr(R)$ và $tsr(R)$.

2. Lặp lại Bài tập 1 với
$$A := \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

3. Với Bài tập 1, liệt kê các lớp tương đương của $tsr(R)$.

4. Với Bài tập 2, liệt kê các lớp tương đương của $tsr(R)$.

5. Lặp lại Bài tập 1 với quan hệ R trên $\{1, 2, 3, 4\}$ tương ứng với ma trận Boole
$$A := \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

6. Với Bài tập 5, liệt kê các lớp tương đương của $tsr(R)$.

7. Giả sử R là quan hệ "tựa thứ tự" trên tập các số nguyên dương $\mathbb{P}$: mRn nếu $m < n$. Tìm hoặc mô tả $r(R), sr(R), rs(R), tsr(R), t(R)$ và $st(R)$.

8. Lặp lại Bài tập 7 với mRn nếu m là ước của n.

9. (a) Chứng minh rằng nếu (R_k) là một dãy các quan hệ đối xứng trên S thì hợp $\cup_{k=1}^{\infty} R_k$ là đối xứng.

   (b) Giả sử R là quan hệ đối xứng trên S. Chứng minh rằng $R^n, n \in \mathbb{P}$, là quan hệ đối xứng.

   (c) Chứng minh rằng nếu R là quan hệ đối xứng trên S thì $r(R), t(R)$ là các quan hệ đối xứng trên S.

10. Xét quan hệ R trên tập S.

    (a) Chứng minh rằng $sr(R) = rs(R)$.

    (b) Chứng minh rằng $tr(R) = rt(R)$.

11. Bằng phản ví dụ, chứng minh rằng $st(R) \neq ts(R)$.

12. Giả sử R là quan hệ trên $S := \{1, 2\}$ tương ứng ma trận Boole $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$. Chứng minh rằng không tồn tại quan hệ R' nhỏ nhất chứa R sao cho $sR's$ sai với mọi $s \in S$.

13. Ta nói quan hệ R trên S là *quan hệ lên* nếu với mọi $y \in S$ tồn tại $x \in S$ sao cho $(x, y) \in R$. Chứng minh rằng không tồn tại một quan hệ lên nhỏ nhất chứa quan hệ R trên $\{1, 2\}$ được xác định trong Bài tập 12.

14. Giả sử tính chất p của quan hệ trên tập khác trống S thoả mãn

    (i) *Quan hệ phổ dụng* $U := S \times S$ có tính chất p;

    (ii) p *đóng đối với phép giao*, tức là, nếu $\{R_i \mid i \in I\}$ là một họ các quan hệ trên S có tính chất p thì giao $\cap_{i\in I} R_i$ cũng có tính chất p.

    (a) Chứng minh rằng với mọi quan hệ R trên S tồn tại một quan hệ nhỏ nhất chứa R và có tính chất p.

    (b) Nhận xét rằng các tính chất phản xạ, đối xứng và bắc cầu thoả mãn cả hai tính chất (i) và (ii).

    (c) Tính chất *quan hệ lên* trong Bài tập 13 không thoả tính chất nào trong số (i), (ii)?

5.6 Lattice của các phân hoạch

Nhận xét rằng họ $\mathcal{C} = \mathcal{P}(S \times S)$ tất cả các quan hệ tương đương trên S là tập được sắp thứ tự với quan hệ bao hàm. Phần tử nhỏ nhất là quan hệ đồng nhất E và phần tử lớn nhất là quan hệ phổ dụng U vì $E \subset R \subset U$ với mọi quan hệ R trên S. Họ $\mathcal{C}$ là lattice với hai phép toán

$$R_1 \vee R_2 := tsr(R_1 \cup R_2), \qquad R_1 \wedge R_2 := R_1 \cap R_2.$$

Chú ý rằng $tsr(R_1 \cup R_2) = t(R_1 \cup R_2)$ vì $R_1 \cup R_2$ là quan hệ có tính phản xạ và đối xứng.

Ví dụ 5.6.1. Xét hộp S chứa các viên bi và hai quan hệ tương đương:

- $(s,t) \in R_1$ nếu s và t có cùng màu;
- $(s,t) \in R_2$ nếu s và t có cùng kích thước.

Khi đó $(s,t) \in R_1 \wedge R_2$ nếu và chỉ nếu s và t có cùng màu và cùng kích thước. Cặp (s,t) thuộc $R_1 \vee R_2$ nếu tồn tại dãy các viên bi $t_1, t_2, \ldots, t_{m-1} \in S$ sao cho

$$(s,t_1), (t_1,t_2), \ldots, (t_{m-1},t) \in R_1 \cup R_2.$$

Ví dụ 5.6.2. Trên tập các số nguyên dương $\mathbb{P}$ xét các quan hệ tương đương R_6 và R_8 trong đó $(m,n) \in R_6$ nếu $m = n \pmod 6$ và $(m,n) \in R_8$ nếu $m = n \pmod 8$.

(a) Nếu $(m,n) \in R_6 \wedge R_8$ thì $m-n$ là bội số của 6 và 8, tức là $m-n$ là bội số của 24. Do đó $(m,n) \in R_6 \wedge R_8$ nếu và chỉ nếu $m = n \pmod{24}$.

(b) Ta sẽ chứng minh $R_6 \vee R_8 = R_2$ trong đó $(m,n) \in R_2$ nếu và chỉ nếu $m = n \pmod 2$. Chú ý rằng 2 là ước số chung lớn nhất của 6 và 8. Dễ dàng thấy rằng $R_6 \cup R_8 \subset R_2$ và do R_2 là quan hệ tương đương nên $R_6 \vee R_8 \subset R_2$. Ta cần chỉ ra

$$R_2 \subset R_6 \vee R_8 = t(R_6 \cup R_8) \subset R_2.$$

Nhận xét là

$$(k, k+2) \in R_6 \vee R_8 \tag{5.1}$$

với mọi $k \in \mathbb{P}$ vì cả hai $(k, k+8)$ và $(k+8, k+2)$ thuộc $R_6 \cup R_8$. Giả sử $(m, n) \in R_2, m < n$. Ta có thể viết $n = m + 2r$ với $r \in \mathbb{P}$ nào đó. Từ (5.1) suy ra tất cả các cặp

$$(m, m+2), (m+2, m+4), \ldots, (m+2r-2, m+2r)$$

thuộc $R_6 \vee R_8$. Do đó theo tính bắc cầu, $(m, m+2r) = (m, n)$ cũng thuộc $R_6 \vee R_8$, suy ra điều cần chứng minh.

Ta biết rằng, có một tương ứng giữa các quan hệ tương đương trên S và tập $\Pi(S)$ tất cả các phân hoạch của S. Mặt khác tập các quan hệ tương đương tạo thành lattice. Vì vậy tồn tại cấu trúc lattice trên $\Pi(S)$.

Thật vậy, xét các quan hệ tương đương R_1 và R_2 tương ứng các phân hoạch π_1 và π_2. Khi đó $R_1 \subset R_2$ nếu và chỉ nếu $(s, t) \in R_1$ thì $(s, t) \in R_2$. Nói cách khác, $R_1 \subset R_2$ nếu và chỉ nếu mỗi tập trong π_1 là tập con nào đó trong π_2; trong trường hợp này ta nói π_1 *mịn hơn* π_2 và ký hiệu $\pi_1 \leq \pi_2$. Ta có $\leq$ là quan hệ thứ tự trên $\Pi(S)$ và $\Pi(S)$ là lattice với các phép toán $\pi_1 \wedge \pi_2$ và $\pi_1 \vee \pi_2$ tương ứng các quan hệ $R_1 \cap R_2$ và $R_1 \vee R_2$. Phân hoạch $\pi_1 \wedge \pi_2$ dễ dàng tìm: gồm tất cả các tập con khác trống nhận được bằng cách giao một tập trong π_1 với một tập trong π_2. Việc xác định $\pi_1 \vee \pi_2$ khó hơn.

Ví dụ 5.6.3. (a) Xét hộp đựng các viên bi trong Ví dụ 5.6.1, mỗi tập trong phân hoạch $\pi_1 \wedge \pi_2$ gồm tất cả các viên bi có cùng màu và cùng kích thước. Phân hoạch $\pi_1 \vee \pi_2$ phụ thuộc vào các viên bi trong S và mối quan hệ giữa chúng (xem các Bài tập từ 1 đến 4).

(b) Phân hoạch $\pi_6 \wedge \pi_8$ của $\mathbb{P}$ tương ứng $R_6 \wedge R_8$ trong Ví dụ 5.6.2 gồm các lớp tương đương được xác định theo quan hệ $m = n \pmod{24}$ (có 24 lớp).

Trong trường hợp này, phân hoạch $\pi_1 \vee \pi_2$ tương ứng quan hệ tương đương $R_6 \vee R_8 = R_2$ và do đó có hai lớp tương đương là $[0]$ và $[1]$.

Phần cuối trình bày thuật toán xác định các phân hoạch $\pi_1 \vee \pi_2$ và $\pi_1 \wedge \pi_2$ khi S hữu hạn. Giả sử $S := \{1, 2, \ldots, n\}$ và π là phân hoạch của S. Với mỗi $A \in \pi$, chọn một phần tử $m_A \in A$ và định nghĩa $\alpha(k) := m_A$, với mọi $k \in A$ (chẳng hạn m_A là số nhỏ nhất của A). Mỗi phần tử của S thuộc một tập A nào đó, bởi vậy ta có hàm $\alpha \colon S \to S$ thoả mãn

(i) $\alpha(j) = \alpha(k)$ nếu và chỉ nếu j, k thuộc cùng một tập của phân hoạch π;

(ii) $\alpha(\alpha(k)) = \alpha(k)$, với mọi k.

Với mỗi $k \in S$, tập $A \in \pi$ sao cho $k \in A$ thì $\alpha(k) \in A$. Vậy $A = \alpha^{-1}(\alpha(k))$. Do đó π được xác định bởi α. Như vậy, để xác định $\pi_1 \vee \pi_2$ và $\pi_1 \wedge \pi_2$, ta cần tìm các hàm tương ứng thoả (i) và (ii). Nếu R là quan hệ tương đương tương ứng với phân hoạch π thì tính chất (i) suy ra

(i') $\alpha(j) = \alpha(k)$ nếu và chỉ nếu jRk.

Ví dụ 5.6.4. Giả sử R là quan hệ tương đương trên $S := \{1, 2, \ldots, 10\}$ mà phân hoạch π của nó là

$$\{\{1, 4, 6\}, \{2\}, \{3, 7, 10\}, \{5, 9\}, \{8\}\}.$$

Hàm α chọn số nhỏ nhất trong mỗi lớp là

k	1	2	3	4	5	6	7	8	9	10
$\alpha(k)$	1	2	3	1	5	1	3	8	5	3

Chú ý rằng α thoả (i) và (ii). Cũng có thể chọn hàm

k	1	2	3	4	5	6	7	8	9	10
$\alpha(k)$	4	2	3	4	9	4	3	8	9	3

Với hai phân hoạch π_1, π_2 của tập $S := \{1, 2, \ldots, n\}$, giả sử α, β là hai hàm thoả mãn (i) và (ii). Chú ý rằng, π_1 mịn hơn π_2 nếu

$$\alpha(i) = \alpha(j) \text{ suy ra } \beta(i) = \beta(j), \text{ với mọi } i, j \in S.$$

Bây giờ ta trình bày thuật toán tìm hàm γ tương ứng với $\pi_1 \wedge \pi_2$. Thuật toán duyệt mỗi phần tử của S một lần. Khi gặp phần tử s trong một khối mới của phân hoạch $\pi_1 \wedge \pi_2$ ta gán nhãn γ của khối này là s.

5.6.1 Thuật toán xác định hội của hai phân hoạch

Bước 1. Đặt $\gamma(k) = 0, k = 1, 2, \ldots, n$.

Bước 2. Chọn $k = 1$.

Bước 3. Nếu $\gamma(k) \neq 0$ thì chuyển sang Bước 4; ngược lại, với mỗi $j = k, k+1, \ldots, n$ thoả $\alpha(j) = \alpha(k)$ và $\beta(j) = \beta(k)$, đặt $\gamma(j) = k$.

Bước 4. Nếu $k = n$, dừng; ngược lại, $k := k + 1$ và chuyển sang Bước 3.

Ví dụ 5.6.5. Giả sử π_1 và π_2 là các phân hoạch của $S := \{1, 2, \ldots, 8\}$ tương ứng các hàm α và β :

k	1	2	3	4	5	6	7	8
$\alpha(k)$	3	2	3	2	3	7	7	2
$\beta(k)$	5	4	4	4	5	5	5	4

Ta có $\pi_1 = \{\{1, 3, 5\}, \{2, 4, 8\}, \{6, 7\}\}$; π_2 gồm hai tập. Bảng 5.1 minh họa thuật toán chạy từng bước. Phân hoạch $\pi_1 \wedge \pi_2$ tương ứng hàng cuối trong bảng và do đó có bốn tập.

Thuật toán kế tiếp tìm hàm γ tương ứng với $\pi_1 \vee \pi_2$.

k	$\gamma(1)$	$\gamma(2)$	$\gamma(3)$	$\gamma(4)$	$\gamma(5)$	$\gamma(6)$	$\gamma(7)$	$\gamma(8)$
0	0	0	0	0	0	0	0	0
1	1	0	0	0	1	0	0	0
2	1	2	0	2	1	0	0	2
3	1	2	3	2	1	0	0	2
4	1	2	3	2	1	0	0	2
5	1	2	3	2	1	0	0	2
6	1	2	3	2	1	6	6	2
7	1	2	3	2	1	6	6	2
8	1	2	3	2	1	6	6	2

Bảng 5.1:

k	$\gamma(1)$	$\gamma(2)$	$\gamma(3)$	$\gamma(4)$	$\gamma(5)$	$\gamma(6)$	$\gamma(7)$	$\gamma(8)$	
0	1	2	5	4	5	1	7	4	[hàm α]
1	5	2	5	4	5	5	7	4	
2, 3, 4, 5, 6	5	4	5	4	5	5	7	4	
7, 8	5	4	5	4	5	5	5	4	

Bảng 5.2:

5.6.2 Thuật toán xác định tuyến của hai phân hoạch

Bước 1. Đặt $\gamma(k) = \alpha(k), k = 1, 2, \ldots, n$.

Bước 2. Với $k = 1, \ldots, n$ nếu $\gamma(k) \neq \gamma(\beta(k))$ thì tìm tất cả j với $\gamma(j) = \gamma(k)$ thay $\gamma(j)$ bằng $\gamma(\beta(k))$ với mọi j như thế.

Ví dụ 5.6.6. Giả sử π_1 và π_2 là các phân hoạch của $S := \{1, 2, \ldots, 8\}$ tương ứng các hàm α và β :

k	1	2	3	4	5	6	7	8
$\alpha(k)$	1	2	5	4	5	1	7	4
$\beta(k)$	3	4	3	4	5	6	6	8

Mỗi phân hoạch π_1 và π_2 có năm tập. Bảng 5.2 minh họa thuật toán chạy từng bước. Phân hoạch $\pi_1 \vee \pi_2$ tương ứng hàng cuối trong bảng và do đó có hai tập.

Bài tập

1. Giả sử một hộp đựng 10 viên bi, trong đó 6 viên nhỏ màu xanh, 3 viên lớn màu đỏ và 1 viên lớn màu xanh. Mô tả $\pi_1 \vee \pi_2$ và $\pi_1 \wedge \pi_2$. Có bao nhiêu tập trong mỗi phân hoạch này?

2. Câu trả lời của bạn như thế nào đối với Bài tập 1, nếu viên bi lớn màu xanh biến mất?

3. Lặp lại Bài tập 1, nếu hộp bi có 10 viên, trong đó 4 viên nhỏ màu vàng, 3 viên vừa màu xanh, 2 viên vừa màu trắng và 1 viên lớn màu vàng.

4. Câu trả lời của bạn như thế nào đối với Bài tập 3, nếu một viên bi lớn màu xanh rơi vào hộp?

5. Khảo sát các quan hệ tương đương R_3, R_5 trên $\mathbb{P}$, trong đó $(m,n) \in R_3$ nếu $m \equiv n \pmod 3$ và $(m,n) \in R_5$ nếu $m \equiv n \pmod 5$ tương ứng với các phân hoạch π_3, π_5.

   (a) Mô tả quan hệ tương đương $R_3 \wedge R_5$.

   (b) Mô tả phân hoạch $\pi_3 \wedge \pi_5$.

   (c) Suy ra rằng, $R_3 \vee R_5$ là quan hệ phổ dụng trên $\mathbb{P}$. Kiểm tra lại

   $$(1,2), (1,30), (1,73), (47,73), (72,73) \in R_3 \vee R_5.$$

   (d) Mô tả quan hệ phân hoạch $\pi_3 \vee \pi_5$.

6. Với mỗi phân hoạch dưới đây của $S := \{1, 2, \ldots, 6\}$ tìm hàm α thoả mãn các tính chất (i) và (ii):

   (a) $\pi_1 = \{\{1,3,5\}, \{2,6\}, \{4\}\}$.

   (b) $\pi_2 = \{\{1,2,4\}, \{3,6\}, \{5\}\}$.

   (c) $\pi_3 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\}$.

   (d) $\pi_4 = \{\{1,2,3,4,5,6\}\}$.

   (e) Quan hệ tương đương nào tương ứng với π_3, π_4?

7. Tìm các phân hoạch $\pi_1, \pi_2, \pi_3, \pi_4$ của $\{1, 2, \ldots, 8\}$ được xác định bởi các hàm $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ sau

k	1	2	3	4	5	6	7	8
$\alpha_1(k)$	1	1	3	1	5	6	3	5
$\alpha_2(k)$	2	2	6	8	5	6	7	8
$\alpha_3(k)$	4	4	3	4	5	3	3	4
$\alpha_4(k)$	3	2	3	8	2	3	7	8

8. Tìm các hàm tương ứng với phân hoạch $\pi_1 \vee \pi_2$ và $\pi_1 \wedge \pi_2$ trong Bài tập 7.

9. Như Bài tập 8 cho π_3 và π_4.

10. Như Bài tập 8 cho π_2 và π_3.

11. Thuật toán trộn các phân hoạch vẫn chạy đúng nếu hoán đổi vai trò của α và β?

12. (a) Chứng minh quan hệ $\leq$ xác định trên $\Pi(S)$ bởi "$\pi_1 \leq \pi_2$ nếu và chỉ nếu π_1 mịn hơn π_2" là thứ tự bộ phận trên $\Pi(S)$.

    (b) Chứng minh rằng nếu $\pi_1, \pi_2, \pi_3 \in \Pi(S)$ và nếu $\pi_3 \leq \pi_1, \pi_3 \leq \pi_2$ thì $\pi_3 \leq \pi_1 \wedge \pi_2$.

13. Phân tích thuật toán tìm giao và trộn các phân hoạch trong trường hợp π_1 mịn hơn π_2 qua ví dụ $S := \{1, 2, 3, 4, 5, 6, 7\}$ và

k	1	2	3	4	5	6	7
$\alpha(k)$	1	4	3	4	1	6	7
$\beta(k)$	5	4	5	4	5	4	7

14. Kiểm tra tính đúng đắn của thuật toán giao các phân hoạch bằng cách chỉ ra rằng

    (a) Giá trị $\gamma(j)$ thay đổi ít nhất một lần với mỗi j trong suốt quá trình thực hiện thuật toán;

    (b) Nếu giá trị $\gamma(j)$ thay đổi khi $k \leq k_0$ và nếu $\alpha(k') = \alpha(j)$ và $\beta(k') = \beta(j)$ thì $\gamma(k')$ thay bằng k_0;

    (c) Giá trị $\gamma(j)$ thay đổi đúng một lần với mỗi j trong suốt quá trình thực hiện thuật toán;

    (d) Nêu $0 \neq \gamma(a) = \gamma(j)$ thì $\alpha(a) = \alpha(j)$ và $\beta(a) = \beta(j)$;

    (e) Nếu $\alpha(a) = \alpha(j)$ và $\beta(a) = \beta(j)$ thì $\gamma(a) = \gamma(j)$ vào lúc kết thúc thuật toán.

Chương 6

ĐẠI SỐ BOOLE

Để tưởng nhớ nhà toán học G. Boole, một vài khái niệm được mang tên ông: đại số Boole, hàm Boole, biểu thức Boole và vành Boole. G. Boole là một trong những nhà toán học quan tâm đến việc hình thức hoá và cơ chế hoá tư duy logic (xem *The law of thought* của ông xuất bản năm 1854). G. Boole có nhiều đóng góp trong việc phát triển lý thuyết logic sử dụng các ký hiệu thay cho các từ.

Một thế kỷ sau, nhiều nhà toán học (đặc biệt C. E. Shannon) đã nhận ra rằng đại số Boole có thể sử dụng để phân tích các mạnh điện tử. Do đó đại số Boole trở thành một công cụ không thể thiếu được trong việc phân tích và thiết kế các máy tính điện tử, chẳng hạn trong việc thiết kế các mạch điện tử với số linh kiện ít nhất.

6.1 Lattice

Định nghĩa 6.1.1. Giả sử L là tập khác rỗng và $\vee, \wedge$ là các phép toán hai ngôi trên L. Bộ $(L, \vee, \wedge)$ được gọi là *lattice đại số* nếu với mọi $x, y, z \in L$ các tiên đề sau thỏa mãn

1L. Tính giao hoán.

(a) $x \vee y = y \vee x$;

(b) $x \wedge y = y \wedge x$.

2L. Tính kết hợp

(a) $(x \vee y) \vee z = x \vee (y \vee z)$;

(b) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$.

3L. Tính hấp thụ của các phép toán:

(a) $x \vee (x \wedge y) = x$;

(b) $x \wedge (x \vee y) = x$.

- $x \vee y$ đọc là x *tuyển* y hoặc *tổng* của x và y.
- $x \wedge y$ đọc là x *hội* y hoặc *tích* của x và y.

Nhận xét 7. (a) (1La)-(3La) đối ngẫu với (1Lb)-(3Lb) theo nghĩa nếu ta hoán vị vai trò của hai phép toán $\vee, \wedge$ trong (1La)-(3La) thì ta sẽ được (1Lb)-(3Lb) và ngược lại.

(b) Do tính kết hợp của các phép toán $\vee, \wedge$ ta có thể viết

$$x \vee y \vee z \quad \text{và} \quad x \wedge y \wedge z.$$

Tổng quát, có thể viết cho trường hợp n phần tử

$$x_1 \vee x_2 \vee \ldots \vee x_n \quad \text{và} \quad x_1 \wedge x_2 \wedge \ldots \wedge x_n.$$

Tính chất 6.1.2. *Nếu $(L, \vee, \wedge)$ là lattice đại số thì*

(a) $x \vee x = x$.

