# TOÁN RỜI RẠC

Phạm Tiến Sơn

Đà Lạt, 2005

# 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.

Giáo trình bao gồm sáu chương với 20 tài liệu tham khảo trình bày các vấn đề sau:

*Chương 1: Phép đếm.* Đề cập đến các phương pháp cơ bản của phép đếm: Nguyên lý tích, nguyên lý tổng, nguyên lý bao hàm-loại trừ, nguyên lý các chuồng chim bồ câu... Chúng đóng vai trò quan trọng trong Tin học, chẳng hạn: để ước lượng thời gian thực hiện của một thuật toán chúng ta cần đếm số thời gian thi hành từng dòng lệnh hoặc các vòng lặp. Phép đếm cũng đóng vai trò quan trọng trong lý thuyết xác suất.

*Chương 2: Quan hệ.* Trình bày các quan hệ thứ tự, quan hệ tương đương và cuối cùng là quan hệ tổng quát trên những tập hữu hạn. Chúng ta cũng xét mối quan hệ giữa các quan hệ với ma trận hay đồ thị biểu diễn nó.

*Chương 3: Đại số Boole.* Thuật ngữ "đại số Boole" được sử dụng để mô tả nhiều lĩnh vực có liên quan, từ tư duy logic và các bảng chân trị đến các phép toán số học được thực hiện bởi các mạch điện tử. Chương này bắt đầu với mối quan hệ giữa các tập được sắp thứ tự và các lattice. Kế tiếp là đại số Boole và vấn đề cực tiểu hoá hàm Boole.

*Chương 4: Mã tuyến tính.* Giới thiệu sơ lược về lý thuyết mã bao gồm các mã cho phép phát hiện và sửa sai. Đây là vấn đề thời sự do sự phát triển các công nghệ mới trong việc truyền và lưu trữ dữ liệu.

*Chương 5: Đồ thị.* Chương này giới thiệu một số khái niệm và bài toán cơ bản của lý thuyết đồ thị như chu trình Euler, chu trình Hamilton, đường đi ngắn nhất, tính phẳng của đồ thị...

*Chương 6: Cây.* Nội dung chính của chương đề cập đến những vấn đề: Xây dựng mã tối ưu Huffman, cây bao trùm và hệ các chu trình độc lập, cây bao trùm tối thiểu, liệt kê cây.

Tôi đặc biệt cám ơn các đồng nghiệp, đặc biệt Th.s. Trần Tuấn Minh, các bạn bè và các sinh viên vì những đóng góp của họ trong quá trình biên soạn giáo trình này.

Tôi chân thành cám ơn bạn đọc về những ý kiến đối với các thiếu sót không thể tránh khỏi của cuốn sách.

Đà Lạt, ngày 12 tháng 6 năm 2003
Phạm Tiến Sơn

# Chương 1

# PHÉP ĐẾM

---

Toán tổ hợp nghiên cứu về cách sắp xếp các đối tượng, 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 chính của chương này là thiết lập một số phương pháp đếm các tập hữu hạn phần tử mà không liệt kê các phần tử của chúng.

## 1.1 Các nguyên lý cơ bản của phép đếm

Với tập hữu hạn phần tử $S$, ta ký hiệu $\#S$ là số phần tử của tập $S$. Do đó $\#S = \#T$ nếu hai tập $S$ và $T$ có cùng số các phần tử. Chú ý rằng

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

Chúng ta bắt đầu với một số nguyên lý đếm.

### 1.1.1 Nguyên lý tổng

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

**Ví dụ 1.1.1** Giả sử lớp trưởng có thể 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 nam sinh 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 1.1.2** Giả sử một sinh viên có thể chọn đúng một chuyên đề tự chọn trong một trong ba danh sách. Ba danh sách này gồm 3, 5 và 9 chuyên đề tương ứng. Hỏi sinh viên đó có bao nhiêu cách lựa chọn?

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

**Nhận xét 1** Nguyên lý tổng có thể phát biểu 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

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

### 1.1.2 Nguyên lý tích

*Giả sử $A_1, A_2, \ldots, A_m$ là các sự kiện đôi một loại trừ nhau; và 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 1.1.3** 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 2** 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 1.1.4** 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 1.1.5** 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 1.1.6** Có bao nhiêu ánh xạ khác nhau từ tập $X$ có $m$ phần tử lên 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 1.1.7** Có bao nhiêu ánh xạ một-một (đơn ánh) khác nhau từ tập $X$ có $m$ phần tử lên tập $Y$ có $n$ phần tử?

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

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 1.1.8** 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 1.1.9** 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 $n_1 \times n_2 \times \cdots \times n_m$.

**Ví dụ 1.1.10** Trong nhiều trường hợp cần phải phối hợp cả hai nguyên lý tổng và tích: 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 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 xâu 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 xâu 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 3** 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.

### 1.1.3 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 lần ($A_1$ 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 1.1.11** 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 trên 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 trong đó hoặc bit thứ hai, hoặc bit thứ tư bằng 1?

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

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

6. 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?

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

   (a) Có bao nhiêu số chẵn, 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 $y > z$?

8. 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?

9. Có 10 bản copy của một cuốn sách và có một copy của 10 cuốn sách khác. Có bao nhiêu cách có thể chọn 10 cuốn sách?

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

11. 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?

## 1.2 Hoán vị và tổ hợp

**Định nghĩa 1.2.1** Một *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 1.2.1** 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 1.2.2** *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 1.2.2** 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 1.2.3** 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 1.2.2 có $4! = 24$ hoán vị của các ký tự $ABCDEF$ chứa chuỗi con $DEF$.

**Ví dụ 1.2.4** 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 1.2.2, bước đầu tiên có $3! = 6$ cách; theo Ví dụ 1.2.3 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 1.2.3** Một *$r$-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. Số các $r$-hoán vị của tập $n$ phần tử phân biệt ký hiệu là $P(n, r)$.

**Ví dụ 1.2.5** Ta có một số 2-hoán vị của $a, b, c$ là

$$ab, bc, ac.$$

Nếu $r = n$ trong Định nghĩa 1.2.3, chúng ta nhận được một thứ tự của tất cả $n$ phần tử. Do đó theo Định lý 1.2.2 $P(n, n) = n!$. Tổng quát ta có

**Định lý 1.2.4** *Số các $r$-hoán vị của tập $n$ phần tử phân biệt là*

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

*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

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

$\square$

**Ví dụ 1.2.6** Theo Định lý 1.2.4, 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 1.2.7** Có bao nhiêu cách chọn một chủ tịch, một phó chủ tịch, một thư ký và một thủ quỹ từ một nhóm 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 1.2.4 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 1.2.8** 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 1.2.5** Xét tập $X := \{x_1, x_2, \ldots, x_n\}$ 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 $\binom{n}{r}$.

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

$$P(n,r) = C(n,r)r!.$$

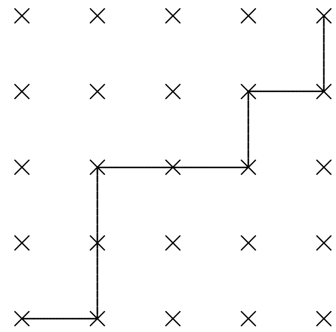
Vậy

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

Do đó theo Định lý 1.2.4 ta có

**Định lý 1.2.6** *Số các $r$-hoán vị của tập $n$ phần tử phân biệt là*

$$C(n,r) = \frac{n!}{(n-r)!r!}, \quad r \leq n.$$



Hình 1.1:

**Ví dụ 1.2.9** 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 1.2.10** 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 $10 \cdot 20 = 200$.

**Ví dụ 1.2.11** 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 1.2.12** 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 $4 \times 4$ được cho trong Hình 1.1.

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 1.1 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 có phân biệt thứ tự được tạo ra từ các ký tự $ABCDE$ 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.

## 1.3 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

$$t_1, t_2, \ldots, t_n. \tag{1.1}$$

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

$$\sum_{j=1}^{k} t_{i_j}$$

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 (1.1) 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 đươc 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 1.3.1** Giả sử $\alpha = s_1 s_2 \ldots s_p$ và $\beta = t_1 t_2 \ldots t_q$ là các chuỗi trên tập $\{1, 2, \ldots, n\}$. Ta nói $\alpha$ *có thứ tự từ điển nhỏ hơn* $\beta$, ký hiệu $\alpha < \beta$, nếu hoặc

(a) $p < q$ và $s_i = t_i$ với $i = 1, 2, \ldots, p$; 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 1.3.1** 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 $\{1, 2, \ldots, n\}$. Trong thuật toán, chúng ta sẽ liệt kê $r$-tổ hợp $\{x_1, x_2, \ldots, x_r\}$ tương ứng chuỗi $s_1 s_2 \ldots s_r$ trong đó

$s_1 < s_2 < \cdots < s_r$ và $\{x_1, x_2, \ldots, x_r\} = \{s_1, s_2, \ldots, s_r\}$. Chẳng hạn, 3-tổ hợp $\{6, 2, 4\}$ sẽ tương ứng chuỗi 246.

Ta sẽ liệt kê các $r$-tổ hợp của tập $\{1, 2, \ldots, n\}$ theo thứ tự từ điển. Do đó, các chuỗi được liệt kê đầu tiên và cuối cùng tương ứng là $12 \ldots r$ và $(n - r + 1) \ldots n$.

**Ví dụ 1.3.2** 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 1.3.3** 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 1.3.4** 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 $\alpha = s_1 s_2 \ldots s_r$ biểu diễn tổ hợp $\{x_1, x_2, \ldots, x_r\}$. Để tìm chuỗi kế tiếp $\beta = t_1 t_2 \ldots t_r$ 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 $n - 1, \ldots$ ). Khi đó

$$t_i = s_i, \quad \text{với } i = 1, 2, \ldots, m - 1.$$

Phần tử $t_m$ bằng $s_m + 1$. Những phần tử còn lại của chuỗi $\beta$ xác định bởi

$$t_{m+1} = s_m + 2, \quad t_{m+2} = s_m + 3, \ldots.$$

## Thuật toán sinh các tổ hợp

Bước 1. [Khởi tạo chuỗi] Đặt $s_i = i, i = 1, 2 \ldots, r$.

Bước 2. [Xuất tổ hợp đầu tiên] Xuất chuỗi $s = s_1 s_2 \ldots s_r$.

Bước 3. [Lặp] Với mỗi $i = 2, 3, \ldots, C(n, r)$ 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 $j = m + 1, \ldots, r$, đặt $s_j = s_{j-1} + 1$.

3.5. Xuất $s$.

**Ví dụ 1.3.5** 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 1.3.6** 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 1.3.7** 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 16435.

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 1.3.7 để tạo hoán vị kế tiếp. Thuật toán kết thúc khi tạo ra hoán vị $n(n-1) \ldots 21$.

**Ví dụ 1.3.8** Áp dụng phương pháp của Ví dụ 1.3.7, ta có thể liệt kê tất cả các hoán vị của $\{1, 2, 3, 4\}$ theo thứ tự từ điển như sau:

$$\begin{array}{cccccccc} 1234, & 1243, & 1324, & 1342, & 1423, & 1432, & 2134, & 2143, \\ 2314, & 2341, & 2413, & 2431, & 3124, & 3142, & 3214, & 3241, \\ 3412, & 3421, & 4123, & 4132, & 4213, & 4231, & 4312, & 4321. \end{array}$$

## 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 1.3.9** 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 $s_n$.

## 1.4 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 1.4.1** 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 1.4.1** *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 1.4.2** 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 $E$. Những ký tự này 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 1.4.3** 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 1.4.2** *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*

$$\frac{n!}{n_1!n_2!\dots n_t!}.$$

*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 1.4.4** 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

$$\begin{array}{ccccc} \text{Máy tính} & & \text{Vật lý} & & \text{Lịch sử} \\ \times\ \times\ \times & | & \times\ \times & | & \times \end{array}$$

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 $\times$ 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 1.4.3** *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

$$\_\ \_\ \_ \cdots \_\ \_$$

gồm $k$ ký hiệu $\times$ 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 $\times$ đến ký hiệu | đầu tiên tương ứng phép chọn $n_1$ phần tử $a_1$; $n_2$ ký hiệu $\times$ 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 $\times$; 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 1.4.5** 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 1.4.3, 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 1.4.3 ta có

$$C(5+3-1, 3-1) = C(7,2) = 21$$

cách.

**Ví dụ 1.4.6** (a) Có bao nhiêu nghiệm nguyên không âm của phương trình

$$x_1 + x_2 + x_3 + x_4 = 29? \tag{1.2}$$

Mỗi nghiệm của phương trình (1.2) tương đương với phép chọn 29 phần tử $x_i$ có kiểu $i, i = 1, 2, 3, 4$. Theo Định lý 1.4.3 số phép chọn là

$$C(29 + 4 - 1, 4 - 1) = C(32, 3) = 4960.$$

(b) Có bao nhiêu nghiệm nguyên của phương trình (1.2) thoả mãn

$$x_1 > 0, \quad x_2 > 1, \quad x_3 > 2, \quad x_4 \geq 0?$$

Mỗi nghiệm của (1.2) 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 1.4.3 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 1.2(a));

(b) Nếu lấy $\#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C)$ : có phần không được tính lần nào (Hình 1.2(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 1.2(c)).

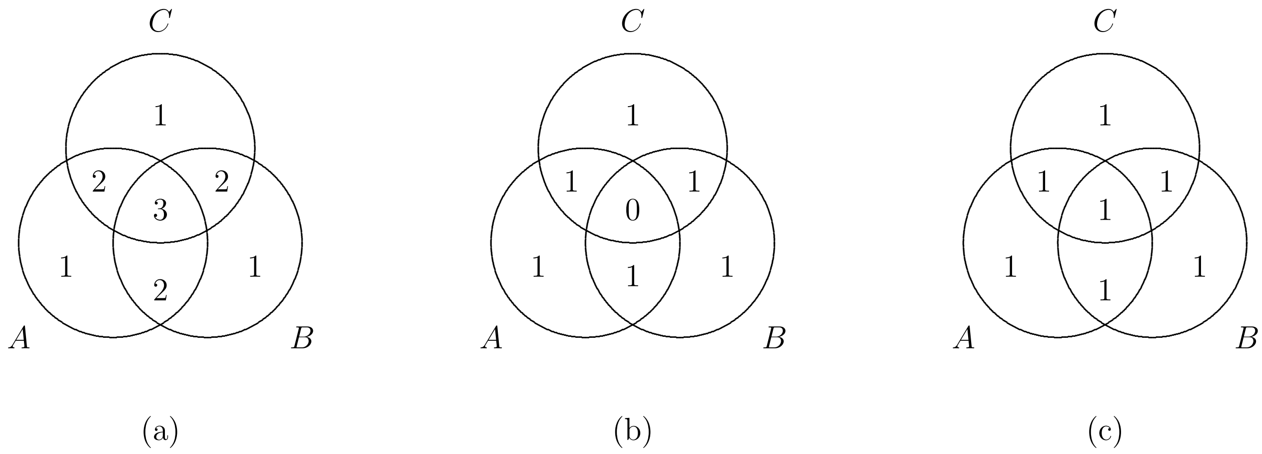
Vậy

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

Tổng quát ta có

**Định lý 1.4.4** *Giả sử có $m$ sự kiện $A_1, A_2, \ldots A_m$. Khi đó*

$$\begin{aligned}\#(A_1 \cup A_2 \cup \cdots \cup A_m) \;=\; & \sum_{i=1}^{m} \#A_i - \sum_{1 \leq i < j \leq m} \#(A_i \cap A_j) + \sum_{1 \leq i < j < k \leq m} \#(A_i \cap A_j \cap A_k) \\ & + \cdots + (-1)^{m+1} \#(A_1 \cap A_2 \cap \cdots \cap A_m).\end{aligned}$$




Hình 1.2:

*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 $A_1 \cap A_2 \cap \cdots \cap A_r, r \leq m$. 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 1.4.7** Có bao nhiêu nghiệm nguyên không âm của phương trình

$$x_1 + x_2 + x_3 = 11$$

với điều kiện $x_1 \leq 3, x_2 \leq 4$ và $x_3 \leq 6$?

Tương tự như Ví dụ 1.4.6, ta có

+ Tổng số nghiệm nguyên không âm của phương trình (1.4.7) là

$$C(3 + 11 - 1, 11) = 78.$$

+ Số nghiệm với điều kiện $x_1 \geq 4$ là

$$C(3 + 7 - 1, 7) = C(9, 7) = 36.$$

+ Số nghiệm với điều kiện $x_2 \geq 5$ là

$$C(3 + 6 - 1, 6) = C(8, 6) = 28.$$

+ Số nghiệm với điều kiện $x_3 \geq 7$ là

$$C(3 + 4 - 1, 4) = C(6, 4) = 15.$$

+ Số nghiệm với điều kiện $x_1 \geq 4, x_2 \geq 5$ là

$$C(3 + 2 - 1, 2) = C(4, 2) = 6.$$

+ Số nghiệm với điều kiện $x_1 \geq 4, x_3 \geq 7$ là

$$C(3 + 0 - 1, 0) = C(2, 0) = 1.$$

+ 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 1.4.4 số nghiệm đòi hỏi là

$$78 - 36 - 28 - 15 + 6 + 1 + 0 - 0 = 6.$$

**Định lý 1.4.5** *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 1.4.8** 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 1.4.5 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

$$x_1 + x_2 + x_3 = n \qquad (n \in \mathbb{N}).$$

## 1.5 Các hệ số nhị thức và các đồng nhất thức

**Định lý 1.5.1** (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

$$(a+b)^n = C(n,0)a^nb^0 + C(n,1)a^{n-1}b^1 + \cdots + C(n,n)a^0b^n.$$

□

Chính vì lý do trên mà $C(n,r)$ được gọi là *hệ số nhị thức*.

**Ví dụ 1.5.1** 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 1.5.2** 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 1.5.3** Sử dụng Định lý nhị thức ta có
$$2^n = (1+1)^n = \sum_{k=0}^{n} C(n,k).$$

**Định lý 1.5.2** (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 1.5.4** Chứng minh đẳng thức
$$\sum_{i=k}^{n} C(i,k) = C(n+1,k+1).$$

Theo Định lý 1.5.2
$$C(i,k) = C(i+1,k+1) - C(i,k+1).$$
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 1.5.5** Từ đẳng thức (1.5.4) 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 1.5.3** (Đẳng thức Vandermonde)

$$C(m+n,r)=\sum_{k=0}^{r} C(m,k)C(n,r-k)$$

*với* $r \le \min(m,n)$.

*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 $0 \le k \le r$.

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 cực đại của $C(n,k)$ với $k = 0, 1, \ldots, n$ là $C(n,[n/2])$.

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

$$(a+b+c)^n = \sum_{0 \le i+j \le n}^{n} \frac{n!}{i!j!(n-i-j)!} a^i b^j c^{n-i-j}.$$

12. Chứng minh rằng

$$3^n = \sum_{0 \le i+j \le n}^{n} \frac{n!}{i!j!(n-i-j)!}.$$

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

$$n2^{n-1} = \sum_{k=1}^{n} kC(n,k).$$

## 1.6 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.

### 1.6.1 Nguyên lý chuồng chim bồ câu (dạng thứ nhất)

*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.*

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 1.6.1** 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 1.6.2** 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 $0 \leq a_i \leq 2n$. 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 $a_i \vdots a_j$ nếu $k_i > k_j$ và $a_j \vdots a_i$ 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 1.6.3** 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.

## 1.6.2 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 1.6.4** 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 $A$ tương ứng là $X := \{1, 2, \ldots, 20\}$ và $Y := \{0, 1, \ldots, 19\}$. Tuy nhiên, $\#X = \#\{0, 1, \ldots, 19\}$ 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 1.6.5** 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

$$c_1, c_2, \ldots, c_{151}. \tag{1.3}$$

Các số này cùng với

$$c_1 + 1, c_2 + 1, \ldots, c_{151} + 1 \tag{1.4}$$

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 (1.3) là phân biệt và do đó các số trong (1.4) cũng khác nhau. Vì vậy phải có một số trong dãy (1.3) bằng một số trong dãy (1.4). 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 1.6.6** 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 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).

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

$$a_1, a_2, \ldots, a_{45} \tag{1.5}$$

và

$$a_1 + 9, a_2 + 9, \ldots, a_{45} + 9. \tag{1.6}$$

90 số trong (1.5) và (1.6) 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 (1.5) hoặc (1.6) bằng nhau; nên tồn tại một số trong dãy (1.5) bằng một số trong dãy (1.6). Vậy $a_i - a_j = 9$ với $i, j$ nào đó.

Ký hiệu $\lceil x \rceil$ là số nguyên nhỏ nhất lớn hơn $x$. Ví dụ $\lceil 8.3 \rceil = 9$. Ký hiệu $[x]$ là số nguyên lớn nhất nhỏ hơn $x$. Ví dụ $[2.3] = 2$.

### 1.6.3 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 1.6.7** 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

$$(P_i, P_j), (P_i, P_k), (P_j, P_k) \tag{1.7}$$

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 (1.7) không tương tự thì ta có ba ảnh tương ứng không tương tự.

**Ví dụ 1.6.8** 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 1.6.9** 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 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 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 1.6.5 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 1.6.5 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

$$a_k := \begin{cases} k & \text{nếu } k \leq \frac{m}{2}, \\ m-k & \text{nếu } k > \frac{m}{2}. \end{cases}$$

   (a) Chứng minh miền giá trị của $a$ chứa trong $\{1, 2, \ldots, n\}$.

   (b) Suy ra tồn tại $i \neq j$ sao cho $a_i \neq a_j$.

   (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

$$s_i := \begin{cases} r_i & \text{nếu } r_i \leq 8, \\ 16 - r_i & \text{nếu } r_i > 8. \end{cases}$$

   (a) Chứng minh rằng $s_1, s_2, \ldots, s_{10}$ thay đổi từ 0 đến 8.

   (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 rằng 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 $3 \times 7$ 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 2

# QUAN HỆ

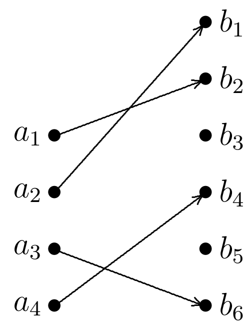
Như đã biết, tất cả các đối tượng trong thế giới xung quanh ta đều có những mối quan hệ nhất định với nhau. Rõ ràng không có một đối tượng nào có thể tồn tại tách rời (không liên quan) với thế giới bên ngoài. Mặt khác, mỗi đối tượng lại chứa đựng rất nhiều mối quan hệ nội tại của bản thân nó. Xét một 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 mối quan hệ hai ngôi trên hai tập hợp và trên cùng một tập hợp, cùng với các tính chất của các mối quan hệ đó. Tiếp theo, chúng ta sẽ xét đến quan hệ thứ tự, quan hệ tương đương và các mối liên quan.

## 2.1 Quan hệ hai ngôi

**Định nghĩa 2.1.1** *Quan hệ hai ngôi* từ tập $S$ lên tập $T$, kí hiệu $R$, là một tập 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 2.1.1** 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



Hình 2.1:

chứng chỉ mà sinh viên $a$ theo học. Tập $\{a \mid (a,b) \in R\}$ là danh sách các sinh viên theo học chứng chỉ $b$.

**Ví dụ 2.1.2** 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 2.1.3** 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* (xem thêm Chương 5) 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 2.1.3 có đồ thị trong Hình 2.1.

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 2.1.4** Ma trận biểu diễn quan hệ $R$ trong Ví dụ 2.1.3 là

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{array} \begin{array}{c} \begin{array}{cccccc} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}.$$

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.

**Ví dụ 2.1.5** 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

$$R_1R_2 := \{(x,z) \in S_1 \times S_3 \mid \text{ tồn tại } y \in S_2 \text{ để } (x,y) \in R_1, (y,z) \in R_2\}.$$

**Ví dụ 2.1.6** Giả sử $T$ là tập các chứng chỉ, $U$ là tập các khoa. 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 $U$. Xét quan hệ $R$ như trong Ví dụ 2.1.1. Thế thì $RR'$ 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 $R'R$ là không có nghĩa!

Dễ dàng chứng minh rằng (giả sử các phép toán hợp là có nghĩa):

**Tính chất 2.1.2** (a) *Tính kết hợp*

$$(R_1R_2)R_3 = R_1(R_2R_3).$$

(b) *Tính phân bố đối với phép hợp, nghĩa là*

$$(R_1 \cup R_2)R_3 = (R_1R_3) \cup (R_2R_3), \quad R_1(R_2 \cup R_3) = (R_1R_2) \cup (R_1R_3).$$

(c) *Tính chính quy đối với các phép bao hàm, nghĩa là nếu* $R_1 \subset R_2$ *và* $R_3 \subset R_4$, *thì*

$$R_1 \cup R_3 \subset R_2 \cup R_4, \quad R_1 \cap R_3 \subset R_2 \cap R_4.$$

*Hơn nữa, nếu* $R_1 \subset R_2$ *và* $R_3 \subset R_4$ *thì* $R_1R_3 \subset R_2R_4$.

**Ví dụ 2.1.7** 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

$$R_1R_2 = \{(1,e),(1,g),(2,e),(2,g),(2,h),(3,e),(3,f),(3,g),(3,h),$$
$$(4,e),(4,f),(4,g),(4,h),(5,f),(5,g),(5,h)\},$$

và các ma trận $A_1, A_2$ và $A$ tương ứng các quan hệ $R_1, R_2$ và $R_1R_2$ 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 2.1.3** 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

$$R^{-1} := \{(x,y) \in T \times S \mid (x,y) \in R\}.$$

**Tính chất 2.1.4** *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 $R_1(R_3 \cup R_4) = R_1R_3 \cup R_1R_4$.

   (b) Chứng minh rằng $(R_1 \cap R_2)R_3 \subseteq R_1R_3 \cap R_2R_3$ và đẳng thức không nhất thiết đúng.

   (c) Các quan hệ $R_1(R_3 \cap R_4)$ và $R_1R_3 \cap R_1R_4$ có liên hệ như thế nào?

## 2.2 Quan hệ và ma trận

Như Ví dụ 2.1.7 chỉ ra, ma trận của quan hệ $R_1R_2$ 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 |

Dễ thấy rằng

**Tính chất 2.2.1** *Với mọi* $x, y \in \mathbb{B}$ *ta có*

$$x \vee y = \max\{x, y\}, \quad x \wedge y = \min\{x, y\}.$$

**Định nghĩa 2.2.2** (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 2.2.1** Trong Ví dụ 2.1.7 thì $A = A_1 * A_2$.

**Định lý 2.2.3** *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* $R_1R_2$.

*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 2.2.2** 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 $R^2 := RR$ có ma trận

$$A * A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Và quan hệ $R^3 := RR^2$ 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

$$R^{n+2} = R^{(n-1)+3} = R^{n-1}.R^3 = R^{n-1}.R = R^n!$$

**Ví dụ 2.2.3** 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 $R_1R_2 \neq R_2R_1$. Bất đẳng thức này chỉ ra rằng $(2, 2) \in R_1R_2$ nhưng $(2, 2) \notin R_2R_1$.

**Định lý 2.2.4** *Tập $\mathcal{P}(S \times S)$, tất cả các quan hệ trên $S$, với phép toán hợp là nửa nhóm.*

*Chứng minh.* Thật vậy, phép hợp có tính chất kết hợp do Tính chất 2.1.2(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 2.2.5** *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*

$$R_1R_2 = R \Leftrightarrow A_1 * A_2 = A.$$

*Chứng minh.* Hiển nhiên theo các kết quả trên. □

**Định nghĩa 2.2.6** 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 2.2.4** 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 $m < n$. 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 2.2.5** (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 2.2.7** *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 2.2.8** *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 2.2.9** *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 $(R_1 \cap R_2)R_1^{-1}, R_1R_1^{-1} \cap R_2R_1^{-1}$.

   (c) Tìm các ma trận Boole của $R_2(R_1^{-1} \cup R_2^{-1}), R_2R_1^{-1} \cup R_2R_2^{-1}$.

   (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 $R, RR^{-1}$ và $R^{-1}R$.

   (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 $R^2R$.

   (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 $R^n, n \in \mathbb{Z}$.

   (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 $R_1 R_2$ phản xạ.

    (b) Nếu $R_1$ và $R_2$ đối xứng thì $R_1 R_2$ đối xứng.

    (c) Nếu $R_1$ và $R_2$ bắc cầu thì $R_1 R_2$ 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 $RR^{-1}$ là quan hệ đối xứng trên $S$.

(b) Chứng minh rằng $R^{-1}R$ là quan hệ đối xứng trên $S$.

(c) Các quan hệ $RR^{-1}, R^{-1}R$ là phản xạ? Bắc cầu?

14. Giả sử $R$ là quan hệ từ $S$ lên $T$.

(a) Chứng minh rằng $RR^{-1}$ 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 $R^{-1}R$ là đối xứng trên $T$.

(c) Khi nào thì $RR^{-1}$ 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. Dùng ma trận Boole, chứng minh rằng

$$(R_1R_2)^{-1} = R_2^{-1}R_1^{-1}.$$

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, khi đó $\mathcal{P}(S \times S)$ 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 $R^* \subset S$.

## 2.3 Quan hệ thứ tự

**Định nghĩa 2.3.1** 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 2.3.1** 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

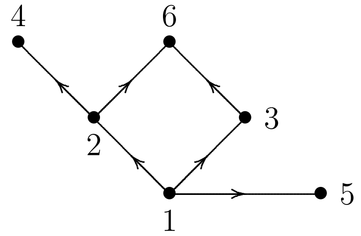
$$A := \{x \in \mathbb{C} \mid x = a + i0, a \in \mathbb{R}\}.$$

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 2.3.2** (a) Xét quan hệ thứ tự $\leq$ trên tập $S$. Ta nói rằng *$t$ phủ $s$* nếu $s < t$ và không tồn tại $u \in S$ sao cho $s < u < t$.

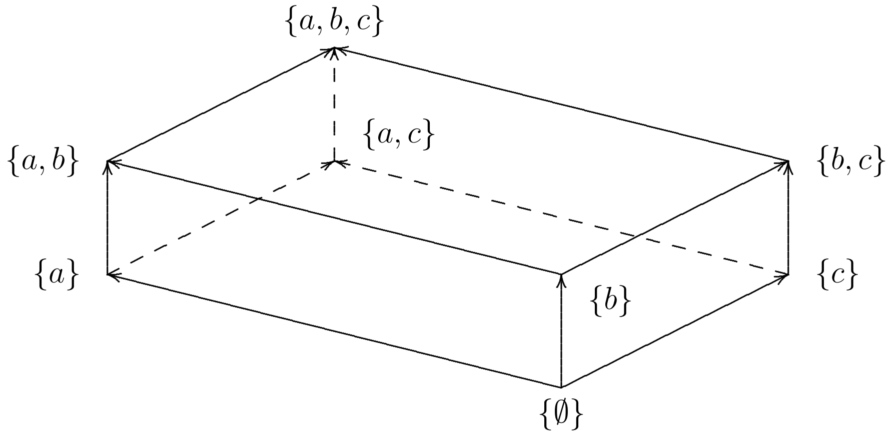
(b) Lược đồ *Hasse* của $(S, \leq)$ là một *đồ thị có hướng* gồm các đỉnh là các phần tử của $S$ và nếu $t$ phủ $s$ thì có một cung nối từ $s$ đến $t$.

**Ví dụ 2.3.2** (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 2.2.

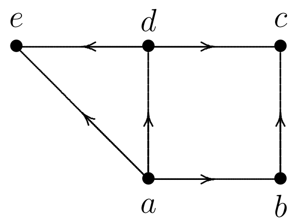



Hình 2.2:

(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 2.3.



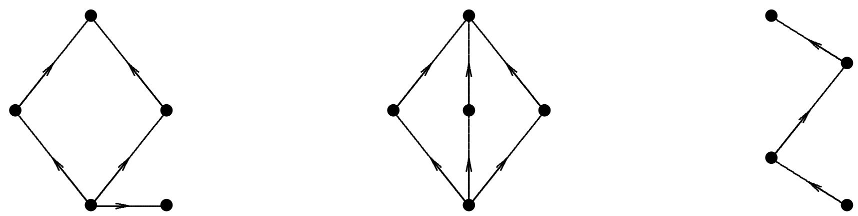

Hình 2.3:




Hình 2.4:

(c) Lược đồ trong Hình 2.5 không phải là lược đồ Hasse (tại sao?):

(d) Các lược đồ trong Hình **??** là lược đồ Hasse của các tập được sắp thứ tự bộ phận (được suy trực tiếp từ biểu đồ).



Hình 2.5:

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 $A \subset S, A \neq \emptyset$.

**Định nghĩa 2.3.3** (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

$$\inf A := \inf\{a \mid a \in A\}.$$

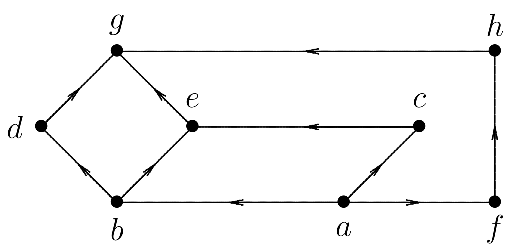
**Ví dụ 2.3.3** Xét tập được sắp thứ tự bộ phận trong Ví dụ 2.3.2(a). Tập $S$ không có phần tử lớn nhất; 1 là phần tử nhỏ nhất.

**Nhận xét 4** (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 2.3.4** (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 2.6. Ta có $\sup\{d,f\} = h$ và $\inf\{b,d,e,f\} = a$. Nhưng $\inf\{b,c\}$ và $\sup\{d,e,f\}$ không tồn tại.




