KENNETH H. ROSEN

TOÁN HỌC RỜI RẠC
ỨNG DỤNG TRONG TIN HỌC

Người dịch: ***Phạm Văn Thiều***
Đặng Hữu Thịnh

NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT
HÀ NỘI

Dịch từ

Discrete Mathematics and Its Applications

McGraw - Hill, 1994

5-519
KHKT-2003 111-29-02

Lời giới thiệu

Toán học rời rạc không phải là một chủ đề mới nhưng giáo trình hay về toán học rời rạc và ứng dụng của nó thì không có nhiều. Mà hay đến mức được tái bản nhiều lần và được sử dụng trong hơn 300 trường học như quyển sách của Giáo sư Kenneth H. Rosen thì lại càng hiếm, nếu không muốn nói là chưa hề thấy. Chất lượng của một giáo trình được thể hiện ở sự súc tích của nội dung và tính sư phạm của cấu trúc và cách trình bày nội dung đó. Điều này đòi hỏi tác giả phải thấu hiểu sâu sắc chủ đề, có bề dày thực nghiệm sư phạm và dĩ nhiên có sở trường viết lách. K.H.Rosen đúng là một người như vậy : là một tiến sĩ toán học, đã giảng dạy nhiều năm ở các đại học Mỹ, đã tham gia nghiên cứu toán ứng dụng cho tin học và các ngành kỹ thuật khác, và đã viết nhiều cuốn sách khoa học được xếp vào hàng "best seller". Đọc cuốn sách này, chúng ta sẽ bị hấp dẫn bởi nhiều điều độc đáo của nó. Nhưng có lẽ điều làm kinh ngạc và thán phục nhất là khối lượng đồ sộ các ví dụ, câu hỏi, bài tập, đề tài ứng dụng tin học ... giúp cho người đọc dễ dàng hiểu và biết ứng dụng có hiệu quả các kiến thức đa dạng không chỉ thuần tuý về toán học rời rạc.

Giáo trình tuyệt diệu này có thể sử dụng cho nhiều đối tượng khác nhau, nhưng trước hết là cho thầy và trò ở các trường đại học khoa học tự nhiên và công nghệ – đặc biệt là công nghệ thông tin. Cấu trúc lôgic và độc đáo của cuốn sách cùng những ví dụ, bài tập, đề tài tiếp cận từ góc độ tin học đã làm cho người đọc luôn

luôn có thể tìm thấy cách đọc thích hợp với mình, tiếp thu đầy đủ và nhanh chóng những kiến thức mong muốn.

Điều cuối cùng, nhưng rất quan trọng đối với chất lượng của một cuốn sách dịch đó là dịch giả. Anh Phạm Văn Thiều (chủ biên dịch cuốn sách này) là nhà vật lý lý thuyết, đã giảng dạy đại học nhiều năm và đã từng dịch nhiều sách nước ngoài, kể cả về văn học. Cuốn sách dịch gần đây của anh (cùng với Cao Chi), "Lược sử thời gian" của nhà vật lý nổi tiếng thế giới S.W. Hawking..., đã được bạn đọc và đồng nghiệp đánh giá rất cao.

Xin trân trọng giới thiệu cuốn sách ***TOÁN HỌC RỜI RẠC ỨNG DỤNG TRONG TIN HỌC*** *này với bạn đọc.*

GS.TS. NGUYỄN THÚC HẢI

TRƯỞNG KHOA CÔNG NGHỆ THÔNG TIN
ĐẠI HỌC BÁCH KHOA HÀ NỘI.

CHƯƠNG 1

CÁC KIẾN THỨC CƠ SỞ : LOGIC, TẬP HỢP VÀ HÀM

Chương này ôn lại những cơ sở của toán học rời rạc. Ba chủ đề sẽ được đề cập tới, đó là logic, tập hợp và hàm. Các qui tắc của logic xác định ý nghĩa chính xác của các mệnh đề toán học. Ví dụ, những qui tắc đó cho chúng ta ý nghĩa của các mệnh đề như : "Tồn tại một số nguyên lớn hơn 100 là luỹ thừa của 2" và "Đối với mọi số nguyên n, tổng các số nguyên dương không lớn hơn n bằng $\frac{n(n+1)}{2}$". Logic là cơ sở của mọi suy luận toán học và có nhiều ứng dụng thực tiễn trong việc thiết kế các máy tính.

Có rất nhiều môn toán học rời rạc chuyên nghiên cứu các cấu trúc rời rạc, tức là những cấu trúc được dùng để biểu diễn các đối tượng rời rạc. Tất cả các cấu trúc này đều được dựng lên từ tập hợp các đối tượng vật. Những ví dụ về các cấu trúc rời rạc được dựng lên từ các tập hợp bao gồm : tổ hợp – đó là tập hợp không sắp thứ tự của các đối tượng được dùng rộng rãi trong phép đếm ; quan hệ – đó là tập hợp các cặp sắp thứ tự biểu diễn mối quan hệ giữa các vật ; đồ thị – đó là tập hợp các đỉnh và các cạnh nối các đỉnh ; và các máy trạng thái hữu hạn – đó là các máy được dùng để mô hình hóa các máy tính.

Hàm là một khái niệm cực kỳ quan trọng trong toán học rời rạc. Hàm gán cho mỗi phần tử của một tập hợp một phần tử xác định của một tập hợp. Các cấu trúc tiện ích như dãy và xâu là những loại hàm đặc biệt. Các hàm cũng được dùng để biểu diễn số các bước của một thủ tục dùng để giải một bài toán. Sự phân tích các thuật toán thường dùng các thuật ngữ và khái niệm có liên quan đến độ tăng của các hàm. Các hàm đệ qui, tức là các hàm được định nghĩa bằng cách cho các giá trị của chúng ở các số nguyên dương qua các giá trị của chúng ở các số nguyên dương nhỏ hơn – đã được dùng để giải nhiều bài toán đếm.

1.1. LOGIC

MỞ ĐẦU

Các qui tắc của logic cho ý nghĩa chính xác của các mệnh đề. Các qui tắc này được sử dụng để phân biệt giữa các lập luận toán học đúng và không đúng. Vì mục đích chủ yếu của cuốn sách này là dạy cho độc giả hiểu và xây dựng được những lập luận toán học đúng đắn, nên chúng ta sẽ bắt đầu việc nghiên cứu toán học rời rạc từ một nhập môn vào logic học.

Cùng với tầm quan trọng của nó trong việc hiểu sự suy luận toán học, logic học còn có nhiều ứng dụng trong tin học. Các qui tắc của logic được dùng để thiết kế các mạng trong máy tính, để xây dựng các chương trình của máy tính, để kiểm tra tính đúng đắn của các chương trình và nhiều ứng dụng khác. Chúng ta sẽ xem xét các ứng dụng đó trong các chương sau.

MỆNH ĐỀ

Chúng ta sẽ bắt đầu bằng việc xem xét những viên gạch cơ sở xây dựng nên môn logic – đó là các mệnh đề. Một **mệnh đề** là một câu đúng hoặc sai, chứ không thể vừa đúng vừa sai.

Ví dụ 1. Tất cả các câu sau đều là các mệnh đề.

1. Washington D.C. là thủ đô của Hoa Kỳ.
2. Toronto là thủ đô của Canada
3. $1 + 1 = 2$,
4. $2 + 2 = 3$.

Các mệnh đề 1 và 3 là đúng, trong khi các mệnh đề 2 và 4 là sai. ■

Có những câu không phải là mệnh đề được cho trong các ví dụ dưới đây

Ví dụ 2. Xét các câu sau :

1. Bây giờ là mấy giờ?
2. Hãy đọc cái này cho kỹ lưỡng.
3. $x + 1 = 2$,
4. $x + y = z$

Các câu 1 và 2 không phải là mệnh đề vì chúng không phải là câu trần thuật. Còn các câu 3 và 4 không phải là mệnh đề vì chúng chẳng đúng cũng chẳng sai bởi các biến trong những câu đó còn chưa được gán cho giá trị cụ thể nào. Các cách khác nhau để tạo thành các mệnh đề từ những câu loại như thế này sẽ được thảo luận trong Tiết 3 của chương này. ■

Các chữ cái sẽ được dùng để ký hiệu các mệnh đề, cũng như để ký hiệu các biến. Những chữ cái qui ước được dùng vào mục đích này là *p, q, r, s*... **Giá trị chân lý** của một mệnh đề là đúng và sẽ được ký hiệu là *T* nếu đó là một mệnh đề đúng, và là sai, được ký hiệu là *F*, nếu đó là một mệnh đề sai.

Bây giờ chúng ta xem xét các phương pháp tạo ra các mệnh đề mới từ các mệnh đề chúng ta đã có. Các phương pháp này đã được nghiên cứu hồi nhà toán học người Anh Geogre Boole, và được trình bày trong cuốn sách "*Các định luật của tư duy*" xuất bản năm 1854 của ông. Rất nhiều mệnh đề toán học được xây dựng bằng cách tổ hợp một hoặc nhiều mệnh đề. Các mệnh đề mới được gọi là **các mệnh đề phức hợp**, chúng được tạo ra từ các mệnh đề hiện có bằng cách dùng các toán tử logic.

ĐỊNH NGHĨA 1. Giả sử p là một mệnh đề.

Câu "không phải là p"

là một mệnh đề khác, được gọi là *phủ định* của p. Phủ định của p được ký hiệu là $\neg p$ (trong nhiều sách được ký hiệu là $\overline{p}$ – ND).

BẢNG 1. Bảng giá trị chân lý đối với phủ định của một mệnh đề

p	$\neg p$
T	F
F	T

Ví dụ 3. Tìm phủ định của mệnh đề :

"Hôm nay là thứ sáu"

Giải : Phủ định của mệnh đề trên là :

"Hôm nay không phải là thứ sáu" ■

Một **bảng giá trị chân lý** trình bày mối quan hệ giữa các giá trị chân lý của các mệnh đề. Bảng giá trị chân lý đặc biệt có ý nghĩa trong việc xác định giá trị chân lý của các mệnh đề được tạo ra từ các mệnh đề đơn giản hơn. Bảng 1 trình bày các giá trị chân lý của một mệnh đề và phủ định của nó.

Phủ định của một mệnh đề cũng có thể được xem như là kết quả tác dụng của **toán tử phủ định** lên một mệnh đề. Toán tử phủ định xây dựng một mệnh đề mới từ một mệnh đề đơn hiện có. Bây giờ chúng ta sẽ đưa vào các toán tử logic được dùng để tạo ra các mệnh đề mới từ hai hoặc nhiều hơn các mệnh đề hiện có.

ĐỊNH NGHĨA 2. Giả sử p và q là hai mệnh đề. Mệnh đề "p và q", được ký hiệu bởi $p \wedge q$, là đúng khi cả p và q đều đúng, còn sai trong các trường hợp còn lại. Mệnh đề $p \wedge q$ được gọi là *hội* của p và q.

BẢNG 2. Bảng giá trị chân lý đối với hội của hai mệnh đề

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

Bảng chân lý đối với $p \wedge q$ được cho trong Bảng 2. Chú ý rằng, trong bảng chân lý này có bốn dòng, mỗi dòng là một tổ hợp khả dĩ các giá trị chân lý của các mệnh đề p và q.

Ví dụ 4. Tìm hội của các mệnh đề p và q, trong đó p là mệnh đề "Hôm nay là thứ sáu" và q là mệnh đề "Hôm nay trời mưa".

Giải : Hội của hai mệnh đề đó $p \wedge q$ là mệnh đề "Hôm nay thứ sáu và trời mưa". Mệnh đề này là đúng vào hôm thứ sáu trời mưa và là sai vào bất kỳ ngày nào không phải thứ sáu và vào ngày thứ sáu nhưng trời lại không mưa.

■

ĐỊNH NGHĨA 3. Cho p và q là hai mệnh đề. Mệnh đề : "p hoặc q", được ký hiệu là $p \vee q$, là mệnh đề sai khi cả p và q đều sai, và đúng trong các trường hợp còn lại. Mệnh đề $p \vee q$ được gọi là *tuyển* của p và q.

Bảng giá trị chân lý đối với $p \vee q$ được cho trong Bảng 3.

Việc dùng liên từ "hoặc" trong phép tuyển tương ứng với một trong hai sắc thái nghĩa của từ "or" trong tiếng Anh (từ hoặc tiếng Việt cũng thế – ND) – đó là sắc thái nghĩa có tính bao hàm. Một phép tuyển là đúng khi một trong hai mệnh đề là đúng hoặc cả hai mệnh đề đều đúng. Ví dụ từ "hoặc" có sắc thái nghĩa bao hàm được dùng trong câu sau :

BẢNG 3. Bảng giá trị chân lý đối với tuyển của hai mệnh đề

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

"Các sinh viên đã học giải tích hoặc tin học có thể theo lớp này".

Ở đây, người ta muốn nói rằng các sinh viên đã học cả giải tích lẫn tin học, cũng như các sinh viên chỉ đã học một trong hai môn trên đều có thể theo lớp này.

Trái lại, chúng ta dùng từ hoặc với sắc thái nghĩa loại trừ, khi ta nói :

"Các sinh viên đã học giải tích hoặc tin học,
nhưng không phải cả hai môn, đều có thể theo lớp này".

Ở đây, người ta muốn nói rằng các sinh viên đã học cả giải tích lẫn tin học thì không được theo lớp này. Chỉ những người đã học chính xác một trong hai môn trên mới được vào lớp đó.

Tương tự, khi thực đơn trong một nhà hàng ghi "Món khai vị : súp hoặc xa lat" thì nhà hàng đó hầu như đều muốn nói rằng khách hàng có thể ăn súp hoặc xa lát chứ không phải cả hai. Ở đây từ "hoặc" có sắc thái nghĩa loại trừ chứ không phải hao hàm.

Ví dụ 5. Lập tuyển của hai mệnh đề p và q với p và q là những mệnh đề như ở Ví dụ 4

Giải : Tuyển của p và q, tức $p \vee q$, là mệnh đề :

"Hôm này là thứ sáu hoặc hôm nay trời mưa".

Mệnh đề này đúng vào bất kỳ ngày nào là thứ sáu hoặc ngày có mưa (kể cả ngày thứ sáu có mưa). Nó chỉ sai vào ngày không phải là thứ sáu và ngày đó trời không mưa.

■

Như chúng ta đã nhận xét ở trên, việc dùng liên từ "hoặc" trong phép tuyển tương ứng với một trong hai sắc thái nghĩa của từ đó, cụ thể ở đây là theo sắc thái nghĩa bao hàm. Như vậy, phép tuyển là đúng khi một trong hai mệnh đề là đúng hoặc khi cả hai mệnh đề đều đúng. Đôi khi, chúng ta cũng dùng từ *hoặc* theo sắc thái nghĩa loại trừ. Khi dùng từ hoặc có sắc thái nghĩa loại trừ để liên kết hai mệnh đề p và q, ta nhận được mệnh đề "p hoặc q (nhưng không cả hai)".

Mệnh đề này đúng khi p đúng và q sai hoặc ngược lại và nó sai khi cả p và q đều sai và khi cả p và q đều đúng.

ĐỊNH NGHĨA 4. Cho p và q là hai mệnh đề.

Mệnh đề *tuyển loại* của p và q, được ký hiệu là $p \oplus q$, là một mệnh đề chỉ đúng khi một trong p và q là đúng và sai trong mọi trường hợp còn lại.

Bảng giá trị chân lý của phép tuyển loại của hai mệnh đề được cho trong Bảng 4.

BẢNG 4. Bảng giá trị chân lý đối với phép tuyển loại của hai mệnh đề

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Bây giờ chúng ta sẽ xem xét một số phương pháp quan trọng khác có thể tạo nên các mệnh đề.

ĐỊNH NGHĨA 5. Cho p và q là hai mệnh đề.

Mệnh đề kéo theo $p \rightarrow q$ là một mệnh đề chỉ sai khi p đúng và q sai, còn đúng trong mọi trường hợp còn lại.

Trong phép kéo theo nói trên p được gọi là *giả thiết* còn q được gọi là *kết luận*.

BẢNG 5. Bảng giá trị chân lý đối với phép kéo theo $p \rightarrow q$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Bảng giá trị chân lý đối với mệnh đề kéo theo $p \rightarrow q$ được cho trong Bảng 5.

Vì phép kéo theo xuất hiện ở nhiều chỗ trong các suy luận toán học, nên có rất nhiều thuật ngữ được dùng để biểu đạt $p \rightarrow q$. Dưới đây là một số ví dụ thường gặp nhất :

- "Nếu p thì q"
- "p kéo theo q"
- "p là điều kiện đủ của q"
- "q là điều kiện cần của p".

Chú ý rằng $p \rightarrow q$ chỉ sai trong trường hợp p đúng và q sai, sao cho nó đúng khi cả p và q đều đúng và khi p sai (bất kể q đúng hay sai).

Cách mà chúng ta định nghĩa phép kéo theo là tổng quát hơn ý nghĩa gắn liền với từ kéo theo trong ngôn ngữ thông thường. Ví dụ phép kéo theo

"Nếu hôm nay trời nắng, chúng tôi sẽ đi ra bãi biển"

là một phép kéo theo được dùng trong ngôn ngữ thông thường, vì ở đây có mối quan hệ giữa giả thiết và kết luận. Hơn nữa, phép kéo theo này được xem là đúng trừ phi hôm nay trời thực sự nắng, nhưng chúng tôi không đi ra bãi biển. Trái lại, phép kéo theo

"Nếu hôm nay là thứ sáu, thì 2 + 3 = 5"

là đúng theo định nghĩa của phép kéo theo, vì kết luận là đúng (khi đó giá trị chân lý của giả thiết là không quan trọng). Phép kéo theo

"Nếu hôm nay là thứ sáu, thì 2 + 3 = 6"

là đúng với mọi ngày trừ thứ sáu, thậm chí mặc dù 2 + 3 = 6 là sai.

Trong ngôn ngữ tự nhiên chúng ta thường không dùng hai phép kéo theo sau trong ba ví dụ nêu ở trên, vì không có mối quan hệ giữa giả thiết và kết luận trong hai phép kéo theo đó. Trong suy luận toán học chúng ta xét các phép kéo theo thuộc loại tổng quát hơn trong ngôn ngữ thông thường. Khái niệm toán học về phép kéo theo độc lập với mối quan hệ nhân – quả giữa giả thiết và kết luận.

Không may, cấu trúc nếu – thì được dùng trong nhiều ngôn ngữ lập trình lại khác với cấu trúc được dùng trong logic học. Đa số các ngôn ngữ lập trình chứa những câu lệnh như nếu p thì S (**if** p **then** S) trong đó p là một mệnh đề còn S là một đoạn chương trình (gồm một hoặc nhiều

lệnh cần phải thực hiện). Khi thực hiện một chương trình gặp những cấu trúc như vậy, S sẽ được thực hiện nếu p là đúng, trong khi đó S sẽ không được thực hiện nếu p là sai. Điều này được minh hoạ trong ví dụ sau :

Ví dụ 6. Xác định giá trị của biến x sau câu lệnh :

if $2 + 2 = 4$ **then** $x := x + 1$

nếu trước câu lệnh đó $x = 0$? (Ở đây ký hiệu := là chỉ phép gán. Câu lệnh $x := x + 1$ có nghĩa là gán giá trị $x + 1$ cho biến x).

Giải : Vì $2 + 2 = 4$ là đúng nên câu lệnh gán $x := x + 1$ được thực hiện. Vì thế x sẽ có giá trị $0 + 1 = 1$ sau khi gặp câu lệnh này. ■

Chúng ta cũng có thể tạo các mệnh đề phức hợp bằng cách dùng toán tử phủ định và các liên từ khác nhau đã được định nghĩa ở trên. Các dấu ngoặc sẽ được dùng để chỉ định trật tự thực hiện các toán tử logic khác nhau trong một mệnh đề phức hợp. Đặc biệt, các toán tử logic nằm ở dấu ngoặc trong cùng sẽ được thực hiện trước tiên. Ví dụ, $(p \vee q) \wedge (\neg r)$ là hội của $p \vee q$ và $\neg r$. Để giảm bớt số các dấu ngoặc cần dùng, ta qui ước toán tử phủ định sẽ được thực hiện trước tất cả các toán tử logic khác. Điều này có nghĩa là $\neg p \vee q$ là hợp của $\neg p$ và q, tức là $(\neg p) \wedge q$, chứ không phải là phủ định của phép hợp của p và q, tức là $\neg(p \wedge q)$.

Có một số phép kéo theo liên quan có thể được tạo từ $p \to q$. Mệnh đề $q \to p$ được gọi là mệnh đề **đảo** của $p \to q$ và mệnh đề **phản đảo** của $p \to q$ là mệnh đề $\neg q \to \neg p$.

Ví dụ 7: Tìm các mệnh đề đảo và phản đảo của phép kéo theo

"Nếu hôm nay là thứ năm, thì hôm nay tôi có cuộc trắc nghiệm"

Giải : Mệnh đề đảo là :

"Nếu hôm nay tôi có cuộc trắc nghiệm,
thì hôm nay là thứ năm".

Và mệnh đề phản đảo là :

"Nếu hôm nay tôi không có cuộc trắc nghiệm
thì hôm nay không phải là thứ năm".

■

Bây giờ chúng tôi giới thiệu một cách nữa để tổ hợp các mệnh đề.

ĐỊNH NGHĨA 6. Cho p và q là hai mệnh đề. Mệnh đề *tương đương* $p \leftrightarrow q$ là mệnh đề chỉ đúng khi p và q có cùng giá trị chân lý và sai trong mọi trường hợp còn lại.

BẢNG 6. Bảng giá trị chân lý đối với mệnh đề tương đương $p \leftrightarrow q$

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

Bảng giá trị chân lý đối với $p \leftrightarrow q$ được cho trong Bảng 6. Chú ý rằng mệnh đề tương đương $p \leftrightarrow q$ là đúng chỉ khi hai mệnh đề kéo theo $p \rightarrow q$ và $q \rightarrow p$ đều đúng. Vì thế thuật ngữ :

"p nếu và chỉ nếu q"

là được dùng để chỉ phép tương đương này. Một số cách diễn đạt thường dùng nhất của mệnh đề $p \leftrightarrow q$ là "p là cần và đủ đối với q" và "nếu p thì q và ngược lại".

DỊCH NHỮNG CÂU THÔNG THƯỜNG

Có nhiều lý do để phải dịch những câu thông thường thành những biểu thức liên quan đến các biến mệnh đề và các liên từ logic. Tiếng Anh (cũng như tất cả các thứ tiếng khác của loài người) đều thường không rõ ràng. Dịch một câu thông thường ra các biểu thức logic là làm mất đi tính không rõ ràng đó. Chú ý rằng điều này có thể dẫn đến phải làm một tập hợp các giả thiết hợp lí dựa trên ý nghĩa hàm định của câu đó. Hơn nữa, một khi đã dịch những câu thông thường thành các biểu thức logic, chúng ta có thể phân tích các biểu thức logic đó để xác định các giá trị chân lý của chúng, có thể thao tác với chúng và chúng ta cũng có thể sử dụng những qui tắc suy diễn (sẽ được xét ở Chương 3) để suy luận về chúng.

Để minh hoạ quá trình dịch một câu thông thường thành các biểu thức logic, ta hãy xét ví dụ sau :

Ví dụ 8. Làm thế nào có thể dịch câu thông thường sau ra biểu thức logic ?

"Bạn không được lái xe máy nếu bạn cao dưới 1,5m
trừ phi bạn trên 18 tuổi".

Giải : Có nhiều cách để dịch câu này thành một biểu thức logic. Cách đơn giản nhất, nhưng lại kém ích lợi nhất là biểu diễn câu đó đơn giản chỉ là một biến mệnh đề đơn, ví dụ, p. Mặc dù điều này không sai, nhưng làm như vậy chẳng giúp ích gì cho ta, khi ta thử phân tích nó hoặc dùng nó để suy luận. Thích hợp hơn là nên dùng các biến mệnh đề để biểu diễn các bộ phận của câu đó và quyết định dùng các liên từ logic nào cho thích hợp để liên kết chúng. Đặc biệt, chúng ta cho q, r và s biểu diễn "Bạn được lái xe máy", "Bạn cao dưới 1,5m" và "Bạn trên 18 tuổi", tương ứng. Khi đó câu trên có thể được dịch thành :

$$(r \wedge \neg s) \rightarrow \neg q.$$

Tất nhiên, có nhiều cách khác để biểu diễn câu trên như một biểu thức logic, nhưng cách mà chúng tôi vừa đưa ra có lẽ đáp ứng được yêu cầu của chúng ta.

■

CÁC PHÉP TOÁN LOGIC VÀ CÁC PHÉP TOÁN BIT

Các máy tính dùng các bit để biểu diễn thông tin. Một **bit** có hai giá trị khả dĩ là 0 và 1. Ý nghĩa của từ này bắt nguồn từ hai từ tiếng Anh *b*inary dig*it* (số nhị phân) vì các số 0 và 1 là các số được dùng trong biểu diễn nhị phân của các số. Thuật ngữ này do nhà thống kế học nổi tiếng John Tukey đưa ra vào năm 1946. Bit cũng có thể được dùng để biểu diễn giá trị chân lý, vì giá trị chân lý cũng chỉ có hai giá trị là *đúng* và *sai*. Như người ta thường làm, chúng ta sẽ dùng bit 1 để biểu diễn giá trị đúng và bit 0 để biểu diễn giá trị sai. Một biến được gọi là **biến Boole** (Boolean variable) nếu giá trị của nó hoặc là đúng hoặc là sai. Do đó, cũng có thể dùng bit để biểu diễn một biến Boole.

Các **phép toán bit** trong máy tính tương ứng với các liên từ logic. Bằng cách thay đúng bằng 1 và sai bằng 0 trong các bảng giá trị chân lý đối với các toán tử $\wedge$, $\vee$ và $\oplus$, ta sẽ nhận được các phép toán bit tương ứng trong các bảng cho trong Bảng 7. Chúng ta sẽ dùng các ký hiệu OR, AND và XOR thay cho các toán tử $\vee$, $\wedge$ và $\oplus$ như thường được làm trong các ngôn ngữ lập trình khác nhau.

Thông tin thường được biểu diễn bằng cách dùng các xâu bit, đó là dãy các số 0 và 1. Khi đã làm như thế, các phép toán trên các xâu bit cũng có thể được dùng để thao tác thông tin đó

BẢNG 7. Bảng cho các toán tử bit OR, AND và XOR

$\vee$	0	1	$\wedge$	0	1	$\oplus$	0	1
0	0	1	0	0	0	0	0	1
1	1	1	1	0	1	1	1	0

ĐỊNH NGHĨA 7. Một *xâu bit* (hoặc xâu nhị phân) là dãy không hoặc nhiều bit. *Chiều dài* của xâu là số các bit trong xâu đó.

Ví dụ 9. 101010011 là một xâu bit có chiều dài là 9. ■

Chúng ta có thể mở rộng các phép toán bit tới các xâu bit. Chúng ta định nghĩa các **OR bit, AND bit** và **XOR bit** đối với hai xâu bit có cùng chiều dài là các xâu có các bit của chúng là các OR, AND và XOR của các bit tương ứng trong hai xâu tương ứng. Chúng ta cũng dùng các ký hiệu $\vee$, $\wedge$ và $\oplus$ để biểu diễn các phép toán bit OR, AND và XOR, tương ứng. Chúng ta sẽ minh hoạ các phép toán bit trên các xâu bit bằng ví dụ sau :

Ví dụ 10. Tìm OR bit, AND bit và XOR bit đối với hai xâu 01101 10110 và 11000 11101 (ở đây và trong suốt cuốn sách này, các xâu bit sẽ được tách thành các khối, mỗi khối có 5 bit cho dễ đọc).

Giải : OR bit, AND bit và XOR bit của hai xâu này nhận được bằng cách lấy OR, AND và XOR của các bit tương ứng của hai xâu đó, cụ thể là :

01101 10110
11000 11101

11101 11111 $\vee$ OR bit

01000 10100 $\wedge$ AND bit

10101 01011 $\oplus$ XOR bit.

■

BÀI TẬP

1. Trong các câu dưới đây câu nào là một mệnh đề?

   a) Boston là thủ phủ của bang Massachusetts.

   b) Miami là thủ phủ của bang Florida.

   c) $2 + 3 = 5$

   d) $5 + 7 = 10$

   e) $x + 2 = 11$

   f) Hãy trả lời câu hỏi này.

   g) $x + y = y + x$ với mọi cặp số thực x và y.