(b) $x \wedge x = x$.

(c) $x \vee y = y$ *nếu và chỉ nếu* $x \wedge y = x$.

Chứng minh. (a) Đặt $y := x \vee x$. Khi đó

$$\begin{array}{rcll} x & = & x \vee (x \wedge y) & \text{(theo 3La)} \\ & = & x \vee [x \wedge (x \vee x)] & \\ & = & x \vee x & \text{(theo 3Lb).} \end{array}$$

(b) Sử dụng tính chất đối ngẫu.

(c) Giả sử rằng $x \vee y = y$. Ta có

$$\begin{array}{ll} x = x \wedge (x \vee y) & \text{(theo 3Lb)} \\ \quad = x \wedge y & \text{(theo giả thiết).} \end{array}$$

Ngược lại: bài tập. □

Định lý 6.1.3. *Giả sử $(L, \leq)$ là lattice. Đặt*

$$x \vee y := \sup(x, y),$$
$$x \wedge y := \inf(x, y).$$

Khi đó $(L, \vee, \wedge)$ là lattice đại số.

Chứng minh. Ta kiểm tra $(L, \vee, \wedge)$ thỏa mãn các tiên đề của lattice đại số.

+ (1L). Hiển nhiên.

+ (2La). Lấy $x, y, z \in L$. Đặt

$$\begin{cases} u := (x \vee y) \vee z, \\ v := x \vee (y \vee z). \end{cases}$$

Vì

$$y \leq x \vee y \leq u, \qquad z \leq u.$$

Suy ra u là một cận trên của y, z. Nhưng $y \vee z$ là cận trên nhỏ nhất của y và z nên

$$y \vee z \leq u.$$

Mặt khác

$$x \leq x \vee y \leq u.$$

Nên u là cận trên của x và $y \vee z$. Vậy

$$x \vee (y \vee z) \leq u.$$

Tức là $v \leq u$.

Chứng minh tương tự ta cũng có $u \leq v$. Vậy $u = v$.

+ (2Lb). Tương tự như chứng minh (2La).

+ (3La). Lấy $x, y \in L$. Vì $x \leq x \vee w$ với w tùy ý. Đặc biệt, với $w := x \wedge y$, ta có

$$x \leq x \vee (x \wedge y).$$

Vì $x \leq x$ và $x \wedge y \leq x$ nên x là cận trên của x và $x \wedge y$. Do đó

$$x \vee (x \wedge y) \leq x.$$

Vậy

$$x \vee (x \wedge y) = x.$$

+ (3Lb). Tương tự như chứng minh (3La). □

Định lý 6.1.3 chỉ ra rằng lattice đại số $(L, \vee, \wedge)$ cảm sinh từ lattice $(L, \leq)$. Định lý sau cho chúng ta khẳng định ngược lại.

Định lý 6.1.4. *Giả sử $(L, \vee, \wedge)$ là một lattice đại số. Ký hiệu*

$$x \leq y \Leftrightarrow x \vee y = y,$$

với mọi $x, y \in L$. Khi đó $\leq$ là quan hệ thứ tự trên L và $(L, \leq)$ là lattice thỏa

$$x \vee y = \sup(x, y), \quad x \wedge y = \inf(x, y).$$

Chứng minh. • Ta chứng minh $\leq$ là quan hệ thứ tự trên L.

+ Tính phản xạ: vì $x \vee x = x$ nên $x \leq x$.

+ Tính phản đối xứng: giả sử $x \leq y$ và $y \leq x$, tức là

$$x \vee y = y \quad \text{và} \quad y \vee x = x.$$

Do phép toán $\vee$ giao hoán, nên $x = y$.

+ Tính bắc cầu: giả sử $x \leq y$ và $y \leq z$, tức là

$$x \vee y = y \quad \text{và} \quad y \vee z = z.$$

Suy ra

$$\begin{aligned} x \vee z &= x \vee (y \vee z) \\ &= (x \vee y) \vee z \\ &= y \vee z \\ &= z. \end{aligned}$$

• Chứng minh $x \vee y = \sup(x, y)$. Vì

$$\begin{aligned} x \vee (x \vee y) &= (x \vee x) \vee y \\ &= x \vee y. \end{aligned}$$

Nên

$$x \leq x \vee y.$$

Tương tự, ta có

$$y \leq x \vee y.$$

Vậy $x \vee y$ là một cận trên của x và y.

Giả sử u là một cận trên của x và y. Khi đó

$$x \leq u \quad \text{và} \quad y \leq u.$$

Hay

$$x \vee u = u \quad \text{và} \quad y \vee u = u.$$

Vì vậy

$$\begin{aligned} (x \vee y) \vee u &= x \vee (y \vee u) \\ &= x \vee u \\ &= u. \end{aligned}$$

Suy ra

$$x \vee y \leq u.$$

Do đó

$$x \vee y = \sup(x, y).$$

• Chứng minh tương tự cho $x \wedge y = \inf(x, y)$. $\square$

Nhận xét 8. (a) Từ Tính chất 6.1.2, chúng ta có thể định nghĩa

$$x \leq y \Leftrightarrow x \wedge y = x, \text{ với mọi } x, y \in L.$$

(b) Hai Định lý 6.1.3 và 6.1.4 cho ta mối quan hệ giữa lattice đại số và lattice. Hơn nữa, nếu cho lattice $(L, \leq)$ thì quan hệ thứ tự bộ phận cảm sinh bởi lattice đại số $(L, \vee, \wedge)$ trùng với quan hệ thứ tự $\leq$ ban đầu; ngược lại nếu cho lattice đại số $(L, \vee, \wedge)$ thì các phép toán hai ngôi cảm sinh bởi lattice $(L, \leq)$ trùng với các phép toán $\vee, \wedge$ ban đầu.

Ví dụ 6.1.1. Cho S là tập bất kỳ. Với các phép toán hợp và giao, $(\mathcal{P}(S), \cup, \cap)$ là một lattice đại số. Theo Định lý 6.1.4, với mỗi tập A, B trong $\mathcal{P}(S)$, ta định nghĩa $A \leq B$ nếu và chỉ nếu $A \cup B = B$. Thì $(\mathcal{P}(S), \leq)$ là tập được sắp thứ tự bộ phận và

$$\begin{cases} \sup(A, B) = A \cup B, \\ \inf(A, B) = A \cap B. \end{cases}$$

Ví dụ 6.1.2. Giả sử L là tập hợp các mệnh đề. Trên L ta xét quan hệ " $\equiv$ " được định nghĩa như sau: $p \equiv q$ nếu và chỉ nếu "$p \Leftrightarrow q$" là một mệnh đề logic. Khi đó " $\equiv$ " là quan hệ tương đương trên L. Gọi Σ là tập hợp các lớp tương đương trên L xác định bởi " $\equiv$ ". Tức là

$$\Sigma := \{[p] \mid p \in L\}.$$

Đặt

$$[p] \vee [q] := [p \text{ or } q], \qquad [p] \wedge [q] := [p \text{ and } q].$$

Khi đó $(\Sigma, \vee, \wedge)$ là một lattice đại số. Ký hiệu $[p] \leq [q]$ nếu và chỉ nếu $[p] \vee [q] = [q]$. Ta có $(\Sigma, \leq)$ là tập được sắp thứ tự và

$$\sup([p], [q]) = [p] \vee [q], \qquad \inf([p], [q]) = [p] \wedge [q].$$

Ví dụ 6.1.3. Ký hiệu $\text{Fun}(\mathbb{R}, \mathbb{R})$ là tập tất cả các hàm số thực xác định trên $\mathbb{R}$. Trên $\text{Fun}(\mathbb{R}, \mathbb{R})$ ta xét quan hệ "$\leq$" được định nghĩa như sau: $f \leq g, f, g \in \text{Fun}(\mathbb{R}, \mathbb{R})$, nếu và chỉ nếu $f(x) \leq g(x)$ với mọi $x \in \mathbb{R}$.

Khi đó "$\leq$" là quan hệ thứ tự trên $\text{Fun}(\mathbb{R}, \mathbb{R})$. Dễ thấy rằng $\sup(f, g)$ và $\inf(f, g)$ tồn tại với mọi $f, g \in \text{Fun}(\mathbb{R}, \mathbb{R})$. Với mọi $x \in \mathbb{R}$, đặt

$$(f \vee g)(x) := \max(f(x), g(x)),$$
$$(f \wedge g)(x) := \min(f(x), g(x)).$$

Khi đó $(\text{Fun}(\mathbb{R}, \mathbb{R}), \vee, \wedge)$ là lattice đại số và

$$f \vee g = \sup(f, g), \quad f \wedge g = \inf(f, g).$$

Định nghĩa 6.1.5. Cho lattice đại số $(L, \vee, \wedge)$ tương ứng với tập được sắp thứ tự $(L, \leq)$.

(a) Phần tử trong L, kí hiệu 1, thỏa mãn

$$x \leq 1 \text{ với mọi } x \in L, \tag{6.1}$$

gọi là *phần tử lớn nhất.*

(b) Phần tử trong L, ký hiệu 0, thỏa mãn

$$0 \leq x \text{ với mọi } x \in L, \tag{6.2}$$

gọi là *phần tử nhỏ nhất.*

(c) Nếu tồn tại phần tử nhỏ nhất, thì các phần tử phủ 0 gọi là các *nguyên tử* (atom).

(d) Phần tử x trong lattice đại số được gọi là *bất khả quy* (hay *tối giản*) đối với phép tuyển nếu $x = y \vee z$ thì hoặc $x = y$ hoặc $x = z$.

Hiển nhiên (6.1) tương đương với

$$x \vee 1 = 1 \text{ và } x \wedge 1 = x.$$

Và (6.2) tương đương với

$$0 \vee x = x \text{ và } 0 \wedge x = 0.$$

Nhận xét 9. (a) Trong lattice, các phần tử nhỏ nhất và lớn nhất có thể tồn tại hoặc không tồn tại. Trong trường hợp tồn tại thì chúng duy nhất.

(b) Các nguyên tử là bất khả quy. Hơn nữa ta có

Định lý 6.1.6. *Trong lattice đại số hữu hạn phần tử, mọi phần tử có thể biểu diễn ở dạng tuyển các phần tử bất khả quy.*

Chứng minh. Bài tập! □

Ví dụ 6.1.4. (a) Lattice đại số cho trong Ví dụ 6.1.1 có

+ tập trống là phần tử nhỏ nhất;

+ S là phần tử lớn nhất;

+ $\{x\}, x \in S$, là các nguyên tử.

(b) Giả sử S là tập bất kỳ khác trống. Xét lattice $\mathrm{Fun}(S, \mathbb{B})$. Theo Ví dụ 6.1.3.

$$(f \vee g)(x) = \max(f(x), g(x)),$$
$$(f \wedge g)(x) = \min(f(x), g(x)),$$

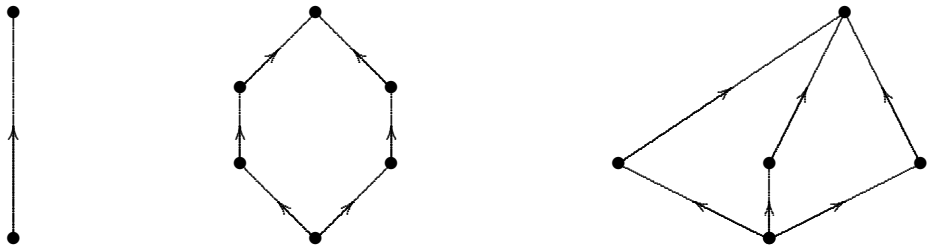
với mọi $x \in S$. Nên

$$(f \vee g)(x) = \begin{cases} 1 & \text{nếu } f(x) = 1 \text{ hoặc } g(x) = 1, \\ 0 & \text{nếu ngược lại,} \end{cases}$$

$$(f \wedge g)(x) = \begin{cases} 1 & \text{nếu } f(x) = g(x) = 1, \\ 0 & \text{nếu ngược lại.} \end{cases}$$

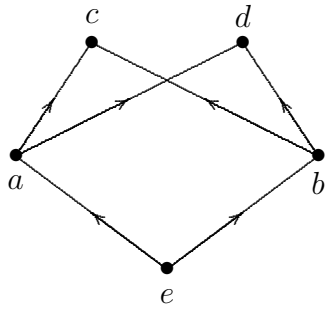
Các nguyên tử trong $\mathrm{Fun}(S, \mathbb{B})$ là các hàm đặc trưng $1_{\{x\}}, x \in S$.

Ví dụ 6.1.5. Các lược đồ Hasse trong Hình 6.1 tương ứng các lattice đại số.



Hình 6.1:

Lược đồ Hasse trong Hình 6.2 không tượng trưng cho một lattice nào vì hai phần tử a, b không có cận trên nhỏ nhất, mặc dù chúng có cận dưới lớn nhất là e :



Hình 6.2:

Định nghĩa 6.1.7. Giả sử $(L, \vee, \wedge)$ là lattice đại số. Tập con M khác rỗng của L được gọi là *lattice con* (sublattice) của L nếu với mọi $x, y \in M$, ta có

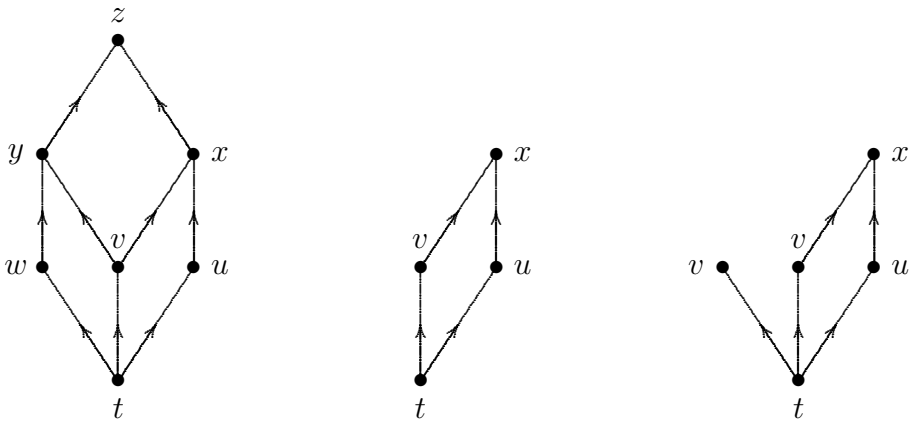
$$x \vee y \in M, \qquad x \wedge y \in M.$$

Tức là M đóng đối với các phép toán tuyển và hội.

Ví dụ 6.1.6. Xét lattice đại số $(L, \vee, \wedge)$ có lược đồ Hasse trong Hình 6.3(a). Ta có M_1 trong Hình 6.3(b) là lattice con của L; còn M_2 trong Hình 6.3(c) không phải là lattice con của L.

Bài tập

1. Viết dưới dạng đối ngẫu các phương trình sau (mà không phải lúc nào cũng đúng):
   (a) $x \vee (y \wedge z) = (x \vee y) \wedge z$.
   (b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.



(a) (b) (c)

Hình 6.3:

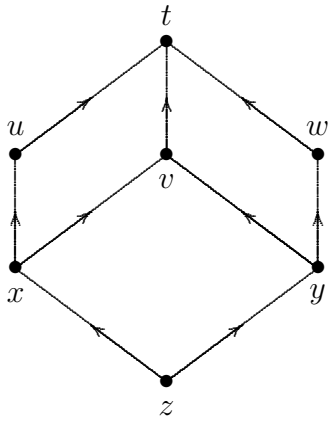
2. Giả sử L là lattice đại số với phần tử lớn nhất 1 và phần tử nhỏ nhất 0.

   (a) 1 là bất khả quy? Giải thích.

   (b) 0 là bất khả quy? Giải thích.

3. Xét lattice hữu hạn $(P, \leq)$ và lược đồ Hasse của nó. Giải thích tại sao một phần tử là bất khả quy nếu và chỉ nếu nó phủ nhiều nhất một phần tử.

4. Xét lattice trong các hình dưới:

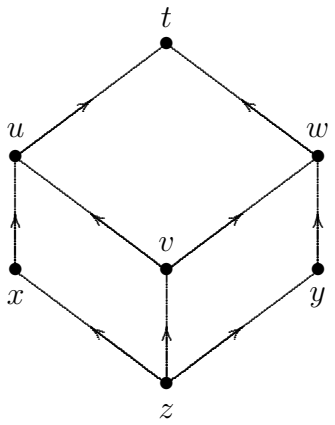


   (a) Liệt kê các nguyên tử của lattice.

   (b) Liệt kê các phần tử bất khả quy.

   (c) Viết các phần tử của lattice dưới dạng tuyển của các phần tử bất khả quy.

5. Lặp lại Bài tập 4 cho hình dưới:



6. Ký hiệu $\mathbb{P}$ là tập các số nguyên dương. Xét lattice $(\mathbb{P}, |)$, trong đó $m|n$ nếu m là ước số của n.

   (i) Cận dưới đúng của $\mathbb{P}$ bằng mấy?

   (b) Tồn tại cận trên đúng của $\mathbb{P}$?

   (c) Mô tả các nguyên tử của $\mathbb{P}$.

   (d) Mô tả các phần tử bất khả qui theo phép tuyển của $\mathbb{P}$.

7. Giả sử D_{90} là tập tất cả các ước số của 90 bao gồm 1 và 90. Chứng minh rằng D_{90} là lattice với thứ tự $|$.

   (a) Vẽ lược đồ Hasse của lattice này.

   (b) Tính $6 \vee 10, 6 \wedge 10, 9 \vee 30, 9 \wedge 30$.

   (c) Liệt kê các nguyên tử của D_{90}.

   (d) Liệt kê các phần tử bất khả qui của D_{90}.

   (e) Viết 90, 18, 5 dạng tuyển của các phần tử bất khả qui.

8. Tìm tất cả các lattice con của D_{90} mà có bốn phần tử bao gồm 1 và 90.

9. Với mỗi $x, y \in \mathbb{R}$, định nghĩa $x \vee y := \max\{x, y\}$ và $x \wedge y := \min\{x, y\}$.

   (a) Chứng minh rằng $(\mathbb{R}, \vee, \wedge)$ là lattice đại số.

   (b) Thứ tự cảm sinh bởi lattice này là gì?

   (c) Tại sao các phần tử của $\mathbb{R}$ là bất khả qui theo phép tuyển?

10. Hai lattice $(L_1, \vee, \wedge)$ và $(L_2, \cup, \cap)$ được gọi là *đẳng cấu* nếu tồn tại một tương ứng một-một lên $\varphi\colon L_1 \to L_2$ sao cho

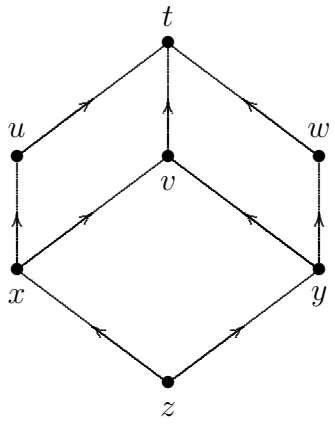
$$\varphi(x \vee y) = \varphi(x) \cup \varphi(y), \quad \varphi(x \wedge y) = \varphi(x) \cap \varphi(y)$$

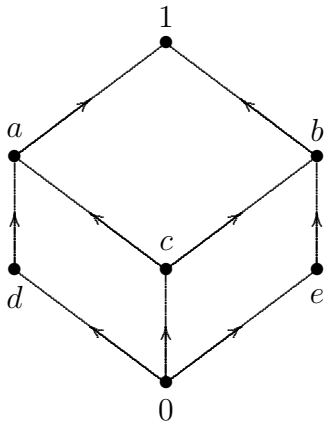
    với mọi $x, y \in L_1$.

    (a) Chứng minh rằng trong trường hợp này $\varphi(x) \leq \varphi(y)$ nếu và chỉ nếu $x \leq y$.

(b) Chứng minh rằng nếu $(L_1, \vee, \wedge)$ và $(L_2, \cup, \cap)$ đẳng cấu thì x là nguyên tử của L_1 nếu và chỉ nếu $\varphi(x)$ là nguyên tử của L_2.

(c) Chứng minh rằng hai lattice trong hình sau không đẳng cấu:





(d) Chứng minh rằng lattice D_{30} gồm các ước số của 30 (kể cả 1 và 30) đẳng cấu với lattice $\mathcal{P}(S)$, trong đó $|S| = 3$. (HD. Sử dụng $S = \{2, 3, 5\}$).

11. Giả sử $(L, \leq)$ là lattice. Chứng minh rằng nếu $x \leq y$, thì $x \vee (z \wedge y) \leq (x \vee z) \wedge y$ với mọi $z \in L$.

6.2 Lattice phân bố

Định nghĩa 6.2.1. Lattice đại số $(L, \vee, \wedge)$ được gọi là *lattice phân bố* (distributive) nếu các phép toán $\vee, \wedge$ phân phối đối với nhau, tức là với mọi $x, y, z \in L$ ta có

(a) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$;

(b) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

Ví dụ 6.2.1. (a) Lattice đại số trong Ví dụ 6.1.1 là phân bố.

(b) Lattice đại số trong Ví dụ 6.1.2 là lattice phân bố.

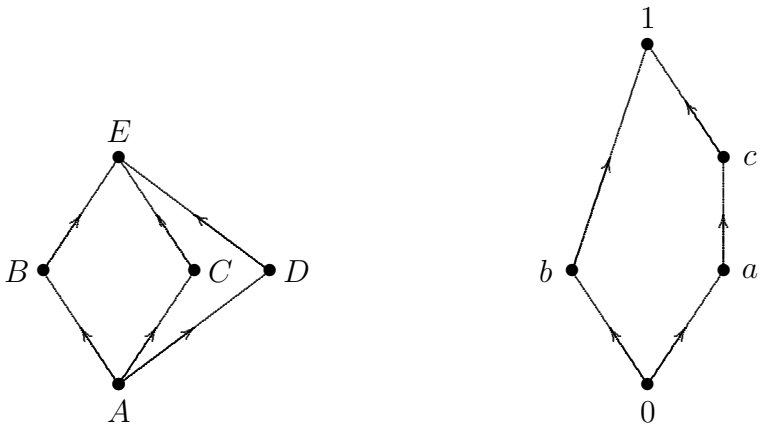
(c) $\mathbb{R}$ hoặc $\mathbb{N}$ là tập được sắp thứ tự đối với quan hệ thứ tự tuyến tính thông thường. Đó là các lattice phân bố, với

$$x \vee y = \max(x, y) \quad \text{và} \quad x \wedge y = \min(x, y).$$

Ví dụ 6.2.2. Các lattice đại số trong Hình 6.4 không phân bố.