Hình 2.6:

**Định nghĩa 2.3.4** 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 hữu hạn phần tử $A$ của lattice $L$ luôn tồn tại $\sup A, \inf A$.

**Ví dụ 2.3.5** (a) Tập được sắp thứ tự trong Ví dụ 2.3.2(b) là lattice.

(b) Tập được sắp thứ tự trong Ví dụ 2.3.2(a) không là lattice do tập $\{3, 4\}$ không có cận trên trong $S$.

Các định nghĩa của $\wedge$ và $\vee$ chỉ ra 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 $\mathbb{R}$.

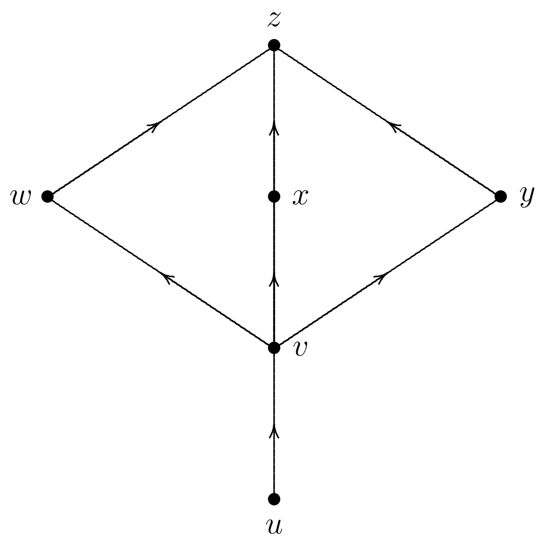
   (b) Tìm ví dụ của tập con khác trống của $\mathbb{R}$ mà không có cận trên nhỏ nhất.

   (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 $\Sigma$ là một bảng các ký tự và $\Sigma^*$ là tập các chuỗi ký tự. Xét quan hệ $\preceq$ trên $\Sigma^*$ 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 $\Sigma$ 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 $\Sigma^*$? Tại sao?

14. Giả sử $\Sigma$ 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 $\Sigma^*$? Giải thích.

(b) Trả lời câu hỏi trên nếu hạn chế $x, y \in \Sigma$.

15. Ký hiệu $\Sigma^*$ 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 $\Sigma$ 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. Giả sử $x, y, z$ là các chuỗi. Ý nghĩa của biểu thức sau

$$Q(x, y) \Leftrightarrow (\exists z)(\text{concat}(z, x) = y)?$$

19. 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.

20. Giả sử $\Sigma^*$ là tập các dãy hữu hạn phần tử của tập $\Sigma$ 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 $w_1 w' w_2 = w$.

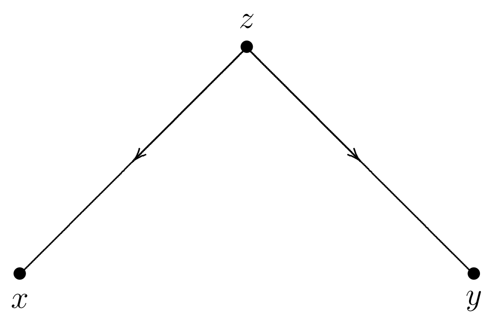
21. Lặp lại bài tập trên, nếu thay $\mathcal{J}(\mathbb{N})$ là họ các tập con vô hạn của $\mathbb{N}$.

    (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 $(x \vee y) \vee z = x \vee (y \vee z)$.

22. 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$(x, w)$.

23. 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 $R$.

24. 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 $(A, \geq)$.

25. 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 $a \in A$.

## 2.4 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 2.4.1** 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 2.4.1** (a) Trên tập các số tự nhiên $\mathbb{N}$, quan hệ sau là quan hệ tương đương:

$$mRn \;\Leftrightarrow\; m - n \,\vdots\, p \;\Leftrightarrow\; m = n \pmod p,\ \forall\, m, n \in \mathbb{N} \text{ ($p$ là số tự nhiên } > 2).$$

(b) Giả sử $S$ là tập các tam giác trong mặt phẳng. Xét quan hệ $R$ trên $S$: $T_1RT_2$ 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 2.4.2** Giả sử $\sim$ là quan hệ tương đương trong Ví dụ 2.4.1(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 2.4.2** *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 $s \sim t$. □

**Định nghĩa 2.4.3** Một *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 2.4.3** 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 2.4.4** (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 2.4.2.

(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 2.4.4** (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

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \quad (m, n) \mapsto m^2 + n^2,$$

thì các lớp tương đương chính là các tập con khác trống $f^{-1}(u), u \in \mathbb{N}$.

**Định lý 2.4.5** (a) *Giả sử $S \neq \emptyset$ và ánh xạ $f : S \longrightarrow T$. 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

$$f : S \longrightarrow [S], \qquad s \mapsto [s].$$

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) | $n \equiv m \pmod 4$. | (c) | $mn > 0$. |
| (b) | $mn = 0$. | (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 $\Sigma$ xác định bởi phân hoạch $\{\{a, d\}, \{c, e, f\}, \{b, g\}\}$.

5. (a) Khảo sát quan hệ trống $\emptyset$ trên tập khác trống $S$. 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) $RR \subset R$.

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 $f(n) = g(n)$ với mọi $n \in \mathbb{N}$ trừ một số hữu hạn.

    (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 $f(n) \leq g(n)$ với mọi $n \in \mathbb{N}$ trừ một số hữu hạn.

    (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 $\Sigma$ 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 $\mathbb{Z}$, $[m] \oplus [n] = [m+n]$?

## 2.5 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 2.5.1** (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 2.5.1** 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 2.5.2** *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

$$R^{k+1} = R^k R \subset R_1 R_1 \subset R_1$$

(bao hàm thức cuối có được do $R_1$ bắc cầu).

Vậy với mọi $k > 1$ ta có

$$R^k \subset R_1.$$

Hay $U \subset R_1$. $\square$

**Ví dụ 2.5.2** (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 2.5.3 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 2.5.1, dễ dàng kiểm tra lại các đẳng thức trên.

**Định lý 2.5.3** *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. $\square$

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 2.5.3** Xét $R$ trong Ví dụ 2.5.1. 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 2.5.4** 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. Quan hệ $s(R)$ có ma trận

$$s(A) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Dễ thấy rằng quan hệ $s(R)$ không bắc cầu!

Ví dụ này chứng tỏ bao đóng đối xứng của bao đóng bắc cầu $st(R)$ của quan hệ $R$ không phải 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 2.5.4** (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 $(x, z) \in R \cup E$. $\square$

**Định lý 2.5.5** *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 2.5.4(a), suy ra $tsr(R)$ phản xạ.

+ Từ $sr(R)$ đối xứng và Bổ đề 2.5.4(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 $R$. $\square$

**Ví dụ 2.5.5** Giả sử $R$ là quan hệ trên $\{1, 2, 3\}$ trong Ví dụ 2.5.4. 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 $\{1, 2, 3\}$ với 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 $\mathbb{P}$ : $mRn$ 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 $mRn$, nghĩa là, $m$ 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 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 $R$, 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* không thoả tính chất nào trong số (i), (ii)?

## 2.6 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 2.6.1** 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 2.6.2** 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

$$(k, k+2) \in R_6 \vee R_8 \tag{2.1}$$

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 (2.1) 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 $\pi_1$ và $\pi_2$. 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 $\pi_1$ là tập con nào đó trong $\pi_2$; trong trường hợp này ta nói $\pi_1$ *mịn hơn* $\pi_2$ 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 $\pi_1$ với một tập trong $\pi_2$. Việc xác định $\pi_1 \vee \pi_2$ khó hơn.

**Ví dụ 2.6.3** (a) Xét hộp đựng các viên bi trong Ví dụ 2.6.1, 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 hoạh $\pi_6 \wedge \pi_8$ của $\mathbb{P}$ tương ứng $R_6 \wedge R_8$ trong Ví dụ 2.6.2 gồm các lớp tương đương được xác định theo quan hệ $m = n$ (mod 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 $\pi$ 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 $\pi$;

(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 $\pi$ được xác định bởi $\alpha$. 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 $\pi$ thì tính chất (i) suy ra (i') $\alpha(j) = \alpha(k)$ nếu và chỉ nếu $jRk$.

**Ví dụ 2.6.4** Giả sử $R$ là quan hệ tương đương trên $S := \{1, 2, \ldots, 10\}$ mà phân hoạch $\pi$ của nó là

$$\{\{1,4,6\},\{2\},\{3,7,10\},\{5,9\},\{8\}\}.$$

Hàm $\alpha$ 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 $\alpha$ 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 $\pi_1, \pi_2$ của tập $S := \{1, 2, \ldots, n\}$, giả sử $\alpha, \beta$ là hai hàm thoả mãn (i) và (ii). Chú ý rằng, $\pi_1$ mịn hơn $\pi_2$ 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 $\gamma$ 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 $\gamma$ của khối này là $s$.

### 2.6.1 Thuật toán giao các 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 2.6.5** Giả sử $\pi_1$ và $\pi_2$ là các phân hoạch của $S := \{1, 2, \ldots, 8\}$ tương ứng các hàm $\alpha$ và $\beta$ :

| $k$ | 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 $\pi_1 = \{\{1,3,5\},\{2,4,8\},\{6,7\}\}$; $\pi_2$ gồm hai tập. Bảng 2.1 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 $\gamma$ 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 2.1:

| $k$ | $\gamma(1)$ | $\gamma(2)$ | $\gamma(3)$ | $\gamma(4)$ | $\gamma(5)$ | $\gamma(6)$ | $\gamma(7)$ | $\gamma(8)$ | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 5 | 4 | 5 | 1 | 7 | 4 | [hàm $\alpha$] |
| 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 2.2:

### 2.6.2 Thuật toán trộn các 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 2.6.6** Giả sử $\pi_1$ và $\pi_2$ là cá phân hoạch của $S := \{1, 2, \ldots, 8\}$ tương ứng các hàm $\alpha$ và $\beta$ :

| $k$ | 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 $\pi_1$ và $\pi_2$ có năm tập. Bảng 2.2 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 $\pi_3, \pi_5$.

   (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 $\alpha$ 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 $\pi_3, \pi_4$?

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 $\pi_3$ và $\pi_4$.

10. Như Bài tập 8 cho $\pi_2$ và $\pi_3$.

11. Thuật toán trộn các phân hoạch vẫn chạy đúng nếu hoán đổi vai trò của $\alpha$ và $\beta$?

12. (a) Chứng minh quan hệ $\leq$ xác định trên $\Pi(S)$ bởi "$\pi_1 \leq \pi_2$ nếu và chỉ nếu $\pi_1$ mịn hơn $\pi_2$" 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 $\pi_1$ mịn hơn $\pi_2$ 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 3

# 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.

## 3.1 Lattice

**Định nghĩa 3.1.1** 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 5** (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 3.1.2** *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 mi nh.* (a) Đặt $y := x \vee x$. Khi đó

$$\begin{array}{rcll} x & = & \vee(x \wedge y) & \text{(theo 3La)} \\ & = & \vee[x \wedge (x \vee x)] & \\ & = & \vee x & \text{(theo 3Lb).} \end{array}$$

(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 3.1.3** *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 3.1.3 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 3.1.4** *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 6** (a) Từ Tính chất 3.1.2, 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 3.1.3 và 3.1.4 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 3.1.1** $S$ là tập bất kỳ. Với các phép toán hợp và giao, $(\mathcal{P}(S), \cup, \cap)$ là một lattice đại số. Theo Định lý 3.1.4, 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 3.1.2** 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 $\Sigma$ 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 3.1.3** 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 mỗi $x \in \mathbb{R}$.

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

$$\begin{aligned} (f \vee g)(x) &:= \max(f(x), g(x)), \\ (f \wedge g)(x) &:= \min(f(x), g(x)). \end{aligned}$$

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 3.1.5** 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

$$x \leq 1 \text{ với mọi } x \in L, \tag{3.1}$$

gọi là *phần tử lớn nhất*.

(b) Phần tử trong $L$, ký hiệu 0, thỏa mãn

$$0 \leq x \text{ với mọi } x \in L, \tag{3.2}$$

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 (3.1) tương đương với

$$x \vee 1 = 1 \text{ và } x \wedge 1 = x.$$

Và (3.2) tương đương với

$$0 \vee x = x \text{ và } 0 \wedge x = 0.$$

**Nhận xét 7** (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 3.1.6** *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 3.1.4** (a) Lattice đại số cho trong Ví dụ 3.1.1 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 con của $\mathbb{B}$. Xét lattice $\mathrm{Fun}(S, \mathbb{B})$. Theo Ví dụ 3.1.3.

$$(f \vee g)(x) = \max(f(x), g(x)),$$
$$(f \wedge g)(x) = \min(f(x), g(x)),$$

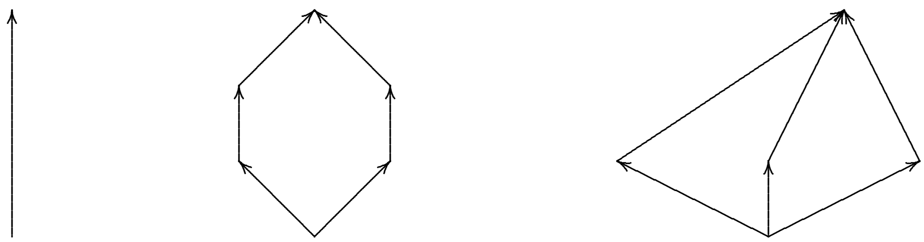
với mọi $x \in S$. Nên

$$(f \vee g)(x) = \begin{cases} 1 & \text{nếu } f(x) = 1 \text{ hoặc } g(x) = 1, \\ 0 & \text{nếu ngược lại,} \end{cases}$$

$$(f \wedge g)(x) = \begin{cases} 1 & \text{nếu } f(x) = g(x) = 1, \\ 0 & \text{nếu ngược lại.} \end{cases}$$

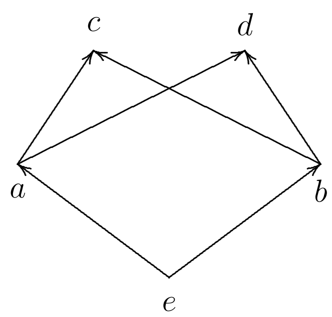
Các nguyên tử trong $\mathrm{Fun}(S, \mathbb{B})$ là các hàm đặc trưng $1_{\{x\}}, x \in S$.

**Ví dụ 3.1.5** Các lược đồ Hasse trong Hình 3.1 tương ứng các lattice đại số.



Hình 3.1:

Lược đồ Hasse trong Hình 3.2 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 $e$ :

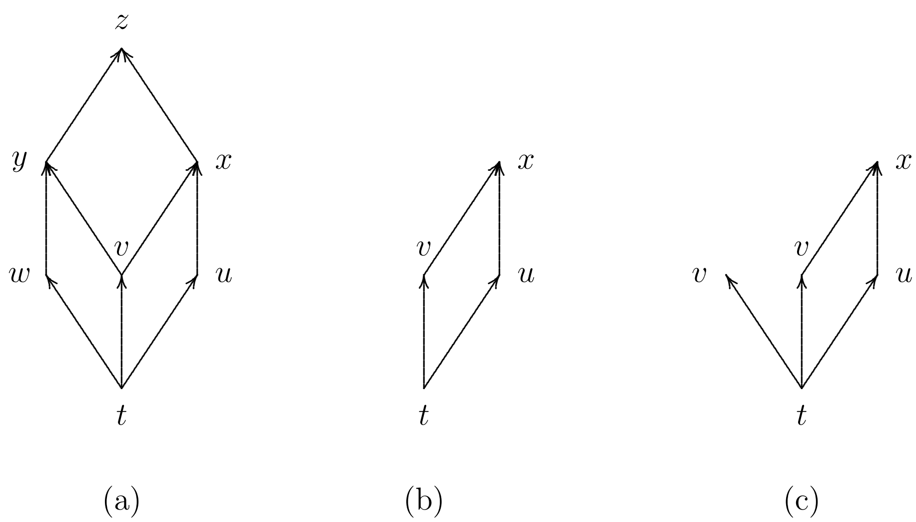



Hình 3.2:

**Định nghĩa 3.1.7** 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.




Hình 3.3:

**Ví dụ 3.1.6** Xét lattice đại số $(L, \vee, \wedge)$ có lược đồ Hasse trong Hình 3.3(a). Ta có $M_1$ trong Hình 3.3(b) là lattice con của $L$; còn $M_2$ trong Hình 3.3(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) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

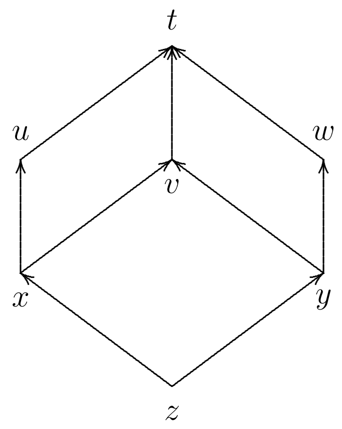
2. Giả sử $L$ là lattice đại số với phần tử lớn nhất 1 và phần tử nhỏ nhất 0.

   (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:

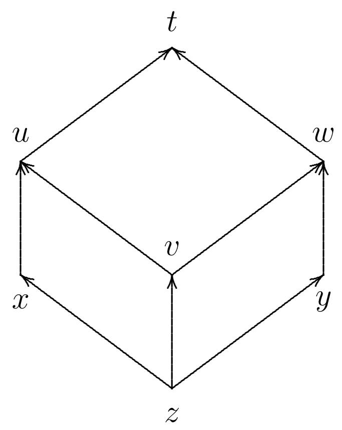



(a) Liệt kê các nguyên tử của lattice.

(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

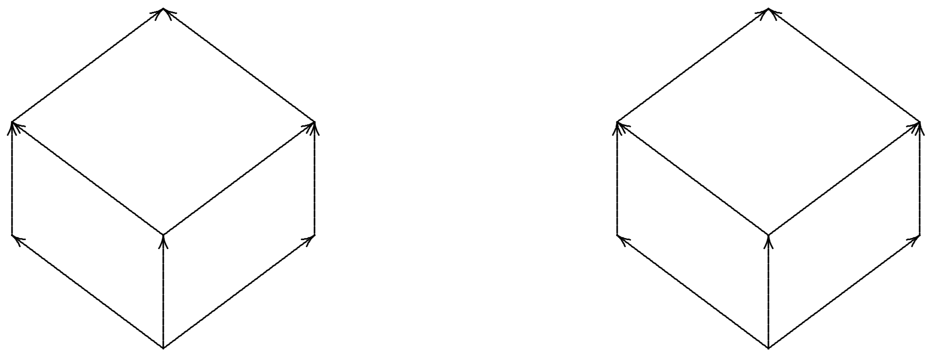
$$\varphi(x \vee y) = \varphi(x) \cup \varphi(y), \quad \varphi(x \wedge y) = \varphi(x) \cap \varphi(y)$$

   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 $(P, \leq)$ là lattice. Chứng minh rằng nếu $x \leq y$, thì $x \vee (z \wedge y) \leq (x \vee z) \wedge y$ với mọi $z \in P$.

## 3.2 Latiice phân bố

**Định nghĩa 3.2.1** 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) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

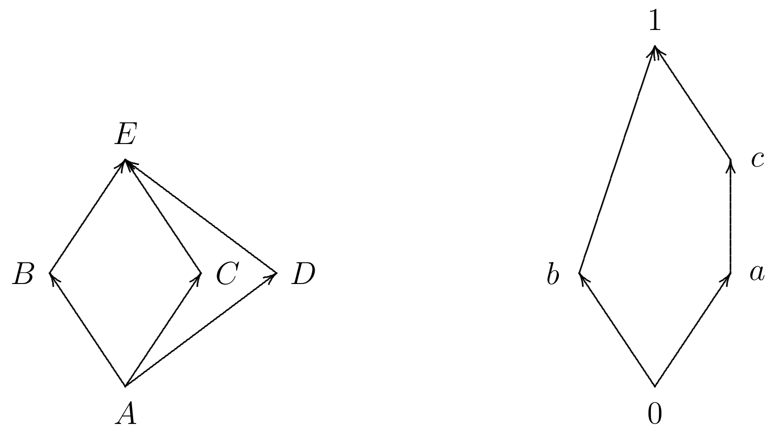
**Ví dụ 3.2.1** (a) Lattice đại số trong Ví dụ 3.1.1 là phân bố.

(b) Lattice đại số trong Ví dụ 3.1.2 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 3.2.2** Các lattice đại số trong Hình 3.4 không phân bố.




(a) (b)

Hình 3.4: Các lattice không phân bố.

Chẳng hạn, chứng minh (a). Ta có

$$B \vee (C \wedge D) = B \vee A = B.$$

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 3.2.2.* Định lý sau chỉ ra rằng chỉ cần kiểm tra một tiêu chuẩn của luật phân bố.

**Định lý 3.2.2** *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).

$$\begin{array}{rcll}
(x \wedge y) \vee (x \wedge z) & = & [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z] & \text{(do (a))} \\
& = & [x \vee (x \wedge y)] \wedge [z \vee (x \wedge y)] & \text{(tính giao hoán)} \\
& = & x \wedge [z \vee (x \wedge y)] & \text{(tính hấp thụ)} \\
& = & x \wedge [(z \vee x) \wedge (z \vee y)] & \text{(do (a))} \\
& = & [x \wedge (z \vee x)] \wedge (z \vee y) & \text{(tính kết hợp)} \\
& = & [x \wedge (x \vee z)](y \vee z) & \text{(tính giao hoán)} \\
& = & x \wedge (y \vee z) & \text{(tính hấp thụ)}
\end{array}$$

(b) $\Leftarrow$ (a). Do nguyên lý đối ngẫu. $\square$

**Định lý 3.2.3** *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

$$\begin{array}{rcl}
x & = & x \vee (x \wedge a) \\
& = & x \vee (y \wedge a) \\
& = & (x \vee y) \wedge (x \vee a) \\
& = & (y \vee x) \wedge (y \vee a) \\
& = & y \vee (x \wedge a) \\
& = & y \vee (y \wedge a) \\
& = & y.
\end{array}$$

$\square$

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 3.2.4** 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 8** (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 3.2.3** (a) Lattice trong Ví dụ 3.2.2(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 3.2.2(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 3.2.4** Lattice trong Hình 3.5 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.

$$0 \longrightarrow x \longrightarrow 1$$

Hình 3.5:

**Định lý 3.2.5** *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

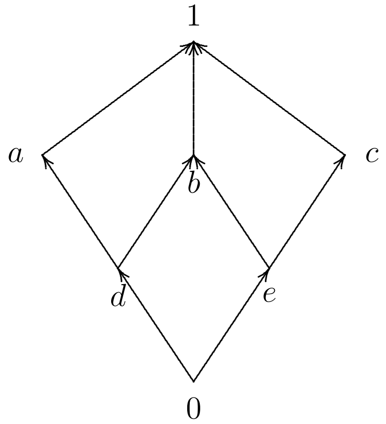
$$\begin{aligned}
y &= y \vee 0 && (\text{vì } 0 \leq y)\\
&= y \vee (x \wedge z) && (\text{vì } x \wedge z = 0)\\
&= (y \vee x) \wedge (y \vee z) && (\text{vì tính phân bố})\\
&= 1 \wedge (y \vee z) && (\text{vì } y \vee x = x \vee y = 1)\\
&= (x \vee z) \wedge (y \vee z) && (\text{vì } x \vee z = 1)\\
&= (x \wedge y) \vee z && (\text{vì tính phân bố})\\
&= 0 \vee z && (\text{vì } x \wedge y = 0)\\
&= z && (\text{vì } 0 \leq z).
\end{aligned}$$

□

**Nhận xét 9** 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 $L_1$.

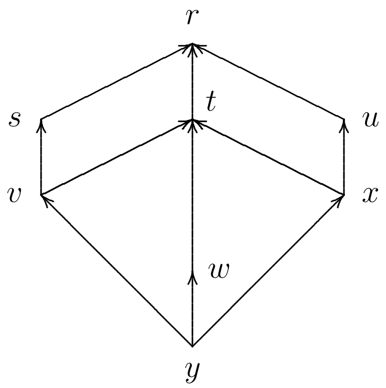
   (c) Viết 1 dưới dạng tuyển của các phần tử bất khả qui.

   (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 cận trên và dưới đúng của $L_2$.

   (b) Tìm $v \vee x, s \vee v$ và $u \wedge v$.

   (c) $L_2$ là lattice khả bù? Giải thích.

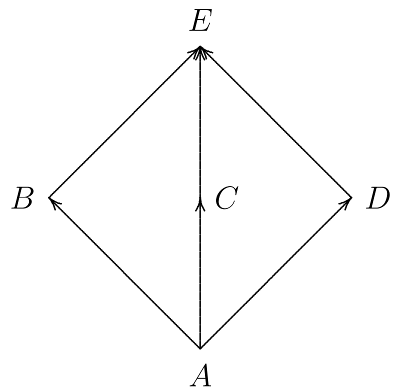
   (d) Tìm phần tử có hai phần tử bù.

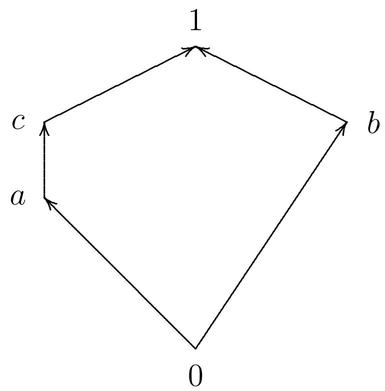
   (e) $L_2$ là lattice phân bố?

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 khả 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 8 cho $(D_{36}, |)$.
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. Giả sử $L$ là lattice phân bố. Chứng minh rằng nếu $x, y \in L$ thoả $x \vee a = y \vee a$ và $x \wedge a = y \wedge a$ với $a \in L$ nào đó, thì $x = y$.
11. Sử dụng Định lý 3.2.5 chứng minh các lattice trong hình sau không phân bố:




[1] *Xích* là tập được sắp thứ tự mà hai phần tử bất kỳ có thể so sánh được với nhau.

12. 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.

13. Chứng minh, hoặc bằng phản ví dụ, rằng

    (a) Mọi lattice hữu hạn là phân bố.

    (a) Mọi lattice hữu hạn có cận trên.

14. Giả sử $L$ 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 $z \preceq x'$.

## 3.3 Đại số Boole

**Định nghĩa 3.3.1** *Đại số Boole* (còn gọi là lattice Boole) là một lattice phân bố khả bù.

**Nhận xét 10** (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 3.3.1** Lattice $\mathcal{P}(S)$ trong Ví dụ 3.1.1 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 3.3.2** Lattice $\Sigma$ trong Ví dụ 3.1.2 là lattice phân bố trong đó

+ phần tử lớn nhất là 1 = [True].

+ phần tử phần tử nhỏ nhất là 0 = [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 3.3.3** (a) Xét lattice $\text{Fun}(S, \mathbb{B})$ trong Ví dụ 3.1.4 (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 $\text{Fun}(S, \mathbb{B})$ 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 3.3.2** (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
$$(x \vee y) \wedge (x' \vee y') = 0.$$

(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 3.3.3** *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*

$$x = a_{i_1} \vee a_{i_2} \vee \ldots \vee a_{i_k}. \tag{3.3}$$

*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

$$x = \vee\{a \in S \mid a \leq x\}. \tag{3.4}$$

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 (3.3) 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 (3.4).

+ 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 3.3.4** *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 3.3.3, 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 3.3.3, 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 3.3.3, 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 $[f(x)]' = f(x')$. $\square$

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 3.3.5** *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 $B$ với hai phép toán

   $$\begin{aligned} (f \vee g)(x) &:= f(x) \vee g(x), \\ (f \wedge g)(x) &:= f(x) \wedge g(x), \\ (f')(x) &:= [f(x)]', \end{aligned}$$

   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 0 và phần tử lớn nhất 1.

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 $(S, +, \cdot, ')$ 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 $xy' \in S$ 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 $\Phi$ 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.

## 3.4 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 3.4.1** 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 11** 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 3.4.1** (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 trân 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 3.4.2** Bảng chân trị của hàm

$$f(x, y, z) = y' \wedge (x \vee z)$$

là

| $x$ | $y$ | $z$ | $y'$ | $x \vee z$ | $f$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 | 0 |

**Nhận xét 12** 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 3.4.3** Xét bảng chân trị

| $x$ | $y$ | $z$ | $f$ | |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | x |
| 1 | 1 | 0 | 0 | |
| 1 | 0 | 1 | 1 | x |
| 1 | 0 | 0 | 0 | |
| 0 | 1 | 1 | 1 | x |
| 0 | 1 | 0 | 0 | |
| 0 | 0 | 1 | 0 | |
| 0 | 0 | 0 | 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 3.4.2** Hai hàm Boole được gọi là *tương đương* với nhau nếu chúng có cùng một bảng chân trị.

**Ví dụ 3.4.4** 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: $\mathrm{Fun}(\mathbb{B}^n, \mathbb{B}) := \{f : \mathbb{B}^n \to \mathbb{B}\}$.

**Định lý 3.4.3** *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 3.4.5** (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 3.4.4** *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 $f\colon \mathbb{B}^3 \to \mathbb{B}$ 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 $f_1 \vee f_2$ và $f_2 \vee f_1$ tương đương.

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.

## 3.5 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 3.5.1** 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 3.5.2** (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 3.5.3** *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*

$$f(x) = \sum f(e_1, e_2, \ldots, e_i, x_{i+1}, x_{i+2}, \ldots, x_n) x_1^{e_1} \wedge x_2^{e_2} \wedge \ldots \wedge x_i^{e_i}, \tag{3.5}$$

*hoặc dưới dạng hội chính quy*

$$f(x) = \prod f(e_1, e_2, \ldots, e_i, x_{i+1}, x_{i+2}, \ldots, x_n) x_1^{e_1} \vee x_2^{e_2} \vee \ldots \vee x_i^{e_i}, \tag{3.6}$$

*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 (3.5). 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 (3.5)

$$x_1^{e_1} x_2^{e_2} \ldots x_i^{e_i} f(e_1, e_2, \ldots, e_i, x_{i+1}, x_{i+2}, \ldots, x_n)$$

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 3.5.4** *Hàm Boole $f$ có thể được khai triển theo một đối số $x_i$*

$$f(x) = x_i' f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \vee x_i f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n), \tag{3.7}$$

*hoặc*

$$f(x) = x_i' f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \wedge x_i f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n). \tag{3.8}$$

Cho $i = n$ trong định lý và bỏ đi các phần tử bằng 1 trong một tích, ta được

**Hệ quả 3.5.5** *Mọi hàm Boole có thể được khai triển dưới dạng tuyển chính quy*

$$f(x) = \sum_{e \in T_f} x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n} \tag{3.9}$$

*hoặc dưới dạng hội chính quy*

$$f(x) = \prod_{e \in T_f} x_1^{e_1} \vee x_2^{e_2} \vee \ldots \vee x_n^{e_n} \tag{3.10}$$

Công thức khai triển (3.9) 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 3.5.1** 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

$$\begin{aligned} f_\Sigma &= x_1'x_2'x_3' + x_1'x_2x_3' + x_1'x_2x_3 + x_1x_2'x_3 + x_1x_2x_3, \\ f_\Pi &= (x_1 + x_2 + x_3')(x_1' + x_2 + x_3)(x_1' + x_2' + x_3). \end{aligned}$$

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 **??**, ta nhận được

**Hệ quả 3.5.6** *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 3.5.7** *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 3.5.6.

(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) | $xy$. | (e) | $[(xy \vee xyz) \vee xz] \vee z$. |
| (b) | $z'$. | (f) | $xy \vee z'$. |
| (c) | $xz \vee (y' \vee y'z) \vee xy'z'$. | (g) | $[(x \vee y)' \vee z]'$. |
| (d) | $x \vee yz$. | (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.

## 3.6 Biểu diễn tối thiểu của hàm Boole

### 3.6.1 Khái niệm

Biểu diễn hàm đại số Boole qua một hệ hàm đầy đủ $H$ là không duy nhất. Ví dụ hàm Sheffer,

$$x \uparrow y := \begin{cases} 0 & \text{nếu } x = y = 1, \\ 1 & \text{nếu ngược lại,} \end{cases}$$

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

|  | $y'$ | $y$ |
| --- | --- | --- |
| $x'$ | $x' \wedge y'$ | $x' \wedge y$ |
| $x$ | $x \wedge y'$ | $x \wedge y$ |

Hình 3.6: Bản đồ Karnaugh hai biến

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.

## 3.6.2 Phương pháp bản đồ Karnaugh

Như đã biết, thông qua Ví dụ 3.4.3, 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 3.6.

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 3.7.

