

# Mục lục

<b>I</b>	<b>Cơ sở của Toán rời rạc</b>	<b>1</b>
<b>1</b>	<b>Nguyên lý đếm cơ bản</b>	<b>2</b>
1.1	Quy tắc cộng, nhân	2
1.2	Biểu đồ cây	9
1.3	Hoán vị, chỉnh hợp	10
1.4	Tổ hợp	15
1.5	Hoán vị lặp	22
1.6	Tổ hợp lặp	27
1.7	Sinh các hoán vị và tổ hợp	31
1.8	Số Catalan	34
1.9	Tóm tắt	34
<b>2</b>	<b>Nguyên lý cơ bản của logic</b>	<b>47</b>
2.1	Phép toán cơ bản và bảng chân lý	47
2.2	Tương đương logic: luật logic	52
2.3	Kéo theo logic: quy tắc suy luận	58
2.4	Lượng từ: tình huống sử dụng	64
2.5	Các lượng từ, định nghĩa, và chứng minh định lý	71
2.6	Tóm tắt	74
<b>3</b>	<b>Lý thuyết tập hợp</b>	<b>76</b>
3.1	Tập và tập con	76
3.2	Phép toán tập hợp và quy luật	85
3.3	Phép đếm và biểu đồ Venn	94
3.4	Tóm tắt	97
<b>4</b>	<b>Tính chất của số nguyên: quy nạp toán học</b>	<b>100</b>
4.1	Nguyên lý sắp tốt: quy nạp toán học	100
4.2	Định nghĩa đệ quy	112
4.3	Thuật toán chia: số nguyên tố	119

4.4	Ước chung lớn nhất: thuật toán Euclid	123
4.5	Định lý cơ bản của số học	129
4.6	Biểu diễn số nguyên và thuật toán	133
4.7	Tóm tắt	139
<b>5</b>	<b>Quan hệ: hàm</b>	<b>142</b>
5.1	Tích Descartes và quan hệ	142
5.2	Biểu diễn quan hệ	148
5.3	Hàm: đơn ánh	149
5.4	Toàn ánh: số Stirling loại II	159
5.5	Hàm đặc biệt	164
5.6	Nguyên lý chuồng bồ câu	168
5.7	Hàm hợp và hàm ngược	171
5.8	Độ phức tạp tính toán	179
5.9	Phân tích thuật toán	183
<b>6</b>	<b>Quan hệ: hướng tiếp cận thứ hai</b>	<b>186</b>
6.1	Quan hệ: thuộc tính và phép toán	186
6.2	Kiểm tra thuộc tính của quan hệ	194
6.3	Thứ tự bộ phận: biểu đồ Hasse	198
6.4	Quan hệ tương đương và phân hoạch	204
6.5	Bao đóng của quan hệ	206
<b>II</b>	<b>Các phép đếm nâng cao</b>	<b>202</b>
<b>7</b>	<b>Nguyên lý bù trừ</b>	<b>203</b>
7.1	Nguyên lý bù trừ	203
7.2	Nguyên lý bù trừ tổng quát	211
7.3	Sắp xếp: không vật nào đúng vị trí	212
7.4	Đa thức rook	212
7.5	Sắp xếp có vị trí bị cấm	212
7.6	Tóm tắt	212
7.7	Bài tập bổ sung	212
<b>8</b>	<b>Hàm sinh</b>	<b>213</b>
8.1	Ví dụ mở đầu	214
8.2	Định nghĩa và ví dụ: kỹ thuật tính	218
8.3	Phân hoạch số nguyên	231
8.4	Hàm sinh mũ	236

8.5	Toán tử tổng	241
<b>9</b>	<b>Hệ thức đệ quy</b>	<b>246</b>
9.1	Hệ thức đệ quy tuyến tính cấp một	247
9.2	Hệ thức đệ quy tuyến tính thuần nhất cấp cao hệ số hằng	256
9.3	Hệ thức đệ quy không thuần nhất	265
9.4	Phương pháp hàm sinh	266
9.5	Hệ thức đệ quy phi tuyến đặc biệt	270
9.6	Thuật toán chia để trị	271
<b>III</b>	<b>Lý thuyết đồ thị và ứng dụng</b>	<b>278</b>
<b>10</b>	<b>Mở đầu về lý thuyết đồ thị</b>	<b>279</b>
10.1	Định nghĩa và ví dụ	279
10.2	Đồ thị con, phần bù và đẳng cấu đồ thị	280
10.3	Bậc của đỉnh: đường và chu trình Euler	281
10.4	Đồ thị phẳng	284
10.5	Đường và chu trình Hamilton	285
10.6	Tô màu đồ thị và đa thức sắc độ	286
<b>11</b>	<b>Cây</b>	<b>287</b>
11.1	Định nghĩa, tính chất, và ví dụ	287
11.2	Cây có gốc	288
11.3	Cây và sắp xếp	293
11.4	Cây có trọng số và mã tiền tố	293
11.5	Các thành phần liên thông và điểm nối	298
<b>12</b>	<b>Tối ưu và tìm kiếm</b>	<b>299</b>
12.1	Thuật toán đường đi ngắn nhất Dijkstra	299
12.2	Cây bao trùm nhỏ nhất: thuật toán Kruskal, Prim	299
12.3	Mạng vận tải: định lý Max-Flow Min-Cut	299
12.4	Lý thuyết tìm kiếm	299
<b>IV</b>	<b>Đại số hiện đại ứng dụng</b>	<b>300</b>
<b>13</b>	<b>Vành và số học đồng dư</b>	<b>301</b>
13.1	Cấu trúc vành: định nghĩa và ví dụ	301
13.2	Tính chất vành và vành con	307
13.3	Vành các số nguyên modulo $n$	309
13.4	Đồng cấu và đẳng cấu nhóm, vành	315

13.5 Định lý phần dư Trung Quốc . . . . .	316
13.6 Mã hóa khóa công khai: Giới thiệu . . . . .	319
13.7 Mã hóa khóa công khai: Phương pháp Rabin . . . . .	321
13.8 Mã hóa khóa công khai: RSA . . . . .	326
<b>13 Nhóm, lý thuyết mã, và phương pháp liệt kê Polya</b>	<b>300</b>
13.1 Định nghĩa, ví dụ, và tính chất cơ bản . . . . .	300
13.2 Đồng cấu, đẳng cấu, và nhóm cyclic . . . . .	301
13.3 Lớp kề và định lý Lagrange . . . . .	302
13.4 Sơ lược về lý thuyết mã . . . . .	302
13.5 Khoảng cách Hamming . . . . .	302
13.6 Ma trận sinh và kiểm tra chẵn lẻ . . . . .	302
13.7 Nhóm các mã: giải mã với coset leaders . . . . .	303
13.8 Ma trận Hamming . . . . .	303
13.9 Phép đếm và sự tương đương: định lý Burnside . . . . .	303
13.10 Chỉ số chu trình . . . . .	306
13.11 Định lý liệt kê Polya . . . . .	306
<b>14 Trường hữu hạn và thiết kế tổ hợp</b>	<b>308</b>

# Chương 5

## Quan hệ: hàm

---

5.1	Tích Descartes và quan hệ . . . . .	142
5.2	Biểu diễn quan hệ . . . . .	148
5.3	Hàm: đơn ánh . . . . .	149
5.4	Toàn ánh: số Stirling loại II . . . . .	159
5.5	Hàm đặc biệt . . . . .	164
5.6	Nguyên lý chuồng bồ câu . . . . .	168
5.7	Hàm hợp và hàm ngược . . . . .	171
5.8	Độ phức tạp tính toán . . . . .	179
5.9	Phân tích thuật toán . . . . .	183

---

### 5.1 Tích Descartes và quan hệ

---

**Định nghĩa 5.1.** Cho hai tập  $A, B$ . Tích Descartes, hay tích chéo của  $A$  và  $B$  là tập

$$A \times B = \{(a, b) \mid a \in A, b \in B\}. \tag{5.1}$$

Mỗi phần tử của  $A \times B$  gọi *cặp có thứ tự*. Với  $(a, b), (c, d) \in A \times B$

$$(a, b) = (c, d) \Leftrightarrow a = c, b = d. \tag{5.2}$$

Nếu  $A, B$  hữu hạn, theo quy tắc nhân

$$|A \times B| = |A| \cdot |B| = |B| \cdot |A| = |B \times A|, \tag{5.3}$$

tuy nhiên nói chung  $A \times B \neq B \times A$ .

Tổng quát, với  $n \in \mathbb{Z}^+$ ,  $n \geq 2$ , tích Descartes của  $n$  tập  $A_1, A_2, \dots, A_n$  là

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, 1 \leq i \leq n\}. \quad (5.4)$$

Mỗi phần tử của  $A_1 \times A_2 \times \dots \times A_n$  gọi là bộ có thứ tự  $n$  chiều. Với  $(a_1, a_2, \dots, a_n)$ ,  $(b_1, b_2, \dots, b_n) \in A_1 \times A_2 \times \dots \times A_n$

$$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n) \Leftrightarrow a_i = b_i, \forall i = \overline{1, n}. \quad (5.5)$$

Ngoài ra, nếu  $A_1, A_2, \dots, A_n$  hữu hạn thì

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|. \quad (5.6)$$

Ta cũng viết lũy thừa Descartes của một tập

$$A^2 = A \times A = \{(a, b) \mid a, b \in A\} \quad (5.7)$$

và tổng quát với  $n \in \mathbb{Z}^+$ ,  $n \geq 2$

$$A^n = \underbrace{A \times A \times \dots \times A}_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A, i = \overline{1, n}\}. \quad (5.8)$$

#### Ví dụ 5.1. Tập

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$

biểu diễn mặt phẳng tọa độ Descartes  $Oxy$  và là một không gian vectơ thực hai chiều. Tập  $\mathbb{R}^+ \times \mathbb{R}^+$  là miền trong góc phần tư thứ nhất của mặt phẳng này. Tương tự

$$\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$$

biểu diễn không gian ba chiều.

**Ví dụ 5.2.** Cho  $A = \{1, 2, 3\}$ ,  $B = \{3, 4\}$ ,  $C = \{x, y\}$ . Xác định

- |                 |          |                          |
|-----------------|----------|--------------------------|
| a) $A \times B$ | c) $B^2$ | e) $A \times B \times C$ |
| b) $B \times A$ | d) $B^3$ |                          |

**Giải.** a)  $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$

```

1 A = {1, 2, 3}
2 B = {3, 4}
3 [(a, b) for a in A for b in B]
```

b)  $B \times A = \{(3, 1), (3, 2), (3, 3), (4, 1), (4, 2), (4, 3)\}$

$$c) B^2 = B \times B = \{(3, 3), (3, 4), (4, 3), (4, 4)\}$$

$$d) B^3 = B \times B \times B = \{(a, b, c) \mid a, b, c \in B\}$$

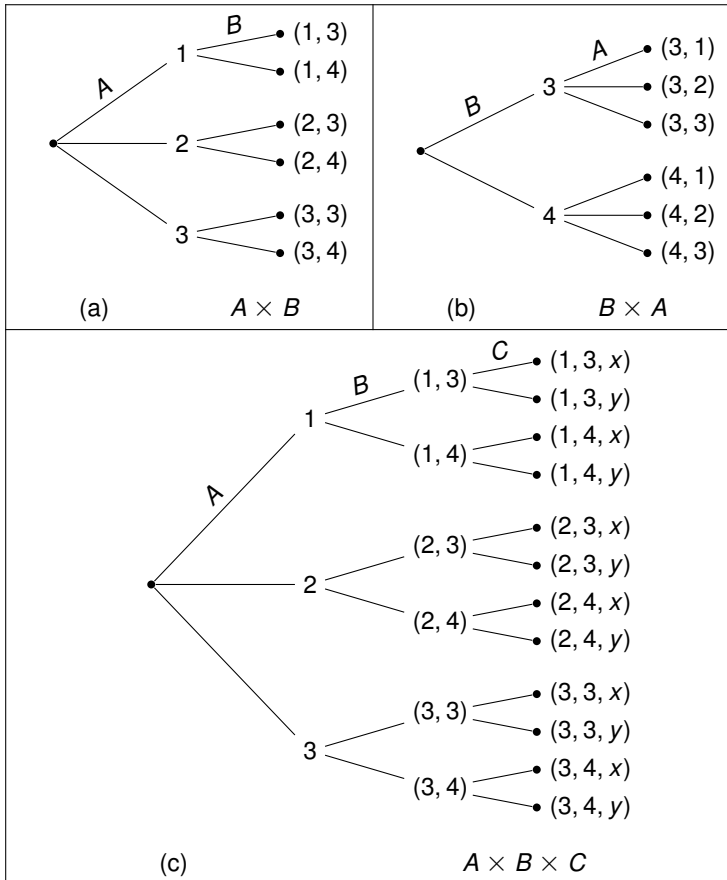
$$= \{(3, 3, 3), (3, 3, 4), (3, 4, 3), (3, 4, 4), (4, 3, 3), (4, 3, 4), (4, 4, 3), (4, 4, 4)\}$$

$$e) A \times B \times C = \{(a, b, c) \mid a \in A, b \in B, c \in C\}$$

$$= \{(1, 3, x), (1, 3, y), (1, 4, x), (1, 4, y), (2, 3, x), \dots, (3, 4, x), (3, 4, y)\}$$

□

Trong ví dụ trên, tích Descartes  $A \times B$  có thể biểu diễn trực quan thông qua *sơ đồ cây* (a) ở hình dưới. Sơ đồ này thác triển từ trái sang phải. Xuất phát từ điểm ngoài cùng bên trái, có ba nhánh, mỗi nhánh ứng với một phần tử của  $A$ . Sau đó từ mỗi điểm 1, 2, 3, có hai nhánh, mỗi nhánh ứng với một trong các phần tử 3, 4 của  $B$ . Sáu cặp có thứ tự ở các điểm cuối bên phải tạo thành các phần tử của  $A \times B$ . Sơ đồ (b, c) của hình mô tả cách xây dựng hai tập  $B \times A$  và  $A \times B \times C$ .



**Định nghĩa 5.2.** Cho hai tập  $A, B$ . Mỗi tập con của  $A \times B$  gọi là một quan hệ (hai ngôi) từ  $A$  vào  $B$ . Mỗi tập con của  $A \times A$  gọi là một quan hệ (hai ngôi) trên  $A$ .

Cho  $\mathcal{R}$  là quan hệ từ  $A$  vào  $B$ . Nếu  $(a, b) \in \mathcal{R}$ , ta viết  $a \mathcal{R} b$ , và nói  $a$  có quan hệ  $\mathcal{R}$  với  $b$ ; ngược lại,  $(a, b) \notin \mathcal{R}$ , ta viết  $a \not\mathcal{R} b$ , và nói  $a$  không có quan hệ  $\mathcal{R}$  với  $b$ .

Hiển nhiên  $\emptyset$  và  $A \times B$  là hai quan hệ từ  $A$  vào  $B$ , gọi là quan hệ tầm thường.

Nếu  $|A| = m$ ,  $|B| = n$  thì  $|A \times B| = mn$ . Theo **Định lý 3.3**, có  $2^{mn}$  quan hệ từ  $A$  vào  $B$ .

**Ví dụ 5.3.** Cho  $A = \{1, 2, 3\}$ ,  $B = \{x, y\}$ .

- a) Có bao nhiêu quan hệ từ  $A$  vào  $B$ ?
- b) Cho bốn ví dụ về quan hệ không tầm thường từ  $A$  vào  $B$ .

**Giải.** a)  $|A| = 3, |B| = 2 \Rightarrow |A \times B| = 3 \cdot 2 = 6$ . Số quan hệ từ  $A$  vào  $B$  là  $2^6 = 64$ .

- b) i)  $\{(1, x)\}$  iii)  $\{(1, x), (2, x), (3, x)\}$   
 ii)  $\{(1, x), (1, y)\}$  iv)  $\{(1, x), (2, x), (3, y)\}$



**Ví dụ 5.4.** Với  $\mathcal{U} = \{1, 2\}$ , đặt  $\mathcal{A} = \mathcal{P}(\mathcal{U}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ . Quan hệ tập con  $\mathcal{R}$  trên  $\mathcal{A}$  xác định bởi: với  $A, B \in \mathcal{P}(\mathcal{U})$ ,  $A \mathcal{R} B \Leftrightarrow A \subseteq B$ . Xác định  $\mathcal{R}$ .

*Giải.*

$$\mathcal{R} = \{ (\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\}) \}.$$

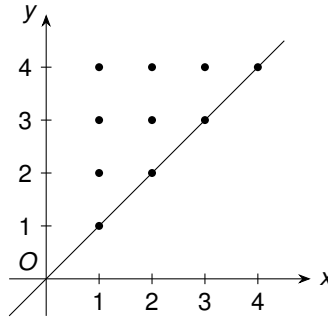


**Ví dụ 5.5.** Trên  $A = \mathbb{Z}^+$ , xét quan hệ thứ tự “bé hơn hoặc bằng”,  $\mathcal{R} = \{(x, y) \mid x \leq y\}$ .

- a) Mô tả quan hệ  $\mathcal{R}$ .
- b) Cho một định nghĩa đệ quy của  $\mathcal{R}$ , từ đó chứng minh  $(2, 4) \in \mathcal{R}$ .

*Giải.* a)  $\mathcal{R}$  là tập các điểm có các tọa độ nguyên dương, nằm phía trên hoặc ở đường  $y = x$  trên mặt phẳng Euclid, được biểu diễn một phần trên hình sau





b) Quan hệ  $\mathcal{R}$  trên  $\mathbb{Z}^+$  được định nghĩa đệ quy bởi

1)  $(1, 1) \in \mathcal{R}$ ; và

2)  $(x, y) \in \mathcal{R} \Rightarrow (2a) (x, y + 1) \in \mathcal{R}$ , và  $(2b) (x + 1, y + 1) \in \mathcal{R}$ .

Xuất phát từ  $(1, 1) \in \mathcal{R}$ , theo quy tắc  $(2a)$ ,  $(1, 1 + 1) = (1, 2) \in \mathcal{R}$ . Từ đó, lại áp dụng quy tắc  $(2a)$ , được  $(1, 2 + 1) = (1, 3) \in \mathcal{R}$ . Cuối cùng, áp dụng quy tắc  $(2b)$ , ta có  $(1 + 1, 3 + 1) = (2, 4) \in \mathcal{R}$ . Quá trình lập luận này có thể rút gọn thành sơ đồ

$$\xrightarrow{(1)} (1, 1) \xrightarrow{(2a)} (1, 2) \xrightarrow{(2a)} (1, 3) \xrightarrow{(2b)} (2, 4).$$

□

Ý tưởng xây dựng định nghĩa đệ quy cho một quan hệ gồm hai bước

- 1) Chọn các điểm xuất phát ban đầu. Các điểm này thường nằm trên biên của miền biểu diễn của quan hệ.
- 2) Tìm quy tắc đi từ các điểm xuất phát tới được điểm bất kỳ còn lại trên miền biểu diễn, nhưng các quy tắc này không gây ra việc đi đến các điểm khác nằm ngoài miền biểu diễn.