Chẳng hạn, chứng minh (a). Ta có

$$B \vee (C \wedge D) = B \vee A = B.$$



(a) (b)

Hình 6.4: Các lattice không phân bố.

Mặt khác

$$(B \vee C) \wedge (B \vee D) = E \wedge E = E.$$

Vậy

$$B \vee (C \wedge D) = B \neq E = (B \vee C) \wedge (B \vee D).$$

Một điều thú vị là có thể chứng minh được *một lattice là phân bố nếu và chỉ nếu nó không chứa lattice con giống như các lattice trong Ví dụ 6.2.2.* Định lý sau chỉ ra rằng chỉ cần kiểm tra một tiêu chuẩn của luật phân bố.

Định lý 6.2.2. *Giả sử L là lattice đại số. Hai khẳng định sau là tương đương*

(a) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, *với mọi* $x, y \in L$.

(b) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, *với mọi* $x, y \in L$.

Chứng minh. (a) $\Rightarrow$ (b).

$$\begin{array}{rcll}
(x \wedge y) \vee (x \wedge z) & = & [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z] & \text{(do (a))} \\
& = & [x \vee (x \wedge y)] \wedge [z \vee (x \wedge y)] & \text{(tính giao hoán)} \\
& = & x \wedge [z \vee (x \wedge y)] & \text{(tính hấp thụ)} \\
& = & x \wedge [(z \vee x) \wedge (z \vee y)] & \text{(do (a))} \\
& = & [x \wedge (z \vee x)] \wedge (z \vee y) & \text{(tính kết hợp)} \\
& = & [x \wedge (x \vee z)] \wedge (y \vee z) & \text{(tính giao hoán)} \\
& = & x \wedge (y \vee z) & \text{(tính hấp thụ)}
\end{array}$$

(b) $\Leftarrow$ (a). Do nguyên lý đối ngẫu. $\square$

Định lý 6.2.3. *Giả sử $(L, \vee, \wedge)$ là lattice phân bố và $x, y, a \in L$ sao cho*

$$x \vee a = y \vee a \quad \text{và} \quad x \wedge a = y \wedge a.$$

Thì $x = y$.

Chứng minh. Ta có

$$\begin{aligned} x &= x \vee (x \wedge a) \\ &= x \vee (y \wedge a) \\ &= (x \vee y) \wedge (x \vee a) \\ &= (y \vee x) \wedge (y \vee a) \\ &= y \vee (x \wedge a) \\ &= y \vee (y \wedge a) \\ &= y. \end{aligned}$$

□

Từ đây về sau chúng ta luôn giả sử $(L, \vee, \wedge)$ là lattice có phần tử lớn nhất là 1 và phần tử nhỏ nhất là 0 (1 khác 0).

Định nghĩa 6.2.4. Hai phần tử $x, y \in L$ được gọi là *bù nhau* (complement) nếu

$$x \vee y = 1 \quad \text{và} \quad x \wedge y = 0.$$

Lattice L được gọi là *khả bù* (complemented) nếu mọi phần tử của L đều tồn tại phần tử bù.

Nhận xét 10. (a) Một phần tử của lattice L có thể có hoặc không có phần tử bù. Trong trường hợp tồn tại, có thể duy nhất hoặc không duy nhất.

(b) Các phần tử 1 và 0 là bù nhau và là phần tử bù duy nhất của nhau.

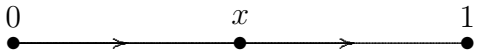
Ví dụ 6.2.3. (a) Lattice trong Ví dụ 6.2.2(a) là khả bù. Các phần tử bù không nhất thiết duy nhất: B là phần tử bù của cả C và D.

(b) Lattice L trong Ví dụ 6.2.2(b) cũng khả bù. Các phần tử bù cũng không duy nhất. Chẳng hạn, cả A và C đều là bù của B.

Ví dụ 6.2.4. Lattice trong Hình 6.5 là phân bố nhưng không khả bù. Vì nếu có

$$x \vee y = 1 \quad \text{và} \quad x \wedge y = 0.$$

Thì đẳng thức đầu cho $y = 1$ còn đẳng thức sau cho $y = 0$. Vô lý.



Hình 6.5:

Định lý 6.2.5. *Trong lattice phân bố L có phần tử 1 và 0, bù của phần tử x (nếu có) là duy nhất.*

Chứng minh. Giả sử rằng

$$x \vee y = 1, \quad x \wedge y = 0, \quad x \vee z = 1, \quad x \wedge z = 0.$$

Ta có

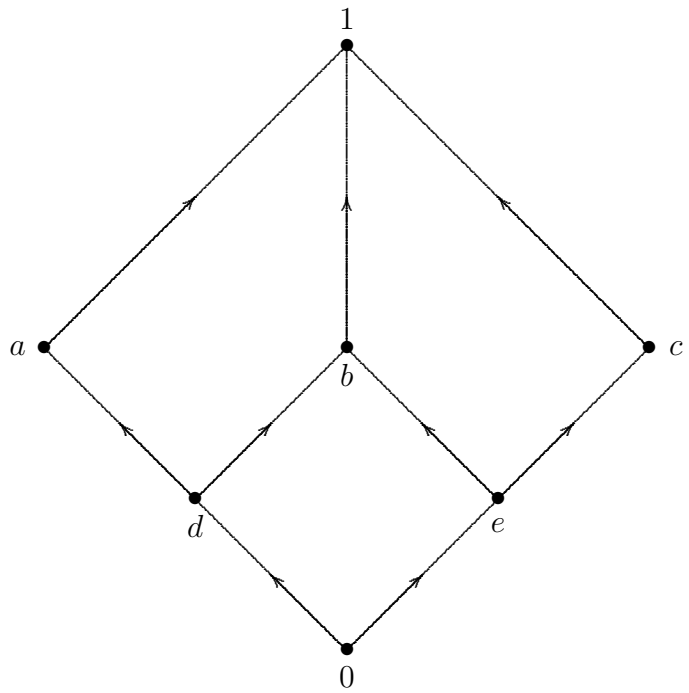
$$\begin{aligned}
y &= y \vee 0 && (\text{vì } 0 \leq y)\\
&= y \vee (x \wedge z) && (\text{vì } x \wedge z = 0)\\
&= (y \vee x) \wedge (y \vee z) && (\text{vì tính phân bố})\\
&= 1 \wedge (y \vee z) && (\text{vì } y \vee x = x \vee y = 1)\\
&= (x \vee z) \wedge (y \vee z) && (\text{vì } x \vee z = 1)\\
&= (x \wedge y) \vee z && (\text{vì tính phân bố})\\
&= 0 \vee z && (\text{vì } x \wedge y = 0)\\
&= z && (\text{vì } 0 \leq z).
\end{aligned}$$

□

Nhận xét 11. Nếu phần tử trong lattice tồn tại duy nhất phần tử bù, thì phần tử bù của x được ký hiệu là x'.

Bài tập

1. Xét lattice đại số L_1 với lược đồ Hasse:



   (a) Liệt kê các nguyên tử của L_1.

   (b) Liệt kê các phần tử bất khả qui của L_1.

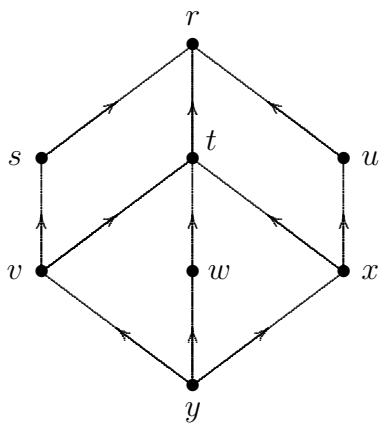
   (c) Viết 1 dưới dạng tuyển của các phần tử bất khả qui.

   (d) Tìm các phần tử bù, nếu tồn tại, của $a, b, d, 0$.

(e) L_1 là lattice khả bù? Giải thích.

(f) L_1 là lattice phân bố?

2. Xét lattice L_2 với lược đồ Hasse trong hình:



(a) Tìm các phần tử lớn nhất và phần tử nhỏ nhất của L_2.

(b) Tìm $v \vee x, s \vee v$ và $u \wedge v$.

(c) L_2 là lattice khả bù? Giải thích.

(d) Tìm phần tử có hai phần tử bù.

(e) L_2 là lattice phân bố?

3. (a) Chứng minh rằng các phần tử 2 và 6 trong lattice D_{12} không có phần tử bù.

(b) Chứng minh rằng $D_m, m \geq 2$, là khả bù nếu và chỉ nếu m là tích của các số nguyên tố phân biệt, tức là nếu phân tích thành các thừa số nguyên tố $m = p_1^{\alpha_1}.p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, thì $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 1$.

4. (a) Vẽ lược đồ Hasse của lattice $(D_{24}, |)$.

(b) Tìm các phần tử bù, nếu tồn tại, của $2, 3, 4, 6$.

(c) D_{24} là lattice khả bù? Giải thích.

(d) D_{24} là lattice phân bố? Giải thích.

5. (a) Vẽ lược đồ Hasse của lattice $(D_{36}, |)$.

(b) D_{36} là lattice khả bù? Giải thích.

(d) D_{36} là lattice phân bố? Giải thích.

6. Chứng minh các đồ thị trong hình sau là lược đồ Hasse của lattice phân bố. Nó là khả bù?

7. Ký hiệu D_{70} là tập tất cả các ước số của 70 bao gồm 1 và 70.

(a) Vẽ lược đồ Hasse của lattice $(D_{70}, |)$.

(b) Tính $10 \vee 14, 10 \wedge 14$.

(c) Liệt kê các nguyên tử của D_{70}.

(d) Liệt kê các phần tử bất khả qui của D_{70}.

(e) Viết $70, 10, 5$ dạng tuyển của các phần tử bất khả qui.

(f) D_{70} là lattice khả bù? Tìm các phần tử bù của $2, 5$.

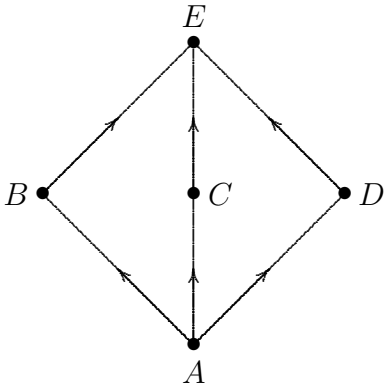
8. Lặp lại Bài tập trên đối với $(D_{36}, |)$.

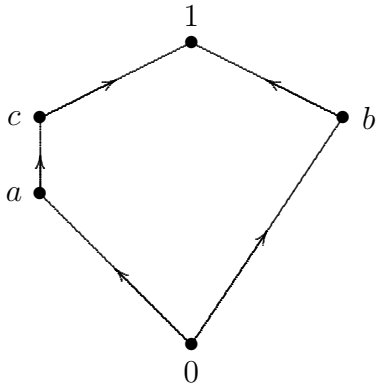
9. (a) Các xích[1] nào có cận trên và dưới?

(b) Các xích nào là phân bố?

(c) Các xích nào là khả bù?

10. Sử dụng Định lý 6.2.5 chứng minh các lattice trong hình sau không phân bố:





11. Giả sử L là lattice với phần tử lớn nhất 1, phần tử nhỏ nhất 0. Chứng minh rằng 0 là bù duy nhất của 1 và ngược lại.

12. Chứng minh hoặc cho phản ví dụ:

(a) Mọi lattice hữu hạn là phân bố.

(b) Mọi lattice hữu hạn có cận trên.

13. Giả sử $(L, \wedge, \vee)$ là lattice phân bố khả bù.

(a) Chứng minh rằng nếu $x \preceq y$ thì $y' \preceq x'$.

(b) Chứng minh rằng nếu $y \wedge z = 0$ thì $y \preceq z'$.

(c) Chứng minh rằng nếu $x \preceq y$ và $y \wedge z = 0$ thì $z \preceq x'$.

6.3 Đại số Boole

Định nghĩa 6.3.1. *Đại số Boole* (còn gọi là lattice Boole) là một lattice phân bố khả bù.

[1] *Xích* là tập được sắp thứ tự mà hai phần tử bất kỳ có thể so sánh được với nhau.

Nhận xét 12. (a) Đại số Boole là một lattice phân bố có phần tử lớn nhất 1, phần tử nhỏ nhất 0 ($1 \neq 0$), và mọi phần tử của nó luôn tồn tại duy nhất phần tử bù. Các phép toán hai ngôi

$$(x, y) \mapsto x \vee y, \qquad (x, y) \mapsto x \wedge y$$

và phép toán một ngôi

$$x \mapsto x'$$

được gọi là các *phép toán Boole*.

(b) Ta thường ký hiệu $(x')' = x''$.

(c) Trong đại số Boole : $(x')' = x$.

Ví dụ 6.3.1. Lattice $\mathcal{P}(S)$ trong Ví dụ 6.1.1 là lattice phân bố, trong đó $1 = S, 0 = \emptyset$ và với mọi $A \subset S$ ta có

$$A \cup A^c = S, \qquad A \cap A^c = \emptyset.$$

Nên $\mathcal{P}(S)$ là đại số Boole.

Ví dụ 6.3.2. Lattice Σ trong Ví dụ 6.1.2 là lattice phân bố trong đó

+ phần tử lớn nhất là $1 = [\text{True}]$.

+ phần tử phần tử nhỏ nhất là $0 = [\text{False}]$.

+ với mọi mệnh đề p,

$$[p] \text{ or } [\text{not } p] = [\text{True}]; \quad [p] \text{ and } [\text{not } p] = [\text{False}].$$

Tức là

$$p' = \text{ not } p.$$

Nên là đại số Boole.

Ví dụ 6.3.3. (a) Xét lattice $\text{Fun}(S, \mathbb{B})$ trong Ví dụ 6.1.4 (b).

+ $\text{Fun}(S, \mathbb{B})$ là lattice phân bố vì $\max, \min$ phân bố với nhau.

+ Có phần tử lớn nhất là 1 định nghĩa bởi $1(x) = 1$ với mọi $x \in S$.

+ Có phần tử nhỏ nhất là 0 định nghĩa bởi $0(x) = 0$ với mọi $x \in S$.

+ Với mọi $f \in \text{Fun}(S, \mathbb{B})$ ta có $[f(x)]' = 1$ nếu và chỉ nếu $f(x) = 0$ với mọi $x \in S$. Vì

$$(f' \vee f)(x) = \max([f(x)]', f(x)) = 1,$$
$$(f' \wedge f)(x) = \min([f(x)]', f(x)) = 0.$$

Nên $\mathrm{Fun}(S, \mathbb{B})$ là đại số Boole.

(b) Trên $\mathbb{B}^n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{B}, i = 1, 2, \ldots, n\}$ xét các phép toán

$$\begin{aligned} x \vee y &:= (\max(x_1, y_1), \max(x_2, y_2), \ldots, \max(x_n, y_n)), \\ x \wedge y &:= (\min(x_1, y_1), \min(x_2, y_2), \ldots, \min(x_n, y_n)). \end{aligned}$$

Khi đó $\mathbb{B}^n$ là đại số Boole với phần tử lớn nhất là $1 = (1, 1, \ldots, 1)$ và phần tử nhỏ nhất là $0 = (0, 0, \ldots, 0)$.

Định lý 6.3.2. (Luật de Morgan) *Nếu A là đại số Boole thì với mọi $x, y \in A$ ta có*

(a) $(x \vee y)' = x' \wedge y'$;

(b) $(x \wedge y)' = x' \vee y'$.

Chứng minh. (a) Ta có

$$\begin{aligned} (x \vee y) \vee (x' \wedge y') &= [(x \vee y) \vee x'] \wedge [(x \vee y) \vee y'] && \text{(do tính phân bố)} \\ &= [y \vee (x \vee x')] \wedge [x \vee (y \vee y')] && \text{(do tính kết hợp và giao hoán)} \\ &= [y \vee 1] \wedge [x \vee 1] \\ &= 1 \wedge 1 \\ &= 1. \end{aligned}$$

Tương tự

$$(x \vee y) \wedge (x' \wedge y') = 0.$$

Từ đó có (a). (b) Vì

$$\begin{aligned} x \wedge y &= (x')' \wedge (y')' \\ &= (x' \vee y')'. \end{aligned}$$

Nên

$$\begin{aligned} (x \wedge y)' &= (x' \vee y')'' \\ &= x' \vee y'. \end{aligned}$$

□

Định lý 6.3.3. *Giả sử A là đại số Boole hữu hạn với tập các nguyên tử $S := \{a_1, a_2, \ldots, a_n\}$. Với mỗi $x \in A, x \neq 0$, ta có thể viết dưới dạng tuyển các nguyên tử khác nhau như sau*

$$x = a_{i_1} \vee a_{i_2} \vee \ldots \vee a_{i_k}. \tag{6.3}$$

Hơn nữa biểu thức trên là duy nhất không kể thứ tự của các nguyên tử trong biểu thức, và $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$ là các nguyên tử $\leq x$.

Chứng minh. + Đầu tiên ta chứng minh tính tồn tại.

Nếu $x = 0$ hoặc x là nguyên tử thì hiển nhiên. Ngược lại, tồn tại $y \in A$ sao cho $0 < y < x$. Ta có

$$\begin{aligned} x &= x \vee y \\ &= (x \vee y) \wedge 1 \\ &= (x \vee y) \wedge (y' \vee y) \\ &= (x \wedge y') \vee y. \end{aligned}$$

Mặt khác $x \wedge y' < x$. Vì nếu ngược lại, thì $x \wedge y' = x$. Do đó

$$y < x = x \wedge y' \leq y'.$$

Vậy

$$0 < y = y \wedge y'.$$

Mà không thể.

Vậy ta phân tích x dạng tuyển các phần tử nhỏ hơn là $x \wedge y'$ và y. (Lý luận này chứng tỏ chỉ có các nguyên tử và phần tử nhỏ nhất 0 là bất khả quy). Nếu cả hai y và $x \wedge y'$ là nguyên tử, chứng minh xong. Ngược lại, bằng phương pháp trên ta phân tích chúng ở dạng tuyển các phần tử nhỏ hơn.

Vì A hữu hạn, nên cuối cùng quá trình trên phải dừng và phân tích x dạng tuyển các nguyên tử.

Chú ý rằng phương pháp trên cho chúng ta thuật toán đệ quy tìm biểu diễn của một phần tử qua các nguyên tử.

+ Ta chứng minh rằng với mọi $x \in A$ đều thỏa

$$x = \vee\{a \in S \mid a \leq x\}. \tag{6.4}$$

Ký hiệu bên phải chỉ phần tử là tuyển các phần tử trong tập $\{a \in S \mid a \leq x\}$. Vì có thể xem phần tử 0 là tuyển của tập trống của các nguyên tử, nên có thể giả sử $x \neq 0$. Từ (6.3) ta dễ dàng suy ra

$$1 = \vee\{a \in S \mid a \leq 1\} = a_1 \vee a_2 \vee \ldots \vee a_n.$$

Nên

$$\begin{aligned} x &= x \wedge 1 \\ &= x \wedge (a_1 \vee a_2 \vee \ldots \vee a_n) \\ &= (x \wedge a_1) \vee (x \wedge a_2) \vee \ldots \vee (x \wedge a_n). \end{aligned}$$

Mặt khác

$$x \wedge a_i = \begin{cases} a_i & \text{nếu } a_i \leq x, \\ 0 & \text{nếu ngược lại,} \end{cases}$$

do a_i là nguyên tử. Vậy x có biểu diễn dạng (6.4).

+ Tính duy nhất. Giả sử rằng

$$x = b_1 \wedge b_2 \wedge \ldots \wedge b_m,$$

trong đó b_i là các nguyên tử. Khi đó $b_i \leq x, i = 1, 2, \ldots, m$.

Vậy

$$b_i \in \{a \in S \mid a \leq x\}, \quad i = 1, 2, \ldots, m.$$

Mặt khác, nếu $a \in S, a \leq x$, thì

$$\begin{aligned} 0 \neq a &= a \wedge x \\ &= a \wedge (b_1 \vee b_2 \vee \ldots \vee b_m) \\ &= (a \wedge b_1) \vee (a \wedge b_2) \vee \ldots \vee (a \wedge b_m). \end{aligned}$$

Vậy tồn tại chỉ số i sao cho

$$a \wedge b_i \neq 0.$$

Do a và b_i là các nguyên tử, nên

$$a \wedge b_i = a = b_i.$$

Nói cách khác, a là phần tử b_i nào đó. Điều phải chứng minh. □

Kết quả sau đây sẽ chứng tỏ đại số Boole được hoàn toàn xác định bởi số các nguyên tử của nó.

Định lý 6.3.4. *Cho A, B là các đại số Boole hữu hạn với tập các nguyên tử $S := \{a_1, a_2, \ldots, a_n\}$ và $T := \{b_1, b_2, \ldots, b_n\}$ tương ứng. Khi đó tồn tại một đẳng cấu đại số Boole từ A lên B; tức là tồn tại ánh xạ một-một lên $f\colon A \to B$ sao cho*

(a) $f(x \vee y) = f(x) \vee f(y)$;

(b) $f(x \wedge y) = f(x) \wedge f(y)$;

(c) $f(x') = [f(x)]'$.

Ngoài ra

$$f(a_i) = b_i, \quad i = 1, 2, \ldots, n.$$

Chứng minh. Theo Định lý 6.3.3, mọi $x \in A$ có thể biểu diễn duy nhất dưới dạng

$$x = a_{i_1} \vee a_{i_2} \vee \ldots \vee a_{i_k}.$$

Ta định nghĩa

$$f(x) = b_{i_1} \vee b_{i_2} \vee \ldots \vee b_{i_k}.$$

Đặc biệt

$$f(a_i) = b_i, \quad i = 1, 2, \ldots, n.$$

Theo định nghĩa của f và do Định lý 6.3.3, ta có

$$f(x) = \vee\{f(a) \mid a \in S, a \leq x\}$$

và

$$f(x) = \vee\{b \in T \mid b \leq f(x)\}.$$

Vì biểu diễn của $f(x)$ là duy nhất, nên với mọi $a \in S$ ta có

$$a \leq x \quad \text{nếu và chỉ nếu } f(a) \leq f(x).$$

Để chứng minh (a), lấy $x, y \in A$ và chú ý rằng $a \in S$, ta có

$$\begin{aligned} f(a) \leq f(x \vee y) &\Leftrightarrow a \leq (x \vee y) \\ &\Leftrightarrow a \leq x \text{ hoặc } a \leq y \\ &\Leftrightarrow f(a) \leq f(x) \text{ hoặc } f(a) \leq f(y). \end{aligned}$$

Tức là, với mỗi $b \in T$ ta có

$$\begin{aligned} b \leq f(x \vee y) &\Leftrightarrow b \leq f(x) \text{ hoặc } b \leq f(y) \\ &\Leftrightarrow b \leq f(x) \vee f(y). \end{aligned}$$

Áp dụng Định lý 6.3.3, suy ra

$$f(x \vee y) = f(x) \vee f(y).$$

Vậy khẳng định (a) được chứng minh. Tương tự ta cũng có (b).