Ta minh họa phương pháp qua ví dụ sau.

| | |
|---|---|
| 1 | |
| 1 | |

$y'$

| | |
|---|---|
| 1 | 1 |
| | |

$x'$

| | |
|---|---|
| | 1 |
| | 1 |

$y$

| | |
|---|---|
| | |
| 1 | 1 |

$x$

Hình 3.7: Kết hợp các hình vuông kề nhau

**Ví dụ 3.6.1** 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 3.8.

| | $y'$ | $y$ |
|---|---|---|
| $x'$ | | 1 |
| $x$ | 1 | 1 |

Hình 3.8:

*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 3.9.

| | $y'$ | $y$ |
|---|---|---|
| $x'$ | | 1 |
| $x$ | 1 | 1 |

Hình 3.9:

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | $x' \wedge y' \wedge z'$ | $x' \wedge y' \wedge z$ | $x' \wedge y \wedge z$ | $x' \wedge y \wedge z'$ |
| $x$ | $x \wedge y' \wedge z'$ | $x \wedge y' \wedge z$ | $x \wedge y \wedge z$ | $x \wedge y \wedge z'$ |

Hình 3.10:

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | 1 | 1 | | |
| $x$ | | | 1 | |

$xyz \vee x'y'$

(a)

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | | | | |
| $x$ | 1 | 1 | 1 | 1 |

$x$

(b)

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | | 1 | 1 | |
| $x$ | | 1 | 1 | |

$z$

(c)

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | 1 | | 1 | 1 |
| $x$ | 1 | | | 1 |

$x'y \vee z'$

(d)

Hình 3.11:

*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 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 3.10. 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

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | 1 | | | 1 |
| $x$ | 1 | | | 1 |

$z'$

Hình 3.12:

một biểu thức Boole hai biến, chẳng hạn như Hình 3.11. Hơn nữa bốn hình vuông kề nhau (gọi là quadruple) tương ứng biểu thức một biến như Hình 3.12.

Ta minh họa phương pháp qua các ví dụ sau.

**Ví dụ 3.6.2** 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 3.13

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | | 1 | 1 | |
| $x$ | 1 | | 1 | |

Hình 3.13:

*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 3.14.

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | | 1 | 1 | |
| $x$ | 1 | | 1 | |

Hình 3.14:

(Chú ý rằng, nếu có thể, hãy sử dụng các quadruple như Ví dụ 3.6.3 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

$$g(x, y, z) = (x \wedge y' \wedge z') \vee (x' \wedge z) \vee (y \wedge z).$$

**Ví dụ 3.6.3** 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 3.15).

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | 1 | 1 | 1 | 1 |
| $x$ | | 1 | 1 | |

Hình 3.15:

*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 3.16(a) ta có

$$g_1(x, y, z) = x' \vee (x \wedge z).$$

Sử dụng Hình 3.16(b) ta có

$$g_2(x, y, z) = z \vee (x' \wedge z').$$

Sử dụng Hình 3.16(c) ta có

$$g_3(x, y, z) = x' \vee z.$$

Hiển nhiên hàm $g_3$ là hàm đơn giản nhất!

## 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:

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | 1 | 1 | 1 | 1 |
| $x$ | | 1 | 1 | |

(a)

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | 1 | 1 | 1 | 1 |
| $x$ | | 1 | 1 | |

(b)

| | $y'z'$ | $y'z$ | $yz$ | $yz'$ |
|---|---|---|---|---|
| $x'$ | 1 | 1 | 1 | 1 |
| $x$ | | 1 | 1 | |

(c)

Hình 3.16:

(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) $xyz \vee xy'z' \vee x'yz' \vee x'y'z$.

# Chương 4

# 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.

## 4.1 Mở đầu

### 4.1.1 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.

### 4.1.2 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 $x_1x_2\ldots x_n$ thành từ mã $x_1x_2\ldots x_{n+1}$, 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 13** 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 4.1.1** Nếu nhận được chuỗi bit 1110011 thì đây là từ mã không hợp lệ.

**Ví dụ 4.1.2** 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 4.1.3** Chuỗi 011001 được mã hóa thành từ mã 001111000011.

**Nhận xét 14** 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).

### 4.1.3 Mã sửa sai

Để phát hiện lỗi, trong các ví dụ trước, chúng ta xây dựng 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 4.1.4** 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

000000000, 001001001, 010010010, 011011011,
100100100, 101101101, 111111111.

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.

## 4.2 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 mỗi vector $x = (x_1, x_2, \dots, x_n)^t$ với từ mã $x_1 x_2 \dots x_n$.

**Định nghĩa 4.2.1** $[n, k]$-*mã tuyến tính* trên $\mathbb{B}^n$ là một không gian vector con $k$ chiều của không gian vector $\mathbb{B}^n$ trên trường $\mathbb{B}$; $n$ được gọi là *độ dài* của bộ mã và $k$ là *chiều*. *Hệ số* của bộ mã là tỉ số $k/n$.

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 $x^1, x^2, \dots, x^k$ 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 4.2.2** 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 15** 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 $C$ :

$$\begin{array}{rcl} c^1 & = & 0\,0\,0\,0 \\ c^2 & = & 0\,1\,0\,1 \\ c^3 & = & 1\,1\,1\,0 \\ c^4 & = & 1\,0\,1\,1 \end{array}$$

**Ví dụ 4.2.1** $[5,1]$-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 4.2.2** $[5,3]$-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 4.2.3** $[7,4]$-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

$$x = u^t G. \tag{4.1}$$

Chẳng hạn, sử dụng ma trận sinh $G_2$ của Ví dụ 4.2.2 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 $\pi$ 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 $\pi$ là hoán vị của các ký hiệu $\{0, 1\}$, ta nói $\pi$ 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 4.2.4** (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

$$C := \begin{cases} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{cases}$$

tương đương với mã

$$C' := \begin{cases} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{cases}$$

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 4.2.3** *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 4.2.5** (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 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 thứ $t_i$ thì $t_1 < t_2 < \cdots < t_n$.

(b) Ma trận $G_2$ có thể đưa về ma trận bậc thang

$$G_2' := \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Sử dụng $G_2'$ cho bộ mã $C_2$, mã hoá (4.1) có dạng

$$\begin{cases} x_1 = u_1, \\ x_2 = u_1, \\ x_3 = u_2, \\ x_4 = u_3, \\ x_5 = u_1 + u_2 + u_3. \end{cases}$$

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 4.2.3, ma trận $G_2'$ có thể đưa về

$$G_2'' := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Tổng quát ta có

**Định lý 4.2.4** *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. $\square$

**Định nghĩa 4.2.5** 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

$$Hx = 0 \pmod 2. \tag{4.2}$$

Hệ (4.2) được gọi là *hệ phương trình kiểm tra chẵn lẻ.*

**Ví dụ 4.2.6** $[4,3]$-mã $C_4$ bằng cách thêm một bit kiểm tra chẵn lẻ trong Phần 4.1.2: 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 4.2.7** 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 4.2.6** *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 (4.2) 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 (4.2). 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. $\square$

**Ví dụ 4.2.8** 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 (4.2) 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 các 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 4.2.9** (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

00000 10000 01000 00100
11000 10100 01100 11100.

(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 4.2.7** *Mã đối ngẫu* hay *mã trực giao* $C^{\perp}$ 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 4.2.8** *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. $\square$

## Bài tập

1. Giả sử $H$ là ma trận Boole cấp $r \times n$. Chứng minh tập $C := \{x \in B^n | Hx = 0\}$ 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:

$$C_1 := \begin{cases} 0000 \\ 1100 \\ 0011 \\ 1111 \end{cases}, \qquad C_2 := \begin{cases} 000 \\ 110 \\ 011 \\ 101 \end{cases}.$$

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 $E_n^{\perp}$.

## 4.3 Khoảng cách Hamming

**Định nghĩa 4.3.1** *Khoảng cách Hamming,* ký hiệu $d(x, y)$, giữa hai vector $x = x_1x_2 \ldots x_n$ và $y = y_1y_2 \ldots y_n$ là số các vị trí $i$ mà $x_i \neq y_i, i = 1, 2, \ldots, n$.

Nhận xét rằng $d(x, y)$ chính là số lần thay đổi cần thiết từng bit từ $x$ sang $y$.

**Ví dụ 4.3.1** $d(10111, 00101) = 2, \qquad d(0111, 0000) = 3.$

**Định lý 4.3.2** *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. $\square$

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 không có lỗi, khi đó $y = x$.

(b) Hoặc có lỗi, 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 4.3.2** 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 gởi đi có cùng xác xuất sai $p, 0 \leq p < 1/2$. Chúng ta gọi kênh như thế là *kênh đối xứng nhị phân.*

**Ví dụ 4.3.3** Ký hiệu $P(X)$ là xác suất xảy ra biến cố $X$. Ta có trong kênh đối xứng nhị phân

$$\begin{aligned} P(\{e = 00000\}) = &\quad (1-p)^5, \\ P(\{e = 01000\}) = &\quad p(1-p)^4, \\ P(\{e = 10010\}) = &\quad p^2(1-p)^3. \end{aligned}$$

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 4.3.3** *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 $d$. Do đó $P(x : y)$ cực đại khi $x$ là từ mã gần với $y$ nhất. □

**Định nghĩa 4.3.4** *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 4.3.4** (a) Với $C = \{00000, 01110, 10011, 11111\}$, thì $d(C) = 2$.

(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 4.3.5** *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. $\square$

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 4.3.6** *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. $\square$

**Ví dụ 4.3.5** 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 4.3.7** *Trọng lượng Hamming,* ký hiệu $wt(x)$, của vector $x = x_1x_2\ldots x_n$ là số các chỉ số $i$ sao cho $x_i \neq 0$.

**Ví dụ 4.3.6** $wt(00000) = 0, wt(10111) = 4, wt(11111) = 5$.

**Bổ đề 4.3.8** *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 4.3.9** *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 $1 \leq t \leq k$. 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 $d(C_t) \geq d(C)$.

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 $d \leq n - k + 1$.

    (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

$$2^k(2^k-1)d \leq \sum_{x,y\in C} d(x,y) \leq n2^{2k-1}.$$

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 $M' \geq M/2$.

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 $(d \geq d_1+d_2)$.

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.

## 4.4 Hội chứng

**Định nghĩa 4.4.1** 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 16** (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 4.4.2** *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 4.4.2 ta có thể phân tích $\mathbb{B}^n$ thành hợp các coset rời nhau của $C$ :

$$\mathbb{B}^n = C \cup (a^1 + C) \cup \cdots \cup (a^t + C), \tag{4.3}$$

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 (4.3) 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:

$$x^{(1)} = 0, x^{(2)}, \dots, x^{(s)}, \qquad s = 2^k;$$

các hàng tiếp theo là các coset $a^i + C$ được sắp xếp theo cùng thứ tự với coset leader đặt bên trái:

$$a^i + x^{(1)}, a^i + x^{(2)}, \dots, a^i + x^{(s)}.$$

**Ví dụ 4.4.1** $[4,2]-$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 | | | |

### 4.4.1 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 17** (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

$$s = Hy = Hx + He = He \tag{4.4}$$

(c) Nếu các lỗi xuất hiện tại các vị trí $a, b, c \ldots$ tức là

$$e = 00\ldots 0 \underset{a}{\rightarrow} 100\ldots 00\ldots 0 \underset{b}{\rightarrow} 100\ldots 00\ldots 0 \underset{c}{\rightarrow} 100\ldots$$

thì từ (4.4) 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 4.4.3** *Hội chứng bằng tổng các cột xuất hiện lỗi của ma trận $H$.*

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 4.4.4** *Tồn tại tương ứng một-một lên giữa coset và hội chứng trong mã $C$.*

**Ví dụ 4.4.2** Sử dụng ma trận kiểm tra chẵn lẻ trong Ví dụ 4.2.7 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 $C$ là $[8,4,4]$-mã với 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.

## 4.5 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 $C$, ký hiệu $\#C$.

**Bổ đề 4.5.1** *Giả sử $x \in \mathbb{B}^n, 0 \le k \le n$. Khi đó*

$$\#\{y \in \mathbb{B}^n \mid d(x,y) \le k\} = C(n,0) + C(n,1) + \cdots + C(n,k).$$

*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 bằng $C(n,i)$. □

**Bổ đề 4.5.2** *Giả sử $C$ là bộ mã gồm các từ mã có độ dài $n$ và*

$$d(C) \ge 2k+1.$$

*Khi đó với mỗi $y \in \mathbb{B}^n$, tồn tại nhiều nhất một phần tử $x \in C$, sao cho*

$$y \in B(x,k) := \{z \in \mathbb{B}^n \mid d(x,z) \le k\}.$$

*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. $\square$

**Định lý 4.5.3** *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 4.5.1).

+ Với mỗi $x, x' \in C, x \neq x'$, thì $B(x,k) \cap B(x',k) = \emptyset$. $\square$

**Ví dụ 4.5.1** 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 4.5.4** *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 4.5.2** Mã gồm hai từ mã 00000 và 11111 là mã hoàn hảo.

## Bài tập

1. Tìm số cực đại các từ mã trong một 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

$$\left[\begin{array}{ccccc|cccccccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & G_1 & & & & & & & G_1 & & & \end{array}\right].$$

Chứng minh $\mathcal{G}_2$ sinh ra $[8, 5, 3]$-mã, mâu thuẫn với Định lý 4.5.3).

## 4.6 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 4.4.3, 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 4.6.1** Nếu $r = 3$ thì có $2^3 - 1 = 7$ cột

$$\begin{matrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix}$$

là biểu diễn nhị phân của các số từ 1 đến 7.

**Định nghĩa 4.6.1** *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 4.6.2** 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 4.6.3** 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 4.6.2** *Mã Hamming bậc $r$ chứa $2^{n-r}$ từ mã với $n = 2^r - 1$.*

*Chứng minh.* Hiển nhiên theo định nghĩa. □

**Bổ đề 4.6.3** *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 4.3.6 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 4.3.9 thì

$$d(C) \leq wt(x) = 3.$$

□

**Định lý 4.6.4** *Mã Hamming bậc $r$ là mã hoàn hảo.*

*Chứng minh.* Đặt $n := 2^r - 1$. Theo Bổ đề 4.6.2 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 4.6.4 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 vector 0000111 0001110.

   (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

$$H := \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

   (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 ma trận kiểm tra chẵn lẻ của mã Hamming $[15, 11, 3]$. 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 mã Hamming $\mathcal{H}_3$.

5. Liệt kê ba dạng của ma trận kiểm tra chẵn lẻ $H$ của mã Hamming $\mathcal{H}_4$. 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 $\mathcal{H}_r$ duy nhất theo nghĩa: Bất kỹ mã với các tham số $[2^r - 1, 2^r - 1 - r, 3]$ tương đương với $\mathcal{H}_r$.

7. Tìm ma trận sinh $G$ của mã Hamming $\mathcal{H}_r$ và sử dụng nó để chứng minh mọi từ mã khác không có trọng lượng $\geq 3$. (HD. Nếu tồn tại từ mã có trọng lượng $\leq 2$ 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

$$\frac{(2^r - 1)!}{\prod_{i=0}^{m-1}(2^m - 2^i)}.$$

# Chương 5

# ĐỒ THỊ

Bài báo đầu tiên về lý thuyết đồ thị xuất hiện vào năm 1736 từ một công trình của L. Euler. Sau đó, một vài kết quả quan trọng của lãnh vực này nhận được trong Thế kỷ 19. Tuy nhiên phải đến năm 1920 trở đi, lý thuyết đồ thị mới thực sự phát triển mạnh mẽ và thu hút sự quan tâm của nhiều nhà toán học. Hiển nhiên, một trong những lý do của sự quan tâm này là những ứng dụng của lý thuyết đồ thị trong nhiều lĩnh vực bao gồm Tin học, Hoá học, Ngôn ngữ học, Kinh tế.

## 5.1 Các khái niệm

**Định nghĩa 5.1.1** *Đồ thị vô hướng* $G$, hay đơn giản *graph*, gồm một tập $V$ các *đỉnh* (hay *node*) và một tập $E$ các *cạnh* sao cho mỗi cạnh $e \in E$ tương ứng với một cặp các đỉnh không sắp thứ tự. Nếu có đúng một cạnh $e$ tương ứng các đỉnh $a$ và $b$, ta viết $e := (a, b)$ hoặc $e := (b, a)$.

*Đồ thị có hướng* $G$, hay đơn giản *digraph*, gồm một tập $V$ các *đỉnh* (hay *node*) và một tập $E$ các *cung* sao cho mỗi cung $e \in E$ tương ứng với một cặp các đỉnh được sắp thứ tự. Nếu có đúng một cung $e$ tương ứng các đỉnh được sắp thứ tự $(a, b)$, ta sẽ viết $e := (a, b)$.

Hai đỉnh $a$ và $b$ của đồ thị (vô hướng hoặc có hướng) $G := (V, E)$ gọi là *kề nhau* khi chúng khác nhau và là hai đầu mút của cùng một cạnh (hoặc cung) $e \in E$. Trong trường hợp này ta nói cạnh (cung) $e$ *liên thuộc* $a$ và $b$.

Trong giáo trình này ta sẽ giả thiết các tập $V$ và $E$ là hữu hạn và $V \neq \emptyset$.

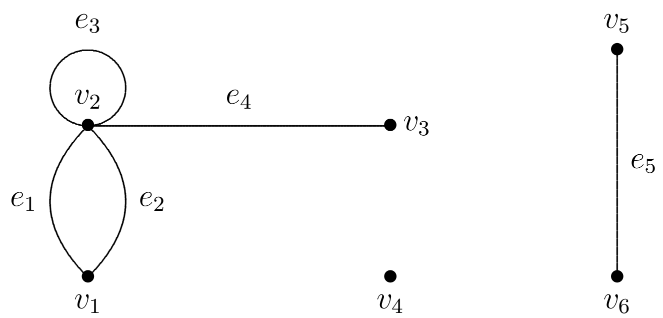
**Ví dụ 5.1.1** Đồ thị vô hướng $G$ trong Hình 5.1 có tập các đỉnh

$$V := \{v_1, v_2, v_3, v_4, v_5, v_6\}$$

và tập các cạnh

$$E := \{e_1, e_2, e_3, e_4, e_5\}.$$

Cạnh $e_1$ liên thuộc các đỉnh $v_1$ và $v_2$. Các đỉnh $v_5$ và $v_6$ là kề nhau (được liên thuộc bởi cạnh $e_5$).




Hình 5.1:

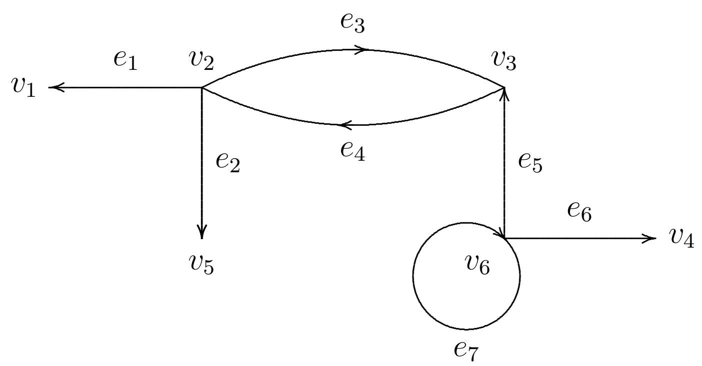
**Ví dụ 5.1.2** Đồ thị có hướng $G$ trong Hình 5.2 có tập các đỉnh

$$V := \{v_1, v_2, v_3, v_4, v_5, v_6\}$$

và tập các cung

$$E := \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}.$$

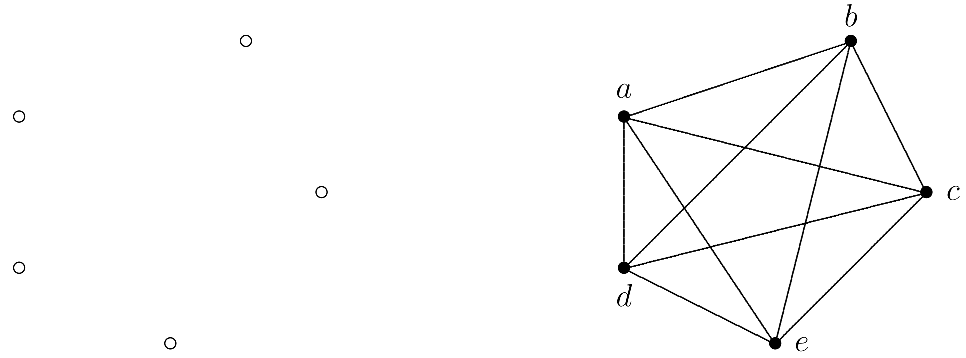
Các cung được biểu diễn bởi các mũi tên. Cung $e_1$ liên thuộc cặp đỉnh $(v_2, v_1)$ và cung $e_7$ liên thuộc cặp đỉnh $(v_6, v_6)$. Hai đỉnh $v_3$ và $v_6$ kề nhau trong khi $v_4$ và $v_5$ không kề nhau.




Hình 5.2:

Nhận xét rằng các cạnh $e_1$ và $e_2$ trong Hình 5.1 tương ứng với cùng cặp đỉnh $v_1$ và $v_2$. Những cạnh như vậy gọi là *song song.* Cạnh liên thuộc với một đỉnh gọi là *khuyên.* Chẳng hạn, trong Hình 5.1 cạnh $e_3 = (v_2, v_2)$ là khuyên. Một đỉnh như $v_4$ trong Hình 5.1 không được liên thuộc với cạnh nào gọi là *đỉnh cô lập.* Đồ thị vô hướng không khuyên và cạnh song song gọi là *đơn đồ thị vô hướng.*

**Ví dụ 5.1.3** Trong các xưởng chế tạo, chúng ta thường dùng máy tính điều khiển máy khoan để khoan các lỗ trên những tấm kim loại như Hình 5.3(a).




(a) (b)

Hình 5.3:

Để tiết kiệm thời gian và tiền bạc, ta cần di chuyển mũi khoan sao cho nhanh nhất. Bài toán có thể mô hình hoá dạng đồ thị như sau: Các đỉnh của đồ thị tương ứng với các lỗ cần khoan (xem Hình 5.3(b)); mỗi cặp đỉnh được nối bằng một cạnh. Với mỗi cạnh ta gán một số thực tương ứng thời gian để di chuyển mũi khoan giữa hai lỗ. Đồ thị với các số được gán trên các cạnh gọi là *đồ thị có trọng số.* Nếu cạnh $e$ được gán nhãn $k$ ta nói rằng trọng lượng của $e$ là $k$. Chẳng hạn, trọng lượng của $G$ cho bởi ma trận trọng lượng

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{pmatrix} 0 & 8 & 2 & 4 & 6 \\ 8 & 0 & 6 & 12 & 9 \\ 2 & 6 & 0 & 3 & 5 \\ 4 & 12 & 3 & 0 & 4 \\ 6 & 9 & 5 & 4 & 0 \end{pmatrix} \end{array}.$$

Trong đồ thị có trọng số, *độ dài của dây chuyền* là tổng của các trọng lượng của các cạnh trên dây chuyền. Ví dụ, trong Hình 5.3(b) độ dài của dây chuyền từ $a$ viếng thăm $b$ và kết thúc tại $c$ là 14. Trong bài toán này, độ dài của dây chuyền xuất phát từ $v_1$ và đi qua $v_2, v_3, \ldots$, theo thứ tự này và kết thúc tại $v_n$ là thời gian để di chuyển mũi khoan khởi đầu từ lỗ $h_1$ và sau đó đến $h_2, h_3, \ldots$, theo thứ tự này và kết thúc tại $h_n$, trong đó ta ký hiệu lỗ $h_i$ tương ứng đỉnh $v_i$. Dây chuyền với độ dài nhỏ nhất đi qua mọi đỉnh của đồ thị tương ứng đường đi tối ưu để di chuyển mũi khoan.

| Dây chuyền | Độ dài |
|---|---|
| $a, b, c, d, e$ | 21 |
| $a, b, d, c, e$ | 28 |
| $a, c, b, d, e$ | 24 |
| $a, c, d, b, e$ | 26 |
| $a, d, b, c, e$ | 27 |
| $a, d, c, b, e$ | 22 |

Bảng 5.1:

| Chương trình | $n_1$ | $n_2$ | $n_3$ |
|---|---|---|---|
| 1 | 66 | 20 | 1 |
| 2 | 41 | 10 | 2 |
| 3 | 68 | 5 | 8 |
| 4 | 90 | 34 | 5 |
| 5 | 75 | 12 | 14 |

Bảng 5.2:

Giả sử trong bài toán trên dây chuyền đòi hỏi bắt đầu từ $a$ và kết thúc tại $e$. Chúng ta có thể tìm dây chuyền có độ dài nhỏ nhất bằng cách liệt kê tất cả các dây chuyền có thể giữa hai đỉnh này và đi qua tất cả các đỉnh khác, mỗi đỉnh một lần và chọn dây chuyền ngắn nhất (xem Bảng 5.1). Ta có dây chuyền qua các đỉnh $a, b, c, d, e$ theo thứ tự này có độ dài nhỏ nhất. Dĩ nhiên với những cặp đỉnh xuất phát và kết thúc khác có thể có dây chuyền với độ dài nhỏ hơn.

Liệt kê tất cả các khả năng như ví dụ trên là tốn nhiều thời gian để tìm dây chuyền có độ dài ngắn nhất. Tuy nhiên, bài toán này-một dạng của *bài toán người du lịch*-trong trường hợp tổng quát không có thuật toán thời gian đa thức!

**Ví dụ 5.1.4** Ví dụ này tìm hiểu bài toán nhóm các đối tượng "tương tự" thành các lớp dựa trên các tính chất của những đối tượng. Chẳng hạn, xét một thuật toán được viết bằng ngôn ngữ PASCAL bởi một số người và chúng ta muốn nhóm các chương trình "tương tự" thành các lớp dựa trên những tính chất nào đó của chương trình (xem Bảng 5.2). Giả sử ta chọn các tính chất

1. Số các dòng lệnh trong chương trình: $n_1$.

2. Số các lệnh "IF" trong chương trình: $n_2$.

3. Số lời gọi thủ tục con trong chương trình: $n_3$.

*Đồ thị vô hướng tương tự* $G$ được xây dựng như sau: Các đỉnh tương ứng với các chương trình. Mỗi đỉnh tương ứng bộ $(p_1, p_2, p_3)$, trong đó $p_i$ là giá trị của tính chất $i$. Ta định nghĩa *hàm phân loại* $s$ như sau: Với mỗi cặp đỉnh $v = (p_1, p_2, p_3)$ và $w = (q_1, q_2, q_3)$ đặt

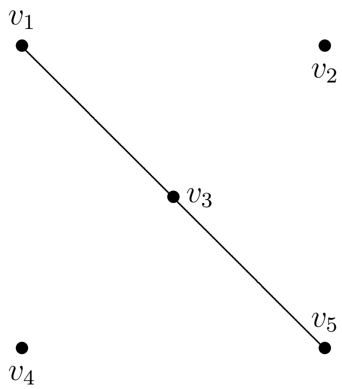
$$s(v, w) := |p_1 - q_1| + |p_2 - q_2| + |p_3 - q_3|.$$

Nếu ký hiệu $v_i$ là đỉnh tương ứng chương trình $i$ thì

$$\begin{aligned}
&s(v_1, v_2) = 36, s(v_1, v_3) = 24, s(v_1, v_4) = 42, s(v_1, v_5) = 30,\\
&s(v_2, v_3) = 38, s(v_2, v_4) = 76, s(v_2, v_5) = 48,\\
&s(v_3, v_4) = 54, s(v_3, v_5) = 20, s(v_4, v_5) = 46.
\end{aligned}$$

Nếu $v, w$ là các đỉnh tương ứng hai chương trình thì $s(v, w)$ đánh giá sự khác nhau của hai chương trình này. Giá trị $s(v, w)$ càng lớn thì sự khác nhau càng nhiều và ngược lại.

Với $S$ cố định cho trước, chèn cạnh $e$ giữa hai đỉnh $v$ và $w$ nếu $s(v, w) < S$. Ta nói rằng $v$ và $w$ *thuộc cùng một lớp* nếu hoặc $v = w$ hoặc tồn tại một dây chuyền từ $v$ đến $w$. Hình 5.4 tương ứng với các chương trình trong Bảng 5.2 với $S = 25$.




Hình 5.4:

Trong đồ thị vô hướng này, các chương trình được nhóm thành ba lớp $\{1, 3, 5\}, \{2\}$ và $\{4\}$. Trong các bài toán thực tế giá trị $S$ thường được chọn thông qua phép thử đúng sai hoặc được chọn tự động theo tiêu chuẩn thực nghiệm trước đó.

Ví dụ này minh họa ứng dụng của đồ thị trong việc *nhận dạng mẫu:* nhóm các dữ liệu thành các lớp dựa trên các tính chất của dữ liệu.

**Nhận xét 18** (a) Theo định nghĩa, các cạnh (cung) của đồ thị thẳng hay cong, dài hay ngắn, các đỉnh ở vị trí nào đều không phải là điều quan trọng, mà điều bản chất là đồ thị có bao nhiêu đỉnh, bao nhiêu cạnh (cung) và đỉnh nào được nối với đỉnh nào.

(b) Tồn tại tương ứng một-một lên giữa đồ thị (vô hướng hoặc có hướng) $G = (V, E)$ và quan hệ hai ngôi trên tập $V$.

## Bài tập

1. Graph $K_n$, gọi là *graph đầy đủ n đỉnh*, có $n$ đỉnh và mọi đỉnh được nối với đỉnh khác bằng một cạnh (không có khuyên và cạnh song song).

   (a) Vẽ $K_3, K_4$ và $K_5$.

   (b) Tìm công thức liên hệ giữa số cạnh và số đỉnh của $K_n$.

2. Graph có các đỉnh được phân hoạch thành hai tập rời nhau $V_1$ và $V_2$ trong đó mỗi cạnh liên thuộc một đỉnh thuộc $V_1$ và một đỉnh thuộc $V_2$ gọi là *graph hai phần*. Cho một ví dụ graph hai phần.

3. Graph hai phần $K_{m,n} = (V_1 \cup V_2, E)$ có $m = \#V_1, n = \#V_2$; mỗi đỉnh của $V_1$ được nối với một đỉnh của $V_2$ bởi một cạnh (không có khuyên và cạnh song song).

   (a) Vẽ $K_{2,3}, K_{2,4}$ và $K_{3,3}$.

   (b) Tìm công thức liên hệ giữa số cạnh và số đỉnh của $K_{m,n}$.

4. Tìm dây chuyền có độ dài nhỏ nhất từ $v$ đến $w$ của graph trong Hình 5.3(b) đi qua mỗi đỉnh chính xác một lần nếu

   (a) $v = b, w = e$.

   (b) $v = c, w = d$.

   (c) $v = a, w = b$.

5. Vẽ graph tương tự trong Ví dụ 5.1.4 nếu $S = 40$. Có bao nhiêu lớp khác nhau?

6. Vẽ graph tương tự trong Ví dụ 5.1.4 nếu $S = 50$. Có bao nhiêu lớp khác nhau?

7. Nói chung, quan hệ "tương tự" là quan hệ tương đương?

# 5.2 Dây chuyền và chu trình

**Định nghĩa 5.2.1** Giả sử $v_0, v_k$ là các đỉnh của đồ thị vô hướng $G := (V, E)$. *Dây chuyền* $\mu$ từ $v_0$ đến $v_k$ độ dài $k$ là một dãy xen kẽ $k + 1$ đỉnh và $k$ cạnh bắt đầu từ $v_0$ và kết thúc tại $v_k$,

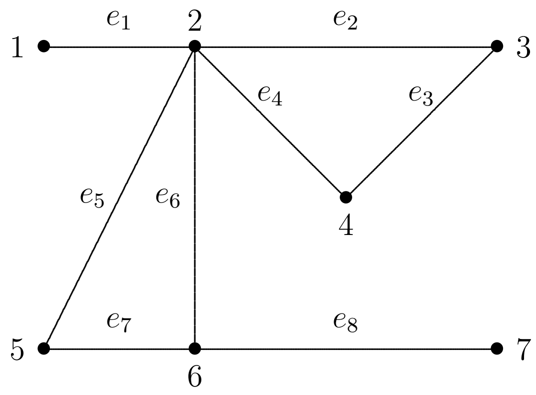
$$\mu := \{v_0, e_1, v_1, e_2, v_2, \ldots, v_{k-1}, e_k, v_k\},$$

trong đó cạnh $e_i$ liên thuộc các đỉnh $v_{i-1}$ và $v_i, i = 1, 2, \ldots, k$.

**Ví dụ 5.2.1** Đồ thị vô hướng trong Hình 5.5 có

$$(1, e_1, 2, e_2, 3, e_3, 4, e_4, 2)$$

là dây chuyền có độ dài 4 từ đỉnh 1 đến đỉnh 2.



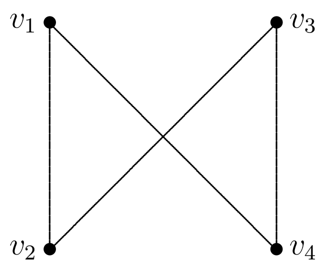

Hình 5.5:

Trong trường hợp đồ thị vô hướng $G$ không có cạnh song song, để đơn giản, dây chuyền $\mu$ được viết

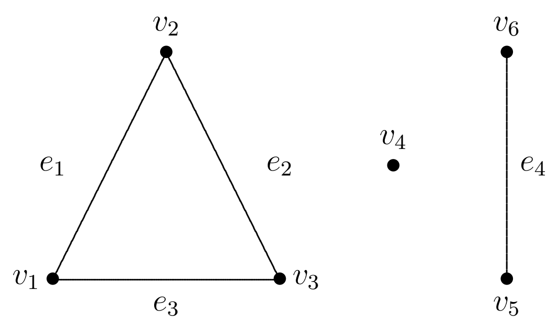
$$\mu := \{v_0, v_1, \dots, v_k\}.$$

**Định nghĩa 5.2.2** Đồ thị vô hướng $G$ được gọi là *liên thông* nếu với hai đỉnh $a, b$ bất kỳ đều tồn tại một dây chuyền nối $a$ với $b$.