Số điểm xuất phát và số quy tắc càng ít càng tốt.

**Ví dụ 5.6.** Trên  $\mathbb{N}$  cho quan hệ  $\mathcal{R} = \{(m, n) \mid n = 7m\}$ . Chẳng hạn, một vài cặp thuộc  $\mathcal{R}$  như  $(0, 0)$ ,  $(1, 7)$ ,  $(11, 77)$  và  $(15, 105)$ .

a) Cho một định nghĩa đệ quy của  $\mathcal{R}$ .

b) Dùng định nghĩa đệ quy ở ý (a), chỉ ra  $(3, 21) \in \mathcal{R}$ .

*Giải.* a)  $\mathcal{R}$  được định nghĩa đệ quy bởi

1)  $(0, 0) \in \mathcal{R}$ ; và



- 5.8. a) Nếu  $A = \{1, 2, 3, 4, 5\}$  và  $B = \{w, x, y, z\}$ , thì  $\mathcal{P}(A \times B)$  có bao nhiêu phần tử?  
b) Tổng quát hóa kết quả của ý (a).

5.9. Chứng minh  $A \times (B - C) = (A \times B) - (A \times C)$ .

5.10. Cho hai tập  $A, B$  với  $|B| = 3$ . Nếu có 4096 quan hệ từ  $A$  vào  $B$ , thì  $|A| = ?$

5.11. Cho  $\mathcal{R} \subseteq \mathbb{N} \times \mathbb{N}$  trong đó  $(m, n) \in \mathcal{R}$  nếu  $n = 5m + 2$ .

- a) Nêu định nghĩa đệ quy cho  $\mathcal{R}$ .  
b) Dùng định nghĩa đệ quy ở ý (a) để chỉ ra  $(4, 22) \in \mathcal{R}$ .

- 5.12. a) Nêu định nghĩa đệ quy cho quan hệ  $\mathcal{R} \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$  trong đó  $(m, n) \in \mathcal{R}$  nếu  $m \geq n$ .  
b) Từ định nghĩa ở ý (a), chỉ ra  $(5, 2)$  và  $(4, 4)$  thuộc  $\mathcal{R}$ .


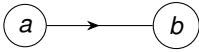

## 5.2 Biểu diễn quan hệ

### 5.2.1 Biểu diễn đồ thị của quan hệ

**Định nghĩa 5.3.** Cho  $V$  là tập hữu hạn khác rỗng. Một đồ thị có hướng  $G$  trên  $V$  gồm các phần tử của  $V$ , gọi là các đỉnh của  $G$ , và một tập con  $E$  của  $V \times V$  chứa các cạnh của  $G$ . Ta viết  $G = (V, E)$ .

Nếu  $(a, b) \in E$ , ta nói có cạnh từ  $a$  tới  $b$ . Đỉnh  $a$  là đỉnh đầu của cạnh,  $b$  là đỉnh cuối. Ta nói  $a$  kề trước  $b$ , hay  $b$  kề sau  $a$ . Cạnh có dạng  $(a, a)$  gọi là vòng. Đỉnh không có cạnh gọi là đỉnh cô lập.

Một quan hệ  $\mathcal{R}$  trên  $A$  được biểu diễn bằng đồ thị có hướng  $G = (A, \mathcal{R})$ .

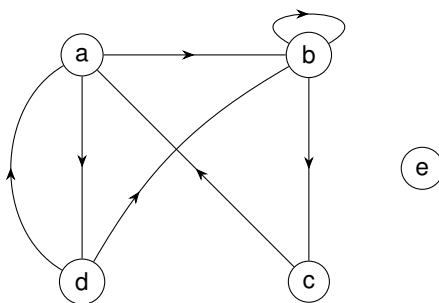
Đối tượng	Biểu diễn	Tên gọi
$a \in A$		đỉnh
$a \mathcal{R} b$		cạnh
$a \mathcal{R} a$		vòng

**Ví dụ 5.7.** Cho  $A = \{a, b, c, d, e\}$ . Mô tả quan hệ

$$\mathcal{R} = \{(a, b), (a, d), (b, b), (b, c), (c, a), (d, a), (d, b), (d, d)\}$$

trên  $A$  bằng đồ thị.

*Giải.*



□

### 5.2.2 Ma trận quan hệ

**Định nghĩa 5.4.** Ma trận  $E = (e_{ij})_{m \times n}$  có  $e_{ij} \in \{0, 1\}$ ,  $1 \leq i \leq m$ ,  $1 \leq j \leq n$  gọi là ma trận 0–1.

**Định nghĩa 5.5.** Cho hai tập  $A = \{a_1, a_2, \dots, a_m\}$ ,  $B = \{b_1, b_2, \dots, b_n\}$  khác rỗng. Cố định vị trí các phần tử. Quan hệ  $\mathcal{R} \subseteq A \times B$  được biểu diễn bằng ma trận quan hệ, ký hiệu  $M(\mathcal{R})$ , hay  $M_{\mathcal{R}} = (m_{ij})_{m \times n}$  xác định bởi  $m_{ij} = \begin{cases} 1, & \text{nếu } (a_i, b_j) \in \mathcal{R} \\ 0, & \text{nếu } (a_i, b_j) \notin \mathcal{R}. \end{cases}$

**Nhận xét:**  $M_{\mathcal{R}} = \mathbf{0}$  (ma trận toàn 0)  $\Leftrightarrow \mathcal{R} = \emptyset$ , và  $M_{\mathcal{R}} = \mathbf{1}$  (ma trận toàn 1)  $\Leftrightarrow \mathcal{R} = A \times B$ .

**Ví dụ 5.8.** Cho  $A = \{1, 2, 3\}$ ,  $B = \{x, y, z, t\}$ , và  $\mathcal{R} = \{(1, w), (1, z), (2, x), (2, z), (3, w)\} \subseteq A \times B$ . Xác định  $M_{\mathcal{R}}$ .

*Giải.*

$$M_{\mathcal{R}} = \begin{matrix} & \begin{matrix} x & y & z & t \end{matrix} \\ \begin{matrix} (1) \\ (2) \\ (3) \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

có các hàng được đánh dấu bởi các phần tử của  $A$ , các cột được đánh dấu bởi các phần tử của  $B$ . □

## 5.3 Hàm: đơn ánh

Phần này tập trung vào loại quan hệ đặc biệt gọi là *hàm*, xuất hiện trong nhiều lĩnh vực của toán học và khoa học máy tính. Quan hệ tổng quát sẽ được nghiên cứu kỹ hơn

ở Chương 6.

**Định nghĩa 5.6.** Cho hai tập  $A, B \neq \emptyset$ . Quan hệ  $f$  từ  $A$  vào  $B$  gọi là hàm, hay ánh xạ, từ  $A$  vào  $B$ , ký hiệu  $f : A \rightarrow B$ , nếu mỗi phần tử của  $A$  xuất hiện đúng một lần ở thành phần thứ nhất trong các cặp của  $f$ .

$$\forall a \in A, \exists! b \in B, (a, b) \in f. \quad (5.9)$$

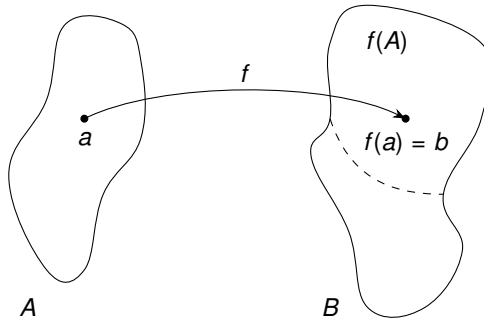
Phần tử duy nhất  $b \in B$  thỏa mãn  $(a, b) \in f$ , ký hiệu  $b = f(a)$ , gọi là ảnh của  $a$  qua  $f$ .  $a$  là một tạo ảnh của  $b$ .

$A$  là tập nguồn hay tập xác định,  $B$  là tập đích của  $f$ .

**Định nghĩa 5.7.** Cho  $f : A \rightarrow B$ . Miền giá trị của  $f$  là tập các phần tử ở thành phần thứ hai trong các cặp của  $f$ :

$$\begin{aligned} f(A) &= \{b \mid \exists a \in A, b = f(a)\} \\ &= \{f(a) \mid a \in A\}. \end{aligned}$$

Ta mô tả khái niệm trên bằng hình sau.



Một cách hình dung sơ đồ này, xem  $a$  là nguồn dữ liệu (input), được biến đổi bởi  $f$  thành kết quả tương ứng  $f(a)$  (output). Theo đó, trình biên dịch C++ được xem như hàm biến đổi một mã nguồn thành chương trình thực thi tương ứng.

**Ví dụ 5.9.** Với  $A = \{1, 2, 3\}$  và  $B = \{x, y, z, t\}$ , xét các quan hệ từ  $A$  vào  $B$ :

- a)  $f = \{(1, x), (2, t), (3, t)\}$  từ  $A$  vào  $B$  là hàm từ  $A$  vào  $B$ , và  $f(A) = \{x, t\}$ .
- b)
  - i)  $\mathcal{R}_1 = \{(1, w), (2, w)\}$  không phải hàm từ  $A$  vào  $B$ , vì  $3 \in A$  không xuất hiện ở thành phần thứ nhất trong các cặp;
  - ii)  $\mathcal{R}_2 = \{(1, w), (2, w), (2, x), (3, z)\}$  cũng vậy, vì  $2 \in A$  xuất hiện nhiều hơn một lần ở thành phần thứ nhất của các cặp.

Giả sử  $A = \{a_1, a_2, \dots, a_m\}$ ,  $B = \{b_1, b_2, \dots, b_n\}$ .

- Mỗi hàm  $f : A \rightarrow B$  có dạng

$$f = \{(a_1, x_1), (a_2, x_2), \dots, (a_m, x_m)\}$$

trong đó mỗi  $x_i \in B$ ,  $1 \leq i \leq m$  có  $n$  cách nhận giá trị. Theo quy tắc nhân, số hàm từ  $A$  vào  $B$  là

$$\underbrace{n \times n \times \dots \times n}_m = n^m = |B|^{|A|}. \quad (5.10)$$

- Coi mỗi phần tử của  $A$  là một vật, mỗi phần tử của  $B$  là một hộp. Khi  $f(a) = b$ , ta xếp vật  $a$  vào hộp  $b$ . Như vậy mỗi hàm từ  $A$  vào  $B$  là một cách sắp xếp  $m$  vật vào  $n$  hộp, và có  $n^m$  cách xếp  $m$  vật vào  $n$  hộp.
- Quan hệ  $\mathcal{R}$  từ  $A$  vào  $B$  với ma trận quan hệ  $M_{\mathcal{R}} = (m_{ij})_{m \times n}$ , là hàm từ  $A$  vào  $B$  nếu

$$\forall i = \overline{1, m}, \sum_{j=1}^n m_{ij} = 1. \quad (5.11)$$

Có nhiều hàm thú vị trong khoa học máy tính.

**Định nghĩa 5.8.** Hàm sàn  $f : \mathbb{R} \rightarrow \mathbb{Z}$ , ký hiệu  $f(x) = \lfloor x \rfloor$  là số nguyên lớn nhất không vượt quá  $x$ :

$$\begin{cases} \lfloor x \rfloor \in \mathbb{Z} \\ \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \text{ hay } x - 1 < \lfloor x \rfloor \leq x. \end{cases}$$

Nếu  $x \in \mathbb{Z}$  thì  $\lfloor x \rfloor = x$ ; và nếu  $x \in \mathbb{R} - \mathbb{Z}$ ,  $\lfloor x \rfloor$  là số nguyên ngay bên trái  $x$  trên đường thẳng thực. Chẳng hạn  $\lfloor 3.8 \rfloor = 3$ ,  $\lfloor 3 \rfloor = 3$ ,  $\lfloor -3.8 \rfloor = -4$ ,  $\lfloor -3 \rfloor = -3$ . Ngoài ra, ta thấy

$$\lfloor 7.1 + 8.2 \rfloor = \lfloor 15.3 \rfloor = 15 \text{ và } \lfloor 7.1 \rfloor + \lfloor 8.2 \rfloor = 7 + 8 = 15, \text{ nhưng}$$

$$\lfloor 7.7 + 8.4 \rfloor = \lfloor 16.1 \rfloor = 16 \text{ và } \lfloor 7.7 \rfloor + \lfloor 8.4 \rfloor = 7 + 8 = 15.$$

tức là hàm sàn không có tính cộng tính.

**Định nghĩa 5.9.** Hàm trần  $c : \mathbb{R} \rightarrow \mathbb{Z}$ , ký hiệu  $c(x) = \lceil x \rceil$  là số nguyên bé nhất lớn hơn hoặc bằng  $x$ :

$$\begin{cases} \lceil x \rceil \in \mathbb{Z} \\ \lceil x \rceil \geq x > \lceil x \rceil - 1 \text{ hay } x \leq \lceil x \rceil < x + 1. \end{cases}$$

Như vậy,  $\lceil x \rceil = x$  nếu  $x \in \mathbb{Z}$ , và khi  $x \in \mathbb{R} - \mathbb{Z}$ ,  $\lceil x \rceil$  là số nguyên ngay bên phải  $x$  trên đường thẳng thực. Chẳng hạn

$$\lceil 3 \rceil = 3, \lceil 3.01 \rceil = \lceil 3.7 \rceil = 4 = \lceil 4 \rceil, \lceil -3 \rceil = -3, \lceil -3.01 \rceil = \lceil -3.7 \rceil = -3.$$

Ta cũng thấy hàm trần không có tính cộng tính

$$\lceil 3.6 + 4.5 \rceil = \lceil 8.1 \rceil = 9 \text{ và } \lceil 3.6 \rceil + \lceil 4.5 \rceil = 4 + 5 = 9, \text{ nhưng}$$

$$\lceil 3.3 + 4.2 \rceil = \lceil 7.5 \rceil = 8 \text{ và } \lceil 3.3 \rceil + \lceil 4.2 \rceil = 4 + 5 = 9.$$

```
1 from sympy import *
2 floor(3.8)      # → 3
3 ceiling(3.7)    # → 4
```

Hàm cắt  $t : \mathbb{R} \rightarrow \mathbb{Z}$ , với  $t(x)$  là phần còn lại sau khi bỏ đi phần sau dấu phẩy trong biểu diễn thập phân của  $x$ . Chẳng hạn,  $t(3.78) = 3$ ,  $t(5) = 5$ ,  $t(-7.22) = -7$ . Lưu ý,  $t(3.78) = \lfloor 3.78 \rfloor = 3$  và  $t(-3.78) = \lceil -3.78 \rceil = -3$ . Có thể thấy

$$t(x) = \begin{cases} \lfloor x \rfloor, & \text{nếu } x \geq 0 \\ \lceil x \rceil, & \text{nếu } x < 0 \end{cases}$$

Các hàm sàn, hàm trần, và hàm cắt thường gọi là các hàm nguyên. Ta có

$$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$$

**Ví dụ 5.10.** Khi lưu ma trận  $A = (a_{ij})_{m \times n}$  bởi mảng một chiều, hàng 1 của  $A$  được lưu vào  $n$  vị trí đầu của mảng, là  $1, 2, \dots, n$ , hàng 2 được lưu vào  $n$  vị trí kế tiếp  $n + 1, n + 2, \dots, 2n$ , hàng 3 được lưu vào các vị trí từ  $2n + 1$  tới  $3n$ , hàng  $i$  gồm  $a_{i1}, a_{i2}, \dots, a_{in}$  vào các vị trí  $(i - 1)n + 1, (i - 1)n + 2, \dots, in$ , với  $1 \leq i \leq m$ . Hàm truy cập  $f$  xác định vị trí của  $a_{ij}$  trong mảng

$a_{11}$	$a_{12}$	$\dots$	$a_{1n}$	$a_{21}$	$a_{22}$	$\dots$	$a_{2n}$	$a_{31}$	$a_{32}$	$\dots$	$a_{3n}$	$\dots$	$a_{mn}$
1	2	$\dots$	$n$	$n + 1$	$n + 2$	$\dots$	$2n$	$2n + 1$	$2n + 2$	$\dots$	$3n$	$\dots$	$mn$

Để biết vị trí của  $a_{ij}$ ,  $1 \leq i \leq m$ ,  $1 \leq j \leq n$  trong mảng, ta dùng hàm truy cập  $f$  xác định bởi  $f(a_{ij}) = (i - 1)n + j$ .

**Ví dụ 5.11.** Trong [Chương 4](#), xét phép chia số nguyên  $a$  cho số nguyên dương  $b$ .

$$\exists! q, r \in \mathbb{Z}, (0 \leq r < b), a = qb + r$$

a) Biểu diễn  $q, r$  bởi hàm nguyên và phép toán số học.

b) Chứng minh  $\lfloor \frac{a}{b} \rfloor + 1 = \lceil \frac{a+1}{b} \rceil$ .

c) Cho  $a, b \in \mathbb{Z}^+$ . Tìm công thức đếm số bội của  $b$  (i) từ 1 tới  $a$ , và (ii) từ 0 tới  $a$ .

*Giải.* a) Ta có  $\frac{a}{b} = q + \frac{r}{b}$ , mà  $0 \leq r < b$  nên  $q \leq \frac{a}{b} < q + 1$  với  $q \in \mathbb{Z}$ , suy ra

$$q = \lfloor \frac{a}{b} \rfloor, \quad \text{và} \quad r = a - \lfloor \frac{a}{b} \rfloor b.$$

b) Ta có  $\frac{a+1}{b} = q + \frac{r+1}{b}$ . Vì  $0 \leq r < b$  nên  $1 \leq r+1 \leq b$ , suy ra  $q < \frac{a+1}{b} \leq q+1$ .  
 Vậy  $\lceil \frac{a+1}{b} \rceil = q+1 = \lfloor \frac{a}{b} \rfloor + 1$ .

c) i) Trong các số nguyên từ 1 tới  $a$ , xét các bội của  $b$ , có dạng  $qb$  với  $q \in \mathbb{Z}$  và  $1 \leq qb \leq a$ . Suy ra  $\frac{1}{b} \leq q \leq \frac{a}{b}$ , nên  $q$  có thể nhận các giá trị  $1, 2, \dots$ , tới  $\lfloor \frac{a}{b} \rfloor$  (số nguyên lớn nhất bé hơn hoặc bằng  $\frac{a}{b}$ ). Do đó, từ 1 tới  $a$ , có  $\lfloor \frac{a}{b} \rfloor$  bội của  $b$ .

ii) Lập luận tương tự ý (i), số bội của  $b$  từ 0 đến  $a$  là  $\lfloor \frac{a}{b} \rfloor + 1$ . Theo ý (b), số này bằng  $\lceil \frac{a+1}{b} \rceil$ .