Chứng minh (c). Ta có

$$\begin{aligned} f(x) \vee f(x') &= f(x \vee x') = f(1) = 1, \\ f(x) \wedge f(x') &= f(x \wedge x') = f(0) = 0. \end{aligned}$$

Vậy $[f(x)]' = f(x')$. □

Nếu S là tập có n phần tử thì $\mathcal{P}(S)$ là một đại số Boole (tương ứng với các phép toán hợp, giao và lấy phần bù) có n nguyên tử, cụ thể $\{x\}, x \in S$. Vậy

Hệ quả 6.3.5. *Một đại số Boole hữu hạn có n nguyên tử thì đẳng cấu đại số Boole với* $\mathcal{P}(S), \#S = n$, *và vì vậy có đúng* 2^n *phần tử.*

Bài tập

1. (a) Kiểm tra $\mathbb{B} := \{1, 0\}$ với hai phép toán $\vee, \wedge$ thông thường và $0' = 1, 1' = 0$, là đại số Boole.

(b) Kiểm tra tập $\mathrm{Fun}(S, \mathbb{B})$ các hàm từ S lên $\mathbb{B}$ với hai phép toán

$$(f \vee g)(x) := f(x) \vee g(x),$$
$$(f \wedge g)(x) := f(x) \wedge g(x),$$
$$(f')(x) := [f(x)]',$$

là đại số Boole.

2. (a) Đặt $S := \{a, b, c, d, e\}$. Viết $\{a, c, d\}$ như tuyển của các nguyên tử trong $\mathcal{P}(S)$.

   (b) Biểu diễn phần tử $(1, 0, 1, 1, 0)$ dạng tuyển các nguyên tử trong $\mathbb{B}^5$.

   (c) Giả sử $f \in \mathrm{Fun}(S, \mathbb{B})$ sao cho $f(a) = f(c) = f(d) = 1$, $f(b) = f(e) = 0$. Biểu diễn f dạng tuyển các nguyên tử trong $\mathrm{Fun}(S, \mathbb{B})$.

3. Trên tập $D_6 := \{1, 2, 3, 6\}$ xét các phép toán:

$$x + y := \mathrm{BSCNN}(x, y), \quad x.y := \mathrm{USCLN}(x, y), \quad x' := \frac{6}{x}.$$

   Chứng minh rằng $(D_6, +, \cdot, ')$ là đại số Boole. Tìm các phần tử nhỏ nhất và phần tử lớn nhất.

4. Trên tập $D_8 := \{1, 2, 4, 8\}$ xét các phép toán $+$ và $\cdot$ như trong Bài tập 3 và $x' = 8/x$. Chứng minh $(D_8, +, \cdot, ')$ không phải đại số Boole.

5. Lattice $(D_{30}, |)$ là đại số Boole.

   (a) Vẽ lược đồ Hasse của lattice này.

   (b) Liệt kê các nguyên tử của D_{30}.

   (c) Tìm tất cả các đại số Boole con của D_{30}. Chú ý rằng, các đại số con cần chứa 1 và 30.

   (d) Tìm lattice con có bốn phần tử nhưng không phải là đại số Boole con.

6. Lattice $(D_{210}, |)$ là đại số Boole. Tìm tập S sao cho $\mathcal{P}(S)$ và D_{210} là đẳng cấu đại số Boole và tìm đẳng cấu này.

7. Với những giá trị m nào thì lattice $(D_m, |)$ là đại số Boole?

8. Trên tập $S_n := \{1, 2, \ldots, n\}$ xét các phép toán:

$$x + y := \max(x, y), \quad x.y := \min(x, y).$$

   (a) Chứng minh trên S_n các phép toán này thỏa mãn các tính chất giao hoán, kết hợp và hấp thụ.

   (b) Chứng minh có thể định nghĩa phần tử nhỏ nhất 0, phần tử lớn nhất 1 và phép toán phủ định $'$ sao cho S_n với các phép toán này là đại số Boole nếu và chỉ nếu $n = 2$.

9. Giả sử $(A, \vee, \wedge)$ là đại số Boole và S là tập con của A. Chứng minh S với các phép toán $\vee, \wedge$ cảm sinh là đại số Boole nếu và chỉ nếu $1 \in S$ và $x \wedge y' \in S$ với mọi $x, y \in S$.

10. (a) Chứng minh trong đại số Boole, $[x(x'+y))]' = x'+y'$ với mọi x, y.

    (b) Viết đối ngẫu và chứng minh biểu thức trên.

11. Giả sử $\mathbb{P}$ là tập các số nguyên dương và S là họ các tập con hữu hạn của $\mathbb{P}$. Giải thích tại sao S với các phép hợp, giao và lấy phần bù không là đại số Boole.

12. Tìm tập S sao cho $\mathcal{P}(S)$ và $\mathbb{B}^5$ là đẳng cấu đại số Boole và tìm đẳng cấu này.

13. Mô tả các nguyên tử của $\mathrm{Fun}(S, \mathbb{B}), S := \mathbb{N}$. Điều này còn đúng nếu $S := \mathbb{R}$?

14. (a) Tồn tại đại số Boole với 6 phần tử? Giải thích.

    (b) Mọi đại số Boole hữu hạn phần tử đẳng cấu với đại số Boole $\mathcal{J}_n$ của các hàm Boole? Giải thích.

15. (a) Mô tả các nguyên tử của lattice $\mathcal{P}(\mathbb{N})$.

    (b) Mỗi phần tử của lattice là tuyển của các nguyên tử? Thảo luận.

16. Giả sử x, y là các phần tử của đại số Boole, và a là một nguyên tử.

    (a) Chứng minh rằng $a \leq x \vee y$ nếu và chỉ nếu $a \leq x$ hoặc $a \leq y$.

    (b) Chứng minh rằng $a \leq x \wedge y$ nếu và chỉ nếu $a \leq x$ và $a \leq y$.

    (c) Chứng minh rằng hoặc $a \leq x$ hoặc $a \leq x'$ và không đồng thời cả hai.

17. Giả sử x, y là các phần tử của đại số Boole hữu hạn mà được viết dưới dạng tuyển các nguyên tử

$$x = a_1 \vee a_2 \vee \cdots \vee a_n, \text{ và } \ y = b_1 \vee b_2 \vee \cdots \vee b_m.$$

18. (a) Giải thích cách viết $x \vee y$ và $x \wedge y$ dạng tuyển các nguyên tử phân biệt. Minh họa bằng ví dụ.

    (b) Viết s' dạng tuyển các nguyên tử phân biệt.

19. Chứng minh rằng nếu Φ là đẳng cấu đại số Boole giữa các đại số Boole A và B thì $x \leq y$ nếu và chỉ nếu $\Phi(x) \leq \Phi(y)$.

20. Giả sử $S := [0, 1]$ và $\mathcal{A}$ gồm tập trống và tất cả các tập con của S sao cho có thể viết ở dạng hợp hữu hạn các khoảng có dạng $[a, b)$.

    (a) Chứng minh rằng mỗi phần tử của $\mathcal{A}$ có thể viết như hợp hữu hạn của các khoảng rời nhau dạng $[a, b)$.

    (b) Chứng minh $\mathcal{A}$ là đại số Boole tương ứng với các phép toán giao ($\cap$), hợp ($\cup$) và lấy phần bù.

    (c) Chứng minh $\mathcal{A}$ không có nguyên tử.

21. Giả sử $a \to \bar{a}, a \to \tilde{a}$ là hai phép toán lấy phần bù tương ứng với đại số Boole $(A, \vee, \wedge)$. Chứng minh rằng $\bar{a} = \tilde{a}$, với mọi $a \in A$.

6.4 Hàm Boole

Phần này chúng ta sẽ định nghĩa một cách tổng quát về "hàm Boole", đồng thời mô tả các dạng "chính quy" của chúng. Nghiên cứu hàm Boole tức là nghiên cứu các ánh xạ Boole từ một đại số Boole vào chính bản thân nó. Mỗi phần tử của đại số Boole gọi là "hằng số". Mỗi một ký hiệu biểu diễn một trong các phần tử của đại số Boole gọi là "biến Boole".

Định nghĩa 6.4.1. Ánh xạ

$$f\colon \mathbb{B}^n \longrightarrow \mathbb{B}, \quad (x_1,\ x_2, \ldots, x_n) \mapsto f(x_1, x_2, \ldots, x_n),$$

được gọi là *hàm Boole n biến* nếu nó được cấu tạo theo nguyên tắc sau đây

(a) Hàm hằng $f(x) = a, a \in \mathbb{B}$, và phép chiếu lên thành phần thứ i : $f(x) = x_i$ là hàm Boole.

(b) Nếu f là hàm Boole thì hàm phủ định f' cũng là hàm Boole.

(c) Nếu f và g là các hàm Boole thì $f \vee g$ và $f \wedge g$ cũng là hàm Boole.

(d) Mọi hàm số được cấu tạo bằng cách áp dụng một số hữu hạn lần các quy luật kể trên đều là hàm Boole.

Nhận xét 13. Theo định nghĩa trên thì hàm Boole là một hàm số được cấu tạo từ các hằng số và các phép chiếu bằng cách ứng dụng một số hữu hạn lần các phép toán hội, tuyển và phủ định.

Ví dụ 6.4.1. (a) Các hàm dưới đây là các hàm Boole theo ba biến x, y, z :

$$(x \vee y) \wedge (x' \vee z) \wedge y, \quad y' \vee (x \vee z'), \quad x \vee y, \quad z.$$

(b) Hàm Boole n biến

$$(x_1 \wedge x_2 \wedge \ldots \wedge x_n) \vee (x_1' \wedge x_2 \wedge \ldots \wedge x_n) \vee (x_1 \wedge x_2' \wedge \ldots \wedge x_n).$$

Để giản tiện, ta sử dụng các ký hiệu + (cộng) và . (nhân) thay cho $\vee$ và $\wedge$.

Một trong những cách thuận tiện nhất để mô tả hàm Boole là cho tương ứng một-một với *bảng chân trị* (hay *bảng giá trị thật),* tức là bảng giá trị của hàm số ứng với những tổ hợp giá trị khác nhau của các biến.

Ví dụ 6.4.2. Bảng chân trị của hàm

$$f(x, y, z) = y' \wedge (x \vee z)$$

là

x	y	z	y'	$x \vee z$	f
0	0	0	1	0	0
0	0	1	1	1	1
0	1	0	0	0	0
0	1	1	0	1	0
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	0	1	0
1	1	1	0	1	0

Nhận xét 14. Mỗi hàm Boole có *duy nhất* một bảng chân trị. Ngược lại, ta luôn luôn có thể xây dựng được *vô số* hàm Boole n biến có bảng chân trị gồm 2^n hàng cho trước.

Ví dụ 6.4.3. Xét bảng chân trị

x	y	z	f	
0	0	0	1	x
0	0	1	0	
0	1	0	0	
0	1	1	1	x
1	0	0	0	
1	0	1	1	x
1	1	0	0	
1	1	1	1	x

Để tìm hàm Boole $f(x, y, z)$ có bảng chân trị trên, chúng ta tiến hành theo các bước sau

+ Đầu tiên, đánh dấu mỗi hàng mà có cột cuối bằng 1.

+ Với mỗi hàng được đánh dấu, ta đặt tương ứng một số hạng dạng:

$$e_1 \wedge e_2 \wedge e_3,$$

trong đó $e_1 = x$ nếu phần tử trong cột đầu của hàng này bằng một và $e_1 = x'$ nếu ngược lại. Tương tự $e_2 = y$ nếu phần tử trong cột thứ hai của hàng này bằng 1 và $e_2 = y'$ nếu ngược lại. Cuối cùng $e_3 = z$ nếu phần tử trong cột thứ ba của hàng này bằng 1 và $e_3 = z'$ nếu ngược lại.

Do đó các phần tử tương ứng với bốn hàng được đánh dấu là

$$x \wedge y \wedge z, \quad x \wedge y' \wedge z, \quad x' \wedge y \wedge z, \quad x' \wedge y' \wedge z'.$$

+ Cuối cùng, ta tuyển các biểu thức này để có hàm

$$f(x, y, z) = (x \wedge y \wedge z) \vee (x \wedge y' \wedge z) \vee (x' \wedge y \wedge z) \vee (x' \wedge y' \wedge z').$$

Nếu cột cuối của bảng chân trị gồm toàn số 0, thì phương pháp trên không làm việc; tuy nhiên, hàm Boole $f \equiv 0$ là hàm có bảng chân trị như vậy.

Định nghĩa 6.4.2. Hai hàm Boole được gọi là *tương đương* với nhau nếu chúng có cùng một bảng chân trị.

Ví dụ 6.4.4. Các biểu thức $x(y \vee z)$ và $xy \vee xz$ là tương đương.

Định lý sau cho chúng ta số các phần tử của tập tất cả các hàm Boole n biến: $\text{Fun}(\mathbb{B}^n, \mathbb{B}) := \{f : \mathbb{B}^n \to \mathbb{B}\}$.

Định lý 6.4.3. *Có 2^{2^n} ánh xạ từ $\mathbb{B}^n$ vào $\mathbb{B}$.*

Chứng minh. Rõ ràng $\#\mathbb{B}^n = 2^n$. Mỗi hàm từ $\mathbb{B}^n$ vào $\mathbb{B}$ có thể lấy một trong hai giá trị độc lập là 0 và 1. Do vậy ta có 2^{2^n} tổ hợp khả năng khác nhau; nghĩa là có 2^{2^n} ánh xạ khác nhau. □

Ví dụ 6.4.5. (a) Trường hợp $n = 1$ ta có bốn hàm Boole:

$$f_1 = 0, f_2 = x, f_3 = x', f_4 = 1.$$

(b) Trường hợp $n = 2$ ta có 16 hàm số Boole được liệt kê trong bảng sau

STT	f	Tên gọi
1	0	Hàm hằng 0
2	x_1x_2	Hàm AND
3	x_1x_2'	Hàm kéo theo không điều kiện
4	x_1	Phép chiếu lên biến thứ nhất
5	$x_1'x_2$	Hàm kéo theo không đảo
6	x_2	Phép chiếu lên biến thứ hai
7	$x_1x_2' + x_1'x_2$	Hàm cộng modulo 2
8	$x_1 + x_2$	Hàm OR
9	$x_1'x_2'$	Hàm NOR
10	$x_1x_2 + x_1'x_2'$	Hàm tương đương
11	x_2'	Hàm phủ định x_2
12	$x_1 + x_2'$	Hàm kéo theo đảo
13	x_1'	Hàm phủ định x_1
14	$x_1' + x_2$	Hàm kéo theo có điều kiện
15	$x_1' + x_2'$	Hàm NAND (Sheffer)
16	1	Hàm hằng 1

Hệ quả 6.4.4. *$\text{Fun}(\mathbb{B}^n, \mathbb{B})$ với các phép toán $+, ., -$ là một đại số Boole đẳng cấu với $\mathbb{B}^{2^n}$.*

Bài tập

1. Chứng minh các biểu thức dưới đây là các hàm Boole và tìm giá trị của các hàm này khi $x = 1, y = 1, z = 0$:

(a) $(x \wedge y) \vee (y' \wedge z)$.

(b) $(x \wedge y)'$.

(c) $x \vee (y' \wedge z)$.

(d) $(x \wedge y') \vee (y \wedge z')$.

(e) $(x \wedge (y \vee (x \wedge y'))) \vee ((x \wedge y') \vee (x \wedge z')')$.

2. Các biểu thức nào là hàm Boole:

(a) $x \wedge (y \wedge z)$.

(b) $x \wedge (y' \wedge z)$.

(c) (x).

(d) $(x \wedge y) \vee z'$.

(e) $((x))$.

3. Tìm hàm Boole $f : \mathbb{B}^3 \to \mathbb{B}$ nếu $f(0,0,0) = f(0,0,1) = f(1,1,0) = 1$ và $f(a,b,c) = 0$ với tất cả $(a,b,c) \in \mathbb{B}^3$ khác.

4. Kiểm tra các đẳng thức sau:

(a) $x \vee x = x$.

(b) $x \vee (x \wedge y) = x$.

(c) $x \wedge y' = (x' \vee y)'$.

(d) $x \wedge (y \wedge z)' = (x \wedge y') \vee (x \wedge z')$.

(e) $x' \wedge ((y \wedge z) \vee (x \wedge y \wedge z)) = x \wedge z$.

5. Đúng hay sai:

(a) $(x \wedge y) \vee (x' \wedge z) \vee (x' \wedge y \wedge z') = y \vee (x' \wedge z)$.

(b) $(x \wedge y \wedge z) \vee (x \wedge z)' = (x \wedge z) \vee (x' \wedge z')$.

6. Chứng minh nếu f_1 và f_2 là các hàm Boole theo các biến $x_1, x_2, \ldots, x_n$ thì $f_1 \vee f_2$ tương đương với $f_2 \vee f_1$.

7. Các hàm Boole như x hay y' gồm một biến đơn hoặc phần bù của nó được gọi là *literal*.

(a) Chứng minh $x'z \vee y'z$ không tương đương với tích các literal.

(b) Chứng minh $x'z \vee y'z$ không tương đương với tuyển của các tích của các literal mà trong đó một tích là một literal đơn. (Phần (a) và (b) chỉ ra rằng $x'z \vee y'z$ là tối ưu).

(c) Nhóm ba số hạng $xyz \vee xyz' \vee xy'z$ dạng các cặp để nhận được một biểu thức tương đương dạng tuyển của hai tích mà mỗi tích gồm hai literal.

6.5 Biểu diễn các hàm Boole qua hệ tuyển, hội và phủ định

Như chúng ta đã biết, một trong những cách cho hàm Boole là dùng bảng chân trị. Mỗi bảng chân trị có thể biểu diễn nhiều hàm số khác nhau, nhưng các hàm số này phải tương đương với nhau. Nói một cách khác có thể dùng bảng chân trị để kiểm tra các hàm Boole có tương đương với nhau hay không?

Ngoài ra, để so sánh các hàm Boole với nhau người ta đưa ra dạng *chính quy* (hay *dạng chuẩn).* Hai cách biểu diễn khác nhau của hàm Boole có cùng một dạng chính quy nếu và chỉ nếu chúng tương đương với nhau. Nói cách khác, dạng chính quy của một cách biểu diễn hàm Boole là duy nhất. Có hai dạng chính quy thường dùng, đó là dạng *tuyển chính quy* (hay dạng tổng của các tích) và *dạng hội chính quy* (hay dạng tích của các tổng).

Để tiện trình bày, ta đưa vào quy ước sau. Giả sử x là một biến và $e \in \mathbb{B}$. Ký hiệu

$$x^e := \begin{cases} x & \text{nếu } e = 1, \\ x' & \text{nếu ngược lại.} \end{cases}$$

Từ định nghĩa ta có

$$x^e = 1 \text{ nếu và chỉ nếu } x = e.$$

Định nghĩa 6.5.1. Giả sử f là hàm Boole n biến. Tập

$$T_f := \{x = (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n \mid f(x) = 1\}$$

được gọi là *tập đặc trưng* của f.

Tính chất 6.5.2. (a) $T_{f'} = [T_f]' = \{x = (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n \mid f(x') = 1\}$.

(b) $T_{f+g} = T_f \cup T_g$.

(c) $T_{fg} = T_f \cap T_g$.

Chứng minh. Hiển nhiên theo định nghĩa. □

Hơn nữa có một tương ứng một-một giữa các hàm Boole và tập đặc trưng của nó. Các tính chất này cho phép chuyển chứng minh trên đại số logic sang các chứng minh tương ứng trên đại số tập hợp.

Định lý 6.5.3. *Cố định $i \in \{1, 2, \ldots, n\}$. Khi đó mọi hàm Boole n biến f đều có thể biểu diễn dưới dạng tuyển chính quy*

$$f(x) = \sum f(e_1, e_2, \ldots, e_i, x_{i+1}, x_{i+2}, \ldots, x_n) x_1^{e_1} \wedge x_2^{e_2} \wedge \ldots \wedge x_i^{e_i}, \tag{6.5}$$

hoặc dưới dạng hội chính quy

$$f(x) = \prod f(e_1, e_2, \ldots, e_i, x_{i+1}, x_{i+2}, \ldots, x_n) x_1^{e_1} \vee x_2^{e_2} \vee \ldots \vee x_i^{e_i}, \tag{6.6}$$

trong đó tuyển, hội lấy trên tập $(e_1, e_2, \ldots, e_i) \in \mathbb{B}^i$.

Chứng minh. Bằng luật đối ngẫu, ta chỉ cần chứng minh biểu diễn dạng (6.5). Giả sử $(x_1, x_2, \ldots, x_n) \in T_f$. Khi đó số hạng ứng với bộ giá trị $e_1 = x_1, e_2 = x_2, \ldots, e_i = x_i$ trong tuyển vế phải của (6.5)

$$x_1^{e_1} x_2^{e_2} \ldots x_i^{e_i} f(e_1, e_2, \ldots, e_i, x_{i+1}, x_{i+2}, \ldots, x_n)$$

sẽ bằng 1. Điều này kéo theo toàn bộ vế phải bằng 1.

Ngược lại, nếu vế phải bằng 1 thì phải xảy ra tại số hạng nào đó, chẳng hạn tại số hạng tương ứng với bộ giá trị $(e_1, e_2, \ldots, e_i)$ và do đó $(x_1, x_2, \ldots, x_n) \in T_f$. □

Cho $i = 1$ trong định lý và nhận xét rằng vai trò của các biến x_i là như nhau, ta được

Hệ quả 6.5.4. *Hàm Boole f có thể được khai triển theo một đối số x_i*

$$f(x) = x_i' f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \vee x_i f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n), \tag{6.7}$$

hoặc

$$f(x) = x_i' f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \wedge x_i f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n). \tag{6.8}$$

Cho $i = n$ trong định lý và bỏ đi các phần tử bằng 1 trong một tích, ta được

Hệ quả 6.5.5. *Mọi hàm Boole có thể được khai triển dưới dạng tuyển chính quy*

$$f(x) = \sum_{e \in T_f} x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n} \tag{6.9}$$

hoặc dưới dạng hội chính quy

$$f(x) = \prod_{e \in T_f} x_1^{e_1} \vee x_2^{e_2} \vee \ldots \vee x_n^{e_n} \tag{6.10}$$

Công thức khai triển (6.9) còn được gọi là *dạng tuyển chuẩn tắc hoàn toàn* của f và mỗi số hạng của nó được gọi là một *cấu tạo đơn vị* (hay *phần tử tối thiểu)* của f.