**Ví dụ 5.2.2** Dễ kiểm tra rằng đồ thị vô hướng trong Hình 5.6(a) liên thông; còn đồ thị vô hướng trong Hình 5.6(b) không liên thông.




(a)




(b)

Hình 5.6:

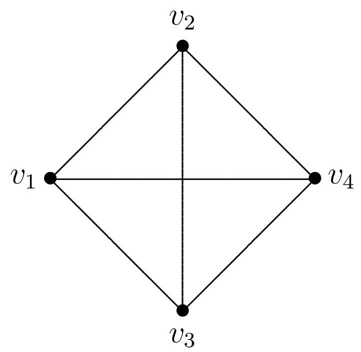
**Định nghĩa 5.2.3** Ta nói $(V', E')$ là *đồ thị con* của đồ thị vô hướng $G := (V, E)$ nếu

(a) $V' \subset V$ và $E' \subset E$;

(b) Nếu cạnh $e' \in E'$ liên thuộc $a$ và $b$ thì $a, b \in V'$.

Giả sử $G := (V, E)$ là đồ thị vô hướng và $a \in V$. Đò thị con $G_a$ của $G$ gồm tất cả các cạnh và các đỉnh trong $G$ mà chứa trong dây chuyền nào đó xuất phát từ $a$ gọi là *thành phần liên thông* của $G$ chứa $a$.

**Ví dụ 5.2.3** Đồ thị vô hướng $G$ trong Hình 5.7 có một thành phần liên thông. Thật vậy, đồ thị vô hướng liên thông nếu và chỉ nếu nó có đúng một thành phần liên thông.




Hình 5.7:

**Ví dụ 5.2.4** Đồ thị vô hướng $G$ trong Hình 5.6(b) gồm ba thành phần liên thông. Thành phần liên thông chứa $v_3$ là đồ thị con

$$G_1 := (V_1, E_1), \quad V_1 = \{v_1, v_2, v_3\}, \quad E_1 = \{e_1, e_2, e_3\}.$$

Thành phần liên thông chứa $v_4$ là đồ thị con

$$G_2 := (V_2, E_2), \quad V_2 = \{v_4\}, \quad E_2 = \emptyset.$$

Thành phần liên thông chứa $v_5$ là đồ thị con

$$G_3 := (V_3, E_3), \quad V_3 = \{v_5, v_6\}, \quad E_3 = \{e_4\}.$$

Ta có thể đặc trưng các thành phần của đồ thị vô hướng $G := (V, E)$ bởi một quan hệ $R$ trên tập $V$ như sau: $aRb$ nếu tồn tại dây chuyền từ $a$ đến $b$. Dễ dàng thấy rằng $R$ là quan hệ tương đương trên $V$ và với mỗi $a \in V$, tập các đỉnh trong thành phần liên thông chứa $a$ là lớp tương đương

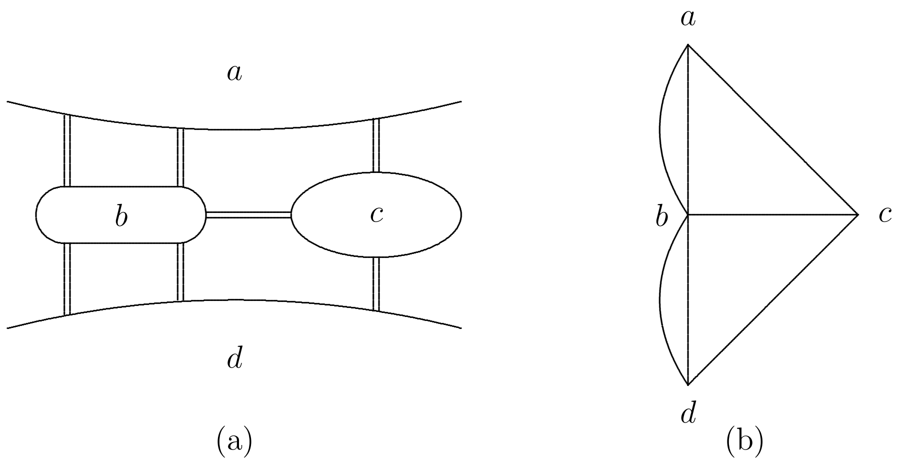
$$[a] = \{b \in V \mid aRb\}.$$

**Định nghĩa 5.2.4** Dây chuyền được gọi là *đơn giản* nếu nó không đi hai lần qua cùng một cạnh. *Chu trình* là một dây chuyền trong đó đỉnh đầu trùng với đỉnh cuối. Chu trình là *đơn giản* nếu nó là một chu trình và là một dây chuyền đơn giản.

**Ví dụ 5.2.5** Các ví dụ về dây chuyền và chu trình của đồ thị vô hướng trong Hình 5.5 được liệt kê trong Bảng 5.3.

| Dây chuyền | Dây chuyền đơn? | Chu trình? | Chu trình đơn? |
|---|---|---|---|
| $(6, 5, 2, 4, 3, 2, 1)$ | Không | Không | Không |
| $(6, 5, 2, 4)$ | Đúng | Không | Không |
| $(2, 6, 5, 2, 4, 3, 2)$ | Không | Đúng | Không |
| $(5, 6, 2, 5)$ | Không | Đúng | Đúng |
| $(7)$ | Đúng | Không | Không |

Bảng 5.3:

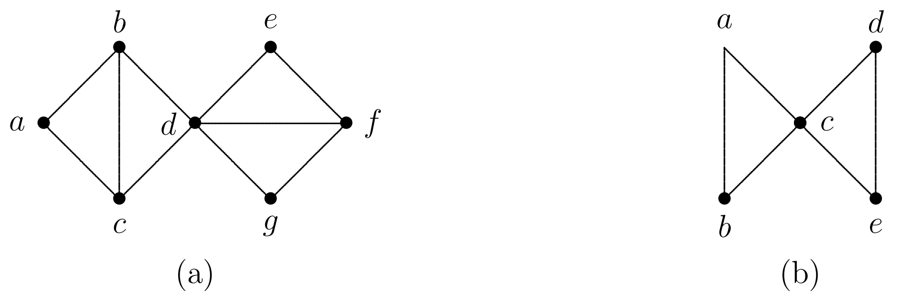



Hình 5.8: (a) Bản đồ của thành phố Königsberg. (b) Đồ thị tương đương.

**Ví dụ 5.2.6** (Bài toán Euler) Cách đây gần ba trăm năm, nhiều người dân thành phố Königsberg của nước Nga (sau này là thành phố Kaliningrat) đã từng thắc mắc vấn đề như sau: Thành phố có sông Pregel chảy qua, giữa sông có cù lao Kneiphof, và có 7 chiếc cầu bắc qua sông như trên Hình 5.8(a); có thể đi dạo qua khắp các cầu nhưng mỗi cầu chỉ đi một lần thôi không? Nếu ta coi mỗi khu vực $a, b, c, d$ của thành phố như một đỉnh, mỗi cầu qua lại hai khu vực như một cạnh nối hai đỉnh, thì bản đồ thành phố Königsberg là một đồ thị vô hướng (Hình 5.8(b)). Thắc mắc của người dân thành phố chính là: có thể vẽ được đồ thị vô hướng bằng một nét bút liền hay không? Nói cách khác: tồn tại chu trình đơn giản (gọi là *chu trình Euler*) chứa mọi đỉnh và cạnh của $G$?

Nhà toán học L. Euler (1707-1783) là người đầu tiên đã chứng minh bài toán không có lời giải (năm 1736), và vì vậy bài toán thường được gọi là bài toán Euler về các cầu ở Königsberg.

**Ví dụ 5.2.7** Có thể vẽ đồ thị vô hướng trên Hình 5.9(a) mà không nhấc bút khỏi mặt giấy và không vẽ một cạnh nào quá hai lần không? Sau khi thử nhiều cách vẽ, dù không có kinh nghiệm bạn đọc cũng có thể kết luận rằng bài toán đó không thể giải được. Trái lại, đồ thị vô hướng ở Hình 5.9(b) có thể vẽ bằng một nét. Tại sao?




Hình 5.9:

**Định nghĩa 5.2.5** Số các cạnh liên thuộc với đỉnh $a$, với khuyên được đếm hai lần, được gọi là *bậc* của đỉnh $a$, ký hiệu $d(a)$. Đỉnh bậc một gọi là *đỉnh treo*, cạnh liên thuộc đỉnh treo gọi là *cạnh treo*.

**Định lý 5.2.6** *Đồ thị vô hướng $G$ có chu trình Euler nếu và chỉ nếu $G$ liên thông và mọi đỉnh của nó đều có bậc chẵn.*

*Chứng minh. Điều kiện cần.* Thật vậy, từ định nghĩa của chu trình Euler suy ra ngay rằng $G$ liên thông. Khi ta vạch ra một chu trình Euler thì mỗi khi đi tới một đỉnh nào theo một cạnh ta lại đi ra khỏi đỉnh ấy theo một cạnh khác, do đó số lần đi tới và số lần đi ra ở mỗi đỉnh luôn luôn bằng nhau; riêng với đỉnh xuất phát $a$, lần đầu ta ra khỏi $a$, lần cuối ta đi tới $a$ khi kết thúc chu trình. Vì vậy mọi đỉnh của $G$ đều có bậc chẵn.

*Điều kiện đủ.* Chứng minh dựa vào bổ đề sau. □

**Bổ đề 5.2.7** *Nếu đồ thị vô hướng $H$ có tất cả các đỉnh bậc chẵn thì từ bất cứ đỉnh nào của nó cũng có thể vạnh được một chu trình đơn giản.*

*Chứng minh.* Thật vậy, từ đỉnh $a$ ta đi theo một cạnh $(a, b)$, rồi từ $b$ đi theo một cạnh khác..., mỗi lần đi theo một cạnh mới. Vì mọi đỉnh của đồ thị vô hướng đều bậc chẵn, nên nếu ta đi theo được một cạnh để tới đỉnh nào thì ta cũng có một cạnh khác để đi ra khỏi đỉnh đó. Do số cạnh của $H$ là hữu hạn nên đường đi phải trở lại $a$ (nơi ta xuất phát theo cạnh $(a, b)$) và ta có một chu trình đơn giản. Bổ đề được chứng minh. □

**Nhận xét 19** Nếu đồ thị vô hướng $G$ chứa một chu trình xuất phát từ $a$ thì nó chứa chu trình đơn giản từ $a$ (tại sao?).

Bây giờ ta chứng minh phần đảo của định lý.

Theo Bổ đề 5.2.7, vì $G$ có tất cả các đỉnh bậc chẵn nên có thể vạch được một chu trình đơn giản $\mu_1$ từ một đỉnh $a$ tùy ý. Ta đánh số 1 tất cả các cạnh của $\mu_1$. Nếu $\mu_1$ chứa tất cả các cạnh của $G$ thì đó là chu trình Euler cần tìm. Giả sử còn một số cạnh của $G$ chưa được đánh số. Các cạnh chưa được đánh số cùng với các đỉnh của chúng lập thành một đồ thị vô hướng $G'$ có các tính chất:

+ Mọi đỉnh của $G'$ đều chẵn (vì mọi đỉnh của $G$ đều chẵn, và ta đánh số một số chẵn cạnh có đầu mút tại mỗi đỉnh).

+ $G'$ và $G$ có ít nhất một đỉnh chung, $b$ chẳng hạn (nếu ngược lại thì $G$ không liên thông, trái giả thiết).

Do đó, theo Bổ đề 5.2.7, từ $b$ ta vạch được một chu trình đơn giản $\mu'$ trong $G'$. Đánh số 2 tất cả các cạnh của $\mu'$. Ta được một chu trình mới $\mu_2$ như sau: đi trên $\mu_1$ từ $a$ đến $b$, rồi đi theo $\mu'$ (các cạnh đánh số 2) cho đến khi quay về $b$, sau đó tiếp tục đi theo $\mu_1$ để trở về $a$. Nếu vẫn còn có cạnh của $G$ chưa được đánh số thì các cạnh này, cùng với đầu mút của chúng, lập thành một đồ thị vô hướng $G''$ có các đỉnh đều chẵn và có chung với $G$ ít nhất một đỉnh ($c$ chẳng hạn). Áp dụng Bổ đề 5.2.7, ta lại vạch được một chu trình đơn giản $\mu''$ trong $G''$ (qua $c$). Đánh số 3 tất cả các cạnh của $\mu''$. Ta được một chu trình mới $\mu_3$ từ $a$ đi theo $\mu_2$ cho đến đỉnh $c$ thì theo $\mu''$ (cạnh đánh số 3) cho tới khi quay về $c$ thì tiếp tục theo $\mu_2$ để trở về $a$. Tiếp tục quá trình trên cho đến khi mọi cạnh của $G$ đều được đánh số (điều này phải xảy ra vì số cạnh của $G$ là hữu hạn), ta được một chu trình $\mu_k$ chứa mọi cạnh của $G$ và đó là chu trình Euler cần tìm. Định lý được chứng minh. □

Cách chứng minh định lý cho ta một thuật toán để vạch được một chu trình Euler trong một đồ thị vô hướng có các đỉnh bậc chẵn: chọn đỉnh xuất phát ($a$); đánh số các chu trình $\mu_1, \mu', \mu_2, \ldots$ như trên, cho đến khi mọi cạnh của $G$ đều được đánh số. Luôn theo quy tắc: mỗi khi đi ra một đỉnh nào thì đi theo một cạnh được đánh số cao nhất trong tất cả các cạnh chưa được dùng, cho đến khi trở lại đỉnh xuất phát mà không thể đi tiếp được nữa (mọi cạnh có đầu mút tại đỉnh xuất phát đã được dùng hết rồi).

**Ví dụ 5.2.8** Cho đồ thị vô hướng trong Hình 5.10. Ta có

$$\begin{aligned} &d(v_1) = d(v_2) = d(v_3) = d(v_5) = 4, \\ &d(v_4) = 6, d(v_6) = d(v_7) = 2. \end{aligned}$$

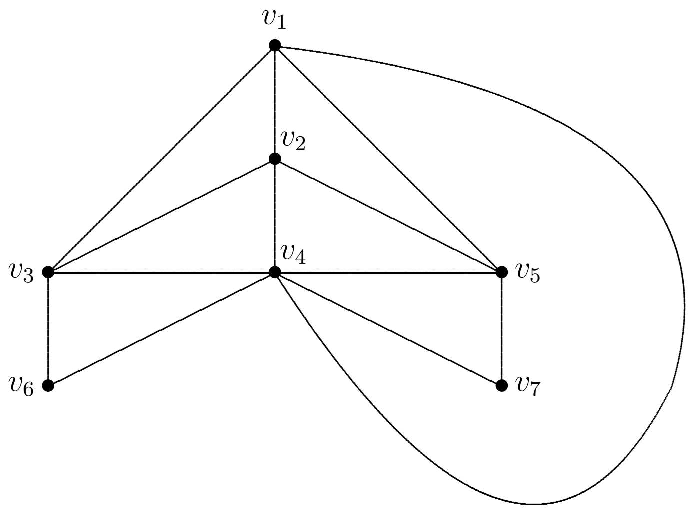
Theo Định lý 5.2.6, $G$ có chu trình Euler, cụ thể là

$$(v_6, v_4, v_7, v_5, v_1, v_3, v_4, v_1, v_2, v_5, v_4, v_2, v_3, v_6).$$

**Định lý 5.2.8** *Giả sử $G$ là đồ thị vô hướng với $m$ cạnh và các đỉnh $\{v_1, v_2, \ldots, v_n\}$. Khi đó*

$$\sum_{i=1}^{n} d(v_i) = 2m.$$

*Do đó, tổng tất cả các bậc của các đỉnh trong đồ thị vô hướng là một số chẵn.*




Hình 5.10:

*Chứng minh.* Bài tập. $\square$

**Hệ quả 5.2.9** *Số các đỉnh bậc lẻ là một số chẵn.*

*Chứng minh.* Ký hiệu $V(c)$ (tương ứng $V(l)$) là tập các đỉnh có bậc chẵn (tương ứng, lẻ) của đồ thị vô hướng $G := (V, E)$. Theo Định lý 5.2.8,

$$2\#E = \sum_{a \in V(c)} d(a) + \sum_{a \in V(l)} d(a).$$

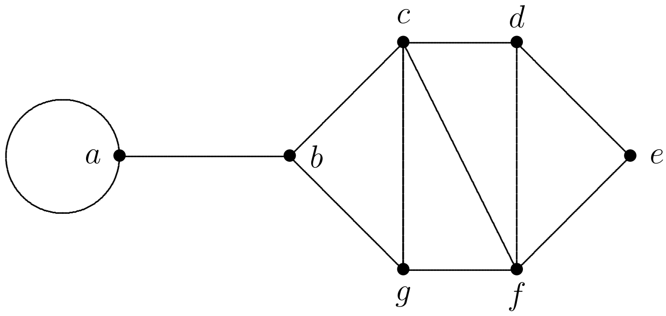
Mà vế trái là một số chẵn và tổng đầu của vế phải cũng là một số chẵn, do đó tổng thứ hai của vế phải là một số chẵn. $\square$

Từ Định lý 5.2.6 ta dễ dàng chứng minh

**Định lý 5.2.10** *Đồ thị vô hướng $G$ có dây chuyền đơn giản từ $a$ đến $b$ ($a \neq b$) chứa tất cả các cạnh và các đỉnh nếu và chỉ nếu $G$ liên thông và mọi đỉnh của nó đều có bậc chẵn ngoại trừ $a$ và $b$ có bậc lẻ.*

## Bài tập

1. Xét graph $G$ trong hình sau:
   (a) Tìm tất cả các dây chuyền đơn giản từ $a$ đến $e$ của graph $G$.
   (b) Tìm tất cả các chu trình đơn giản của graph $G$.
   (c) Tính bậc của các đỉnh của $G$.
   (d) $G$ có thể vẽ bằng mấy nét bút? Như thế nào?




2. Khi nào các đồ thị $K_n$ và $K_{m,n}$ chứa chu trình Euler?

3. Cho ví dụ minh họa graph có chu trình Euler và tìm chu trình này.

4. Xét graph $G$ và hai đỉnh phân biệt $v, w$. Chứng minh rằng nếu tồn tại một dây chuyền từ $v$ đến $w$ thì tồn tại một dây chuyền đơn giản từ $v$ đến $w$.

5. Giả sử $G := (V, E)$ là graph liên thông và cạnh $e$ thuộc một chu trình nào đó. Chứng minh rằng nếu loại cạnh $e$ ra khỏi $G$ thì graph thu được vẫn liên thông. Điều này còn đúng nếu cạnh $e$ không thuộc chu trình nào của $G$?

6. Một con mã có thể đi đến tất cả các ô của bàn cờ quốc tế, mỗi lần di chuyển từ ô này sang ô khác đúng một lần, sau đó trở về vị trí xuất phát?

7. Chứng minh rằng nếu $G'$ là graph con liên thông của $G$ thì $G'$ chứa trong một thành phần liên thông của $G$.

8. Chứng minh rằng nếu $G$ được phân hoạch thành các graph con liên thông sao cho mỗi cạnh và mỗi đỉnh của $G$ thuộc một graph con nào đó thì các graph con là các thành phần liên thông của $G$.

9. Chứng minh rằng số cực đại các cạnh trong đơn graph liên thông $n$ đỉnh là $(n-1)(n-2)/2$.

10. Chứng minh rằng số cực đại các cạnh trong graph đơn hai phần $n$ đỉnh là $n^2/4$.

11. Nếu $G$ là đơn graph liên thông, thì chu trình có độ dài ngắn nhất bằng bao nhiêu? Chu trình sơ cấp có độ dài dài nhất bằng bao nhiêu?

12. Giả sử graph $G$ có $n$ đỉnh thoả $d(v) + d(w) \leq n - 1$ với mọi cặp đỉnh $v$ và $w$ không kề nhau. Chứng minh rằng $G$ liên thông.

13. Chứng minh graph liên thông $G$ là hai phần nếu mọi chu trình của nó có độ dài chẵn.

14. Có bao nhiêu dây chuyền có độ dài $k$ trong $K_n$?

15. Chứng minh tồn tại
$$\frac{n(n-1)[(n-1)^k - 1]}{n-2}$$
dây chuyền độ dài từ 1 đến $n$ trong $K_n, n \geq 2$.

16. Giả sử $v$ và $w$ là các đỉnh phân biệt của $K_n, n \geq 2$. Chứng minh số các dây chuyền đơn giản từ $v$ đến $w$ là

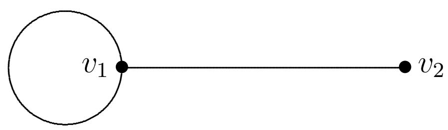
$$(n-2)!\sum_{k=0}^{n-2}\frac{1}{k!}.$$

17. Tìm công thức cho số $N$ các dây chuyền đơn giản trong $K_n$. Chứng minh

$$n! \leq N \leq 3n!.$$

18. Giả sử $G := (V, E)$ là graph. Xét quan hệ $R$ trên $V$ như sau: "$vRw$ nếu và chỉ nếu tồn tại dây chuyền từ $v$ đến $w$". Chứng minh $R$ là quan hệ tương đương trên $V$.

19. Chứng minh số các dây chuyền từ $v_1$ đến $v_1$ độ dài $n$ trong graph sau:



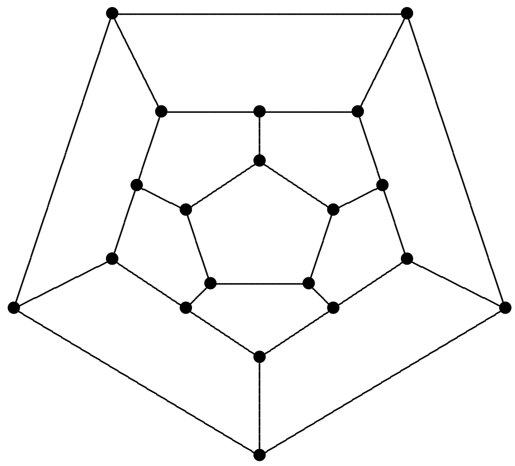

bằng số Fibonacci thứ $n$, trong đó dãy Fibonacci $f_n$ định nghĩa quy nạp như sau:

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

20. Đưa về đồ thị và chứng minh bài toán sau: Trong một câu lạc bộ hai hội viên bất kỳ có chung một người quen thì tồn tại một người quen với tất cả các hội viên khác.

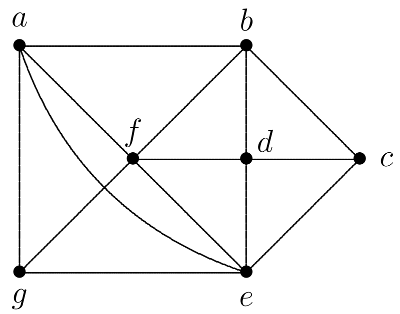
## 5.3 Chu trình Hamilton và bài toán người du lịch

Năm 1859, nhà toán học người Ailen W. R. Hamilton (1805-1865) đã cho bán một đồ chơi độc đáo, phần chính là một khối nhị diện đều (khối đa diện có 12 mặt ngũ giác đều và 20 đỉnh, mỗi đỉnh có 3 cạnh) làm bằng gỗ. Ở mỗi đỉnh có ghi tên một thành phố lớn: Beruych, Quảng châu, Deli, Frangfua, v.v... Cách chơi là tìm một đường đi dọc theo các cạnh của thập nhị diện đều và qua mỗi đỉnh (thành phố) vừa đúng một lần. Một đường đi như thế gọi là một hành trình Hamilton. Muốn trò chơi được hấp dẫn hơn có thể quy định trước trình tự qua một vài thành phố đầu tiên, và để giúp nhớ dễ dàng các thành phố đã đi qua, ở mỗi đỉnh của khối thập nhị diện đều có đóng một chiếc đinh mũ to, quanh đó có thể quấn sợi dây nhỏ để chỉ đoạn đường đã đi qua. Về sau để đơn giản, Hamilton đã thay khối thập nhị diện đều bằng một hình phẳng. Bài toán được phát biểu dưới dạng đồ thị vô hướng như sau. Ta biết rằng hình thập nhị diện đều có 12 mặt, 30 cạnh, 20 đỉnh; mỗi mặt là một ngũ giác đều, mỗi đỉnh là đầu mút của 3 cạnh. Các đỉnh và các cạnh của hình thập nhị diện đều lập thành một đồ thị vô hướng như Hình 5.11. Bài toán đặt ra là hãy tìm một chu trình (gọi là *chu trình Hamilton)* đi qua tất cả các đỉnh của đồ thị vô hướng G, mỗi đỉnh đúng một lần.



Hình 5.11: Hành trình xung quanh thế giới (khối thập nhị diện đều) của Hamilton.

**Ví dụ 5.3.1** $\mu := (a, b, c, d, e, f, g, a)$ là một chu trình Hamilton trong đồ thị vô hướng của Hình 5.12.

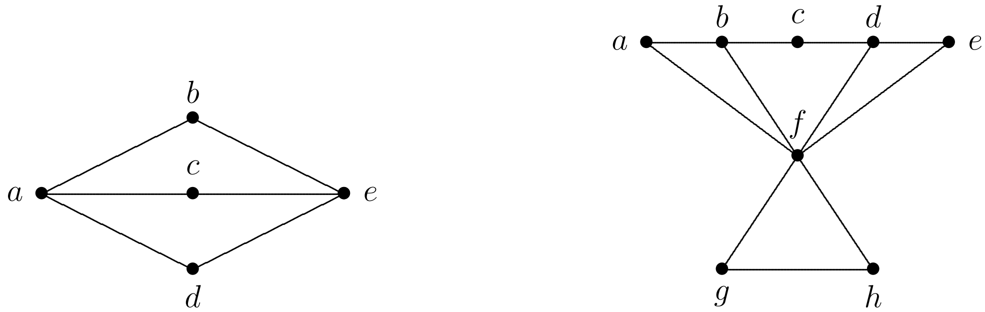



Hình 5.12:

**Ví dụ 5.3.2** Các đồ thị vô hướng trong Hình 5.13 không chứa chu trình Hamilton.

Liên quan đến bài toán tìm chu trình Hamilton trong một đồ thị vô hướng ta có *bài toán người du lịch* sau: Giả sử $G := (V, E)$ là đồ thị vô hướng có trọng số. Tìm một chu trình Hamilton $\mu$ trong $G$ có độ dài tối thiểu:

$$\sum_{e \in \mu} w(e) \to \min .$$




Hình 5.13:

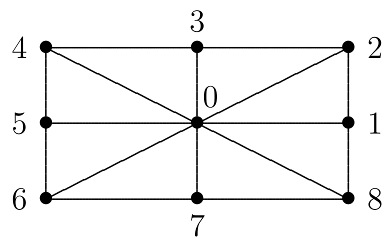
Mặc dù có sự giống nhau nào đó giữa chu trình Euler và chu trình Hamilton, song bài toán tìm chu trình Hamilton khó hơn rất nhiều, còn bài toán người du lịch lại càng khó hơn nữa.

Dựa vào nhận xét là mỗi đỉnh trong chu trình Hamilton đều liên thuộc với đúng hai cạnh trong chu trình này, ta suy ra các quy tắc tìm chu trình Hamilton (nếu có) như sau:

## 5.3.1 Quy tắc tìm chu trình Hamilton

1. Nếu tồn tại đỉnh $a$ sao cho $d(a) \leq 1$ thì $G$ không có chu trình Hamilton.
2. Nếu đỉnh $a$ có bậc là 2 thì cả hai cạnh tới $a$ đều phải thuộc chu trình Hamilton.
3. Chu trình Hamilton không chứa bất kỳ chu trình con thực sự nào.
4. Trong quá trình xây dựng chu trình Hamilton, sau khi đã lấy hai cạnh tới một đỉnh $a$ đặt vào chu trình Hamilton rồi thì không thể lấy thêm cạnh nào tới $a$ nữa, do đó có thể xóa mọi cạnh tới $a$.

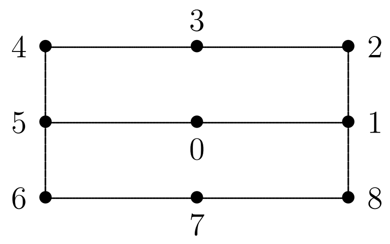
**Ví dụ 5.3.3** Tìm chu trình Hamilton của đồ thị vô hướng trong Hình 5.14.




Hình 5.14:

Xét đỉnh 0. Ta có thể chọn hai cạnh tới đỉnh này là

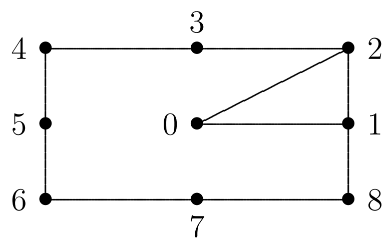
(a) $(0,1),(0,5)$ : xóa các cạnh tới 0 khác (theo Quy tắc 4), ta còn lại đồ thị vô hướng trong Hình 5.15.




Hình 5.15:

Các đỉnh 2, 3, 4 còn lại bậc 2, vậy phải lấy các cạnh $(1, 2), (2, 3), (3, 4), (4, 5)$, nhưng như vậy tạo ra chu trình con thực sự, vô lý.

(b) $(0, 1), (0, 2)$ : xóa các cạnh tới 0 khác (theo Quy tắc 4), ta còn lại đồ thị vô hướng trong Hình 5.16.




Hình 5.16:

Các đỉnh 3, 4, 5, 6, 7 còn lại bậc 2, ta nhận được chu trình Hamilton

$$(0, 2, 3, 4, 5, 6, 7, 8, 1, 0).$$

(c) Lập luận tương tự, các trường hợp chọn $(0, 1), (0, 3)$ và $(0, 1), (0, 4)$ đều không được.

**Ví dụ 5.3.4** Đồ thị vô hướng đầy đủ $K_n$ (có $n$ đỉnh và hai đỉnh bất kỳ là kề nhau) có chu trình Hamilton.

**Định lý 5.3.1** (O. Ore) *Giả sử đơn đồ thị vô hướng $G$ có $n$ đỉnh, và tổng các bậc của hai đỉnh bất kỳ $a, b$ không kề nhau ít nhất bằng $n$. Khi đó tồn tại một chu trình Hamilton.*

*Chứng minh.* Ngược lại với chứng minh định lý Euler, chứng minh này không kiến thiết cho chúng ta một thuật toán để tìm chu trình Hamilton.

Bằng phản chứng, giả sử rằng $G$ là đồ thị vô hướng thỏa mãn điều kiện của định lý, nhưng không tồn tại chu trình Hamilton. Chúng ta cũng có thể giả sử rằng $G$ là *cực đại* theo nghĩa

+ G thỏa điều kiện định lý; và

+ nếu thêm một cạnh (không phải là khuyên) bất kỳ vào $G$, thì đồ thị vô hướng thu được là Hamilton.

Vì $G$ không đầy đủ, nên tồn tại hai đỉnh $a, b$ không kề nhau. Thêm cạnh $e := (a, b)$ vào đồ thị vô hướng $G$, ta thu được đồ thị vô hướng $G'$ có chu trình Hamilton $G'$. Chu trình này chứa cạnh $e$. Do đó $G$ chứa một dây chuyền Hamilton:

$$\mu := \{a = v_1, v_2, \ldots, v_n = b\}.$$

Đặt $A$ là tập tất cả các đỉnh của $G$ kề với đỉnh $a$; và

$$B = \{v_i \mid \text{ đỉnh } v_{i-1} \text{ kề với đỉnh } b\}.$$

Theo giả thiết ta có

$$\#A + \#B \geq n.$$

Nhưng đỉnh $v_n = b$ không thuộc tập $A \cup B$, nên

$$\#(A \cup B) \leq n - 1.$$

Suy ra

$$\#(A \cap B) \geq 1,$$

do đó tồn tại một đỉnh $v_i$ nằm trong $A \cap B$.

Bây giờ chúng ta nhận được mâu thuẫn bằng cách xây dựng một chu trình Hamilton trong $G$ như sau:

+ Bắt đầu từ $a = v_1$, chúng ta đi theo dây chuyền $v_2, v_3, \ldots, v_{i-1}$.

+ Từ đỉnh $v_{i-1}$ chúng ta đi tiếp đến đỉnh $b = v_n$ (do $v_{i-1}$ kề với đỉnh $b$).

+ Từ đỉnh $v_n$ chúng ta quay ngược trở lại $v_{n-1}, v_{n-2}, ..., v_i$ (do $v_i$ kề với đỉnh $a$).

+ Từ đỉnh $v_i$ chúng ta về $v_1$. $\square$

Từ Định lý 5.3.1 dễ dàng suy ra:

**Hệ quả 5.3.2** (Dirac) *Giả sử $G$ là đồ thị vô hướng liên thông $n$ đỉnh ($n \geq 3$) sao cho $d(a) \geq \frac{n}{2}$, với mọi $a \in V$. Khi đó $G$ có chu trình Hamilton.*

### 5.3.2 Mã Gray

Khảo sát sự hoạt động của một đồng hồ đo. Có những vị trí mà tại đó một vài chữ số cần phải thay đổi đồng thời. Do giới hạn của bộ phận cơ khí, các thay đổi này không hoàn toàn đồng thời. Do đó, số ghi tại các vị trí này có thể xảy ra lỗi. Chẳng hạn, trong quá trình thay đổi từ 36999 đến 37000, số ghi trên đồng hồ đo có thể là 36000 hoặc là 37999; và thậm chí nếu chúng ta giả sử rằng các chữ số thay đổi tuần tự từ phải sang trái, thì giá trị 36000 vẫn có thể xuất hiện trên đồng hồ đo.