□

Cho  $n \in \mathbb{Z}^+$  với  $n > 1$ , theo Định lý cơ bản của số học,  $n$  có phân tích

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

trong đó  $k \in \mathbb{Z}^+$ ,  $p_1, p_2, \dots, p_k$  nguyên tố và đôi một khác nhau,  $e_i \in \mathbb{Z}^+$ ,  $\forall i = \overline{1, k}$ . Khi đó với  $r \in \mathbb{Z}^+$ , ta đếm các ước dương  $m$  của  $n$  là  $r$ -phương (bằng lũy thừa bậc  $r$  của số nguyên dương nào đó)

$$m = (p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k})^r = p_1^{rf_1} p_2^{rf_2} \cdots p_k^{rf_k}$$

Để  $m \mid n$ , ta cần  $0 \leq rf_i \leq e_i$ ,  $\forall i = \overline{1, k}$ . Số cách chọn  $f_i$  chính là số bội của  $r$  từ 0 tới  $e_i$ . Theo quy tắc nhân, số ước của  $n$  và là  $r$ -phương là  $\prod_{i=1}^k \lceil \frac{e_i+1}{r} \rceil$ . Khi  $r = 1$ , ta được

$$\prod_{i=1}^k \lceil e_i + 1 \rceil = \prod_{i=1}^k (e_i + 1) \text{ ước dương của } n.$$

Trong Ví dụ 4.32, số

$$29\,338\,848\,000 = 2^8 3^5 5^3 7^3 11$$

có

$$60 = 5 \cdot 3 \cdot 2 \cdot 2 \cdot 1 = \lceil \frac{8+1}{2} \rceil \lceil \frac{5+1}{2} \rceil \lceil \frac{3+1}{2} \rceil \lceil \frac{3+1}{2} \rceil \lceil \frac{1+1}{2} \rceil$$

ước dương chính phương.

**Ví dụ 5.12.** Dãy số thực  $r_1, r_2, \dots$  có thể xem như một hàm  $f : \mathbb{Z}^+ \rightarrow \mathbb{R}$  trong đó  $f(n) = r_n$ ,  $\forall n \in \mathbb{Z}^+$ . Tương tự, ta xem dãy số nguyên  $a_0, a_1, a_2, \dots$  như hàm  $g : \mathbb{N} \rightarrow \mathbb{Z}$  trong đó  $g(n) = a_n$ ,  $\forall n \in \mathbb{N}$ .

**Định nghĩa 5.10.** Hàm  $f : A \rightarrow B$  gọi là đơn ánh nếu mỗi phần tử của  $B$  xuất hiện không quá một lần ở thành phần thứ hai trong các cặp của  $f$ :

$$\forall b \in B, [\exists! a \in A, b = f(a)] \vee [\exists! a \in A, b = f(a)]$$



Hai định nghĩa khác của đơn ánh này

$$1) \forall a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2, \text{ hoặc}$$

$$2) \forall a_1, a_2 \in A, a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

tức là hai phần tử khác nhau trong  $A$  có ảnh khác nhau.

Thêm nữa, nếu  $f : A \rightarrow B$  là đơn ánh, và  $A, B$  hữu hạn, thì  $|A| \leq |B|$ .

**Ví dụ 5.13.** a) Xét  $f : \mathbb{R} \rightarrow \mathbb{R}$  trong đó  $f(x) = 3x + 7 \forall x \in \mathbb{R}$ . Khi đó  $\forall x_1, x_2 \in \mathbb{R}$ , ta có

$$f(x_1) = f(x_2) \Rightarrow 3x_1 + 7 = 3x_2 + 7 \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2,$$

vì thế,  $f$  là đơn ánh.

b) Hàm  $g : \mathbb{R} \rightarrow \mathbb{R}$  xác định bởi  $g(x) = x^4 - x \forall x \in \mathbb{R}$ . Ta thấy

$$g(0) = 0^4 - 0 = 0 \text{ và } g(1) = 1^4 - 1 = 0.$$

Do đó,  $g$  không là đơn ánh, vì  $0 \neq 1$  nhưng  $g(0) = g(1)$  (có hai phần tử khác nhau có chung ảnh).

**Ví dụ 5.14.** Cho  $A = \{1, 2, 3\}$  và  $B = \{1, 2, 3, 4, 5\}$ . Xét hai hàm từ  $A$  vào  $B$ .

a)  $f = \{(1, 2), (2, 3), (3, 4)\}$  là đơn ánh.

b)  $g = \{(1, 2), (2, 3), (3, 3)\}$  không là đơn ánh vì  $g(2) = g(3)$  nhưng  $2 \neq 3$ .

Giả sử  $A = \{a_1, a_2, \dots, a_m\}$ ,  $B = \{b_1, b_2, \dots, b_n\}$ .

• Mỗi đơn ánh  $f : A \rightarrow B$  có dạng

$$f = \{(a_1, x_1), (a_2, x_2), \dots, (a_m, x_m)\}$$

trong đó  $x_1, x_2, \dots, x_m \in B$  và đôi một khác nhau. Như vậy,  $x_1$  có  $n$  cách chọn,  $x_2$  có  $n-1$  cách chọn,  $x_3$  có  $n-2$  cách chọn, ... và cuối cùng  $x_m$  có  $n-(m-1) = n-m+1$  cách chọn. Theo quy tắc nhân, số đơn ánh từ tập  $A$  cỡ  $m$  vào tập  $B$  cỡ  $n$  là

$$n(n-1)(n-2) \cdots (n-m+1) = \frac{n!}{(n-m)!} = P(n, m). \quad (5.12)$$

Chẳng hạn, với  $A = \{1, 2, 3\}$  và  $B = \{x, y, z, u, v\}$ , có  $5 \cdot 4 \cdot 3 = 60$  đơn ánh từ  $A$  vào  $B$ .

- Nếu coi mỗi phần tử của  $A$  là một vật, mỗi phần tử của  $B$  là một hộp, thì mỗi đơn ánh từ  $A$  vào  $B$  là một cách sắp xếp  $m$  vật vào  $n$  hộp sao cho mỗi hộp chứa nhiều nhất một vật, hay hai vật khác nhau ở hai hộp khác nhau.
- Hàm  $f : A \rightarrow B$ , với ma trận quan hệ  $M_f = (m_{ij})_{m \times n}$ , là đơn ánh, nếu

$$\forall j = \overline{1, n}, \sum_{i=1}^m m_{ij} \leq 1. \quad (5.13)$$

**Định nghĩa 5.11.** Cho  $f : A \rightarrow B$  và  $A_1 \subseteq A$ . Ảnh của  $A_1$  qua  $f$ :

$$\begin{aligned} f(A_1) &= \{b \mid \exists a \in A_1, b = f(a)\} \\ &= \{f(a) \mid a \in A_1\}. \end{aligned}$$

**Ví dụ 5.15.** Với  $A = \{1, 2, 3, 4, 5\}$  và  $B = \{w, x, y, z\}$ , cho  $f : A \rightarrow B$  xác định bởi  $f = \{(1, w), (2, x), (3, x), (4, y), (5, y)\}$ . Khi đó  $A_1 = \{1\}$ ,  $A_2 = \{1, 2\}$ ,  $A_3 = \{1, 2, 3\}$ ,  $A_4 = \{2, 3\}$  và  $A_5 = \{2, 3, 4, 5\}$  có các ảnh tương ứng qua  $f$ :

$$\begin{aligned} f(A_1) &= \{f(a) \mid a \in A_1\} = \{f(a) \mid a \in \{1\}\} = \{f(a) \mid a = 1\} = \{f(1)\} = \{w\}; \\ f(A_2) &= \{f(a) \mid a \in A_2\} = \{f(a) \mid a \in \{1, 2\}\} \\ &= \{f(a) \mid a = 1 \text{ hoặc } 2\} = \{f(1), f(2)\} = \{w, x\}; \\ f(A_3) &= \{f(1), f(2), f(3)\} = \{w, x, x\} = \{w, x\} = f(A_2) \\ f(A_4) &= \{x\}; \text{ và } f(A_5) = \{x, y\}. \end{aligned}$$

**Ví dụ 5.16.** a) Cho  $g : \mathbb{R} \rightarrow \mathbb{R}$  xác định bởi  $g(x) = x^2$ . Khi đó  $g(\mathbb{R}) = [0, +\infty)$ ,  $g(\mathbb{Z}) = \{0, 1, 4, 9, \dots\}$ , và với  $A_1 = [-2, 1]$  ta có  $g(A_1) = [0, 4]$ .

b) Cho  $h : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  bởi  $h(x, y) = 2x + 3y$ . Chẳng hạn,  $h(0, 0) = 2 \cdot 0 + 3 \cdot 0 = 0$ ,  $h(-3, 7) = 2(-3) + 3 \cdot 7 = 15$ . Thêm nữa,  $h(2, -1) = 2 \cdot 2 + 3(-1) = 1$ , và  $\forall n \in \mathbb{Z}$ ,  $h(2n, -n) = 2 \cdot 2n + 3(-n) = n$ . Do đó  $h(\mathbb{Z} \times \mathbb{Z}) = \mathbb{Z}$ . Với  $A_1 = \{(0, n) \mid n \in \mathbb{Z}^+\}$ , ta có  $h(A_1) = \{3, 6, 9, \dots\} = \{3n \mid n \in \mathbb{Z}^+\}$ .

**Định lý 5.2.** Cho  $f : A \rightarrow B$  và  $A_1, A_2 \subseteq A$ . Khi đó

$$a) f(A_1 \cup A_2) = f(A_1) \cup f(A_2) \quad b) f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$$

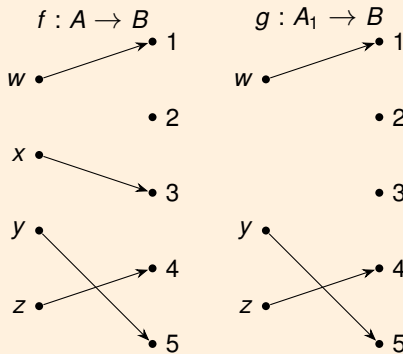
$$c) \text{ Nếu } f \text{ là đơn ánh thì } f(A_1 \cap A_2) = f(A_1) \cap f(A_2).$$

**Định nghĩa 5.12.** Cho  $f : A \rightarrow B$ ,  $A_1 \subseteq A$  và  $g : A_1 \rightarrow B$  sao cho  $g(a) = f(a) \forall a \in A_1$ . Khi đó  $g$  gọi là hạn chế của  $f$  (từ  $A$ ) lên  $A_1$ , ký hiệu  $g = f|_{A_1}$ , và  $f$  là một mở rộng của  $g$  (từ  $A_1$ ) lên  $A$ .

**Ví dụ 5.17.** Với  $A = \{1, 2, 3, 4, 5\}$  cho  $f : A \rightarrow \mathbb{R}$  bởi  $f = \{(1, 10), (2, 13), (3, 16), (4, 19), (5, 22)\}$ . Cho  $g : \mathbb{Q} \rightarrow \mathbb{R}$  bởi  $g(q) = 3q + 7 \forall q \in \mathbb{Q}$  và  $h : \mathbb{R} \rightarrow \mathbb{R}$  với  $h(r) = 3r + 7 \forall r \in \mathbb{R}$ . Khi đó  $h|_{\mathbb{Q}} = g$ ,  $g|_A = f$  và  $h|_A = f$ . Tương ứng, ta nói

- i)  $h$  là một mở rộng của  $g$  (từ  $\mathbb{Q}$ ) lên  $\mathbb{R}$ ;
- ii)  $g$  là hạn chế của  $h$  (từ  $\mathbb{R}$ ) lên  $\mathbb{Q}$ ;
- iii)  $g$  là một mở rộng của  $f$  (từ  $A$ ) lên  $\mathbb{Q}$ ;
- iv)  $f$  là hạn chế của  $g$  (từ  $\mathbb{Q}$ ) lên  $A$ ;
- v)  $h$  là một mở rộng của  $f$  (từ  $A$ ) lên  $\mathbb{R}$ ; và
- vi)  $f$  là hạn chế của  $h$  (từ  $\mathbb{R}$ ) lên  $A$ .

**Ví dụ 5.18.** Cho  $A = \{w, x, y, z\}$ ,  $B = \{1, 2, 3, 4, 5\}$  và  $A_1 = \{w, y, z\}$ . Cho  $f : A \rightarrow B$  và  $g : A_1 \rightarrow B$  biểu diễn bằng sơ đồ trong hình sau. Khi đó  $g = f|_{A_1}$  và  $f$  là một mở rộng của  $g$  từ  $A_1$  lên  $A$ , trong số tất cả 5 mở rộng của  $g$  lên  $A$ .



### Bài tập 5.3

**5.13.** Xác định quan hệ sau có là hàm không. Nếu quan hệ là hàm, tìm tập giá trị của nó.

- a) Quan hệ  $\{(x, y) \mid x, y \in \mathbb{Z}, y = x^2 + 7\}$  từ  $\mathbb{Z}$  vào  $\mathbb{Z}$
- b) Quan hệ  $\{(x, y) \mid x, y \in \mathbb{R}, y^2 = x\}$  từ  $\mathbb{R}$  vào  $\mathbb{R}$
- c) Quan hệ  $\{(x, y) \mid x, y \in \mathbb{R}, y = 3x + 1\}$  từ  $\mathbb{R}$  vào  $\mathbb{R}$

- d) Quan hệ  $\{(x, y) \mid x, y \in \mathbb{Q}, x^2 + y^2 = 1\}$  từ  $\mathbb{Q}$  vào  $\mathbb{Q}$   
 e) Quan hệ  $\mathcal{R}$  từ  $A$  vào  $B$  trong đó  $|A| = 5$ ,  $|B| = 6$ , và  $|\mathcal{R}| = 6$ .

5.14. Công thức  $f(x) = \frac{1}{x^2 - 2}$  có xác định một hàm  $f : \mathbb{R} \rightarrow \mathbb{R}$ ? hàm  $f : \mathbb{Z} \rightarrow \mathbb{R}$ ?

5.15. Cho  $A = \{1, 2, 3, 4\}$  và  $B = \{x, y, z\}$ .

- a) Liệt kê năm hàm từ  $A$  vào  $B$ .  
 b) Có bao nhiêu hàm  $f : A \rightarrow B$ ?  
 c) Có bao nhiêu đơn ánh  $f : A \rightarrow B$ ?  
 d) Có bao nhiêu hàm  $g : B \rightarrow A$ ?  
 e) Có bao nhiêu đơn ánh  $g : B \rightarrow A$ ?  
 f) Có bao nhiêu hàm  $f : A \rightarrow B$  thỏa mãn  $f(1) = x$ ?  
 g) Có bao nhiêu hàm  $f : A \rightarrow B$  thỏa mãn  $f(1) = f(2) = x$ ?  
 h) Có bao nhiêu hàm  $f : A \rightarrow B$  thỏa mãn  $f(1) = x$  và  $f(2) = y$ ?

5.16. Nếu có 2187 hàm  $f : A \rightarrow B$  và  $|B| = 3$ , thì  $|A| = ?$

5.17. Cho  $A, B, C \subseteq \mathbb{R}^2$  trong đó  $A = \{(x, y) \mid y = 2x + 1\}$ ,  $B = \{(x, y) \mid y = 3x\}$ , và  $C = \{(x, y) \mid x - y = 7\}$ .  
 Xác định

- a)  $A \cap B$       b)  $B \cap C$       c)  $\overline{A \cup C}$       d)  $\overline{B \cup C}$

5.18. Cho  $A, B, C \subseteq \mathbb{Z}^2$  với  $A = \{(x, y) \mid y = 2x + 1\}$ ,  $B = \{(x, y) \mid y = 3x\}$ , và  $C = \{(x, y) \mid x - y = 7\}$ .

- a) Tìm  
 i)  $A \cap B$       ii)  $B \cap C$       iii)  $\overline{A \cup C}$       iv)  $\overline{B \cup C}$   
 b) Đáp án của các ý (i)–(iv) bị ảnh hưởng thế nào nếu  $A, B, C \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$ ?

5.19. Tính

- a)  $\lfloor 2.3 - 1.6 \rfloor$       c)  $\lceil 3.4 \rceil \lfloor 6.2 \rfloor$       e)  $\lfloor 2\pi \rfloor$   
 b)  $\lfloor 2.3 \rfloor - \lfloor 1.6 \rfloor$       d)  $\lfloor 3.4 \rfloor \lceil 6.2 \rceil$       f)  $2\lceil \pi \rceil$

5.20. Chỉ ra khẳng định sau đúng hay sai. Nếu sai, hãy cho phản ví dụ.

- a)  $\lfloor a \rfloor = \lceil a \rceil$ ,  $\forall a \in \mathbb{Z}$       c)  $\lfloor a \rfloor = \lceil a \rceil - 1$ ,  $\forall a \in \mathbb{R} - \mathbb{Z}$   
 b)  $\lfloor a \rfloor = \lceil a \rceil$ ,  $\forall a \in \mathbb{R}$       d)  $-\lceil a \rceil = \lceil -a \rceil$ ,  $\forall a \in \mathbb{R}$

5.21. Tìm tất cả  $x \in \mathbb{R}$  sao cho

a)  $7 \lfloor x \rfloor = \lfloor 7x \rfloor$

c)  $\lfloor x + 7 \rfloor = x + 7$

b)  $\lfloor 7x \rfloor = 7$

d)  $\lfloor x + 7 \rfloor = \lfloor x \rfloor + 7$

5.22. Tìm tất cả  $x \in \mathbb{R}$  sao cho  $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = \lfloor 2x \rfloor$ .

5.23. a) Tìm tất cả  $x \in \mathbb{R}$  thỏa mãn  $\lceil 3x \rceil = 3 \lceil x \rceil$ .

b) Cho  $n \in \mathbb{Z}^+$ ,  $n > 1$ . Tìm tất cả  $x \in \mathbb{R}$  sao cho  $\lceil nx \rceil = n \lceil x \rceil$ .

5.24. Với  $n, k \in \mathbb{Z}^+$ , chứng minh  $\lceil \frac{n}{k} \rceil = \lfloor \frac{n-1}{k} \rfloor + 1$ .

5.25. a) Cho  $a \in \mathbb{R}^+$ ,  $a \geq 1$ . Chứng minh (i)  $\lfloor \frac{a}{a} \rfloor = 1$ ; và (ii)  $\lceil \frac{a}{a} \rceil = 1$ .

b) Nếu  $a \in \mathbb{R}^+$  và  $0 < a < 1$ , các kết luận ở ý (a) còn đúng không?