2. Trong các câu sau đây câu nào là một mệnh đề? Xác định giá trị chân lý của các mệnh đề đó?

   a) Không được đi qua.

   b) Bây giờ là mấy giờ?

   c) Không có ruồi đen ở Maine.

   d) $4 + x = 5$.

   e) $x + 1 = 5$ nếu $x = 1$.

   f) $x + y = y + z$ nếu $x = z$.

3. Tìm phủ định của các mệnh đề sau :

   a) Hôm nay là thứ năm.

   b) Không có ô nhiễm ở New Jersey.

   c) $2 + 1 = 3$.

   d) Mùa hè ở Maine nóng và nắng.

4. Cho p và q là hai mệnh đề.

   p : Tôi đã mua vé xổ số tuần này.

   q : Tôi đã trúng giải độc đắc 1 triệu đô la vào hôm thứ sáu.

   Diễn đạt các mệnh đề sau bằng các câu thông thường :

   a) $\neg p$ b) $p \vee q$

   c) $p \rightarrow q$ d) $p \wedge q$

   e) $p \leftrightarrow q$ f) $\neg p \rightarrow \neg q$

g) $\neg p \wedge \neg q$ h) $\neg p \vee (p \wedge q)$.

5. Cho p và q là hai mệnh đề.

p : Nhiệt độ dưới không.

q : Tuyết rơi..

Dùng p và q và các liên từ logic viết các mệnh đề sau :

a) Nhiệt độ dưới không và tuyết rơi.

h) Nhiệt độ dưới không nhưng không có tuyết rơi.

c) Nhiệt độ không dưới không và không có tuyết rơi.

d) Có tuyết rơi hoặc nhiệt độ dưới không (hoặc cả hai).

e) Nếu nhiệt độ đưới không thì cũng có tuyết rơi.

f) Hoặc nhiệt độ dưới không hoặc có tuyết rơi nhưng sẽ không có tuyết rơi nếu nhiệt độ dưới không.

g) Nhiệt độ dưới không là điều kiện cần và đủ để có tuyết rơi.

6. Cho p, q và r là những mệnh đề :

p : Bạn bị cúm.

q : Bạn thi trượt kỳ thi cuối khoá.

r : Bạn được lên lớp.

Hãy diễn đạt những mệnh đề sau thành những câu thông thường.

a) $p \rightarrow q$ b) $\neg q \leftrightarrow r$

c) $q \rightarrow \neg r$ d) $p \vee q \vee r$

e) $(p \rightarrow \neg r) \vee (q \rightarrow \neg r)$ f) $(p \wedge q) \vee (\neg q \wedge r)$.

7. Cho p và q là hai mệnh đề

p : Bạn lái xe với tốc độ trên 65 dặm/h.

q : Bạn hị phạt vì vượt quá tốc độ cho phép.

Hãy viết các mệnh đề sau bằng cách dùng p và q và các liên từ logic.

a) Bạn không lái xe với tốc độ trên 65 dặm/h.

h) Bạn lái xe với tốc độ trên 65 dặm/h, nhưng bạn không bị phạt vì vượt quá tốc độ cho phép.

c) Bạn sẽ hị phạt vì vượt quá tốc độ cho phép nếu bạn lái xe với tốc độ trên 65 dặm/h.

d) Nếu bạn không lái xe với tốc độ trên 65 dặm/h thì bạn sẽ không bị phạt vì vượt quá tốc độ cho phép.

e) Lái xe với tốc độ trên 65 dặm/h là đủ để bị phạt vì vượt quá tốc độ cho phép.

f) Bạn bị phạt vì vượt quá tốc độ cho phép nhưng bạn không lái xe với tốc độ trên 65 dặm/h.

g) Mỗi lần bạn bị phạt vì vượt quá tốc độ cho phép là bạn đã lái xe với tốc độ trên 65 dặm/h.

8. Cho p, q và r là các mệnh đề

p : Bạn nhận được điểm giỏi trong kỳ thi cuối khoá.

q : Bạn làm hết các bài tập trong quyển sách này.

r : Bạn sẽ được công nhận là giỏi ở lớp này.

Hãy dùng p,q và r cùng với các liên từ logic để viết các mệnh đề sau:

a) Bạn được công nhận là giỏi ở lớp này, nhưng bạn không làm hết các bài tập ở quyển sách này.

b) Bạn nhận được điểm giỏi ở kỳ thi cuối khoá, bạn làm hết các bài tập trong quyển sách này và bạn được công nhận là giỏi ở lớp này.

c) Để được công nhận là giỏi ở lớp này bạn cần phải được điểm giỏi ở kỳ thi cuối khoá.

d) Bạn nhận được điểm giỏi ở kỳ thi cuối khoá, nhưng bạn không làm hết các bài tập ở quyển sách này, tuy nhiên bạn vẫn được công nhận là giỏi ở lớp này.

e) Nhận được điểm giỏi ở kỳ thi cuối khoá và làm hết những bài tập ở quyển sách này là đủ để bạn được công nhận là giỏi ở lớp này.

f) Bạn sẽ được công nhận là giỏi ở lớp này, nếu và chỉ nếu bạn làm hết các bài tập trong quyển sách này hoặc nhận được điểm giỏi ở kỳ thi cuối khoá.

9. Đối với các câu sau đây, hãy cho hiết các câu đó sẽ có ý nghĩa nào nếu liên từ hoặc ở đây sắc thái nghĩa bao hàm (tức là tuyển) so với liên từ hoặc có sắc thái nghĩa loại trừ? Theo bạn trong hai nghĩa đó, nghĩa nào là nghĩa hàm định?

a) Để theo học môn toán học rời rạc, bạn cần phải đã học giải tích hoặc một khoá tin học.

b) Khi bạn mua một chiếc xe mới của hãng Acme Motor hạn sẽ được bớt lại 2000 USD tiền mặt hoặc được nợ 2% giá trị chiếc xe.

c) Bữa ăn tối gồm hai món ở cột A hoặc ba món ở cột B.

d) Trường sẽ đóng cửa nếu tuyết rơi dày hơn 2m hoặc gió lạnh dưới -100.

10. Một nhà thám hiểm bị một nhóm người ăn thịt người bắt cóc. Có hai loại người ăn thịt người : loại luôn luôn nói thật và loại luôn luôn nói dối. Họ sẽ nướng sống nhà thám hiểm nếu ông không xác định được một người nào đó trong họ là luôn luôn nói dối hay nói thật. Ông được phép hỏi người đó chỉ một câu hỏi.

a) Hãy giải thích tại sao câu hỏi "Anh là người nói dối?" không mang lại kết quả?

b) Tìm câu hỏi mà nhà thám hiểm đã dùng để xác định người ăn thịt người đó là luôn luôn nói dối hay nói thật.

11. Hãy viết những câu sau dưới dạng "nếu p thì q"
(*Gợi ý* : Tham khảo các cách thường dùng để diễn đạt phép kéo theo đã được liệt kê trong Tiết này.

a) Có tuyết rơi mỗi khi có gió Đông Bắc.

b) Các cây táo sẽ nở hoa nếu trời ấm kéo dài một tuần.

c) Việc đội Pistons dành chức vô địch ngụ ý rằng họ đã đánh bại đội Lakers.

d) Cần phải đi 8 dặm nữa mới tới được đỉnh núi Long.

e) Để được phong giáo sư, nổi tiếng thế giới là đủ.

f) Nếu bạn cho xe chạy hơn 400 dặm, bạn sẽ cần phải mua xăng.

g) Giấy bảo hành của bạn còn hiệu lực nếu bạn đã mua chiếc đầu CD của bạn ít hơn 90 ngày trước đây.

12. Viết các mệnh đề sau dưới dạng "p nếu và chỉ nếu q" trong ngôn ngữ thông thường.

a) Để nhận được điểm giỏi trong khoá học này cần và đủ là phải học giải được các bài tập của toán học rời rạc.

b) Nếu bạn đọc báo mỗi ngày bạn sẽ thạo tin tức và ngược lại.

c) Trời mưa nếu là ngày cuối tuần và là ngày cuối tuần nếu trời mưa.

d) Bạn có thể nhìn thấy lão phù thuỷ nếu lão không ở trong đó và lão phù thuỷ không ở trong đó nếu bạn nhìn thấy lão.

13. Phát biểu mệnh đề đảo và phản đảo của các mệnh đề kéo theo sau :

a) Nếu hôm nay tuyết rơi, ngày mai tôi sẽ đi trượt tuyết.

b) Tôi tới lớp mỗi khi sắp có kỳ thi.

c) Một số nguyên dương là số nguyên tố nếu nó không có một ước số nào khác 1 và chính nó.

14. Phát biểu mệnh đề đảo và phản đảo của các mệnh đề kéo theo sau :

a) Nếu đêm nay có tuyết rơi, tôi sẽ ở nhà.

b) Tôi đều đi ra bãi tắm bất cứ ngày nào trời nắng.

c) Khi tôi ở lại muộn, cần phải để tôi ngủ đến trưa.

15. Lập bảng giá trị chân lý đối với các mệnh đề phức hợp sau :

a) $p \wedge \neg p$ b) $p \vee \neg p$

c) $(p \vee \neg q) \rightarrow q$ d) $(p \vee q) \rightarrow (p \wedge q)$

e) $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ f) $(p \rightarrow q) \rightarrow (q \rightarrow p)$.

16. Lập bảng giá trị chân lý cho các mệnh đề phức hợp sau :

a) $p \oplus q$ b) $p \oplus \neg p$

c) $p \oplus \neg q$ d) $\neg p \oplus \neg q$

e) $(p \oplus q) \vee (p \oplus \neg q)$ f) $(p \oplus q) \wedge (p \oplus \neg q)$

17. Lập bảng giá trị chân lý cho các mệnh đề phức hợp sau

a) $p \rightarrow \neg q$ h) $\neg p \leftrightarrow q$

c) $(p \rightarrow q) \vee (\neg p \rightarrow q)$ d) $(p \rightarrow q) \wedge (\neg p \rightarrow q)$

e) $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$ f) $(\neg p \leftrightarrow \neg q) \leftrightarrow (p \leftrightarrow q)$

18. Lập bảng giá trị chân lý cho các mệnh đề phức hợp sau :

a) $(p \vee q) \vee r$ b) $(p \vee q) \wedge r$

c) $(p \wedge q) \vee r$ d) $(p \wedge q) \wedge r$

e) $(p \vee q) \wedge \neg r$ f) $(p \wedge q) \vee \neg r$

19. Lập bảng giá trị chân lý cho các mệnh đề phức hợp sau :

a) $p \rightarrow (\neg q \vee r)$ h) $\neg p \rightarrow (q \rightarrow r)$

c) $(p \rightarrow q) \vee (\neg p \rightarrow r)$ d) $(p \rightarrow q) \wedge (\neg p \rightarrow r)$

e) $(p \leftrightarrow q) \vee (\neg q \leftrightarrow r)$ f) $(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$

20. Xác định giá trị của x sau mỗi khi gặp câu lệnh dưới đây trong một chương trình máy tính, nếu trước khi tới câu lệnh đó $x = 1$.

a) **if** 1 + 2 = 3 **then** x := x + 1.

b) **if** (1 + 1 = 3) OR (2 + 2 = 3) **then** $x := x + 1$.

c) if (2 + 3 = 5) AND (3 + 4 = 7) **then** $x := x + 1$.

d) **if** (1 + 1 = 2) XOR (1 + 2 = 3) **then** $x := x + 1$.

e) **if** $x < 2$ **then** $x := x + 1$.

21. Tìm các OR bit, AND bit và XOR bit của các cặp xâu bit sau :

a) 10 11110 ; 01 00001

b) 111 10000 ; 101 01010

c) 00011 10001 ; 10010 01000

d) 11111 11111 ; 00000 00000

22. Xác định các biểu thức sau :

a) 11000 $\wedge$ (01011 $\vee$ 11011)

b) (01111 $\wedge$ 10101) $\vee$ 01000

c) (01010 $\oplus$ 11011) $\oplus$ 01000

d) (11011 $\vee$ 01010) $\wedge$ (10001 $\vee$ 11011)

Logic mờ *được sử dụng trong trí tuệ nhân tạo. Trong logic mờ, giá trị chân lý của một mệnh đề là một số nằm giữa 0 và 1. Một mệnh đề với giá trị chân lý 0 là sai, và giá trị chân lý 1 là đúng. Còn giá trị chân lý nằm giữa 0 và 1 chỉ ra mức độ thay đổi của chân lý. Ví dụ, giá trị chân lý 0,8 có thể được gán cho mệnh đề "Fred hạnh phúc" vì phần lớn thời gian Fred sống hạnh phúc, giá trị chân lý 0,4 có thể được gán cho mệnh đề "John hạnh phúc" vì John hạnh phúc gần một nửa thời gian.*

23. Giá trị chân lý của phủ định một mệnh đề trong logic mờ là hiệu của 1 và giá trị chân lý của mệnh đề đó. Hãy xác định giá trị chân lý của mệnh đề "Fred không hạnh phúc" và "John không hạnh phúc".

24. Giá trị chân lý của hợp hai mệnh đề trong logic mờ là giá trị chân lý nhỏ nhất của hai mệnh đề đó. Hãy xác định giá trị chân lý của các mệnh đề sau "Fred và John đều hạnh phúc" và "Cả Fred và John đều không hạnh phúc".

25. Giá trị chân lý của tuyển hai mệnh đề trong logic mờ là giá trị chân lý lớn nhất của hai mệnh đề đó. Xác định giá trị chân lý của các mệnh đề sau : "Fred hạnh phúc hoặc John hạnh phúc" và "Fred không hạnh phúc hoặc John không hạnh phúc".

26. Khẳng định "Mệnh đề này sai" có là một mệnh đề không?

Một tập hợp các biểu thức mệnh đề được gọi là phi mâu thuẫn (hay nhất quán) nếu có một sự gán các giá trị chân lý cho các biến trong những biểu thức đó làm cho mỗi biểu thức đó đều đúng. Khi cho những đặc điểm của một hệ thống thì điều quan trọng là những đặc điểm đó phải phi mâu thuẫn.

27. Các đặc điểm sau có phi mâu thuẫn không?
"Hệ thống ở trạng thái nhiều người dùng nếu và chỉ nếu nó hoạt động hình thường. Nếu một hệ thống hoạt động hình thường thì hạt nhân của nó cũng hoạt động. Hạt nhân không hoạt động hoặc hệ thống ở mode ngắt. Nếu hệ thống không ở trạng thái nhiều người dùng thì nó là ở mode ngắt. Hệ thống không ở mode ngắt".

28. Các đặc điểm sau có phi mâu thuẫn không? "Nếu hệ thống tệp không hị khóa thì các thông báo mới sẽ phải xếp hàng (chờ đợi). Nếu hệ thống tệp không hị khóa thì hệ thống đó sẽ hoạt động hình thường và ngược lại. Nếu các thông háo mới không phải xếp hàng (chờ đợi) thì chúng sẽ được gửi tới bộ đệm thông báo. Nếu hệ thống tệp không hị khóa, thì các thông báo mới sẽ được gửi tới bộ đệm thông báo. Các thông báo mới sẽ không được gửi tới bộ đệm thông báo.

1.2. SỰ TƯƠNG ĐƯƠNG CỦA CÁC MỆNH ĐỀ

MỞ ĐẦU

Một bước quan trọng được đùng trong lập luận toán học là thay một mệnh đề này bằng một mệnh đề khác có cùng giá trị chân lý. Vì thế, các phương pháp tạo ra các mệnh đề có cùng giá trị chân lý với một

mệnh đề phức hợp đã cho được dùng rất rộng rãi trong việc xây dựng các lập luận toán học.

Chúng ta sẽ bắt đầu bằng việc phân loại các mệnh đề phức hợp theo các giá trị chân lý khả đĩ của chúng.

ĐỊNH NGHĨA 1. Một mệnh đề phức hợp mà luôn luôn đúng bất kể các giá trị chân lý của các mệnh đề thành phần của nó được gọi là *hằng đúng* (tautology). Một mệnh đề mà luôn luôn sai được gọi là *mâu thuẫn*. Cuối cùng, một mệnh đề không phải là hằng đúng, cũng không phải là mâu thuẫn được gọi là *tiếp liên* (contingency).

Hằng đúng và mâu thuẫn thường là quan trọng trong các suy luận toán học. Các ví dụ dưới đây minh họa cho các loại mệnh đề trên.

Ví dụ 1. Chúng ta có thể xây dựng các ví dụ về các mệnh đề hằng đúng và mâu thuẫn bằng cách chỉ dùng một mệnh đề. Hãy xét bảng giá trị chân lý của $p \vee \neg p$ và $p \wedge \neg p$ cho trong Bảng 1. Vì $p \vee \neg p$ là luôn luôn đúng vậy nó là hằng đúng. Vì $p \wedge \neg p$ là luôn luôn sai, nên nó là mâu thuẫn.

■

BẢNG 1. Ví dụ về mệnh đề hằng đúng và mệnh đề mâu thuẫn

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

TƯƠNG ĐƯƠNG LOGIC

Các mệnh đề phức hợp luôn luôn có cùng giá trị chân lý được gọi là **tương đương logic**. Ta có thể định nghĩa khái niệm này như sau.

ĐỊNH NGHĨA 1. Các mệnh đề p và q được gọi là *tương đương logic* nếu $p \leftrightarrow q$ là hằng đúng.

Ký hiệu $p \Leftrightarrow q$ để chỉ p và q là tương đương logic.

Một cách để xác định hai mệnh đề có tương đương hay không là dùng bảng giá trị chân lý. Đặc biệt, các mệnh đề p và q là tương đương nếu

và chỉ nếu các cột cho giá trị chân lý của chúng phù hợp với nhau. Ví dụ sau đây minh họa phương pháp này.

BẢNG 2. Bảng chân lý đối với $\neg(p \vee q)$ và $\neg p \wedge \neg q$

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Ví dụ 2. Chứng minh rằng $\neg(p \vee q)$ và $\neg p \wedge \neg q$ là tương đương logic. Sự tương đương này là một trong số các luật De Morgan đối với các mệnh đề, các luật này được gọi theo tên nhà toán học Anh Augustus De Morgan, giữa thế kỷ 19.

Giải : Bảng giá trị chân lý đối với các mệnh đề này được cho trong Bảng 2. Vì bảng giá trị chân lý của các mệnh đề $\neg(p \vee q)$ và $\neg p \wedge \neg q$ phù hợp với nhau đối với mọi tổ hợp khả dĩ các giá trị chân lý của p và q, suy ra hai mệnh đề này là tương đương logic.

■

BẢNG 3. Bảng giá trị chân lý đối với $\neg p \vee q$ và $p \rightarrow q$

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Ví dụ 3. Chứng minh rằng $p \rightarrow q$ và $\neg p \vee q$ là tương đương logic.

Giải : Chúng ta lập bảng chân lý cho các mệnh đề này trong Bảng 3. Vì các giá trị chân lý của $\neg p \vee q$ và $p \rightarrow q$ phù hợp nhau, nên các mệnh đề này là tương đương logic.

■

Ví dụ 4. Chứng minh rằng các mệnh đề $p \vee (q \wedge r)$ và $(p \vee q) \wedge (p \vee r)$ là tương đương logic. Đây là luật phân bố của phép tuyển đối với phép hợp.

Giải : Bảng giá trị chân lý của các mệnh đề đó cho trong Bảng 4. Vì giá trị chân lý của các mệnh đề $p \vee (q \wedge r)$ và $(p \vee q) \wedge (p \vee r)$ là phù hợp nhau nên chúng là tương đương logic.

■

BẢNG 4. Một cách chứng minh p ∨ (q ∧ r) và (p ∨ q) ∧ (p ∨ r) là tương đương logic

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

Chú ý : Bảng chân lý của một mệnh đề phức hợp gồm ba mệnh đề thành phần khác nhau đòi hỏi phải có 8 hàng, mỗi hàng cho một tổ hợp khả dĩ các giá trị chân lý của ba mệnh đề đó. Nói chung, một mệnh đề phức hợp gồm n mệnh đề thành phần khác nhau đòi hỏi phải có 2^n hàng.

Bảng 5 cho một số tương đương logic quan trọng. Trong các tương đương đó, **T** là ký hiệu mệnh đề bất kỳ là đúng và **F**– ký hiệu mệnh đề sai. Yêu cầu độc giả kiểm tra lại các tương đương đó trong những bài tập ở cuối Tiết này.

Luật kết hợp đối với phép tuyển chứng tỏ rằng biểu thức $p \vee q \vee r$ là hoàn toàn xác định, theo nghĩa là kết quả sẽ không thay đổi bất kể trước hết ta lấy tuyển giữa p và q rồi sau đó lấy tuyển của $p \vee q$ và r hay trước hết ta lấy tuyển của q và r rồi sau đó mới lấy tuyển p và $q \vee r$. Tương tự, biểu thức $p \wedge q \wedge r$ cũng hoàn toàn xác định. Mở rộng suy luận trên, ta suy ra rằng $p_1 \vee p_2 \vee \ldots \vee p_n$ và $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ là hoàn toàn xác định nếu p_1, p_2 ... p_n là các mệnh đề. Hơn nữa, chú ý rằng luật De Morgan cũng được mở rộng thành :

$$\neg(p_1 \vee p_2 \vee \ldots \vee p_n) \Leftrightarrow (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n)$$

và $$\neg(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Leftrightarrow (\neg p_1 \vee \neg p_2 \vee \ldots \vee \neg p_n).$$

(Các phương pháp chứng minh những đẳng thức này sẽ được trình bày trong Chương 3).

Các tương đương logic cho trong Bảng 5, cũng như các tương đương khác đã được thiết lập (như được cho trong Bảng 6) lại có thể được dùng để lập các tương đương logic bổ sung. Bởi vì một mệnh đề trong một mệnh đề phức hợp có thể được thay thế bằng một mệnh đề khác tương đương với nó mà không làm thay đổi giá trị chân lý của mệnh đề phức hợp đang xét. Kỹ thuật này sẽ được minh họa trong Ví dụ 5 và 6 ở đó chúng ta cũng dùng tính chất nói rằng nếu p và q là tương đương logic và q và r là tương đương logic thl p và r cũng là tương đương logic (xem Bài tập 40).

BẢNG 5. Các tương đương logic

TƯƠNG ĐƯƠNG	TÊN GỌI
$p \wedge \mathbf{T} \Leftrightarrow p$ $p \vee \mathbf{F} \Leftrightarrow p$	Luật đồng nhất
$p \vee \mathbf{T} \Leftrightarrow \mathbf{T}$ $p \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$	Luật nuốt
$p \vee p \Leftrightarrow p$ $p \wedge p \Leftrightarrow p$	Luật lũy đẳng
$\neg(\neg p) \Leftrightarrow p$	Luật phủ định kép
$p \vee q \Leftrightarrow q \vee p$ $p \wedge q \Leftrightarrow q \wedge p$	Luật giao hoán
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	Luật kết hợp
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Luật phân phối
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	Luật De Morgan

BẢNG 6. Một số tương đương tiện ích
$p \vee \neg p \Leftrightarrow \mathbf{T}$
$p \wedge \neg p \Leftrightarrow \mathbf{F}$
$(p \rightarrow q) \Leftrightarrow (\neg p \vee q)$

Ví dụ 5. Chứng minh rằng $\neg(p \vee (\neg p \wedge q))$ và $\neg p \wedge \neg q$ là tương đương logic.

Giải : Chúng ta có thể dùng bảng chân lý để chứng minh sự tương đương của các mệnh đề trên. Tuy nhiên, thay vì thế, ta sẽ phát triển một chuỗi các tương đương logic, mỗi lần dùng một tương đương cho trong Bảng 5, bắt đầu với $\neg(p \vee (\neg q \wedge q))$ và kết thúc với $\neg p \wedge \neg q$. Ta có các tương đương sau :

$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q)$ theo Luật De Morgan thứ hai

$\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q]$ theo Luật De Morgan thứ nhất

$\Leftrightarrow \neg p \wedge [p \vee \neg q]$ theo Luật phủ định kép.

$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q)$ theo Luật phân phối.

$\Leftrightarrow \mathbf{F} \vee (\neg p \wedge \neg q)$ Vì $\neg p \wedge p \Leftrightarrow \mathbf{F}$

$\Leftrightarrow (\neg p \wedge \neg q) \vee \mathbf{F}$ theo Luật giao hoán đối với phép tuyển

$\Leftrightarrow \neg p \wedge \neg q$ theo Luật đồng nhất đối với **F**

Vậy $\neg(p \vee (\neg p \wedge q))$ và $\neg p \wedge \neg q$ là tương đương logic.

■

Ví dụ 6. Chứng minh rằng $(p \wedge q) \rightarrow (p \vee q)$ là hằng đúng.

Giải : Để chứng minh một mệnh đề là hằng đúng, ta sẽ dùng các tương đương logic để chứng tỏ rằng nó tương đương logic với **T** (*Chú ý* : Điều này cũng có thể làm được bằng cách lập bảng chân lý).

$(p \wedge q) \rightarrow (p \vee q) \Leftrightarrow \neg(p \wedge q) \vee (p \vee q)$ theo Ví dụ 3

$\Leftrightarrow (\neg p \vee \neg q) \vee (p \vee q)$ theo Luật De Morgan thứ nhất

$\Leftrightarrow (\neg p \vee p) \vee (\neg q \vee q)$ theo Luật kết hợp và giao hoán đối với phép tuyển

$\Leftrightarrow \mathbf{T} \vee \mathbf{T}$ theo Ví dụ 1 và Luật giao hoán đối với phép tuyển

$\Leftrightarrow \mathbf{T}$ theo Luật nuốt.

BÀI TẬP

1. Dùng bảng chân lý để chứng minh các tương đương sau :

a) $p \wedge \mathbf{T} \Leftrightarrow p$

b) $p \vee \mathbf{F} \Leftrightarrow p$

c) $p \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$

d) $p \vee \mathbf{T} \Leftrightarrow \mathbf{T}$

e) $p \vee p \Leftrightarrow p$

f) $p \wedge p \Leftrightarrow p$

2. Chứng minh rằng $\neg(\neg p)$ và p là tương đương logic.

3. Dùng bảng chân lý để chứng minh luật giao hoán :

a) $p \vee q \Leftrightarrow q \vee p$

b) $p \wedge q \Leftrightarrow q \wedge p$

4. Dùng bảng chân lý để chứng minh luật kết hợp :

a) $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

b) $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

5. Dùng bảng chân lý để chứng minh luật phân phối :

$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

6. Dùng bảng chân lý để chứng minh tương đương :

$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

7. Dùng bảng chân lý chứng minh các mệnh đề kéo theo sau là hằng đúng :

a) $(p \wedge q) \rightarrow p$

b) $p \rightarrow (p \vee q)$

c) $\neg p \rightarrow (p \rightarrow q)$

d) $(p \wedge q) \rightarrow (p \rightarrow q)$

e) $\neg(p \rightarrow q) \rightarrow p$

f) $\neg(p \rightarrow q) \rightarrow \neg q$

8. Bằng cách dùng bảng chân lý chứng minh rằng các mệnh đề kéo theo sau là hằng đúng :

a) $[\neg p \wedge (p \vee q)] \rightarrow q$

b) $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow p \rightarrow r)$

c) $[p \wedge (p \rightarrow q)] \rightarrow q$

d) $[(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)] \rightarrow r$

9. Làm lại Bài tập 7 nhưng không dùng các bảng chân lý.

10. Làm lại Bài tập 8 nhưng không dùng các bảng chân lý.

11. Chứng minh các tương đương được gọi là **luật hấp thụ** sau :

a) $[p \vee (p \wedge q)] \Leftrightarrow p$

b) $[p \wedge (p \vee q)] \Leftrightarrow p.$

12. Xác định xem $(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$ có phải là hằng đúng không?

13. Cũng hỏi như trên với mệnh đề $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$

14. Chứng minh rằng $p \leftrightarrow q$ và $(p \wedge q) \vee (\neg p \wedge \neg q)$ là tương đương.

15. Chứng minh rằng $(p \rightarrow q) \rightarrow r$ và $p \rightarrow (q \rightarrow r)$ là không tương đương.

16. Chứng minh rằng $p \rightarrow q$ và $\neg q \rightarrow \neg p$ là tương đương.

17. Chứng minh rằng $\neg p \leftrightarrow q$ và $p \leftrightarrow \neg q$ lả tương đương.

18. Chứng minh rằng $\neg(p \oplus q)$ và $p \leftrightarrow q$ là tương đương.

19. Chứng minh rằng $\neg(p \leftrightarrow q)$ và $\neg p \leftrightarrow q$ là tương đương.

Đối ngẫu *của một mệnh đề phức hợp chỉ chứa các toán tử logic* $\vee$, $\wedge$ *và* $\neg$ *là một mệnh đề nhận được bằng cách thay mỗi* $\vee$ *bằng* $\wedge$, *mỗi* $\wedge$ *bằng* $\vee$, *mỗi* **T** *bằng* **F** *và mỗi* **F** *bằng* **T**. *Đối ngẫu của* s *được ký hiệu là* s^*.