Ví dụ 6.5.1. Dạng tuyển chính quy và dạng hội chính quy của hàm Boole có bảng chân trị

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

tương ứng là

$$f_\Sigma = x_1'x_2'x_3' + x_1'x_2x_3' + x_1'x_2x_3 + x_1x_2'x_3 + x_1x_2x_3,$$
$$f_\Pi = (x_1 + x_2 + x_3')(x_1' + x_2 + x_3)(x_1' + x_2' + x_3).$$

Như vậy dạng chính quy không những giúp chúng ta so sánh các hàm số mà còn giúp chúng ta trong việc biểu diễn hàm Boole dưới dạng biểu thức đại số từ bảng chân trị và trong việc đơn giản hóa tối thiểu các hàm Boole. Từ Hệ quả 6.5.5, ta nhận được

Hệ quả 6.5.6. *Mọi hàm Boole đều có thể xây dựng từ các biến nhờ các hàm OR, AND, và NOT.*

Ngoài hệ tuyển, hội và phủ định, tồn tại nhiều hệ khác cũng có tính chất *mọi hàm Boole đều biểu diễn qua các thành viên của hệ.* Một hệ hàm như vậy được gọi là *hệ đầy đủ.*

Hệ quả 6.5.7. *Các hệ*

(a) {AND, NOT}; *và*

(b) {OR, NOT} *là những hệ hàm đầy đủ hai biến.*

Chứng minh. (a) Thật vậy, do

$$\begin{aligned} x \vee y &= (x')' \vee (y')' \\ &= (x'y')' \end{aligned}$$

nên hàm OR được thay bằng hai hàm AND và NOT. Kết luận được suy từ Hệ quả 6.5.6.

(b) Bài tập. □

Việc nghiên cứu tính đầy đủ của một hệ hàm có ý nghĩa thực tiễn quan trọng, nó trả lời câu hỏi có thể xây dựng một hàm Boole từ một số hàm đơn giản chọn trước hay không?

Bài tập

1. Chứng minh các khai triển trong Hệ quả 3.5.5 là duy nhất.
2. Tìm dạng tuyển chính quy của hàm Boole ba biến:

   (a) xy.
   (b) z'.
   (c) $xz \vee (y' \vee y'z) \vee xy'z'$.
   (d) $x \vee yz$.
   (e) $[(xy \vee xyz) \vee xz] \vee z$.
   (f) $xy \vee z'$.
   (g) $[(x \vee y)' \vee z]'$.
   (h) $(x \vee y)' \vee z \vee x(yz \vee y'z')$.

3. Trình bày phương pháp tìm dạng hội chính quy. Cho ví dụ minh họa.
4. Sử dụng các phương pháp đại số, tìm dạng tuyển chính quy của các hàm Boole sau:

   (a) $x \vee xy$.
   (b) $(x \vee y)(x' \vee y')$.
   (c) $(yz \vee xz')(xy' \vee z)'$.
   (d) $(x'y \vee x'z')(x \vee yz)'$.
   (e) $x \vee (y' \vee (xy' \vee xz'))$.

5. Chứng minh nếu $m_1 \vee m_2 \vee \cdots \vee m_k$ là dạng tuyển chính quy của f thì $m_1' \wedge m_2' \wedge \cdots \wedge m_k'$ là dạng hội chính quy của f'. Cho ví dụ minh họa.
6. Chứng minh các hệ hàm sau là đầy đủ: {OR, NOT}, {NOR}, và {NAND}. (Hàm NAND và NOR còn ký hiệu tương ứng là $\uparrow$ và $\downarrow$).
7. Chứng minh các hệ hàm sau không đầy đủ: {AND}, {OR }, {NOT}, và {AND, OR}.
8. Chứng minh hoặc tìm phản ví dụ: $x \uparrow (y \uparrow z) = (x \uparrow y) \uparrow z$ với mọi $x, y, z \in \mathbb{B}$.
9. Biểu diễn hàm XOR qua hệ hàm NAND.

6.6 Biểu diễn tối thiểu của hàm Boole

6.6.1 Khái niệm

Biểu diễn hàm Boole qua một hệ hàm đầy đủ H là không duy nhất. Ví dụ hàm Sheffer định nghĩa bởi

$$x \uparrow y := \begin{cases} 0 & \text{nếu } x = y = 1, \\ 1 & \text{nếu ngược lại,} \end{cases}$$

khi biểu diễn qua hệ tuyển, hội và phủ định, có thể có các cách

$$x \uparrow y = x'y' \vee x'y \vee xy' = x' \vee y'.$$

Mỗi một biểu diễn f tương ứng với một cách "ghép" các thành viên của H (mà ta gọi là *các yếu tố cơ bản)* để thu được f. Hiển nhiên, một vấn đề có ý nghĩa thực tiễn quan trọng là tìm một biểu diễn sao cho việc ghép như thế tốn ít yếu tố cơ bản nhất. Theo một nghĩa nào đó, điều này dẫn về việc tìm một công thức trên hệ H biểu diễn hàm f với số ký hiệu các yếu tố này là ít nhất. Một công thức như vậy, được gọi là một *biểu diễn tối thiểu* của hàm f trong hệ H.

Về nguyên tắc, số công thức biểu diễn f là hữu hạn, nên bằng cách duyệt tất cả các khả năng, ta luôn tìm được biểu diễn tối thiểu của f. Tuy nhiên, số khả năng này là rất lớn và việc duyệt nó đòi hỏi một khối lượng tính toán khổng lồ, do đó trên thực tế khó mà thực hiện được dù rằng ngay cả với những siêu máy tính. Việc xây dựng những thuật toán hữu hiệu tìm biểu diễn tối thiểu của các hàm Boole, vì thế càng trở nên cấp bách. Nhưng đồng thời nó cũng là bài toán rất khó. Cho đến nay vẫn chưa được giải quyết thỏa đáng ngay cả trong một số trường hợp đơn giản và còn đang được tiếp tục nghiên cứu.

Một hệ đầy đủ được nghiên cứu nhiều nhất là hệ tuyển, hội và phủ định. Bài toán tìm biểu diễn tối thiểu của các hàm Boole trong hệ này đã được nghiên cứu trong vài chục năm gần đây. Như đã biết, một hàm Boole nói chung có thể biểu diễn theo nhiều biểu thức Boole khác nhau, với độ phức tạp nhiều ít cũng khác nhau. Thực chất của vấn đề tối thiểu hóa là tìm dạng biểu diễn đơn giản nhất cho một biểu thức Boole. Như vậy bài toán tối thiểu các biểu thức Boole trở thành bài toán so sánh mức độ phức tạp của các biểu thức tương đương.

Nói chung, có hai nhóm phương pháp để tối thiểu hóa các biểu thức Boole. Nhóm thứ nhất bao gồm các phương pháp biến đổi đại số các biểu thức Boole dựa trên cơ sở các đẳng thức đã giới thiệu trong phần các tính chất của đại số Boole. Các phương pháp này không tiện lợi, đòi hỏi nhiều thời gian, đặc biệt trong trường hợp có nhiều biến. Nhóm thứ hai bao gồm các phương pháp thuật toán, các phương pháp này cho phép dễ dàng tự động hoá biểu thức Boole.

6.6.2 Phương pháp bản đồ Karnaugh

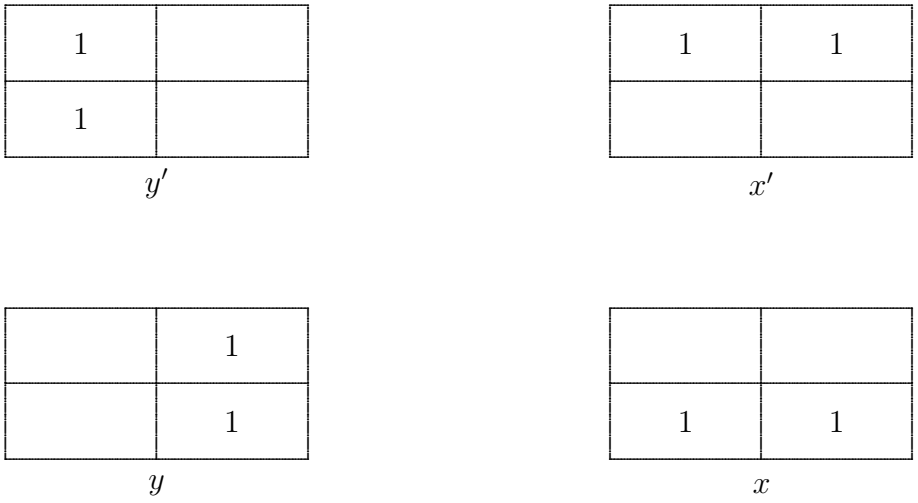
Như đã biết, thông qua Ví dụ 6.4.3, chúng ta có thể xây dựng được một hàm Boole dạng tuyển chính quy tương ứng bảng chân trị đó. Khó khăn chính là tìm một hàm Boole đã cho có dạng tối thiểu. Dưới đây chúng ta sẽ đưa ra phương pháp bản đồ Karnaugh để giải quyết khó khăn này. Phương pháp này chỉ hữu ích với số biến ít, và chúng ta sẽ hạn chế cho các trường hợp hai và ba biến.

Bản đồ Karnaugh hai biến

Bản đồ Karnaugh hai biến là một hình vuông được chia thành bốn hình vuông nhỏ hơn như trong Hình 6.6.

	y'	y
x'	$x' \wedge y'$	$x' \wedge y$
x	$x \wedge y'$	$x \wedge y$

Hình 6.6: Bản đồ Karnaugh hai biến



Hình 6.7: Kết hợp các hình vuông kề nhau

Nhận xét là mỗi hình vuông con tương ứng một-một với một phần tử tối thiểu và có đúng bốn phần tử tối thiểu trong trường hợp hai biến.

Ta nói rằng hai hình vuông con là *kề nhau* nếu chúng có chung một cạnh. Vì một hình vuông con tương ứng một phần tử tối thiểu (là biểu thức Boole hai biến) nên các hình vuông con kề nhau là biểu thức Boole một biến như Hình 6.7.

Ta minh họa phương pháp qua ví dụ sau.

Ví dụ 6.6.1. Xét hàm Boole

$$f(x, y) = (x' \wedge y) \vee (x \wedge y) \vee (x \wedge y').$$

Ta chia làm ba bước.

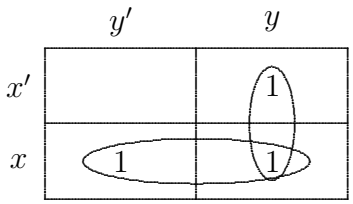
Bước 1. Vẽ một bản đồ Karnaugh và đặt 1 vào mỗi hình vuông con tương ứng với một phần tử tối thiểu của f. Ta có Hình 6.8.

Bước 2. Bây giờ vẽ các ellipse chứa các số 1 kề nhau sao cho các ellipse này chứa tất cả các số 1. Chú ý là không vẽ nhiều hơn cần thiết. Ta có Hình 6.9.

Bước 3. Với mỗi ellipse có được trong bước trước, chúng ta tổ hợp lại thành một biểu thức Boole một biến, và rồi tuyển các biến này lại để có dạng đơn giản $g(x, y)$. Trong ví dụ

	y'	y
x'		1
x	1	1

Hình 6.8:



Hình 6.9:

này ta có

$$g(x, y) = x \vee y.$$

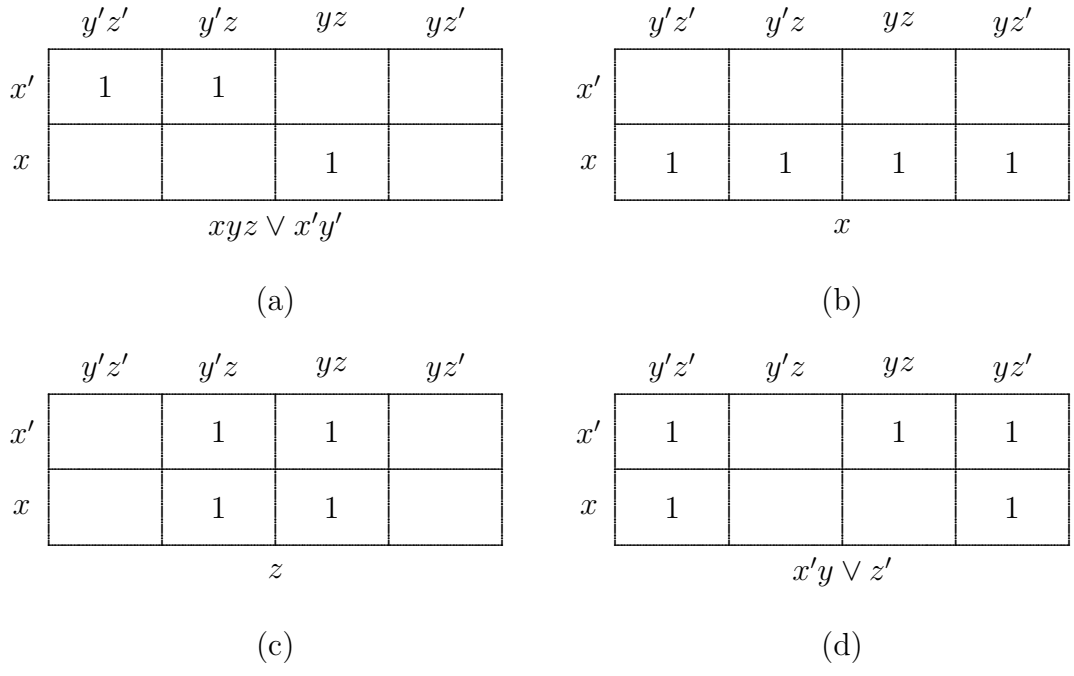
Bản đồ Karnaugh ba biến

Bản đồ Karnaugh ba biến là một hình chữ nhật được chia thành tám hình vuông con như Hình 6.10. Như trường hợp hai biến, mỗi hình vuông con được gán với một trong tám khả năng của các phần tử tối thiểu ba biến. Một trong những lý do để thuật toán Karnaugh thực hiện là hai hình vuông con kề nhau tương ứng hai phần tử tối thiểu chỉ khác nhau một biến. Tuy nhiên cần chú ý rằng, các hình vuông con ở cột đầu và cột cuối (trong cùng một hàng) là kề nhau. Trong trường hợp ba biến, mỗi hình vuông con tương ứng một phần tử tối thiểu mà là biểu thức Boole ba biến. Do đó hai hình vuông con kề nhau tương ứng một biểu thức Boole hai biến, chẳng hạn như Hình 6.11. Hơn nữa bốn hình vuông kề nhau (gọi là quadruple) tương ứng biểu thức một biến như Hình 6.12.

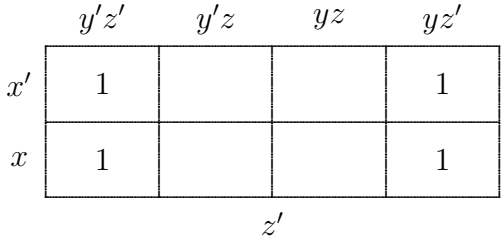
Ta minh họa phương pháp qua các ví dụ sau.

	$y'z'$	$y'z$	yz	yz'
x'	$x' \wedge y' \wedge z'$	$x' \wedge y' \wedge z$	$x' \wedge y \wedge z$	$x' \wedge y \wedge z'$
x	$x \wedge y' \wedge z'$	$x \wedge y' \wedge z$	$x \wedge y \wedge z$	$x \wedge y \wedge z'$

Hình 6.10:



Hình 6.11:



Hình 6.12:

Ví dụ 6.6.2. Xét hàm Boole

$$f(x, y, z) = (x' \wedge y' \wedge z) \vee (x \wedge y' \wedge z') \vee (x \wedge y \wedge z) \vee (x' \wedge y \wedge z).$$

Bước 1. Đầu tiên vẽ bản đồ Karnaugh và đặt trong mỗi hình vuông một số 1 tương ứng phần tử tối thiểu trong f. Ta được Hình 6.13

Bước 2. Vẽ các ellipse hay quadruple chứa các số 1 kề nhau sao cho phủ tất cả các số 1 và không sử dụng các ellipse hay quadruple hơn số cần thiết. Ta có Hình 6.14.

(Chú ý rằng, nếu có thể, hãy sử dụng các quadruple như Ví dụ 6.6.3 dưới đây).

Bước 3. Bây giờ với mỗi ellipse (hoặc quadruple) ta có tương ứng một biểu thức một hoặc hai biến. Tuyển các biểu thức này ta được hàm tối thiểu

$$g(x, y, z) = (x \wedge y' \wedge z') \vee (x' \wedge z) \vee (y \wedge z).$$

	$y'z'$	$y'z$	yz	yz'
x'		1	1	
x	1		1	

Hình 6.13:

	$y'z'$	$y'z$	yz	yz'
x'		1	1	
x	1		1	

Hình 6.14:

Ví dụ 6.6.3. Xét hàm Boole

$$f(x, y, z) = (x' \wedge y' \wedge z') \vee (x \wedge y \wedge z) \vee (x \wedge y' \wedge z) \vee (x' \wedge y' \wedge z) \vee (x' \wedge y \wedge z) \vee (x' \wedge y \wedge z').$$

Bước 1. Ta có bản đồ Karnaugh và đặt số 1 vào các hình vuông tương ứng các phần tử tối thiểu (Hình 6.15).

	$y'z'$	$y'z$	yz	yz'
x'	1	1	1	1
x		1	1	

Hình 6.15:

Bước 2. Vẽ các ellipse hay các quadruple của các số 1 kề nhau sao cho phủ tất cả các số 1 và không vẽ thừa. Có thể làm ba cách như sau

Sử dụng Hình 6.16(a) ta có

$$g_1(x, y, z) = x' \vee (x \wedge z).$$

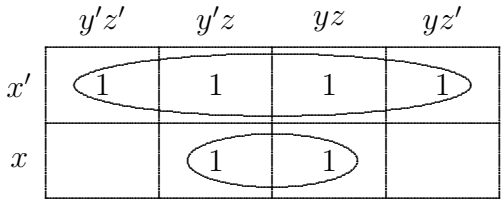
Sử dụng Hình 6.16(b) ta có

$$g_2(x, y, z) = z \vee (x' \wedge z').$$

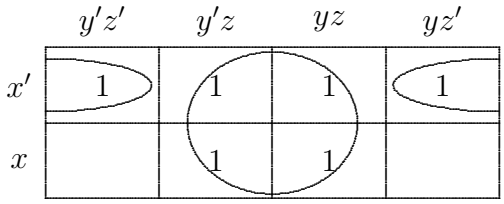
Sử dụng Hình 6.16(c) ta có

$$g_3(x, y, z) = x' \vee z.$$

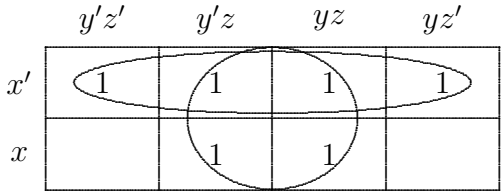
Hiển nhiên hàm g_3 là hàm đơn giản nhất!



(a)



(b)



(c)

Hình 6.16:

Bài tập

1. Vẽ các bản đồ Karnaugh và tìm dạng tuyển chính tắc tối thiểu của các hàm Boole hai biến:

   (a) $xy + xy'$. (b) $xy + x'y + x'y'$. (c) $xy + x'y'$.

2. Vẽ các bản đồ Karnaugh và tìm dạng tuyển chính tắc tối thiểu của các hàm Boole ba biến:

   (a) $x \vee x'yz$. (b) $(x \vee yz)'$. (c) $y'z \vee xyz$.
   (d) $(y \vee z)$. (e) $xz \vee yz$. (f) $xy \vee xz \vee yz$.
   (g) $xyz \vee xy'z' \vee x'yz' \vee x'y'z$. (h) $xy \vee yz \vee zx$. (h) $xy \wedge yz \wedge zx$.

Chương 7

MÃ TUYẾN TÍNH

Lý thuyết mã bắt đầu hình thành và phát triển từ năm 1940 với những kết quả rất cơ bản của M. J. E. Golay, R. W. Hamming và C. E. Shannon. Mặc dù ban đầu là bài toán của kỹ sư, nhưng vấn đề đã được phát triển sử dụng rất nhiều công cụ toán học. Chương này trình bày lý thuyết các mã phát hiện và sửa sai ở mức độ đơn giản nhất. Qua đó người đọc có thể thấy rõ mối liên hệ mật thiết với những bài toán đặt ra do sự phát triển công nghệ viễn thông.

7.1 Mở đầu

7.1.1 Khái niệm

Cách thông thường để biểu diễn, lưu trữ và truyền thông tin là sử dụng chuỗi các bit, tức là dãy các số 0 và 1. Thật là khó khăn và thường không thể ngăn ngừa các lỗi xảy ra khi dữ liệu được lưu trữ, phục hồi, xử lý hay được truyền từ nơi này sang nơi này khác. Các lỗi có thể xuất hiện do tiếng ồn của kênh thông tin, do nhiễu, do con người hay do thiết bị. Các lỗi cũng có thể xảy ra khi dữ liệu được lưu trữ trong thời gian dài trên các băng từ

Độ tin cậy của dữ liệu nhận được từ các tập tin lớn hay khi dữ liệu được gửi từ một nơi rất xa là quan trọng. Tương tự, việc phục hồi dữ liệu được lưu trữ khắp nơi trên băng từ cũng là vấn đề đáng quan tâm.

Lý thuyết mã nảy sinh từ bài toán đảm bảo độ tin cậy hay phục hồi dữ liệu. Các bản tin ở dạng chuỗi bit được *mã hóa* thành chuỗi bit dài hơn gọi là *từ mã*. *Bộ mã* là tập hợp các từ mã.