5.26. Cho  $a_1, a_2, a_3, \dots$  là dãy số nguyên định nghĩa đệ quy bởi

1)  $a_1 = 1$ , và

2)  $a_n = 2a_{\lfloor n/2 \rfloor}, \forall n \geq 2$ .

Hãy

a) Tìm  $a_n$ , với  $2 \leq n \leq 8$ .

b) Chứng minh  $a_n \leq n, \forall n \in \mathbb{Z}^+$ .

5.27. Xác định hàm sau có là đơn ánh không và tìm miền giá trị của nó.

a)  $f: \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = 2x + 1$

d)  $f: \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = e^x$

b)  $f: \mathbb{Q} \rightarrow \mathbb{Q}, f(x) = 2x + 1$

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

c)  $f: \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = x^3 - x$

f)  $f: [0, \pi] \rightarrow \mathbb{R}, f(x) = \sin x$

5.28. Cho  $f: \mathbb{R} \rightarrow \mathbb{R}$  với  $f(x) = x^2$ . Tìm  $f(A)$  nếu

a)  $A = \{2, 3\}$

c)  $A = (-3, 3)$

e)  $A = [-7, 2]$

b)  $A = \{-3, -2, 2, 3\}$

d)  $A = (-3, 2]$

f)  $A = (-4, -3] \cup [5, 6]$

5.29. Cho  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{w, x, y, z\}$ ,  $A_1 = \{2, 3, 5\} \subseteq A$ , và  $g: A_1 \rightarrow B$ . Có bao nhiêu mở rộng của  $g$  từ  $A_1$  lên  $A$ .

5.30. Cho ví dụ hàm  $f: A \rightarrow B$  và  $A_1, A_2 \subseteq A$  sao cho  $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$ . [Suy ra kết luận trong Định lý 5.2(b) có thể là tập con thực sự.]

**5.31.** Chứng minh ý (a) và (c) của [Định lý 5.2](#).

**5.32.** Nếu  $A = \{1, 2, 3, 4, 5\}$  và có 6720 đơn ánh  $f : A \rightarrow B$ , thì  $|B| = ?$

**5.33.** Cho  $f : A \rightarrow B$ , trong đó  $A = X \cup Y$  với  $X \cap Y = \emptyset$ . Nếu  $f|_X$  và  $f|_Y$  là đơn ánh, có suy ra được  $f$  cũng là đơn ánh?

**5.34.** Với  $n \in \mathbb{Z}^+$ , xét  $X_n = \{1, 2, 3, \dots, n\}$ . Với  $m, n \in \mathbb{Z}^+$ ,  $f : X_m \rightarrow X_n$  gọi là *đơn điệu tăng* nếu  $\forall i, j \in X_m, i < j \Rightarrow f(i) \leq f(j)$ .

- Có bao nhiêu hàm đơn điệu tăng với tập nguồn  $X_7$  và tập đích  $X_5$ ?
- Trả lời ý (a) với tập nguồn  $X_6$  và tập đích  $X_9$ ?
- Tổng quát kết quả ở ý (a) và (b).
- Tìm số hàm đơn điệu tăng  $f : X_{10} \rightarrow X_8$  trong đó  $f(4) = 4$ .
- Có bao nhiêu hàm đơn điệu tăng  $f : X_7 \rightarrow X_{12}$  thỏa mãn  $f(5) = 9$ ?
- Tổng quát kết quả ở ý (d) và (e).

**5.35.** Hàm Ackermann\*  $A(m, n)$  với  $m, n \in \mathbb{N}$  định nghĩa đệ quy bởi

$$A(0, n) = n + 1, n \geq 0$$

$$A(m, 0) = A(m - 1, 1), m > 0; \text{ và}$$

$$A(m, n) = A(m - 1, A(m, n - 1)), m, n > 0.$$

- Tìm  $A(1, 3)$  và  $A(2, 3)$ .
- Chứng minh  $\forall n \in \mathbb{N}$ ,

i)  $A(1, n) = n + 2$

ii)  $A(2, n) = 3 + 2n$

iii)  $A(3, n) = 2^{n+3} - 3$

**5.36.** Cho ma trận biểu diễn của quan hệ  $\mathcal{R}$  từ  $A$  vào  $B$ . Lập trình kiểm tra  $\mathcal{R}$  là

a) hàm

b) đơn ánh

## 5.4 Toàn ánh: số Stirling loại II

**Định nghĩa 5.13.** Hàm  $f : A \rightarrow B$  gọi là *toàn ánh* nếu  $f(A) = B$ , hay  $\forall b \in B, \exists a \in A, f(a) = b$ , tức là, mọi phần tử của  $B$  đều có tạo ảnh (trong  $A$ ).

\*Wilhem Ackermann, 1896–1962, nhà toán học, logic học Đức, học trò của David Hilbert (1862–1943). Số Ackermann được đưa ra vào 1920, có vai trò quan trọng trong khoa học máy tính –trong lý thuyết hàm đệ quy và trong phân tích thuật toán liên quan đến hợp các tập.

**Ví dụ 5.19.** a) Hàm  $f : \mathbb{R} \rightarrow \mathbb{R}$  xác định bởi  $f(x) = x^3$ , vì  $\forall r \in \mathbb{R}$  –tập đích, ta có  $\sqrt[3]{r} \in \mathbb{R}$  –tập nguồn, và  $f(\sqrt[3]{r}) = (\sqrt[3]{r})^3 = r$ .

b) Hàm  $g : \mathbb{R} \rightarrow \mathbb{R}$  với  $g(x) = x^2$  không là toàn ánh, vì miền giá trị của  $g$  không có số âm, và do đó, khác tập đích  $\mathbb{R}$ . Chẳng hạn, nếu  $-9 \in g(\mathbb{R})$ , ta phải tìm được  $r \in \mathbb{R}$  –tập đích, sao cho  $g(r) = r^2 = -9$ . Khi đó  $r = 3i$  hoặc  $r = -3i$ . Nhưng  $3i, -3i \in \mathbb{C} - \mathbb{R}$ , mâu thuẫn.

Tuy nhiên, hàm  $h : \mathbb{R} \rightarrow [0, +\infty)$  trong đó  $h(x) = x^2$  lại là toàn ánh.

**Ví dụ 5.20.** Hàm  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  với  $f(x) = 3x + 1$  không là toàn ánh vì miền giá trị  $f(\mathbb{Z}) = \{\dots, -8, -5, -2, 1, 4, 7, \dots\} \neq \mathbb{Z}$ . Chẳng hạn,  $8 \notin f(\mathbb{Z})$ , vì phương trình  $f(x) = 8$  hay  $3x + 1 = 8$  cho  $x = \frac{7}{3}$ , nhưng  $\frac{7}{3} \notin \mathbb{Z}$ .

Tuy nhiên, các hàm

1)  $g : \mathbb{Q} \rightarrow \mathbb{Q}$  trong đó  $g(x) = 3x + 1 \forall x \in \mathbb{Q}$ ; và

2)  $h : \mathbb{R} \rightarrow \mathbb{R}$  trong đó  $h(x) = 3x + 1 \forall x \in \mathbb{R}$

đều là toàn ánh. Ngoài ra,  $f, g$  và  $h$  đều là đơn ánh, vì  $3x_1 + 1 = 3x_2 + 1 \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2$  bất kể  $x_1, x_2$  là số nguyên, hữu tỷ, hay số thực.

**Ví dụ 5.21.** Cho  $A = \{1, 2, 3, 4\}$  và  $B = \{x, y, z\}$ . Khi đó

a)  $f_1 = \{(1, z), (2, y), (3, x), (4, y)\}$  và  $f_2 = \{(1, x), (2, x), (3, y), (4, z)\}$  là toàn ánh.

b)  $g = \{(1, x), (2, x), (3, y), (4, y)\}$  không là toàn ánh vì  $g(A) = \{x, y\} \subset B$ .

Biểu diễn các hàm trong **Ví dụ 5.21** dưới dạng  $f_1 = \{3\}_x \cup \{2, 4\}_y \cup \{1\}_z$ ,  $f_2 = \{1, 2\}_x \cup \{3\}_y \cup \{4\}_z$ , và  $g = \{1, 2\}_x \cup \{3, 4\}_y \cup \{\}_z$ , trong đó thành phần  $\{2, 4\}_y$  của  $f_1$  ngụ ý  $f_1$  chứa các cặp  $(2, y)$  và  $(4, y)$ ; thành phần  $\{\}_z$  của  $g$  cho biết  $g$  không có cặp nào chứa  $z$  ở thành phần thứ hai. Ta có quan sát rõ hơn về sự khác biệt giữa hàm toàn ánh với hàm không toàn ánh.

Giả sử  $A = \{a_1, a_2, \dots, a_m\}$ ,  $B = \{b_1, b_2, \dots, b_n\}$ .

- Hàm  $f : A \rightarrow B$  là toàn ánh, nếu mỗi phần tử của  $B$  xuất hiện ít nhất một lần ở thành phần thứ hai trong các cặp của  $f$ , tức là

$$\forall j = \overline{1, n}, \sum_{i=1}^m m_{ij} \geq 1. \quad (5.14)$$

- Nếu coi mỗi phần tử của  $A$  là một vật, mỗi phần tử của  $B$  là một hộp thì mỗi toàn ánh từ  $A$  vào  $B$  là một cách xếp  $m$  vật khác nhau vào  $n$  hộp khác nhau sao cho không

có hợp nào trống. Để tồn tại toàn ánh từ  $A$  vào  $B$ , phải có  $m \geq n$ . Hơn nữa, dùng nguyên lý bù trừ trong [Phần 7.1](#), có thể chỉ ra

Số toàn ánh từ tập  $A$  cỡ  $m$  vào  $B$  cỡ  $n$  là

$$\begin{aligned} \sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m &= \sum_{k=0}^{n-1} (-1)^k \binom{n}{n-k} (n-k)^m \\ &= \binom{n}{n} n^m - \binom{n}{n-1} (n-1)^m + \binom{n}{n-2} (n-2)^m - \cdots + (-1)^{n-2} \binom{n}{2} 2^m + \\ &\quad + (-1)^{n-1} \binom{n}{1} 1^m. \end{aligned} \tag{5.15}$$

**Ví dụ 5.22.** Nếu  $|B| = n = 2$ , có  $\sum_{k=0}^2 (-1)^k \binom{2}{2-k} (2-k)^m = \binom{2}{2} 2^m - \binom{2}{1} 1^m = 2^m - 2$  toàn ánh từ  $A$  vào  $B$ . Lúc này, trong  $2^m$  hàm từ  $A = \{a_1, a_2, \dots, a_m\}$  vào  $B$ , có hai hàm không phải toàn ánh là

$$f_1 = \{(a_1, b_1), (a_2, b_1), \dots, (a_m, b_1)\}, \text{ và } f_2 = \{(a_1, b_2), (a_2, b_2), \dots, (a_m, b_2)\}.$$

**Ví dụ 5.23.** Với  $A = \{1, 2, 3, 4, 5, 6, 7\}$  và  $B = \{w, x, y, z\}$ , áp dụng công thức tổng quát với  $m = 7$  và  $n = 4$ , ta có  $\sum_{k=0}^4 (-1)^k \binom{4}{4-k} (4-k)^7 = \binom{4}{4} 4^7 - \binom{4}{3} 3^7 + \binom{4}{2} 2^7 - \binom{4}{1} 1^7 = 8400$  toàn ánh từ  $A$  vào  $B$ . Kết quả này có thể dùng trong các lập luận như

- 1) Để giao 7 hợp đồng cho 4 công ty (mỗi hợp đồng chỉ giao cho một công ty, công ty nào cũng có hợp đồng), có 8400 cách.
- 2) Có 7 người vào 4 phòng. Số cách để phòng nào cũng có người là 8400. Xác suất để không có phòng trống là  $\frac{8400}{4^7} = 0.5127$ .

**Ví dụ 5.24.** Để giao 7 tài khoản, trong đó có một tài khoản quản trị, còn lại là tài khoản thường, cho nhóm 4 người (mỗi tài khoản chỉ giao cho một người, ai cũng quản lý ít nhất một tài khoản) biết trưởng nhóm luôn quản lý tài khoản quản trị, có hai trường hợp

- a) Trưởng nhóm chỉ quản lý tài khoản quản trị. Khi đó chỉ cần giao 6 tài khoản thường cho 3 người kia, với  $\sum_{k=0}^3 (-1)^k \binom{3}{3-k} (3-k)^6 = 540$  cách.
- b) Ngoài tài khoản quản trị, trưởng nhóm còn quản lý cả tài khoản thường, tức là, cần



giao 6 tài khoản thường cho cả 4 người, sao cho ai cũng quản lý tài khoản thường,

$$\text{với } \sum_{k=0}^4 (-1)^k \binom{4}{4-k} (4-k)^6 = 1560 \text{ cách.}$$

Theo quy tắc cộng, có  $540 + 1560 = 2100$  cách giao 7 tài khoản cho 4 người thỏa mãn yêu cầu trên.

**Ví dụ 5.25.** Nếu  $m < n$ , thì không có toàn ánh từ tập cỡ  $m$  vào tập cỡ  $n$ , tức là

$$\sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m = 0.$$

Với  $m \geq n$ , để xếp  $m$  vật vào  $n$  hộp khác nhau, với  $\sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m$  cách, có thể thực hiện qua hai bước:

1) Chia  $m$  vật ra  $n$  thành phần khác rỗng, có (ký hiệu)  $S(m, n)$  cách.

2) Xếp  $n$  thành phần ở bước (1) vào  $n$  hộp, có  $n!$  cách.

Theo quy tắc nhân,  $\sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m = S(m, n) \cdot n!$ . Do đó

Số cách chia  $m$  vật ra  $n$  thành phần khác rỗng là

$$S(m, n) = \frac{1}{n!} \sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m. \quad (5.16)$$

$S(m, n)$  gọi là số Stirling<sup>†</sup> loại II.

**Nhận xét:**  $S(m, n)$  cũng là số cách xếp  $m$  vật vào  $n$  hộp giống nhau, không quan tâm thứ tự các hộp, để không có hộp trống.

**Ví dụ 5.26.** Với  $A = \{a, b, c, d\}$  và  $B = \{1, 2, 3\}$ , có  $\sum_{k=0}^3 (-1)^k (3-k)^4 = 3^4 - 2^4 + 1^4 = 36$  toàn ánh từ  $A$  vào  $B$ , hay, có 36 cách xếp 4 vật khác nhau vào 3 hộp khác nhau, để không có hộp trống (và không quan tâm vị trí của các vật trong hộp). Trong 36 cách xếp này, có những nhóm gồm 6 cách xếp tương ứng với một cách chia  $A$  thành 3 phần khác rỗng, chẳng hạn, cách chia  $A = \{a, b\} \cup \{c\} \cup \{d\}$  ứng với 6 cách xếp:

<sup>†</sup> James Stirling, 1692-1770, nhà toán học Scotland

- 1)  $\{a, b\}_1 \quad \{c\}_2 \quad \{d\}_3$
- 2)  $\{a, b\}_1 \quad \{c\}_3 \quad \{d\}_2$
- 3)  $\{a, b\}_2 \quad \{c\}_1 \quad \{d\}_3$
- 4)  $\{a, b\}_2 \quad \{c\}_3 \quad \{d\}_1$
- 5)  $\{a, b\}_3 \quad \{c\}_1 \quad \{d\}_2$
- 6)  $\{a, b\}_3 \quad \{c\}_2 \quad \{d\}_1,$

trong đó  $\{c\}_2$  ngụ ý  $c$  ở trong hộp 2. Do đó nếu các hộp giống nhau, thì có  $\frac{36}{3!} = 6$  cách xếp các vật  $a, b, c, d$  vào 3 hộp này mà không có hộp trống.

**Định lý 5.3.** Với các số nguyên  $m > n > 1$ , ta có

$$S(m, n) = S(m-1, n-1) + n \cdot S(m-1, n). \quad (5.17)$$

Chứng minh. content...

□

Lược đồ, và vì thế cách lập trình, tìm số Stirling loại II gần giống với cách hệ số nhị thức theo hằng đẳng thức Pascal ở [trang 19](#).

Bảng sau liệt kê một số số Stirling loại II.

	$S(m, n)$							
$m \backslash n$	1	2	3	4	5	6	7	8
1	1							
2	1	1						
3	1	3	1					
4	1	7	6	1				
5	1	15	25	10	1			
6	1	31	90	65	15	1		
7	1	63	301	350	140	21	1	
8	1	127	966	1701	1050	266	28	1

**Ví dụ 5.27.** Với  $m \geq n$ ,  $\sum_{i=1}^n S(m, i)$  là số cách xếp  $m$  vật vào  $n$  hộp giống nhau mà có thể có hộp trống, cũng là số cách chia  $m$  vật ra không quá  $n$  phần. Từ hàng ứng với  $m = 4$  của bảng trên, có  $1 + 7 + 6 = 14$  cách chia các vật  $a, b, c, d$  thành không quá 3 phần.

**Ví dụ 5.28.** Cho số  $30\,030 = 2 \times 3 \times 5 \times 7 \times 11 \times 13$ . Phân tích số này thành tích các số nguyên lớn hơn 1, không quan tâm thứ tự, chẳng hạn

i)  $30 \times 1001 = (2 \times 3 \times 5)(7 \times 11 \times 13)$

ii)  $110 \times 273 = (2 \times 5 \times 11)(3 \times 7 \times 13)$

$$\text{iii)} \quad 2310 \times 13 = (2 \times 3 \times 5 \times 7 \times 11)(13)$$

$$\text{iv)} \quad 14 \times 33 \times 65 = (2 \times 7)(3 \times 11)(5 \times 15)$$

$$\text{v)} \quad (22 \times 35 \times 39) = (2 \times 11)(5 \times 7)(3 \times 13)$$

Các cách (i), (ii) và (iii) ứng với ba trong các cách chia sáu vật 2, 3, 5, 7, 11, 13 ra hai phần, tức là ba trong  $S(6, 2) = 31$  cách phân tích ra hai thừa số của 30 030. Tương tự, các cách (iv) và (v) là hai trong  $S(6, 3) = 90$  cách phân tích 30 030 ra ba thừa số. Như vậy, mỗi cách phân tích 30 030 thành tích các số nguyên lớn hơn 1, không quan tâm thứ tự, là một cách xếp các vật 2, 3, 5, 7, 11 và 13 thành ít nhất hai phần, và tối đa sáu phần. Do đó có  $\sum_{n=2}^6 S(6, n) = 202$  cách thực hiện việc này.

## Bài tập 5.4

**5.37.** Cho ma trận biểu diễn của quan hệ  $\mathcal{R}$  từ  $A$  vào  $B$ . Lập trình kiểm tra  $\mathcal{R}$  là toàn ánh.