Để loại trừ lỗi loại này, chúng ta cần sắp xếp các số theo thứ tự (khác với thứ tự thông thường) sao cho chỉ có một chữ số thay đổi tại mỗi bước. Nếu điều đó thực hiện được, thì các lỗi chỉ có thể xảy ra khi các thao tác của máy bị trễ, và nhiều nhất là một lỗi. Trong trường hợp biểu diễn nhị phân, một dãy như vậy được gọi là *mã Gray*.

Xét đồ thị vô hướng $Q_n := (V, E)$, trong đó mỗi đỉnh tương ứng với một vector $n$ chiều trong $\mathbb{B}^n$; hai đỉnh kề nhau nếu hai vector tương ứng chỉ khác nhau đúng một vị trí. (Chú ý rằng đồ thị vô hướng này có $2^n$ đỉnh, mà chúng ta viết như biểu diễn nhị phân của các số nguyên từ 0 đến $2^n - 1$).

**Định lý 5.3.3** *Đồ thị vô hướng $Q_n, n \geq 2$, chứa chu trình Hamilton.*

*Chứng minh.* Chứng minh định lý bằng quy nạp.

+ Với $n = 2$ : ta có chu trình Hamilton $\{00, 01, 11, 10, 00\}$.

+ Giả sử định lý đúng đến $n$ : $Q_n$ có chu trình Hamilton $(v_0, v_1, ..., v_k)$, với $k = 2^n - 1$.

Khi đó

$$0v_0, 0v_1, \ldots, 0v_{k-2}, 0v_{k-1}, 1v_{k-1}, 1v_{k-2}, 1v_1, 1v_0, 0v_0$$

là chu trình Hamilton trong $Q_{n+1}$. $\square$

Chu trình Hamilton trong $Q_n$ cho ta mã Gray. Đặc biệt, chúng ta có thể "mã hóa" và "giải mã" bộ mã này. Thật vậy ta có thể tính số hạng thứ $N, 2^n \geq N$, trong bộ mã Gray, và vị trí (biểu diễn nhị phân) của $N$ trong bộ mã.

**Định lý 5.3.4** *Giả sử $x_{n-1}x_{n-2}\ldots x_0$ là biểu diễn nhị phân của $N$, và*

$$y_i = x_i + x_{i+1} \text{ (mod 2)},\ i = 0, 1, \ldots, n-1 \qquad (x_n = 0).$$

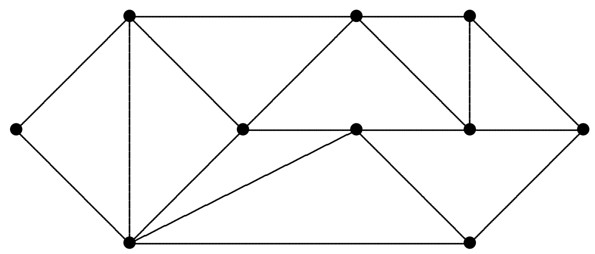
*Nếu $y_{n-1}y_{n-2}\ldots y_0$ là biểu diễn nhị phân của $M$ thì số ở vị trí thứ $N$ trong mã Gray là $M$.*

*Ngược lại đặt $y_{n-1}y_{n-2}\ldots y_0$ là biểu diễn nhị phân của $M$. Giả sử $x_i$ là số các số một trong tập $\{y_{n-1}, y_{n-2}, \ldots, y_i\}$ (lấy mod 2); và đặt $x_{n-1}x_{n-2}\ldots x_0$ là biểu diễn nhị phân của $N$. Khi đó số $M$ xuất hiện ở vị trí thứ $N$ trong mã Gray.*

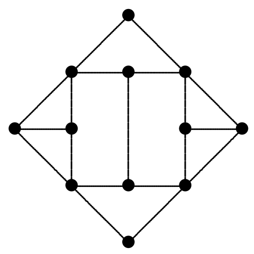
*Chứng minh.* Bài tập. $\square$

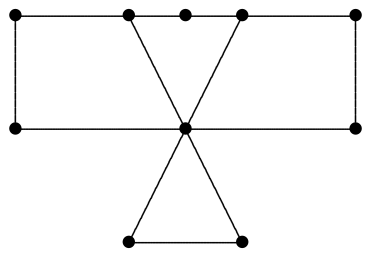
## Bài tập

1. Tìm chu trình Hamilton trong đồ thị sau:



2. Chứng minh các đồ thị sau không chứa chu trình Hamilton:





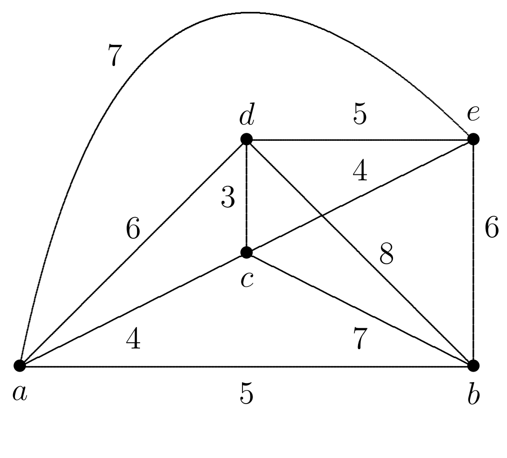
3. Cho ví dụ đồ thị có chu trình Euler nhưng không có chu trình Hamilton.

4. Cho ví dụ đồ thị có các chu trình Euler và chu trình Hamilton và hai chu trình này khác nhau.

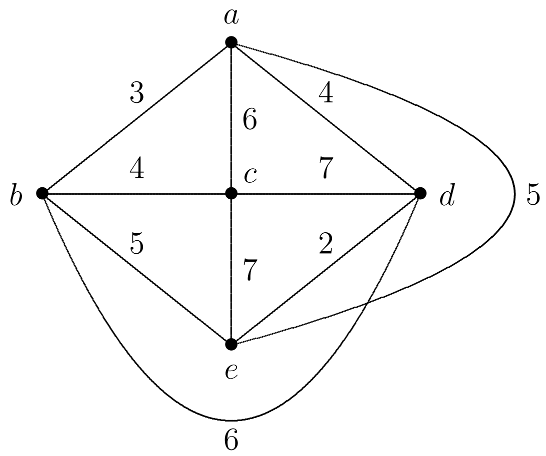
5. Chứng minh $K_n, n \geq 3$, có chu trình Hamilton.

6. Với những giá trị $m, n$ nào thì $K_{m,n}$ có chu trình Hamilton.

7. Chứng minh chu trình $(e, b, a, c, d, e)$ là một lời giải của bài toán người du lịch trong đồ thị sau



8. Giải bài toán người du lịch trong đồ thị:




9. Giả sử $m, n \in \mathbb{N}$ sao cho $1 \leq m \leq 2^n$. Chứng minh đồ thị $Q_n$ có chu trình độ dài $m$ nếu và chỉ nếu $m \geq 4$ và $m$ chẵn.

10. Chứng minh số cực đại các cạnh trong đơn đồ thị hai phần $n$ đỉnh là $n^2/4$.

11. Xét đồ thị hai phần với hai tập đỉnh rời nhau $V_1$ và $V_2$. Chứng minh nếu $G$ có chu trình Hamilton thì $V_1$ và $V_2$ có cùng số phần tử.

12. (a) Đưa về đồ thị bài toán sau: Có thể có các hoán vị của tập $\{1, 2, \ldots, n\}$ được sắp xếp thành một dãy sao cho hai hoán vị kề nhau

$$p : p_1, p_2, \ldots, p_n$$

và

$$q : q_1, q_2, \ldots, q_n$$

thoả mãn $p_i \neq q_i$ với mọi $i = 1, 2, \ldots, n$?

(b) Giải bài toán trên với $n = 1, 2, 3, 4$. (Câu trả lời là "tồn tại" với $n \geq 5$).

## 5.4 Đường đi và mạch

**Định nghĩa 5.4.1** Giả sử $v_0, v_k$ là các đỉnh của đồ thị có hướng $G := (V, E)$. *Đường đi* $\mu$ từ $v_0$ đến $v_k$ độ dài $k$ là một dãy xen kẽ $k+1$ đỉnh và $k$ cung bắt đầu từ $v_0$ và kết thúc tại $v_k$,

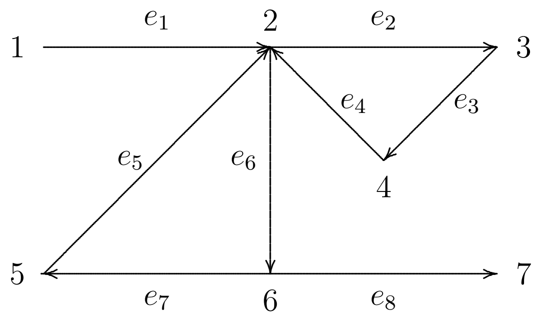
$$\mu := \{v_0, e_1, v_1, e_2, v_2, \ldots, v_{k-1}, e_k, v_k\},$$

trong đó cung $e_i$ liên thuộc các đỉnh $v_{i-1}$ và $v_i, i = 1, 2, \ldots, k$.

**Ví dụ 5.4.1** Đồ thị có hướng trong Hình 5.17 có

$$(1, e_1, 2, e_2, 3, e_3, 4, e_4, 2)$$

là đường đi có độ dài 4 từ đỉnh 1 đến đỉnh 2.




Hình 5.17:

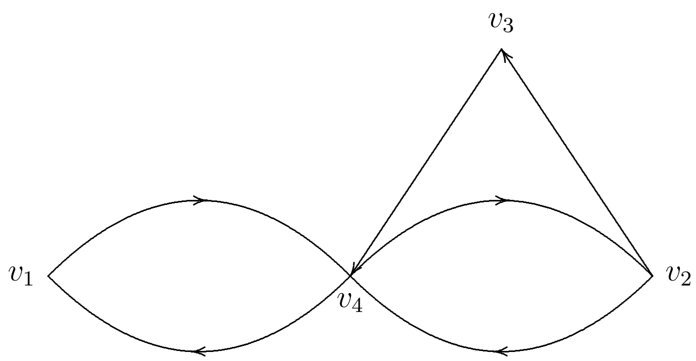
Trong trường hợp đồ thị có hướng không có cung song song, để đơn giản, đường đi $\mu$ trong được viết lại

$$\mu := \{v_0, v_1, \ldots, v_k\}.$$

**Định nghĩa 5.4.2** Số các cung đi khỏi đỉnh $a$ được gọi là *bậc ngoài* của đỉnh $a$, ký hiệu $d^+(a)$. Số các cung đi tới đỉnh $a$ được gọi là *bậc trong* của đỉnh $a$, ký hiệu $d^-(a)$. Đỉnh có bậc ngoài (hay trong) bằng một được gọi là *đỉnh treo;* cung liên thuộc đỉnh treo được gọi là cung treo. Đỉnh có bậc trong bằng không được gọi là *đỉnh vào* (source). Đỉnh có bậc ngoài bằng không được gọi là đỉnh ra (sink).

**Ví dụ 5.4.2** Đồ thị có hướng trong Hình 5.18 có

$$\begin{aligned} d^+(v_1) &= d^-(v_1) = 1, & d^+(v_2) &= 2, d^-(v_2) = 1, \\ d^+(v_3) &= d^-(v_3) = 1, & d^+(v_4) &= 2, d^-(v_4) = 3. \end{aligned}$$




Hình 5.18:

**Định lý 5.4.3** *Trong đồ thị có hướng tổng các bậc trong bằng tổng các bậc ngoài.*

*Chứng minh.* Vì trong đồ thị có hướng $G$ mỗi cung liên thuộc hai đỉnh, mỗi lần đi ra khỏi một đỉnh thì phải đi tới một đỉnh khác. □

*Mạch* là một đường đi trong đó đỉnh đầu trùng với đỉnh cuối. Mạch là *đơn giản (sơ cấp)* nếu nó là một mạch và là một đường đi đơn giản (sơ cấp).

**Định lý 5.4.4** *Mọi đồ thị có hướng không mạch, luôn luôn có thể đánh số thứ tự các đỉnh sao cho mọi đường đi từ đỉnh a đến đỉnh b có $a < b$.*

*Chứng minh.* Bài tập. □

**Định lý 5.4.5** *Tồn tại mạch đơn giản đi qua tất cả các cung của đồ thị có hướng $G$, gọi là mạch Euler, nếu và chỉ nếu graph nhận được bằng cách bỏ qua tất cả các hướng của các cung của $G$ là liên thông và $G$ tựa đối xứng, tức là*

$$d^+(a) = d^-(a)$$

*với mọi đỉnh $a \in V$.*

*Chứng minh.* Bài tập. □

Chúng ta kết thúc mục này với *thuật toán tìm kiếm theo chiều rộng* xác định đường đi giữa hai đỉnh cho trước $s, t \in V$.

### 5.4.1 Thuật toán

Gán mỗi đỉnh của $G$ một chỉ số. Bằng phương pháp lặp, dần dần ta sẽ cho mỗi đỉnh $v$ một chỉ số nào đó bằng độ dài đường đi ngắn nhất từ $s$ tới $v$.

Bước 1. Đánh dấu đỉnh $s$ bằng chỉ số 0.

Bước 2. Nếu các đỉnh được đánh dấu bằng chỉ số $m$ lập thành một tập hợp $V(m)$ đã biết, thì ta đánh dấu chỉ số $m+1$ cho mọi đỉnh của tập hợp:

$$V(m+1) := \{j \text{ chưa được đánh dấu} \mid \text{tồn tại } i \in V(m) \text{ với } (i,j) \in U\}.$$

Ta dừng lại khi không thể đánh dấu được nữa.

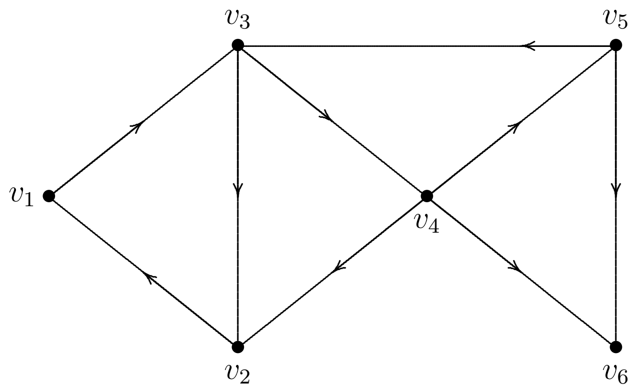
Có hai trường hợp xảy ra:

(a) Đỉnh $t$ được đánh dấu. Nếu $t \in V(m)$, thì xét các đỉnh $v_1, v_2, \ldots,$ sao cho

$$v_1 \in V(m-1), v_2 \in V(m-2), \ldots, v_m \in V(0).$$

Ta có $\mu := \{s = v_m, v_{m-1}, ..., v_1, t\}$ là đường đi phải tìm.

(b) Đỉnh $t$ không được đánh dấu. Khi đó không tồn tại đường đi từ $s$ đến $t$.



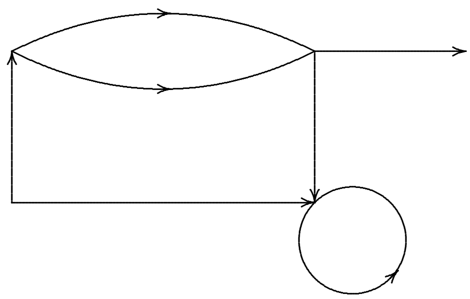

Hình 5.19:

**Ví dụ 5.4.3** Áp dụng thuật toán trên cho đồ thị có hướng trong Hình 5.19, ta có đường đi từ $s = v_1$ đến $t = v_5$ là

$$\mu := (v_1, v_3, v_4, v_5).$$

## Bài tập

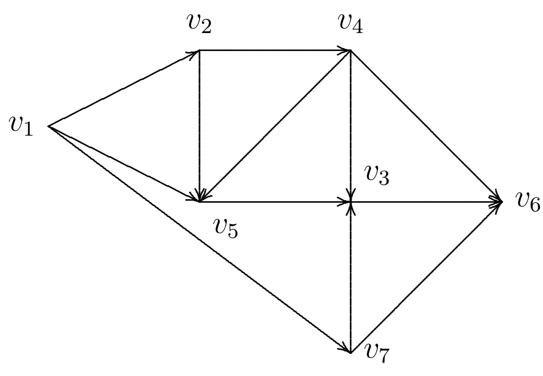
1. Xét các digraph cho trong hình sau



   (a) Tìm bậc trong, bậc ngoài.

   (b) Xác định đỉnh vào, đỉnh ra (nếu có).

2. Xét digraph cho trong hình sau



(a) Tìm các đường đi từ đỉnh $v_1$ đến $v_6$.

(b) Tìm đường đi ngắn nhất từ đỉnh $v_1$ đến $v_6$.

(c) Tìm các đường đi đơn giản từ đỉnh $v_1$ đến $v_6$.

(d) Tìm mạch đi qua đỉnh $v_3$.

3. Cho digraph $G := (V, E)$. Xét quan hệ hai ngôi $\preceq$ trên $V$ định nghĩa như sau: "$x \preceq y$ nếu và chỉ nếu $x = y$ hoặc tồn tại đường đi từ $x$ đến $y$".

   (a) Chứng minh quan hệ $\preceq$ có các tính chất phản xạ và bắc cầu.

   (b) $G$ không có mạch nếu và chỉ nếu từ $x \preceq y$ và $y \preceq x$ suy ra $x = y$, với mọi $x, y \in V$.

   (c) Nếu hai đỉnh bất kỳ có đường đi nối chúng thì với mọi $x, y \in V$, bao giờ cũng có $x \preceq y$ hoặc $y \preceq x$.

4. *Dãy de Bruijin bậc n* là một dãy

$$a_1, a_2, \ldots, a_{2^n}$$

   các bit có tích chất: Nếu $s$ là chuỗi bit độ dài $n$ thì tồn tại $m$ sao cho

$$s = a_m a_{m+1} \cdots a_{m+n-1}.$$

   Trong biểu thức trên, ta định nghĩa $a_{2^n+i} = a_i$ với $i = 1, 2, \ldots, 2^n - 1$.

   (a) Kiểm tra 00011101 là dãy de Bruijn bậc $n = 3$.

   (b) Giả sử $G$ là digraph với các đỉnh tương ứng tất cả các chuỗi bit độ dài $n-1$. Một cung tồn tại và được định hướng từ đỉnh $x_1x_2 \ldots x_{n-1}$ đến đỉnh $x_2x_3 \ldots x_n$. Chứng minh mạch Euler trong $G$ tương ứng với dãy de Bruijn.

   (c) Chứng minh tồn tại dãy de Bruijn với mọi $n = 1, 2, \ldots$.

# 5.5 Ma trận biểu diễn đồ thị

## 5.5.1 Ma trận kề

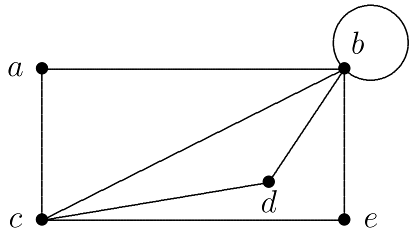
Xét graph $G := (V, U), V := \{v_1, v_2, \ldots, v_n\}$, không có cạnh song song.

**Định nghĩa 5.5.1** *Ma trận kề* (adjacency matrix) của graph $G$, ký hiệu $A(G) := (a_{ij})$, là ma trận boole vuông cấp $n$, xác định bởi

$$a_{ij} := \begin{cases} 1 & \text{nếu có một cạnh nối đỉnh } v_i \text{ với đỉnh } v_j, \\ 0 & \text{nếu ngược lại.} \end{cases}$$

**Ví dụ 5.5.1** Graph $G$ trong Hình 5.20 có ma trận kề là

$$A(G) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$




Hình 5.20:

Từ định nghĩa, dễ dàng suy ra

**Tính chất 5.5.2** *(a) $a_{ii} = 1$ nếu và chỉ nếu $G$ có khuyên tại đỉnh $i$.*

*(b) $A(G)$ là ma trận đối xứng.*

*(c) Nếu graph không khuyên (và không có cạnh song song) thì bậc của một đỉnh bằng số các số 1 trong hàng hay cột tương ứng.*

*d. Hoán vị các hàng và các cột tương ứng tương đương với việc đánh số lại các đỉnh. Tuy nhiên cần chú ý rằng, các hàng và các cột cần được sắp xếp theo cùng một thứ tự. Do đó nếu hai hàng thay đổi thì hai cột tương ứng cũng cần phải thay đổi.*

*e. Graph $G$ có thể tách thành hai thành phần liên thông $G_1$ và $G_2$ nếu và chỉ nếu ma trận kề $A(G)$ có thể viết ở dạng*

$$A(G) = \begin{pmatrix} A(G_1) & 0 \\ 0 & A(G_2) \end{pmatrix},$$

*trong đó $A(G_1)$ và $A(G_2)$ là các ma trận kề tương ứng của các thành phần liên thông $G_1$ và $G_2$.*

*f. Cho trước ma trận $Q$ boole vuông đối xứng cấp $n$, chúng ta có thể xây dựng một graph $n$ đỉnh (không có cạnh song song) sao cho $Q$ là ma trận kề của graph $G$.*

Đặt $A = A^1 := A(G), A^k := (a_{ij}^k) := A^{k-1}A, k \geq 2$. Ta có

**Định lý 5.5.3** *Phần tử $a_{ij}^k, k \geq 1$, là số các dây chuyền khác nhau có độ dài $k$, nối đỉnh $v_i$ với đỉnh $v_j$.*

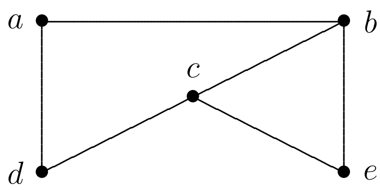
*Chứng minh.* Bài tập. $\square$

**Ví dụ 5.5.2** Graph $G$ trong Hình 5.21 có ma trận kề

$$A(G) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Do đó

$$A^2 = \begin{pmatrix} 2 & 0 & 2 & 0 & 1 \\ 0 & 3 & 1 & 2 & 1 \\ 2 & 1 & 3 & 0 & 1 \\ 0 & 2 & 0 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{pmatrix}, \quad A^4 = \begin{pmatrix} 9 & 3 & 11 & 1 & 6 \\ 3 & 15 & 7 & 11 & 8 \\ 11 & 7 & 15 & 3 & 8 \\ 1 & 11 & 3 & 9 & 6 \\ 6 & 8 & 8 & 6 & 8 \end{pmatrix}.$$




Hình 5.21:

**Hệ quả 5.5.4** *(a) Trong graph liên thông, dây chuyền có độ dài ngắn nhất giữa hai đỉnh $v_i$ và $v_j, i \neq j$, bằng $k$ nếu và chỉ nếu $k$ là số tự nhiên nhỏ nhất sao cho $a_{ij}^k \neq 0$.*

*(b) Đặt $B := A + A^2 + \cdots + A^{n-1}$. Khi đó $G$ không liên thông nếu và chỉ nếu tồn tại ít nhất một phần tử trong ma trận $B$ bằng không.*

## 5.5.2 Ma trận liên thuộc

Giả sử graph $G := (V, E)$ không khuyên, trong đó

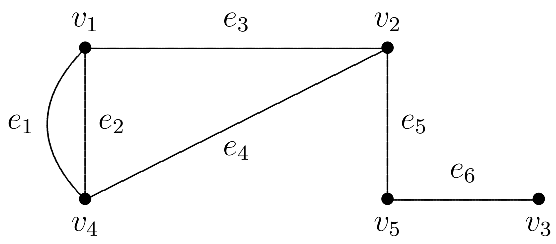
$$V := \{v_1, v_2, \ldots, v_n\}, E := \{e_1, e_2, \ldots, e_m\}.$$

**Định nghĩa 5.5.5** *Ma trận liên thuộc* (incidence matrix) của $G$, ký hiệu $I(G) = (a_{ij})$, là ma trận boole cấp $n \times m$, xác định bởi

$$a_{ij} := \begin{cases} 1 & \text{nếu cạnh thứ } j \text{ liên thuộc đỉnh thứ } i, \\ 0 & \text{nếu ngược lại.} \end{cases}$$

**Ví dụ 5.5.3** Graph $G$ trong Hình 5.22 có ma trận liên thuộc

$$I(G) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$




Hình 5.22:

Như vậy, cho một biểu diễn hình học của graph $G$, không khuyên, chúng ta có thể viết được ma trận liên thuộc của nó. Ngược lại, cho trước ma trận liên thuộc $I(G)$, chúng ta có thể xây dựng dạng hình học của một graph không khuyên. Nói cách khác, ma trận liên thuộc và biểu diễn hình học chứa cùng một thông tin-chúng là hai cách đơn giản để biểu diễn cùng một graph không khuyên.

**Tính chất 5.5.6** *(a) Do mỗi cạnh của graph liên thuộc chính xác hai đỉnh, nên mỗi cột của ma trận $I(G)$ có đúng hai phần tử bằng 1.*

*(b) Số các số 1 trong hàng thứ i bằng bậc của đỉnh tương ứng.*

*(c) Hàng với toàn số 0, tương ứng đỉnh cô lập.*

*(d) Các cạnh song song của graph tương ứng với hai cột trùng nhau của ma trận liên thuộc.*

*(e) Nếu graph $G$ không liên thông, và gồm hai thành phần liên thông $G_1$ và $G_2$ thì ma trận liên thuộc $I(G)$ có dạng*

$$I(G) = \begin{pmatrix} I(G_1) & 0 \\ 0 & I(G_2) \end{pmatrix}, \tag{5.1}$$

*trong đó $I(G_1)$ và $I(G_2)$ là các ma trận liên thuộc tương ứng của các thành phần liên thông $G_1$ và $G_2$.*

*(f) Hoán vị hai hàng hay cột bất kỳ trong ma trận liên thuộc tương ứng với việc thay đổi nhãn của các đỉnh hay các cạnh.*

Kết quả sau cho biết hạng của ma trận liên thuộc của các graph trên trường $B$.

**Định lý 5.5.7** *Hạng của ma trận liên thuộc của graph $n$ đỉnh bằng $n-1$.*

*Chứng minh.* Mỗi hàng trong ma trận liên thuộc $I(G)$ có thể được xem như một vector của không gian vector $m$ chiều trên $\mathbb{B}$. Ký hiệu vector $I_i, i = 1, 2, \ldots, n$, là hàng thứ $i$ của ma trận $I(G)$. Do mỗi cột của ma trận $I(G)$ có chính xác hai số 1, nên tổng của tất cả các vector $I_i$ bằng 0 (modulo 2). Vậy các vector hàng $I_i$ phụ thuộc tuyến tính trên $\mathbb{B}$. Suy ra hạng Rank $I(G)$ của ma trận $I(G)$ nhỏ hơn hoặc bằng $n-1$.

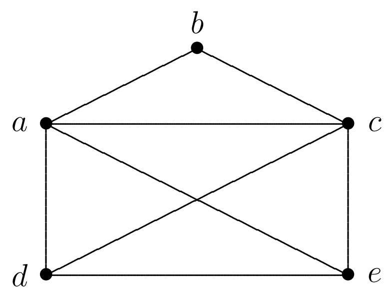
Bây giờ khảo sát tổng của $k, k \leq n-1$, vector trong $n$ vector này. Nếu graph liên thông, thì ma trận $I(G)$ không thể tách như trong (5.1), sao cho $I(G_1)$ tương ứng với $k$ hàng và $I(G_2)$ tương ứng với $n-k$ hàng. Nói một cách khác, không tồn tại ma trận con cấp $k \times k$ của $I(G)$ sao cho tổng của $k$ hàng này (modulo 2) bằng 0.

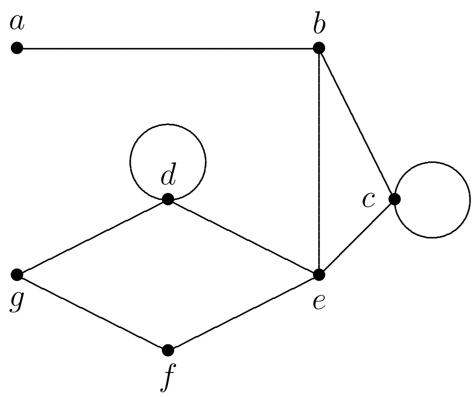
Vì $\mathbb{B} = \{0, 1\}$, nên tổ hợp tuyến tính tùy ý của tất cả $k$ vector (trong $\{I_1, I_2, \ldots, I_n\}$) khác không, với $k = 1, 2, \ldots, n-1$. Vậy Rank $I(G) \geq n-1$. $\square$

Để kết thúc mục này, chúng ta nêu ra câu hỏi sau. Đề nghị bạn đọc tự giải quyết: *Nếu $G$ là đơn graph thì các ma trận kề và ma trận liên thuộc của đồ thị $G$ cùng chứa tất cả các thông tin về $G$. Vì vậy câu hỏi đặt ra là hãy tìm mối liên quan giữa hai ma trận này?*

## Bài tập

1. Viết ma trận kề của các graph sau:




2. Vẽ các graph tương ứng các ma trận kề sau:

$$\begin{array}{c c} & \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \\ e \end{array} & \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \end{array}, \qquad \begin{array}{c c} & \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \\ e \end{array} & \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \end{array}.$$

3. Tính ma trận lũy thừa hai của $K_5$ và các đồ thị trong Bài tập 2.

4. Giả sử $A$ là ma trận kề của graph trong Bài tập 1. Tìm phần tử ở hàng $a$ cột $d$ của $A^5$.

5. Vẽ các graph tương ứng các ma trận liên thuộc sau:

$$\begin{array}{c} a \\ b \\ c \\ d \\ e \end{array}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \qquad \begin{array}{c} a \\ b \\ c \\ d \\ e \end{array}\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

6. Giả sử $A$ là ma trận kề của $K_5$.

   (a) Giải thích tại sao với mọi $n$ nguyên dương, trong ma trận $A^n$ các phần tử trên đường chéo bằng nhau (bằng $d_n$); và các phần tử ngoài đường chéo cũng bằng nhau (bằng $a_n$).

   (b) Chứng minh rằng

$$d_{n+1} = 4a_n; \quad a_{n+1} = d_n + 3a_n; \quad a_{n+1} = 3a_n + 4a_{n-1}.$$

   (c) Chứng minh rằng

$$a_n = \frac{1}{5}[4^n + (-1)^{n+1}].$$

   (d) Chứng minh rằng

$$d_n = \frac{4}{5}[4^{n-1} + (-1)^n].$$

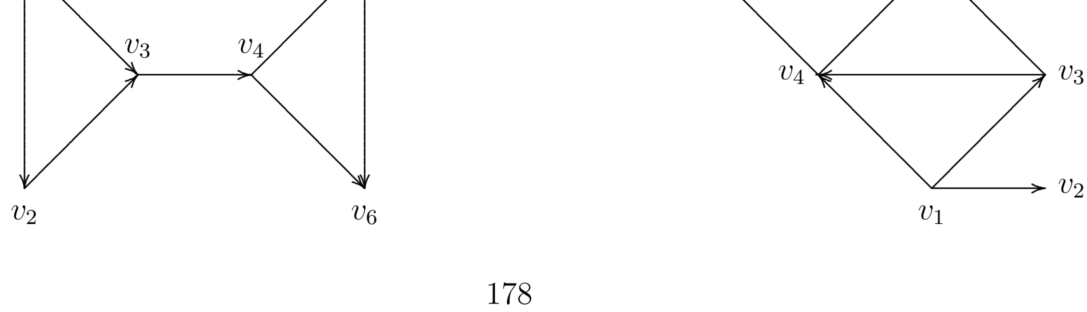
7. Tổng quát hoá Bài tập 8 với $K_n$.

8. Giả sử $A$ là ma trận kề của $K_{m,n}$. Tìm công thức đối với tất cả các phần tử của $A^j$.

9. Ma trận kề của digraph $G$ không khuyên và cung song song với tập đỉnh $V := \{v_1, v_2, \ldots, v_n\}$ là ma trận vuông $A(G) := (a_{ij})$ cấp $n$ có các phần tử xác định bởi

$$a_{ij} = \begin{cases} 1 & \text{nếu hai đỉnh } v_i \text{ và } v_j \text{ kề nhau,} \\ 0 & \text{nếu ngược lại.} \end{cases}$$

   Tìm các ma trận kề của các digraph trong hình sau:



10. Vẽ digraph tương ứng các ma trận kề sau:

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

11. (a) Vẽ digraph tương ứng ma trận kề sau

$$A := \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

    (b) Tìm tất cả các mạch có độ dài 3.

12. Chứng minh phần tử $ij$ của ma trận $A^k$ của digraph $G$ là số các đường đi có độ dài $k$ từ đỉnh $v_i$ đến đỉnh $v_j$.

13. Chứng minh rằng nếu tồn tại đường đi từ $v$ đến $w$ thì tồn tại đường đi đơn giản từ $v$ đến $w$ với độ dài nhiều nhất là $n-1$ trong đó $n$ là số đỉnh của digraph.

14. Giả sử $A$ là ma trận kề của digraph với $n$ đỉnh. Xét *ma trận phạm vi*

$$R = (r_{ij}) := A + A^2 + \cdots + A^{n-1}.$$

    Chứng minh rằng tồn tại đường đi từ đỉnh $v_i$ đến $v_j, i \neq j$, nếu và chỉ nếu $r_{ij} \neq 0$.