20. Tlm đối ngẫu của các mệnh đề sau :

a) $p \wedge \neg q \wedge \neg r$

b) $(p \wedge q \wedge r) \vee s$

c) $(p \vee \mathbf{F}) \wedge (q \vee \mathbf{T})$

21. Chứng minh rằng $(s^*)^* = s$.

22. Chứng minh rằng các tương đương logic trong Bảng 5, trừ luật phủ định kép, đều đi từng cặp, mỗi cặp chứa hai mệnh đề là đối ngẫu của nhau.

23.** Tại sao đối ngẫu của hai mệnh đề phức hợp tương đương cũng là tương đương, nếu các mệnh đề phức hợp đó chỉ chứa các toán tử $\vee$, $\wedge$ và $\neg$?

24. Lập mệnh đề phức hợp gồm các mệnh đề p, q và r sao cho nó đúng khi p và q là đúng và r là sai, nhưng là sai trong mọi trường hợp còn lại (*Gợi ý* : Dùng hợp của mỗi mệnh đề hoặc phủ định của nó).

25. Lập mệnh đề phức hợp gồm các mệnh đề p, q và r sao cho nó đúng chỉ khi hai trong ba mệnh đề p, q, và r là đúng và sai trong mọi trường hợp còn lại. (*Gợi ý* : Lập tuyển các hội. Đối với mỗi tổ hợp các giá trị sao cho mệnh đề là đúng, ta đưa vào một hội. Mỗi một hội này lại chứa ba mệnh đề p, q, r hoặc phủ định của chúng).

26. Giả sử rằng bảng chân lý với n biến mệnh đề đã được cho trước đầy đủ các giá trị chân lý. Chứng minh rằng một mệnh đề phức hợp tương ứng với bảng giá trị chân lý đó có thể tạo thành bằng cách lấy tuyển các hội của các biến hoặc phủ định của chúng. Đối với mỗi tổ hợp các giá trị sao cho mệnh đề phức hợp là đúng ta đưa vào một hội. Mệnh đề kết quả tạo thành được gọi là có **dạng tuyển chuẩn tắc.**

Một tập hợp các toán tử logic được gọi là **đầy đủ**, *nếu mỗi mệnh đề phức hợp đều tương đương logic với một mệnh đề chỉ chứa các toán tử logic đó.*

27. Chứng minh rằng $\vee$, $\wedge$ và $\neg$ tạo thành một tập hợp đầy đủ các toán tử logic. (*Gợi ý* : Dùng sự thật là mỗi mệnh đề đều tương đương logic với một mệnh đề ở dạng tuyển chuẩn tắc như đã được chứng minh trong Bài tập 26).

28*. Chứng minh rằng $\wedge$ và $\neg$ tạo nên một tập đầy đủ các toán tử logic (*Gợi ý* : Trước hết dùng luật De Morgan để chứng minh rằng $p \vee q$ tương đương với $\neg(\neg p \wedge \neg q)$.

29*. Chứng minh rằng $\neg$ và $\vee$ cũng tạo nên một tập đầy đủ các toán tử logic.

Các bài tập dưới đây liên quan đến các toán tử logic NAND và NOR. Mệnh đề p NAND q là đúng khi p hoặc q hoặc cả hai đều sai ; và nó là sai khi cả p và q đều đúng. Mệnh đề p NOR q là đúng khi cả p và q đều sai ; và sai trong các trường hợp còn lại. Các mệnh đề p NAND q và p NOR q được ký hiệu tương ứng là $p \mid q$ và $p \downarrow q$.

30. Lập bảng giá trị chân lý cho toán tử logic NAND.

31. Chứng minh rằng $p \mid q$ là tương đương logic với $\neg(p \wedge q)$.

32. Lập bảng giá trị chân lý của toán tử logic NOR.

33. Chứng minh rằng $p \downarrow p$ là tương đương logic với $\neg(p \vee q)$.

34. Trong bài tập này ta sẽ chứng minh rằng $\{\downarrow\}$ là một tập đầy đủ của các toán tử logic.

a) Chứng minh rằng $p \downarrow p$ là tương đương logic với $\neg p$

b) Chứng minh rằng $(p \downarrow q) \downarrow (p \downarrow q)$ tương đương logic với $p \vee q$.

c) Từ phần a, b và Bài tập 29 kết luận rằng $\{\downarrow\}$ là một tập hợp đầy đủ các toán tử logic.

35*. Tìm mệnh đề tương đương với $p \rightarrow q$ bằng cách chỉ dùng toán tử $\downarrow$.

36. Chứng minh rằng $\{\mid\}$ cũng là một tập đầy đủ các toán tử logic.

37. Chứng minh rằng $p \mid q$ và $q \mid p$ là tương đương.

38. Chứng minh rằng $p \mid (q \mid r)$ và $(p \mid q) \mid r$ là không tương đương, suy ra phép toán $\mid$ không có tính chất kết hợp.

39*. Có bao nhiêu bảng giá trị chân lý khác nhau của các mệnh đề phức hợp chứa hai mệnh đề p và q ?

40. Chứng minh rằng nếu p, q và r là những mệnh đề phức hợp sao cho p tương đương logic với q và q tương đương logic với r, thì p và r cũng tương đương logic.

41. Câu sau được trích từ bản ghi đặc điểm kỹ thuật của một hệ điện thoại : "Nếu cơ sở dữ liệu danh bạ được mở, thì monitor được đặt ở trạng thái đúng, nếu hệ không ở trạng thái ban đầu của nó". Câu này đọc thật khó hiểu vì nó liên quan tới hai phép kéo theo. Tìm một mệnh đề tương đương dễ hiểu hơn liên quan chỉ với các phép tuyển và phủ định, chứ không chứa phép kéo theo.

1.3. VỊ NGỮ VÀ LƯỢNG TỪ

MỞ ĐẦU

Các câu có liên quan đến các biến như :

"$x > 3$" ; "$x = y + 3$" và "$x + y = z$"

rất thường gặp trong các khẳng định toán học và trong các chương trình máy tính. Các câu này không đúng cũng không sai chừng nào các biến còn chưa được cho những giá trị xác định. Trong tiết này chúng ta sẽ xem xét các cách tạo ra những mệnh đề từ những câu như vậy.

Câu "x lớn hơn 3" có hai bộ phận. Bộ phận thứ nhất, tức là biến x, là chủ ngữ của câu. Bộ phận thứ hai "lớn hơn 3" - **là vị ngữ**, nó cho biết một tính chất mà chủ ngữ có thể có. Chúng ta có thể ký hiệu câu "x lớn hơn 3" là $P(x)$, với P ký hiệu vị ngữ "lớn hơn 3" và x là biến. Người ta cũng nói câu $P(x)$ là giá trị của **hàm mệnh đề** P tại x. Một khi biến x được gán cho một giá trị, thì câu $P(x)$ sẽ có giá trị chân lý. Ta hãy xét các ví dụ sau.

Ví dụ 1. Cho $P(x)$ là ký hiệu của câu "$x > 3$". Xác định giá trị chân lý của $P(4)$ và $P(2)$.

Giải : Mệnh đề $P(4)$ nhận được khi thay $x = 4$ vào câu "$x > 3$". Do đó $P(4)$ - tức là câu "$4 > 3$" - là đúng. Tuy nhiên $P(2)$ - tức là câu "$2 > 3$" - lại là sai.

■

Chúng ta cũng thường gặp những câu có nhiều biến hơn. Ví dụ, xét câu "$x = y + 3$". Chúng ta sẽ ký hiệu câu này là $Q(x, y)$, trong đó x, y là các biến và Q là vị ngữ. Khi các biến x và y được gán cho một giá trị xác định, câu $Q(x,y)$ sẽ có giá trị chân lý.

Ví dụ 2. Cho $Q(x,y)$ là ký hiệu của câu "$x = y + 3$". Xác định giá trị chân lý của các mệnh đề $Q(1,2)$ và $Q(3,0)$.

Giải : Để nhận được $Q(1,2)$ ta đặt $x = 1$ và $y = 2$ vào câu $Q(x,y)$. Do đó, $Q(1,2)$ là mệnh đề "1 = 2 + 3", nó là sai. Câu $Q(3,0)$ là mệnh đề "3 = 0 + 3", nó là đúng.

■

Tương tự, ta có thể ký hiệu câu "$x + y = z$" là $R(x,y,z)$. Khi ta gán cho x, y, z các giá trị xác định, câu đó sẽ có giá trị chân lý.

Ví dụ 3. Xác định giá trị chân lý của các mệnh đề $R(1,2,3)$ và $R(0,0,1)$.

Giải : Mệnh đề $R(1,2,3)$ nhận được bằng cách đặt $x = 1$, $y = 2$ và $z = 3$ vào câu $R(x,y,z)$.

Ta thấy rằng $R(1,2,3)$ chính là mệnh đề "1 + 2 = 3", nó là đúng. Trong khi đó, $R(0,0,1)$ là mệnh đề "0 + 0 = 1", là sai.

■

Nói chung, câu có nhiều biến x_1, x_2 ..., x_n có thể được ký hiệu bởi :

$$P(x_1, x_2, ..., x_n)$$

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

Các hàm mệnh đề rất thường gặp trong máy tính, như ví dụ dưới đây.

Ví dụ 4. Xét câu :

if $x > 0$ **then** $x := x + 1$

Khi gặp câu này trong chương trình, giá trị của biến x ở điểm đó trong quá trình thực hiện chương trình sẽ được đặt vào $P(x)$, tức là đặt vào câu "$x > 0$". Nếu $P(x)$ là đúng đối với giá trị này của x, thì lệnh gán $x := x + 1$ sẽ được thực hiện và giá trị của x sẽ tăng lên 1. Nếu $P(x)$ là sai đối với giá trị đó của x, thì lệnh gán sẽ không được thực hiện và giá trị x không thay đổi.

LƯỢNG TỪ

Khi tất cả các biến trong một hàm mệnh đề đều được gán cho giá trị xác định, thì mệnh đề tạo thành sẽ có giá trị chân lý. Tuy nhiên, còn có một cách quan trọng khác để biến các hàm mệnh đề thành các mệnh đề, mà người ta gọi là **sự lượng hóa**. Ta sẽ xét ở đây hai loại lượng hóa (còn gọi là các lượng từ - ND), đó là lượng từ phổ dụng (cũng quen gọi là lượng từ "với mọi" - ND) và lượng từ tồn tại.

Có nhiều phát biểu toán học khẳng định rằng một tính chất nào đó đúng với mọi giá trị của biến trong một miền đặc biệt nào đó. Miền này được gọi là **không gian** hay **vũ trụ biện luận** (dưới đây ta sẽ gọi tắt là không gian - ND). Một câu như vậy sẽ được diễn đạt bằng lượng từ "với mọi". Lượng từ "với mọi" của một mệnh đề tạo nên một mệnh đề, mệnh đề này là đúng nếu và chỉ nếu $P(x)$ là đúng với mọi giá trị của x trong không gian. Không gian sẽ chỉ rõ các giá trị khả dĩ của biến x.

ĐỊNH NGHĨA 3. *Lượng từ "với mọi"* của $P(x)$ là mệnh đề "$P(x)$ đúng với mọi giá trị của x trong không gian".

Lượng từ "với mọi" của $P(x)$ được ký hiệu là : $\forall x\ P(x)$

Mệnh đề $\forall x\ P(x)$ cũng được diễn đạt như :

"Đối với mọi x $P(x)$"

Ví dụ 5. Diễn đạt câu

"Tất cả sinh viên ở lớp này đều đã học giải tích"

như một lượng từ "với mọi".

Giải : Cho $P(x)$ là ký hiệu của câu :

"x đã học giải tích"

Khi đó câu "Tất cả sinh viên ở lớp này đều đã học giải tích" có thể được viết như $\forall x\ P(x)$, ở đây không gian gồm tất cả các sinh viên trong lớp đó.

Câu trên cũng có thể được diễn đạt như sau :

$$\forall x\ (S(x) \longrightarrow P(x))$$

ở đây $S(x)$ là câu :

"x ở lớp này".

$P(x)$ vẫn như trước và không gian bây giờ là tập hợp tất cả sinh viên. ■

Ví dụ 5 cho thấy thường có nhiều cách để thể hiện một lượng từ.

Ví dụ 6. Cho $P(x)$ là hàm mệnh đề "$x + 1 > x$". Xác định giá trị chân lý của lượng từ $\forall x\ P(x)$, ở đây không gian là tập hợp các số thực.

Giải : Vì $P(x)$ đúng với mọi số thực x, nên lượng từ $\forall x\ P(x)$ là đúng. ■

Ví dụ 7. Cho $Q(x)$ là câu "$x < 2$". Xác định giá trị chân lý của lượng từ $\forall x\ P(x)$ với không gian là tập hợp các số thực.

Giải : $Q(x)$ là không đúng với mọi số thực x, vì, ví dụ, $Q(3)$ là sai. Do đó, $\forall x\ Q(x)$ là sai.

■

Khi tất cả các phần tử của không gian có thể được liệt kê ra, chẳng hạn như $x_1, x_2 \ldots x_n$, thì lượng từ "với mọi" giống hệt như phép hội

$$P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$$

vì phép hội này là đúng nếu và chỉ nếu $P(x_1), P(x_2), \ldots P(x_n)$ đều là đúng.

Ví dụ 8. Xác định giá trị của $\forall x\ P(x)$, với $P(x)$ là câu "$x^2 < 10$" và không gian bao gồm các số nguyên dương không vượt quá 4.

Giải : Câu $\forall x\ P(x)$ giống như là phép hội

$$P(1) \wedge P(2) \wedge P(3) \wedge P(4)$$

vì không gian ở đây gồm các số nguyên 1,2,3 và 4.

Vì P(4) – tức là mệnh đề "$4^2 < 10$" – là sai, suy ra $\forall x\ P(x)$ là sai.

■

Có nhiều phát biểu toán học khẳng định rằng có tồn tại một phần tử có một tính chất nào đó. Những câu như vậy được diễn đạt bằng cách dùng lượng từ tồn tại. Bằng lượng từ tồn tại, chúng ta lập được một mệnh đề, mệnh đề này là đúng nếu và chỉ nếu $P(x)$ là đúng ít nhất ở một giá trị của x trong không gian.

ĐỊNH NGHĨA 3. *Lượng từ tồn tại* của $P(x)$ là mệnh đề "Tồn tại một phần tử x trong không gian sao cho $P(x)$ là đúng ".

Lượng từ tồn tại của $P(x)$ được ký hiệu là : $\exists x\ P(x)$

Lượng từ tồn tại $\exists x\ P(x)$ cũng được diễn đạt như sau :

"Tồn tại một x sao cho $P(x)$"

"Tồn tại ít nhất một x sao cho $P(x)$"

hay "Đối với một x nào đó $P(x)$".

Ví dụ 9. Cho $P(x)$ là câu "$x > 3$". Tìm giá trị chân lý của $\exists x\ P(x)$ với không gian là tập hợp các số thực.

Giải : Vì "$x > 3$" là đúng, chẳng hạn với $x = 4$, nên lượng từ tồn tại của $P(x)$, $\exists x\ P(x)$, là đúng.

■

Ví dụ 10. Cho $Q(x)$ là câu "$x = x + 1$". Tìm giá trị chân lý của lượng từ $\exists x\ P(x)$, với không gian là tập hợp các số thực.

Giải : Vì $Q(x)$ là sai đối với mọi số thực x, nên lượng từ tồn tại của $Q(x)$, $\exists x\ Q(x)$, là sai.

BẢNG 1. Các lượng từ

MỆNH ĐỀ	KHI NÀO ĐÚNG ?	KHI NÀO SAI?
$\forall x\ P(x)$	$P(x)$ đúng với mọi x	Có một giá trị của x để $P(x)$ sai
$\exists x\ P(x)$	Có một giá trị của x để $P(x)$ đúng	$P(x)$ sai với mọi x

Khi tất cả các phần tử của không gian có thể được liệt kê ra, chẳng hạn x_1, x_2, ... x_n, thì lượng từ tồn tại $\exists x\ P(x)$ giống hệt như phép tuyển :

$$P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$$

vì phép tuyển này là đúng nếu và chỉ nếu có ít nhất một trong các $P(x_1)$, $P(x_2)$, ... $P(x_n)$ là đúng.

Ví dụ 11. Xác định giá trị chân lý của $\exists x\ P(x)$, với $P(x)$ là câu "$x^2 > 10$" và không gian gồm các số nguyên dương không lớn hơn 4.

Giải : Vì không gian là {1, 2, 3, 4}, mệnh đề $\exists x\ P(x)$ giống hệt như phép tuyển :

$$P(1) \vee P(2) \vee P(3) \vee P(4)$$

Vì $P(4)$ – tức là câu "$4^2 > 10$" – là đúng nên suy ra $\exists x\ P(x)$ là đúng.

■

Bảng 1 cho tóm tắt ý nghĩa của các lượng từ tồn tại và phổ dụng (tức "với mọi"}.

Khi xác định giá trị chân lý của một lượng từ, đôi khi sẽ rất hữu ích nếu chúng ta suy nghĩ lướt qua tất cả một vòng và tìm kiếm. Giả sử rằng ta có n phần tử trong không gian của biến x. Để xác định $\forall x\ P(x)$ có đúng không ta có thể lướt một vòng qua tất cả n giá trị đó của biến x để xem $P(x)$ có luôn luôn đúng không. Nếu chúng ta gặp một giá trị của x sao cho $P(x)$ là sai, thì chúng ta đã chứng minh được rằng

$\forall x\ P(x)$ là sai. Ngược lại, $\forall x\ P(x)$ là đúng. Để xem $\exists x\ P(x)$ có đúng không, chúng ta có thể lướt một vòng qua tất cả n giá trị của x và tìm kiếm một giá trị của x sao cho $P(x)$ đúng. Nếu tìm được một giá trị như vậy, thì $\exists x\ P(x)$ là đúng. Nếu không tìm được một giá trị nào như vậy của x thì chúng ta đã xác định được rằng $\exists x\ P(x)$ là sai. (Chú ý rằng quá trình tìm kiếm này sẽ không áp dụng được nếu không gian có vô số các giá trị. Tuy nhiên, đây vẫn còn là một cách suy nghĩ hữu ích về giá trị chân lý của các lượng từ).

DỊCH CÁC CÂU THÔNG THƯỜNG THÀNH CÁC BIỂU THỨC LOGIC

Trong Tiết 1.1 chúng ta đã mô tả quá trình dịch các câu thông thường thành các biểu thức logic chứa nhiều mệnh đề và các liên từ logic. Đến đây, sau khi đã thảo luận về các lượng từ, chúng ta có thể biểu diễn được một tập hợp rộng lớn hơn các câu thông thường thành các biểu thức logic. Làm như vậy cốt là để loại đi những điều mù mờ, chưa rõ ràng và làm cho ta có thể dùng các câu đó để suy luận được. (Tiết 3.1 sẽ trình hày các qui tắc suy luận đối với các biểu thức logic)

Các ví dụ sau đây cho thấy các toán tử logic và các lượng từ được dùng để diễn đạt các câu thông thường, tương tự như loại câu thường gặp trong các phát biểu toán học, trong việc lập trình logic và trí tuệ nhân tạo, như thế nào.

Ví dụ 12. Biểu diễn câu "Mọi người đều có chính xác một người bạn tốt nhất" thành một biểu thức logic.

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

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

■

Ví dụ 13. Biểu diễn câu : "Nếu một người nào đó là phụ nữ và đã sinh đẻ, thì người đó sẽ là mẹ của một người nào đó" thành một biểu thức logic.

Giải : Giả sử $F(x)$ là câu "x là phụ nữ" ; $P(x)$ là câu "x đã sinh đẻ" và $M(x,y)$ là câu "x là mẹ của y". Vì câu trong ví dụ áp đụng cho tất cả mọi người, nên ta có thể viết nó thành biểu thức sau :

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

■

CÁC VÍ DỤ CỦA LEWIS CARROLL (Tùy chọn)

Lewis Carroll (bút danh của C.L. Dodgson) là tác giả của cuốn truyện *Alice trong đất nước kỳ lạ* nổi tiếng thế giới, nhưng ông cũng là tác giả của một số công trình về logic ký hiệu. Các cuốn sách của ông chứa nhiều ví dụ về sự suy luận bằng cách dùng các lượng từ. Hai ví dụ ngay đưới đây lấy từ cuốn sách *Logic ký hiệu* của ông ; một ví dụ khác lấy từ cuốn sách đó được cho trong phần bài tập ở cuối tiết này. Các ví dụ này minh họa các lượng từ đã được sử dụng để diễn đạt các loại câu khác nhau như thế nào.

Ví dụ 14. Xét các câu sau. Hai câu đầu được gọi là *tiền đề* và câu thứ ba được gọi là *kết luận*. Toàn bộ tập hợp ba câu này được gọi là một *suy lí*

"Tất cả sư tử đều hung dữ"

"Một số sư tử không uống cà phê"

"Một số sinh vật hung dữ không uống cà phê".

(Trong Tiết 3.1 chúng ta sẽ bàn tới vấn đề xác định kết luận có là hệ quả đúng của các tiền đề hay không. Trong thí dụ này, thì có). Gọi $P(x)$, $Q(x)$ và $R(x)$ là các câu "x là sư tử", "x hung dữ" và "x uống cà phê", tương ứng. Giả sử rằng không gian là tập hợp toàn bộ các sinh vật, hãy diễn đạt các câu trong suy lý trên bằng cách dùng $P(x)$, $Q(x)$, $R(x)$ và các lượng từ.

Giải : Ta có thể biểu điễn các câu đó như sau :

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

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

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

Chú ý rằng câu thứ hai không thể viết là $\exists x \ (P(x) \rightarrow \neg R(x))$, bởi vì $P(x) \rightarrow \neg R(x)$ là đúng bất cứ khi nào x không phải là sư tử, do đó $\exists x$

$(P(x) \rightarrow \neg R(x))$ là đúng chừng nào còn có ít nhất một sinh vật không phải là sư tử, thậm chí mặc dù tất cả các sư tử đều uống cà phê. Tương tự, câu thứ ba không thể được viết là :

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

Ví dụ 15. Xét các câu sau, trong đó ba câu đầu là tiền đề và câu thứ tư là kết luận đúng.

"Tất cả chim ruồi đều có màu sặc sỡ"

"Không có con chim lớn nào sống bằng mật ong"

"Các chim không sống bằng mật ong đều có màu xám"

"Chim ruồi là nhỏ".

Gọi $P(x)$, $Q(x)$, $R(x)$ và $S(x)$ là các câu "x là chim ruồi" ; "x là lớn", "x sống bằng mật ong", và "x có màu sặc sỡ", tương ứng. Giả sử rằng không gian là tất cả các loại chim, hãy diễn đạt các câu trong suy lí trên bằng cách dùng $P(x)$, $Q(x)$, $R(x)$, $S(x)$ và các lượng từ.

Giải : Ta có thể biểu diễn các câu trong suy lí trên như sau :

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

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

$\forall x \ (\neg R(x) \rightarrow \neg \ S(x))$

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

(Chú ý ở đây chúng ta đã cho rằng "nhỏ" tức là "không lớn", và "màu xám" tức là "không có màu sặc sỡ". Để chứng tỏ câu thứ tư là một kết luận đúng của ba câu đầu tiên, chúng ta cần phải dùng các qui tắc suy luận sẽ được trình bày ở Tiết 3.1).

CÁC BIẾN BỊ RÀNG BUỘC

Khi một lượng từ được dùng đối với biến x hoặc khi chúng ta gán một giá trị cho hiến đó, chúng ta nói rằng sự thâm nhập này của biến là **bị ràng buộc**. Sự thâm nhập của một hiến không bị ràng buộc hoặc không được đặt bằng một giá trị đặc biệt nào đó được gọi là **tự do**. Tất cả các biến thâm nhập trong các hàm mệnh đề đều phải bị ràng huộc để biến nó thành một mệnh đề. Điều này được làm bằng cách dùng các lượng từ phổ dụng và tồn tại kết hợp với việc gán giá trị.

Nhiều phát biểu toán học chứa nhiều các lượng từ của các hàm mệnh đề và các hàm mệnh đề này lại chứa nhiều biến. Điều cần phải lưu ý là trật tự của các lượng từ này là rất quan trọng nếu tất cả các lượng từ không cùng là lượng từ phổ dụng hoặc cùng là lượng từ tồn tại. Điều này sẽ được minh hoạ trong các Ví dụ 16, 17 và 18. Trong các ví dụ đó, không gian của mỗi biến đều là tập hợp các số thực.

Ví dụ 16. Cho $P(x,y)$ là câu "$x + y = y + x$". Xác định giá trị chân lý của các lượng từ $\forall x\ \forall y\ P(x,y)$.

Giải : Lượng từ

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

là ký hiệu của mệnh đề :

"Với mọi số thực x và với mọi số thực y,
$x + y = y + x$ là đúng".

Vì $P(x,y)$ đúng với mọi số thực x và y, nên mệnh đề $\forall x \forall y\ P(x,y)$ là đúng ■

Ví dụ 17. Cho $Q(x,y)$ là câu "$x + y = 0$". Xác định giá trị chân lý của các lượng từ $\exists y\ \forall x\ Q(x,y)$ và $\forall x \exists y\ Q(x,y)$.

Giải : Lượng từ

$$\exists y \forall x\ Q(x,y)$$

là ký hiệu của mệnh đề :

"Tồn tại một số thực y sao cho với mọi số thực x,
$Q(x,y)$ là đúng".

Bất kể số y được chọn là bao nhiêu, chỉ có một giá trị của x thoả mãn $x + y = 0$. Vì không có một số thực y sao cho $x + y = 0$ đúng với mọi số thực x, nên mệnb đề $\exists y \forall x\ Q(x,y)$ là sai.

Lượng từ

$$\forall x \exists y\ Q(x,y)$$

là ký hiệu của cảu

"Với mọi số thực x, tồn tại một số thực y sao cho $Q(x,y)$ là đúng".

Với số thực x đã cho, luôn có một số thực y sao cho $x + y = 0$, cụ thể là $y = -x$. Từ đó suy ra mệnh đề $\forall x \exists y\ Q(x,y)$ là đúng.

■

Ví dụ 17 cho thấy rằng thứ tự xuất hiện khác nhau của các lượng từ có thể dẫn đến các kết quả khác nhau. Các mệnh đề $\exists x\ \forall y\ P(x, y)$ và $\forall y\ \exists x\ P(x, y)$ không phải là tương đương logic. Mệnh đề $\exists x\ \forall y\ P(x,y)$ là đúng nếu và chỉ nếu có một x làm cho $P(x,y)$ đúng với mọi y. Vì vậy để cho mệnh đề này đúng, cần phải có một giá trị đặc biệt của x để cho $P(x,y)$ là đúng bất kể chọn y bằng bao nhiêu. Mặt khác, mệnh đề $\forall y\ \exists x\ P(x,y)$ là đúng nếu và chỉ nếu với mọi giá trị của y có một giá trị của x sao cho $P(x, y)$ là đúng. Vì vậy, để cho mệnh đề này là đúng, bất kể giá trị của y được chọn như thế nào, cần phải có một giá trị của x (có thể phụ thuộc vào giá trị đã chọn của y) để $P(x,y)$ là đúng. Nói một cách khác, trong trường hợp thứ hai, y có thể phụ thuộc vào x, trong khi ở trường hợp thứ nhất x là hằng số độc lập với y.

Từ những nhận xét trên, suy ra rằng nếu $\exists x\ \forall y\ P(x,y)$ là đúng, thì $\forall y\ \exists x\ P(x,y)$ cũng cần phải đúng. Tuy nhiên, nếu $\forall y\ \exists x\ P(x, y)$ đúng thì không nhất thiết $\exists x\ \forall y\ P(x,y)$ phải là đúng. (Xem các Bài tập bổ sung 8 và 10 ở cuối chương này).