## 5.5 Hàm đặc biệt

Ta đã biết phép cộng là phép toán hai ngôi đóng trên tập  $\mathbb{Z}^+$ , phép lấy đối là toán tử trên  $\mathbb{Z}$ . Trong [Phần 3.2](#),  $\cup$  và  $\cap$  là phép toán hai ngôi đóng trên  $\mathcal{P}(\mathcal{U})$  với tập phổ dụng  $\mathcal{U}$  cho trước, phép lấy phần bù là toán tử trên  $\mathcal{P}(\mathcal{U})$ . Trong phần này, ta tiếp cận các khái niệm phép toán hai ngôi đóng và toán tử theo quan điểm hàm.

**Định nghĩa 5.14.** Với hai tập  $A, B \neq \emptyset$ , hàm  $f : A \times A \rightarrow B$  gọi là phép toán (hai ngôi) trên  $A$ . Nếu  $B \subseteq A$ ,  $f$  gọi là đóng trên  $A$  hay  $A$  đóng đối với  $f$ .

**Định nghĩa 5.15.** Hàm  $g : A \rightarrow A$  gọi là toán tử trên  $A$ .

**Ví dụ 5.29.** a) Hàm  $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  xác định bởi  $f(a, b) = a - b$  là phép toán đóng trên  $\mathbb{Z}$ .

b) Cho  $g : \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}$  bởi  $g(a, b) = a - b$ . Khi đó  $g$  là phép toán trên  $\mathbb{Z}^+$ , nhưng không đóng. Chẳng hạn, với  $3, 7 \in \mathbb{Z}^+$ ,  $g(3, 7) = 3 - 7 = -4 \notin \mathbb{Z}^+$ .

c) Hàm  $h : \mathbb{R}^+ \rightarrow \mathbb{R}^+$  với  $h(a) = \frac{1}{a}$  là toán tử trên  $\mathbb{R}^+$ .

**Ví dụ 5.30.** Cho trước tập phổ dụng  $\mathcal{U}$ , và  $A, B \subseteq \mathcal{U}$ . Các hàm

- a)  $f : \mathcal{P}(\mathcal{U}) \times \mathcal{P}(\mathcal{U}) \rightarrow \mathcal{P}(\mathcal{U})$  cho bởi  $f(A, B) = A \cup B$  là phép toán đóng trên  $\mathcal{P}(\mathcal{U})$ .  
b)  $g : \mathcal{P}(\mathcal{U}) \rightarrow \mathcal{P}(\mathcal{U})$  với  $g(A) = \bar{A}$  là toán tử trên  $\mathcal{P}(\mathcal{U})$ .

**Định nghĩa 5.16.** Cho phép toán  $f : A \times A \rightarrow B$ .

- a)  $f$  gọi là giao hoán nếu  $f(a, b) = f(b, a)$ ,  $\forall a, b \in A$ .  
b) Khi  $f$  đóng ( $B \subseteq A$ ),  $f$  gọi là kết hợp nếu  $f[f(a, b), c] = f[a, f(b, c)]$ ,  $\forall a, b, c \in A$ .

**Ví dụ 5.31.** a) Định nghĩa phép toán đóng  $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  bởi  $f(a, b) = a + b - 3ab$ .  
Vì phép cộng và nhân số nguyên đều giao hoán nên

$$f(a, b) = a + b - 3ab = b + a - 3ab = f(b, a),$$

tức là  $f$  giao hoán.

Để xác định tính kết hợp của  $f$ , xét  $a, b, c \in \mathbb{Z}$  bất kỳ. Ta tính

$$\begin{aligned} f[f(a, b), c] &= f[a + b - 3ab, c] = (a + b - 3ab) + c - 3(a + b - 3ab)c \\ &= a + b + c - 3ab - 3ac - 3bc + 9abc, \text{ và} \\ f[a, f(b, c)] &= f[a, b + c - 3bc] = a + (b + c - 3bc) - 3a(b + c - 3bc) \\ &= a + b + c - 3ab - 3ac - 3bc + 9abc. \end{aligned}$$

Vậy  $f[f(a, b), c] = f[a, f(b, c)]$ ,  $\forall a, b, c \in \mathbb{Z}$ , tức là  $f$  kết hợp.

b) Xét phép toán đóng  $h : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  với  $h(a, b) = a|b|$ . Khi đó  $h(3, -2) = 3|-2| = 6$  nhưng  $h(-2, 3) = -2|3| = -6 \neq h(3, -2)$ , vì vậy  $h$  không giao hoán. Tuy nhiên,  $\forall a, b, c \in \mathbb{Z}$ , ta tính

$$\begin{aligned} h[h(a, b), c] &= h(a|b|, c) = a|b||c|, \text{ và} \\ h[a, h(b, c)] &= h(a, b|c|) = a|b|c| = a|b| \cdot |c| = a|b||c|, \end{aligned}$$

và suy ra  $h$  kết hợp.

**Ví dụ 5.32.** Cho tập  $A$  cỡ  $n$ . Khi đó  $|A \times A| = n^2$ , nên có  $n^{n^2}$  hàm  $f : A \times A \rightarrow A$ ; tức là, có  $n^{n^2}$  phép toán đóng trên  $A$ .

Mỗi phép toán đóng giao hoán  $f : A \times A \rightarrow A$ , là một cách gán giá trị trong  $A$  cho tất cả  $f(a, b)$  với  $a, b \in A$  sao cho  $f(a, b) = f(b, a)$ , gồm hai bước: (1) gán giá trị cho  $n$  biểu thức

$f(a, a)$ , với  $a \in A$ ; và (2) gán đồng thời một giá trị cho cặp biểu thức  $f(a, b)$  và  $f(b, a)$  với  $a, b \in A$  và  $a \neq b$ . Vì có  $n^2 - n$  biểu thức  $f(a, b)$  với  $a, b \in A$  và  $a \neq b$  nên có  $\frac{n^2 - n}{2}$  cặp biểu thức như vậy. Do đó, có  $n^{n+\frac{n^2-n}{2}} = n^{\frac{n(n+1)}{2}}$  phép toán đóng giao hoán trên  $A$ .

**Định nghĩa 5.17.** Cho phép toán  $f : A \times A \rightarrow B$ . Phần tử  $x \in A$  gọi là một đơn vị của  $f$  nếu  $f(a, x) = f(x, a) = a, \forall a \in A$ .

**Ví dụ 5.33.** a) Xét phép toán đóng  $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  với  $f(a, b) = a + b$ . Ở đây số nguyên 0 là đơn vị vì  $f(a, 0) = a + 0 = a$  và  $f(0, a) = 0 + a = a, \forall a \in \mathbb{Z}$ .

b) Hàm trong phần (a) của Ví dụ 5.29 không có đơn vị. Vì nếu  $f$  có một đơn vị  $x$ , thì  $\forall a \in \mathbb{Z}, f(a, x) = a \Rightarrow a - x = a \Rightarrow x = 0$ . Nhưng khi đó  $f(x, a) = f(0, a) = 0 - a = -a \neq a$  trừ khi  $a = 0$ , mâu thuẫn.

c) Cho  $A = \{1, 2, 3, 4, 5, 6, 7\}$  và  $g : A \times A \rightarrow A$  là phép toán đóng xác định bởi  $g(a, b) = \min\{a, b\}$ . Đây là phép toán giao hoán, kết hợp, và  $\forall a \in A, g(a, 7) (= g(7, a)) = \min\{a, 7\} = a$ . Vì vậy 7 là một đơn vị của  $g$ .

**Định lý 5.4.** Cho phép toán  $f : A \times A \rightarrow B$ . Nếu  $f$  có đơn vị, thì đơn vị đó là duy nhất.

**Ví dụ 5.34.** Cho tập  $A$  cỡ  $n, x \in A$  cố định. Ta xác định số phép toán  $f$  đóng trên  $A$  và có đơn vị  $x$ . Giả sử phép toán  $f$  trên  $A$  có đơn vị  $x$ , hay  $f(a, x) = f(x, a) = a, \forall a \in A$ , tức là mỗi  $f(a, x)$  và  $f(x, a)$  chỉ có một cách gán trị. Để  $f$  đóng, tức là  $f : A \times A \rightarrow A$ , cần gán giá trị trong  $A$  cho mỗi  $f(b, c), b, c \in A - \{x\}$ . Vì có  $(n - 1)^2$  biểu thức cần gán giá trị nên có  $n^{(n-1)^2}$  phép toán đóng trên  $A$  nhận  $x$  là đơn vị.

Cách lập luận này khá giống Ví dụ 5.32. Theo đó, số phép toán đóng trên  $A$ , giao hoán, có đơn vị  $x$  là  $n^{\frac{n(n-1)}{2}}$ .

Từ Định lý 5.4, có  $n$  cách chọn đơn vị có vai trò giống  $x$ . Do đó có  $n \cdot n^{(n-1)^2}$  phép toán đóng, có đơn vị trên  $A$ ; và có  $n \cdot n^{\frac{n(n-1)}{2}}$  phép toán đóng, giao hoán, có đơn vị trên  $A$ .

**Định nghĩa 5.18.** Cho hai tập  $A, B$  và xét  $D \subseteq A \times B$ . Hàm  $\pi_A : D \rightarrow A$  xác định bởi  $\pi_A(a, b) = a$  gọi là phép chiếu lên tọa độ thứ nhất. Hàm  $\pi_B : D \rightarrow B$  cho bởi  $\pi_B(a, b) = b$  là phép chiếu lên tọa độ thứ hai.

Nếu  $D = A \times B$  thì  $\pi_A, \pi_B$  là toàn ánh.



**Ví dụ 5.35.** Cho  $A = \{w, x, y\}$  và  $B = \{1, 2, 3, 4\}$ , đặt  $D = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 4)\}$ . Với phép chiếu  $\pi_A : D \rightarrow A$ , ta có  $\pi(x, 1) = x = \pi_A(x, 2) = \pi_A(x, 3)$  và  $\pi_A(y, 1) = \pi_A(y, 4) = y$ . Vì  $\pi_A(D) = \{x, y\} \subset A$  nên  $\pi_A$  không là toàn ánh.

Với  $\pi_B : D \rightarrow B$ , ta có  $\pi_B(x, 1) = \pi_B(y, 1) = 1$ ,  $\pi_B(x, 2) = 2$ ,  $\pi_B(x, 3) = 3$ , và  $\pi_B(y, 4) = 4$ . Vì vậy  $\pi_B(D) = B$ , nên phép chiếu này là toàn ánh.

**Ví dụ 5.36.** Cho  $A = B = \mathbb{R}$ , xét  $D \subseteq A \times B$  xác định bởi  $D = \{(x, y) \mid y = x^2\}$ . Ta thấy  $(3, 9) \in D$  và  $\pi_A(3, 9) = 3$  là hoành độ,  $\pi_B(3, 9) = 9$  là tung độ của  $(3, 9)$ . Vì  $\pi_A(D) = \mathbb{R} = A$  nên  $\pi_A$  là toàn ánh. Tuy nhiên,  $\pi_B(D) = [0, +\infty) \subset \mathbb{R}$ , nên  $\pi_B$  không là toàn ánh. Thêm nữa,  $\pi_A$  là đơn ánh và  $\pi_B$  không là đơn ánh.

Tổng quát, cho các tập  $A_1, A_2, \dots, A_n$ , và bộ chỉ số  $\{i_1, i_2, \dots, i_m\} \subseteq \{1, 2, \dots, n\}$  với  $i_1 < i_2 < \dots < i_m$ ,  $m \leq n$ . Xét  $D \subseteq A_1 \times A_2 \times \dots \times A_n$ . Hàm  $\pi : D \rightarrow A_{i_1} \times A_{i_2} \times \dots \times A_{i_m}$  xác định bởi  $\pi(a_1, a_2, \dots, a_n) = (a_{i_1}, a_{i_2}, \dots, a_{i_m})$  là phép chiếu của  $D$  lên các tọa độ thứ  $i_1, i_2, \dots, i_m$ .

Các phép chiếu này xuất hiện một cách tự nhiên trong nghiên cứu *cơ sở dữ liệu quan hệ*, một kỹ thuật tiêu chuẩn để tổ chức (thêm, bớt, chỉnh sửa, sắp xếp, tìm kiếm) và mô tả một lượng lớn dữ liệu bằng hệ thống tính toán quy mô lớn hiện đại.

**Ví dụ 5.37.** Tại một trường đại học, các tập sau hình thành trong quá trình phân công chuyên môn

- $A_1$  = tập các mã học phần
- $A_2$  = tập các tên môn học, tương ứng với mã học phần
- $A_3$  = tập các chữ cái, chỉ các phần trong học phần
- $A_4$  = tập các giảng viên, giảng dạy một phần trong học phần.

Quan hệ bốn ngôi  $D \subseteq A_1 \times A_2 \times A_3 \times A_4$  được cho trong bảng:

Mã học phần	Tên học phần	Phần giảng dạy	Giảng viên
MA 111	Giải tích I	A	P. Z. Chinn
MA 111	Giải tích I	B	V. Larney
MA 112	Giải tích II	A	J. Kinney
MA 112	Giải tích II	B	A. Schmidt
MA 112	Giải tích II	C	R. Mines
MA 113	Giải tích III	A	J. Kinney

Bảng 5.1

Các tập  $A_1, A_2, A_3, A_4$  gọi là các miền xác định của cơ sở dữ liệu quan hệ, và bảng  $D$  gọi là có *bậc* 4. Mỗi phần tử của  $D$  tương ứng với một hàng của bảng trên, gọi là một *danh sách*. Hình chiếu của  $D$  lên  $A_1 \times A_3 \times A_4$  và lên  $A_1 \times A_2$  được mô tả trong [Bảng 5.2](#) và [5.3](#).

Mã học phần	Phần giảng dạy	Giảng viên
MA 111	A	P. Z. Chinn
MA 111	B	V. Larney
MA 112	A	J. Kinney
MA 112	B	A. Schmidt
MA 112	C	R. Mines
MA 113	A	J. Kinney

Bảng 5.2

Mã học phần	Tên học phần
MA 111	Giải tích I
MA 112	Giải tích II
MA 113	Giải tích III

Bảng 5.3

[Bảng 5.2](#) và [5.3](#) là cách biểu diễn khác của cùng một dữ liệu mô tả trong bảng [Bảng 5.1](#). Nếu có [Bảng 5.2](#) và [5.3](#), ta có thể xây dựng lại được [Bảng 5.1](#).

Lý thuyết về cơ sở dữ liệu quan hệ liên quan đến việc biểu diễn dữ liệu theo những cách khác nhau thông qua các phép toán, chẳng hạn như phép chiếu.

### 5.6 Nguyên lý chuồng bồ câu

Xét bài toán xếp  $m$  vật vào  $n$  hộp.

a) Với  $m > n$ , có hộp chứa ít nhất 2 vật.

b) Tổng quát, có hộp chứa ít nhất  $\left\lceil \frac{m}{n} \right\rceil$  vật.

*Chứng minh.* Ta chứng minh trường hợp tổng quát bằng phương pháp phản chứng. Giả sử kết luận không đúng, tức là hộp nào cũng nhỏ hơn  $\left\lceil \frac{m}{n} \right\rceil$  vật, hay không quá  $\left\lceil \frac{m}{n} \right\rceil$  vật. Mặt khác  $\left\lceil \frac{m}{n} \right\rceil - 1 < \frac{m}{n}$  nên số vật trong  $n$  hộp nhỏ hơn  $n \times \frac{m}{n} = m$  vật, mâu thuẫn!  $\square$

**Ví dụ 5.38.** Trong 13 người có ít nhất hai người cùng tháng sinh.

*Giải.* Xếp 13 vật (người) vào 12 hộp (tháng sinh) thì có hộp chứa ít nhất hai vật, tức là có ít nhất hai người cùng tháng sinh.  $\square$

**Ví dụ 5.39.** Trong túi có 12 đôi tất khác màu nhau. Cần lấy trong túi ít nhất bao nhiêu chiếc tất để luôn có được một đôi?

*Giải.* Gọi  $m$  số chiếc tất cần lấy. Xếp  $m$  vật (chiếc tất) vào 12 hộp (màu tất). Để lấy được một đôi, hay có (ít nhất hoặc đúng) hai chiếc cùng màu, tức là có hộp chứa ít nhất hai vật, cần  $m > 12$ . Số tất cần lấy ít nhất là 13.  $\square$

**Ví dụ 5.40.** Một văn bản có 500 000 từ, mỗi từ không quá 4 ký tự và chỉ gồm chữ cái thường thì có từ bị lặp lại.

*Giải.* Từ điển không quá 4 ký tự và chỉ gồm chữ cái thường có số từ  $26^4 + 26^3 + 26^2 + 26 = 475\,254 < 500\,000$ . Xếp 500 000 vật (từ trong văn bản) vào 475 254 hộp (từ trong từ điển), có hộp chứa ít nhất hai vật, tức là có từ bị lặp lại.  $\square$

**Ví dụ 5.41.** Cho  $n \in \mathbb{Z}^+$ . Trong  $n + 1$  số nguyên có hai số có cùng số dư khi chia cho  $n$ .

*Giải.*  $\forall a \in \mathbb{Z}, \exists! q, r \in \mathbb{Z} (0 \leq r < n), a = qn + r$ . Xếp  $a$  (vật) vào nhóm  $r$  (hộp). Xếp  $n + 1$  vật vào  $n$  hộp, có hộp chứa ít nhất hai vật, tức là có hai số cùng phần dư khi chia cho  $n$ .  $\square$

**Ví dụ 5.42.** Trong  $n + 1$  số nguyên từ 1 tới  $2n$  có hai số mà số này là bội của số kia.

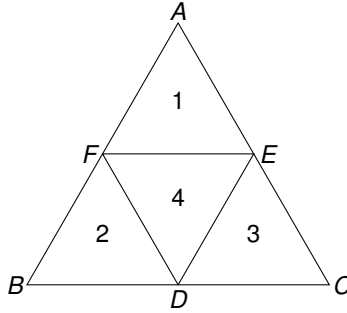
*Giải.* Mỗi  $x \in \{1, 2, \dots, 2n\}$  có dạng  $x = 2^k y$  với  $k, y \in \mathbb{Z}, k \geq 0, y > 0$  và  $\gcd(2, y) = 1$ . Vì thế  $y$  lẻ, cho nên  $y \in \{1, 3, 5, \dots, 2n - 1\} = C$  với  $|C| = n$ . Xếp  $x$  (vật) vào nhóm  $y$  (hộp). Xếp  $n + 1$  vật vào  $n$  hộp thì có hộp  $y$  nào đó chứa ít nhất hai vật  $a, b$ , tức là  $a = 2^k y, b = 2^m y$ . Nếu  $k < m$  thì  $a \mid b$ ; ngược lại,  $k > m$ , thì  $b \mid a$ .  $\square$

**Ví dụ 5.43.** Mọi tập con cỡ 6 của tập  $S = \{1, 2, 3, \dots, 9\}$  luôn có hai số có tổng bằng 10.

*Giải.* Xét các tập con  $\{1, 9\}, \{2, 8\}, \{3, 7\}, \{4, 6\}, \{5\}$ . Mỗi  $x \in S$  (vật) gán vào tập chứa  $x$  (hộp). Xếp 6 vật vào 5 hộp, có hộp chứa hai vật, tức là hai số đó có tổng bằng 10.  $\square$



**Ví dụ 5.44.** Chọn 5 điểm thuộc miền trong tam giác đều có cạnh độ dài 1 thì có ít nhất hai điểm có khoảng cách nhỏ hơn  $\frac{1}{2}$ .