Chúng ta có thể phát hiện các lỗi khi sử dụng các bộ mã nào đó. Tức là, nếu không có quá nhiều lỗi, chúng ta có thể xác định được các lỗi xảy ra khi truyền dữ liệu. Hơn nữa,

với một vài bộ mã, chúng ta có thể sửa được các lỗi đó. Nói cách khác, nếu không có quá nhiều lỗi xảy ra trong đường truyền, chúng ta có thể phục hồi từ mã từ chuỗi bit nhận được.

Lý thuyết mã ra đời từ năm 1940 nhằm nghiên cứu các bộ mã, bao gồm *phát hiện* và *sửa sai* các lỗi. Sự phát triển công nghệ mới nhằm truyền và lưu dữ liệu khiến cho việc nghiên cứu lý thuyết mã càng trở nên quan trọng. Chương này giới thiệu sơ lược về việc phát hiện lỗi và sửa sai lỗi với hai giả thiết:

1. Xác suất truyền bit 1 và nhận được bit 0 bằng xác suất truyền bit 0 nhận bit 1 và bằng p với $0 \leq p < \frac{1}{2}$ (gọi là *kênh đối xứng nhị phân*).
2. Các bit được truyền một cách độc lập.

7.1.2 Mã phát hiện lỗi

Cách đơn giản để phát hiện các lỗi khi một chuỗi bit được truyền là thêm một bit kiểm tra chẵn lẻ vào cuối chuỗi: chúng ta mã hoá bản tin $x_1x_2 \dots x_n$ thành từ mã $x_1x_2 \dots x_{n+1}$, trong đó

$$x_{n+1} = (x_1 + x_2 + \cdots + x_n) \bmod 2.$$

Việc thêm bit chẵn lẻ bảo đảm rằng số các số 1 trong từ mã phải là số chẵn. Dễ dàng thấy rằng trong bộ mã này, các từ mã là các chuỗi bit với một số chẵn các số 1.

Nhận xét 15. Nếu một lỗi xuất hiện, số các số 1 trong chuỗi nhận được là một số lẻ, do đó lỗi này được phát hiện. Nếu hai lỗi xuất hiện, số các số 1 trong chuỗi nhận được là một số chẵn, do đó các lỗi này không được phát hiện. Tổng quát một số lẻ các lỗi có thể được phát hiện, trong khi một số chẵn các lỗi thì không.

Ví dụ 7.1.1. Nếu nhận được chuỗi bit 1110011 thì đây là từ mã không hợp lệ.

Ví dụ 7.1.2. Nếu nhận được chuỗi bit $y = 10111101$ thì hoặc y là từ mã hợp lệ, hoặc có một số chẵn lỗi xảy ra.

Một cách đơn giản khác để phát hiện lỗi là *lặp* mỗi bit trong một thông báo hai lần như ví dụ sau.

Ví dụ 7.1.3. Chuỗi 011001 được mã hóa thành từ mã 001111000011.

Nhận xét 16. Chúng ta có thể phát hiện các lỗi trong bit thứ 2, 3 và thứ 8 của các từ mã có 8 bit (như khi từ mã 00001111 gởi và nhận được 01101110 là có lỗi). Mặt khác, không thể phát hiện ra lỗi nếu bit thứ 3, 4 bị thay đổi (như khi 00111111 nhận được từ mã 00001111 là có lỗi).

Chúng ta đã thảo luận hai bộ mã có thể dùng để phát hiện lỗi. Khi các lỗi được phát hiện, chúng ta có thể yêu cầu truyền lại và hy vọng rằng không có lỗi nào xuất hiện. Tuy nhiên, có các bộ mã không chỉ phát hiện sai mà còn sửa chữa các lỗi sai (nếu có).

7.1.3 Mã sửa sai

Để phát hiện lỗi, trong các ví dụ trước, chúng ta xây dụng từ mã bằng cách thêm các bit thích hợp vào bản tin. Chúng ta không chỉ phát hiện các lỗi mà còn sửa chúng nếu thêm nhiều bit hơn vào bản tin. Chính xác hơn, nếu các lỗi là đủ ít, chúng ta có thể xác định từ mã nào được truyền.

Ví dụ 7.1.4. Mã hóa một bản tin, chúng ta có thể dùng *mã lặp ba lần.* Chẳng hạn, nếu thông báo là $x_1x_2x_3$, chúng ta mã hóa nó thành từ mã $x_1x_2x_3x_4x_5x_6x_7x_8x_9$, trong đó $x_1 = x_4 = x_7, x_2 = x_6 = x_8, x_3 = x_5 = x_9$.

Các từ mã hợp lệ là

$$\begin{array}{llll} 000000000, & 001001001, & 010010010, & 011011011, \\ 100100100, & 101101101, & 111111111. & \end{array}$$

Chúng ta phát hiện một chuỗi bit nhận được có lỗi bằng cách sử dụng "luật số lớn". Chẳng hạn để xác định x_1, xét các bit x_1, x_4, x_7. Nếu hai trong ba bit bằng 1, ta kết luận $x_1 = 1$, ngược lại kết luận $x_1 = 0$.

Bài tập

1. Các chuỗi bit nhận được sau có thể là đúng (sử dụng bit kiểm tra chẵn lẻ):
   (a) 1000011.
   (b) 111111000.
   (c) 10101010101.
   (d) 110111011100.

2. Các chuỗi bit nhận được sau có thể là đúng (lặp mỗi bit trong thông báo hai lần):
   (a) 110011.
   (b) 1100000011.
   (c) 101111.

3. Các bản tin được lặp ba lần. Sửa sai các chuỗi bit nhận được sau (nếu sai):
   (a) 111000101.
   (b) 110000001.
   (c) 111011111000.

7.2 Các khái niệm

Trong chương này, giả thiết mỗi bản tin $u \in \mathbb{B}^k$ được mã hoá thành các "từ mã" $x \in \mathbb{B}^n, n > k$. Để đơn giản, ta sẽ đồng nhất vector cột $x = (x_1, x_2, \ldots, x_n)^t$ với chuỗi bit $x_1x_2\ldots x_n$.

Định nghĩa 7.2.1. Không gian vector con k chiều C của không gian vector $\mathbb{B}^n$ trên trường $\mathbb{B}$ gọi là $[n,k]$-*mã tuyến tính*. n được gọi là *độ dài* của bộ mã và $\dim C := k$ là *chiều*. *Hệ số* của bộ mã là tỉ số k/n. Các phần tử của C gọi là các *từ mã*.

Nói cách khác, tập con C của $\mathbb{B}^n$ là một mã tuyến tính nếu

(a) $x + y \in C$ với mọi $x, y \in C$; và

(b) $\alpha x \in C$ với mọi $x \in C, \alpha \in \mathbb{B}$.

Từ định nghĩa ta thấy rằng, $[n,k]$ mã tuyến tính C hoàn toàn được xác định bởi tập bất kỳ các từ mã độc lập tuyến tính $x^1, x^2, \ldots, x^k$ vì mỗi từ mã $x \in C$ đều có thể biểu diễn dạng

$$x = \sum_{i=1}^{k} \alpha_i x^i \qquad (\text{mod } 2),$$

trong đó $\alpha_i \in \mathbb{B}$. Nếu chúng ta sắp xếp các từ mã này thành một ma trận Boole G cấp $k \times n$ ta sẽ được một *ma trận sinh* của mã C. Chính xác hơn:

Định nghĩa 7.2.2. Giả sử C là $[n,k]$-mã tuyến tính. Ma trận Boole G cấp $k \times n$ mà các hàng của nó sinh ra không gian vector C gọi là *ma trận sinh* của C. Ngược lại, nếu G là ma trận Boole cấp $k \times n$ thì không gian vector sinh bởi các hàng của nó gọi là *mã sinh bởi* G.

Nhận xét 17. Một mã có thể có nhiều ma trận sinh khác nhau. Chẳng hạn các ma trận

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

cùng là các ma trận sinh của mã với các phần tử:

$$\begin{aligned} c^1 &= 0\,0\,0\,0 \\ c^2 &= 0\,1\,0\,1 \\ c^3 &= 1\,1\,1\,0 \\ c^4 &= 1\,0\,1\,1 \end{aligned}$$

Ví dụ 7.2.1. $[5,1]$-mã tuyến tính C_1 với ma trận sinh

$$G_1 := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

chứa hai từ mã là 00000 và 11111.

Ví dụ 7.2.2. $[5,3]$-mã tuyến tính C_2 với ma trận sinh

$$G_2 := \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Ví dụ 7.2.3. $[7,4]$-mã tuyến tính C_3 với ma trận sinh

$$G_3 := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Do $[n,k]$-mã tuyến tính C có 2^k từ mã nên ta có thể truyền đi tối đa 2^k bản tin khác nhau; nếu giả thiết các hàng của ma trận G độc lập tuyến tính thì bản tin $u \in \mathbb{B}^k$ sẽ được mã hoá thành vector

$$x = u^t G. \tag{7.1}$$

Chẳng hạn, sử dụng ma trận sinh G_2 của Ví dụ 7.2.2 ta có

$$\begin{cases} x_1 = u_1 + u_3, \\ x_2 = u_1 + u_3, \\ x_3 = u_1 + u_2 + u_3, \\ x_4 = u_2 + u_3, \\ x_5 = u_3. \end{cases}$$

Ký hiệu M là số phần tử của mã C (độ dài n). Ta biểu diễn các phần tử của C bằng một mảng kích thước $M \times n$ mà các hàng là các từ mã.

Giả sử π là hoán vị của tập $\{1, 2, \ldots, n\}$ và với mỗi từ mã $x \in C$ ta áp dụng phép biến đổi, gọi là *hoán vị vị trí,*

$$\pi \colon x \mapsto x'$$

xác định bởi

$$x'_i := x_{\pi(i)}, \qquad i = 1, 2, \ldots, n.$$

Tương tự, nếu π là hoán vị của các ký hiệu $\{0, 1\}$, ta nói π cảm sinh một phép *hoán vị ký hiệu* nếu với chỉ số i nào đó, và với mỗi từ mã $x \in C$ ta áp dụng phép biến đổi

$$x \mapsto x',$$

trong đó x' xác định bởi

$$x'_j := \begin{cases} x_j & \text{nếu } i \neq j, \\ \pi(x_i) & \text{nếu } i = j. \end{cases}$$

Nếu mã C' có thể nhận được từ mã C bằng một dãy các phép hoán vị vị trí hoặc phép hoán vị ký hiệu thì ta nói hai mã C và C' là *tương đương.*

Ví dụ 7.2.4. (a) Hai mã sau là tương đương bằng cách sử dụng hoán vị $\pi(\{1,2,3,4\}) = \{1,3,2,4\}$:

$$\begin{matrix}0&0&0&0\\0&0&1&1\\1&1&0&0\\1&1&1&1\end{matrix} \quad \text{và} \quad \begin{matrix}0&0&0&0\\0&1&0&1\\1&0&1&0\\1&1&1&1\end{matrix}.$$

(b) Mã

$$C := \begin{pmatrix}0&0&1&0&0\\0&0&0&1&1\\1&1&1&1&1\\1&1&0&0&0\end{pmatrix}$$

tương đương với mã

$$C' := \begin{pmatrix}0&0&0&0&0\\0&1&1&0&1\\1&1&0&1&1\\1&0&1&1&0\end{pmatrix}$$

qua phép hoán vị

$$\begin{pmatrix}0&1\\\downarrow&\downarrow\\1&0\end{pmatrix}$$

các ký hiệu ở vị trí thứ ba trong C và sau đó hoán vị hai vị trí thứ 2 và thứ 4.

Bổ đề 7.2.3. *Hai ma trận Boole cùng cấp $k \times n$ sinh ra hai mã tuyến tính tương đương nếu chúng nhận được từ nhau bằng dãy các phép toán:*

(a) hoán vị các hàng;

(b) cộng hai hàng; và

(c) hoán vị các cột.

Chứng minh. Các phép toán trên hàng (a) và (b) không thay đổi hạng của ma trận sinh (chỉ thay đổi các vector cơ sở). Phép toán (c) tương đương với hoán vị vị trí các từ mã. □

Ví dụ 7.2.5. (a) Ma trận sinh G_1 và G_3 có dạng *bậc thang*, tức ma trận có các tính chất:

1. Phần tử khác không bên trái nhất trong mỗi hàng bằng 1.
2. Cột chứa phần tử bên trái nhất của một hàng bằng 1 có tất cả các phần tử khác bằng 0.

3. Nếu phần tử bằng 1 bên trái nhất trong hàng thứ i xuất hiện ở cột t_i thì

$$t_1 < t_2 < \cdots < t_n.$$

(b) Ma trận G_2 có thể đưa về ma trận bậc thang

$$G_2' := \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Sử dụng G_2' cho bộ mã C_2, mã hoá (7.1) có dạng

$$\begin{cases} x_1 = u_1, \\ x_2 = u_1, \\ x_3 = u_2, \\ x_4 = u_3, \\ x_5 = u_1 + u_3. \end{cases}$$

Điều này chỉ ra rằng các ký hiệu bản tin u_1, u_2, u_3 xuất hiện tường minh trong các từ mã; nói chung, ký hiệu u_i sẽ xuất hiện tại vị trí thứ t_i của từ mã $x = u^t G$ nếu phần tử bên trái nhất của hàng thứ i của G xuất hiện trong cột thứ t_i.

Nhận xét rằng, các ma trận bậc thang của mã C_1 và C_3 có dạng $G = (I_k\ A)$, trong đó I_k là ma trận đơn vị cấp k. Áp dụng phương pháp của Bổ đề 7.2.3, ma trận G_2' có thể đưa về

$$G_2'' := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Tổng quát ta có

Định lý 7.2.4. *Giả sử C là $[n,k]$-mã. Khi đó tồn tại mã C' tương đương C với ma trận sinh dạng $(I_k\ A)$.*

Chứng minh. Bài tập. □

Theo kết quả trên, ta luôn có thể giả thiết ma trận sinh G có dạng $(I_k \mid A)$.

Định nghĩa 7.2.5. Giả sử C là $[n,k]$-mã tuyến tính và H là ma trận Boole cấp $(n-k)\times n$. H gọi là *ma trận kiểm tra chẵn lẻ* của C nếu với mọi từ mã $x \in C$ ta có

$$Hx = 0 \qquad (\text{mod } 2). \tag{7.2}$$

Hệ (7.2) được gọi là *hệ phương trình kiểm tra chẵn lẻ.*

Ví dụ 7.2.6. $[4,3]$-mã C_4 bằng cách thêm một bit kiểm tra chẵn lẻ trong Phần 7.1.2: Bản tin $u_1u_2u_3$ được mã hóa thành từ mã $x = x_1x_2x_3x_4$, trong đó

$$x_1 = u_1, x_2 = u_2, x_3 = u_3,$$

và

$$x_1 + x_2 + x_3 + x_4 = 0.$$

Do đó nếu bản tin là $u = 101$ thì từ mã là $x = 1010$. Có $2^3 = 8$ từ mã là

$$\begin{array}{cccc} 0000 & 0011 & 0101 & 1001 \\ 1010 & 0110 & 1100 & 1111. \end{array}$$

Tức là tất cả các vector có một số chẵn số bit bằng 1. Dễ dàng thử lại ma trận kiểm tra chẵn lẻ của C_4 là $H_5 = (1\ 1\ 1\ 1)$.

Ví dụ 7.2.7. Xét $[6,3]$-mã lặp C_5 : Bản tin $u_1u_2u_3$ được mã hóa thành từ mã $x = x_1x_2\dots x_6$, trong đó

$$x_1 = u_1, x_2 = u_2, x_3 = u_3,$$

và

$$\begin{cases} x_2 + x_3 + x_4 = 0, \\ x_1 + x_3 + x_5 = 0, \\ x_1 + x_2 + x_6 = 0. \end{cases}$$

Mã C_5 có ma trận kiểm tra chẵn lẻ:

$$H := \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Định lý 7.2.6. *Giả sử G và H là các ma trận với các hàng độc lập tuyến tính có kích thước tương ứng $k \times n$ và $(n-k) \times n$. Khi đó G và H là các ma trận sinh và ma trận kiểm tra chẵn lẻ của một mã nếu và chỉ nếu $GH^t = 0$.*

Chứng minh. Giả sử $GH^t = 0$. Khi đó mỗi hàng của G là nghiệm của hệ phương trình (7.2) và do đó không gian sinh bởi tất cả các tổ hợp tuyến tính của các hàng của G chứa trong không gian các nghiệm của (7.2). Nhưng cả hai không gian này có chiều bằng k nên chúng bằng nhau. Bằng cách suy luận tương tự ta có chiều ngược lại. □

Ví dụ 7.2.8. Các mã C_1, C_2, C_3 trong các ví dụ trên có các ma trận kiểm tra chẵn lẻ tương ứng là

$$H_1 := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad H_2 := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

và

$$H_3 := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Nhận xét rằng nếu $G = (I_k\ A)$ thì ma trận kiểm tra chẵn lẻ có dạng $H = (A^t\ I_{n-k})$. Khi đó hệ phương trình kiểm tra chẵn lẻ (7.2) cho một phụ thuộc hàm tường minh giữa các ký hiệu bản tin (các bit thông tin) và các ký hiệu kiểm tra. Ma trận sinh và ma trận kiểm tra chẵn lẻ của mã tuyến tính không chỉ có ý nghĩa về mặt lý thuyết mà nó còn có những ứng dụng chủ yếu trong việc mã hoá và giải mã. Thật vậy, mỗi bản tin $u \in \mathbb{B}^k$ được mã hoá duy nhất thành từ mã $x = u^tG$. Vì các hàng của ma trận sinh độc lập tuyến tính nên ánh xạ $u \mapsto u^tG$ là song ánh từ $\mathbb{B}^k$ lên C. Việc giải mã khó khăn hơn sẽ được trình bày trong mục tiếp theo.

Ví dụ 7.2.9. (a) Mã C_1 có $x_1 = u_1$ là bit thông tin và các ký hiệu còn lại là các bit kiểm tra: $x_2 = x_3 = x_4 = x_5 = x_1$. Do đó C_1 có hai từ mã là 00000 và 11111.

(b) Mã C_2 có x_1, x_3, x_4 là các bit thông tin và các ký hiệu còn lại là các bit kiểm tra: $x_2 = x_1, x_5 = x_1 + x_3 + x_4$. Do đó C_2 có $2^3 = 8$ từ mã là

$$\begin{array}{cccc} 00000 & 10000 & 01000 & 00100 \\ 11000 & 10100 & 01100 & 11100. \end{array}$$

(c) Mã C_3 có x_1, x_2, x_3, x_4 là các bit thông tin và các ký hiệu còn lại là các bit kiểm tra:

$$\begin{cases} x_5 = x_2 + x_3 + x_4, \\ x_6 = x_1 + x_3 + x_4, \\ x_7 = x_1 + x_2 + x_4, \end{cases}$$

Do đó C_3 có $2^4 = 16$ từ mã (hãy liệt kê chúng!).

Trên $\mathbb{B}^n$ xét *tích vô hướng* của hai vector định nghĩa bởi

$$\langle x, y\rangle := \sum_{i=1}^{n} x_i y_i \pmod 2.$$

Chú ý rằng, khác với tích vô hướng thông thường trên không gian Euclide, có thể xảy ra $\langle x, x\rangle = 0$ với vector $x \neq 0$ nào đó.

Định nghĩa 7.2.7. *Mã đối ngẫu* hay *mã trực giao*, ký hiệu $C^\perp$, của mã tuyến tính C xác định bởi

$$C^\perp := \{y \in \mathbb{B}^n \mid \langle x, y\rangle = 0 \text{ với mọi } x \in C\}.$$

Dễ dàng thấy rằng $C^\perp$ là mã tuyến tính thoả $\dim C + \dim C^\perp = n$. Hơn nữa

Định lý 7.2.8. *Với mọi mã tuyến tính C, ma trận kiểm tra chẵn lẻ của $C^\perp$ bằng ma trận sinh của C và ngược lại.*

Chứng minh. Bài tập. □

Bài tập

1. Giả sử H là ma trận Boole cấp $r \times n$. Chứng minh tập $C := \{x \in \mathbb{B}^n | Hx = 0\}$ là mã tuyến tính.

2. Chứng minh nếu C là $[n, k]$-mã thì

$$\hat{C} := \{(x, x_{n+1}) \in \mathbb{B}^n \times \mathbb{B}^1 | x = x_1 x_2 \dots x_n \in C, x_{n+1} := x_1 + x_2 + \dots + x_n\}$$

   cũng là mã tuyến tính (gọi là *mã mở rộng*). Tìm mối liên hệ giữa các ma trận kiểm tra chẵn lẻ của C và $\hat{C}$.

3. Chứng minh rằng trong một mã nhị phân tuyến tính, hoặc tất cả các từ mã bắt đầu bằng số 0, hoặc có chính xác một nửa bắt đầu bằng số 0, và một nửa bắt đầu bằng số 1.

4. Đưa các ma trận sinh sau về dạng chuẩn $(I_k \ A)$:

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

5. Chứng minh rằng các ma trận sinh

$$G := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \qquad G' := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

   sinh ra các mã tương đương.

6. Chứng minh rằng các ma trận sinh

$$G := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \qquad G' := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

   sinh ra các mã tương đương.

7. Giả sử C có ma trận sinh

$$G := \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

   Tìm ma trận A sao cho mã có ma trận sinh $(I_3 \ A)$ tương đương với C. Liệt kê tất cả các từ mã của C.

8. Giả sử mã C có ma trận sinh dạng chuẩn $(I_k \ A)$. Chứng minh hoán vị các hàng của A cho ma trận sinh của mã tương đương C.

9. Chứng minh rằng quan hệ "mã tương đương" là quan hệ tương đương.

10. Giả sử C là $[n,k]$-mã và $a \in \mathbb{B}^n$. Chứng minh rằng tồn tại mã C' chứa a và tương đương với C.

11. Chứng minh số các mã không tương đương với độ dài n và chứa hai từ mã là n.

12. Giả sử C là $[7,4]$-mã tuyến tính với ma trận sinh

$$G := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

    Mã hoá các bản tin: $0000, 1000$ và 1110.

13. Tìm ma trận sinh và các từ mã của $[6,3]-$mã có ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

14. (Mã lặp) Tìm ma trận sinh và các từ mã của $[5,1]-$mã có ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

15. (Mã trọng lượng chẵn) Cho ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

    Tìm ma trận sinh và các từ mã.

16. Tìm ma trận sinh và các từ mã có ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

17. Cho ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

    Liệt kê tất cả các từ mã.

18. Cho ma trận kiểm tra chẵn lẻ:

$$H := \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Tìm ma trận sinh và các từ mã.