Khi làm việc với các lượng từ có nhiều biến, đôi khi sẽ rất hữu ích nếu chúng ta suy nghĩ bằng cách đi qua các vòng kín theo từng nhóm. (Tất nhiên, nếu đối với một biến nào đó mà không gian của nó có vô số phần tử, thì chúng ta không thể thực sự đi qua một vòng hết các phần tử đó được. Tuy nhiên, đây vẫn là cách suy nghĩ rất hữu ích để hiểu các lượng từ theo từng nhóm). Ví dụ, để xem $\forall x\ \forall y\ P(x,y)$ có đúng không, ta đi vòng hết các giá trị của x, rồi đối với mỗi một x, ta lại đi vòng hết các giá trị của y. Nếu ta thấy $P(x,y)$ đúng với mọi giá trị của x và y, là ta đã xác định được rằng $\forall x\ \forall y\ P(x,y)$ là đúng. Còn nếu chúng ta vấp phải một giá trị của y sao cho $P(x, y)$ là sai, thì như vậy chúng ta đã chứng minh được rằng $\forall x\ \forall y\ P(x,y)$ là sai.

Tương tự, để xác định xem $\forall x\ \exists y\ P(x,y)$ có đúng không, ta đi một vòng qua các giá trị của x. Đối với mỗi x, ta lại đi một vòng qua tất cả các giá trị của y, cho đến khi ta tìm được một y sao cho $P(x, y)$ là đúng. Nếu đối với mọi x chúng ta đều tìm được một y có tính chất đó, thì $\forall x\ \exists y\ P(x, y)$ là đúng. Còn nếu đối với một x nào đó chúng ta không tìm được một y như vậy thì $\forall x\ \exists y\ P(x,y)$ là sai.

Để xem $\exists x\ \forall y\ P(x, y)$ có đúng không, chúng ta đi một vòng hết các giá trị của x cho đến khi tìm được một x sao cho $P(x,y)$ luôn luôn đúng khi ta đi hết một vòng qua tất cả các giá trị của y. Nếu tìm được một x

có tính chất đó, thì ta biết được rằng $\exists x\ \forall y\ P(x,y)$ là đúng. Còn nếu không tìm được một x như vậy, thì $\exists x\ \forall y\ P(x,y)$ là sai.

BẢNG 2. Các lượng từ hai biến

MỆNH ĐỀ	KHI NÀO ĐÚNG?	KHI NÀO SAI ?
$\forall x\ \forall y\ P(x,y)$ $\forall y\ \forall x\ P(x,y)$	$P(x,y)$ đúng với mọi cặp (x,y)	Có một cặp (x,y) đối với nó $P(x,y)$ là sai
$\forall x\ \exists y\ P(x,y)$	Với mọi x, có một y sao cho $P(x,y)$ là đúng	Có một x sao cho $P(x,y)$ là sai với mọi y
$\exists x\ \forall y\ P(x,y)$	Có một x sao cho $P(x,y)$ đúng với mọi y	Với mọi x có một y sao cho $P(x,y)$ là sai
$\exists x\ \exists y\ P(x,y)$ $\exists y\ \exists x\ P(x,y)$	Có một cặp (x, y) sao cho $P(x,y)$ là đúng	$P(x,y)$ là sai đối với mọi cặp (x,y)

Cuối cùng, để xem $\exists x\ \exists y\ P(x,y)$ có đúng không, ta đi một vòng qua tất cả các giá trị của x, rồi đối với mỗi một x ta lại đi một vòng qua tất cả các giá trị của y cho đến khi tìm được một x, ở đó ta lại tìm được một y sao cho $P(x,y)$ là đúng. Mệnh đề $\exists x\ \exists y\ P(x,y)$ là sai nếu chúng ta không tìm được một x nào, ở đó tìm được một y sao cho $P(x,y)$ là đúng.

Bảng 2 tóm tắt ý nghĩa của các lượng từ hai biến khả dĩ.

Người ta cũng thường gặp các lượng từ có hơn hai biến, như Ví dụ 18 dưới đây.

Ví dụ 18. Cho $Q(x,y,z)$ là câu "$x + y = z$". Xác định giá trị chân lý của $\forall x\ \forall y\ \exists z\ Q(x,y,z)$ và $\exists z\ \forall x\ \forall y\ Q(x,y,z)$.

Giải : Giả sử x,y đã được gán giá trị. Khi đó tồn tại một giá trị z sao cho $x + y = z$. Vì vậy, lượng từ :

$$\forall x\ \forall y\ \exists z\ Q(x,y,z)$$

là ký hiệu của câu :

> "Đối với mọi số thực x và mọi số thực y, tồn tại một số thực z sao cho $x + y = z$" là đúng. Thứ tự của các lượng từ ở đây là quan trọng, vì lượng từ :

$$\exists z \ \forall x \ \forall y \ Q(x,y,z)$$

là ký hiệu của câu :

> "Có một số thực z sao cho với mọi số thực x và mọi số thực y đẳng thức $x + y = z$ là đúng" lại là một mệnh đề sai, vì không có một giá trị nào của z lại thoả mãn phương trình $x + y = z$ với mọi giá trị của x và y.

■

Ví dụ dưới đây minh hoạ các lượng từ có thể được dùng để diễn đạt các câu có nhiều biến như thế nào. Như ví dụ sẽ cho thấy, thường có nhiều cách để làm việc này.

Ví dụ 19. Dùng các lượng từ để diễn đạt câu :

"Có một phụ nữ đã bay một lần tất cả các tuyến bay trên thế giới".

Giải : Cho $P(w,f)$ là câu "w đã bay chuyến bay f" và $Q(f,a)$ là câu "f là chuyến bay trên tuyến a".

Ta có thể diễn đạt câu trong đầu bài như sau :

$$\exists w \ \forall a \ \exists f \quad (P(w,f) \ \wedge \ Q(f, \ a))$$

Ở đây không gian của w, f và a bao gồm tất cả phụ nữ trên thế giới, tất cả các chuyến bay và tất cả các tuyến bay, tương ứng.

Câu trên cũng có thể diễn đạt như sau :

$$\exists w \ \forall a \ \exists f \quad R(w, \ f, \ a)$$

Ở đây $R(w, \ f, \ a)$ là câu

"w đã đi chuyến bay f trên tuyến bay a".

Mặc dù, xem ra gọn hơn, nhưng nó vẫn có gì đó làm cho mối quan hệ giữa các biến thiếu rõ ràng. Do đó, cách thứ nhất vẫn được ưa dùng hơn.

Các lượng từ cũng thường được dùng để định nghĩa các khái niệm toán học. Một ví dụ khá quen thuộc với chúng ta, đó là khái niệm giới hạn, một khái niệm quan trọng của giải tích.

Ví dụ 20. Diễn đạt định nghĩa giới hạn bằng cách dùng các lượng từ.

Giải : Ta hãy nhớ lại rằng, định nghĩa của giới hạn :

$$\lim_{x \to a} f(x) = L$$

là : "Với mọi số thực $\varepsilon > 0$ tồn tại một số thực $\delta > 0$ sao cho $|f(x) - L| < \varepsilon$ khi $0 < |x - a| < \delta$" .

Định nghĩa này của giới hạn có thể được diễn đạt bằng cách dùng các lượng từ như sau :

$$\forall \varepsilon \; \exists \delta \; \forall x \; (0 < |x - a| < \delta \rightarrow |f(x) - L| < \varepsilon)$$

ở đây không gian đối với các biến δ và ε là tập các số thực dương, còn đối với x là tập các số thực.

■

Chúng ta cũng thường muốn xem xét phủ định của các biểu thức có chứa các lượng từ. Ví dụ, hãy xét phủ định của câu sau :

"Tất cả các sinh viên trong lớp đều đã học môn giải tích".

Câu này chính là một lượng từ phổ dụng, cụ thể là :

$$\forall x \; P(x)$$

ở đây $P(x)$ là câu "x đã học môn giải tích".

Phủ định của câu này là "Không phải tất cả các sinh viên ở lớp này đều đã học môn giải tích". Điều này tương đương với : "Có một sinh viên ở lớp này chưa học môn giải tích". Và đây đơn giản là lượng từ tồn tại của phủ định hàm mệnh đề ban đầu, cụ thể là :

$$\exists x \; \neg P(x)$$

Ví dụ này minh hoạ phép tương đương sau :

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

Giả sử chúng ta muốn lấy phủ định một lượng từ tồn tại. Ví dụ, xét câu" Có một sinh viên trong lớp đã học môn giải tích". Đây là lượng từ tồn tại

$$\exists x \; Q(x)$$

Với $Q(x)$ là câu "x đã học môn giải tích". Phủ định của câu này là mệnh đề : "Không có một sinh viên nào ở lớp này đã học môn giải tích". Điều này tương đương với "Mọi sinh viên ở lớp này đều chưa học môn giải tích". Đây chính là lượng từ phổ dụng của phủ định hàm mệnh đề ban đầu, hay viết theo ngôn ngữ các lượng từ :

$$\forall x \ \neg Q(x)$$

Ví dụ này minh hoạ sự tương đương

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

Phép phủ định các lượng từ được tóm tắt trong Bảng 3

BẢNG 3. Phủ định các lượng từ

PHỦ ĐỊNH	MỆNH ĐỀ TƯƠNG ĐƯƠNG	KHI NÀO PHỦ ĐỊNH LÀ ĐÚNG?	KHI NÀO SAI?
$\neg \exists x \ P(x)$	$\forall x \ \neg P(x)$	$P(x)$ sai với mọi x	Có một x để $P(x)$ là đúng.
$\neg \forall x \ P(x)$	$\exists x \ \neg P(x)$	Có một x để $P(x)$ là sai	$P(x)$ đúng với mọi x

BÀI TẬP

1. Cho $P(x)$ là câu "$x \leq 4$". Xác định giá trị chân lý của các mệnh đề sau:

   a) $P(0)$; b) $P(4)$; c) $P(6)$

2. Cho $P(x)$ là câu "từ x chứa chữ cái a". Xác định giá trị chân lý của các mệnh đề sau :

   a) P(orange) b) P(lemon)

   c) P(true) d) P(false)

3. Cho $Q(x,y)$ là câu "x là thủ phủ của y". Xác định giá trị chân lý của các mệnh đề sau :

   a) Q (Denver, Colorado)

   b) Q (Detroit, Michigan)

   c) Q (Massachusetts, Boston)

   d) Q (New York, New York)

4. Cho biết giá trị của x sau khi lệnh **if** $P(x)$ **then** $x := 1$ được thực hiện, biết rằng $P(x)$ là câu "$x > 1$" và giá trị của x khi tới câu lệnh này là :

   a) $x = 0$ b) $x = 1$ c) $x = 2$

5. Cho $P(x)$ là câu "x học ở lớp hơn 5 giờ mỗi ngày trong tuần", ở đây không gian là tập hợp các sinh viên. Hãy diễn đạt các lượng từ sau thành câu thông thường :

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

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

6. Cho $P(x,y)$ là câu "x đã học môn y", với không gian của x là tập hợp tất cả sinh viên trong lớp bạn, và không gian của y là tập hợp tất cả các môn tin học ở trường bạn. Hãy diễn đạt các lượng từ sau thành câu thông thường :

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

c) $\forall x\ \exists y\ P(x,y)$, d) $\exists y\ \forall x\ P(x,y)$

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

7. Cho $P(x)$ là câu "x nói được tiếng Nga" và $Q(x)$ là câu "x biết ngôn ngữ C^{++}". Hãy diễn đạt các câu sau bằng cách dùng $P(x)$, $Q(x)$, các lượng từ và các liên từ logic. Cho không gian đối với các lượng từ là tập hợp tất cả sinh viên ở trường bạn.

a) Có một sinh viên ở trường bạn nói được tiếng Nga và biết C^{++}.

b) Có một sinh viên ở trường bạn nói được tiếng Nga nhưng không biết C^{++}.

c) Mọi sinh viên ở trường bạn đều nói được tiếng Nga hoặc biết C^{++}.

d) Không có một sinh viên nào ở trường bạn nói được tiếng Nga hoặc biết C^{++}.

8. Cho $Q(x,y)$ là câu "x đã là người tham gia cuộc thi y". Hãy diễn đạt các câu sau bằng cách dùng $Q(x,y)$, các lượng từ và các liên từ logic. Cho không gian của x là tập hợp tất cả sinh viên ở trường bạn, còn không gian của y là tập hợp tất cả các cuộc thi trên truyền hình.

a) Có một sinh viên ở trường bạn đã tham gia một cuộc thi trên truyền hình.

b) Không có một sinh viên nào ở trường bạn đã tham gia cuộc thi trên truyền hình.

c) Có một sinh viên ở trường bạn đã tham gia cuộc thi *Jeopardy* và *Wheel of Fortune* trên truyền hình.

d) Mọi cuộc thi trên truyền hình đều có một sinh viên ở trường bạn tham gia.

e) Ít nhất có hai sinh viên ở trường bạn đã tham gia cuộc thi *Jeopardy* trên truyền hình.

9. Cho $L(x, y)$ là câu "x yêu y", với không gian của cả x và y là tập hợp mọi người trên thế giới. Hãy dùng các lượng từ để diễn đạt các câu sau :

a) Mọi người đều yêu Jerry

b) Mọi người đều yêu một ai đó.

c) Có một người mà tất cả mọi người đều yêu.

d) Không có ai yêu tất cả mọi người.

e) Có một người mà Lydia không yêu.

f) Có một người mà không ai yêu.

g) Có đúng một người mà tất cả mọi người đều yêu.

h) Có đúng hai người mà Lynn yêu.

i) Mọi người đều yêu chính mình.

f) Có một người nào đó không yêu ai ngoài chính mình.

10. Cho $F(x,y)$ là câu "x có thể lừa gạt y", với không gian là tập hợp mọi người trên thế giới. Hãy dùng các lượng từ để diễn đạt các câu sau:

a) Mọi người đều có thể lừa gạt Fred.

b) Evelyn có thể lừa gạt được mọi người.

c) Mọi người đều có thể lừa gạt được ai đó.

d) Không có ai có thể lừa gạt được tất cả mọi người.

e) Mọi người đều có thể bị lừa gạt bởi ai đó.

f) Không ai có thể lừa gạt được cả Fred lẫn Jerry.

g) Nancy có thể lừa được chính xác hai người.

h) Có chính xác một người mà ai cũng lừa gạt được.

i) Không ai có thể lừa gạt được chính mình.

j) Có một người nào đó có thể lừa gạt được chính xác một người trừ bản thân mình.

11. Dùng các lượng từ để diễn đạt các câu sau :

a) Tất cả các sinh viên tin học đều cần phải học môn toán học rời rạc.

b) Có một sinh viên ở lớp này đã có máy vi tính.

c) Tất cả các sinh viên ở lớp này đã học ít nhất một môn tin học.

d) Có một sinh viên ở lớp này đã học ít nhất một môn tin học.

e) Mỗi sinh viên ở lớp này ở một nhà trong ký túc xá.

f) Có một sinh viên ở lớp này đã ở tất cả các phòng của ít nhất một nhà trong ký túc xá.

g) Tất cả các sinh viên ở lớp này ít nhất đã ở một phòng trong tất cả các nhà của ký túc xá.

12. Lớp toán học rời rạc có một sinh viên ngành toán năm thứ nhất, 12 sinh viên ngành toán năm thứ hai, 15 sinh viên tin học năm thứ hai, hai sinh viên toán năm thứ ba, hai sinh viên tin học năm thứ ba và một sinh viên tin học năm thứ tư (năm cuối cùng). Diễn đạt các câu sau bằng cách đùng các lượng từ rồi sau đó xác định giá trị chân lý của chúng.

a) Có một sinh viên trong lớp là sinh viên năm thứ ba.

b) Mọi sinh viên trong lớp đều là sinh viên ngành tin học.

c) Có một sinh viên trong lớp không phải là sinh viên ngành toán và cũng không phải sinh viên năm thứ ba.

d) Mọi sinh viên trong lớp hoặc là sinh viên năm thứ hai hoặc là sinh viên ngành tin.

e) Có một ngành học sao cho mỗi khóa học có một sinh viên ở lớp này học ngành đó.

13. Cho $P(x)$ là câu "$x = x^2$". Nếu không gian là tập hợp các số nguyên, thì giá trị chân lý của các mệnh đề sau là như thế nào?

a) $P(0)$, b) $P(1)$,

c) $P(2)$, d) $P(-1)$,

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

14. Cho $Q(x,y)$ là câu "$x + y = x - y$". Nếu không gian của hai biến là tập hợp các số nguyên, hãy xác định giá trị chân lý của các mệnh đề sau :

a) $Q(1,1)$ b) $Q(2,0)$

c) $\forall y\ Q(1,y)$ d) $\exists x\ Q(x,2)$

e) $\exists x\ \exists y\ Q(x,y)$ f) $\forall x\ \exists y\ Q(x,y)$

g) $\exists y\ \forall x\ Q(x,y)$ h) $\forall y\ \exists x\ Q(x,y)$

i) $\forall x\ \forall y\ Q(x,y)$

15. Giả sử không gian của hàm mệnh đề $P(x,y)$ gồm các cặp số x và y với x là 1,2 hoặc 3 và y là 1, 2 hoặc 3. Dùng các phép hội và tuyển viết các mệnh đề sau :

a) $\exists x\ P(x,3)$ b) $\forall y\ P(1,y)$

c) $\forall x\ \forall y\ P(x,y)$ d) $\exists x\ \exists y\ P(x,y)$

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

16. Dùng các lượng từ diễn đạt phủ định của các mệnh đề sau, rồi dịch các phủ định đó ra các câu thông thường.

a) Mọi sinh viên ở lớp này đều thích môn toán.

b) Có một sinh viên trong lớp này chưa hề bao giờ nhìn thấy một chiếc máy tính.

c) Có một sinh viên ở lớp này đã học tất cả các môn toán được dạy ở trường này.

d) Có một sinh viên ở lớp này đã ở ít nhất một phòng trong tất cả các toà nhà ở ký túc xá.

Các Bài tập 17 - 20 dựa trên các câu hỏi lấy từ cuốn sách Logic ký hiệu của Lewis Carroll.

17. Cho $P(x)$, $Q(x)$ và $R(x)$ là các câu "x là giáo sư", "x là kẻ ngu dốt" và "x là kẻ vô tích sự", tương ứng. Bằng cách dùng các lượng từ, các liên từ logic cùng với $P(x)$, $Q(x)$ và $R(x)$ diễn đạt các câu sau với không gian là tập hợp toàn thể loài người.

a) Không có giáo sư nào là kẻ ngu dốt.

b) Mọi kẻ ngu dốt đều là vô tích sự.

c) Không có giáo sư nào là vô tích sự.

*d) (c) có thể suy ra từ (a) và (b) không? Nếu không, liệu có một kết luận đúng nào không?

18. Cho $P(x)$, $Q(x)$ và $R(x)$ tương ứng là các câu "x là lời giải thích rõ ràng", "x là thoả đáng" và "x là một lý do". Giả sử không gian của biến x là tập hợp toàn bộ văn bản. Dùng các lượng từ, các liên từ logic, cùng với $R(x)$, $Q(x)$, $R(x)$ diễn đạt các câu sau :

a) Tất cả các giải thích rõ ràng đều là thoả đáng.

b) Một số lý do là không thoả đáng.

c) Một số lý do không phải là giải thích rõ ràng.

*d) (c) có thể suy ra từ (a) và (b) không? Nếu không, thì liệu có một kết luận đúng không?

19. Cho $P(x)$, $Q(x)$, $R(x)$và $S(x)$ tương ứng là các câu "x là một đứa bé". "x là logic", "x có khả năng cai quản một con cá sấu" và "x bị coi thường". Giả sử rằng không gian là tập hợp tất cả mọi người. Hãy dùng các lượng từ, các liên từ logic cùng với $P(x)$, $Q(x)$, $R(x)$ và $S(x)$ để diễn đạt các câu sau :

a) Những đứa bé là không logic.

b) Không ai bị coi thường nếu cai quản được cá sấu.

c) Những người không logic bị coi thường.

d) Những đứa bé không cai quản được cá sấu.

*e) (d) có suy ra được từ (a), (b) và (c) không? Nếu không, thì liệu có một kết luận đúng không?

20. Cho $P(x)$, $Q(x)$, $R(x)$ và $S(x)$ tương ứng là các câu sau : "x là một con vịt", "x là một trong số gia cầm của tôi", "x là một viên sĩ quan" và "x sẵn lòng khiêu vũ". Dùng các lượng từ, các liên từ logic cùng với $P(x)$, $Q(x)$, $R(x)$ và $S(x)$ để diễn đạt các câu sau :

a) Không có con vịt nào sẵn lòng khiêu vũ cả.

b) Không có viên sĩ quan nào từ chối khiêu vũ.

c) Toàn bộ đàn gia cầm của tôi đều là vịt.

d) Đàn gia cầm của tôi không phải là các sĩ quan.

*e) (d) có thể suy ra từ (a), (b) và (c) không? Nếu không, thì liệu có một kết luận đúng không?

21. Chứng tỏ rằng các câu $\neg\exists x\ \forall y\ P(x,y)$ và $\forall x\ \exists y\ \neg P(x,y)$ có cùng giá trị chân lý.

22. Chứng tỏ rằng $\forall x\ (P(x) \wedge Q(x))$ và $\forall x\ P(x) \wedge \forall x\ Q(x)$ có cùng giá trị chân lý.

23. Chứng tỏ rằng $\exists x\ (P(x) \vee Q(x))$ và $\exists x\ P(x) \vee \exists x\ Q(x)$ có cùng giá trị chân lý.

24. Xác lập các tương đương logic sau, trong đó A là một mệnh đề không có chứa các lượng từ.

a) $(\forall x\ P(x)) \vee A \Leftrightarrow \forall x\ (P(x) \vee A)$

b) $(\exists x\ P(x)) \vee A \Leftrightarrow \exists x\ (P(x) \vee A)$

25. Xác lập các tương đương logic sau, trong đó A là mệnh đề không có liên quan với lượng từ nào :

a) $(\forall x\ P(x)) \wedge A \Leftrightarrow \forall x\ (P(x) \wedge A)$

b) $(\exists x\ P(x)) \wedge A \Leftrightarrow \exists x\ (P(x) \wedge A)$

26. Chứng minh rằng $\forall x\ P(x) \vee \forall x\ Q(x)$ và $\forall x\ (P(x) \vee Q(x))$ là không tương đương logic.

27. Chứng minh rằng $\exists x\ P(x) \wedge \exists x\ Q(x)$ và $\exists x\ (P(x) \wedge Q(x))$ là không tương đương logic.

28*. Chứng minh rằng $\forall x\ P(x) \vee \forall x\ Q(x)$ và $\forall x\ \forall y\ (P(x) \vee Q(y))$ là tương đương logic. (Biến mới y được dùng để kết hợp một cách đúng đắn các lượng từ).

29*. a) Chứng tỏ rằng $\forall x\ P(x) \wedge \exists x\ Q(x)$ và $\forall x\ \exists y\ (P(x) \wedge Q(y))$ là tương đương logic.

b) Chứng tỏ rằng $\forall x\ P(x) \vee \exists x\ Q(x)$ và $\forall x\ \exists y\ (P(x) \vee Q(y))$ là tương đương logic.

30. $\exists!x\ P(x)$ là ký hiệu của mệnh đề "Tồn tại duy nhất một x sao cho $P(x)$ là đúng". Nếu không gian là tập các số nguyên, hãy xác định giá trị chân lý của các lượng từ sau :

a) $\exists!x\ (x > 1)$ b) $\exists!x\ (x^2 = 1)$

c) $\exists!x\ (x + 3 = 2x)$ d) $\exists!x\ (x = x + 1)$

31. Xác định giá trị chân lý của các mệnh đề sau :

a) $\exists!x\ P(x) \rightarrow \exists x\ P(x)$

b) $\forall x\ P(x) \rightarrow \exists!x\ P(x)$

c) $\exists!x\ \neg P(x) \rightarrow \neg\forall x\ P(x)$

32. Biểu diễn lượng từ $\exists!x\ P(x)$ qua các phủ định, các phép hội và tuyển với không gian gồm các số nguyên 1, 2 và 3.

33*. Biểu diễn lượng từ $\exists!x\ P(x)$ qua lượng từ phổ dụng, lượng từ tồn tại và các toán tử logic.

Một câu được gọi là ở dạng tiền lượng chuẩn tắc (prenex normal form – viết tắt là PNF) nếu và chỉ nếu nó có dạng :

$$Q_1x_1Q_2x_2 \ \ldots\ Q_kx_kP(x_1,\ x_2,\ \ldots,\ x_n)$$

Ở đây Q_i với $i = 1, 2, \ldots k$ hoặc là lượng từ tồn tại hoặc là lượng từ phổ dụng và $P(x_1, x_2 \ldots x_n)$ là hàm mệnh đề không có liên quan đến các lượng từ nào.

Ví dụ, $\exists x\ \forall y\ (P(x,y) \wedge Q(y))$ là ở dạng tiền lượng chuẩn tắc, trong khi $\exists x\ P(x) \vee \forall x\ Q(x)$ không phải ở dạng đó (vì các lượng từ không xuất hiện trước hết).

Tất cả các câu được tạo từ các biến mệnh đề, từ các hàm mệnh đề, từ **T** *và* **F** *bằng cách dùng các liên từ logic và các lượng từ đều tương đương với một câu ở dạng tiền lượng chuẩn tắc. Bài tập 35 yêu cầu chứng minh khẳng định này.*

34*. Đặt các câu sau ở dạng tiền lượng chuẩn tắc (*Gợi ý* : Dùng tương đương logic ở các Bảng 5 và 6 trong Tiết 1.2 ; Bảng 2 trong Tiết này cùng các Bài tập 22 – 25 và 28 – 29 ở Tiết này).

a) $\exists x\ P(x) \vee \exists x\ Q(x) \vee A$, ở đây A là một mệnh đề không có liên quan gì với các lượng từ.

b) $\neg(\forall x\ P(x) \vee \forall x\ Q(x))$

c) $\exists x\ P(x) \rightarrow \exists x\ Q(x)$

35.** Hãy chỉ rõ cách làm thế nào để biến đổi được một câu bất kỳ thành một câu ở dạng tiền lượng chuẩn tắc tương ứng với câu đã cho.

1.4. TẬP HỢP

MỞ ĐẦU

Trong cuốn sách này chúng ta sẽ nghiên cứu một lớp rộng lớn các cấu trúc rời rạc. Chúng bao gồm : các quan hệ – đó là các cặp phần tử sắp thứ tự ; các tổ hợp – đó là những tập hợp không sắp thứ tự của các phần tử ; và các đồ thị – đó là tập hợp các đỉnh và các cạnh nối các đỉnh đó. Hơn nữa, chúng ta cũng sẽ minh hoạ các cấu trúc rời rạc này hay khác đã được sử dụng như thế nào để mô hình hoá hoặc để giải các bài toán. Đặc biệt, nhiều ví dụ về việc dùng các cấu trúc rời rạc trong lưu trữ, truyền thông và thao tác dữ liệu cũng sẽ được mô tả trong quyển sách này. Trong tiết này, chúng ta sẽ nghiên cứu một cấu trúc rời rạc cơ bản từ đó dựng lên tất cả các cấu trúc khác, đó là tập hợp.

Các tập hợp được dùng để nhóm các đối tượng lại với nhau. Thường thường, các đối tượng trong một tập hợp có các tính chất tương tự nhau. Ví dụ, tất cả các sinh viên vừa mới nhập trường lập nên một tập hợp. Tương tự như vậy, tất cả các sinh viên đang học môn toán rời rạc ở trường trên cũng tạo nên một tập hợp. Thêm vào đó, những sinh viên vừa tựu trường và đang theo học môn toán rời rạc tạo nên một tập hợp có thể nhận được bằng cách lấy các phần tử chung của hai tập hợp đầu. Ngôn ngữ tập hợp là phương tiện để nghiên cứu các tập hợp như vậy một cách có tổ chức.