## 5.6 Đẳng cấu giữa các đồ thị

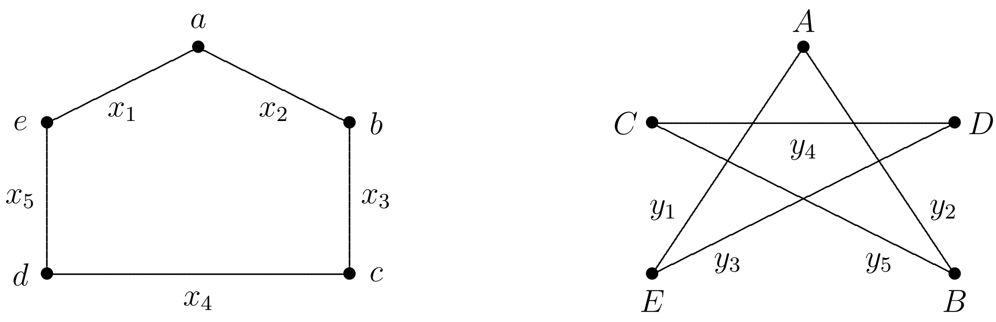
**Định nghĩa 5.6.1** Hai graph $G_1 := (V_1, E_1)$ và $G_2 := (V_2, E_2)$ gọi là *đẳng cấu*, ký hiệu $G_1 \simeq G_2$, nếu tồn tại các ánh xạ một-một lên $f\colon V_1 \to V_2$ và $g\colon E_1 \to E_2$ sao cho cạnh $e$ liên thuộc hai đỉnh $a$ và $b$ nếu và chỉ nếu cạnh $g(e)$ liên thuộc hai đỉnh $f(a)$ và $f(b)$.

Dễ dàng thấy rằng, nếu $G_1 \simeq G_2$ thì $\#V_1 = \#V_2$ và $\#E_1 = \#E_2$. Nói cách khác, số đỉnh và số cạnh là những bất biến.

**Ví dụ 5.6.1** Các graph trong Hình 5.23 là đẳng cấu qua các ánh xạ $f$ và $g$ xác định bởi:

$$f(a) = A, \quad f(b) = B, \quad f(c) = C, \quad f(d) = D, \quad f(e) = E$$

$$g(x_i) = y_i, i = 1, 2, \ldots, 5.$$




Hình 5.23:

Nhận xét rằng quan hệ trên tập các graph xác định bởi $G_1RG_2$ nếu và chỉ nếu $G_1$ và $G_2$ đẳng cấu là quan hệ tương đương.

**Định lý 5.6.2** *Giả sử $G_1 := (V_1, E_1)$ và $G_2 := (V_2, E_2)$ là hai đơn graph. Các khẳng định sau là tương đương.*

(a) *$G_1$ và $G_2$ đẳng cấu;*

(b) *Tồn tại các ánh xạ một-một lên $f: V_1 \to V_2$ sao cho: $a$ và $b$ kề nhau trong $G_1$ nếu và chỉ nếu $f(a)$ và $f(b)$ kề nhau trong $G_2$;*

(c) *Có thể đánh lại số thứ tự các đỉnh sao cho các ma trận kề $A(G_1)$ và $A(G_2)$ là trùng nhau.*

(d) *Các ma trận liên thuộc $I(G_1)$ và $I(G_2)$ chỉ khác nhau bởi các hoán vị hàng hay cột.*

*Chứng minh.* Bài tập. □

**Ví dụ 5.6.2** Ma trận kề của graph $G_1$ trong Hình 5.23 tương ứng thứ tự $a, b, c, d, e$ bằng ma trận kề của graph $G_2$ tương ứng thứ tự $A, B, C, E, E$ và bằng

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

## Bài tập

1. Ta nói tính chất $P$ là *bất biến* nếu với hai graph đẳng cấu $G_1$ và $G_2$ thì $G_1$ có tính chất $P$ suy ra $G_2$ cũng có tính chất $P$. Chứng minh các tính chất sau là bất biến:

   (a) Có chu trình đơn giản độ dài $k$.

(b) Có $n$ đỉnh bậc $k$.

(c) Tính liên thông.

(d) Có $n$ chu trình đơn giản độ dài $k$.

(e) Có một cạnh $(v, w)$ sao cho $d(v) = i, d(w) = j$.

2. Các tính chất sau là bất biến? Nếu đúng, chứng minh; ngược lại cho phản ví dụ:

   (a) Có chu trình Euler.

   (b) Có một đỉnh nằm trong chu trình đơn giản nào đó.

   (c) Graph là hai phần.

3. Vẽ tất cả các đơn graph ba đỉnh không đẳng cấu.

4. Vẽ tất cả các đơn graph bốn đỉnh không đẳng cấu.

5. Vẽ tất cả các graph liên thông không chu trình năm đỉnh không đẳng cấu.

6. Vẽ tất cả các graph liên thông không chu trình sáu đỉnh không đẳng cấu.

7. Cho $G = (V, E)$ là đơn graph. Ta gọi *đồ thị bù* của $G$ là đơn graph $G^c = (V, E^c)$ trong đó tồn tại cạnh trong $G^c$ nếu và chỉ nếu không tồn tại cạnh trong $G$. Chứng minh rằng nếu $G$ là đơn graph thì hoặc $G$ hoặc $G^c$ liên thông.

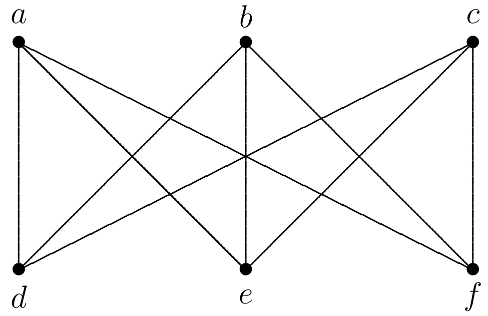
8. Đơn graph $G$ gọi là *tự bù* nếu $G$ và $G^c$ là đẳng cấu. Tìm các graph tự bù có năm đỉnh.

9. Giả sử $G_1$ và $G_2$ là đơn graph. Chứnh minh rằng $G_1$ đẳng cấu với $G_2$ nếu và chỉ nếu $G_1^c$ đẳng cấu với $G_2^c$.

10. *Đồng phôi* $f$ từ graph $G_1$ đến graph $G_2$ là một ánh xạ từ tập các đỉnh của $G_1$ đến tập các đỉnh của $G_2$ sao cho nếu $v$ và $w$ kề nhau trong $G_1$ thì $f(v)$ kề với $f(w)$ trong $G_2$. Chứng minh rằng nếu $f$ là đồng phôi giữa hai đơn graph $G_1$ và $G_2$ và $f$ là một-một lên thì $G_1$ và $G_2$ đẳng cấu.

## 5.7 Đồ thị phẳng

**Ví dụ 5.7.1** (Bài toán ba biệt thự và ba nhà máy). Có ba biệt thự $A, B, C$ và ba nhà máy: một nhà máy nước $D$, một nhà máy hơi đốt $E$ và một nhà máy điện $F$. Mỗi biệt thự nối với các nhà máy bằng những ống dẫn nước, ống dẫn hơi và đường dây điện. Vậy có thể vẽ trên mặt phẳng ba biệt thự và ba nhà máy và tất cả các đường vận chuyển sao cho không có hai đường nào cắt nhau ở một điểm khác các đầu mút của chúng hay không? Ta có mô hình hoá bởi graph $K_{3,3}$ : Các đỉnh của graph tương ứng các nhà và các nhà máy (xem Hình 5.24); một cạnh liên thuộc hai đỉnh tương ứng với một nhà và một nhà máy.



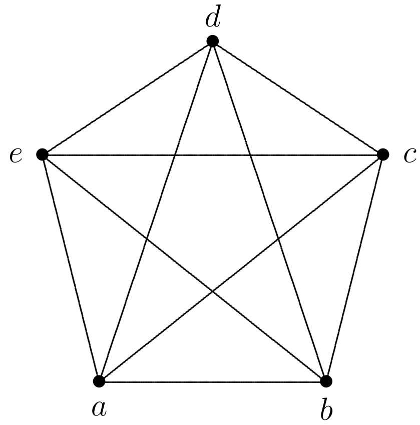

Hình 5.24: Đồ thị Kuratowski $K_{3,3}$.

**Định nghĩa 5.7.1** Graph $G$ được gọi là *phẳng* nếu tồn tại một phép biểu diễn $G$ lên một mặt phẳng sao cho hai cạnh bất kỳ của graph không cắt nhau ngoại trừ tại đỉnh của chúng.

Như vậy Ví dụ 5.7.1 đưa đến câu hỏi: Graph $K_{3,3}$ là phẳng? Điều này sẽ được trả lời trong phần sau.

Câu hỏi tự nhiên đặt ra là: cho trước một đồ thị, thì có một đặc trưng nào cho chúng ta biết được đồ thị là phẳng hay không?

**Ví dụ 5.7.2** Graph $K_5$ trong Hình 5.25 là không phẳng (tại sao?).




Hình 5.25: Đồ thị Kuratowski $K_5$.

Các graph $K_5$ và $K_{3,3}$ có những tính chất:

(a) cả hai là không phẳng;

(b) nếu xoá một cạnh hoặc một đỉnh của graph thì sẽ nhận được một graph phẳng.

(c) $K_5$ là graph không phẳng có số đỉnh nhỏ nhất; $K_{3,3}$ là graph không phẳng có số cạnh nhỏ nhất.

**Định lý 5.7.2** (I. Fary) *Mọi graph phẳng có thể được nhúng trong một mặt phẳng sao cho các cạnh là các đoạn thẳng.*

*Chứnh minh.* Xem [I. Fary, *On straight Line Repesentation of Planar Graphs*, Acta Sci. Math. Szeged, Vol. 11, 229-293 (1948).]. □

Hơn nữa,

**Định lý 5.7.3** *Một graph có thể nhúng trên mặt cầu sao cho các cạnh không tự cắt nếu và chỉ nếu nó có thể nhúng trong mặt phẳng.*

*Chứnh minh.* Sử dụng phép chiếu nổi và Định lý 5.7.2. □

**Định nghĩa 5.7.4** (a) *Diện* của graph phẳng $G$ là một miền của mặt phẳng giới hạn bởi các cạnh của $G$ và sao cho có thể nối hai điểm bằng một nét liền mà không gặp một đỉnh hay một cạnh nào ở bên trong.

(b) *Biên* của diện $z$ là tập các cạnh giới hạn diện $z$.

(c) Hai diện $z$ và $z'$ được gọi là *kề nhau* nếu biên của chúng có ít nhất một cạnh chung (các diện tiếp xúc với nhau chỉ tại một đỉnh thì không phải là kề nhau).

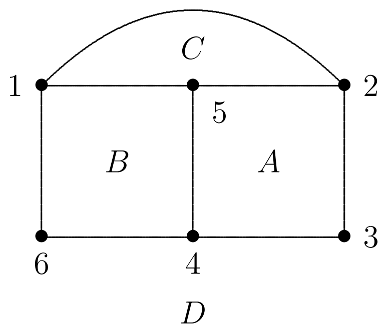
(d) *Chu tuyến* của diện $z$ là các chu trình sơ cấp chứa mọi cạnh khác của biên ở bên trong nó.

Chú ý rằng luôn luôn chỉ có một *diện vô hạn:* nó không có chu tuyến, mọi diện khác được gọi là *diện hữu hạn* và có chu tuyến. Trong graph phẳng, biên của diện $z$ gồm: một hay nhiều chu trình sơ cấp rời nhau, các cạnh treo hay các cạnh nối hai chu trình rời nhau (các cầu).

**Ví dụ 5.7.3** Xét graph trong Hình 5.26. Diện $A$ có biên là chu trình $(5, 2, 3, 4, 5)$ và diện $C$ có biên là chu trình $(1, 2, 5, 1)$. Diện vô hạn $D$ có biên là chu trình $(1, 2, 3, 4, 6, 1)$.

**Định lý 5.7.5** *Một graph phẳng có thể nhúng trong một mặt phẳng sao cho diện bất kỳ cho trước là diện vô hạn.*

*Chứng minh.* Dùng phép quay và Định lý 5.7.3. □




Hình 5.26:

**Ví dụ 5.7.4** Bản đồ địa lý là một graph phẳng. Graph đó có tính chất đặc biệt là bậc của mỗi đỉnh $\geq 3$. Một diện có thể kề với một diện khác ở nhiều cạnh.

**Định lý 5.7.6** (Công thức Euler, 1752) *Giả sử $G$ là graph phẳng liên thông $n$ đỉnh, $m$ cạnh, $d$ diện. Khi đó*

$$d = m - n + 2. \tag{5.2}$$

*Chứng minh. Cách 1:* Chứng minh quy nạp theo số cạnh $m$.

+ Trường hợp $m = 1$. Khi đó $G$ hoặc là một cạnh, hoặc là một khuyên và do đó định lý đúng.

+ Giả sử công thức đúng với mọi graph liên thông phẳng $m$ cạnh.

+ Xét trường hợp $G$ với $m + 1$ cạnh. Trước hết giả sử $G$ không có chu trình. Khi đó tồn tại cạnh treo $e$. Gọi $G'$ là graph (phẳng, liên thông) nhận được từ $G$ bằng cách xoá cạnh $e$ và đỉnh treo liên thuộc $e$. Theo giả thiết quy nạp, (5.2) đúng với $G'$ và do đó suy ra cũng đúng đối với $G$.

Bây giờ giả sử $G$ chứa một chu trình. Đặt $e$ là một cạnh trong chu trình. Khi đó $e$ thuộc đúng hai diện của $G$. Xoá cạnh $e$ (không xoá đỉnh) khỏi $G$ ta nhận được graph phẳng, liên thông $G'$ có $m$ cạnh. Do đó (5.2) đúng đối với $G'$. Một kiểm tra đơn giản chỉ ra đẳng thức cũng đúng đối với $G$. Định lý được chứng minh.

*Cách 2:* Nhận xét rằng chỉ cần chứng minh cho một đơn graph, vì việc thêm một khuyên hoặc thêm một cạnh song song chỉ đơn giản là tăng số diện và số cạnh của graph lên một đơn vị. Chúng ta cũng có thể xoá tất cả các đỉnh treo và các cạnh liên thuộc nó. Nếu thêm (hoặc bớt) một cạnh và một đỉnh thì hiệu số $m - n$ không đổi.

Vì mỗi đơn graph phẳng có thể biểu diễn trên mặt phẳng sao cho mỗi cạnh là một đoạn thẳng (Định lý 5.7.2), nên một graph phẳng có thể được vẽ trên mặt phẳng sao cho các diện là các đa giác. Ký hiệu $d$ là số diện và $k_p$ là số các diện có $p$ cạnh. Vì mỗi cạnh thuộc biên của đúng hai đa giác, nên

$$3k_3 + 4k_4 + 5k_5 + \cdots + rk_r = 2m,$$

trong đó $k_r$ là số các đa giác với số cạnh cực đại.

Mặt khác

$$k_3 + k_4 + \cdots + k_r = d.$$

Tổng tất cả các góc tại mỗi đỉnh trong đa giác tương ứng graph là $2n\pi$. Nhắc lại rằng tổng tất cả các góc trong một đa giác $p$ cạnh là $(p-2)\pi$ và tổng tất cả các góc ngoài là $(p+2)\pi$. Do đó

$$\begin{aligned} 2n\pi &= (3-2)\pi k_3 + (4-2)\pi k_4 + \cdots + (r-2)\pi k_r + 4\pi \\ &= (2m-2d)\pi + 4\pi. \end{aligned}$$

Từ các đẳng thức trên, ta suy ra

$$2(m-d)\pi + 4\pi = 2n\pi.$$

Vậy $d = m - n + 2$. □

**Hệ quả 5.7.7** *Trong một đơn graph phẳng, liên thông có $d$ diện, $n$ đỉnh, $m$ cạnh $(m \geq 2)$, các bất đẳng thức sau luôn nghiệm đúng*

$$\begin{cases} 2m & \geq 3d, \\ 3n-6 & \geq m. \end{cases} \tag{5.3}$$

*Chứng minh.* Mỗi diện có biên ít nhất là ba cạnh, mỗi cạnh là chung của chính xác hai diện, do đó

$$2m \geq 3d.$$

Thay thế $d = m - n + 2$ trong công thức Euler, ta có bất đẳng thức thứ hai. □

Chúng ta lưu ý rằng bất đẳng thức thứ hai chỉ là một điều kiện cần mà không đủ về tính phẳng của một graph phẳng. Nói một cách khác, mọi đơn graph phẳng cần phải thỏa mãn (5.3), nhưng điều ngược lại là không đúng. Chẳng hạn graph Kuratowski $K_{3,3}$ thỏa (5.3), vì

$$m = 9,$$

$$3n - 6 = 3.6 - 6 = 12.$$

Nhưng $K_{3,3}$ không phẳng. Để chứng minh chúng ta cần chỉ ra rằng trong graph này không tồn tại diện mà biên của nó có số cạnh nhỏ hơn 5. Thật vậy, nếu graph là phẳng thì $2m \geq 4d$.

Theo công thức Euler

$$2m \geq 4(m - n + 2).$$

Vậy

$$2.9 \geq 4(9 - 6 + 2).$$

Hay $18 \geq 20$! Mâu thuẫn. Vậy graph $K_{3,3}$ không phẳng.

**Hệ quả 5.7.8** *Mỗi bản đồ địa lý có ít nhất một diện mà số cạnh của chu tuyến nhỏ hơn hoặc bằng 5.*

*Chứng minh.* Thật vậy, trong bản đồ địa lý, mỗi đỉnh là đầu mút của ít nhất 3 cạnh; nếu lập đơn graph liên thuộc đỉnh-cạnh thì số cạnh một mặt $\leq 2m$, mặt khác lại $\geq 3n$, vậy $n \leq 2m/3$. Nếu giả thuyết rằng mỗi diện có chu tuyến gồm ít nhất 6 cạnh và nếu lập đơn graph liên thuộc diện-cạnh, thì số cạnh của nó, một mặt $\leq 2m$, mặt khác lại $\geq 6d$. Vậy $d \leq 2m/6$. Ta luôn luôn có thể giả thiết là graph liên thông (nếu không thì chứng minh hệ quả cho từng thành phần), và do đó có thể viết

$$2 = n - m + d \leq 2m/3 - m + m/3 = 0.$$

Điều đó không thể xảy ra. □

**Hệ quả 5.7.9** *Giả sử $G$ là đơn graph phẳng liên thông. Khi đó tồn tại đỉnh $a \in V$ sao cho $d(a) \leq 5$.*

*Chứng minh.* Thật vậy, trong graph $G$, mỗi diện được bao ít nhất bởi 3 cạnh khác nhau; nếu lập graph $H$ liên thuộc diện-cạnh (tức là graph gồm tập $X$ các điểm dùng để biểu thị các diện, tập hợp $Y$ các điểm dùng để biểu thị các cạnh và các cạnh nối điểm $x \in X$ với $y \in Y$ nếu diện $x$ liên thuộc cạnh $y$) thì số cạnh của graph $H$, một mặt $\leq 2m$, mặt khác lại $\geq 3d$, vậy $d \leq 2m/3$. Nếu mỗi đỉnh là đầu mút ít nhất là của 6 cạnh, thì cũng bằng cách như vậy ta thu được $n \leq 2m/6$, nghĩa là (theo công thức Euler)

$$2 = n - m + d \leq m/3 - m + 2m/3 = 0.$$

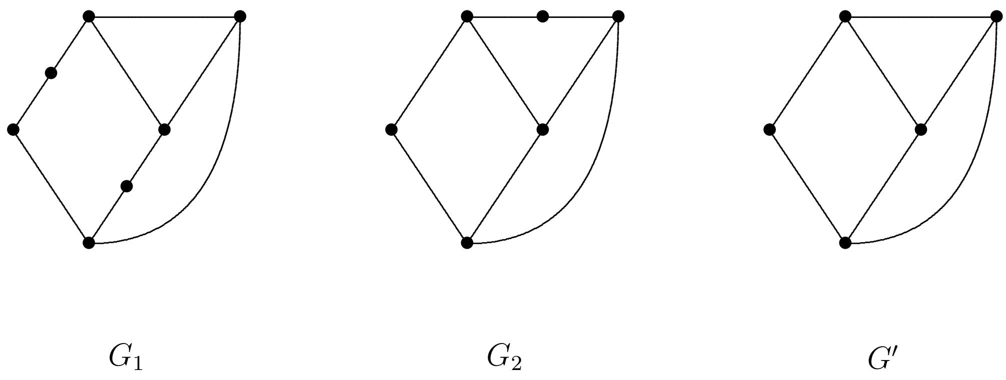
Vô lý! □

**Định nghĩa 5.7.10** (a) Trong một graph, hai cạnh được gọi là trong một *chuỗi*, nếu chúng có đúng một đỉnh chung và nếu đỉnh này có bậc 2.

(b) Hai graph được gọi là *đồng phôi* nếu graph này có thể nhận được từ graph kia bằng cách tạo thêm các cạnh trong chuỗi (tức là chèn thêm các đỉnh bậc hai) hay hợp nhất các cạnh trong chuỗi.

**Ví dụ 5.7.5** Các graph $G_1$ và $G_2$ trong Hình 5.27 là đồng phôi, do có thể đưa về cùng graph $G'$.

Hiển nhiên rằng graph là phẳng nếu và chỉ nếu mọi graph đồng phôi với nó là phẳng. Hơn nữa, quan hệ $R$ trên tập các graph xác định bởi $G_1 R G_2$ nếu và chỉ nếu $G_1$ và $G_2$ đồng phôi là quan hệ tương đương.



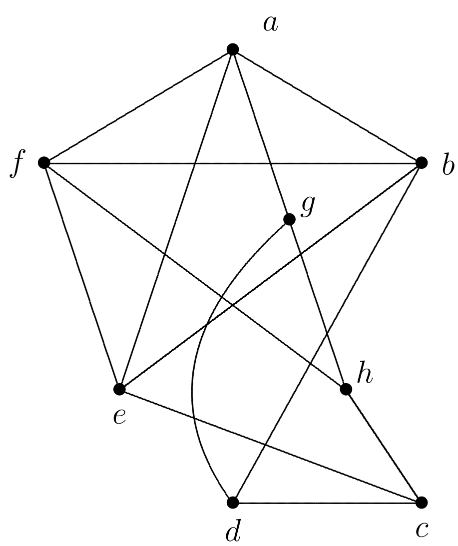

Hình 5.27:

**Định lý 5.7.11** (K. Kuratowski, 1930) *Graph G là phẳng nếu và chỉ nếu G không chứa graph con đồng phôi với hoặc $K_5$ hoặc $K_{3,3}$.*

*Chứng minh.* $\Rightarrow$ Rõ ràng, vì $G$ không thể nhúng trong mặt phẳng nếu nó chứa graph con không thể nhúng được.

$\Leftarrow$ Xem [1]. $\square$

**Ví dụ 5.7.6** Bằng cách áp dụng Định lý Kuratowski ta có đồ thị trong Hình 5.28 không phẳng. Thật vậy, trước hết xoá các cạnh $(a, b), (e, f)$ và $(g, h)$; sau đó "rút gọn" các chuỗi $(a, g), (g, d)$ và $(f, h), (h, c)$ để được các cạnh mới $(a, d)$ và $(f, c)$. Đồ thị thu được là $K_{3,3}$. Suy ra $G$ chứa một đồ thị con đồng phôi với $K_{3,3}$ và do đó không phẳng.

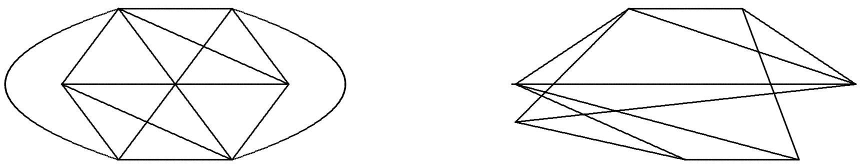



Hình 5.28:

## Bài tập

1. Bằng cách vẽ lại, chứng minh các graph sau là phẳng:

2. Chứng minh các graph sau không phẳng:



3. Một graph liên thông phẳng có chín đỉnh có các bậc tương ứng 2, 2, 2, 3, 3, 3, 4, 4, và 5. Graph này có bao nhiêu cạnh? Có bao nhiên diện?

4. Chứng minh rằng thêm hoặc xoá các khuyên, các cạnh song song, các cạnh trong chuỗi không ảnh hưởng đến tính phẳng của graph.

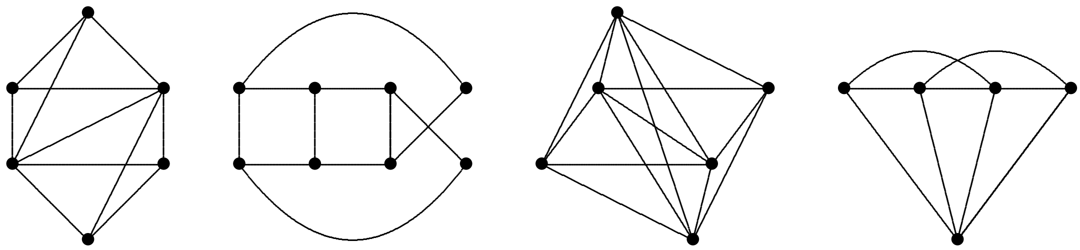
5. Chứng minh rằng graph có nhiều nhất bốn đỉnh là phẳng.

6. Chứng minh rằng graph có nhiều nhất năm đỉnh và một đỉnh bậc hai là phẳng.

7. Chứng minh $K_5$ không phẳng.

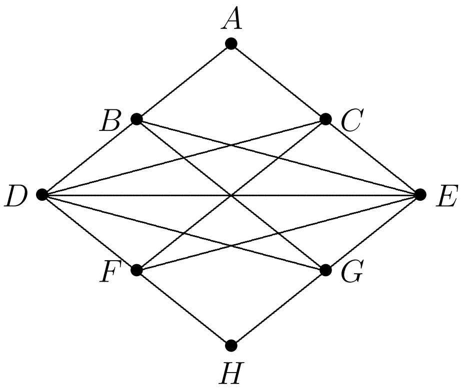
8. Chứng minh nếu đơn graph $G$ có ít nhất 11 đỉnh thì hoặc $G$ hoặc phần bù $G^c$ không phẳng.

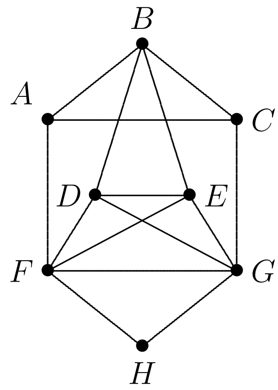
9. Kiểm tra tính phẳng của các đồ thị sau



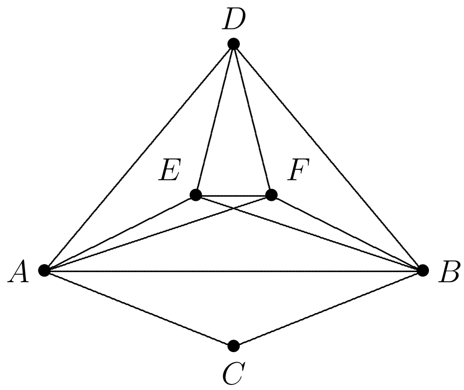
(a) (b) (c) (d)

10. Kiểm tra tính phẳng của các graph sau:

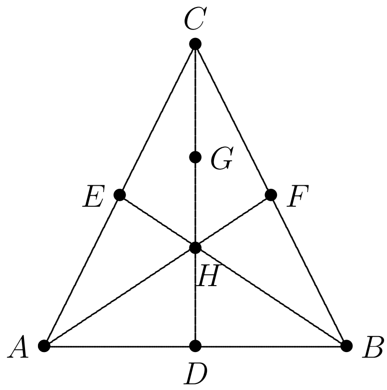



11. Kiểm tra tính phẳng của các graph sau:




(a)




(b)

# Chương 6

# CÂY

## 6.1 Mở đầu

Cây là một trong những khái niệm quan trọng nhất của lý thuyết đồ thị, và thường xuất hiện trong những lãnh vực ít có liên quan đến đồ thị. Khái niệm về cây như một thực thể của toán học được đưa ra lần đầu tiên bởi Kirchhoff [13] khi liên hệ với định nghĩa các mạch cơ bản được sử dụng trong phân tích các mạng điện. Khoảng 10 năm sau đó, một cách độc lập, Cayley [2] đã phát hiện lại các cây và những tích chất của nó khi nghiên cứu các tính chất hoá học của các chất đồng phân của hydrocarbon.

Trong chương này, trước hết sẽ nghiên cứu *cây Huffman* và những ứng dụng của nó trong việc nén dữ liệu. Kế tiếp chúng ta xét trình bày các thuật toán tìm cây bao trùm, cây bao trùm có trọng lượng nhỏ nhất khi các cạnh của đồ thị được gắn với các chi phí (trọng lượng). Cây bao trùm nhỏ nhất của đồ thị có nhiều ứng dụng trong những trường hợp các đường dẫn (ống dẫn ga, dây dẫn trong mạng điện, v.v) được sử dụng để nối $n$ điểm với nhau theo cách tốt nhất: tổng khoảng cách của các đường dẫn là nhỏ nhất. Nếu $n$ điểm được nối với nhau trên một mặt phẳng, ta có thể biểu diễn bởi một đồ thị đầy đủ trong đó các chi phí cạnh là khoảng cách giữa hai điểm tương ứng. Khi đó cây bao trùm với trọng lượng nhỏ nhất sẽ cho mạng giao thông với chi phí ít nhất.

### 6.1.1 Các khái niệm

**Định nghĩa 6.1.1** Các định nghĩa sau của *cây* (vô hướng) là tương đương:

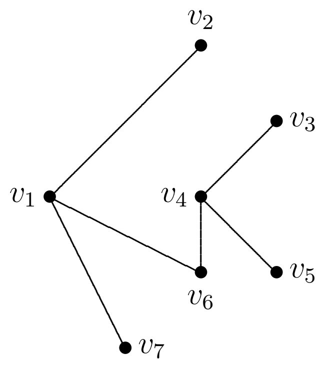
1. Đồ thị liên thông có $n$ đỉnh và $(n-1)$ cạnh.

2. Đồ thị liên thông không có chu trình.

3. Đồ thị mà mọi cặp đỉnh được nối với nhau bởi một và chỉ một dây chuyền sơ cấp.

4. Đồ thị liên thông và khi bớt một cạnh bất kỳ thì mất tính liên thông.

Hình 6.1 minh họa cây có bảy đỉnh và sáu cạnh.




Hình 6.1: Một ví dụ về cây.

*Cây có gốc* (còn gọi là *cây gia phả*) được định nghĩa tương tự như sau:

**Định nghĩa 6.1.2** *Cây có gốc* $T$ là đồ thị có hướng không mạch mà mọi đỉnh, ngoại trừ một đỉnh (chẳng hạn $v_1$), có bậc trong bằng một: bậc trong của đỉnh $v_1$ (gọi là *gốc* của cây) bằng không; nói cách khác, mọi đỉnh $v \in T$ tồn tại duy nhất một đường đi từ gốc đến $v$.

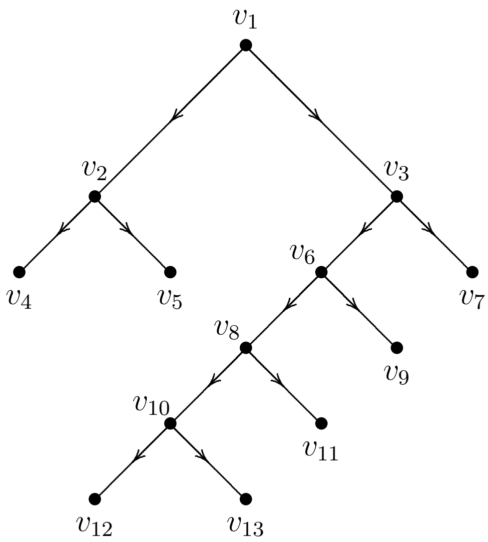
Hình 6.2 minh họa một đồ thị là cây có gốc với đỉnh $v_1$ là gốc. Từ định nghĩa suy ra rằng cây có gốc $n$ đỉnh có $(n-1)$ cung và là đồ thị liên thông (khi bỏ qua hướng trên các cung).

Cần chú ý rằng, có thể định hướng trên một cây (vô hướng) sao cho đồ thị thu được là cây có gốc: Ta chỉ cần chọn một đỉnh tuỳ ý, chẳng hạn $v_1$, làm gốc và định hướng các cung theo dây chuyền từ $v_1$ đến các đỉnh treo. Ngược lại, nếu bỏ qua các hướng trên cây có gốc ta thu được một cây.

Cây gia phả mà trong đó mỗi người đàn ông biểu thị một đỉnh và các cung được vẽ từ các cha đến các con của họ là một ví dụ quen thuộc của cây có gốc, gốc của cây là người đầu tiên trong dòng họ mà có thể xác định được.

### 6.1.2 Mã Huffman

Phương pháp thường dùng để biểu diễn các ký tự trong máy tính là sử dụng các bit có độ dài cố định. Chẳng hạn, mã ASCII (American Standard Code for Information Interchange) biểu diễn mỗi ký tự bởi một chuỗi bảy bit.




Hình 6.2: Một ví dụ về cây có gốc.

Có những bộ mã khác biểu diễn các ký tự bằng các chuỗi bit có độ dài thay đổi như *Mã Huffman*. Ý tưởng là sử dụng các chuỗi bit ngắn để biểu diễn các ký tự thường xuyên xuất hiện và ngược lại. Theo cách này, nói chung, việc lưu trữ các chuỗi văn bản sẽ có lợi hơn khi sử dụng mã ASCII.