*Giải.* Xét  $\triangle ABC$  đều,  $AB = 1$ .  $D, E, F$  là trung điểm của  $BC, CA, AB$ . Các tam giác  $AEF, BDF, CDE, DEF$  đều có cạnh bằng  $\frac{1}{2}$ .

$R_1, R_2, R_3$  là miền trong tam giác  $AEF, BDF, CDE$ ;  $R_4$  là tam giác  $DEF$  ngoại trừ ba đỉnh.

Trong 5 đỉnh, có ít nhất hai đỉnh cùng thuộc  $R_i$ , khoảng cách giữa chúng nhỏ hơn  $\frac{1}{2}$ .  $\square$

**Ví dụ 5.45.** Cho  $S \subset \mathbb{Z}^+, |S| = 6, \max S \leq 14$ . Chứng minh có hai tập con khác rỗng của  $S$  mà tổng các phần tử của chúng bằng nhau.

*Giải.* Với  $A \subseteq S, A \neq \emptyset$ , ký hiệu  $s_A$  là tổng các số trong  $A$ . Ta có  $1 \leq s_A \leq 14 + 13 + \dots + 9 = 69$ . Xếp  $A$  (vật) vào nhóm  $s_A$  (hộp). Số tập  $A$  như vậy là  $2^6 - 1 = 63$ . Bài toán xếp 63 vật vào 69 hộp không cho kết luận như ý.

Ta thấy  $S$  chỉ có 1 tập con có 6 phần tử (1 vật), trong khi các trường hợp để tổng của 6 phần tử không trùng với tổng của không quá 5 phần tử bao gồm  $(14 + 13 + \dots + 10) + i$  với  $i = \overline{1, 9}$ , gồm 9 trường hợp (9 hộp, nhiều hơn hẳn số vật).

Vì vậy, trong các tập con khác rỗng của  $S$ , xét các tập  $A$  có  $|A| \leq 5$ . Khi đó  $1 \leq s_A \leq 14 + 13 + \dots + 10 = 60$ , và số tập  $A$  như vậy là  $2^6 - 2 = 62$ . Xếp 62 tập vào 60 nhóm thì có nhóm chứa ít nhất hai tập, với tổng các phần tử bằng nhau.  $\square$

**Ví dụ 5.46.** Cho  $m \in \mathbb{Z}^+$  lẻ. Khi đó  $\exists n \in \mathbb{Z}^+, m \mid (2^n - 1)$ .

*Giải.* Xét  $m + 1$  số nguyên  $2^0 - 1, 2^1 - 1, \dots, 2^m - 1$ . Mỗi số này (vật) được xếp vào nhóm phần dư khi chia cho  $m$  (hộp). Vì số hộp là  $m$  nên có hộp  $r$  chứa ít nhất hai vật  $2^s - 1 = mq_1 + r, 2^t - 1 = mq_2 + r$  với  $0 \leq s < t, q_1, q_2 \in \mathbb{Z}$ . Vì thế  $(2^t - 1) - (2^s - 1) = (mq_2 + r) - (mq_1 + r)$ , hay  $2^s(2^{t-s} - 1) = m(q_2 - q_1)$ , nên  $m \mid 2^s(2^{t-s} - 1)$ . Mặt khác, vì  $m$  lẻ nên  $\gcd(2^s, m) = 1$ . Do đó  $m \mid (2^{t-s} - 1)$  với  $n = t - s > 0$ .  $\square$

**Ví dụ 5.47.** Một người chơi quần vợt liên tục trong bốn tuần, ngày nào cũng chơi ít nhất một set nhưng không quá 40 set suốt thời gian này. Chứng minh có một số ngày liên tiếp mà người đó chơi đúng 15 set.

*Giải.* Gọi  $x_i$  là số set người đó chơi trong  $i$  ngày đầu,  $i = \overline{1, 28}$ . Khi đó  $1 \leq x_1 < x_2 < \dots < x_{28} \leq 40$  và  $x_1 + 15 < x_2 + 15 < \dots < x_{28} + 15 \leq 55$ . Ta có 28 số phân biệt  $x_1, x_2, \dots, x_{28}$  và 28 số phân biệt  $x_1 + 15, x_2 + 15, \dots, x_{28} + 15$ , gồm 56 số, chỉ nhận 55 giá trị, nên có hai số bằng nhau, tức là  $\exists 1 \leq j < i \leq 28$  sao cho  $x_i = x_j + 15$  hay  $x_i - x_j = 15$ . Vậy trong các ngày liên tiếp  $j + 1, j + 2, \dots, i$  người đó chơi 15 set.  $\square$

**Ví dụ 5.48.** (Paul Erdős, George Szekeres, 1935) Cho  $n \in \mathbb{Z}^+$ . Khi đó dãy  $n^2 + 1$  số thực phân biệt luôn có dãy con đơn điệu độ dài  $n + 1$ .

*Giải.* Chẳng hạn, dãy 6, 5, 8, 3, 7 (độ dài 5) có dãy con giảm 6, 5, 3 (độ dài 3); dãy 11, 8, 7, 1, 9, 6, 5, 10, 3, 12 (độ dài 10) có dãy con tăng 8, 9, 10, 12 (độ dài 4).

Xét dãy  $n^2 + 1$  số thực phân biệt  $a_1, a_2, \dots, a_{n^2+1}$ . Đặt, với  $1 \leq k \leq n^2 + 1$ :

$x_k$  = độ dài lớn nhất của dãy con giảm kết thúc tại  $a_k$ , và

$y_k$  = độ dài lớn nhất của dãy con tăng kết thúc tại  $a_k$

Chẳng hạn

$k$	1	2	3	4	5	6	7	8	9	10
$a_k$	11	8	7	1	9	6	5	10	3	12
$x_k$	1	2	3	4	2	4	5	2	6	1
$y_k$	1	1	1	1	2	2	2	3	2	4

Nếu không có dãy đơn điệu độ dài  $n + 1$  thì  $1 \leq x_k, y_k \leq n, \forall 1 \leq k \leq n^2 + 1$ . Như vậy, có không quá  $n^2$  giá trị của  $(x_k, y_k)$ . Nhưng có  $n^2 + 1$  cặp  $(x_k, y_k)$  nên có hai cặp  $(x_i, y_i) = (x_j, y_j)$  với  $i < j$ . Dãy  $a_1, a_2, \dots, a_{n^2+1}$  phân biệt, nên nếu  $a_i < a_j$  thì  $y_i < y_j$ , ngược lại,  $a_i > a_j$  thì  $x_i > x_j$ , dẫn đến mâu thuẫn  $(x_i, y_i) \neq (x_j, y_j)$ . Vậy  $x_k = n + 1$  hoặc  $y_k = n + 1$  với  $k$  nào đó.  $\square$

## 5.7 Hàm hợp và hàm ngược

**Định nghĩa 5.19.** Hàm  $f : A \rightarrow B$  gọi là song ánh, nếu  $f$  vừa là đơn ánh, vừa là toàn ánh.

**Ví dụ 5.49.** Với  $A = \{1, 2, 3, 4\}$  và  $B = \{w, x, y, z\}$ , thì  $f = \{(1, w), (2, x), (3, y), (4, z)\}$  là song ánh từ  $A$  vào  $B$ , và  $g = \{(w, 1), (x, 2), (y, 3), (z, 4)\}$  là song ánh từ  $B$  vào  $A$ .

**Định nghĩa 5.20.** Hàm  $1_A : A \rightarrow A$  xác định bởi  $1_A(a) = a, \forall a \in A$ , gọi là hàm đồng nhất trên  $A$ .

**Định nghĩa 5.21.** Hai hàm  $f, g : A \rightarrow B$  gọi là bằng nhau, ký hiệu  $f = g$ , nếu  $f(a) = g(a), \forall a \in A$ .

Hai hàm bằng nhau trước hết, ngoài việc có cùng tập nguồn và cách xác định ảnh, phải có cùng tập đích.



**Ví dụ 5.50.** Cho  $f : \mathbb{Z} \rightarrow \mathbb{Z}, g : \mathbb{Z} \rightarrow \mathbb{Q}$  trong đó  $f(x) = x = g(x), \forall x \in \mathbb{Z}$ , nhưng  $f \neq g$ . Mặc dù có cùng tập nguồn và cách xác định ảnh, nhưng  $f \neq g$ , chẳng hạn,  $f$  là song ánh,  $g$  là đơn ánh nhưng không là toàn ánh.

**Ví dụ 5.51.** Xét hai hàm  $f, g : \mathbb{R} \rightarrow \mathbb{Z}$  với  $f(x) = \begin{cases} x, & \text{nếu } x \in \mathbb{Z} \\ \lfloor x \rfloor + 1, & \text{nếu } x \in \mathbb{R} - \mathbb{Z} \end{cases}$  và  $g(x) = \lceil x \rceil, \forall x \in \mathbb{R}$ .

Nếu  $x \in \mathbb{Z}$  thì  $g(x) = \lceil x \rceil = x = f(x)$ .

Với  $x \in \mathbb{R} - \mathbb{Z}$ , ta có  $\lfloor x \rfloor < x < \lfloor x \rfloor + 1$ , nên  $g(x) = \lceil x \rceil = \lfloor x \rfloor + 1 = f(x)$ .

Do đó,  $f = g$ , mặc dù chúng có công thức khác nhau.

**Định nghĩa 5.22.** Cho  $f : A \rightarrow B$  và  $g : B \rightarrow C$ . Hàm hợp  $g \circ f : A \rightarrow C$  xác định bởi  $(g \circ f)(a) = g[f(a)], \forall a \in A$ .

**Ví dụ 5.52.** Cho  $A = \{1, 2, 3, 4\}, B = \{a, b, c\}$  và  $C = \{w, x, y, z\}$ . Hàm  $f : A \rightarrow B$  và  $g : B \rightarrow C$  cho bởi  $f = \{(1, a), (2, a), (3, b), (4, c)\}$  và  $g = \{(a, x), (b, y), (c, z)\}$ . Với mỗi phần tử của  $A$  ta có

$$\begin{aligned} (g \circ f)(1) &= g[f(1)] = g(a) = x & (g \circ f)(3) &= g[f(3)] = g(b) = y \\ (g \circ f)(2) &= g[f(2)] = g(a) = x & (g \circ f)(4) &= g[f(4)] = g(c) = z \end{aligned}$$

Vậy  $g \circ f = \{(1, x), (2, x), (3, y), (4, z)\}$ .

$f \circ g$  không được định nghĩa.



**Ví dụ 5.53.** Cho  $f : \mathbb{R} \rightarrow \mathbb{R}$ ,  $g : \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(x) = x^2$ ,  $g(x) = x + 5$ . Khi đó

$$(g \circ f)(x) = g[f(x)] = g(x^2) = x^2 + 5$$

$$(f \circ g)(x) = f[g(x)] = f(x + 5) = (x + 5)^2.$$

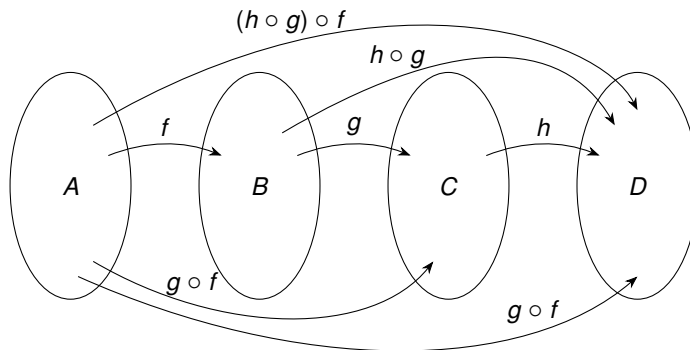
Như vậy,  $g \circ f : \mathbb{R} \rightarrow \mathbb{R}$  và  $f \circ g : \mathbb{R} \rightarrow \mathbb{R}$  đều xác định, nhưng  $g \circ f \neq f \circ g$ , chẳng hạn  $(g \circ f)(1) = 6 \neq (f \circ g)(1) = 36$ .

**Ví dụ 5.54.** Với  $f : A \rightarrow B$  thì  $f \circ 1_A = f = 1_B \circ f$ .

**Định lý 5.5.** Cho  $f : A \rightarrow B$  và  $g : B \rightarrow C$ .

- a) Nếu  $f$  và  $g$  là đơn ánh, thì  $g \circ f$  là đơn ánh.
- b) Nếu  $f$  và  $g$  là toàn ánh, thì  $g \circ f$  là toàn ánh.

**Định lý 5.6.** Nếu  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  và  $h : C \rightarrow D$ , thì  $(h \circ g) \circ f = h \circ (g \circ f)$ , tức là, phép hợp thành có tính kết hợp.



Nhờ tính kết hợp, ta có thể viết  $h \circ g \circ f$ ,  $(h \circ g) \circ f$  hoặc  $h \circ (g \circ f)$  mà không lo nhầm lẫn.

**Định nghĩa 5.23.** Cho  $f : A \rightarrow A$ . Định nghĩa lũy thừa của  $f$ :

- 1)  $f^1 = f$ , và
- 2)  $f^{n+1} = f \circ f^n$ ,  $\forall n \in \mathbb{Z}^+$ .

**Ví dụ 5.55.** Cho  $A = \{1, 2, 3, 4\}$  và  $f : A \rightarrow A$  với  $f = \{(1, 2), (2, 2), (3, 1), (4, 3)\}$ . Ta có

$$f^2 = f \circ f = \{(1, 2), (2, 2), (3, 2), (4, 1)\}$$

$$f^3 = f \circ f^2 = \{(1, 2), (2, 2), (3, 2), (4, 2)\}.$$

**Định nghĩa 5.24.** Cho quan hệ  $\mathcal{R}$  từ  $A$  vào  $B$ . Quan hệ đảo của  $\mathcal{R}$ , ký hiệu  $\mathcal{R}^c$ , là quan hệ từ  $B$  vào  $A$ , xác định bởi  $\mathcal{R}^c = \{(b, a) \mid (a, b) \in \mathcal{R}\}$  – thu được bằng cách đổi chỗ hai thành phần trong mỗi cặp của  $\mathcal{R}$ .

Nếu  $A = \{1, 2, 3, 4\}$  và  $B = \{w, x, y\}$ , và  $\mathcal{R} = \{(1, w), (2, w), (3, x)\}$  thì  $\mathcal{R}^c = \{(w, 1), (w, 2), (x, 3)\}$ .

Vì mỗi hàm là một quan hệ, ta cũng có quan hệ đảo của hàm. Xét hàm  $f : A \rightarrow B$  với  $f = \{(1, w), (2, x), (3, y), (4, x)\}$ . Khi đó  $f^c = \{(w, 1), (x, 2), (y, 3), (x, 4)\}$  là quan hệ từ  $B$  vào  $A$ , nhưng không là hàm. Vậy khi nào quan hệ đảo của hàm cũng là hàm?

**Ví dụ 5.56.** Với  $A = \{1, 2, 3\}$  và  $B = \{w, x, y\}$ , cho  $f : A \rightarrow B$  bởi  $f = \{(1, w), (2, x), (3, y)\}$ . Khi đó  $f^c = \{(w, 1), (x, 2), (y, 3)\}$  là hàm từ  $B$  vào  $A$ . Ta thấy, và  $f^c \circ f = 1_A$ ,  $f \circ f^c = 1_B$ .

**Định nghĩa 5.25.** Hàm  $f : A \rightarrow B$  gọi là khả nghịch nếu có hàm  $g : B \rightarrow A$  sao cho  $g \circ f = 1_A$  và  $f \circ g = 1_B$ .

**Ví dụ 5.57.** Cho  $f, g : \mathbb{R} \rightarrow \mathbb{R}$  xác định bởi  $f(x) = 2x + 5$ ,  $g(x) = \frac{x - 5}{2}$ . Khi đó

$$(g \circ f)(x) = g[f(x)] = g(2x + 5) = \frac{(2x + 5) - 5}{2} = x \Rightarrow g \circ f = 1_{\mathbb{R}}, \text{ và}$$

$$(f \circ g)(x) = f[g(x)] = f\left(\frac{x - 5}{2}\right) = 2 \cdot \frac{x - 5}{2} + 5 = x \Rightarrow f \circ g = 1_{\mathbb{R}}.$$

Như vậy, các hàm  $f, g$  đều khả nghịch.

**Định lý 5.7.** Nếu  $f : A \rightarrow B$  khả nghịch, thì hàm  $g : B \rightarrow A$  thỏa mãn  $g \circ f = 1_A$  và  $f \circ g = 1_B$  là duy nhất.

Hàm  $g$  duy nhất này gọi là hàm ngược của  $f$ , ký hiệu  $g = f^{-1}$ . Định lý 5.7 cũng cho ta  $f^{-1} = f^c$ .

Nếu  $f$  khả nghịch thì  $f^{-1}$  cũng khả nghịch, và  $(f^{-1})^{-1} = f$ , vẫn do tính duy nhất của hàm ngược trong Định lý 5.7.

**Định lý 5.8.** Hàm  $f : A \rightarrow B$  khả nghịch khi và chỉ khi nó là song ánh.

**Ví dụ 5.58.** Hàm  $f_1 : \mathbb{R} \rightarrow \mathbb{R}$  xác định bởi  $f_1(x) = x^2$  không khả nghịch (không là đơn ánh cũng như toàn ánh), nhưng hàm  $f_2 : [0, +\infty) \rightarrow [0, +\infty)$  với  $f_2(x) = x^2$  khả nghịch và  $f_2^{-1}(x) = \sqrt{x}$ .