Chú ý rằng thuật ngữ *đối tượng* được dùng ở đây không có chỉ rõ là đối tượng cụ thể nào. Sự mô tả một tập hợp các đối tượng dựa trên khái niệm trực giác về một đối tượng nào đó đã được nhà toán học người Đức Georg Cantor đưa ra lần đầu tiên vào năm 1895. Lý thuyết hình thành từ định nghĩa trực giác đó của tập hợp đã dẫn đến những **nghịch lý** hoặc các mâu thuẫn logic như nhà triết học người Anh Bertrand Russell đã chỉ ra năm 1902. (xem Bài tập 24 trong đó có mô tả một trong số các nghịch lý đó). Những mâu thuẫn logic đó có thể tránh được bằng cách xây dựng một lý thuyết tập hợp xuất phát từ những giả thiết cơ

bản, gọi là các **tiên đề**. Tuy nhiên, chúng ta sẽ dùng phiên bản ban đầu của Cantor – được gọi là **lý thuyết tập hợp ngây thơ,** chứ không phát triển phiên bản tiên đề của lý thuyết này, bởi vì tất cả các tập hợp được xem xét trong cuốn cách này đều có thể được xử lý phi mâu thuẫn bằng cách dùng lý thuyết ban đầu của Cantor.

ĐỊNH NGHĨA 1. Các đối tượng trong một tập hợp cũng được gọi là các phần tử của tập hợp đó. Tập hợp được nói là *chứa* các phần tử của nó.

Có nhiều cách mô tả một tập hợp. Một trong số những cách đó là liệt kê hết các phần tử của một tập hợp, khi có thể. Chúng ta sẽ dùng ký hiệu trong đó tất cả các phần tử của một tập hợp được liệt kê ở giữa hai dấu móc. Ví dụ ký hiệu $\{a, b, c, d\}$ biểu diễn một tập hợp có bốn phần tử là a, b, c và d. (Sau này để cho gọn có chỗ "tập hợp" sẽ được gọi tắt là "tập" – ND).

Ví dụ 1. Tập V của tất cả các nguyên âm trong bảng chữ cái tiếng Anh có thể được viết như $V = \{a, e, i, o, u\}$.

■

Ví dụ 2. Tập O của các số nguyên, dương, lẻ nhỏ hơn 10 có thể được biểu diễn bởi $O = \{1, 3, 5, 7, 9\}$.

■

Ví dụ 3. Mặc dù, các tập hợp thường dùng để nhóm các phần tử có các tính chất chung lại với nhau, nhưng cũng không có gì ngăn cản một tập hợp chứa các phần tử dường như chẳng có liên quan gì với nhau. Ví dụ, {a, 2, Fred, New Jersey} là một tập hợp có bốn phần tử là a, 2, Fred và New Jersey.

■

Người ta thường dùng các chữ hoa để ký hiệu các tập hợp. Các chữ **N**, **Z**, và **R** in đậm sẽ được dùng để ký hiệu tập hợp các số tự nhiên {0, 1, 2, 3...}, tập hợp các số nguyên {... –2, –1, 0, 1, 2 ...} và tập hợp các số thực, tương ứng. Đôi khi chúng ta cũng dùng $\mathbf{Z}^+$ để ký hiệu tập hợp các số nguyên dương.

Đôi khi ký hiệu dấu móc cũng được dùng để mô tả một tập hợp không thể liệt kê hết các phần tử của nó. Khi ấy một số phần tử sẽ được liệt kê và sau đó sẽ dùng các dấu chấm chấm (...).

■

Ví dụ 4. Tập hợp các số nguyên dương bé hơn 100 có thể được ký hiệu bởi {1, 2, 3, ..., 99}.

■

Vì có nhiều phát biểu toán học khẳng định rằng hai tập hợp các đối tượng được mô tả khác nhau, nhưng thực sự chỉ là một tập hợp, nên ta cần phải hiểu thế nào là hai tập hợp bằng nhau.

ĐỊNH NGHĨA 2. Hai tập hợp là *bằng nhau* nếu và chỉ nếu chúng có cùng các phần tử.

Ví dụ 5. Các tập {1, 3, 5} và {3, 5, 1} là bằng nhau vì chúng có cùng các phần tử. Chú ý rằng trật tự trong đó các phần tử được liệt kê là hoàn toàn không quan trọng. Cũng cần chú ý rằng, việc cùng một phần tử được liệt kê nhiều lần cũng không quan trọng, vì thế {1, 3, 3, 3, 5, 5, 5, 5} cũng chính là tập hợp {1, 3, 5}, vì chúng có cùng các phần tử.

■

Một cách khác để mô tả các tập hợp là *chỉ rõ các thuộc tính đặc trưng* của các phần tử của tập hợp đó. Chúng ta sẽ nêu nét đặc trưng của tất cả các phần tử có trong tập hợp bằng cách chỉ ra một hoặc nhiều tính chất mà chúng cần phải có để trở thành phần tử của tập hợp đang xét. Ví dụ, tập O của tất cả các số nguyên đương, lẻ và nhỏ hơn 10 có thể viết như sau :

$$O = \{x \mid x \text{ là số nguyên đương lẻ nhỏ hơn } 10\}.$$

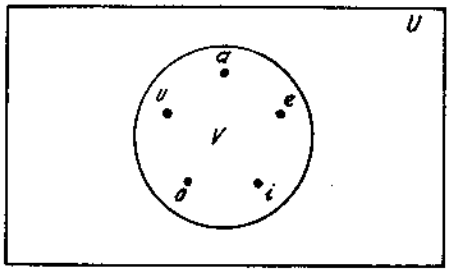
Chúng ta thường dùng cách chỉ rõ thuộc tính đặc trưng này để mô tả các tập hợp khi không thể liệt kê hết tất cả các phần tử của tập hợp đó. Ví dụ, tập hợp tất cả các số thực được viết như sau

$$\mathbf{R} = \{x \mid x \text{ là số thực}\}.$$

Các tập hợp cũng có thể được minh hoạ bằng hình vẽ nhờ dùng các giản đồ Venn, do nhà toán học người Anh John Venn lần đầu tiên đưa ra vào năm 1881. Trong các giản đồ Venn, **tập hợp vũ trụ** U – tập hợp chứa tất cả các đối tượng đang xét – được biểu diễn bằng một hình chữ nhật. Bên trong hình chữ nhật này, những hình tròn hoặc những hình hình học khác được dùng để biểu diễn các tập hợp. Đôi khi các điểm được dùng để biểu diễn các phần tử đặc biệt của tập hợp. Các giản đồ Venn thường được dùng để chỉ ra mối quan hệ giữa các tập hợp. Trong ví dụ dưới đây, bạn có thể thấy các giản đồ Venn đã được sử dụng như thế nào.

Ví dụ 6. Vẽ giản đồ Venn biểu diễn tập V các nguyên âm trong tiếng Anh.

Giải : Ta vẽ một hình chữ nhật để chỉ tập hợp Vũ trụ U - đây là tập hợp gồm 26 chữ cái trong bảng chữ cái tiếng Anh. Trong hình chữ nhật đó ta vẽ một vòng tròn để biểu diễn tập V. Trong vòng tròn này ta dùng các điểm để chỉ các phần tử của V (xem hình 1).



Hình 1. Giản đồ Venn của tập hợp các nguyên âm.

Bây giờ chúng ta đưa ra ký hiệu để chỉ một đối tượng là phần tử của một tập hợp. Ta viết $a \in A$ để chỉ a là phần tử của tập A. Ký hiệu $a \notin A$ ký hiệu a không phải là phần tử thuộc tập A. Chú ý rằng các chữ viết thường thường được dùng để ký hiệu các phần tử của một tập hợp.

Có một tập hợp đặc biệt không chứa một phần tử nào. Tập hợp đó được gọi là **tập rỗng** và được ký hiệu là $\varnothing$. Tập rỗng cũng có thể được ký hiệu là $\{\}$. Thường xảy ra, tập hợp của các phần tử có các tính chất nào đó hoá ra lại là một tập rỗng. Ví dụ, tập hợp các số nguyên dương lớn hơn hình phương của nó là một tập rỗng.

ĐỊNH NGHĨA 3. Tập A được gọi là một *tập con* của B nếu và chỉ nếu mỗi phần tử của A đều là một phần tử của B. Chúng ta dùng ký hiệu $A \subseteq B$ để chỉ A là một tập con của tập B.

Chúng ta thấy rằng $A \subseteq B$ nếu và chỉ nếu lượng từ

$$\forall x \ (x \in A \rightarrow x \in B)$$

là đúng.

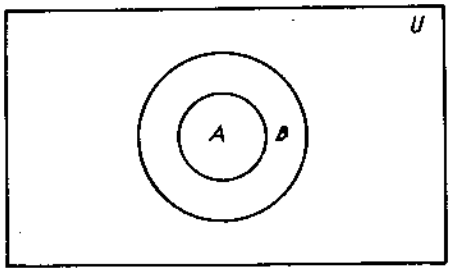
Ví dụ, tập tất cả các số nguyên dương lẻ nhỏ hơn 10 là một tập con của tập tất cả các số nguyên dương nhỏ hơn 10. Tập hợp tất cả các sinh viên học ngành tin học ở trường bạn là một tập con của tập hợp toàn thể học sinh của trường bạn.

Tập rỗng là tập con của mọi tập hợp, tức là

$$\varnothing \subseteq S$$

với S là tập hợp bất kỳ. Để xác lập tập rỗng là tập con của S, chúng ta cần phải chứng minh rằng mọi phần tử của $\varnothing$ cũng là phần tử của S. Nói một cách khác, chúng ta cần phải chứng minh rằng mệnh đề kéo theo "nếu $x \in \varnothing$, thì $x \in S$" là luôn luôn đúng. Chúng ta chỉ cần chú ý rằng giả thiết của mệnh đề kéo theo này – cụ thể là giả thiết "$x \in \varnothing$" – là luôn luôn sai nên mệnh đề kéo theo này là luôn luôn đúng. Vì vậy, tập rỗng là tập con của mọi tập hợp. Hơn nữa, cũng lưu ý rằng mọi tập hợp đều là một tập con của chính nó (độc giả nên tự chứng minh lấy khẳng định này). Do đó, nếu P là một tập hợp thì ta biết chắc rằng $\varnothing \subseteq P$ và $P \subseteq P$.

Khi chúng ta muốn nhấn mạnh rằng tập A là tập con của B nhưng $A \neq B$, ta viết $A \subset B$ và nói rằng A là một **tập con thực sự** của B. Chúng ta hãy vẽ tập vũ trụ U như một hình chữ nhật. Trong hình chữ nhật này, ta vẽ một vòng tròn biểu diễn tập B. Vì A là tập con của B, chúng ta vẽ một vòng tròn biểu diễn A bên trong vòng tròn biểu diễn B. Mối quan hệ này được biểu diễn trên hình 2.



Hình 2. Giản đồ Venn biểu diễn A là tập con của B.

Một cách để chứng minh hai tập hợp có cùng các phần tử là chứng minh tập này là tập con của tập kia và ngược lại. Nói một cách khác, chúng ta có thể chứng minh rằng nếu A và B là các tập hợp với $A \subseteq B$ và $B \subseteq A$ thì $A = B$. Đây thực sự là cách rất tiện ích để chứng minh hai tập bằng nhau.

Các tập cũng có thể có các phần tử là các tập hợp khác. Ví dụ, ta có các tập hợp :

$$\{\varnothing, \{a\}, \{b\}, \{a,b\}\}$$

và

$$\{x \mid x \text{ là tập con của tập } \{a, b\}\}$$

Chú ý rằng hai tập ở trên là bằng nhau.

Các tập được dùng rộng rãi trong các bài toán đếm, và đối với các ứng dụng như vậy chúng ta cần phải bàn về "kích thước" của các tập hợp.

ĐỊNH NGHĨA 4. Cho S là một tập hợp. Nếu có chính xác n phần tử phân biệt trong S, với n là số nguyên không âm, thì ta nói rằng S là một *tập hữu hạn* và n là bản số của S. Bản số của S được ký hiệu là $|S|$.

Ví dụ 7. Cho A là tập hợp các số nguyên dương lẻ nhỏ hơn 10. Khi đó $|A| = 5$.

■

Ví dụ 8. Cho S là tập hợp các chữ cái trong bảng chữ cái tiếng Anh. Khi đó $|S| = 26$.

■

Ví dụ 9. Vì tập rỗng không chứa phần tử nào, suy ra $|\varnothing| = 0$.

■

Chúng ta cũng sẽ quan tâm cả tới những tập hợp không phải là hữu hạn.

ĐỊNH NGHĨA 5. Một tập được nói là *vô hạn*, nếu nó không phải là hữu hạn.

Ví dụ 10. Tập hợp các số nguyên dương là một tập vô hạn.

■

Người ta cũng có thể phát triển một lý thuyết về bản số đối với các tập vô hạn. Điều này sẽ được bàn tới trong Tiết 1.7.

TẬP HỢP LUỸ THỪA

Nhiều bài toán liên quan đến việc trắc nghiệm những tổ hợp của các phần tử thuộc một tập để xem chúng có thoả mãn một tính chất nào đó hay không. Để xét tất cả những tổ hợp của các phần tử thuộc tập S nào đó, chúng ta xây dựng một tập mới có các phần tử là tất cả các tập con của S.

ĐỊNH NGHĨA 6. Cho tập S, *tập luỹ thừa* của S là tập của tất cả các tập con của S. Tập luỹ thừa của S được ký hiệu là $P(S)$.

Ví dụ 11. Xác định tập luỹ thừa của tập {0, 1, 2}.

Giải : Tập luỹ thừa $P(\{0, 1, 2\})$ là tập hợp tất cả các tập con của {0, 1, 2}. Từ đó , ta có :

$P(\{0, 1, 2^a\})$ = {∅ , {0}, {1}, {2}, {0,1}, {0,2}, {1, 2}, {0, 1, 2}}.

Chú ý rằng tập rỗng và chính tập S cũng là các phần tử của $P(S)$.

■

Ví dụ 12. Tìm tập luỹ thừa của tập rỗng và tập luỹ thừa của tập {∅}.

Giải : Tập rỗng chỉ có chính xác một tập con, đó là chính tập đó.

Do đó $P(\emptyset) = \{\emptyset\}$

Tập {∅} có chính xác hai tập con, cụ thể là ∅ và chính {∅}. Do đó

$$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$$

■

Nếu một tập có n phần tử, thì tập luỹ thừa của nó có 2^n phần tử. Chúng ta sẽ chứng minh điều này bằng nhiều cách ở các tiết tiếp sau.

TÍCH ĐỀ CÁC (DESCARTES)

Thứ tự của các phần tử trong một tập hợp thường là rất quan trọng. Vì các tập là không sắp thứ tự, nên cần phải có một cấu trúc khác để hiểu diễn các tập được sắp thứ tự. Điều này được cho bởi các **dãy sắp thứ tự**.

ĐỊNH NGHĨA 7. Dãy sắp thứ tự $(a_1, a_2, \ldots a_n)$ là một tập hợp sắp thứ tự, có a_1 là phần tử thứ nhất, a_2 là phần tử thứ 2, ... và a_n là phần tử thứ n.

Chúng ta nói rằng hai dãy sắp thứ tự là bằng nhau, nếu và chỉ nếu các phần tử tương ứng của chúng bằng nhau. Nói cách khác, $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ nếu và chỉ nếu $a_i = b_i$ đối với $i = 1, 2, \ldots n$. Đặc hiệt, dãy có hai phần tử được gọi là **cặp sắp thứ tự** (hay thường gọi đơn giản là **cặp** – ND). Các cặp (a, b) và (c, d) là bằng nhau nếu và chỉ nếu $a = c$ và $b = d$. Chú ý rằng (a, b) và (b, a) không bằng nhau nếu $a \neq b$.

Rất nhiều các cấu trúc rời rạc mà chúng ta sẽ nghiên cứu trong các chương sau đều dựa trên khái niệm về *tích Đề các* của các tập hợp (gọi theo tên nhà toán học Pháp René Descartes). Trước hết chúng ta hãy định nghĩa tích Đề các của hai tập hợp.

ĐỊNH NGHĨA 8. Cho A và B là hai tập hợp. *Tích Đề các* của A và B, được ký hiệu là $A \times B$, là tập hợp của tất cả các cặp (a, b) với $a \in A$ và $b \in B$. Từ đó,

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

Ví dụ 13. Cho A là tập hợp tất cả các sinh viên ở một trường đại học, và B là tập hợp tất cả các môn học được đạy ở đây. Hãy xác định tích Đề các $A \times B$.

Giải : Tích Đề các $A \times B$ gồm tất cả các cặp có dạng (a, b) với a là một sinh viên của trường và b là một môn học được dạy ở trường. Tập $A \times B$ có thể được dùng để biểu diễn tất cả các khả năng đăng ký theo học các môn được đạy ở trường của các sinh viên. ■

Ví dụ 14. Xác định tích Đề các của $A = \{1, 2\}$ và $B = \{a, b, c\}$.

Giải : Tích Đề các $A \times B$ là :

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

■

Các tích Đề các $A \times B$ và $B \times A$ là không bằng nhau nếu không có $A = \varnothing$ hoặc $B = \varnothing$ (vì khi đó $A \times B = \varnothing$) hoặc nếu $A \neq B$ (xem Bài tập 22 ở cuối tiết này). Điều này được minh hoạ trong ví dụ sau :

Ví dụ 15. Chứng minh rằng tích Đề các $B \times A$ không bằng tích Đề các $A \times B$, với A và B như trong Ví dụ 14.

Giải : Tích Đề các $B \times A$ là :

$$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

Nó không bằng $A \times B$ đã được xác định trong Ví dụ 14. ■

Người ta cũng có thể định nghĩa tích Đề các cho số các tập hợp lớn hơn hai.

ĐỊNH NGHĨA 9. *Tích Đề các* của các tập A_1, A_2, .., A_n, được ký hiệu bởi $A_1 \times A_2 \times \ldots \times A_n$ là tập hợp của các dãy sắp thứ tự $(a_1, a_2, \ldots, a_n)$ trong đó $a_i \in A_i$ với $i = 1, 2, \ldots, n$. Nói một cách khác

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ với } i = 1, 2, \ldots n\}$$

Ví dụ 16. Xác định tích Đề các $A \times B \times C$, ở đây $A = \{0, 1\}$, $B = \{1, 2\}$ và $C = \{0, 1, 2\}$.

Giải : Tích Đề các $A \times B \times C$ gồm tất cả các dãy ba phần tử sắp thứ tự (a, b, c) với $a \in A$, $b \in B$ và $c \in C$. Từ đó,

$$A \times B \times C = \{(0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 0), (0, 2, 1), (0, 2, 2), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 2, 0), (1, 2, 1), (1, 2, 2)\}$$

BÀI TẬP

1. Liệt kê các phần tử của các tập hợp sau :
   a) $\{x \mid x$ là số thực sao cho $x^2 = 1\}$
   b) $\{x \mid x$ là số nguyên dương nhỏ hơn $12\}$
   c) $\{x \mid x$ là bình phương của một số nguyên và $x < 100\}$
   d) $\{x \mid x$ là số nguyên sao cho $x^2 = 2\}$
2. Dừng cách chỉ rõ các thuộc tính đặc trưng mô tả các tập hợp sau :
   a) $\{0, 3, 6, 9, 12\}$
   b) $\{-3, -2, -1, 0, 1, 2, 3\}$
   c) $\{m, n, o, p\}$
3. Xác định xem mỗi cặp tập hợp sau đây có bằng nhau không?
   a) $\{1, 3, 3, 3, 5, 5, 5, 5, 5\}$ và $\{5, 3, 1\}$
   b) $\{\{1\}\}$ và $\{1, \{1\}\}$
   c) $\varnothing$ và $\{\varnothing\}$
4. Giả sử rằng $A = \{2, 4, 6\}$, $B = \{2, 6\}$, $C = \{4, 6\}$ và $D = \{4, 6, 8\}$. Hãy xác định các tập nào là những tập con của tập nào?
5. Xác định xem các mệnh đề sau đúng hay sai :
   a) $x \in \{x\}$ b) $\{x\} \subseteq \{x\}$

c) $\{x\} \in \{x\}$ d) $\{x\} \in \{\{x\}\}$

e) $\varnothing \subseteq \{x\}$ f) $\varnothing \in \{x\}$.

6. Dùng giản đồ Venn minh hoạ mối quan hệ

$$A \subseteq B \quad \text{và} \quad B \subseteq C$$

7. Giả sử A, B và C là các tập sao cho $A \subseteq B$ và $B \subseteq C$. Chứng minh rằng $A \subseteq C$.

8. Tìm hai tập A và B sao cho $A \in B$ và $A \subseteq B$.

9. Xác định bản số của các tập hợp sau :

a) $\{a\}$ b) $\{\{a\}\}$

b) $\{a, \{a\}\}$ d) $\{a, \{a\}, \{a, \{a\}\}\}$

10. Xác định bản số của các tập hợp sau

a) $\varnothing$ b) $\{\varnothing\}$

c) $\{\varnothing, \{\varnothing\}\}$ d) $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$

11. Tìm tập hợp luỹ thừa của mỗi tập hợp sau :

a) $\{a\}$ b) $\{a, b\}$

c) $\{\varnothing, \{\varnothing\}\}$.

12. Có thể kết luận rằng $A = B$ nếu A và B là hai tập có tập luỹ thừa như nhau không?

13. Mỗi tập sau có bao nhiêu phần tử

a) $P(\{a, b, \{a, b\}\})$ b) $P(\{\varnothing, a, \{a\}, \{\{a\}\}\})$

c) $P(P(\varnothing))$.

14. Xác định xem mỗi tập dưới đây có là tập luỹ thừa của một tập nào đó không?

a) $\varnothing$ b) $\{\varnothing, \{a\}\}$

c) $\{\varnothing, \{a\}, \{\varnothing, a\}\}$ d) $\{\varnothing, \{a\}, \{b\}, \{a, b\}\}$

15. Cho $A = \{a, b, c, d\}$ và $B = \{y, z\}$. Tìm

a) $A \times B$ b) $B \times A$

16. Nêu định nghĩa của tích Đề các $A \times B$, trong đó A là tập hợp các môn học được dạy bởi khoa toán của một trường đại học và B là tập hợp các giáo sư toán ở trường đại học đó.

17. Nêu ý nghĩa của tích Đề các $A \times B \times C$ trong đó A là tập hợp tất cả các tuyến bay, B và C là hai tập hợp tất cả các thành phố ở Mỹ.

18. Cho $A \times B = \varnothing$ với A và B là hai tập hợp. Bạn có thể rút ra kết luận gì?

19. Cho tập hợp A. Chứng minh rằng $\varnothing \times A = A \times \varnothing = \varnothing$

20. Cho $A = \{a, b, c\}$, $B = \{x, y\}$ và $C = \{0, 1\}$

Tìm :

a) $A \times B \times C$ b) $C \times B \times A$

c) $C \times A \times B$ d) $B \times B \times B$

21. Có bao nhiêu phần tử khác nhau trong $A \times B$, nếu A có m phần tử và B có n phần tử?

22. Chứng minh rằng $A \times B \neq B \times A$ khi A, B là các tập không rỗng và $A \neq B$.

23*. Chứng minh rằng cặp sắp thứ tự (a, b) có thể được định nghĩa qua các tập như $\{\{a\}, \{a, b\}\}$. (Gợi ý : trước hết hãy chứng minh $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ nếu và chỉ nếu $a = c$ và $b = d$).

24*. Bài tập này giới thiệu **Nghịch lý Russell.**

Cho S là một tập hợp chứa tập x, nếu tập x không thuộc chính nó, tức $S = \{x \mid x \notin x\}$

a) Chứng minh rằng giả thiết S là một phần tử của S sẽ dẫn tới mâu thuẫn.

b) Chứng minh rằng giả thiết S không phải là phần tử của nó cũng dẫn tới mâu thuẫn.

Từ a) và b) suy ra rằng tập S không thể được định nghĩa như ta đã làm. Nghịch lý này có thể tránh được bằng cách hạn chế các loại phần tử mà các tập hợp có thể có.

1.5. CÁC PHÉP TOÁN TẬP HỢP

MỞ ĐẦU

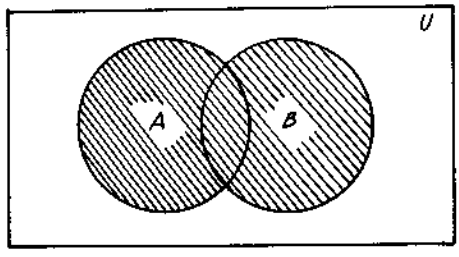
Hai tập hợp có thể được tổ hợp với nhau theo nhiều cách. Ví dụ, khi bắt đầu với tập hợp các sinh viên ngành toán và tập hợp các sinh viên ngành tin học ở trường bạn, chúng ta có thể tạo ra tập gồm các sinh viên học chuyên ngành toán hoặc chuyên ngành tin học, tập hợp các sinh viên không theo ngành toán, v.v...

ĐỊNH NGHĨA 1. Cho A và B là hai tập hợp. *Hợp* của hai tập A và B, được ký hiệu là $A \cup B$, là tập chứa tất cả các phần tử hoặc thuộc A, hoặc thuộc B hoặc thuộc cả hai.

Một phần tử x thuộc hợp của tập A và tập B nếu và chỉ nếu x thuộc A hoặc x thuộc B. Tức là,

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Gián đồ Venn cho trên hình 1 biểu diễn hợp của hai tập A và B. Phần tô sẫm bên trong hình tròn biểu diễn A hoặc hình tròn biểu diễn B là vùng biểu diễn hợp của A và B.



Hình 1. Giản đồ Venn biểu diễn hợp của A và B. $A \cup B$ được gạch chéo.

Dưới đây là một số ví dụ về hợp của các tập hợp.

Ví dụ 1. Hợp của các tập $\{1, 3, 5\}$ và $\{1, 2, 3\}$ là tập $\{1, 2, 3, 5\}$; tức là $\{1, 3, 5\} \cup \{1, 2, 3\} = \{1, 2, 3, 5\}$.

■

Ví dụ 2. Hợp của tập hợp tất cả các sinh viên ngành tin học ở trường bạn và tập hợp tất cả các sinh viên ngành toán của trường bạn là tập hợp tất cả các sinh viên học ngành toán hoặc học ngành tin (hoặc học cả hai ngành).

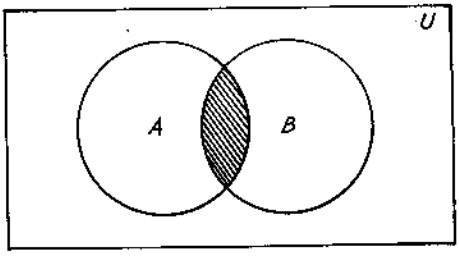
■

ĐỊNH NGHĨA 2. Cho hai tập hợp A và B. *Giao* của hai tập hợp A và B, được ký hiệu là $A \cap B$, là tập hợp chứa các phần tử thuộc cả A và B.

Một phần tử x thuộc giao của hai tập A và B nếu và chỉ nếu x thuộc A và x thuộc B, tức là

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Giản đồ Venn trên hình 2 biểu diễn giao của hai tập A và B. Vùng tô sẫm ở trong hai vòng tròn biểu diễn các tập A và B chính là vùng biểu diễn giao của A và B.



Hình 2. Giản đồ Venn biểu diễn giao của A và B
$A \cap B$ được gạch chéo.

Dưới đây là một số ví dụ về giao của các tập hợp.

Ví dụ 3. Giao của các tập {1, 3, 5} và {1, 2, 3} là tập {1, 3}, tức là {1, 3, 5} ∩ {1, 2, 3} = {1, 3}.

■

Ví dụ 4. Giao của tập hợp tất cả các sinh viên ngành tin học ở trường bạn và tập hợp tất cả các sinh viên ngành toán là tập hợp tất cả các sinh viên đồng thời theo học hai ngành trên.

■

ĐỊNH NGHĨA 3. Hai tập được gọi là *rời nhau* nếu giao của chúng là tập rỗng.

Ví dụ 5. Cho $A = \{1, 3, 5, 7, 9\}$ và $B = \{2, 4, 6, 8, 10\}$. Vì $A \cap B = \varnothing$, A và B là hai tập rời nhau.