19. Tìm ma trận kiểm tra chẵn lẻ tương ứng với mã được thiết lập bằng cách thêm một bit kiểm tra chẵn lẻ đối với chuỗi bit độ dài 4.

20. Tìm ma trận kiểm tra chẵn lẻ tương ứng với mã lặp ba đối với chuỗi bit độ dài 3.

21. Tìm ma trận kiểm tra chẵn lẻ H nếu ma trận sinh là

$$G := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

22. Tìm các mã đối ngẫu của các mã C_2 và C_3 trong các Ví dụ 4.2.2 và 4.2.3.

23. Tìm các mã đối ngẫu của các mã sau:

$$C_1 := \begin{Bmatrix} 0000 \\ 1100 \\ 0011 \\ 1111 \end{Bmatrix}, \qquad C_2 := \begin{Bmatrix} 000 \\ 110 \\ 011 \\ 101 \end{Bmatrix}.$$

24. (a) Chứng minh rằng $(C^\perp)^\perp = C$.

(b) Đặt $C + D := \{x + y | x \in C, y \in D\}$. Chứng minh $(C + D)^\perp = C^\perp + D^\perp$.

25. Ký hiệu E_n là tập tất cả các vector độ dài n có trọng lượng chẵn.

(a) Chứng minh E_n là mã tuyến tính. Tìm các tham số $[n, k]$, ma trận kiểm tra chẵn lẻ và ma trận sinh của E_n.

(b) Tìm mã $E_n^\perp$.

7.3 Khoảng cách Hamming

Định nghĩa 7.3.1. *Khoảng cách Hamming*, ký hiệu $d(x, y)$, giữa hai vector $x = x_1x_2 \dots x_n$ và $y = y_1y_2 \dots y_n$ là số các vị trí i mà $x_i \neq y_i, i = 1, 2, \dots, n$.

Nhận xét rằng $d(x, y)$ chính là số lần thay đổi cần thiết từng bit từ x sang y.

Ví dụ 7.3.1. $d(10111, 00101) = 2, \qquad d(0111, 0000) = 3.$

Định lý 7.3.2. *Khoảng cách Hamming $d(x, y)$ là một metric, tức là*

(a) $d(x, y) \geq 0$ *với mọi* $x, y \in C$; *dấu bằng xảy ra khi và chỉ khi* $x = y$.

(b) $d(x, y) = d(y, x)$.

(c) $d(x, y) \leq d(x, z) + d(z, y)$ *với mọi* $x, y, z \in C$.

Chứng minh. Hai khẳng định đầu suy trực tiếp từ định nghĩa.

Chứng minh (c): Nhận xét rằng

$$\{i \mid x_i \neq y_i\} \subset \{i \mid x_i \neq z_i\} \cup \{i \mid z_i \neq y_i\},$$

vì nếu $x_i \neq y_i$ thì hoặc $x_i \neq z_i$ hoặc $z_i \neq y_i$. Suy ra

$$\#\{i \mid x_i \neq y_i\} \leq \#\{i \mid x_i \neq z_i\} + \#\{i \mid z_i \neq y_i\}.$$

Áp dụng nguyên lý bao hàm-loại trừ và bất đẳng thức:

$$\#(A \cup B) = \#A + \#B - \#(A \cap B) \leq \#A + \#B$$

ta có điều cần chứng minh. □

Giả sử rằng một bản tin được mã hóa thành từ mã $x \in C$ được gửi đi và nhận được vector y. Có hai trường hợp xảy ra

(a) Hoặc $y \in C$ khi đó $y = x$.

(b) Hoặc $y \notin C$ khi đó vector lỗi $e := y - x \neq 0$.

Trong trường hợp (b), vấn đề đặt ra là làm sao sửa được lỗi sai, phục hồi được từ mã x từ vector nhận được y?

Phương pháp giải mã đưa ra ở đây, gọi là *giải mã theo lân cận gần nhất,* nhằm tính khoảng cách Hamming giữa y với mỗi từ mã trong C. Để giải mã y, chúng ta tìm từ mã x có khoảng cách Hamming đến y nhỏ nhất. Nếu

(+) khoảng cách giữa hai từ mã gần nhất trong C đủ lớn; và

(+) nếu các lỗi đủ ít;

thì x là duy nhất-chính là từ mã được gửi.

Ví dụ 7.3.2. Giả sử $C = \{0000, 1110, 1011, 1111\}$. Thì

$$d(0000, 0110) = 2, \quad d(1110, 0110) = 1, \quad d(1011, 0110) = 3.$$

Do đó nếu nhận được $y = 0110 \notin C$ thì chúng ta kết luận (giải mã theo lân cận gần nhất) từ mã gửi là 1110.

Giả sử mỗi bit gửi đi có cùng xác suất sai $p, 0 \leq p < 1/2$. Chúng ta gọi kênh như thế là *kênh đối xứng nhị phân.*

Ví dụ 7.3.3. Ký hiệu $P(X)$ là xác suất xảy ra biến cố X. Ta có trong kênh đối xứng nhị phân

$$\begin{aligned} P(\{e = 00000\}) &= (1-p)^5, \\ P(\{e = 01000\}) &= p(1-p)^4, \\ P(\{e = 10010\}) &= p^2(1-p)^3. \end{aligned}$$

Một cách tổng quát, nếu v là vector có a bit bằng 1 thì

$$P(\{e = v\}) = p^a(1-p)^{n-a}.$$

Vì $p < 1/2$ nên $1 - p > p$; do đó

$$(1-p)^n > p(1-p)^{n-1} > p^2(1-p)^{n-2} > \cdots$$

Phương pháp giải mã *hợp lý nhất* như sau: Giả sử nhận được vector y, chúng ta tìm từ mã x sao cho xác suất $P(x|y)$ của sự kiện truyền từ mã x với điều kiện nhận được y là cực đại. Nói cách khác, tìm một từ mã hợp lý nhất trong bộ mã tương ứng với thông báo nhận được.

Định lý 7.3.3. *Giả sử tất cả các từ mã được truyền với cùng khả năng và sử dụng kênh đối xứng nhị phân. Khi đó giải mã hợp lý nhất trùng với giải mã theo lân cận gần nhất.*

Chứng minh. Trong kênh đối xứng nhị phân, nếu $d(x, y) = d$ thì có d lỗi khi thay đổi từ x sang y; do đó xác suất có điều kiện $P(y|x)$ của sự kiện nhận được y với điều kiện từ mã x được truyền là $p^d(1-p)^{n-d}$. Mặt khác, theo giả thiết, xác suất truyền từ mã x là $P(x) = \frac{1}{\#C}$. Do đó

$$P(x|y) = p^d(1-p)^{n-d}(1/\#C)P(\text{nhận được } y),$$

là hàm giảm theo d. Vậy $P(x|y)$ cực đại khi x là từ mã gần với y nhất. □

Định nghĩa 7.3.4. *Khoảng cách* (Hamming) của bộ mã C, ký hiệu $d(C)$, là khoảng cách nhỏ nhất giữa hai từ mã khác nhau, tức là

$$d(C) := \min\{d(x, y) \mid x, y \in C, x \neq y\}.$$

$[n, k]$-mã C với khoảng cách d được ký hiệu là $[n, k, d]$-mã.

Ví dụ 7.3.4. (a) Với $C = \{00000000, 11111000, 01010111, 10101111\}$ thì $d(C) = 5$.

(b) Với $C = \{000000, 111111\}$, thì $d(C) = 6$.

Khoảng cách Hamming xác định khả năng phát hiện và/hoặc sửa sai các lỗi.

Định lý 7.3.5. *Mã C có thể phát hiện được k lỗi nếu và chỉ nếu $d(C) \geq k + 1$.*

Chứng minh. $\Rightarrow$ Bằng phản chứng. Giả sử C có thể phát hiện k lỗi và $d(C) \leq k$. Khi đó tồn tại $a, b \in C$ sao cho $d(a, b) = d(C) \leq k$. Nói cách khác a và b chỉ khác nhau nhiều nhất k vị trí. Do đó sẽ xuất hiện k lỗi khi truyền từ mã a và nhận được từ mã b. Vì vậy người nhận không thể phát hiện được các lỗi này.

$\Leftarrow$ Giả sử $d(C) \geq k+1$, và khi truyền từ mã x ta nhận được y với $d(x, y) \leq k$. Do khoảng cách giữa hai từ mã ít nhất là $k + 1$, thì từ mã truyền phải là x. Vì vậy người nhận có thể phát hiện được các lỗi này. □

Giả sử $k \in \mathbb{N}$. Ta nói C có thể *sửa k lỗi* nếu với mọi thông báo nhận được $y \in \mathbb{B}^n$ tồn tại nhiều nhất một từ mã x sao cho $d(x, y) \leq k$. Điều này có nghĩa rằng, nếu một từ mã được truyền và có nhiều nhất k lỗi thì giải mã theo lân cận gần nhất sẽ thu được đúng một từ mã được truyền.

Định lý 7.3.6. *Mã C có thể sửa k lỗi nếu và chỉ nếu $d(C) \geq 2k + 1$.*

Chứng minh. $\Rightarrow$ Giả sử C có thể sửa được k lỗi. Nếu $d(C) \leq 2k$ thì tồn tại hai từ mã a và b khác nhau l vị trí, với $l \leq 2k$. Thay đổi $[l/2]$ bit trong a sao cho có vector c chỉ khác vector b đúng $[l/2]$ vị trí. Khi đó

$$d(a, c) = d(b, c) = [l/2].$$

Do đó không thể sửa được $[l/2] \leq k$ lỗi khi nhận được c, mâu thuẫn!

$\Leftarrow$ Ngược lại giả sử $d(C) \geq 2k + 1$. Giả sử từ mã x được truyền và nhận được vector z với $d(x, z) \leq k$. Dễ thấy nếu y là từ mã khác x thì $d(z, y) \geq k + 1$, vì nếu $d(z, y) \leq k$ ta sẽ có

$$d(x, y) \leq d(x, z) + d(z, y) \leq k + k = 2k.$$

Mâu thuẫn với $d(C) \geq 2k + 1$. Điều phải chứng minh. □

Ví dụ 7.3.5. Đặt

$$C := \{00000000, 11111000, 01010111, 10101111\}.$$

Ta có $d(C) = 5$ và do đó có thể phát hiện được $5-1 = 4$ lỗi và có thể sửa được $[(5-1)/2] = 2$ lỗi.

Có một cách dễ dàng để tìm khoảng cách tối thiểu của bộ mã. Trước hết ta có khái niệm sau:

Định nghĩa 7.3.7. *Trọng lượng Hamming*, ký hiệu $wt(x)$, của vector $x = x_1x_2 \dots x_n$ là số các chỉ số i sao cho $x_i \neq 0$.

Ví dụ 7.3.6. $wt(00000) = 0, wt(10111) = 4, wt(11111) = 5$.

Bổ đề 7.3.8. *Giả sử x, y là các từ mã của mã tuyến tính C. Khi đó $d(x, y) = wt(x - y)$.*

Chứng minh. Các vị trí bằng 1 trong vector $x - y$ chính là những vị trí mà hai vector x và y khác nhau. Do đó $d(x, y) = wt(x - y)$. □

Định lý 7.3.9. *Khoảng cách của mã C bằng trọng lượng tối thiểu của từ mã khác không trong C.*

Chứng minh. Giả sử $d(C) = d$ thì tồn tại $x, y \in C, x \neq y$, sao cho $d(x, y) = d$. Do đó

$$wt(x - y) = d.$$

Nhưng C là mã tuyến tính nên $x - y \in C$.

Ngược lại giả sử $x \in C$ là từ mã khác không với trọng lượng tối thiểu. Do C là tuyến tính nên $0 \in C$. Vậy

$$wt(x) = wt(x - 0) = d(x, 0) \geq d(C).$$

□

Bài tập

1. Tìm khoảng cách Hamming của các cặp chuỗi bit sau:
   (a) 00000, 11111;
   (b) 1010101, 0011100;
   (c) 000000001, 111000000;
   (d) 1111111111, 0100100011.
2. Có bao nhiêu lỗi có thể phát hiện và bao nhiêu lỗi có thể sửa sai trong các mã sau:
   (a) $\{0000000, 1111111\}$.
   (b) $\{00000, 00111, 10101, 10010\}$.
   (c) $\{00000000, 11111000, 01100111, 10011111\}$.
3. Chứng minh rằng nếu khoảng cách tối thiểu giữa các từ mã là bốn, thì có thể sửa sai đúng một lỗi và phát hiện sai ba lỗi.

4. Chứng minh rằng một mã có thể sửa sai đồng thời $\leq a$ lỗi và phát hiện $a+1, \ldots, b$ lỗi nếu và chỉ nếu nó có khoảng cách tối thiểu ít nhất $a+b+1$.

5. Chứng minh nếu một mã có khoảng cách tối thiểu là d, từ mã x được truyền, không có quá $(d-1)/2$ lỗi xuất hiện và y nhận được, thì

$$d(x, y) < d(y, z)$$

với tất cả các từ mã $z \neq x$.

6. Chứng minh rằng:

$$wt(x+y) \geq wt(x) - wt(y).$$

Dấu bằng xảy ra nếu và chỉ nếu $x_i = 1$ khi $y_i = 1$.

7. Giả sử rằng x và y là các chuỗi bit có độ dài n, và m là số các vị trí mà ở đó cả x và y bằng 1. Chứng minh rằng

$$wt(x+y) = wt(x) + wt(y) - 2m.$$

8. Cho các ma trận sinh

$$G_1 := \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad G_2 := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

(a) Liệt kê các từ mã tương ứng các ma trận sinh trên.

(b) Tìm khoảng cách tối thiểu của các bộ mã.

9. *Tích của hai vector nhị phân* x và y là vector, ký hiệu $x * y$, xác định bởi

$$x * y = (x_1 y_1, \ldots, x_n y_n),$$

mà bằng 1 tại vị trí thứ i nếu và chỉ nếu $x_i = y_i = 1$. Chứng minh rằng

(a) $wt(x+y) = wt(x) + wt(y) - 2wt(x * y)$.

(b) $wt(x+z) + wt(y+z) + wt(x+y+z) \geq 2wt(x+y+x*y) - wt(z)$. Dấu bằng xảy ra nếu và chỉ nếu không xảy ra đồng thời $x_i = 0, y_i = 0, z_i = 1$.

10. Chứng minh rằng trong một mã nhị phân tuyến tính, hoặc tất cả các từ mã có trọng lượng chẵn, hoặc có chính xác một nửa trọng lượng chẵn và một nửa trọng lượng lẻ.

11. Tính khoảng cách của mã E_n (gồm tất cả vector độ dài n có trọng lượng chẵn).

12. Chứng minh với mọi $x, y \in \mathbb{B}^n$ ta có:

$$\left[\sum_{i=1}^{n} (x_i - y_i)^2\right]^{1/2} = \sqrt{d(x, y)}.$$

13. Giả sử x và y là các vector nhị phân với $d(x,y) = d$. Chứng minh rằng số các vector z sao cho $d(x,z) = r$ và $d(y,z) = s$ là $C(d,i)C(n-d, r-i)$, trong đó $i = (d+r-s)/2$. Nếu $d+r-s$ lẻ thì số này bằng 0, trong khi nếu $r+s = d$, nó bằng $C(d,r)$.

14. Chứng minh rằng

$$\langle x, y\rangle := \sum_{i=1}^{n} x_i y_i = 0 \qquad (\text{mod } 2)$$

nếu và chỉ nếu $wt(x * y)$ chẵn và bằng 1 nếu và chỉ nếu $wt(x * y)$ lẻ. Suy ra $\langle x, x\rangle = 0$ nếu và chỉ nếu $wt(x)$ chẵn.

15. Giả sử u, v, w, x là bốn vector đôi một có khoảng cách d (d phải là số chẵn).

(a) Chứng minh rằng tồn tại chính xác một vector mà khoảng cách đến các vector u, v, w bằng $d/2$.

(b) Chứng minh rằng tồn tại nhiều nhất một vector mà khoảng cách đến các vector u, v, w, x bằng $d/2$.

16. Giả sử C là $[n,k]$-mã với ma trận kiểm tra chẵn lẻ $H = (A\ I_{n-k})$ và $1 \le t \le k$. Mã C_t tương ứng ma trận kiểm tra chẵn lẻ $H_t = (A_t\ I_{n-k})$ trong đó A_t là ma trận cấp $(n-k) \times (k-t)$ nhận được từ A bằng cách xóa đi t cột đầu tiên.

(a) Chứng minh C_t gồm tất cả các từ mã của C với t tọa độ đầu tiên bằng 0 bị xoá.

(b) Chứng minh C_t là $[n-t, k-t]$-mã.

(c) Chứng minh $d(C_t) \ge d(C)$.

17. Với mỗi $n \in \mathbb{N}$, miêu tả mã C với hệ số k/n lớn nhất và $d(C) = 2$. Tồn tại duy nhất C?

18. Chứng minh rằng hai mã tương đương có cùng khoảng cách.

19. Ký hiệu $[n,k,d]$-mã có nghĩa $[n,k]$-mã với độ dài d. Chứng minh rằng nếu tồn tại $[n,k,2d]$-mã thì tồn tại mã với cùng tham số nhưng tất cả các từ mã có độ dài chẵn.

20. Chứng minh rằng nếu H là ma trận kiểm tra chẵn lẻ của mã C có độ dài n thì C có khoảng cách tối thiểu d nếu và chỉ nếu mọi tập gồm $d-1$ cột của H độc lập tuyến tính, nhưng tồn tại tập gồm d cột phụ thuộc tuyến tính. Từ đó suy ra:

(a) Nếu C là $[n,k,d]$-mã thì $d \le n-k+1$.

(b) Khoảng cách tối thiểu của mã có ma trận sinh:

$$\left[\begin{array}{c|cccc} & 1 & 1 & 0 & 0 \\ & 1 & 0 & 1 & 0 \\ & 0 & 1 & 1 & 0 \\ I_7 & 1 & 1 & 1 & 1 \\ & 1 & 1 & 0 & 1 \\ & 0 & 1 & 0 & 1 \\ & 1 & 0 & 0 & 1 \end{array}\right].$$

21. (a) Chứng minh rằng tồn tại mã tuyến tính gồm M phần tử, có độ dài n, nhiều nhất r bit kiểm tra chẵn lẻ, và khoảng cách tối thiểu d, nếu

$$\sum_{i=0}^{d-2}(M-1)^i C(n-1,i) < M^r.$$

(b) Chứng minh rằng nếu

$$2^k \sum_{i=0}^{d-2} C(n-1,i) < 2^n.$$

thì tồn tại mã tuyến tính $[n,k]$ với khoảng cách tối thiểu d.

22. Giả sử C là $[n,k,d]$-mã C với $n < 2d$. Chứng minh

$$2^k(2^k-1)d \le \sum_{x,y\in C} d(x,y) \le n2^{2k-1}.$$

23. Nêu cách xây dựng $[30,11,6]$-mã? Bộ mã này có bao nhiêu từ mã và khả năng phát hiện lỗi là bao nhiêu?

24. Ký hiệu (n,M,d)-mã nghĩa là $[n,k,d]$-mã, trong đó $M := 2^k$ là số các từ mã. Xây dựng, nếu tồn tại, các (n,M,d)-mã với các tham số sau:

$$(6,2,6),(3,8,1),(4,8,2),(5,3,4),(8,4,5),(8,30,3).$$

(Nếu không tồn tại, giải thích tại sao).

25. (a) Giả sử d lẻ. Chứng minh tồn tại (n,M,d)-mã nếu và chỉ nếu tồn tại $(n+1,M,d+1)$-mã.

(b) Chứng minh nếu tồn tại (n,M,d)-mã thì tồn tại $(n-1,M',d)$-mã với $M' \ge M/2$.

26. (Tổ hợp hai mã) Giả sử G_1, G_2 là hai ma trận sinh tương ứng các mã $[n_1,k,d_1]$ và $[n_2,k,d_2]$. Chứng minh rằng các ma trận

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

và $(G_1|G_2)$ là các ma trận sinh của các $[n_1{+}n_2, 2k, \min(d_1,d_2)]$-mã và $[n_1{+}n_2, 2k, d]$-mã $(d \ge d_1+d_2)$.

27. Với $x = x_1x_2\ldots x_m \in \mathbb{B}^m, y = y_1y_2\ldots y_n \in \mathbb{B}^n$ ta ký hiệu

$$(x,y) := x_1x_2\ldots x_my_1y_2\ldots y_n \in \mathbb{B}^{m+n}.$$

Giả sử C_1 là (n,M_1,d_1)-mã và C_2 là (n,M_2,d_2)-mã. Đặt

$$C_3 := \{(x,x+y) | x \in C_1, y \in C_2\}.$$

Chứng minh C_3 là $(2n, M_1M_2, d)$-mã tuyến tính với $d = \min\{2d_1, d_2\}$.

28. Giả sử $C := \{x = x_1x_2\ldots x_n \in \mathbb{B}^n \mid x_1 = x_2 = \cdots = x_n\}$.

(a) Chứng minh C là $[n,1,n]$-mã.

(b) Chứng minh $C^\perp$ là $[n,n-1,2]$-mã.

7.4 Hội chứng

Định nghĩa 7.4.1. Giả sử C là $[n,k]-$mã tuyến tính. Với mỗi vector $a \in \mathbb{B}^n$ tập hợp

$$C_a := a + C = \{a + x \mid x \in C\}$$

được gọi là *coset* (*modulo* hay *tịnh tiến*) của C.

Nhận xét 18. (a) Mọi vector $b \in \mathbb{B}^n$ thuộc một coset nào đó.

(b) Hai vector a và b thuộc cùng một coset nếu và chỉ nếu $(a - b) \in C$.

(c) Mỗi coset chứa 2^k vector.

Mệnh đề 7.4.2. *Hai coset hoặc rời nhau hoặc trùng nhau.*

Chứng minh. Giả sử $v \in (a + C) \cap (b + C)$. Khi đó tồn tại $x, y \in C$ sao cho

$$v = a + x = b + y.$$

Vậy

$$b = a + x - y = a + x',$$

trong đó $x' = x - y \in C$.

Suy ra

$$b + C \subset a + C.$$

Tương tự

$$a + C \subset b + C.$$

□

Từ Mệnh đề 7.4.2 ta có thể phân tích $\mathbb{B}^n$ thành hợp các coset rời nhau của C :

$$\mathbb{B}^n = C \cup (a^1 + C) \cup \cdots \cup (a^t + C), \tag{7.3}$$

trong đó $t = 2^{n-k} - 1, a^i \in C, i = 1, 2, \ldots, t, (a^i + C) \cap (a^j + C) = \emptyset, i \neq j$.