**Định lý 5.9.** Nếu  $f : A \rightarrow B, g : B \rightarrow C$  khả nghịch thì  $g \circ f : A \rightarrow C$  khả nghịch và  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

**Ví dụ 5.59.** Hàm  $f : \mathbb{R} \rightarrow \mathbb{R}$  xác định bởi  $f = \{(x, y) \mid y = ax + b\}$  với  $a, b \in \mathbb{R}, a \neq 0$ , khả nghịch vì nó vừa là đơn ánh, vừa là toàn ánh. Khi đó

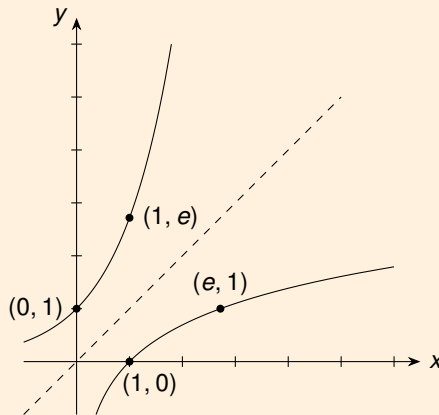
$$\begin{aligned} f^{-1} &= f^c = \{(x, y) \mid y = ax + b\}^c = \{(y, x) \mid y = ax + b\} \\ &= \{(x, y) \mid x = ay + b\} \text{ (đổi biến)} \\ &= \{(x, y) \mid y = \frac{x-b}{a}\} \end{aligned}$$

Vậy  $f$  có hàm ngược  $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$  với  $f^{-1}(x) = \frac{x-b}{a}$ .

**Ví dụ 5.60.** Cho  $f : \mathbb{R} \rightarrow \mathbb{R}^+$  xác định bởi  $f(x) = e^x$ , với đồ thị trong [Hình 5.1](#).  $f$  là song ánh, nên  $\exists f^{-1} : \mathbb{R}^+ \rightarrow \mathbb{R}$  và

$$f^{-1} = f^c = \{(x, y) \mid y = e^x\}^c = \{(y, x) \mid y = e^x\} = \{(x, y) \mid x = e^y\} = \{(x, y) \mid y = \ln x\},$$

tức là  $f^{-1}(x) = \ln x$ .



Hình 5.1

Trong mọi trường hợp, đồ thị của  $f$  và  $f^{-1}$  đối xứng nhau qua đường thẳng  $y = x$ . Chẳng hạn, trong [\(5.1\)](#), đường thẳng  $y = x$  là đường trung trực của đoạn thẳng nối hai điểm  $(1, e)$  và  $(e, 1)$ , và tương tự, của đoạn nối hai điểm  $(x, f(x))$  và  $f(x), f^{-1}[f(x)]$ .

Ta cũng có các công thức:

$$x = 1_{\mathbb{R}}(x) = (f^{-1} \circ f)(x) = \ln(e^x), \quad \forall x \in \mathbb{R}$$

$$x = 1_{\mathbb{R}^+}(x) = (f \circ f^{-1})(x) = e^{\ln x}, \quad \forall x > 0.$$

Khi  $f : A \rightarrow B$  khả nghịch, thì với  $B_1 \subseteq B$ , tập  $f^{-1}(B_1) = \{f^{-1}(b) \mid b \in B_1\} = \{a \in A \mid f(a) \in B_1\}$ . Ngay cả khi hàm  $f$  không khả nghịch, ta vẫn sử dụng ký hiệu  $f^{-1}(B_1)$  như sau:

**Định nghĩa 5.26.** Cho  $f : A \rightarrow B$  và  $B_1 \subseteq B$ . Tạo ảnh của  $B_1$  bởi  $f$ :

$$f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}.$$

Tập  $f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}$  được ký hiệu  $f^{-1}(b)$ .

**Ví dụ 5.61.** Cho  $A = \{1, 2, 3, 4, 5, 6\}$  và  $B = \{7, 8, 9, 10\}$ . Nếu  $f = \{(1, 7), (2, 7), (3, 8), (4, 6), (5, 9), (6, 9)\}$ , thì

- Với  $B_1 = \{6, 8\} \subseteq B$ , ta có  $f^{-1}(B_1) = \{3, 4\}$ , vì  $f(3) = 8$ ,  $f(4) = 6$  và  $\forall a \in A - \{3, 4\}$ ,  $f(a) \notin B_1$ . Ở đây  $|f^{-1}(B_1)| = 2 = |B_1|$ .
- Với  $B_2 = \{8, 9\} \subseteq B$ , ta có  $f^{-1}(B_2) = \{3, 5, 6\}$ , vì chỉ có  $f(3) = 8$  và  $f(5) = 9 = f(6)$ . Lúc này  $|f^{-1}(B_2)| = 3 > 2 = |B_2|$ .
- Xét  $B_3 = \{8, 9, 10\} \subseteq B$ . Vì chỉ có  $f(3) = 8$ ,  $f(5) = f(6) = 9$  và  $\nexists a \in A$ ,  $f(a) = 10$ , nên  $f^{-1}(B_3) = \{3, 5, 6\} = f^{-1}(B_2)$ , mặc dù  $B_3 \supset B_2$ .
- Với  $B_4 = \{8, 10\}$ , ta có  $f^{-1}(B_4) = \{3\}$ . Lúc này  $|f^{-1}(B_4)| = 1 < 2 = |B_4|$ .
- $f^{-1}(6) = \{4\}$ ,  $f^{-1}(7) = \{1, 2\}$ ,  $f^{-1}(8) = \{3\}$ ,  $f^{-1}(9) = \{5, 6\}$ , và  $f^{-1}(10) = \emptyset$ .

**Ví dụ 5.62.** Cho  $f : \mathbb{R} \rightarrow \mathbb{R}$  xác định bởi  $f(x) = \begin{cases} 3x - 5, & x > 0 \\ -3x + 1, & x \leq 0. \end{cases}$

- Xác định  $f(0)$ ,  $f(1)$ ,  $f(-1)$ ,  $f(\frac{5}{3})$ , và  $f(-\frac{5}{3})$ .
- Tìm  $f^{-1}(0)$ ,  $f^{-1}(1)$ ,  $f^{-1}(-1)$ ,  $f^{-1}(3)$ ,  $f^{-1}(-3)$ , và  $f^{-1}(-6)$ .
- Tính  $f^{-1}([-5, 5])$  và  $f^{-1}([-6, 5])$ .

a)

$$f(0) = -3 \cdot 0 + 1 = 1$$

$$f(1) = 3 \cdot 1 - 5 = -2$$

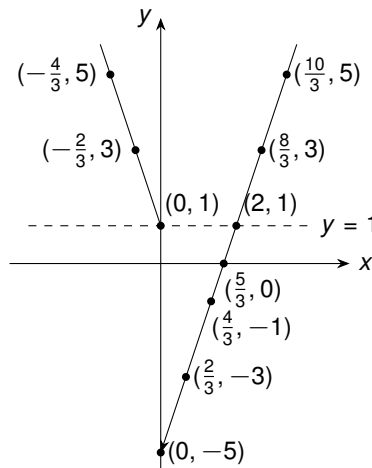
$$f(-1) = -3(-1) + 1 = 4$$

$$f\left(\frac{5}{3}\right) - 5 = 3 \cdot \frac{5}{3} - 5 = 0$$

$$f\left(-\frac{5}{3}\right) = -3\left(-\frac{5}{3}\right) + 1 = 6$$

$$\begin{aligned} \text{b) } f^{-1}(0) &= \{x \in \mathbb{R} \mid f(x) = 0\} \\ &= \{x \in \mathbb{R} \mid x > 0 \text{ và } 3x - 5 = 0\} \cup \{x \in \mathbb{R} \mid x \leq 0 \text{ và } -3x + 1 = 0\} \\ &= \{x \in \mathbb{R} \mid x > 0 \text{ và } x = \frac{5}{3}\} \cup \{x \in \mathbb{R} \mid x \leq 0 \text{ và } x = \frac{1}{3}\} \\ &= \left\{\frac{5}{3}\right\} \cup \emptyset = \left\{\frac{5}{3}\right\} \end{aligned}$$

[Đường thẳng  $y = 0$ , tức là trục hoành, chỉ cắt đồ thị hàm số, trong Hình 5.2 tại điểm  $\left(\frac{5}{3}, 0\right)$ .]



Hình 5.2

$$\begin{aligned} f^{-1}(1) &= \{x \in \mathbb{R} \mid f(x) = 1\} \\ &= \{x \in \mathbb{R} \mid x > 0 \text{ và } 3x - 5 = 1\} \cup \{x \in \mathbb{R} \mid x \leq 0 \text{ và } -3x + 1 = 1\} \\ &= \{x \in \mathbb{R} \mid x > 0 \text{ và } x = 2\} \cup \{x \in \mathbb{R} \mid x \leq 0 \text{ và } x = 0\} \\ &= \{2\} \cup \{0\} = \{0, 2\} \end{aligned}$$

[Đường thẳng  $y = 1$  cắt đồ thị hàm số tại hai điểm  $(0, 1)$  và  $(2, 1)$ .]

$$\text{Tương tự } f^{-1}(-1) = \left\{-\frac{4}{3}\right\}, f^{-1}(3) = \left\{-\frac{2}{3}, \frac{8}{3}\right\}, f^{-1}(-3) = \left\{\frac{2}{3}\right\} \text{ và } f^{-1}(-6) = \emptyset.$$

$$\text{c) } f^{-1}([-5, 5]) = \{x \mid f(x) \in [-5, 5]\} = \{x \mid -5 \leq f(x) \leq 5\}.$$

$$\begin{aligned} \text{(Trường hợp 1) } x > 0: -5 \leq 3x - 5 \leq 5 &\Leftrightarrow 0 \leq 3x \leq 10 \Leftrightarrow 0 \leq x \leq \frac{10}{3}. \text{ Ta} \\ &\text{được } 0 < x \leq \frac{10}{3}. \end{aligned}$$



(Trường hợp 2)  $x \leq 0$ :  $-5 \leq -3x + 1 \leq 5 \Leftrightarrow -6 \leq -3x \leq 4 \Leftrightarrow -\frac{4}{3} \leq x \leq 2$ .

Ta được  $-\frac{4}{3} \leq x \leq 0$ .

Do đó,  $f^{-1}([-5, 5]) = \{x \mid 0 < x < \frac{10}{3} \text{ hoặc } -\frac{4}{3} \leq x \leq 0\} = \left[-\frac{4}{3}, \frac{10}{3}\right]$ .

Vì không có điểm  $(x, y)$  trên đồ thị mà  $y \leq -5$ , nên  $f^{-1}([-6, 5]) = f^{-1}([-5, 5]) = \left[-\frac{4}{3}, \frac{10}{3}\right]$ .

**Ví dụ 5.63.** Cho  $f : \mathbb{Z} \rightarrow \mathbb{R}$  xác định bởi  $f(x) = g(x) = x^2 + 5$ . **Bảng 5.4** tính và chỉ ra sự khác nhau giữa  $f^{-1}(B)$  và  $g^{-1}(B)$  do tập nguồn của hai hàm khác nhau, với một số tập  $B$  cụ thể.

$B$	$f^{-1}(B)$	$g^{-1}(B)$
$\{6\}$	$\{-1, 1\}$	$\{-1, 1\}$
$[6, 7]$	$\{-1, 2\}$	$[-\sqrt{2}, -1] \cup [1, \sqrt{2}]$
$[6, 10]$	$\{-2, -1, 1, 2\}$	$[-\sqrt{5}, -1] \cup [1, \sqrt{5}]$
$[-4, 5)$	$\emptyset$	$\emptyset$
$[-4, 5]$	$\{0\}$	$\{0\}$
$[5, +\infty)$	$\mathbb{Z}$	$\mathbb{R}$

Bảng 5.4

Tạo ảnh có một số tính chất gắn với phép toán tập hợp, gồm phép hợp, giao, và lấy phần bù.

**Định lý 5.10.** Nếu  $f : A \rightarrow B$  và  $B_1, B_2 \subseteq B$  thì

$$a) f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2) \quad c) f^{-1}(\overline{B_1}) = \overline{f^{-1}(B_1)}.$$

$$b) f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$$

Phần (b) của định lý này có sự khác biệt với phần (b) của ??.

Hàm  $f : A \rightarrow B$  là đơn ánh  $\Leftrightarrow |f^{-1}(b)| \leq 1, \forall b \in B$ .



Một tính chất quan trọng của hàm giữa các tập hữu hạn, không còn đúng trong trường hợp tổng quát.

**Định lý 5.11.** Cho  $f : A \rightarrow B$  với các tập  $A, B$  hữu hạn và  $|A| = |B|$ . Khi đó, các khẳng định sau là tương đương:

a)  $f$  là đơn ánh

b)  $f$  là toàn ánh

c)  $f$  khả nghịch.

Xét tập  $A, B$  với  $|A| = |B| = n > 0$ . Vì mỗi đơn ánh từ  $A$  vào  $B$  cũng là toàn ánh từ  $A$  vào  $B$ , và ngược lại, nên số đơn ánh từ  $A$  vào  $B$  bằng số toàn ánh từ  $A$  vào  $B$ , tức là

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

Đẳng thức trên cũng chỉ ra các phần tử đường chéo  $S(n, n)$ ,  $1 \leq n \leq 8$  của ?? đều bằng 1.

## 5.8 Độ phức tạp tính toán

Ta đã làm quen với khái niệm thuật toán ở [Phần 4.4](#), các thuật toán cụ thể như thuật toán chia ở [Phần 4.3](#) và thuật toán Euclid ở [Phần 4.4](#). Nói chung, một thuật toán có các tính chất sau:

- Đầu vào cung cấp cho thuật toán và đầu ra mà thuật toán cung cấp.
- Thuật toán có thể giải một dạng bài toán nhất định, chứ không phải trường hợp cụ thể của bài toán.
- Tính duy nhất của kết quả trung gian và cuối cùng theo đầu vào.
- Các bước của thuật toán phải được xác định một cách chính xác.
- Thuật toán kết thúc sau khi thực hiện một số bước hữu hạn.

Khi đã xây dựng được một thuật toán đúng, thỏa mãn năm điều kiện trên, có thể kiểm tra thêm theo những cách sau.

- 1) Bằng cách nào đó, có thể đo thời gian thuật toán cần để giải một bài toán có kích thước nhất định không? Thời gian này có thể phụ thuộc vào các yếu tố như tốc độ máy tính và trình biên dịch. Vì vậy, ta cần xây dựng một phép đo không phụ thuộc vào các tham số này.

Ví dụ, với một thuật toán để tính  $a^n$  với  $a \in \mathbb{R}$  và  $n \in \mathbb{Z}^+$ , có “hàm phụ thuộc  $n$ ” mô tả thuật toán hoàn thành nhanh như thế nào không?

- 2) Nếu có hai (hoặc nhiều) thuật toán giải cùng một bài toán, có cách nào để xác định một thuật toán là “tốt hơn” thuật toán kia không?

Cụ thể, xét bài toán xác định số thực  $x$  có trong dãy số thực  $a_1, a_2, \dots, a_n$  không. Bài toán này có cỡ  $n$ .

Nếu có thuật toán giải bài toán này, thì nó thực hiện mất bao lâu? Để đánh giá thời gian này, ta tìm hàm  $f(n)$ , gọi là *hàm phức tạp thời gian* của thuật toán. Nói chung,  $f(n)$  tăng khi  $n$  tăng. Ta cũng chủ yếu quan tâm thuật toán thực hiện thế nào khi  $n$  lớn.

**Định nghĩa 5.27.** Cho  $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$ . Ta nói  $g$  trội hơn  $f$  (hay  $f$  được làm trội bởi  $g$ ) nếu

$$\exists C \in \mathbb{R}^+, k \in \mathbb{Z}^+, |f(n)| \leq C|g(n)|, \forall n \in \mathbb{Z}^+, n \geq k. \quad (5.18)$$

Cách nói khác,  $f$  có bậc (cao nhất) là  $g$ , ký hiệu  $f \in O(g)$ , trong đó  $O(g)$ , đọc là “ô-lớn” của  $g$ , là tập các hàm từ  $\mathbb{Z}^+$  vào  $\mathbb{R}$  làm trội bởi  $g$ .

Giả sử  $\exists k \in \mathbb{Z}^+, \forall n \in \mathbb{Z}^+ (n \geq k), g(n) \neq 0$ , khi đó

$$\begin{aligned} f \in O(g) &\Leftrightarrow \exists C \in \mathbb{R}^+, k \in \mathbb{Z}^+, \forall n \in \mathbb{Z}^+ (n \geq k), \left| \frac{f(n)}{g(n)} \right| \leq C \\ &\Leftrightarrow \overline{\lim}_{n \rightarrow +\infty} \left| \frac{f(n)}{g(n)} \right| < +\infty. \end{aligned} \quad (5.19)$$

Việc xác định  $C, k$  trong định nghĩa trên đôi khi khá phức tạp. Với công thức (5.19) trong giải tích cao cấp, cùng với sự hỗ trợ tính toán từ Python, việc xác định ô-lớn cho một hàm trở nên dễ dàng hơn nhiều.

**Ví dụ 5.64.** Cho  $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$  trong đó  $f(n) = 5n, g(n) = n^2$  với  $n \in \mathbb{Z}^+$ .

a) Ta tính  $f(1) = 5, g(1) = 1; f(2) = 10, g(2) = 4; f(3) = 15, g(3) = 9; f(4) = 20, g(4) = 16$  và thấy  $f(n) > g(n), \forall n = \overline{1, 4}$ . Tuy nhiên,  $n \geq 5 \Rightarrow n^2 \geq 5n$  hay  $|f(n)| = 5n \leq n^2 = |g(n)|$ . Như vậy, với  $C = 1$  và  $k = 5$ , ta có  $|f(n)| \leq C|g(n)|, \forall n \geq k$ , nên  $f \in O(g)$ .

Ta cũng thấy  $\forall n \in \mathbb{Z}^+, |f(n)| = 5n \leq 5n^2 = 5|g(n)|$ , nên với  $C = 5$  và  $k = 1$ ,  $|f(n)| \leq C|g(n)|, \forall n \geq k$ . Do đó các hằng số  $C$  và  $k$  trong Định nghĩa 5.27 không duy nhất.

Tổng quát hơn, xét các hàm  $f_1, g_1 : \mathbb{Z}^+ \rightarrow \mathbb{R}$  cho bởi  $f_1(n) = an, g_1(n) = bn^2$ , trong đó  $a, b \in \mathbb{R}^*$ . Với  $n \geq 1$  thì  $|f_1(n)| = |an| = |a|n \leq |a|n^2 = \frac{|a|}{|b|}|bn^2| = \frac{|a|}{|b|}|g_1(n)|$ .

Vậy với  $C = \frac{|a|}{|b|}$  và  $k = 1$  thì  $\forall n \in \mathbb{Z}^+ (n \geq k), |f_1(n)| \leq C|g_1(n)|$ . Do đó  $f_1 \in O(g_1)$ .

b) Giờ ta chứng minh  $g \notin O(f)$ . Giả sử phản chứng,  $g \in O(f)$ , tức là

$$\exists C \in \mathbb{R}^+, k \in \mathbb{Z}^+, \forall n \in \mathbb{Z}^+ (n \geq k), |g(n)| \leq C|f(n)|.$$

Biến đổi

$$|g(n)| \leq C|f(n)| \Leftrightarrow n^2 \leq C \cdot 5n \Leftrightarrow n \leq 5C$$

Điều này không thể đúng  $\forall n \in \mathbb{Z}^+, n \geq k$ , chẳng hạn với  $n > \max\{5C, k\}$  nào đó.