■

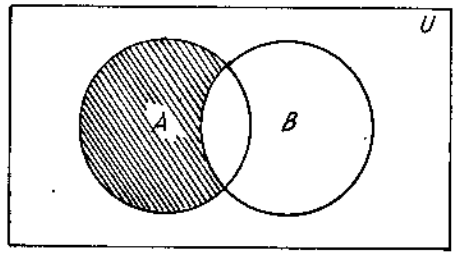
Chúng ta thường phải quan tâm đến việc tìm bản số của hợp các tập hợp. Để tìm số các phần tử trong hợp của hai tập hợp hữu hạn A và B, cần chú ý rằng $|A| + |B|$ sẽ đếm mỗi phần tử thuộc A nhưng không thuộc B hoặc thuộc B nhưng không thuộc A chính xác một lần, và các phần tử thuộc cả A lẫn B chính xác hai lần. Như vậy nếu lấy $|A|+|B|$ trừ đi số phần tử thuộc cả A lẫn B, thì các phần tử thuộc $A \cap B$ sẽ chỉ còn được đếm một lần. Từ đó, ta có :

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Sự tổng quát hoá kết quả này cho hợp của một số tuỳ ý các tập được gọi là *nguyên lý bù trừ*. Nguyên lý này là một kỹ thuật quan trọng được dùng trong nghệ thuật đếm. Chúng ta sẽ bàn tới nguyên lý này và các kỹ thuật đếm khác chi tiết hơn trong các Chương 4 và 5.

Còn có một cách quan trọng khác để tổ hợp các tập hợp.

ĐỊNH NGHĨA 4. Cho A và B là hai tập hợp. *Hiệu* của A và B, được ký hiệu là $A - B$, là tập hợp chứa các phần tử thuộc A nhưng không thuộc B. Hiệu của A và B cũng được gọi là *phần bù của B đối với A*.



Hình 3. Giản đồ Venn biểu diễn hiệu của A và B. $A - B$ được tô gạch chéo.

Một phần tử x thuộc hiệu của A và B nếu và chỉ nếu $x \in A$ và $x \notin B$; tức là :

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Giản đồ Venn trên hình 3 biểu diễn hiệu của tập A và tập B. Vùng tô sẫm bên trong vòng tròn hiểu diễn tập A và ở bên ngoài vòng tròn biểu diễn tập B là vùng biểu điễn $A - B$.

Dưới đây là một số ví dụ về hiệu của các tập.

Ví dụ 6. Hiệu của {1, 3, 5} và {1, 2, 3} là tập {5}, tức là {1, 3, 5} - {1, 2, 3} = {5}. Hiệu này khác với hiệu của {1, 2, 3} và {1, 3, 5}, nó là tập {2}.

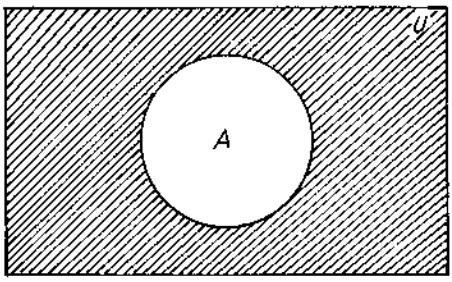
■

Ví dụ 7. Hiệu của tập hợp các sinh viên ngành tin và tập hợp các sinh viên ngành toán của trường bạn là tập hợp tất cả các sinh viên ngành tin ở trường bạn không đồng thời theo học ngành toán.

■

Một khi tập vũ trụ U đã được chỉ rõ, ta có thể định nghĩa được **phần bù** của một tập hợp.

ĐỊNH NGHĨA 5. Cho U là tập vũ trụ. Phần bù của tập A, được ký hiệu là $\overline{A}$, là phần bù của A đối với U. Nói một cách khác phần bù của A chính là $U - A$.



Hình 4. Giản đồ Venn biểu diễn phần bù của tập A. $\overline{A}$ được gạch chéo.

Một phần tử x thuộc $\overline{A}$ nếu và chỉ nếu $x \notin A$, tức là,

$$\overline{A} = \{x \mid x \notin A\}$$

Vùng tô đậm trên hình 4 ở ngoài vòng tròn biểu diễn tập A là vùng biểu diễn $\overline{A}$.

Dưới đây là một số ví dụ về phần bù của một tập.

Ví dụ 8. Cho $A = \{a, e, i, o, u\}$ (ở đây tập vũ trụ là tập các chữ cái trong bảng chữ cái tiếng Anh). Khi đó

$$\overline{A} = \{b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z\}$$

■

Ví dụ 9. Cho A là tập hợp các số nguyên dương lớn hơn 10 (với tập vũ trụ là tập tất cả các số nguyên dương). Khi đó

$$\overline{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

CÁC HẰNG ĐẲNG THỨC TẬP HỢP

Bảng 1 liệt kê các hằng đẳng thức tập hợp quan trọng nhất. Chúng ta sẽ chứng minh ở đây chỉ một số các hằng đẳng thức đó bằng cách dùng các phương pháp khác nhau, để chứng tỏ rằng thường có nhiều cách tiếp cận để giải một bài toán. Việc chứng minh các hằng đẳng thức còn lại sẽ được đưa vào các bài tập. Độc giả nên chú ý sự tương tự giữa các

hằng đẳng thức tập hợp này với các tương đương logic được xét trong Tiết 1.2. Thực tế, các hằng đẳng thức đã cho đều có thể chứng minh trực tiếp từ các tương đương logic tương ứng. Hơn thế nữa, cả hai đều là những trường hợp đặc biệt của các hằng đẳng thức trong đại số Boole (sẽ được nghiên cứu ở Chương 9).

BẢNG 1. Một số Hằng đẳng thức tập hợp

HẰNG ĐẲNG THỨC	TÊN GỌI
$A \cup \varnothing = A$ $A \cap U = A$	Luật đồng nhất
$A \cup U = U$ $A \cap \varnothing = \varnothing$	Luật nuốt
$A \cup A = A$ $A \cap A = A$	Luật luỹ đẳng
$(\overline{A}) = A$	Luật bù
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Luật giao hoán
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Luật kết hợp
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Luật phân phối
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	Luật De Morgan

Một trong những cách để chứng minh hai tập hợp bằng nhau là chứng minh tập này là tập con của tập kia và ngược lại. Chúng ta sẽ minh hoạ phương pháp chứng minh này bằng cách thiết lập luật De Morgan thứ hai.

Ví dụ 10. Chứng minh $\overline{A \cap B} = \overline{A} \cup \overline{B}$ bằng cách chứng tỏ tập này là tập con của tập kia.

Giải : Trước hết, giả sử rằng $x \in \overline{A \cap B}$. Từ đó suy ra $x \notin A \cap B$. Điều này kéo theo $x \notin A$ hoặc $x \notin B$. Do đó $x \in \overline{A}$ hoặc $x \notin \overline{B}$, tức

là $x \in \overline{A} \cup \overline{B}$. Điều này chứng tỏ rằng $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

Bây giờ ta lại giả sử rằng $x \in \overline{A} \cup \overline{B}$. Khi đó $x \in \overline{A}$ hoặc $x \in \overline{B}$. Từ đó suy ra $x \notin A$ hoặc $x \notin B$. Do đó, $x \notin A \cap B$, hay $x \in \overline{A \cap B}$. Điều này chứng minh rằng mỗi tập trên đều là tập con của nhau, vậy hai tập này phải hằng nhau và hằng đẳng thức được chứng minh.

■

Một cách khác để chứng minh các hằng đẳng thức tập hợp là dùng cách chỉ rõ các thuộc tính đặc trưng và các qui tắc logic. Hãy xét chứng minh sau của luật De Morgan thứ hai.

Ví dụ 11. Dùng cách chỉ rõ các thuộc tính đặc trưng và các tương đương logic để chứng minh rằng $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Giải : Dãy các đẳng thức sau cho phép chứng minh hằng đẳng thức trên :

$$\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} \\
&= \{x \mid \neg(x \in (A \cap B))\} \\
&= \{x \mid \neg(x \in A \wedge x \in B)\} \\
&= \{x \mid x \notin A \vee x \notin B\} \\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} \\
&= \{x \mid x \in \overline{A} \cup \overline{B}\}
\end{aligned}$$

Chú ý rằng luật De Morgan thứ hai đối với các tương đương logic cũng đã được dùng ở đẳng thức thứ 4 trong dãy này.

Các hằng đẳng thức cũng có thể được chứng minh bằng cách dùng **bảng tính thuộc** (một tập hợp). Để chỉ một phần tử thuộc một tập hợp ta dùng số 1 ; để chỉ một phần tử không thuộc tập hợp ta dùng số 0. Ta sẽ xét mỗi tổ hợp của các tập mà một phần tử có thể được chứa trong đó và chứng minh rằng các phần tử trong chính các tổ hợp của các tập hợp đó thuộc về cả hai tập ở hai vế của hằng đẳng thức. {Bạn đọc nên lưu ý sự tương tự giữa bảng tính thuộc và bảng giá trị chân lý}

Ví dụ 12. Dùng bảng tính thuộc chứng minh rằng

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Giải : Bảng tính thuộc cho các tổ hợp của các tập hợp được cho trong Bảng 2. Bảng này có 8 dòng. Vì cột $A \cap (B \cup C)$ và $(A \cap B) \cup (A \cap C)$ giống hệt nhau, chứng tỏ hằng đẳng thức là đúng.

BẢNG 2. Bảng tính thuộc đối với tính chất phân phối

A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Ví dụ 13. Cho A, B và C là các tập hợp. Chứng minh rằng :

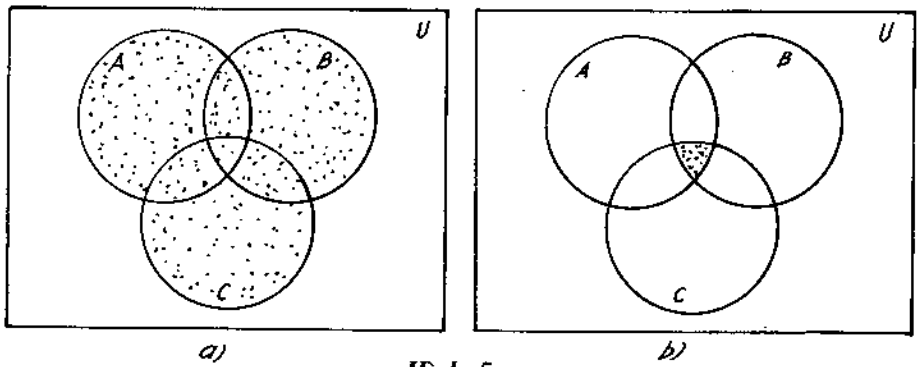
$$\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$$

Giải : Ta có

$$\begin{aligned}
\overline{A \cup (B \cap C)} &= \overline{A} \cap \overline{(B \cap C)} && \text{theo Luật De Morgan thứ nhất} \\
&= \overline{A} \cap (\overline{B} \cup \overline{C}) && \text{theo Luật De Morgan thứ hai} \\
&= (\overline{B} \cup \overline{C}) \cap \overline{A} && \text{theo Luật giao hoán đối với phép giao} \\
&= (\overline{C} \cup \overline{B}) \cap \overline{A} && \text{theo Luật giao hoán đối với phép hợp.}
\end{aligned}$$

HỢP VÀ GIAO TỔNG QUÁT

Vì hợp và giao của các tập hợp thỏa mãn định luật phân phối, nên các tập $A \cup B \cup C$ và $A \cap B \cap C$ là hoàn toàn xác định, khi A, B, C



Hình 5

a) $A \cup B \cup C$ được chấm chấm; b) $A \cap B \cap C$ được chấm chấm.
Hợp và Giao của A, B và C.

là các tập hợp. Chú ý rằng $A \cup B \cup C$ chứa tất cả các phần tử thuộc ít nhất một trong số các tập A, B, C và $A \cap B \cap C$ chứa tất cả các phần tử thuộc cả ha tập đó. Những tổ hợp của ha tập A, B, C được minh họa trên hình 5.

Ví dụ 14. Cho $A = \{0, 2, 4, 6, 8\}$, $B = \{0, 1, 2, 3, 4\}$ và $C = \{0, 3, 6, 9\}$. Xác định $A \cup B \cup C$ và $A \cap B \cap C$.

Giải : Tập hợp $A \cup B \cup C$ chứa tất cả các phần tử thuộc ít nhất một trong ba tập hợp A, B, C. Từ đó :

$$A \cup B \cup C = \{0, 1, 2, 3, 4, 6, 8, 9\}$$

Tập hợp $A \cap B \cap C$ chứa các phần tử thuộc cả ba tập A, B và C, do đó

$$A \cap B \cap C = \{0\}.$$

■

Chúng ta cũng có thể xét giao và hợp của một số tuỳ ý các tập hợp. Chúng ta dùng các định nghĩa sau.

ĐỊNH NGHĨA 6. *Hợp* của n tập hợp là một tập hợp chứa tất cả các phần tử thuộc ít nhất một trong số n tập hợp đó.

Chúng ta dùng ký hiệu :

$$A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i$$

để chỉ hợp của các tập hợp A_1, A_2, ..., A_n.

ĐỊNH NGHĨA 7. *Giao* của n tập hợp là một tập hợp chứa các phần tử thuộc tất cả n tập hợp đó.

Chúng ta ký hiệu :

$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i$$

để chỉ giao của các tập hợp.

Các ví dụ sau minh hoạ hợp và giao tổng quát.

Ví dụ 15. Cho $A_i = \{i, i + 1, i + 2, ...\}$. Khi đó :

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i, i + 1, i + 2, ...\} = \{1, 2, 3, ...\}$$

và $$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i + 1, i + 2, ...\} = \{n, n + 1, n + 2, ...\}$$

■

BIỂU DIỄN CÁC TẬP HỢP TRÊN MÁY TÍNH

Có nhiều cách để biểu diễn các tập hợp trên máy tính. Một phương pháp là lưu trữ các phần tử của tập hợp theo cách không sắp thứ tự. Tuy nhiên, nếu điều đó đã làm được, thì việc tính giao, hợp hoặc hiệu của hai tập hợp sẽ rất mất thời gian, vì mỗi phép tính đó đòi hỏi một lượng tìm kiếm rất lớn đối với các phần tử. Chúng tôi sẽ giới thiệu ở đây một phương pháp lưu trữ các phần tử bằng cách dùng sự sắp tuỳ ý các phần tử của tập vũ trụ. Phương pháp biểu diễn tập hợp này sẽ làm cho việc tính những tổ hợp của các tập hợp trở nên dễ dàng hơn.

Giả sử rằng tập vũ trụ U là hữu hạn (và có kích thước hợp lý để số phần tử của U không lớn hơn dung lượng bộ nhớ của máy tính mà bạn đang dùng). Trước hết, hãy chỉ rõ sự sắp tuỳ ý các phần tử của U, ví dụ $a_1, a_2, ..., a_n$. sau đó biểu diễn tập con A của U bằng một xâu bit có chiều dài n, trong đó bit thứ i ở xâu này là 1 nếu a_i thuộc A và là 0 nếu a_i không thuộc A. Ví dụ sau sẽ minh hoạ kỹ thuật này.

Ví dụ 16. Cho $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ và sự sắp các phần tử trong U theo thứ tự tăng dần ; tức là $a_i = i$. Xác định xâu bit biểu diễn tập con các số nguyên lẻ trong U, tập con các số nguyên chẵn trong U và tập con các số nguyên không vượt quá 5 trong U.

Giải : Xâu bit biểu diễn tập hợp các số nguyên lẻ trong U, cụ thể là tập $\{1, 3, 5, 7, 9\}$, có bit 1 ở các vị trí thứ nhất, thứ ba, thứ năm, thứ bảy và thứ chín, và bit 0 ở các vị trí còn lại. Đó là,

10101 01010

(Ở đây chúng ta đã tách xâu có chiều dài là 10 này thành bai khối, mỗi khối có chiều dài là 5 để dễ đọc vì các xâu bit dài rất khó đọc). Tương

tự, chúng ta biểu diễn tập con tất cả các số nguyên chẵn trong U, cụ thể là tập {2, 4, 6, 8, 10}, bằng xâu

01010 10101

Tập con tất cả các số nguyên trong U không vượt quá 5, cụ thể là tập {1, 2, 3, 4, 5} được biểu diễn bởi xâu :

11111 00000

Bằng cách dùng các xâu bit để biểu diễn các tập hợp, ta dễ dàng tìm được phần bù của các tập hợp, cũng như hợp, giao và hiệu của chúng. Để tìm xâu bit cho phần bù của một tập hợp từ xâu bit của tập hợp đó ta chỉ việc thay mỗi 1 thành 0 và thay mỗi 0 thành 1, vì $x \in A$ nếu và chỉ nếu $x \notin \overline{A}$. Chú ý rằng phép toán này tương ứng với việc lấy phủ định của mỗi bit khi ta gắn một bit với một giá trị chân lý : 1 ứng với đúng và 0 ứng với sai.

■

Ví dụ 17. Chúng ta đã thấy rằng xâu bit đối với tập hợp {1, 3, 5, 7, 9} (với tập hợp vũ trụ {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}) là

10101 01010

Xác định xâu bit đối với phần bù của tập này.

Giải : Xâu bit đối với phần bù của tập này sẽ nhận được bằng cách thay các số 0 thành 1 và ngược lại. Sau khi làm như vậy, ta được xâu :

01010 10101

tương ứng với tập {2, 4, 6, 8, 10}.

■

Để nhận được các xâu bit cho các hợp và giao của hai tập hợp, chúng ta sẽ thực hiện các phép toán Boole trên các xâu bit biểu diễn hai tập hợp đó. Bit ở vị trí i trong xâu bit của hợp là 1 nếu một trong các bit ở vị trí thứ i trong hai xâu là 1 (hoặc cả hai là 1) và là 0 khi cả hai bit đó là 0. Từ đó ta suy ra rằng xâu bit đối với hợp là OR bit của hai xâu hit tương ứng với hai tập số. Còn bit ở vị trí thứ i trong xâu bit của giao sẽ là 1 khi các bit ở vị trí tương ứng trong hai xâu bit đều bằng 1 và bằng 0 khi hoặc một trong hai bit bằng 0 (hoặc cả hai bằng 0). Từ đó suy ra rằng xâu bit đối với giao là một AND bit của hai xâu bit biểu diễn hai tập đã cho.

Ví dụ 18. Xâu bit đối với các tập hợp {1, 2, 3, 4, 5} và {1, 3, 5, 7, 9} là 11111 00000 và 10101 01010. Dùng các xâu bit để tìm hợp và giao của hai tập trên.

Giải : Xâu bit đối với hợp của hai tập là :

$$11111\ 00000 \vee 10101\ 01010 = 11111\ 01010$$

và xâu này tương ứng với tập {1, 2, 3, 4, 5, 7, 9}

Xâu bit đối với giao của hai tập này là :

$$11111\ 00000 \wedge 10101\ 01010 = 10101\ 00000$$

và xâu này tương ứng với tập {1, 3, 5}.

■

BÀI TẬP

1. Cho A là tập hợp các sinh viên sống cách xa trường trong vòng bán kính một dặm, và B là tập hợp các sinh viên đang trên đường tới lớp. Hãy mô tả các sinh viên thuộc một trong các tập hợp sau :

   a) $A \cap B$ b) $A \cup B$

   c) $A - B$ d) $B - A$.

2. Giả sử rằng A là tập hợp các sinh viên năm thứ hai ở trường bạn và B là tập hợp các sinh viên đang học môn toán rời rạc ở trường bạn. Hãy biểu diễn các tập sau đây qua A và B.

   a) Tập hợp các sinh viên năm thứ hai học toán rời rạc ở trường bạn.

   b) Tập hợp sinh viên năm thứ hai ở trường bạn không học toán rời rạc.

   c) Tập hợp các sinh viên ở trường bạn hoặc là năm thứ hai, hoặc đang học toán rời rạc.

   d) Tập hợp các sinh viên ở trường bạn, hoặc không là sinh viên năm thứ hai, hoặc không học toán rời rạc.

3. Cho $A = \{1, 2, 3, 4, 5\}$ và $B = \{0, 3, 6\}$. Tìm

   a) $A \cup B$ h) $A \cap B$

   c) $A - B$ d) $B - A$

4. Cho $A = \{a, b, c, d, e\}$ và $B = \{a, b, c, d, e, f, g, h\}$

Tìm: a) $A \cup B$ b) $A \cap B$

c) $A - B$ d) $B - A$

5. Cho A là một tập hợp, chứng minh rằng $\overline{\overline{A}} = A$

6. Cho A là một tập hợp, chứng minh rằng :

a) $A \cup \varnothing = A$ b) $A \cap \varnothing = \varnothing$

c) $A \cup A = A$ d) $A \cap A = A$

e) $A - \varnothing = A$ f) $A \cup U = U$

g) $A \cap U = A$ h) $\varnothing - A = \varnothing$

7. Cho A và B là hai tập hợp. Chứng minh rằng :

a) $A \cup B = B \cup A$ b) $A \cap B = B \cap A$

8. Tìm các tập A và B nếu $A - B = \{1, 5, 7, 8\}$,

$B - A = \{2, 10\}$ và $A \cap B = \{3, 6, 9\}$

9. Chứng minh rằng nếu A và B là hai tập hợp, thì

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

a) bằng cách chứng minh mỗi vế là tập con của vế kia.

b) bằng cách dùng bảng tính thuộc.

10. Cho A và B là hai tập hợp. Chứng minh rằng :

a) $(A \cap B) \subseteq A$ b) $A \subseteq (A \cup B)$

c) $A - B \subseteq A$ d) $A \cap (B - A) = \varnothing$

e) $A \cup (B - A) = A \cup B$.

11. Chứng minh rằng nếu A, B và C là các tập hợp thì

$$\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cup \overline{C}$$

a) bằng cách chứng tỏ vế này là tập con của vế kia.

b) dùng bảng tính thuộc.

12. Cho A, B và C là các tập hợp, chứng minh rằng :

a) $(A \cup B) \subseteq (A \cup B \cup C)$

b) $(A \cap B \cap C) \subseteq (A \cap B)$

c) $(A - B) - C \subseteq A - C$

d) $(A - C) \cap (C - B) = \varnothing$

e) $(B - A) \cup (C - A) = (B \cup C) - A$.

13. Chứng minh rằng nếu A và B là các tập hợp, thì

$A - B = A \cap \overline{B}$

14. Chứng minh rằng nếu A và B là các tập hợp, thì

$(A \cap B) \cup (A \cap \overline{B}) = A$.

15. Cho A, B, C là các tập hợp. Chứng minh rằng :

a) $A \cup (B \cup C) = (A \cup B) \cup C$

b) $A \cap (B \cap C) = (A \cap B) \cap C$

c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

16. Cho A, B, C là tập hợp. Chứng minh rằng :

$(A - B) - C = (A - C) - (B - C)$

17. Cho $A = \{0, 2, 4, 6, 8, 10\}$; $B = \{0, 1, 2, 3, 4, 5, 6\}$ và $C = \{4, 5, 6, 7, 8, 9, 10\}$. Tìm :

a) $A \cap B \cap C$

b) $A \cup B \cup C$

c) $(A \cup B) \cap C$

d) $(A \cap B) \cup C$

18. Vẽ giản đồ Venn đối với các tổ hợp sau của các tập A, B và C.

a) $A \cap (B \cup C)$

b) $\overline{A} \cap \overline{B} \cap \overline{C}$

c) $(A - B) \cup (A - C) \cup (B - C)$

19. Bạn có thể nói gì về các tập A và B nếu các đẳng thức sau là đúng?

a) $A \cup B = A$

b) $A \cap B = A$

b) $A - B = A$

c) $A \cap B = B \cap A$

e) $A - B = B - A$

20. Liệu có thể kết luận $A = B$ nếu A, B và C là các tập thỏa mãn

a) $A \cup C = B \cup C$?

b) $A \cap C = B \cap C$?

21. Cho A và B là hai tập con của tập vũ trụ U. Chứng minh rằng $A \subseteq B$ nếu và chỉ nếu $\overline{B} \subseteq \overline{A}$.

Hiệu đối xứng *của A và B, được ký hiệu là $A \oplus B$, là tập chứa các phần tử hoặc thuộc A hoặc thuộc B chứ không thuộc cả A và B.*

22. Tìm hiệu đối xứng của {1, 3, 5} và {1, 2, 3}

23. Tìm hiệu đối xứng của tập hợp các sinh viên ngành tin của một trường và tập các sinh viên ngành toán của trường đó.

24. Vẽ giản đồ Venn cho hiệu đối xứng của hai tập A và B.

25. Chứng minh rằng $A \oplus B = (A \cup B) - (A \cap B)$.

26. Chứng minh rằng $A \oplus B = (A - B) \cup (B - A)$.

27. Chứng minh rằng nếu A là tập con của tập vũ trụ U, thì

a) $A \oplus A = \varnothing$ *b)* $A \oplus \varnothing = A$

c) $A \oplus U = \overline{A}$ c) $A \oplus \overline{A} = U$

28. Chứng minh rằng nếu A và B là các tập hợp, thì

a) $A \oplus B = B \oplus A$ b) $(A \oplus B) \oplus B = A$

29. Có thể nói gì về các tập A và B nếu $A \oplus B = A$.

30*. Xác định xem hiệu đối xứng có tính kết hợp không, tức là nếu A, B, C là các tập hợp, liệu có suy ra :

$A \oplus (B \oplus C) = (A \oplus B) \oplus C$ không?

31*. Giả sử A, B, C là các tập hợp sao cho $A \oplus C = B \oplus C$. Liệu có cần phải có $A = B$ không ?

32*. Nếu A, B, C và D là các tập hợp, liệu có suy ra

$(A \oplus B) \oplus (C \oplus D) = (A \oplus C) \oplus (B \oplus D)$ không?

33. Nếu A, B, C và D là các tập hợp, liệu có suy ra

$$(A \oplus B) \oplus (C \oplus D) = (A \oplus D) \oplus (B \oplus C) \text{ không?}$$

34*. Chứng minh rằng nếu A, B, và C là các tập hợp, thì :

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

(Đây là trường bợp đặc biệt của nguyên lý bù trừ sẽ được nghiên cứu chi tiết trong Chương 5).

35. Cbo $A_i = \{1, 2, 3, ..., i\}$ với $i = 1, 2, 3$ ... Tìm

a) $\bigcup_{i=1}^{n} A_i$ b) $\bigcap_{i=1}^{n} A_i$

36. Cho $A_i = \{i, i + 1, i + 2, ...\}$. Tìm

a) $\bigcup_{i=1}^{n} A_i$ b) $\bigcap_{i=1}^{n} A_i$

37. Cho A_i là tập tất cả các xâu bit không rỗng có chiều dài không vượt quá i. Tìm

a) $\bigcup_{i=1}^{n} A_i$ b) $\bigcap_{i=1}^{n} A_i$

38. Giả sử rằng tập vũ trụ $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Biểu diễn các tập dưới đây bằng các xâu bit với bit thứ i trong xâu là 1 nếu i thuộc tập đó, và bằng 0 trong trường hợp ngược lại.

a) $\{3, 4, 5\}$ b) $\{1, 3, 6, 10\}$

c) $\{2, 3, 4, 7, 8, 9\}$

39. Dùng tập vũ trụ như bài tập trên, tìm các tập được biểu diễn bởi các xâu sau :

a) 11110 01111 b) 01011 11000

c) 10000 00001

40. Các tập con nào của một tập vũ trụ hữu hạn được biểu diễn bởi các xâu bit sau :

a) Xâu gồm toàn các số 0.

b) Xâu gồm toàn các số 1.

41. Xác định xâu bit tương ứng với hiệu của hai tập hợp.

42. Xác định xâu bit ứng với hiệu đối xứng của hai tập hợp.

43. Hãy chỉ rõ các phép toán trên các xâu bit được thực hiện như thế nào để tìm các tổ hợp sau của các tập

$A = \{a, b, c, d, e\}$, $B = \{b, c, d, g, p, t, v\}$

$C = \{c, e, i, o, u, x, y, z\}$ và $D = \{d, e, h, i, n, o, t, u, x, y\}$

a) $A \cup B$ b) $A \cap B$

c) $(A \cup D) \cap (B \cup C)$ d) $A \cup B \cup C \cup D$.

44. Làm thế nào dùng các xâu bit để tìm được giao và hợp của n tập hợp, biết rằng n tập này đều là các tập con của tập vũ trụ?

45. Tập $A \cup \{A\}$ được gọi là **người kế thừa** của tập A. Tìm những người kế thừa của các tập sau :

a) $\{1, 2, 3\}$ b) $\varnothing$

c) $\{\varnothing\}$ d) $\{\varnothing, \{\varnothing\}\}$

46. Xác định số phần tử của tập người kế thừa của một tập với n phần tử.

Đôi khi số lần mà một phần tử được gặp trong một tập không sắp thứ tự có ý nghĩa quan trọng. **Đa tập** *là tập hợp không sắp thứ tự của các phần tử trong đó một phần tử có thể gặp nhiều lần. Ký hiệu* $\{m_1.a_1, m_2.a_2, ..., m_r a\}$ *để chỉ một đa tập có phần tử* a_1 *xuất hiện* m_1 *lần, phần tử* a_2 *xuất* m_2 *lần, v.v... Các số* m_i, $i = 1, 2, ..., r$ *được gọi là* **bội** *của phần tử* a_i, $i = 1, 2, ..., r$.