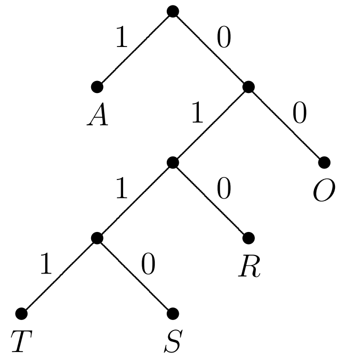
Phương pháp xây dựng mã Huffman dựa trên hai quan sát sau:

1. Trong một bộ mã tốt ưu, các ký hiệu xuất hiện thường xuyên (có xác suất hay tần số xuất hiện lớn) sẽ có các từ mã ngắn hơn các ký hiệu ít xuất hiện.

2. Trong một bộ mã tốt ưu, hai ký hiệu xuất hiện ít nhất sẽ có các từ mã cùng độ dài.

Để xây dựng mã Huffman, chúng ta có thể biểu diễn qua cây nhị phân mà các nút lá tương ứng các ký hiệu. Duyệt cây nhị phân sẽ cho ta các từ mã của bộ mã: xuất phát từ nút gốc và đi đến các nút lá, thêm bit 1 vào từ mã mỗi lần qua nhánh trái và bit 0 mỗi lần qua nhánh phải. Với cây trong Hình 6.3, ta có biểu diễn các ký tự qua các từ mã như sau:

| Ký tự | Mã hoá |
|---|---|
| $A$ | 1 |
| $O$ | 00 |
| $R$ | 010 |
| $S$ | 0110 |
| $T$ | 0111 |




Hình 6.3:

Để giải mã một chuỗi bit, chúng ta bắt đầu từ gốc và di chuyển dọc theo cây cho đến khi gặp ký tự: đi theo nhánh trái nếu đó là bit 1, ngược lại đi theo nhánh phải. Chẳng hạn, chuỗi bit

$$01010111$$

tương ứng từ $RAT$. Với một cây xác định mã Huffman như Hình 6.3, chuỗi bit bất kỳ được giải mã duy nhất mặc dù các ký tự tương ứng với những chuỗi bit có độ dài thay đổi.

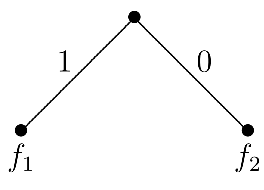
Huffman đã chỉ ra thuật toán xây dựng mã Huffman từ bảng các tần số xuất hiện của các ký tự như sau:

**Thuật toán xây dựng mã Huffman**

Xét chuỗi cần mã hoá $s$ từ $n$ ký tự với $n \geq 2$.

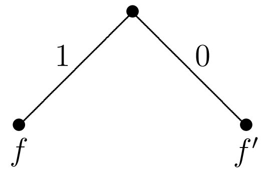
Bước 1. Xây dựng dãy tần số $f_i, i = 1, 2, \ldots, n$, xuất hiện của các ký tự trong chuỗi $s$.

Bước 2. Nếu $n = 2$ (giả sử $f_1 \leq f_2$), xuất cây như trong Hình 6.4 và dừng.




Hình 6.4:

Bước 3. Giả sử $f$ và $f'$ là hai tần số nhỏ nhất và $f \leq f'$. Tạo một danh sách tần số mới bằng cách thay $f$ và $f'$ bởi $f + f'$. Gọi thuật toán này sử dụng danh sách tần số mới để tạo cây $T'$. Thay đỉnh được gán nhãn $f + f'$ để nhận được cây $T$ trong Hình 6.5. Xuất $T$.

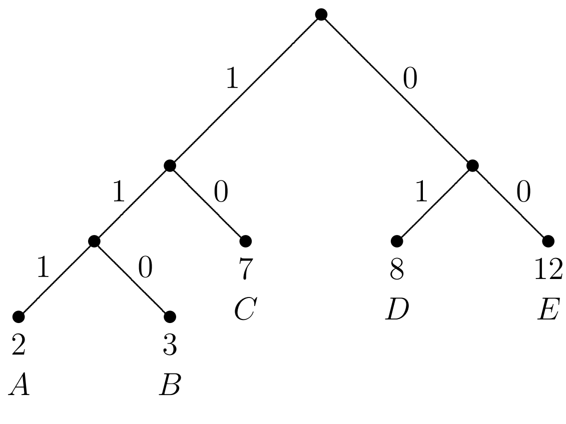



Hình 6.5:

**Ví dụ 6.1.1** Cho bảng tần số

| Ký tự | tần số |
|---|---|
| $A$ | 2 |
| $B$ | 3 |
| $C$ | 7 |
| $D$ | 8 |
| $E$ | 12 |

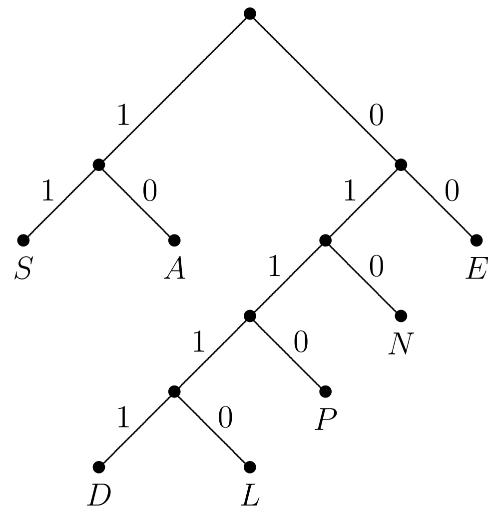
Khi đó cây Huffman tương ứng cho trong Hình 6.6.




Hình 6.6:

## Bài tập

1. Giải mã các chuỗi bit sử dụng cây Huffman sau:




   (a) 011000010.

   (b) 01110100110.

   (c) 01111001001110.

   (d) 1110011101001111.

2. Mã hoá các từ sau sử dụng cây Huffman trong Bài tập 1:

   (a) DEN. (b) NEED. (c) LEADEN. (d) PENNED.

3. Xây dựng cây Huffman với các số liệu sau:

| Ký tự | Tần số |
|---|---|
| $\alpha$ | 5 |
| $\beta$ | 6 |
| $\gamma$ | 6 |
| $\delta$ | 11 |
| $\epsilon$ | 20 |

4. Xây dựng cây Huffman với các số liệu sau:

| Ký tự | Tần số |
|---|---|
| I | 7.5 |
| U | 20.0 |
| B | 2.5 |
| S | 27.5 |
| C | 5.0 |
| H | 10.0 |
| M | 2.5 |
| P | 25.0 |

5. Sử dụng các từ mã trong Bài tập 4 để mã hoá các chuỗi ký tự sau: BUS, MUSH, PUSS, SIP, PUSH, CUSS, HIP, PUP, PUPS, HIPS.

6. Chứng minh cây có ít nhất hai đỉnh thì có một đỉnh treo.

7. Chứng minh cây là graph phẳng.

8. Chứng minh cây là graph hai phần.

9. Chứng minh có thể dùng hai màu để tô màu các đỉnh của cây sao cho hai đỉnh kề nhau có màu khác nhau.

10. Vẽ đồ thị của các công thức hoá học sau: $CH_4, C_2H_6$ và $C_6H_6$.

11. Chứng minh rằng graph $G$ với $n$ đỉnh và ít hơn $n-1$ cạnh không liên thông.

12. Giả sử $G$ liên thông. Chứng minh rằng $G$ là cây nếu và chỉ nếu mọi đỉnh bậc lớn hơn hoặc bằng hai là *khớp*, tức là bỏ đỉnh này đi thì $G$ mất tính liên thông.

## 6.2 Cây bao trùm

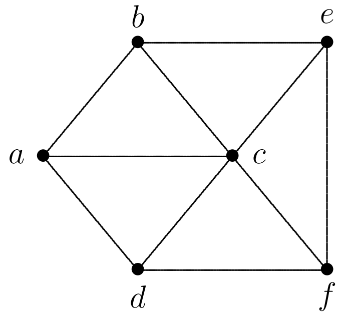
Chúng ta đã nghiên cứu riêng biệt các tính chất của một cây, trong mục này chúng ta sẽ nghiên cứu cây khi gắn nó như một đồ thị con của một đồ thị khác. Chúng ta biết rằng cho đồ thị có $m$ cạnh, có thể xây dựng được $2^m$ đồ thị con khác nhau; rõ ràng là trong số đó có một vài đồ thị con là một cây. Chúng ta quan tâm đến một loại cây đặc biệt: "cây bao trùm". Khái niệm cây bao trùm lần đầu tiên được sử dụng và phát triển lý thuyết về cây bởi nhà vật lý người Đức Kirchoff năm 1847. Kirchoff đã sử dụng cây bao trùm nhằm giải hệ các phương trình tuyến tính để xác định cường độ dòng điện trong mỗi nhánh và xung quanh mạch của một mạng điện.

**Ví dụ 6.2.1** Đồ thị trong Hình 6.7(a) có cây bao trùm trong Hình 6.7(b).

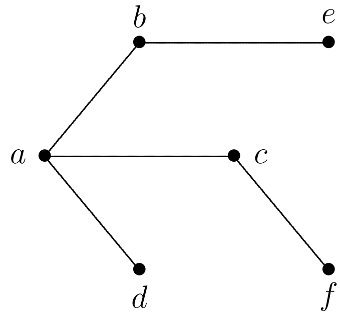
**Định nghĩa 6.2.1** Cây $T$ được gọi là *cây bao trùm* của đồ thị liên thông $G$ nếu $T$ là đồ thị con của $G$ và $T$ chứa tất cả các đỉnh của $G$.

**Định lý 6.2.2** *Đồ thị $G = (V, E)$ có đồ thị bộ phận là một cây nếu và chỉ nếu $G$ liên thông. Nói cách khác, cho trước một đồ thị liên thông và có n đỉnh, bao giờ ta cũng có thể bỏ đi một số cạnh của G để được một cây chứa tất cả các đỉnh của G (cây có n đỉnh).*

*Chứng minh. Điều kiện cần.* Nếu $G$ liên thông thì ta thử tìm xem có cạnh nào mà khi xóa đi không làm cho đồ thị mất tính liên thông không. Nếu không có một cạnh nào như vậy thì $G$ là một cây; nếu có một cạnh như vậy thì xóa nó đi, và ta lại đi tìm một cạnh mới để




(a)




(b)

Hình 6.7:

xóa... Cho tới khi không thể xóa một cạnh nào được nữa thì ta có một cây mà tập hợp các đỉnh của nó đúng bằng $V$.

*Điều kiện đủ.* Giả sử $a, b$ là hai đỉnh trong $G$ và do đó thuộc cây bao trùm $T$ của $G$. Khi đó tồn tại dây chuyền $\mu$ trong $T$ từ $a$ đến $b$. Suy ra $\mu$ cũng thuộc $G$. Vậy $G$ liên thông. $\square$

Chúng ta sẽ sử dụng *thuật toán tìm kiếm theo chiều rộng* để xây dựng cây bao trùm của đồ thị liên thông.

### 6.2.1 Thuật toán tìm kiếm theo chiều rộng xác định cây bao trùm

Trong thuật toán này, $S$ ký hiệu là một dãy.

Nhập: Đồ thị liên thông $G := (V, E)$ với các đỉnh được đánh số thứ tự

$$v_1, v_2, \ldots, v_n.$$

Xuất: Cây bao trùm $T$.

Bước 1. [Khởi tạo] Đặt $S := [v_1]$ và $T$ là đồ thị gồm đỉnh $v_1$ và không có cạnh. Ký hiệu $v_1$ là đỉnh gốc.

Bước 2. [Thêm cạnh] Với mỗi $x \in S$, theo thứ tự, thêm cạnh $(x, y) \in E$ và đỉnh $y$ (theo thứ tự) vào $T$ nếu $T \cup (x, y)$ không tạo thành chu trình. Nếu không có cạnh như vậy, dừng. $T$ là cây bao trùm.

Bước 3. [Cập nhật $S$] Thay $S$ bởi con (trong $T$) của $S$ theo thứ tự. Chuyển sang Bước 2.

Để tìm cây bao trùm của đồ thị liên thông ta còn có thể dùng thuật toán *tìm kiếm theo chiều sâu* (còn gọi là *quay lui*) như sau:

### 6.2.2 Thuật toán tìm kiếm theo chiều sâu xác định cây bao trùm

Nhập: Đồ thị liên thông $G := (V, E)$ với các đỉnh được đánh số thứ tự

$$v_1, v_2, \ldots, v_n.$$

Xuất: Cây bao trùm $T$.

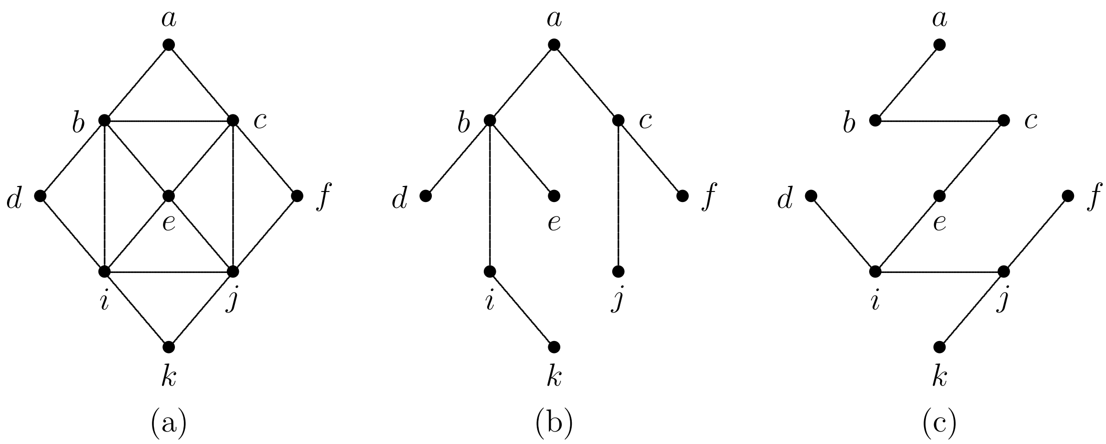
Bước 1. [Khởi tạo] Đặt $w := v_1$ và $T$ là đồ thị gồm đỉnh $v_1$ và không có cạnh. Ký hiệu $v_1$ là đỉnh gốc.

Bước 2. [Thêm cạnh] Chọn cạnh $(w, v_k)$ với chỉ số $k$ nhỏ nhất sao cho việc thêm cạnh này vào $T$ không tạo ra chu trình. Nếu không tồn tại, chuyển sang Bước 3. Ngược lại, thêm cạnh $(w, v_k)$ và đỉnh $v_k$ vào $T$; đặt $w := v_k$ và chuyển sang Bước 2.

Bước 3. [Kết thúc?] Nếu $w = v_1$, thuật toán dừng, $T$ là cây bao trùm.

Bước 4. [Quay lui] Đặt $x$ là cha của $w$ (trong $T$); gán $w := x$ và chuyển sang Bước 2.

**Ví dụ 6.2.2** Đồ thị trong Hình 6.8(a) có các cây bao trùm, Hình 6.8(b) và 6.8(c), được xây dựng theo các thuật toán tìm kiếm theo chiều rộng và chiều sâu tương ứng.




Hình 6.8: (a) Đồ thị $G$. (b) Cây bao trùm sinh bởi thuật toán tìm kiếm theo chiều rộng. (c) Cây bao trùm sinh bởi thuật toán tìm kiếm theo chiều sâu.

## Bài tập

1. Cho các ví dụ minh họa sự hoạt động của các thuật toán tìm kiếm theo chiều rộng (ký hiệu BFS) và chiều sâu (ký hiệu DFS) tìm cây bao trùm của graph.

2. Sắp tám con Hậu trên bàn cờ quốc tế sao cho không con nào ăn con nào.

3. Chứng minh không tồn tại lời giải bài toán hai và ba con hậu.

4. Tìm một lời giải của bài toán năm con hậu và sáu con hậu.

5. Khẳng định sau đúng hay sai, nếu đúng hãy chứng minh; ngược lại, cho phản ví dụ: Nếu $G$ liên thông và $T$ là cây bao trùm của $G$ thì tồn tại một cách đánh số thứ tự các đỉnh của $G$ sao cho thuật toán BFS (tương ứng, DFS) tạo ra cây bao trùm $T$.

6. Bằng ví dụ chứng minh rằng thuật toán BFS (tương ứng, DFS) sinh ra cùng một cây bao trùm từ hai đỉnh phân biệt của graph liên thông $G$.

7. Chứng minh tính đúng đắn của các thuật toán BFS và DFS tìm cây bao trùm.

8. Với những điều kiện nào thì một cạnh trong graph liên thông $G$ được chứa trong mọi cây bao trùm của $G$?

9. Giả sử $T$ và $T'$ là hai cây bao trùm của graph liên thông $G$. Giả sử $x$ là cạnh trong $T$ nhưng không trong $T'$. Chứng minh tồn tại một cạnh $y$ trong $T'$ nhưng không thuộc $T$ sao cho $(T \setminus \{x\}) \cup \{y\}$ và $(T' \setminus \{y\}) \cup \{x\}$ là các cây bao trùm của $G$.

10. Xây dựng thuật toán dựa trên BFS tìm độ dài tối thiểu của mỗi dây chuyền trong graph không có trọng số từ một đỉnh $v$ cố định đến tất cả các đỉnh khác.

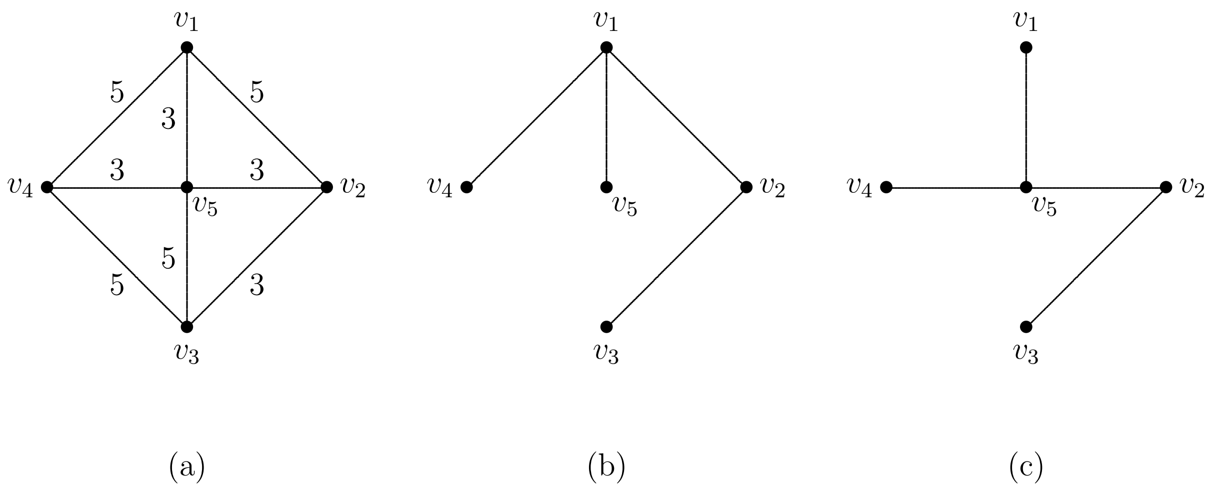
11. Xây dựng các thuật toán BFS, DFS kiểm tra tính liên thông của graph.

## 6.3 Cây bao trùm nhỏ nhất

**Định nghĩa 6.3.1** Giả sử $G$ là đồ thị có trọng số. *Cây bao trùm tối thiểu* của $G$ là một cây bao trùm của $G$ với trọng lượng nhỏ nhất.

Bài toán này rất hay gặp trong thông tin liên lạc và trong các ngành khác. Chẳng hạn ta đặt câu hỏi như sau: độ dài dây điện ngắn nhất cần thiết để nối $n$ thành phố đã định là bao nhiêu? Khi đó coi các thành phố là các đỉnh của đồ thị và $w(a, b)$ là khoảng cách tính bằng km giữa các thành phố $a$ và $b$. Mạng dây điện cần phải liên thông, và vì độ dài dây điện cần ngắn nhất nên nó không có chu trình: vậy mạng đó là một cây. Ở đây ta cần tìm một cây "tối thiểu" có thể được và là một đồ thị bộ phận của đồ thị đầy đủ có $n$ đỉnh. Một ứng dụng gián tiếp: bài toán tìm cây bao trùm tối thiểu là bước trung gian trong việc tìm lời giải của bài toán người du lịch-một bài toán thường xuất hiện trong thực tế.

Cần chú ý rằng, cây bao trùm tối thiểu của đồ thị không liên quan đến cây sinh bởi tất cả các dây chuyền ngắn nhất từ một đỉnh cho trước. Do đó, đồ thị trong Hình 6.9(a), với các số trên các cạnh tương ứng các trọng lượng cạnh, cây sinh ra bởi đường đi ngắn nhất từ đỉnh cho trước, chẳng hạn $v_1$, trong Hình 6.9(b); ngược lại, cây bao trùm tối thiểu cho trong Hình 6.9(c).




Hình 6.9: (a) Đồ thị $G$. (b) Cây sinh bởi đường đi ngắn nhất xuất phát từ $v_1$. (c) Cây bao trùm nhỏ nhất.

### 6.3.1 Thuật toán Kruskal

Ý tưởng của thuật toán Kruskal tìm cây bao trùm trong đồ thị liên thông có trọng số $G$ như sau: Khởi tạo với đồ thị $T$ gồm tất cả các đỉnh của $G$ và không có cạnh. Tại mỗi bước lặp chúng ta thêm một cạnh có trọng lượng nhỏ nhất lên cây $T$ mà không tạo thành chu trình trong $T$. Thuật toán dừng khi $T$ có $(n-1)$ cạnh.

Bước 1. [Khởi tạo] Giả sử $T$ là đồ thị gồm $n$ đỉnh và không có cạnh.

Bước 2. [Sắp xếp] Sắp xếp thứ tự các cạnh của đồ thị $G$ theo thứ tự trọng lượng tăng dần.

Bước 3. [Thêm cạnh] Thêm cạnh (bắt đầu từ cạnh đầu tiên) trong danh sách các cạnh được sắp xếp vào cây $T$ sao cho không tạo thành chu trình trong $T$ khi thêm. (Cạnh được thêm vào gọi là *chấp nhận được)*.

Bước 4. [Kết thúc] Nếu $T$ có $(n-1)$ cạnh thì thuật toán dừng; $T$ là cây bao trùm tối thiểu.

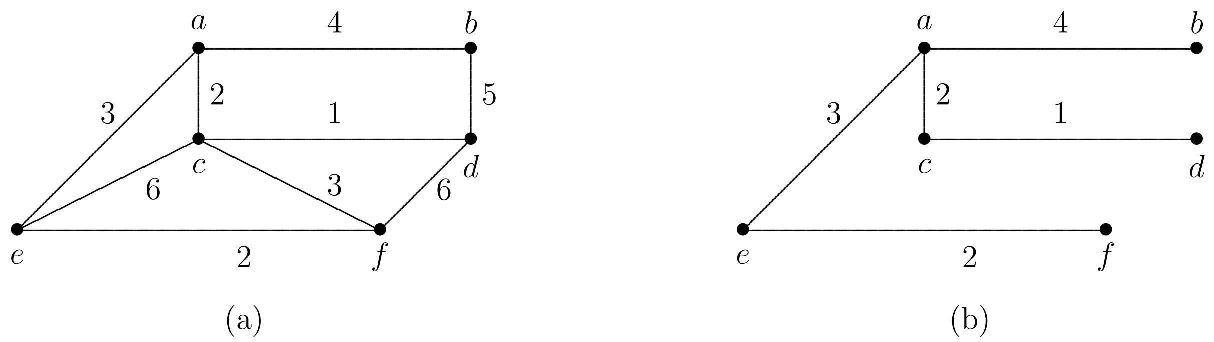
**Ví dụ 6.3.1** Xét đồ thị trong Hình 6.10(a). Sắp xếp các cạnh theo trọng lượng tăng dần (sử dụng hai mảng tuyến tính $\alpha$ và $\beta$) ta được

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| $\alpha$ | $c$ | $a$ | $e$ | $a$ | $c$ | $a$ | $b$ | $c$ | $d$ |
| $\beta$ | $d$ | $c$ | $f$ | $e$ | $f$ | $b$ | $d$ | $e$ | $f$ |
| Trọng lượng | 1 | 2 | 2 | 3 | 3 | 4 | 5 | 6 | 6 |

Các cạnh (không tạo thành chu trình) được thêm vào cây $T$ theo thứ tự là

$$(c, d), (a, c), (e, f), (a, e), (a, b).$$

$T$ là cây bao trùm nhỏ nhất có trọng lượng 12 (Hình 6.10(b)).



Hình 6.10:

**Bổ đề 6.3.2** *Nếu $K_n = (V, E)$ là đồ thị đầy đủ, và nếu tất cả các trọng lượng của các cạnh khác nhau thì tồn tại duy nhất một cây bao trùm tối thiểu $T = (V, E_T)$.*

*Chứng minh.* Ký hiệu $E_k := \{e_1, e_2, \dots, e_k\}$ là tập các cạnh được thêm vào cây $T$ trong Thuật toán 6.3.1 ở bước lặp thứ $k, 1 \leq k \leq n-1$. Hiển nhiên theo cách xây dựng, $T$ là đồ thị có $(n-1)$ cạnh và không có chu trình nên $T$ là cây bao trùm của $K_n$.

Giả sử $T' = (V, E_{T'})$ là cây bao trùm tối thiểu, ta chứng minh $E_{T'} = E_{n-1}$. Thật vậy, giả sử ngược lại tồn tại chỉ số $k$ nhỏ nhất sao cho cạnh $e_k$ không thuộc $E_{T'}$. Khi đó theo tính chất của cây, tồn tại tồn tại một và chỉ một chu trình $\mu$ trong $T' \cup \{e_k\}$. Trên chu trình này có một cạnh $e_0$ mà $e_0 \notin E_{n-1}$, vì nếu ngược lại tồn tại một chu trình, là $\mu$, trong cây $T-$mâu thuẫn. Nếu đặt $E_{T''} := (E_{T'} \cup \{e_k\}) \setminus \{e_0\})$ thì đồ thị $T'' := (V, E_{T''})$ không có chu trình và có $(n-1)$ cạnh nên nó là một cây.

Mặt khác $E_{k-1} \cup \{e_0\} \subset E_{T''}$ nên $E_{k-1} \cup \{e_0\}$ không chứa chu trình. Suy ra

$$w(e_0) > w(e_k).$$

Nhưng cây $T''$ nhận được từ cây $T'$ bằng cách thay cạnh $e_0$ thành cạnh $e_k$ nên $W(T'') < W(T')$. Mâu thuẫn vì $T'$ là cây bao trùm tối thiểu. □

**Định lý 6.3.3** *Thuật toán Kruskal là đúng; tức là, kết thúc thuật toán $T$ là cây bao trùm tối thiểu.*

*Chứng minh.* Thật vậy trước hết ta thu xếp để mọi cạnh đều có độ dài khác nhau; chẳng hạn nếu $w(e_1) = w(e_2) = \cdots = w(e_s)$ thì thực hiện phép biến đổi:

$$\begin{aligned} w(e_1) &= w(e_1) + \epsilon, \\ w(e_2) &= w(e_2) + \epsilon^2, \\ &\vdots \\ w(e_s) &= w(e_s) + \epsilon^s, \end{aligned}$$

trong đó $\epsilon$ là số dương đủ bé sao cho không làm đảo lộn thứ tự về quan hệ giữa trọng lượng của các cạnh.

Cũng thế, ta cũng có thể thêm các cạnh $f$ với trọng lượng đủ lớn $w(f) > \sum_{e \in E} w(e)$ và khác nhau sao cho đồ thị nhận được $K_n = (V, E')$ là đầy đủ.

Theo Bổ đề 6.3.2 tồn tại duy nhất một cây bao trùm tối thiểu $T$ trong đồ thị $K_n$. Mặt khác, mọi cây bao trùm của đồ thị $G$ có trọng lượng không vượt quá $\sum_{e \in E} w(e)$ và mọi cây bao trùm của $G$ cũng là cây bao trùm của $K_n$. Suy ra $T$ là cây bao trùm tối thiểu của $G$. □

Nhận xét rằng, có thể dùng phương pháp đối ngẫu: loại dần các cạnh có trọng lượng lớn nhất của đồ thị mà không làm mất tính liên thông của nó cho đến khi không thể loại cạnh được nữa.

Độ phức tạp tính toán của thuật toán Kruskal phụ thuộc vào Bước 2: đồ thị có $m$ cạnh cần $m \log_2 m$ phép toán để thực hiện sắp xếp mảng theo trọng lượng tăng dần. Tuy nhiên, nói chung ta không cần duyệt toàn bộ mảng vì cây bao trùm tối thiểu gồm $(n-1)$ cạnh chấp nhận được nên chỉ cần kiểm tra $r < m$ phần tử đầu tiên của mảng.

Thuật toán Kruskal chỉ thích hợp với những đồ thị tương đối thưa. Với những đồ thị khác, chẳng hạn đồ thị đầy đủ có số cạnh $m = n(n-1)/2$, Prim [20] và Dijkstra [4] đã đưa ra những thuật toán khác hiệu quả hơn.

## Bài tập

1. Giả sử graph $G$ liên thông có trọng số; $v$ là đỉnh trong $G$ và $e$ là một cạnh liên thuộc $v$ có trọng lượng tối thiểu. Chứng minh rằng $e$ được chứa trong cây bao trùm tối thiểu nào đó.

2. Giả sử graph $G$ liên thông có trọng số; $v$ là đỉnh trong $G$. Giả sử tất cả các cạnh liên thuộc $v$ có trọng lượng phân biệt. Giả sử $e$ là một cạnh liên thuộc $v$ có trọng lượng tối thiểu. Cạnh $e$ được chứa trong mọi cây bao trùm tối thiểu?

3. Giả sử graph có trọng số $K_n$ trong đó tất cả các cạnh có cùng trọng lượng. Chứng minh rằng thuật toán tìm cây bao trùm tối thiểu của $K_n$ phải kiểm tra tất cả các cạnh của $K_n$.

4. Giả sử graph $G$ liên thông có trọng số trong đó tất cả các cạnh có trọng lượng khác nhau. Chứng minh $G$ có duy nhất cây bao trùm tối thiểu.

5. Giả sử $G$ là graph liên thông có trọng số. Các khẳng định sau đúng hay sai? Nếu đúng, chúng minh; ngược lại, cho phản ví dụ:

   (a) Nếu tất cả các trọng lượng của các cạnh khác nhau thì các cây bao trùm khác nhau có tổng trọng lượng khác nhau.

   (b) Nếu $e$ là cạnh có trọng lượng nhỏ hơn tất cả các trọng lượng của các cạnh khác thì $e$ thuộc mọi cây bao trùm tối thiểu.

   (c) Nếu $T$ là cây bao trùm nhỏ nhất của $G$ thì tồn tại cách đánh số thứ tự các cạnh của $G$ sao cho thuật toán Kruskal sinh ra đúng cây bao trùm này.

6. Xây dựng thuật toán đối ngẫu thuật toán Kruskal: xoá các cạnh có trọng lượng lớn nhất mà không làm mất tính liên thông của đồ thị.

7. Xây dựng thuật toán tìm cây bao trùm lớn nhất trong graph liên thông có trọng số.

8. Giả sử $V := \{v_1, v_2, \ldots, v_n\}$ là tập $n$ đỉnh và $s$ là hàm "phân loại" trên $V \times V$ (xem Ví dụ 5.1.4). Giả sử $G$ là graph đầy đủ có trọng số trong đó tập đỉnh là $V$ và các trọng lượng là $s(v_i, v_j)$. Sửa lại thuật toán Kruskal để nhóm dữ liệu thành các lớp (thuật toán này gọi là *phương pháp lân cận gần nhất*).

9. Cho các ví dụ minh họa sự hoạt động của thuật toán Kruskal.

## 6.4 Liệt kê cây

Năm 1857, nhà toán học người Anh, A. Caylay (độc lập với G. Kirchoff) đã khám phá các cây khi cố gắng liệt kê tất cả các chất đồng phân của hydrocarbon. Các phân tử hydrocarbon được cấu tạo từ các nguyên tử hydrogen và carbon, trong đó mỗi nguyên tử carbon có thể liên kết hoá học với bốn nguyên tử khác và mỗi nguyên tử hydrogen có thể liên kết hoá học với một nguyên tử khác. Một hydrocarbon bảo hoà là hydrocarbon chứa số cực đại các nguyên tử hydrogen (với số các nguyên tử carbon cho trước). A. Caylay đã chứng minh rằng, nếu hydrocarbon bảo hoà có $k$ nguyên tử carbon thì nó cần có $2k + 2$ nguyên tử hydrogen và do đó có công thức hoá học $C_kH_{2k+2}$. Ông đã dùng graph liên thông để biểu diễn cấu trúc của một phân tử hydrocarbon $C_kH_{2k+2}$ : các đỉnh là các nguyên tử carbon và hydrogen; các cạnh tương ứng các liên kết hoá học giữa các nguyên tử. Trong trường hợp này, một nguyên tử carbon tương ứng với một đỉnh bậc bốn và một nguyên tử hydrogen tương ứng với một đỉnh bậc một (đỉnh treo). Tổng số các đỉnh trong graph tương ứng như vậy là: $n = k + (2k + 2) = 3k + 2$; và tổng số các cạnh là:

$$\frac{1}{2}\text{ (tổng các bậc) } = (4k + 2k + 2)/2 = 3k + 1.$$

Graph này liên thông và có số cạnh ít hơn số đỉnh là 1 nên nó là một cây. Như vậy vấn đề đếm các cấu trúc đồng phân của một hydrocarbon đưa về bài toán đếm các cây (dĩ nhiên có cùng các tính chất xác định).