Ta cũng có thể chứng minh trực tiếp  $g \notin O(f)$ , tức là

$$\forall C \in \mathbb{R}^+, k \in \mathbb{Z}^+, \exists n \in \mathbb{Z}^+ (n \geq k), |g(n)| > C|f(n)|.$$

Ta thấy  $|g(n)| > C|f(n)| \Leftrightarrow |n^2| > C|5n| \Leftrightarrow n > 5C$ , nên chọn được  $n > \max\{k, 5C\}$  để  $|g(n)| > C|f(n)|$ .

**Ví dụ 5.65.** a) Cho  $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$  với  $f(n) = 5n^2 + 3n + 1$  và  $g(n) = n^2$ . Khi đó  $|f(n)| = |5n^2 + 3n + 1| = 5n^2 + 3n + 1 \leq 5n^2 + 3n^2 + n^2 = 9n^2 = 9|g(n)|$ . Do đó  $\exists C \in \mathbb{R}^+ (C = 9), k \in \mathbb{Z}^+ (k = 1), \forall n \geq k, |f(n)| \leq C|g(n)|$ , hay  $f \in O(g)$ . Ta cũng có thể viết  $f \in O(n^2)$ .

Mặt khác  $|g(n)| = n^2 \leq 5n^2 \leq 5n^2 + 3n + 1 = |f(n)|, \forall n \geq 1$  nên với  $C = 1, k = 1, |f(n)| \leq C|g(n)|, \forall n \geq k$ , tức là  $g \in O(f)$ . [Ở đây  $O(f) = O(g)$ , tức là, hàm từ  $\mathbb{Z}^+$  vào  $\mathbb{R}$  làm trội bởi  $f$  hoặc  $g$  thì cũng làm trội bởi hàm kia.]

b) Xét  $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$  với  $f(n) = 3n^3 + 7n^2 - 4n + 2$  và  $g(n) = n^3$ . Ta có  $|f(n)| = |3n^3 + 7n^2 - 4n + 2| \leq |3n^3| + |7n^2| + |-4n| + |2| \leq 3n^3 + 7n^3 + 4n^3 + 2n^3 = 16n^3 = 16|g(n)|, \forall n \geq 1$ , tức là  $f \in O(g)$  hay  $f \in O(n^3)$ .

Mặt khác  $3n^3 + 7n^2 - 4n + 2 = 3n^3 + (7n - 4)n + 2 \geq 3n^3 \geq n^3, \forall n \geq 1$  nên  $|g(n)| \leq |f(n)|, \forall n \geq 1$ , tức là  $g \in O(f)$ . [Như ý (a), ta cũng có  $O(f) = O(g) = O(n^3)$ .]

Tổng quát, xét các hàm đa thức  $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$  trong đó  $f(n) = a_m n^m + a_{m-1} n^{m-1} + \dots + a_1 n + a_0$ , với  $a_m, a_{m-1}, \dots, a_1, a_0 \in \mathbb{R}, a_m \neq 0, m \in \mathbb{N}$ , và  $g(n) = n^m$ . Khi đó

$$\begin{aligned} |f(n)| &= |a_m n^m + a_{m-1} n^{m-1} + \dots + a_1 n + a_0| \\ &\leq |a_m n^m| + |a_{m-1} n^{m-1}| + \dots + |a_1 n| + |a_0| \\ &= |a_m| n^m + |a_{m-1}| n^{m-1} + \dots + |a_1| n + |a_0| \\ &\leq |a_m| n^m + |a_{m-1}| n^m + \dots + |a_1| n^m + |a_0| n^m \\ &= (|a_m| + |a_{m-1}| + \dots + |a_1| + |a_0|) n^m. \end{aligned}$$

Chọn  $C = |a_m| + |a_{m-1}| + \dots + |a_1| + |a_0|$  và  $k = 1$ . Khi đó  $|f(n)| \leq C|g(n)|, \forall n \geq k$ , tức là  $f \in O(n^m)$ .

Để chỉ ra  $g \in O(f)$ , và do đó  $O(f) = O(g) = O(n^m)$ , ta đánh giá

$$\begin{aligned} |f(n)| &\geq |a_m n^m| - |a_{m-1} n^{m-1}| - \dots - |a_1 n| - |a_0| \\ &= |a_m| n^m - \frac{|a_{m-1}|}{n} n^m - \dots - \frac{|a_1|}{n^{m-1}} n^m - \frac{|a_0|}{n^m} n^m \\ &\geq |a_m| n^m - \frac{|a_{m-1}|}{n} n^m - \dots - \frac{|a_1|}{n} n^m - \frac{|a_0|}{n} n^m \\ &= \left( |a_m| - \frac{|a_{m-1}| + \dots + |a_1| + |a_0|}{n} \right) n^m. \end{aligned}$$

Ở đây ta muốn  $|a_m| - \frac{|a_{m-1}| + \dots + |a_1| + |a_0|}{n} \geq \frac{|a_m|}{2} \Leftrightarrow \frac{|a_m|}{2} \geq \frac{|a_{m-1}| + \dots + |a_1| + |a_0|}{n} \Leftrightarrow$   
 $n \geq 2 \frac{|a_{m-1}| + \dots + |a_1| + |a_0|}{|a_m|}$ . Từ đó, chọn  $k \geq \max\{2 \frac{|a_{m-1}| + \dots + |a_1| + |a_0|}{|a_m|}, 1\}$  thì  
 $\forall n \geq k, |f(n)| \geq \frac{|a_m|}{2} n^m = \frac{|a_m|}{2} |g(n)|$  hay  $|g(n)| \leq \frac{2}{|a_m|} |f(n)|$ .

Kết quả tổng quát trên cho ta đánh giá một số tổng đặc biệt sau.

**Ví dụ 5.66.** a) Cho  $f : \mathbb{Z}^+ \rightarrow \mathbb{R}$  với  $f(n) = 1 + 2 + \dots + n$ . Khi đó  $f(n) = \frac{n(n+1)}{2} = \frac{n^2}{2} + \frac{n}{2} \in O(n^2)$ .

b) Nếu  $g : \mathbb{Z}^+ \rightarrow \mathbb{R}$  cho bởi  $g(n) = 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$  thì  $g(n) = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} \in O(n^3)$ .

c) Nếu  $h : \mathbb{Z}^+ \rightarrow \mathbb{R}$  cho bởi  $h(n) = \sum_{i=1}^n i^t$  với  $t \in \mathbb{Z}^+$  thì  $h(n) = 1^t + 2^t + \dots + n^t \leq n^t + n^t + \dots + n^t = n \cdot n^t = n^{t+1}$  nên  $h(n) \in O(n^{t+1})$ .

Bảng độ lớn của hàm:

Dạng Ô-lớn	Tên gọi	Thuật toán điển hình
$O(1)$	hằng số	không có vòng lặp
$O(\log_2 n)$	loga	tìm kiếm nhị phân, lũy thừa
$O(n)$	tuyến tính	tìm kiếm tuyến tính
$O(n \log_2 n)$	$n \log_2 n$	sắp xếp trộn, sắp xếp đồng
$O(n^2)$	bậc hai	sắp xếp nổi bọt, cộng ma trận
$O(n^3)$	bậc ba	nhân ma trận
$O(n^m), m = 0, 1, 2, \dots$	đa thức	
$O(c^n), c > 1$	hàm mũ	đơn hình
$O(n!)$	giai thừa	liệt kê hoán vị, định thức

a) Với  $m, c > 1$

$$O(1) \subseteq O(\log n) \subseteq O(n) \subseteq O(n \log n) \subseteq O(n^m) \subseteq O(b^x) \subseteq O(n!) \subseteq O(n^n)$$

b)  $cf \in O(f)$

c)  $f, g \in O(h) \Rightarrow f + g, cf \in O(h)$

d)  $f_1 \in O(g_1), f_2 \in O(g_2) \Rightarrow f_1 f_2 \in O(g_1 g_2)$ .

## 5.9 Phân tích thuật toán

Ta đếm các phép toán trong thuật toán, gồm phép toán số học, phép so sánh, phép toán logic, phép gán rồi đánh giá độ phức tạp theo cỡ của dữ liệu đầu vào.

**Ví dụ 5.67.** An mở tài khoản 100 triệu ở ngân hàng với lãi suất 5%/tháng. Đầu chu kỳ mỗi tháng, An gửi thêm 50 triệu.

- Xác định số dư trong tài khoản của An sau 1 tháng, 2 tháng.
- Mô tả thuật toán xác định số dư sau  $n$  tháng.
- Xác định độ phức tạp của thuật toán ở ý (b).

*Giải.* a)

$n$	Số dư sau $n$ tháng (đơn vị: triệu)
1	$100 + 100 \cdot 0.005 + 50 = 150.5$
2	$150.5 + 150.5 \cdot 0.005 + 50 = 201.253$

- b) Thuật toán tìm số dư tài khoản sau  $n$  tháng.

**Data:**  $n$

**Result:** Số dư tài khoản sau  $n$  tháng

```

1 so_du = 100                                // khởi tạo số dư
2 gui_them = 50                               // tiền gửi thêm hàng tháng
3 lai_suat = 0.005                           // lãi suất tháng
4 i = 1                                       // khởi tạo biến đếm
5 while i ≤ n do
6     so_du = so_du + so_du * lai_suat + gui_them
7     i = i + 1

```

- c) 1) Dòng 1, 2, 3 có 3 phép gán.
- 2) Dòng 4, 5, 7 cho  $n$  vòng lặp. Dòng 4 có 1 phép gán, dòng 5 có  $n + 1$  phép so sánh, ứng với  $i = 1, n + 1$ , dòng 7 có 1 phép cộng và 1 phép gán (lặp  $n$  lần). Ba dòng này có số phép toán  $1 + (n + 1) + 2n = 3n + 2$ , với  $n$  là số vòng lặp.
- 3) Dòng 6 có 3 phép toán số học và 1 phép gán (lặp  $n$  lần).

Vậy, số phép toán của thuật toán là  $f(n) = 3 + (3n + 2) + 4n = 7n + 5 \in O(n)$ .

□

Khi  $n$  lớn, “cấp độ lớn” của  $7n + 5$  chủ yếu phụ thuộc vào  $n$ , là số lần lặp của vòng lặp **while**. Do đó để chỉ ra  $f \in O(n)$ , ta chỉ cần đếm số chu trình của vòng lặp **while**.

Các ví dụ về độ phức tạp (trong trường hợp) tốt nhất, độ phức tạp xấu nhất và độ phức tạp trung bình.

**Ví dụ 5.68** (Thuật toán tìm kiếm tuyến tính). Mô tả thuật toán và xác định độ phức tạp của thuật toán tìm vị trí của  $x$  trong dãy  $a_1, a_2, \dots, a_n$ .

*Giải.* a)

**Data:**  $a_1, a_2, \dots, a_n$  và  $x$

**Result:** Vị trí của  $x$  trong dãy

```

1  i = 1                                     // chỉ số dãy
2  while i ≤ n and x ≠ ai do i = i + 1
3  if i ≤ n then
4      viTri = i                             // tìm được
5  viTri = 0                                 // không tìm được
// viTri là chỉ số của phần tử đầu tiên bằng x, là 0 nếu không tìm được

```

b) Đặt  $f(n)$  là số chu trình thực hiện trong vòng lặp **while** ở dòng 2.

- i) Nếu  $x = a_1$ , thì  $f(n) = 1 \in O(1)$ , là độ phức tạp tốt nhất.
- ii) Nếu  $x \neq a_i \forall i = \overline{1, n}$ , hoặc dãy  $a_1, a_2, \dots, a_n$  phân biệt và  $x = a_n$ , thì  $f(n) = n \in O(n)$ , là độ phức tạp xấu nhất.
- iii) Giả sử  $P(x \in \{a_1, a_2, \dots, a_n\}) = p$ , trong đó  $x$  nhận mỗi giá trị với khả năng như nhau  $P(x = a_i) = \frac{p}{n}$  và  $P(x \in \{a_1, a_2, \dots, a_n\}) = 1 - p$ .  
Đặt  $X = f(n)$ . Ta có

$$P(X = i) = P(x = a_i) = \frac{p}{n}, \forall i = \overline{1, n-1}, \quad \text{và}$$

$$P(X = n) = P(x = a_n) + P(X \notin \{a_1, a_2, \dots, a_n\}) = \frac{p}{n} + (1 - p)$$

Khi đó

$$\begin{aligned}
 EX &= \sum_{i=1}^n i \cdot P(X = i) = 1 \cdot \frac{p}{n} + 2 \cdot \frac{p}{n} + \dots + n \left( \frac{p}{n} + 1 - p \right) \\
 &= (1 + 2 + \dots + n) \frac{p}{n} + n(1 - p) = \frac{n(n+1)}{2} \cdot \frac{p}{n} + n(1 - p) \\
 &= \frac{(n+1)p}{2} + n(1 - p) = n \left( 1 - \frac{p}{2} \right) + \frac{p}{2} \in O(n)
 \end{aligned}$$

là độ phức tạp trung bình của thuật toán.

□

**Ví dụ 5.69.** Trình bày các thuật toán tính  $a^n$  với  $a \in \mathbb{R}$ ,  $n \in \mathbb{N}$ , và đánh giá độ phức tạp tương ứng.

*Giải.* **Thuật toán 1:**

**Data:**  $a, n$

**Result:**  $a^n$

```
1  $x = 1$  //  $x$  lưu  $a^1, a^2, \dots, a^n$ 
2 for  $i = 1$  to  $n$  do
3    $x = x * a$ 
```

Vòng lặp **for** ở dòng 2 thực hiện  $n$  chu trình, nên thuật toán có độ phức tạp  $f(n) = n \in O(n)$ , là độ phức tạp tuyến tính.

**Thuật toán 2:** phương pháp chia đôi để tính lũy thừa

```
1  $x = 1$ 
2  $i = n$ 
3 while  $i > 0$  do
4   if  $i$  lẻ then  $x = x * a$ 
5    $a = a * a$ 
6    $i = \lfloor \frac{i}{2} \rfloor$ 
```

Chẳng hạn, tính  $a^{10}$

Bước	$x$	$a$	$i$
Khởi tạo	1	$a$	10
Dòng 3, chu trình 1	1	$a^2$	5
Dòng 3, chu trình 2	$a^2$	$a^4$	2
Dòng 3, chu trình 3	$a^2$	$a^8$	1
Dòng 3, chu trình 4	$a^{10}$	$a^{16}$	0

Đặt  $f(n)$  là số chu trình của của vòng lặp **while**. Ta chứng minh  $f(n) \leq 1 + \log_2 n$ ,  $\forall n \in \mathbb{Z}^+$  bằng quy nạp.

1)  $f(1) = 1 \leq 1 + \log_2 1$ : đúng.



2) Giả sử  $f(k) \leq 1 + \log_2 k$ ,  $\forall k = \overline{1, n}$ . Ta sẽ chứng minh  $f(n+1) \leq 1 + \log_2(n+1)$ .

Xét thuật toán với đầu vào  $n+1$ . Sau bước đầu tiên,  $i = \lfloor \frac{n+1}{2} \rfloor$ , từ đó  $f(n+1) = 1 + f(\lfloor \frac{n+1}{2} \rfloor)$ . Mặt khác,  $1 \leq \frac{n+1}{2} \leq n$  nên  $1 \leq \lfloor \frac{n+1}{2} \rfloor \leq n$ , suy ra

$$f(\lfloor \frac{n+1}{2} \rfloor) \leq 1 + \log_2 \lfloor \frac{n+1}{2} \rfloor \leq 1 + \log_2 \frac{n+1}{2} = \log_2(n+1).$$

Do đó  $f(n+1) \leq 1 + \log_2(n+1)$ .

Vậy  $f(n) \leq 1 + \log_2 n \in O(\log_2 n)$ , thuật toán có độ phức tạp  $\log_a$ .

□

Cỡ đầu vào $n$	Độ phức tạp					
	$\log_2 n$	$n$	$n \log_2 n$	$n^2$	$2^n$	$n!$
2	1	2	2	4	4	2
16	4	16	64	256	$6.5 \times 10^4$	$2.1 \times 13$
64	6	64	384	4096	$1.84 \times 10^{19}$	$> 10^{89}$

Cho tập  $A$  cỡ  $n$ . Xét hai thuật toán:

- 1) Tìm các tập con cỡ 1 của  $A$ . Có  $n$  tập con.
- 2) Tìm tất cả tập con của  $A$ . Có  $2^n$  tập con.

Giả sử máy tính xác định mỗi tập con của  $A$  mất một nano giây ( $10^{-9}$ s). Khi đó nếu  $|A| = 64$ , thuật toán (1) thực thi xong gần như ngay lập tức, trong 64 nano giây. Tuy nhiên, thuật toán (2) thực hiện trong

$$1.84 \times 10^{19} \text{ nano giây} = 2.14 \times 10^5 \text{ ngày} = 585 \text{ năm}.$$

## Bài tập bổ sung

**5.38.** Ước tính mất bao lâu để phân tích nguyên tố cho một số có 1000 chữ số bằng phép chia thử. Giả sử rằng ta thử tất cả các ước có thể đến căn bậc hai của số đó và có thể thực hiện một triệu tỷ phép chia thử mỗi giây (cỗ siêu máy tính). Chọn một đơn vị thời gian hợp lý cho câu trả lời.

# Tài liệu tham khảo

- [1] NumPy community. *NumPy User Guide*. phiên bản 1.22.4. 535 trang. URL: <https://numpy.org/doc/stable>.
- [2] Judi J. McDonald David C. Lay Steven R. Lay. *Linear Algebra and Its Applications*. phiên bản 6. Pearson, 2022. 755 trang.
- [3] Ralph P. Grimaldi. *Discrete and Combinatorial Mathematics: An Applied Introduction*. phiên bản 5. Pearson Addison-Wesley, 2004. 992 trang.
- [4] Ralph P. Grimaldi. *Discrete and Combinatorial Mathematics: Instructor's Solutions Manual*. phiên bản 5. Pearson Addison-Wesley, 2004. 465 trang.
- [5] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. phiên bản 8. McGraw-Hill Education, 2019. 1118 trang.
- [6] Edward R. Scheinerman. *Mathematics: A Discrete Introduction*. phiên bản 3. Brooks/Cole, Cengage Learning, 2013. 506 trang.
- [7] Watson S. Stewart J. Clegg D. *Calculus: Early Transcendentals*. phiên bản 9. Cengage Learning, 2011. 1421 trang.
- [8] SymPy Development Team. *SymPy Documentation*. phiên bản 1.8. 2750 trang. URL: <https://github.com/sympy/sympy/releases>.