Giả sử người giải mã nhận được vector y. Khi đó tồn tại i sao cho

$$y = a^i + x, \quad x \in C.$$

Nếu x' là từ mã truyền thì vector lỗi

$$e = y - x' = a^i + x - x' = a^i + x'' \in a^i + C,$$

trong đó $x'' := x - x' \in C$. Nói cách khác vector lỗi chính là vector trong coset chứa y.

Do đó quyết định của người giải mã là, nếu nhận được vector y thì chọn một vector có trọng lượng nhỏ nhất $\hat{e}$ trong coset chứa y và giải mã y là $\hat{x} = y - \hat{e}$. Vector trọng lượng nhỏ nhất trong coset được gọi là *coset leader* (nếu có hơn một vector với trọng lượng nhỏ nhất, thì chọn ngẫu nhiên một và gọi là coset leader).

Giả sử rằng a^i trong (7.3) là coset leader. Cách thông thường để giải mã là sử dụng *bảng chuẩn* được định nghĩa như sau. Hàng đầu tiên gồm chính bộ mã, với từ mã không đặt bên trái:

$$x^{(1)} = 0, x^{(2)}, \ldots, x^{(s)}, \qquad s = 2^k;$$

các hàng tiếp theo là các coset $a^i + C$ được sắp xếp theo cùng thứ tự với coset leader đặt bên trái:

$$a^i + x^{(1)}, a^i + x^{(2)}, \ldots, a^i + x^{(s)}.$$

Ví dụ 7.4.1. $[4, 2]-$Mã với ma trận sinh $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ có bảng chuẩn

Bản tin	00	10	01	11	Hội chứng
Bộ mã C	0000	1011	0101	1110	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
Coset $a^1 + C$	1000	0011	1101	0110	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
Coset $a^2 + C$	0100	1111	0001	1010	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
Coset $a^3 + C$	0010	1001	0111	1100	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
	coset leader				

7.4.1 Giải mã dùng bảng chuẩn

Nếu nhận được vector y, giả sử 1111, ta sẽ tìm được vị trí của nó trong bảng. Khi đó vector lỗi e là coset leader nằm ở vị trí bên trái nhất cùng hàng với y, trong trường hợp này $e = 0100$, và từ mã được truyền là:

$$x = y - e = 1011$$

nằm trên đỉnh của cột chứa y, bản tin tương ứng là 10.

Nhận xét 19. (a) Giải mã dùng bảng chuẩn là giải mã hợp lý cực đại. Để tìm coset chứa y, chúng ta tìm vector $s := Hy \in \mathbb{B}^{n-k}$, được gọi là *hội chứng* (syndrome) của y.

(b) Nếu y là từ mã thì $s = 0$. Thật vậy nếu $y = x + e, s \in C$, thì

$$s = Hy = Hx + He = He \tag{7.4}$$

(c) Nếu các lỗi xuất hiện tại các vị trí $a, b, c \ldots$ tức là

$$e = 00\ldots\underset{a}{0}100\ldots00\ldots\underset{b}{0}100\ldots00\ldots\underset{c}{0}100\ldots$$

thì từ (7.4) ta có

$$s = \sum e_j H_j = H_a + H_b + H_c + \cdots$$

trong đó H_j là vector tương ứng cột thứ j của ma trận H.Vậy

Định lý 7.4.3. *Hội chứng của vector y bằng tổng các vector cột H_j của ma trận H, trong đó chỉ số j tương ứng vị trí xuất hiện lỗi .*

Hơn nữa, hai vector cùng một coset của C nếu và chỉ nếu chúng có cùng hội chứng.

Thật vậy u và v cùng coset nếu và chỉ nếu $(u - v) \in C$; tức là $H(u - v) = 0$; hay tương đương $Hu = Hv$. Do đó

Định lý 7.4.4. *Tồn tại tương ứng một-một lên giữa coset và hội chứng trong mã C.*

Ví dụ 7.4.2. Sử dụng ma trận kiểm tra chẵn lẻ trong Ví dụ 7.2.7 để xác định từ mã được gửi nếu nhận được thông báo 001111 (giả thiết có nhiều nhất một lỗi xuất hiện). Ta có

$$Hy = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Đây là cột thứ sáu của H. Do đó bit thứ sáu của 001111 là sai. Vậy từ mã được truyền là 001110.

Bài tập

1. Giả sử C là $[n, k]$-mã và $a \in \mathbb{B}^n$. Chứng minh coset $C_a = C$ nếu và chỉ nếu $a \in C$. Từ đó suy ra

   (a) Số phần tử của tập $\{x \in C | d(x, a) = i\}$ bằng A_i-số các từ mã có trọng lượng i.

   (b) Số các cặp từ mã (x, y) sao cho $d(x, y) = i$ bằng $2^k A_i$.

2. Chứng minh rằng nếu C là mã tuyến tính và $a \notin C$, thì $C \cup C_a$ cũng là mã tuyến tính.

3. (a) Xây dựng mảng chuẩn đối với các mã có các ma trận sinh

$$G_1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad G_2 := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad G_3 := \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

   (b) Sử dụng mảng chuẩn thứ ba để giải mã các vector 11111 và 01011.

   (c) Cho các ví dụ: Hai lỗi xuất hiện trong từ mã và sửa đúng; hai lỗi xuất hiện trong từ mã và sửa không đúng.

4. Giả sử C là $[4,2]$-mã với ma trận sinh

$$G := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

   (a) Tìm các từ mã.

   (b) Tìm các coset, coset leader của C.

   (c) Xây dựng mảng chuẩn. Từ đó giải mã khi nhận được các vector $0011, 0001, 0100$.

5. Xây dựng mảng chuẩn đối với mã có ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

   Sử dụng mảng này để giải mã các vector 110100 và 111111.

6. (a) Xây dựng mảng chuẩn đối với mã có ma trận sinh

$$G := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

   (b) Tìm vector hội chứng của $y = 1111$. Từ đó giải mã.

7. Giả sử $[7,4]$-mã có ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

   Xây dựng mảng chuẩn. Từ đó giải mã các vector nhận được: $1111111, 1101011, 0110111$ và 0111000.

8. Nếu $C \subset C^{\perp}$, ta nói rằng C là *tự đối ngẫu yếu,* viết tắt w.s.d (weakly self dual). C là *tự đối ngẫu* nếu $C = C^{\perp}$. Ví dụ mã lặp $[n, 1, n]$ là w.s.d nếu và chỉ nếu n chẵn. Khi $n = 2$, mã lặp $\{00, 11\}$ là tự đối ngẫu. Chứng minh rằng

   (a) C là w.s.d nếu $\langle x, y\rangle = 0$, với mọi $x, y \in C$.

   (b) C tự đối ngẫu nếu nó là w.s.d và có chiều $k = n/2$ (do đó n chẵn).

9. Xây dựng các mã tự đối ngẫu có độ dài 4 và 8.

10. Giả sử n chẵn và C là $[n, (n-1)/2]$ mã w.s.d. Chứng minh rằng $C^{\perp} = C \cup C_a$, trong đó a là vector có tất cả các tọa độ bằng 1.

11. Chứng minh rằng mã với ma trận kiểm tra chẵn lẻ $H = (A\ I)$ tự đối ngẫu nếu và chỉ nếu A là ma trận vuông sao cho $AA^t = I$.

12. Giả sử C là mã w.s.d. Chứng minh rằng mọi từ mã có trọng lượng chẵn. Hơn nữa, nếu mỗi hàng của ma trận sinh của C có trọng lượng chia hết cho 4 thì mọi từ mã cũng có trọng lượng chia hết cho 4.

13. Giả sử $[8, 4, 4]$-mã C có ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Chứng minh C là mã tự đối ngẫu.

7.5 Mã hoàn hảo

Để có thể sửa các lỗi xuất hiện khi truyền dữ liệu, chúng ta cần xây dựng bộ mã C có khoảng cách $d(C)$ lớn. Nhưng điều đó sẽ làm giới hạn số lượng từ mã trong bộ mã. Phần này sẽ chỉ ra mối liên hệ giữa $d(C)$ và số phần tử của tập hợp C.

Bổ đề 7.5.1. *Giả sử $x \in \mathbb{B}^n, 0 \leq k \leq n$. Khi đó*

$$\#\{y \in \mathbb{B}^n \mid d(x, y) \leq k\} = C(n, 0) + C(n, 1) + \cdots + C(n, k).$$

Chứng minh. Với mỗi $i \in \{0, 1, \ldots, n\}$ cố định, ta có

$$\#\{y \in \mathbb{B}^n \mid d(x, y) = i\}$$

bằng số các cách chọn i vị trí sao cho x và y khác nhau tại các vị trí đó và bởi vậy bằng $C(n, i)$. □

Bổ đề 7.5.2. *Giả sử C là bộ mã gồm các từ mã có độ dài n và*

$$d(C) \geq 2k + 1.$$

Khi đó với mỗi $y \in \mathbb{B}^n$, tồn tại nhiều nhất một phần tử $x \in C$, sao cho

$$y \in B(x, k) := \{z \in \mathbb{B}^n \mid d(x, z) \leq k\}.$$

Chứng minh. Giả sử $y \in B(x, k) \cap B(x', k), x, x' \in C$ $(x \neq x')$. Khi đó

$$d(x, x') \leq d(x, y) + d(x', y) \leq 2k.$$

Mâu thuẫn với giả thiết. □

Định lý 7.5.3. *Giả sử C là bộ mã gồm các từ mã độ dài n và $d(C) \geq 2k+1$. Thì*

$$\#C \leq \frac{2^n}{[C(n,0) + C(n,1) + \cdots + C(n,k)]}.$$

Chứng minh. Dựa trên các nhận xét sau

+ Có 2^n vector độ dài n (do $\#\mathbb{B}^n = 2^n$).

+ Mỗi quả cầu $B(x,k), x \in C$, chứa

$$C(n,0) + C(n,1) + \cdots + C(n,k)$$

vector (xem Bổ đề 7.5.1).

+ Với mỗi $x, x' \in C, x \neq x'$, thì $B(x,k) \cap B(x',k) = \emptyset$. □

Ví dụ 7.5.1. Nếu C có độ dài 7 và $d(C) = 3$ thì

$$\#C \leq \frac{27}{[C(7,0) + C(7,1)]} = 128/8 = 16.$$

Định nghĩa 7.5.4. *Mã hoàn hảo* (perfect code) là bộ mã C sao cho $d(C) = 2k+1$ và

$$\#C = \frac{2^n}{[C(n,0) + C(n,1) + \cdots + C(n,k)]}.$$

Nói cách khác, mã hoàn hảo là mã có số phần tử nhiều nhất trong tất cả các mã có khoảng cách $2k+1$ cho trước.

Ví dụ 7.5.2. Mã gồm hai từ mã 00000 và 11111 là mã hoàn hảo.

Bài tập

1. Tìm số cực đại các từ mã trong một bộ mã mà các từ mã là chuỗi các bit có độ dài chín và khoảng cách tối thiểu giữa các từ mã là năm.

2. Chứng minh rằng nếu n là số tự nhiên lẻ, thì mã gồm hai từ mã có độ dài n gồm toàn số 0 và 1 là một mã hoàn hảo.

3. Chứng minh rằng nếu C là mã hoàn hảo không tầm thường với khoảng cách tối thiểu 7 thì độ dài từ mã là 23.

4. Giả sử $\mathcal{G}_{24}$ có ma trận sinh $G = (I_{12}\ A)$ trong đó

$$A := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

   (a) Chứng minh $\mathcal{G}_{24}$ tự đối ngẫu, tức là: $\mathcal{G}_{24}^{\perp} = \mathcal{G}_{24}$.

   (b) Chứng minh $(A\ I_{12})$ cũng là ma trận sinh của $\mathcal{G}_{24}$.

   (c) Chứng minh mọi từ mã của $\mathcal{G}_{24}$ có trọng lượng chia hết cho 4.

   (d) Chứng minh $\mathcal{G}_{24}$ không có từ mã với trọng lượng 4.

   (e) Chứng minh $\mathcal{G}_{24}$ là $[24, 12, 8]$-mã (gọi là *mã Golay).*

   (f) Giả sử $\mathcal{G}_{23}$ nhận được từ $\mathcal{G}_{24}$ bằng cách bỏ tất cả các tọa độ cuối trong các từ mã. Suy ra các tham số của mã $\mathcal{G}_{23}$ và do đó $\mathcal{G}_{23}$ là mã hoàn hảo.

5. Giả sử $x, y \in \mathbb{B}^n$. Ta nói vector x *phủ* vector y nếu $x * y = y$. Chẳng hạn, 111001 phủ 101000.

   (a) Chứng minh rằng nếu vector $y \in \mathbb{B}^{23}$ trọng lượng 4 thì tồn tại duy nhất từ mã $x \in \mathcal{G}_{23}$ phủ y.

   (b) Suy ra số các từ mã trọng lượng 7 trong $\mathcal{G}_{23}$ là 253.

6. Chứng minh không tồn tại $[90, 2^{78}, 5]$-mã tuyến tính.

7. Chứng minh không tồn tại $[13, 64, 5]$-mã tuyến tính. (HD. Giả sử C là $[13, 6, 5]$-mã tương ứng ma trận sinh

$$\left[\begin{array}{ccccc|ccccccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & G_1 & & & & & & & G_1 & & & \end{array}\right].$$

   Chứng minh $\mathcal{G}_2$ sinh ra $[8, 5, 3]$-mã, mâu thuẫn với Định lý 7.5.3).

7.6 Mã Hamming

Phần này nghiên cứu các *mã Hamming* là một trong những bộ mã có thể dễ dàng mã hoá và giải mã. Đây là bộ mã có thể sửa sai một lỗi. Theo Định lý 7.4.3, hội chứng của vector

nhận được bằng tổng các cột của ma trận kiểm tra chẵn lẻ H ứng với lỗi xuất hiện. Do đó để xây dựng bộ mã sửa sai một lỗi, chúng ta phải có (tại sao?) các cột của H khác không và đôi một khác nhau. Nếu H có r hàng thì sẽ có $2^r - 1$ vector cột có độ dài r thỏa giả thiết trên.

Ví dụ 7.6.1. Nếu $r = 3$ thì có $2^3 - 1 = 7$ cột

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

là biểu diễn nhị phân của các số từ 1 đến 7.

Định nghĩa 7.6.1. *Mã Hamming bậc r* là mã có ma trận kiểm tra chẵn lẻ H cấp $r \times (2^r - 1)$ sao cho các cột của H khác không và đôi một khác nhau.

Ví dụ 7.6.2. Ma trận H của mã Hamming bậc 2 có dạng

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Bộ mã này có hai từ mã là 000 và 111. Đây là mã lặp tuyến tính bậc 3.

Ví dụ 7.6.3. Ma trận H của mã Hamming bậc 3 có dạng

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Bộ mã này có 16 từ mã.

Bổ đề 7.6.2. *Mã Hamming bậc r chứa 2^{n-r} từ mã với $n = 2^r - 1$.*

Chứng minh. Hiển nhiên theo định nghĩa. □

Bổ đề 7.6.3. *Khoảng cách tối thiểu của mã Hamming bậc r bằng 3.*

Chứng minh. Vì ma trận kiểm tra chẵn lẻ H có các cột khác 0 và không có hai cột nào giống nhau nên mã Hamming bậc r có thể sửa sai một lỗi. Theo Định lý 7.3.6 ta có $d(C) \geq 3$. Trong số các cột của ma trận H có ba cột sau

$$C_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad C_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Chú ý rằng

$$C_1 + C_2 + C_3 = 0 \qquad (\text{mod } 2).$$

Đặt x là vector bằng 1 ở vị trí của các cột này và bằng 0 nếu ngược lại. Khi đó $Hx = 0$. Nói cách khác, x là từ mã. Nhưng $wt(x) = 3$. Do đó, theo Định lý 7.3.9 thì

$$d(C) \leq wt(x) = 3.$$

□

Định lý 7.6.4. *Mã Hamming bậc r là mã hoàn hảo.*

Chứng minh. Đặt $n := 2^r - 1$. Theo Bổ đề 7.6.2 thì $\#C = 2^{n-r}$. Theo Bổ đề 4.6.3 thì $d(C) = 3$. Vậy

$$2^{n-r}[C(n,0) + C(n,1)] = 2^{n-r}(1+n) = 2^{n-r}(1+2^r-1) = 2^n.$$

□

Định lý 7.6.4 chỉ ra rằng mã Hamming là mã hoàn hảo. Nghiên cứu mã hoàn hảo là một trong những lĩnh vực quan trọng nhất của lý thuyết mã và đã có những kết quả nhất định.

Bài tập

1. $[7,4]-$mã C có ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

   (a) Mã hoá thông báo gồm hai bản tin $u = 0000\ 1101$.

   (b) Giải mã khi nhận được chuỗi bit 0000111 0001110 (giả sử có nhiều nhất một lỗi sai).

   (c) Tìm các tham số n, k, d của C.

2. Giả sử $[7,4,3]$-mã Hamming có ma trận kiểm tra chẵn lẻ

$$H := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

   (a) Tìm ma trận sinh dạng chuẩn.

   (b) Giải mã vector nhận được $y = 1010110$ (giả thiết có nhiều nhất một lỗi sai).

3. Tìm một ma trận kiểm tra chẵn lẻ của mã Hamming bậc 4. Giải mã các vector nhận được (giả thiết có nhiều nhất một lỗi sai):

   (a) 100 000 000 000 000.

   (b) 111 111 111 111 111.

4. Chứng minh rằng các ma trận

$$H := \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad H' := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

   sinh ra cùng một mã Hamming bậc 3.

5. Liệt kê ba dạng của ma trận kiểm tra chẵn lẻ H của mã Hamming bậc 4. Viết H dưới dạng $(A\ I_r)$. Từ đó mã hoá bản tin $u = 11111100000$, và giải mã vector 111000111000111.

6. Chứng minh rằng mã Hamming bậc r được xác định duy nhất theo nghĩa: Bất kỹ mã với các tham số $[2^r - 1, 2^r - 1 - r, 3]$ tương đương với mã Hamming bậc r.

7. Tìm ma trận sinh G của mã Hamming bậc r và sử dụng nó để chứng minh mọi từ mã khác không có trọng lượng ≥ 3. (HD. Nếu tồn tại từ mã có trọng lượng ≤ 2 thì nó phải là tổng của nhiều nhất hai hàng của G).

8. Tìm ma trận kiểm tra chẵn lẻ của $[15, 11, 3]$-mã Hamming. Giải thích cách giải mã nếu có đúng một lỗi xuất hiện. Nếu có hơn hai lỗi thì sao?

9. Chứng minh số các mã Hamming khác nhau có độ dài $n = 2^r - 1$ là

$$\frac{(2^r - 1)!}{\prod_{i=0}^{m-1}(2^m - 2^i)}.$$

Tài liệu tham khảo

[1] S. Arlinghaus, W. Arlinghaus, J. Nystuen, *The Hedetniemi matrix sum: an algorithm for shortest path and shortest distance,* Geographical Analysis, Vol. **22**, No. 4, Oct., 351-360 (1990).

[2] C. Berge, *Lý thuyết đồ thị và ứng dụng,* NXB Khoa học và kỹ thuật Hà Nội, 1971.

[3] A. Cayley, *Collected papers,* Quart. Jl. of Mathematics, **13** Cambridge, 26 (1897).

[4] N. Biggs, *Discrete mathematic,* Clarendon Press Oxford, 1989.

[5] N. Christofides, *Graph theory an algorithmic approach,* Academic Press INC. (1975).

[6] E. W. Dijkstra, *A note on two problems in connection with graphs,* Numerische Mathematik, **1**, 269 (1959).

[7] P. J. Cameron, *Combinatorics: topics, techniques, algorithms,* Cambridge University Press, 1994.

[8] N. Deo, *Graph theory with applications to engineering and computer science,* Prentice-Hall Inc., 1974.

[9] R. J. MC Eliece, M. Kac, *The theory of information and coding,* Addison-Wesley, 1977.

[10] R. W. Floyd, *Algorithm 97-Shortest path,* Comm. of ACM, **5**, 345 (1962).

[11] C. M. Goldie, R. G. E. Pinch, *Communication theory,* Cambridge University Press, 1991.

[12] M. Gondran, M. Minoux, S. Vajda, *Graphs and algorithms,* John Wiley & Sons (1990).

[13] R. W. Hamming, *Coding and information theory,* Prentice Hall, 1980.

[14] R. Hill, *A first course in coding theory,* Clarendon Press Oxford, 1985.

[15] T. C. Hu, *Integer programming and network flows,* Addison-Wesley, Reading, Massachusetts (1969).

[16] R. Johnsonbaugh, *An introduction to discrete mathematic,* Macmillan Publishing Company, 1992.

[17] A. R. Kenneth, C. R. B. Wright, *Discrete mathematics,* Prentice-Hall International Editions, 1978.

[18] V. Kevin, M. Whitney, *Algorithm 422-Minimum spanning tree,* Comm. of ACM, **15**, 273 (1972).

[19] G. Kirchhoff, in "Annalen der Physik and Chemie" **72**, 497 (1847).

[20] S. Lipschutz, *Essential computer mathematic,* McGraw-Hill, 1992.

[21] S. Lipschutz, M. L. Lipson, *2000 sloved problems in discrete mathematics,* McGraw-Hill, 1992.

[22] C. L. Liu, *Introduction to combinationnal mathematic,* McGraw-Hill, 1985.

[23] F. J. MacWilliams, N. J. A. Soane, *The theory of error-correcting codes,* North-Holland, 1981.

[24] A. A. Michael, A. J. Kfoury, R. N. Moll, D. Gries, *A basis for theoretical computer science,* Springer-Verlag NewYork Inc., 1981.

[25] J. G. Michaels, K. H. Rosen, *Applications of discrete mathematics,* McGraw-Hill, 1991.

[26] J. D. Murchland, *A new method for finding all elementary paths in a complete directed graph,* London School of Economics, Report LSE-TNT-22 (1965).

[27] R. C. Prim, *Shortest connection networks and some generalizations,* Bell Syst. Tech. Jl., **36**, 1389 (1957).

[28] S. Roman, *An introduction to discrete mathematic,* Saunders College, 1982.

[29] K. H. Rosen, *Discrete mathematics and its applications,* McGraw-Hill, 1995.

[30] B. M. Stephen, A. Ralston, *Discrete algorithmic mathematics,* Addision-Wesley Publishing Company, 1991.

[31] D. Welsh, *Codes and cryptography,* Clarendon Press Oxford, 1987.