Câu hỏi đầu tiên của Cayley đặt ra như sau: *Số các cây khác nhau có thể xây dựng từ $n$ đỉnh (hay nhãn) khác nhau là bao nhiêu?*

Nếu $n = 4$, thì chúng ta có 16 cây (tại sao?).

Để trả lời câu hỏi trên, ta xét graph mà mỗi đỉnh có một tên hay nhãn duy nhất (tức là không có hai đỉnh mang cùng một nhãn) được gọi là *graph được gán nhãn* (labeled graph).

Kết quả sau lần đầu tiên được đưa ra và chứng minh bởi Cayley. Sau đó nhiều chứng minh khác cũng được công bố. Chứng minh sau đây của H. Prüfer năm 1918.

**Định lý 6.4.1** (A. Cayley) *Số các cây được gán nhãn $n$ đỉnh ($n \geq 2$) là $n^{n-2}$; tức là số các cây bao trùm của graph đầy đủ $K_n$ là $n^{n-2}$.*

*Chứng minh.* Giả sử $V = \{1, 2, \ldots, n\}$. Với mỗi cây bao trùm $T$ của đồ thị $K_n$ ta thiết lập tương ứng một-một với vector $a = (a_1, a_2, \ldots, a_{n-2})$, trong đó các số nguyên $a_i$ thoả mãn $1 \leq a_i \leq n$, như sau:

+ Ký hiệu $b_1$ là đỉnh treo đầu tiên (có chỉ số nhỏ nhất) trong tập được sắp thứ tự $V$ sao cho $e_1 = (a_1, b_1)$ là cạnh treo của $T$ tương ứng (tồn tại do mọi cây có ít nhất một đỉnh treo). Loại cạnh $e_1$ và đỉnh $b_1$ ra khỏi cây $T$ ta được cây $T_1$ mới.

+ Ký hiệu $b_2$ là đỉnh treo đầu tiên (có chỉ số nhỏ nhất) trong tập được sắp thứ tự $V$ sao cho $e_2 = (a_2, b_2)$ là cạnh treo tương ứng trong cây $T_1$ (tồn tại do mọi cây có ít nhất một đỉnh treo). Loại cạnh $e_2$ và đỉnh $b_2$ ra khỏi cây $T_1$ ta được cây $T_2$ mới.

+ Lặp lại theo quy nạp cho đến khi loại cạnh $e_{n-2} = (a_{n-2}, b_{n-2})$ ta được cây gồm đúng một cạnh $e_{n-1} = (a_{n-1}, b_{n-1})$ nối hai đỉnh còn lại.

Khi đó vector $a = (a_1, a_1, \ldots, a_{n-2}) \in V^{n-2}$ được xác định duy nhất bởi cây $T$ và với hai cây khác nhau $T$ và $T'$, ta có tương ứng hai vector khác nhau. Mỗi đỉnh $a_i$ xuất hiện $d(a_i) + 1$ lần trong vector $a$.

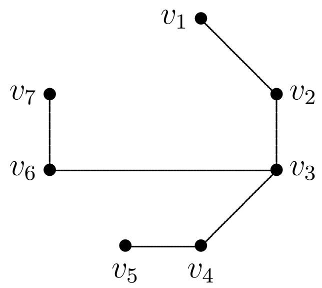
Ngược lại, với mỗi vector $a \in V^{n-2}$, ta có thể xây dựng một cây $T$ như sau:

+ Lấy đỉnh đầu tiên (có chỉ số nhỏ nhất) $b_1 \in V$ mà không xuất hiện trong thành phần của vector $a$. Lấy phần tử đầu tiên $a_1$ trong vector $a$; đặt cạnh $e_1 = (a_1, b_1)$. Loại $a_1$ khỏi vector $a$ và đỉnh $b_1$ ra khỏi tập $V$.

+ Tiếp tục lặp lại theo thủ tục trên với các số còn lại, cuối cùng ta sẽ thu được cây $T$.

Nhận xét rằng $\#V = n^{n-2}$. Định lý được chứng minh. $\square$

**Ví dụ 6.4.1** Xác định vector độ dài năm tương ứng cây bao trùm trong Hình 6.11.




Hình 6.11:

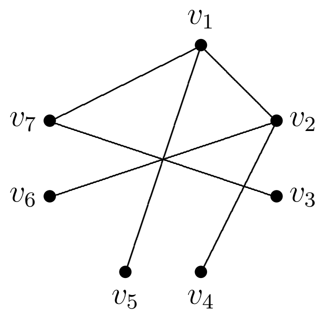
Chú ý rằng $v_1$ là đỉnh treo với chỉ số nhỏ nhất và $v_2$ liên thuộc với $v_1$, do đó $a_1 = 2$. Xoá cạnh $(v_1, v_2)$. Graph còn lại có $v_2$ là đỉnh treo với chỉ số nhỏ nhất; do đó $a_2 = 3$. Xoá cạnh $(v_2, v_3)$ và lặp lại tiến trình trên ta có vector tương ứng cây là $(2, 3, 4, 3, 6)$.

**Ví dụ 6.4.2** Tìm cây bao trùm của $K_7$ tương ứng vector $(7, 2, 1, 2, 1)$.

Lời giải cho trong Hình 6.12. Thật vậy, bắt đầu với danh sách $\{1, 2, 3, 4, 5, 6, 7\}$. Số 3 là số nhỏ nhất trong danh sách nhưng không thuộc vector $a := (7, 2, 1, 2, 1)$ và 7 là số đầu tiên trong vector $a$. Bằng cách nối, ta có cạnh $(v_3, v_7)$. Loại bỏ 3 ra khỏi danh sách và 7 ra khỏi vector $a$ ta có danh sách và vector $a$ mới tương ứng là $\{1, 2, 4, 5, 6, 7\}$ và $a = (2, 1, 2, 1)$. Số 4 là số nhỏ nhất trong danh sách nhưng không thuộc vector $a$ và 2 là số đầu tiên trong vector $a$. Bằng cách nối, ta có cạnh $(v_4, v_2)$. Lặp lại thủ tục trên cho đến khi ta có cạnh cuối cùng $(v_1, v_7)$.

**Ví dụ 6.4.3** Có bao nhiêu cách để xây dựng mạng điện với 12 nút nối tất cả các nút sử dụng số dây dẫn ít nhất có thể.

Chúng ta xây dựng graph con của $K_{12}$ như sau: mỗi nút tương ứng với một đỉnh và mỗi dây dẫn tương ứng các cạnh. Graph $T$ biểu diễn mạng điện với 12 nút nối tất cả các nút sử dụng số dây dẫn ít nhất phải là graph liên thông không chu trình. Vì vậy $T$ là cây bao trùm của $K_{12}$. Theo Định lý 6.4.1, có $12^{10}$ cây bao trùm của $K_{12}$. Do đó có $12^{10}$ cách để xây dựng mạng điện.




Hình 6.12:

**Nhận xét 20** Định lý 6.4.1 không cho ta chính xác số các chất đồng phân của $C_kH_{2k+1}$. Để hạn chế về bậc của các đỉnh, ta nhận xét rằng:

(a) Vì các đỉnh biểu diễn hydrogen là các đỉnh treo, chúng sẽ kết hợp với các nguyên tử carbon theo cùng một cách và do đó không đóng góp vào hiện tượng đồng phân. Vì vậy ta không cần quan tâm đến các đỉnh hydrogen.

(b) Suy ra cây biểu diễn $C_kH_{2k+1}$ đưa về cây có $k$ đỉnh, mỗi đỉnh biểu diễn một nguyên tử carbon. Với cây này ta không phân biệt các đỉnh, và do đó nó là *cây không được gán nhãn*.

Vậy với butane $C_4H_{10}$ chỉ có hai cây khác nhau (hãy vẽ chúng). (Trong hoá học, ta biết rằng có chính xác hai loại buttane khác nhau là: $n$-buttan và isobuttane).

Việc phân biệt giữa graph được gán nhãn và graph không được gán nhãn là rất quan trọng trong bài toán đếm số các graph khác nhau. Bài toán liệt kê các cây không được gán nhãn liên quan đến một số khái niệm khác và vượt ra phạm vi của giáo trình, bạn đọc quan tâm có thể xem tài liệu dẫn [6].

## Bài tập

1. Vẽ tất cả các cây được gán nhãn $n$ đỉnh với $n = 1, 2, 3, 4$ và 5.

2. Vẽ tất cả các cây không được gán nhãn $n$ đỉnh với $n = 1, 2, 3, 4$ và 5.

3. Vẽ tất cả các cây có gốc không được gán nhãn $n$ đỉnh với $n = 1, 2, 3, 4$ và 5.

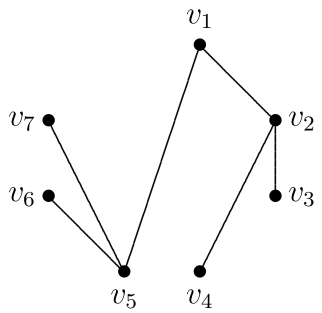
4. Chứng minh chỉ có sáu cây khác nhau (không đẳng cấu), mỗi cây có sáu đỉnh. Vẽ các cây này.

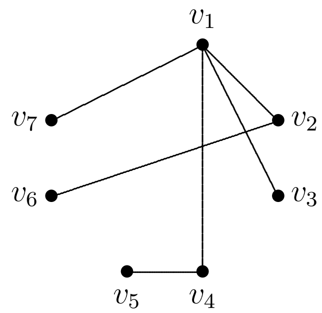
5. (a) Vẽ hai cây butane $C_4H_{10}$ khác nhau.

   (b) Có bao nhiêu chất đồng phân của hydrocarbon bảo hoà $C_6H_{14}$?

6. Chứng minh rằng số các cây có gốc được gán nhãn $n$ đỉnh khác nhau là $n^{n-1}$. Vẽ tất cả các cây có gốc được gán nhãn trong trường hợp $n = 1, 2$ và 3.

7. Với mỗi cây sau, xác định các vector trong chứng minh của Định lý Caylay.



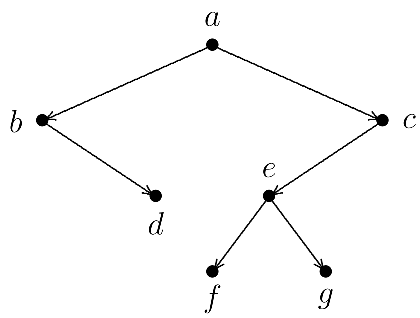

8. Với mỗi vector sau, xác định các cây bao trùm của $K_7$ trong chứng minh của Định lý Caylay:

   (a) $(7, 2, 4, 4, 1)$.

   (b) $(2, 2, 2, 4, 6)$.

## 6.5 Cây nhị phân

"Cây nhị phân" (binary tree) là một trong những lớp quan trọng nhất của cây có gốc. Mỗi đỉnh trong cây nhị phân có nhiều nhất hai con (xem Hình 6.13). Hơn nữa, mỗi đỉnh con được ký hiệu hoặc là "con trái" hoặc là "con phải". Khi vẽ cây nhị phân, đỉnh con trái được vẽ bên trái và đỉnh con phải được vẽ bên phải.




Hình 6.13:

**Định nghĩa 6.5.1** *Cây nhị phân* là một cây có gốc trong đó mỗi đỉnh hoặc không có con, hoặc có một con, hoặc có hai con. Nếu đỉnh có một con, thì con này được xem là con trái hoặc con phải; nếu một đỉnh có hai con, thì một con bên trái và một con bên phải.

**Ví dụ 6.5.1** Trong cây nhị phân Hình 6.13, đỉnh $b$ là con trái của $a$ và đỉnh $c$ là con phải của $a$. Đỉnh $d$ là con phải của $b$; đỉnh $b$ không có con trái. Đỉnh $e$ là con trái của $c$; đỉnh $c$ không có con phải.

**Ví dụ 6.5.2** Một cây xác định bởi mã Huffman là cây nhị phân. Chẳng hạn, với cây Huffman trong Hình 6.3, di chuyển từ một đỉnh đến đỉnh con bên trái tương ứng sử dụng bit 1 và di chuyển từ một đỉnh đến đỉnh con bên phải tương ứng sử dụng bit 0.

*Cây nhị phân đầy đủ* là cây nhị phân mà mỗi đỉnh hoặc có hai con hoặc không có con.

**Định lý 6.5.2** *Nếu $T$ là cây nhị phân đầy đủ với $i$ đỉnh trong thì $T$ có $i+1$ đỉnh treo và có tất cả $2i+1$ đỉnh.*

*Chứng minh* Tập các đỉnh của $T$ gồm những đỉnh là các đỉnh con (một vài đỉnh là cha) và những đỉnh không phải là đỉnh con. Tồn tại duy nhất một đỉnh không phải là con-đỉnh gốc. Do có $i$ đỉnh trong và mỗi đỉnh có hai con nên tồn tại $2i$ đỉnh con. Vậy số các đỉnh của $T$ là $2i+1$ và số các đỉnh treo bằng

$$(2i+1) - i = i+1.$$

□

**Định lý 6.5.3** *Nếu $T$ là cây nhị phân có độ cao $h$ và $t$ đỉnh treo thì*

$$\log t \leq h. \tag{6.1}$$

*Chứng minh* Ta sẽ chứng minh quy nạp theo $h$ bất đẳng thức tương đương:

$$t \leq 2^h. \tag{6.2}$$

Nếu $h=0$ thì cây $T$ gồm một đỉnh; suy ra $t=1$. Do đó (6.2) đúng.

Giả sử khẳng định đúng với mọi cây nhị phân có độ cao nhỏ hơn $h$. Giả sử $T$ là cây nhị phân có độ cao $h>0$ với $t$ đỉnh treo. Xét trường hợp đỉnh gốc của $T$ chỉ có một con. Nếu ta khử gốc và cạnh liên thuộc với gốc thì ta được cây nhị phân có độ cao $h-1$ và cùng số đỉnh treo như $T$. Theo quy nạp, $t \leq 2^{h-1} < 2^h$ và do vậy (6.2) đúng.

Bây giờ giả sử gốc của $T$ có hai con là $v_1$ và $v_2$. Ký hiệu $T_i, i=1,2$, là cây con với gốc tại $v_i$ và giả sử $T_i$ có độ cao $h_i$ và $t_i$ đỉnh treo. Theo giả thiết quy nạp

$$t_i \leq 2^{h_i}, \qquad i=1,2. \tag{6.3}$$

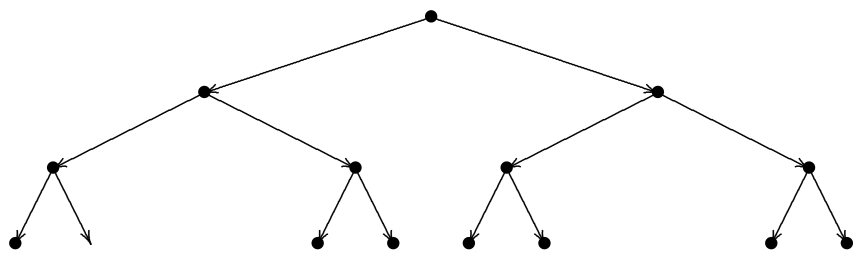
Nhận xét rằng các đỉnh treo của $T$ gồm các nút lá của $T_1$ và $T_2$. Do đó

$$t = t_1 + t_2. \tag{6.4}$$

Từ (6.3) và (6.4) ta có

$$t = t_1 + t_2 \leq 2^{h_1} + 2^{h_2} \leq 2^{h-1} + 2^{h-1} = 2^h.$$

□



Hình 6.14:

**Ví dụ 6.5.3** Cây nhị phân trong Hình 6.14 có độ cao $h = 3$ và số các nút lá là $t = 8$. Trong trường hợp này, (6.1) trở thành đẳng thức.

Giả sử ta có một tập $S$ mà các phần tử của nó được sắp thứ tự. Chẳng hạn, nếu $S \subset \mathbb{R}$ với thứ tự thông thường; nếu $S$ là các chuỗi ký tự, ta có thể sử dụng thứ tự từ điển. Cây nhị phân được sử dụng rất nhiều trong tin học nhằm lưu trữ các phần tử của một tập được sắp thứ tự. Giả sử tại mỗi đỉnh $v$ ta lưu trữ dữ liệu $d(v)$. Khi đó nếu $v$ là con trái (hoặc con phải) của $w$ thì sẽ có một mối quan hệ thứ tự giữa $d(v)$ và $d(w)$.

**Định nghĩa 6.5.4** *Cây tìm kiếm nhị phân* (binary seach tree) là một cây nhị phân trong đó dữ liệu liên kết với mỗi đỉnh. Dữ liệu được sắp xếp sao cho với mỗi đỉnh $v$ dữ liệu trong cây con bên trái của $v$ nhỏ hơn dữ liệu trong $v$; và mỗi dữ liệu trong cây con bên phải của $v$ lớn hơn dữ liệu trong $v$.

**Ví dụ 6.5.4** Chuỗi $S$

OLD PROGRAMMERS NEVER DIE
THEY JUST LOSE THEIR MEMORIES

có thể đặt trong một cây tìm kiếm nhị phân như Hình 6.15.

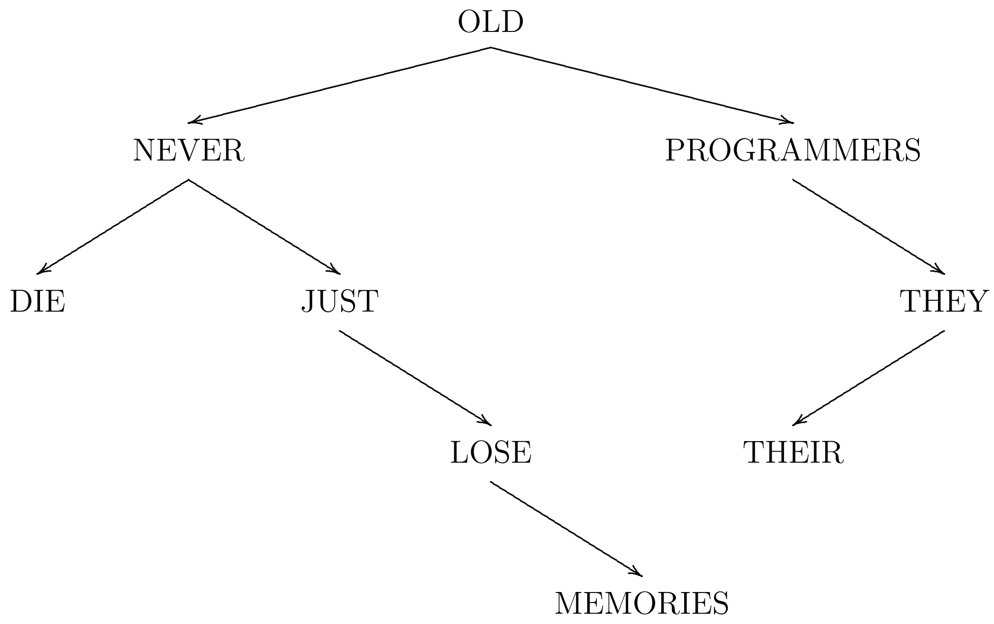
Nói chung, có nhiều cách đặt dữ liệu vào cây tìm kiếm nhị phân. Hình 6.16 minh họa cây nhị phân khác lưu trữ các từ trong chuỗi $S$.

Dưới đây là thuật toán xây dựng cây tìm kiếm nhị phân.

### 6.5.1 Thuật toán xây dựng cây tìm kiếm nhị phân

Nhập: Dãy các từ phân biệt: $S$.

Xuất: Cây tìm kiếm nhị phân $T$.




Hình 6.15:

Bước 1. [Xây dựng nút gốc] Giả sử $w$ là từ đầu tiên trong dãy $S$. Nếu $S = \emptyset$, đặt $T$ là cây không đỉnh và cạnh và dừng; ngược lại, thiết lập $T$ là cây có đúng một đỉnh (là gốc) và lưu trữ $w$ trong gốc.

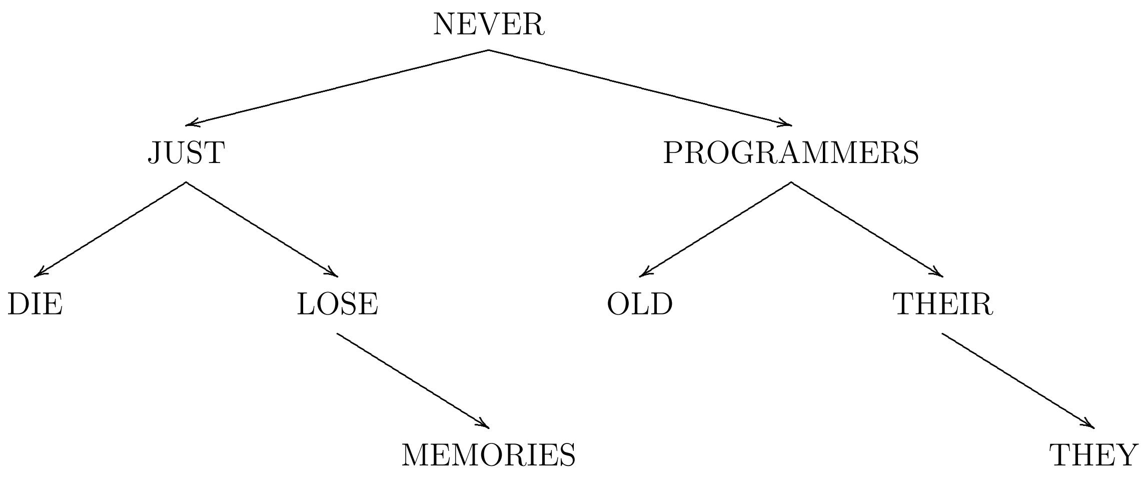
Bước 2. [Lấy ký tự tiếp] Giả sử $w$ là ký tự kế tiếp trong $S$. Nếu không tồn tại, dừng.

Bước 3. [Bắt đầu tìm kiếm để lưu trữ vị trí] Giả sử $v$ là gốc của $T$.

Bước 4. [Kết thúc?] Nếu $w$ nhỏ hơn từ trong $v$ và $v$ không có cây con bên trái thì thêm đỉnh con bên trái vào $v$ và lưu $w$ vào cây con trái sau đó chuyển sang Bước 2. Nếu $w$ lớn hơn từ trong $v$ và $v$ không có cây con bên phải, thêm đỉnh con bên phải vào $v$ và lưu $w$ vào sau đó chuyển sang Bước 2.

Bước 5. [Tiếp tục tìm] Nếu $w$ nhỏ hơn từ trong $v$ đặt $v$ là con bên trái của $v$ và chuyển sang Bước 4. Nếu $w$ lớn hơn từ trong $v$ đặt $v$ là con bên phải của $v$ và chuyển sang Bước 4.

Cây tìm kiếm nhị phân rất tiện lợi trong việc tìm kiếm dữ liệu. Tức là nếu cho dữ liệu $D$ ta có thể xác định vị trí của nó $D$ trong cây tìm kiếm nhị phân (nếu có). Để xác định dữ liệu $D$ trong cây tìm kiếm nhị phân, chúng ta bắt đầu từ gốc. Sau đó ta lặp lại tiến trình so sánh $D$ với dữ liệu tại nút hiện hành. Nếu $D$ bằng dữ liệu tại nút hiện hành, tức đã tìm thấy $D$ và thuật toán dừng. Nếu $D$ nhỏ hơn (tương ứng, lớn hơn) dữ liệu tại nút hiện hành $v$ ta di chuyển xuống nút con bên trái (tương ứng, bên phải) của $v$ và lặp lại quá trình này. Tại thời điểm nào đó, ta không thể di chuyển được nữa thì kết luận $D$ không có trong cây.




Hình 6.16:

Thời gian tìm kiếm dữ liệu trong cây tìm kiếm nhị phân là tối đa khi dữ liệu không nằm trong cây và theo đó ta có dây chuyền dài nhất từ nút gốc. Do đó thời gian tối đa để tìm kiếm tỉ lệ với chiều cao của cây. Hệ quả là độ cao của cây tìm kiếm nhị phân càng nhỏ thì thời gian tìm kiếm càng ít. Có nhiều cách để cực tiểu hoá độ cao của cây (xem [9]).

Để phân tích trường hợp xấu nhất trong cây tìm kiếm nhị phân $T$ (có $n$ đỉnh, $t$ đỉnh treo và độ cao $h$) ta gọi $T^*$ là cây nhị phân đầy đủ nhận được từ $T$ bằng cách thêm các nút con bên trái và bên phải (nếu cần). Chẳng hạn, Hình 6.17 là cây nhị phân đầy đủ từ cây $T$ trong Hình 6.15. Các đỉnh thêm vào được đánh dấu $*$. Việc tìm kiếm không thành công trong $T$ tương ứng đến các đỉnh đánh dấu $*$ trong $T^*$. Theo Định lý 6.5.3, $\log t \leq h$. Nhưng theo cách xây dựng, cây nhị phân đầy đủ $T^*$ có $n$ đỉnh trong và $t$ đỉnh treo, nên theo Định lý 6.5.2, $t = n + 1$. Do đó trong trường hợp xấu nhất thời gian tìm kiếm ít nhất là $\log t = \log(n+1)$. Bài tập 3 chỉ ra rằng nếu độ cao của $T$ tối thiểu thì trường hợp xấu nhất thời gian tìm kiếm bằng $[\log(n+1)]$.

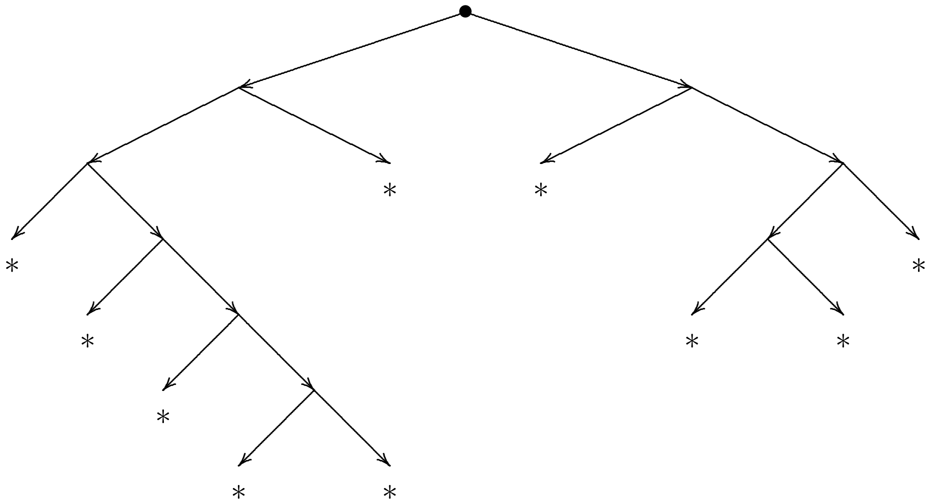
## Bài tập

1. Đặt các từ FOUR SCORE AND SEVEN YEARS AGO OUR FOREFATHERS BROUGHT FORTH theo thứ tự xuất hiện của chúng vào cây tìm kiếm nhị phân.

2. Viết thuật toán tìm kiếm trên cây tìm kiếm nhị phân.

3. Viết thuật toán lưu trữ $n$ từ khác nhau vào cây tìm kiếm nhị phân $T$ với trọng lượng tối thiểu. Chứng minh rằng cây đầy đủ $T^*$ nhận được từ cây $T$ bằng cách thêm các nút con bên trái và bên phải (nếu cần thiết) có trọng lượng $[\log(n+1)]$.

4. Khẳng định sau đúng hay sai: Giả sử $T$ là cây nhị phân. Với mỗi đỉnh $v$ trong $T$,




Hình 6.17:

dữ liệu trong $v$ lớn hơn (tương ứng, nhỏ hơn) dữ liệu trong con trái (tương ứng, con phải) của $v$ thì $T$ là cây tìm kiếm nhị phân. Giải thích.

5. Vẽ các graph (nếu tồn tại) tương ứng với những tính chất đã nêu:

   (a) Cây nhị phân đầy đủ có bốn đỉnh trong và năm đỉnh treo.

   (b) Cây nhị phân đầy đủ có độ cao 3 và chín đỉnh treo.

   (c) Cây nhị phân đầy đủ có độ cao 4 và chín đỉnh treo.

6. *Cây $m$-phân đầy đủ* là cây có gốc sao cho mỗi đỉnh trong có $m$ đỉnh con có thứ tự. Cây $m$-phân đầy đủ $T$ với $i$ đỉnh trong thì có bao nhiêu đỉnh? Có bao nhiêu đỉnh treo? Giải thích.

7. Tìm thuật toán xây dựng cây nhị phân đầy đủ với $n > 1$ đỉnh treo.

8. Viết thuật toán đệ quy xây dựng cây tìm kiếm nhị phân.

9. Tìm độ cao cực đại của cây nhị phân đầy đủ có $t$ đỉnh treo.

10. Viết thuật toán kiểm tra một cây nhị phân với các dữ liệu được lưu trữ tại mỗi đỉnh là cây tìm kiếm nhị phân.

11. Giả sử $T$ là cây nhị phân đầy đủ; $I$ là tổng các độ dài của các dây chuyền đơn giản từ gốc đến các đỉnh trong và $E$ là tổng các độ dài của các dây chuyền đơn giản từ gốc đến các đỉnh treo. Chứng minh rằng nếu $T$ có $n$ đỉnh trong thì $E = I + 2n$.

12. Cây nhị phân $T$ gọi là *cân bằng* nếu với mỗi đỉnh $v$, độ cao của các cây con bên trái và bên phải sai khác nhau nhiều nhất là 1. (Độ cao cây rỗng định nghĩa là $-1$). Ký hiệu $N_h$ là số tối thiểu các đỉnh trong cây nhị phân cân bằng với độ cao $h$ và $f_1, f_2, \ldots$ là dãy Fibonacci.

    (a) Chứng minh rằng $N_0 = 1, N_1 = 2$, và $N_2 = 4$.

(b) Chứng minh rằng $N_h = 1 + N_{h-1} + N_{h-2}$ với mọi $h \geq 0$.

(c) Chứng minh rằng $N_h = f_{h+2} - 1$ với mọi $h \geq 0$.

13. Chứng minh rằng độ cao $h$ của cây nhị phân cân bằng thoả mãn $h = O(\log 2)$. Điều này chỉ ra rằng trong trường hợp xấu nhất, thời gian tìm kiếm trong cây nhị phân cân bằng $n$ đỉnh là $O(\log 2)$.

14. Chứng minh rằng nếu cây nhị phân cân bằng độ cao $h$ có $n \geq 1$ đỉnh thì $\log n < h+1$.

# Tài liệu tham khảo


[1] C. Berge, *Lý thuyết đồ thị và ứng dụng,* NXB Khoa học và kỹ thuật Hà Nội, 1971.

[2] A. Cayley, *Collected papers,* Quart. Jl. of Mathematics, **13** Cambridge, 26 (1897).

[3] N. Biggs, *Discrete mathematic,* Clarendon Press Oxford, 1989.

[4] Dijkstra, E. W., *A note on two problems in connection with graphs,* Numerische Mathematik, **1**, 269 (1959).

[5] P. J. Cameron, *Combinatorics: topics, techniques, algorithms,* Cambridge University Press, 1994.

[6] N. Deo, *Graph theory with applications to engineering and computer science,* Prentice-Hall Inc., 1974.

[7] R. J. MC Eliece, M. Kac, *The theory of information and coding,* Addison-Wesley, 1977.

[8] C. M. Goldie, R. G. E. Pinch, *Communication theory,* Cambridge University Press, 1991.

[9] R. W. Hamming, *Coding and information theory,* Prentice Hall, 1980.

[10] R. Hill, *A first course in coding theory,* Clarendon Press Oxford, 1985.

[11] R. Johnsonbaugh, *An introduction to discrete mathematic,* Macmillan Publishing Company, 1992.

[12] A. R. Kenneth, C. R.B. Wright, *Discrete mathematics,* Prentice-Hall International Editions, 1978.

[13] Kirchhoff G., in "Annalen der Physik and Chemie" **72**, 497 (1847).

[14] S. Lipschutz, *Essential computer mathematic,* McGraw-Hill, 1992.

[15] S. Lipschutz, M. L. Lipson,*2000 sloved problems in discrete mathematics,* McGraw-Hill, 1992.

[16] C. L. Liu, *Introduction to combinationnal mathematic,* McGraw-Hill, 1985.

[17] F. J. MacWilliams, N. J. A. Soane, *The theory of error-correcting codes,* North-Holland, 1981.

[18] A. A. Michael, A. J. Kfoury, R. N. Moll, D. Gries, *A basis for theoretical computer science,* Springer-Verlag NewYork Inc., 1981.

[19] J. G. Michaels, K. H. Rosen, *Applications of discrete mathematics,* McGraw-Hill, 1991.

[20] Prim R. C., *Shortest connection networks and some generalizations,* Bell Syst. Tech. Jl., **36**, 1389 (1957).

[21] S. Roman, *An introduction to discrete mathematic,* Saunders College, 1982.

[22] K. H. Rosen, *Discrete mathematics and its applications,* McGraw-Hill, 1995.

[23] B. M. Stephen, A. Ralston, *Discrete algorithmic mathematics,* Addision-Wesley Publishing Company, 1991.

[24] D. Welsh, *Codes and cryptography,* Clarendon Press Oxford, 1987.