Giả sử P *và* Q *là hai đa tập.* **Hợp** *của các đa tập* P *và* Q *cũng là một đa tập trong đó bội của một phần tử là số lớn nhất trong hai bội của nó ở* P *và* Q. **Giao** *của* P *và* Q *cũng là một đa tập trong đó bội của một phần tử là số bé nhất trong hai bội của nó ở* P *và* Q. **Hiệu** *của* P *và* Q *là một đa tập trong đó bội của một phần tử là hiệu của bội của phần tử đó trong* P *và bội của phần tử đó trong* Q, *nếu hiệu này không âm ; còn ngược lại bội của phần tử trong đa tập bằng 0.* **Tổng** *của* P *và* Q *là một đa tập, trong đó bội của một phần tử là tổng bội của phần tử đó trong* P *và* Q. *Hợp, giao và hiệu của* P *và* Q *được ký hiệu là* $P \cup Q$, $P \cap Q$ *và* $P - Q$, *tương ứng (các phép toán ở đây không nên lẫn lộn với các phép toán đối với các tập hợp). Tổng của* P *và* Q *được ký hiệu là* $P \oplus Q$.

47. Cho A và B là các đa tập {3.a, 2.b, 1.c} và {2.a, 3.b, 4.d}, tương ứng. Tìm :

a) $A \cup B$ b) $A \cap B$

c) $A - B$ d) $B - A$

e) $A + B$

48. Giả sử A là một đa tập có các phần tử là những loại thiết bị tin học mà một khoa ở một trường đại học cần có với bội là số lượng mỗi loại thiết bị cần phải có. Cho B là một đa tập tương tự cho một khoa khác ở trường đó. Ví dụ, A có thể là đa tập {107 máy vi tính, 44. môđem, 6. máy tính mini} và B có thể là đa tập {14. máy vi tính, 6. môđem, 2. máy tính lớn}

a) Tổ hợp nào của A và B sẽ biểu diễn các thiết bị mà trường đó sẽ mua khi cho rằng cả hai khoa sẽ dùng chung các thiết bị đó.

b) Tổ hợp nào của A và B sẽ biểu diễn số thiết bị sẽ được dùng bởi cả hai khoa nếu cả hai khoa cùng dùng chung số thiết bị đó.

c) Tổ hợp nào của A và B biểu diễn các thiết bị mà khoa thứ hai dùng nhưng khoa thứ nhất không dùng, nếu cả hai đều cùng dùng chung các loại thiết bị đó.

d) Tổ hợp nào của A và B biểu diễn các thiết bị mà trường đó sẽ mua nếu khoa này không cho khoa kia dùng chung thiết bị của mình.

Các **Tập mờ** *được dùng trong trí tuệ nhân tạo. Mỗi một phần tử trong tập vũ trụ U có một* **độ thuộc nào đó** *đối với tập mờ S, đó là một số thực nằm giữa 0 và 1 (kể cả 0 và 1). Tập mờ S được ký hiệu bằng cách liệt kê tất cả phần tử cùng với độ thuộc tập đó của nó (các phần tử với độ thuộc bằng 0 sẽ không được kê ra), Ví dụ, ta viết {0,6 Alice, 9,0 Brain, 0,4 Fred, 0,1 Oscar, 0,5 Rita} cho tập F (của những người nổi tiếng) để chỉ ra rằng Alice có độ thuộc trong F là 0,6, Brain là 0,9, Fred là 0,4, Oscar là 0,1 và Rita là 0,5 (như vậy Brian là người nổi tiếng nhất, và Oscar là người kém nổi tiếng nhất trong số người đó). Cũng giả sử rằng R là tập những người giàu với R = {0,4 Alice, 0,8 Brian, 0,2 Fred, 0,9 Oscar, 0,7 Rita}.*

49. Phần bù của tập mờ S là tập $\overline{S}$, với độ thuộc của một phần tử trong $\overline{S}$ bằng 1 trừ đi độ thuộc của phần tử đó trong S. Hãy tìm $\overline{F}$ (tập mờ của những người không nổi tiếng) và $\overline{R}$ (tập mờ của những người không giàu).

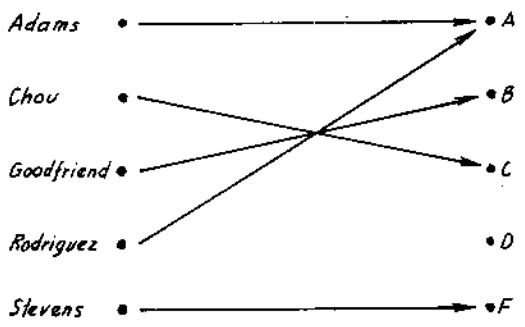
50. Hợp của hai tập mờ S và T là tập mờ $S \cup T$, trong đó độ thuộc của một phần tử trong $S \cup T$ là số lớn nhất trong hai độ thuộc của phần tử đó trong S và trong T. Hãy tìm tập mờ $F \cup R$ của người giàu hoặc nổi tiếng.

51. Giao của hai tập mờ S và T là tập mờ $S \cap T$ trong đó độ thuộc của một phần tử thuộc $S \cap T$ là số nhỏ nhất trong hai độ thuộc của phần tử đó trong S và T. Hãy tìm tập mờ $F \cap R$ những người giàu và nổi tiếng.

1.6. HÀM

MỞ ĐẦU

Ở rất nhiều chỗ, chúng ta đã gán cho mỗi phần tử của một tập hợp một phần tử đặc biệt nào đó của một tập thứ hai (tập này cũng có thể là chính tập hợp thứ nhất). Ví dụ, giả sử rằng mỗi sinh viên ở lớp toán rời rạc được gán cho một điểm chữ lấy từ tập hợp $\{A, B, C, D, F\}$. Và giả sử rằng các điểm là : A cho Adams, C cho Chou, B cho Goodfriend, A cho Rodriguez và F cho Stevens. Sự gán các điểm này được minh hoạ trên hình 1.



Hình 1. Sự gán các điểm trong lớp toán rời rạc.

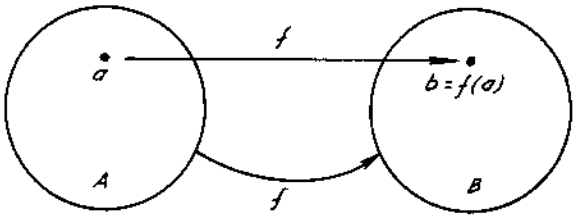
Sự gán này là một ví dụ về hàm. Hàm là một khái niệm cực kỳ quan trọng trong toán học rời rạc. Các hàm được dùng để định nghĩa các cấu trúc rời rạc như các dãy, các xâu. Hàm cũng dùng để biểu diễn thời gian một máy tính phải mất để giải một bài toán có qui mô đã cho. Các hàm đệ qui, tức là các hàm được định nghĩa qua chính chúng, được dùng xuyên suốt trong tin học và chúng sẽ được nghiên cứu trong Chương 3. Tiết này chúng ta sẽ ôn lại một số khái niệm cơ bản liên quan đến các hàm cần thiết trong toán học rời rạc.

ĐỊNH NGHĨA 1. Cho A và B là hai tập hợp. Một *hàm* f từ A đến B là sự gán chính xác một phần tử của B cho mỗi phần tử của A. Ta viết $f(a) = b$ nếu b là phần tử duy nhất của B được gán bởi hàm f cho phần tử a của A. Nếu f là hàm từ A đến B, ta viết $f : A \to B$.

Các hàm được cho bằng nhiều cách. Đôi khi ta phát biểu một cách tường minh sự gán đó. Thường thì chúng ta cho một công thức , chẳng hạn như $f(x) = x + 1$ để định nghĩa hàm. Cũng có trường hợp ta dùng một trình máy tính để cho một hàm.

ĐỊNH NGHĨA 2. Nếu f là một hàm từ A đến B thì A được gọi là *miền xác định* của f và B là *miền giá trị* của f. Nếu $f(a) = b$ ta nói b là *ảnh* của a và a là một *nghịch ảnh* của b. Tập hợp tất cả các ảnh của các phần tử thuộc A được gọi là ảnh của A qua hàm f. Nếu f là một hàm từ A đến B, ta cũng nói rằng f *ánh xạ* từ A đến B.

Hình 2 biểu diễn một hàm f từ A đến B.



Hình 2. Hàm f ánh xạ từ A đến B.

Ta hãy xét ví dụ nêu ở đầu tiết này. Cho G là hàm gán điểm cho mỗi sinh viên trong lớp toán rời rạc của chúng ta. Miền xác định của G là tập hợp {Adams, Chou, Goodfriend, Rodriguez, Stevens} và miền giá trị của nó là tập $\{A, B, C, D, F\}$. Ảnh của miền xác định qua hàm G là tập $\{A, B, C, F\}$.

Ta cũng xét các ví dụ sau :

Ví dụ 1. Cho f là hàm gán hai bit cuối cùng của một xâu bit chiều dài hai hoặc lớn hơn tới xâu đó. Khi đó miền xác định của f là tập tất cả các xâu bit có chiều dài là 2 hoặc lớn hơn còn miền giá trị của f là tập {00, 01, 10, 11}.

■

Ví dụ 2. Giả sử f là hàm từ **Z** đến **Z** gán bình phương của một số nguyên cho số nguyên đó. Khi đó $f(x) = x^2$, ở đây miền xác định của f là tập hợp các số nguyên, miền giá trị của f cũng có thể được chọn là tập tất cả các số nguyên và ảnh của miền xác định là tập hợp tất cả các số nguyên không âm là số chính phương, cụ thể là {0, 1, 4, 9, ...}

■

Ví dụ 3. (Dùng cho các sinh viên đã làm quen với ngôn ngữ Pascal)

Miền xác định và miền giá trị thường được chỉ rõ trong các ngôn ngữ lập trình. Ví dụ, câu lệnh Pascal.

function floor (x : **real**) : **integer**

nói lên rằng miền xác định của hàm floor là tập các số thực, còn miền giá trị là tập các số nguyên.

■

Hai hàm có giá trị thực với cùng miền xác định có thể cộng hoặc nhân với nhau.

ĐỊNH NGHĨA 3. Cho f_1 và f_2 là hai hàm từ A đến **R**. Khi đó $f_1 + f_2$ và f_1f_2 cũng là các hàm từ A đến **R** được định nghĩa hởi :

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$
$$(f_1f_2)(x) = f_1(x)f_2(x)$$

Chú ý rằng các hàm $f_1 + f_2$ và f_1f_2 đã được định nghĩa bằng cách chỉ ra các giá trị của chúng tại x thông qua các giá trị của f_1 và f_2 tại x.

Ví dụ 4. Cho f_1 và f_2 là các hàm từ **R** đến **R** sao cho $f_1(x) = x^2$ và $f_2(x) = x - x^2$. Xác định các hàm $f_1 + f_2$ và f_1f_2 ?

Giải. Từ định nghĩa của tổng và tích hai hàm, suy ra rằng :

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + (x - x^2) = x$$

và

$$(f_1f_2)(x) = x^2(x - x^2) = x^3 - x^4$$

Khi f là một hàm từ tập A đến tập B, thì ảnh của một tập con của A cũng có thể định nghĩa.

■

ĐỊNH NGHĨA 4. Giả sử f là một hàm từ tập A đến tập B và S là một tập con của A. Ảnh của S là một tập con của B gồm ảnh của các phần tử thuộc S. Ta ký hiệu ảnh của S hởi $f(S)$, khi đó :

$$f(S) = \{f(s) \mid s \in S\}$$

Ví dụ 5. Cho $A = \{a, b, c, d, e\}$ và $B = \{1, 2, 3, 4\}$ với $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$ và $f(e) = 1$. Ảnh của tập con $S = \{b, c, d\}$ là tập $f(S) = \{1, 4\}$.

■

CÁC HÀM ĐƠN ÁNH VÀ TOÀN ÁNH

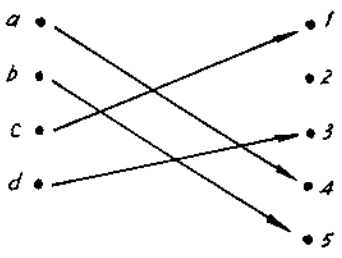
Một số hàm có ảnh phân biệt tại những phần tử phân biệt của miền xác định. Những hàm đó được gọi là **đơn ánh** hay hàm **một – một.**

ĐỊNH NGHĨA 5. Một hàm f được gọi là *đơn ánh* hay *một – một* nếu và chỉ nếu $f(x) = f(y)$ kéo theo $x = y$ đối với mọi x và y trong miền xác định của hàm f.

Chú ý : Một hàm là đơn ánh nếu và chỉ nếu $f(x) \neq f(y)$ với mỗi $x \neq y$. Cách định nghĩa này nhận được bằng cách lấy phần đảo của mệnh đề kéo theo trong định nghĩa.

Chúng ta sẽ minh hoạ khái niệm này bằng cách cho các ví dụ về các hàm đơn ánh và các hàm không đơn ánh.

Ví dụ 6. Xác định xem hàm f từ {a, b, c, d} đến {1, 2, 3, 4, 5} với $f(a) = 4$, $f(b) = 5$, $f(c) = 1$ và $f(d) = 3$ có là hàm đơn ánh không?



Hình 3. Hàm đơn ánh

Giải : Hàm f là đơn ánh vì f nhận các giá trị khác nhau tại bốn phần tử của miền xác định. Điều này được minh hoạ trên hình 3.

■

Ví dụ 7. Xác định xem hàm $f(x) = x^2$ từ tập các số nguyên đến tập các số nguyên có phải là đơn ánh không?

Giải : Hàm $f(x) = x^2$ không phải là đơn ánh vì, ví dụ, $f(1) = f(-1) = 1$ mà $1 \neq -1$.

Ví dụ 8. Xác định xem hàm $f(x) = x + 1$ có phải là đơn ánh không?

Giải : Hàm $f(x) = x + 1$ là hàm đơn ánh. Để chứng minh điều này, chú ý rằng $x + 1 \neq y + 1$ khi $x \neq y$.

■

Bây giờ chúng ta sẽ cho một số điều kiện để đảm bảo rằng một hàm là đơn ánh

ĐỊNH NGHĨA 6. Một hàm f có miền xác định và miền giá trị đều là các tập con của tập các số thực được gọi là *thực sự tăng* nếu $f(x) < f(y)$ khi $x < y$ với x và y thuộc miền xác định của f. Tương tự f được gọi là *thực sự giảm* nếu $f(x) > f(y)$ khi $x < y$ với x và y thuộc miền xác định của f.

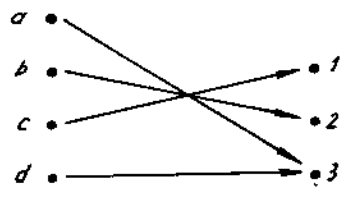
Từ những định nghĩa này ta thấy rằng các hàm hoặc thực sự tăng hoặc thực sự giảm đều là các hàm đơn ánh.

Đối với một số hàm miền giá trị và ảnh của miền xác định bằng nhau. Tức là mọi phần tử của miền giá trị đều là ảnh của một phần tử nào đó thuộc miền xác định. Những hàm có tính chất này được gọi là các **hàm toàn ánh**.

ĐỊNH NGHĨA 7. Hàm f từ A đến B được gọi là *toàn ánh* nếu và chỉ nếu đối với mọi phần tử $b \in B$ tồn tại một phần tử $a \in A$ với $f(a) = b$.

Bây giờ chúng ta sẽ cho những ví dụ về các hàm toàn ánh và các hàm không toàn ánh.

Ví dụ 9. Cho f là hàm từ {a, b, c, d} đến {1, 2, 3} được định nghĩa bởi $f(a) = 3$, $f(b) = 2$, $f(c) = 1$ và $f(d) = 3$. Hàm này có là toàn ánh không?



Hình 4. Một hàm toàn ánh

Giải : Vì tất cả ba phần tử của miền giá trị đều là ảnh của các phần tử trong miền xác định, nên f là một toàn ánh. Điều này được minh hoạ trên hình 4.

■

Ví dụ 10. Hàm $f(x) = x^2$ từ tập các số nguyên đến tập các số nguyên có phải là một toàn ánh không?

Giải : Hàm này không phải là toàn ánh, vì, chẳng hạn, không có một số nguyên nào cho $x^2 = -1$ cả.

Ví dụ 11. Hàm $f(x) = x + 1$ từ tập số nguyên tới tập số nguyên có phải là toàn ánh không?

Giải : Hàm này là toàn ánh, vì với mọi số nguyên y tồn tại một số nguyên x sao cho $f(x) = y$. Để thấy điều này, chú ý rằng $f(x) = y$ nếu và chỉ nếu $x + 1 = y$ và điều này đúng nếu và chỉ nếu $x = y - 1$.

■

ĐỊNH NGHĨA 8. Hàm f là một *song ánh* nếu nó vừa là đơn ánh (một – một) vừa là toàn ánh.

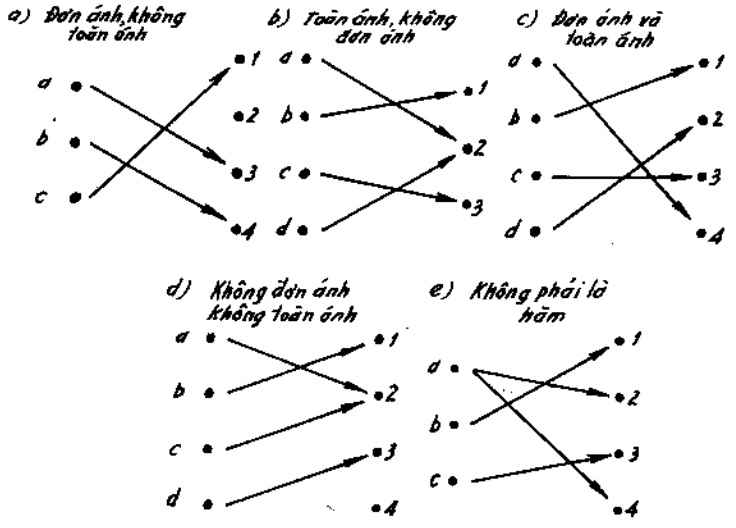
Các ví dụ sau minh hoạ khái niệm song ánh.

Ví dụ 12. Cho f là một hàm từ $\{a, b, c, d\}$ tới $\{1, 2, 3, 4\}$ với $f(a) = 4$, $f(b) = 2$, $f(c) = 1$ và $f(d) = 3$. Hàm f có phải là một song ánh không?

Giải : Hàm f là đơn ánh và toàn ánh. Nó là đơn ánh vì luôn nhận các giá trị phân biệt. Nó là toàn ánh vì bốn phần tử của miền giá trị đều là ảnh của các phần tử thuộc miền xác định. Từ đó, f là một song ánh.

■

Hình 5 minh hoạ bốn hàm, trong đó hàm đầu tiên là đơn ánh, nhưng không phải toàn ánh, hàm thứ hai là toàn ánh nhưng không phải đơn ánh, hàm thứ ba là đơn ánh và là toàn ánh, và hàm thứ tư không là đơn ánh cũng không là toàn ánh, tương ứng thứ năm không phải là một hàm, vì nó cho tương ứng một phần tử với hai phần tử khác nhau.



Hình 5. Ví dụ về các loại tương ứng khác nhau.

Giả sử f là một hàm từ A đến chính nó. Nếu A là hữu hạn, thì f sẽ là đơn ánh nếu và chỉ nếu nó là toàn ánh (Điều nàu suy ra từ kết quả của Bài tập 38 ở cuối chương này). Tuy nhiên, điều này không nhất thiết trong trường hợp A là tập vô hạn (như sẽ được chứng minh trong Tiết 1.7).

Ví dụ 13. Cho A là một tập hợp. *Hàm đồng nhất* trên A là hàm

$$i_A : A \to A, \text{ ở đây } i_A(x) = x \text{ với } x \in A.$$

Nói một cách khác, hàm đồng nhất i_A là hàm gán mỗi một phần tử cho chính nó. Hàm i_A là đơn ánh và toàn ánh, do đó là song ánh. ■

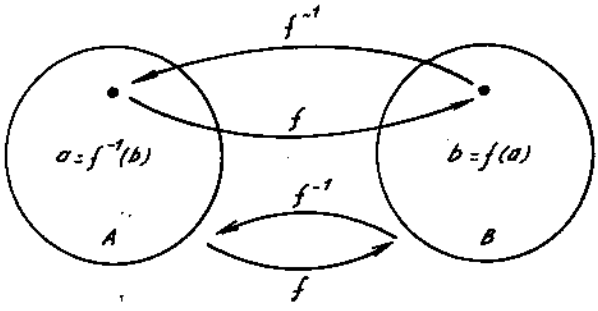
HÀM NGƯỢC VÀ HỢP THÀNH CỦA CÁC HÀM

Bây giờ ta sẽ xét một song ánh từ tập A đến tập B. Vì f là một toàn ánh, nên mỗi phần tử của B đều là ảnh của một phần tử nào đó của A. Hơn nữa, vì f là một đơn ánh, nên mọi phần tử của B là ảnh của một phần tử *duy nhất* thuộc A. Do đó, chúng ta có thể định nghĩa được một hàm mới từ B đến A, ngược với tương ứng được cho bởi hàm f. Điều này dẫn tới định nghĩa sau.

ĐỊNH NGHĨA 9. Cho f là một song ánh từ tập A đến tập B. *Hàm ngược* của f là một hàm gán cho mỗi phần tử b thuộc B một phần tử duy nhất (a thuộc A sao cho $f(a) = b$.) Hàm ngược của f được ký hiệu là f^{-1}. Từ đó, $f^{-1}(b) = a$ khi $f(a) = b$.

Hình 6 minh hoạ cho khái niệm hàm ngược.

Nếu f không phải là một hàm song ánh, thì ta không thể định nghĩa được khái niệm hàm ngược. Khi f không phải là song ánh,



Hình 6. Hàm f^{-1} là hàm ngược của hàm f.

thì hoặc là nó không phải là đơn ánh hoặc không phải toàn ánh. Mà nếu không phải là đơn ánh thì một phần tử b nào đó thuộc miền giá trị sẽ là ảnh của hơn một phần tử trong miền xác định. Còn nếu nó không phải là toàn ánh thì đối với một phần tử b nào đó trong miền giá trị sẽ không có phần tử a nào trong miền xác định sao cho $f(a) = b$. Do đó, nếu f không phải là song ánh, thì chúng ta không thể gán cho mỗi phần tử b thuộc miền giá trị một phần tử a duy nhất trong miền xác định sao cho $f(a) = b$ (vì đối với một b nào đó có thể có nhiều hơn một phần tử a như vậy hoặc không có phần tử a nào).

Hàm song ánh còn được gọi là hàm **khả nghịch**, vì chúng ta có thể xác định được hàm ngược của hàm đó. Một hàm là **không khả nghịch** nếu nó không phải là một song ánh, vì hàm ngược của nó không tồn tại.

Ví dụ 14. Cho f là hàm từ $\{a, b, c\}$ đến $\{1, 2, 3\}$ sao cho $f(a) = 2$, $f(b) = 3$ và $f(c) = 1$. Hàm f có khả nghịch không? Nếu có, hãy tìm hàm ngược đó.

Giải : Hàm f là khả nghịch, vì nó là một song ánh. Hàm ngược f^{-1} giữ nguyên sự tương ứng cho bởi hàm f, sao cho $f^{-1}(1) = c$, $f^{-1}(2) = a$ và $f^{-1}(3) = b$.

■

Ví dụ 15. Cho f là hàm từ tập các số nguyên đến tập các số nguyên sao cho $f(x) = x + 1$. Hàm f có khả nghịch không? Nếu có, hãy xác định hàm ngược.

Giải : Hàm f là khả nghịch, vì nó là một song ánh, như đã biết ở trên. Để giữ nguyên sự tương ứng, ta giả sử rằng y là ảnh của x, sao cho $y = x + 1$. Khi đó $x = y - 1$. Điều này có nghĩa là $y - 1$ là phần tử duy nhất của $\mathbf{Z}$ tương ứng với y qua f. Do đó $f^{-1}(y) = y - 1$.

■

Ví dụ 16. Cho f là một hàm từ $\mathbf{Z}$ đến $\mathbf{Z}$ với $f = x^2$. f có khả nghịch không?

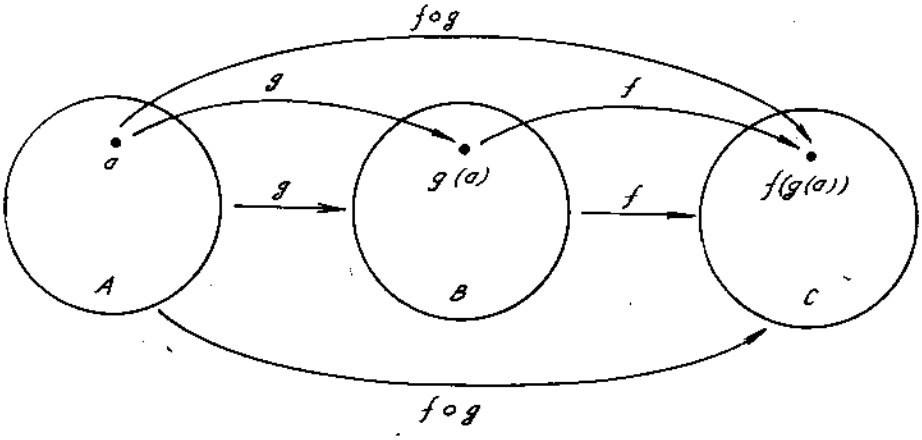
Giải : Vì $f(-1) = f(1) = 1$, nên f không phải là một đơn ánh. Nếu định nghĩa một hàm ngược, ta sẽ cần phải gán hai phần tử cho 1. Do đó, f là không khả nghịch.

■

ĐỊNH NGHĨA 10. Cho g là hàm từ tập A đến tập B và f là hàm từ tập B đến tập C. *Hợp thành* của các hàm f và g, được ký hiệu là fog, được định nghĩa bởi :

$$(fog)(a) = f(g(a))$$

Nói một cách khác, hàm đó gán cho mỗi phần tử a trong A một phần tử được gán bởi hàm f cho $g(a)$. Chú ý rằng, hợp thành $f \circ g$ sẽ không thể định nghĩa được, nếu ảnh miền xác định của g không phải là một tập con của miền xác định của f. Hình 7 minh hoạ hợp thành của các hàm.



***Hình** 7.* Hợp thành của hàm f và hàm g.

Ví dụ 17. Cho g là hàm từ tập $\{a, b, c\}$ đến chính nó, sao cho $g(a) = b$, $g(b) = c$ và $g(c) = a$. Cho f là hàm từ tập $\{a, b, c\}$ đến tập $\{1, 2, 3\}$ sao cho $f(a) = 3$, $f(b) = 2$ và $f(c) = 1$. Xác định hợp thành của f và g và của g và f.

***Giải** :* Hợp thành $f \circ g$ được xác định bởi $(f \circ g)(a) = f(g(a)) = f(b) = 2$; $(f \circ g)(b) = f(g(b)) = f(c) = 1$ và $f \circ g(c) = f(g(c)) = f(a) = 3$.

■

Chú ý rằng $g \circ f$ không xác định, vì ảnh miền giá trị của f không phải là tập con của miền xác định của g.

■

Ví dụ 18. Cho f và g là hai hàm từ tập các số nguyên đến tập các số nguyên được cho bởi : $f(x) = 2x + 3$ và $g(x) = 3x + 2$. Xác định hợp thành $f \circ g$ và $g \circ f$?

***Giải** :* Cả hai hợp thành $f \circ g$ và $g \circ f$ đều xác định. Hơn nữa :

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

và : $(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11$

■

Chú ý : Chú ý rằng mặc dù thậm chí $f \circ g$ và $g \circ f$ đều tồn tại đối với các hàm f và g nhưng chúng không bằng nhau. Nói cách khác, luật giao hoán không đúng đối với hợp thành của các hàm.

Khi hợp thành của một hàm và hàm ngược của nó được tạo thành, theo một thứ tự nào đó , ta sẽ nhận được hàm đồng nhất. Để thấy điều này, giả sử f là một hàm song ánh từ tập A đến tập B. Hàm ngược của nó vẫn giữ nguyên tương ứng này, tức là $f^{-1}(b) = a$ khi $f(a) = b$ và $f(a) = b$ khi $f^{-1}(b) = a$.

Do đó : $$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$$

và $$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$$

Do đó $f^{-1} \circ f = i_A$ và $f \circ f^{-1} = i_B$, ở đây i_A và i_B tương ứng là các hàm đồng nhất trên tập A và tập B. Như vậy : $(f^{-1})^{-1} = f$.

ĐỒ THỊ CỦA HÀM

Chúng ta có thể liên kết một tập các cặp trong $A \times B$ với mỗi một hàm từ A đến B. Tập các cặp này được gọi là **đồ thị** của hàm đó và thường được biểu diễn bằng hình vẽ để giúp ta hiểu rõ hơn dáng điệu của hàm ấy.

ĐỊNH NGHĨA 11. Cho f là một hàm từ tập A đến tập B. *Đồ thị* của hàm f là tập các cặp sắp thứ tự $\{(a, b) \mid a \in A \text{ và } f(a) = b\}$.

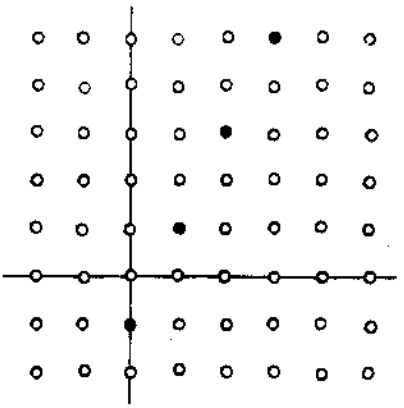
Từ định nghĩa ta thấy đồ thị của một hàm f từ A đến B là một tập con của $A \times B$ chứa các cặp sắp thứ tự với phần tử thứ hai bằng phần tử thuộc B được gán cho phần tử thứ nhất bởi hàm f.

Ví dụ 19. Vẽ đồ thị của hàm $f(n) = 2n + 1$ từ tập các số nguyên tới tập các số nguyên.

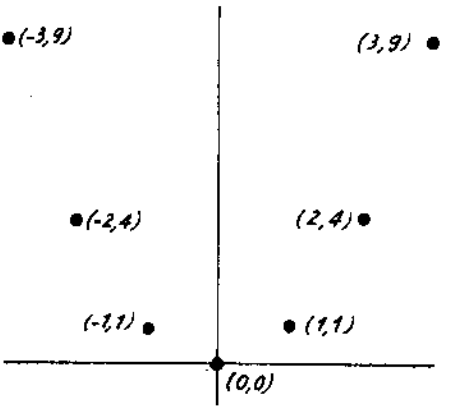
Giải : Đồ thị của f là tập các cặp sắp thứ tự có dạng $(n, 2n + 1)$, với n là một số nguyên. Đồ thị này được cho trên hình 8. ■

Ví dụ 20. Vẽ đồ thị của hàm $f(x) = x^2$ từ tập các số nguyên đến tập các số nguyên.

Giải : Đồ thị của f là tập các cặp sắp thứ tự có dạng $(x, f(x)) = (x, x^2)$, với x là một số nguyên. Đồ thị này được cho trên hình 9. ■



Hình 8. Đồ thị của hàm $f(n) = 2n + 1$ từ **Z** đến **Z**.



Hình 9. Đồ thị của hàm $f(x) = x^2$ từ **Z** đến **Z**.

MỘT SỐ HÀM QUAN TRỌNG

Tiếp theo, chúng tôi sẽ giới thiệu hai hàm quan trọng trong toán học rời rạc, đó là hàm sàn và hàm trần. Cho x là một số thực. Hàm sàn làm tròn số x xuống thành một số nguyên gần nhất nhỏ hơn hoặc bằng nó ; còn hàm trần làm tròn số x lên thành một số nguyên gần nhất lớn hơn hoặc bằng nó. Các hàm này thường được dùng khi đếm các vật. Chúng đóng vai trò quan trọng trong việc phân tích số các bước được dùng bởi các thủ tục để giải các bài toán có qui mô đặc biệt nào đó.

ĐỊNH NGHĨA 12. *Hàm sàn* gán cho số thực x số nguyên lớn nhất có giá trị nhỏ hơn hoặc bằng x. Giá trị của hàm sàn được ký hiệu là $\lfloor x \rfloor$. *Hàm trần* gán cho số thực x số nguyên bé nhất có giá trị lớn hơn hoặc bằng x. Giá trị của hàm trần được ký hiệu là $\lceil x \rceil$.

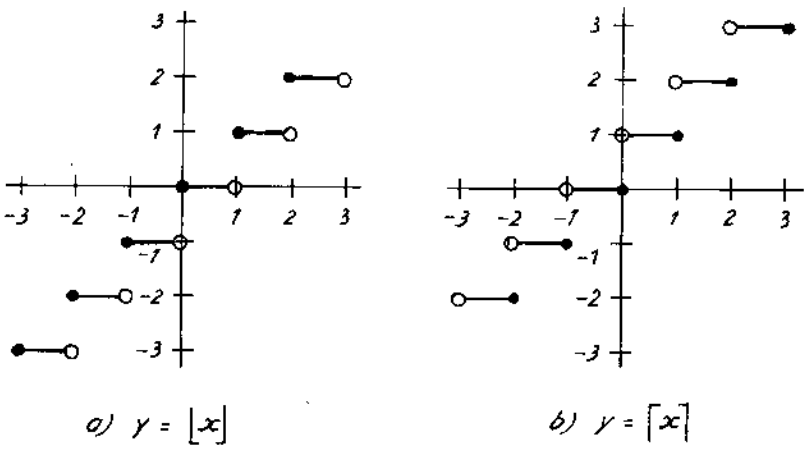
Chú ý : Hàm sàn còn được gọi là *hàm phần nguyên* và thường được ký hiệu là $[x]$.

Ví dụ 21. Dưới đây là một số giá trị của hàm sàn và hàm trần :

$\lfloor \frac{1}{2} \rfloor = 0$, $\lceil \frac{1}{2} \rceil = 1$, $\lfloor -\frac{1}{2} \rfloor = -1$, $\lceil -\frac{1}{2} \rceil = 0$, $\lfloor 3{,}1 \rfloor = 3$, $\lceil 3{,}1 \rceil = 4$, $\lfloor 7 \rfloor = 7$, $\lceil 7 \rceil = 7$.

■

Đồ thị của hàm sàn và hàm trần được cho trên hình 10.



Hình 10. Đồ thị của Hàm sàn (a) và Hàm trần (b).

Còn có một số loại hàm sẽ được dùng suốt trong cuốn sách này. Đó là các hàm đa thức, lôgarit và hàm e mũ. Trong cuốn sách này, ký hiệu $\log x$ được hiểu là log cơ số 2 của x. Khi cần dùng cơ số khác, ví dụ cơ số $b (b > 1)$ ta viết $\log_b x$.

BÀI TẬP

1. Tại sao f trong các phương trình sau không phải là một hàm từ **R** đến **R**?

   a) $f(x) = \dfrac{1}{x}$ b) $f(x) = \sqrt{x}$

   c) $f(x) = \pm\sqrt{(x^2 + 1)}$

2. Xác định xem f có phải là một hàm từ **Z** đến **R** không, nếu :

   a) $f(n) = \pm n$ b) $f(n) = \sqrt{n^2 + 1}$

   c) $f(n) = \dfrac{1}{n^2 - 4}$

3. Xác định xem f có là một hàm từ tập tất cả các xâu bit đến tập các số nguyên không, nếu :

a) $f(S)$ là vị trí của một bit 0 trong S.

b) $f(S)$ là số các bit 1 trong S.

c) $f(S)$ là số nguyên nhỏ nhất i sao cho bit thứ i trong S là 1 và $f(S) = 0$ *khi* S là một xâu rỗng, tức là xâu không có bit nào.

4. Tìm miền xác định, ảnh của miền các định của các hàm sau :

a) hàm gán cho mỗi số nguyên không âm chữ số cuối cùng của nó.

b) hàm gán cho mỗi số nguyên dương số nguyên lớn nhất tiếp sau.

c) hàm gán cho mỗi xâu bit số các bit 1 trong xâu đó.

d) hàm gán cho mỗi xâu bit số các bit trong xâu đó.

5. Tìm các giá trị sau :

a) $\lceil \frac{3}{4} \rceil$ b) $\lfloor \frac{7}{8} \rfloor$ c) $\lceil -\frac{3}{4} \rceil$

d) $\lfloor -\frac{7}{8} \rfloor$ e) $\lceil 3 \rceil$ f) $\lfloor -1 \rfloor$

6. Xác định xem các hàm từ $\{a, b, c, d\}$ đến chính nó cho dưới đây có phải đơn ánh không?

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

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

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

7. Hàm nào trong Bài tập 6 là toàn ánh?

8. Xác định xem các hàm từ **Z** đến **Z** cho dưới đây có là đơn ánh không?

a) $f(n) = n - 1$ b) $f(n) = n^2 + 1$

c) $f(n) = n^3$ d) $f(n) = \lceil \frac{n}{2} \rceil$

9. Hàm nào trong Bài tập 8 là toàn ánh?

10. Cho một ví dụ về hàm từ **N** đến **N** là

a) đơn ánh nhưng không toàn ánh.

b) toàn ánh nhưng không đơn ánh.

c) vừa toàn ánh vừa đơn ánh (nhưng khác hàm đồng nhất).

d) không đơn ánh cũng không toàn ánh.

11. Xác định xem các hàm từ **R** đến **R** cho dưới đây có là song ánh không?

a) $f(x) = 2x + 1$ b) $f(x) = x^2 + 1$

c) $f(x) = x^3$ d) $f(x) = \dfrac{x^2+1}{x^2+2}$

12. Cho $S = \{-1, 0, 2, 4, 7\}$. Tìm $f(S)$ nếu :

a) $f(x) = 1$ b) $f(x) = 2x + 1$

c) $f(x) = \lceil \frac{x}{5} \rceil$ d) $f(x) = \lfloor \frac{x^2+1}{3} \rfloor$

13. Cho $f(x) = \lfloor \frac{x^2}{3} \rfloor$. Tìm $f(S)$ nếu :

a) $S = \{-2, -1, 0, 1, 2, 3\}$ b) $S = \{0, 1, 2, 3, 4, 5\}$

c) $S = \{1, 5, 7, 11\}$ d) $S = \{2, 6, 10, 14\}$

14. Cho $f(x) = 2x$. Tìm

a) $f(\mathbf{Z})$ b) $f(\mathbf{N})$ c) $f(\mathbf{R})$

15. Cho g là một hàm từ A đến B và f là một hàm từ B đến C.

a) Chứng minh rằng nếu cả f lẫn g là các hàm đơn ánh thì $f \circ g$ cũng là hàm đơn ánh.

b) Chứng minh rằng nếu f, g đều là toàn ánh, thì $f \circ g$ cũng là toàn ánh.

16*. Nếu f và $f \circ g$ là đơn ánh, có suy ra g cũng là đơn ánh không? Giải thích.

17*. Nếu f và $f \circ g$ là toàn ánh, có suy ra được g cũng toàn ánh không? Giải thích.

18. Tìm $f \circ g$ và $g \circ f$ với $f(x) = x^2 + 1$ và $g(x) = x + 2$ là các hàm từ **R** đến **R**.

19. Tìm $f + g$ và fg đối với các hàm f và g trong Bài tập **18**.

20. Cho $f(x) = ax + b$ và $g(x) = cx + d$ với a, b, c, d là các hằng số. Hãy xác định a, b, c, d để $f \circ g = g \circ f$.

21. Chứng tỏ rằng hàm $f(x) = ax + b$ từ **R** đến **R** là khả nghịch với a và b là const và $a \neq 0$. Tìm hàm ngược của f.

22. Cho f là một hàm từ tập A đến tập B. Cho S và T là hai tập con của A. Chứng minh rằng :

a) $f(S \cup T) = f(S) \cup f(T)$ b) $f(S \cap T) \subseteq f(S) \cap f(T)$

23. Cho một ví dụ chứng tỏ rằng bao hàm trong phần b của Bài tập 22 là bao hàm thực sự.

Cho f là một hàm từ tập A đến tập B. Cho S là một tập con của B. Ta định nghĩa tập **nghịch ảnh** *của S là tập con của A chứa tất cả các nghịch ảnh của các phần tử của S. Chúng ta ký hiệu nghịch ảnh của S là $f^{-1}(S)$, sao cho $f^{-1}(S) = \{a \in A \mid f(a) \in S\}$.*

24. Cho f là một hàm từ **R** đến **R** được định nghĩa bởi : $f(x) = x^2$. Tìm :

a) $f^{-1}(\{1\})$ b) $f^{-1}(\{x \mid 0 < x < 1\})$

c) $f^{-1}(\{x \mid x > 4\})$

25. Cho $g(x) = \lfloor x \rfloor$. Tìm :

a) $g^{-1}(\{0\})$ b) $g^{-1}(\{-1, 0, 1\})$

c) $g^{-1}(\{x \mid 0 < x < 1\})$

26. Cho f là một hàm từ tập A đến tập B. Giả sử T và S là hai tập con của B. Chứng minh rằng :

a) $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$ b) $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$

27. Cho f là một hàm từ A đến B và S là một tập con của B. Chứng minh rằng :

$$f^{-1}(\overline{S}) = \overline{f^{-1}(S)}$$

28. Chứng minh rằng $\lceil x \rceil = - \lfloor -x \rfloor$.

29. Cho x là một số thực. Chứng minh rằng

$$\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$$

30. Vẽ đồ thị của hàm $f(n) = 1 - n^2$ từ **Z** đến **Z**.

31. Vẽ đồ thị của hàm $f(x) = \lfloor 2x \rfloor$ từ **R** đến **R**.

32. Vẽ đồ thị của hàm $f(x) = \lfloor \frac{x}{2} \rfloor$ từ **R** đến **R**.

33. Vẽ đồ thị của hàm $f(x) = \lfloor x \rfloor + \lfloor \frac{x}{2} \rfloor$ từ **R** đến **R**.

34. Vẽ đồ thị của hàm $f(x) = \lceil x \rceil + \lfloor \frac{x}{2} \rfloor$ từ **R** đến **R**.

35. Tìm hàm ngược của $f(x) = x^3 + 1$.

36. Giả sử f là một hàm khả nghịch từ Y đến Z và g là hàm khả nghịch từ X đến Y. Chứng minh rằng hàm ngược của hợp thành $f \circ g$ được cho bởi :

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

37. Cho S là một tập con của tập vũ trụ U. **Hàm đặc trưng** f_S của S là hàm từ U đến tập $\{0, 1\}$ sao cho $f_S(x) = 1$ nếu $x \in S$ và $f_S(x) = 0$ nếu $x \notin S$. Cho A và B là hai tập. Chứng tỏ rằng với mọi x

a) $f_{A \cap B}(x) = f_A(x).f_B(x)$

b) $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x).f_B(x)$.

c) $f_{\overline{A}}(x) = 1 - f_A(x)$.

d) $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x)\ f_B(x)$

38. Giả sử f là hàm từ A đến B, trong đó A và B là hai tập hữu hạn có $|A| = |B|$. Chứng minh rằng f là đơn ánh nếu và chỉ nếu nó là toàn ánh.

Một chương trình được thiết kế để tính giá trị của một hàm có thể không tạo ra được giá trị đúng của hàm đó đối với mọi phần tử thuộc miền xác định của hàm ấy. Ví dụ, một chương trình không tạo ra được giá trị đúng do quá trình tính dẫn tới một vòng lặp vô hạn hoặc bị tràn bộ nhớ.

Để nghiên cứu những tình huống này, chúng ta sử dụng khái niệm hàm bộ phận. **Hàm bộ phận** *f từ tập A đến tập B là sự gán cho mỗi phần tử a trong một tập con của A, được gọi là* **miền xác định** *của f, một phần tử duy nhất b thuộc B. A được gọi là miền, B được gọi là* **miền giá trị** *của f. Chúng ta nói rằng f* **không xác định** *đối với các phần tử thuộc A nhưng không thuộc miền xác định của f. Ta viết $f : A \to B$ để ký hiệu f là hàm bộ phận từ A đến B. (Chính ký hiệu này cũng được dùng cho các hàm. Vì vậy tuỳ theo bối cảnh cụ thể mà ta xem f là hàm bộ phận hay hàm toàn phần). Khi ta nói miền xác định của f bằng A, ta muốn nói rằng f là một* **hàm toàn bộ**.

39. Đối với các hàm bộ phận sau, hãy xác định miền, miền giá trị, miền xác định và tập hợp các giá trị mà f không xác định :

a) $f : \mathbf{Z} \to \mathbf{R}$, $f(n) = \frac{1}{n}$

b) $f : \mathbf{Z} \to \mathbf{Z}$, $f(n) = \lceil \frac{n}{2} \rceil$

c) $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Q}$, $f(m, n) = \frac{m}{n}$

d) $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $f(m, n) = mn$

e) $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $f(m, n) = m - n$ nếu $m > n$.

40. a) Chứng minh rằng một hàm bộ phận từ A đến B có thể được xem như một hàm f^* từ A đến $B \cup \{u\}$, ở đây u không phải là phần tử của B và :

$$f^*(a) = \begin{cases} f(a) \text{ nếu } a \text{ thuộc miền xác định của } f \\ u \text{ nếu } f \text{ không xác định tại } a \end{cases}$$

b) Dùng cách xây dựng trong *(a)*, tìm hàm f^* tương ứng với các hàm bộ phận trong bài tập 39.

1.7. DÃY VÀ PHÉP TÍNH TỔNG

MỞ ĐẦU

Dãy thường được dùng để biểu diễn bằng liệt kê các phần tử được sắp thứ tự. Trong toán học rời rạc các dãy được dùng theo nhiều cách. Chúng ta có thể dùng chúng để biểu diễn lời giải của một số bài toán đếm, như chúng ta sẽ thấy trong Chương 5. Chúng cũng là một cơ sở dữ liệu quan trọng trong tin học. Tiết này sẽ ôn lại khái niệm hàm, cũng như ký hiệu dùng để biểu diễn các dãy và ký hiệu lấy tổng các số hạng của dãy.

Khi các phần tử của một tập vô hạn có thể được liệt kê, tập đó sẽ được gọi là đếm được. Trong tiết này chúng ta sẽ xét cả các tập đếm được cũng như không đếm được.

DÃY

Một dãy là một cấu trúc rời rạc được dùng để biểu diễn một bảng liệt kê sắp thứ tự.

ĐỊNH NGHĨA 1. Một *dãy* là một hàm từ một tập con của tập các số nguyên (thường là tập {0, 1, 2,...} hoặc {1, 2, 3, ...}) tới một tập S. Chúng ta dùng ký hiệu a_n để chỉ ảnh của số nguyên n. a_n được gọi là *số hạng* của dãy. Ta dùng ký hiệu $\{a_n\}$ để mô tả một dãy. (Chú ý rằng a_n biểu diễn một số hạng của dãy $\{a_n\}$. Cũng chú ý rằng ký hiệu $\{a_n\}$ đối với dãy dễ lẫn với ký hiệu của một tập hợp. Tuy nhiên, tuỳ thuộc bối cảnh sử dụng các ký hiệu đó mà ta dễ dàng phân biệt khi nào nó dùng để biểu diễn một tập hợp, khi nào để biểu diễn một dãy).

Chúng ta mô tả một dãy bằng cách liệt kê các số hạng của nó theo thứ tự chỉ số dưới tăng dần.

Ví dụ 1. Xét dãy $\{a_n\}$, trong đó

$$a_n = \frac{1}{n}$$

Bảng liệt kê các số hạng của dãy này từ a_1, tức là a_1, a_2, a_3, a_4 ...,

bắt đầu với : $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$

■

Ví dụ 2. Xét dãy $\{b_n\}$ với $b_n = (-1)^n$. Bảng liệt kê các số hạng của dãy này : b_0, b_1, b_2, ..., bắt đầu với 1, −1, 1, −1, 1, ...

■

Ví dụ 3. Xét dãy $c_n = 5^n$. Bảng liệt kê các số hạng của dãy này : C_0, c_1, c_2, c_3, c_4, c_5 ... bắt đầu với : 1, 5, 25, 125, 625, 3125, ...

■

Các dãy có dạng : a_1, a_2, ..., a_n thường được dùng trong tin học. Các dãy hữu hạn này cũng được gọi là các **xâu** và được ký hiệu là a_1, a_2 ... a_n. (Hãy nhớ lại xâu bit. Đó là các dãy bit hữu hạn đã được đưa vào ở Tiết 1.1). **Chiều dài** của xâu S là số các hạng trong xãu đó. **Xâu rỗng** là xâu không có số hạng nào. Xâu rỗng có chiều dài là zêro.

Ví dụ 4. Xâu *abcd* là xâu có chiều dài là 4.

■

PHÉP TÍNH TỔNG

Tiếp theo, ta đưa vào **ký hiệu tổng**, tức là ký hiệu dùng để biểu diễn tổng các số hạng.

$$a_m, a_{m+1}, \ldots a_n$$

của dãy $\{a_n\}$. Ta dùng ký hiệu : $\sum_{j=m}^{n} a_j$

để biểu diễn tổng : $a_m + a_{m+1} + \ldots + a_n$

Ở đây biến j được gọi là **chỉ số lấy tổng** và việc chọn chữ j là hoàn toàn tuỳ ý, điều này có nghĩa là, ta có thể dùng một chữ khác, như i hoặc k, chẳng hạn. Hay dưới dạng ký hiệu,

$$\sum_{j=m}^{n} a_j = \sum_{i=m}^{n} a_i = \sum_{k=m}^{n} a_k$$

Ở đây, chỉ số lấy tổng chạy qua tất cả các số nguyên bắt đầu từ **giới hạn dưới** m và kết thúc ở **giới hạn trên** n. Chữ cái Hy lạp hoa $\sum$ (đọc là sigma) được dùng để ký hiệu phép lấy tổng. Dưới đây là một số ví dụ về ký hiệu lấy tổng.

Ví dụ 5. Biểu diễn tổng của 100 số hạng đầu tiên của dãy $\{a_n\}$ với $a_n = \frac{1}{n}$ và $n = 1, 2, 3, \ldots$

Giải : Giới hạn dưới của chỉ số lấy tổng là 1 và giới hạn trên là 100. Như vậy, tổng đó có thể viết như sau :

$$\sum_{j=1}^{100} \left(\frac{1}{j}\right)$$

■

Ví dụ 6. Xác định giá trị của $\sum_{j=1}^{5} j^2$

Giải : Ta có : $\sum_{j=1}^{5} j^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2$

$= 1 + 4 + 9 + 16 + 25 = 55.$

■

Ví dụ 7. Tính giá trị của $\sum_{k=4}^{8} (-1)^k$

Giải : Ta có :

$$\sum_{k=4}^{8} (-1)^k = (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8$$
$$= 1 + (-1) + 1 + (-1) + 1 = 1.$$

■

Ví dụ 8. *Cấp số nhân* là dãy có dạng : a, ar, ar^2, ar^3, ... ar^k, ở đây a là số hạng đầu, r được gọi là công bội, cả hai đều là số thực. Bây giờ chúng ta sẽ tìm công thức tính tổng S của $n + 1$ số hạng đầu tiên của một cấp số nhân với số hạng đầu là a và công bội r, tức là tính :

$$S = \sum_{j=0}^{n} ar^j$$

Để tính S, ta nhân hai vế phương trình trên với r, rồi biến đổi tổng nhận được như sau :

$$rS = r \sum_{j=0}^{n} ar^j = \sum_{j=0}^{n} ar^{j+1}$$

$$= \sum_{k=1}^{n+1} ar^k \quad \text{(đẳng thức này nhận được bằng cách dịch chỉ số lấy tổng khi đặt } k = j + 1)$$

$$= \sum_{k=0}^{n} ar^k + (ar^{n+1} - a) = S + (ar^{n+1} - a)$$

Từ các đẳng thức trên ta thấy rằng : $rS = S + (ar^{n+1} - a)$

Giải phương trình trên cho S, ta được :

$$S = \frac{ar^{n+1} - a}{r - 1}$$

Nếu $r = 1$, thì hiển nhiên tổng này bằng $(n + 1)a$.

■

Ví dụ 9. Tổng kép cũng thường gặp trong nhiều bài toán. Một ví dụ về tổng kép là :

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij$$

Để tính tổng kép này, trước hết hãy khai triển tổng trong rồi sau đó mới triển khai tính tổng ngoài :

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij = \sum_{i=1}^{4}(i + 2i + 3i) = \sum_{i=1}^{4} 6i$$
$$= 6 + 12 + 18 + 24 = 60$$

■

Chúng ta cũng có thể dùng ký hiệu lấy tổng để cộng tất cả các giá trị của một hàm hoặc các số hạng của một tập có chỉ số, ở đây chỉ số lấy tổng chạy qua tất cả các giá trị trong tập. Tức là, ta có thể viết :

$$\sum_{s\in S} f(s)$$

để biểu diễn tổng các giá trị $f(s)$ đối với mọi phần tử s của S.

Ví dụ 10. Xác định giá trị của $\sum_{s\in\{0,2,4\}} s$?

Giải : Vì $\sum_{s\in\{0,2,4\}} s$ biểu diễn tổng các giá trị của s đối với mọi phần tử của tập {0, 2, 4}, từ đó suy ra

$$\sum_{s\in\{0,2,4\}} s = 0 + 2 + 4 = 6$$

■

BẢN SỐ (Tuỳ chọn)

Hãy nhớ lại rằng, trong Tiết 1.4, bản số của một tập hữu hạn được định nghĩa là số phần tử của tập đó. Ta có thể mở rộng khái niệm bản số cho tất cả các tập, hữu hạn cũng như vô hạn, hàng định nghĩa sau :

ĐỊNH NGHĨA 2. Hai tập A và B có cùng *bản số* nếu và chỉ nếu có một hàm song ánh từ A đến B.

Để thấy rõ định nghĩa này phù hợp với định nghĩa trước của bản số của các tập hữu hạn, ta lưu ý rằng luôn luôn có một hàm song ánh giữa hai tập hữu hạn có cùng n phần tử, ở đây n là một số nguyên không âm.

Chúng ta phân các tập vô hạn thành hai nhóm, nhóm cơ cùng bản số với tập hợp các số tự nhiên và nhóm có bản số khác.

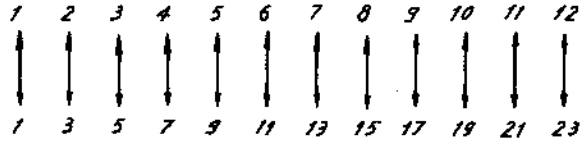
ĐỊNH NGHĨA 3. Các tập hoặc hữu hạn hoặc có cùng bản số với tập hợp các số tự nhiên được gọi là tập *đếm được*. Các tập còn lại được gọi là *không đếm được*.

Dưới đây là ví dụ của các tập đếm được và không đếm được.

Ví dụ 11. Chứng tỏ rằng tập các số nguyên dương lẻ là đếm được.

Giải : Để chứng tỏ tập các số nguyên dương lẻ là đếm được, ta phải chỉ ra một hàm song ánh giữa tập này và tập các số tự nhiên. Hãy xét hàm : $f(n) = 2n - 1$ từ **N** đến tập các số nguyên dương lẻ.

Chúng ta sẽ chứng minh hàm f là song ánh bằng cách chứng tỏ rằng nó là một hàm vừa đơn ánh vừa toàn ánh. Để chứng minh f là đơn ánh, ta giả sử rằng $f(n) = f(m)$. Khi đó, $2n - 1 = 2m - 1$, suy ra $n = m$. Để thấy f là toàn ánh, ta giả sử t là một số nguyên dương lẻ, khi đó nó nhỏ hơn một số chẵn $2k$ nào đó, với k là một số tự nhiên. Từ đó $t = 2k - 1 = f(k)$. Hàm song ánh trên được minh hoạ trên hình 1. ■



Hình 1. Hàm song ánh giữa **N** và tập các số nguyên dương lẻ.

Một tập vô hạn là đếm được nếu và chỉ nếu có thể liệt kê được các phần tử của tập đó thành một dãy (với chỉ số là các số tự nhiên). Lý do là ở chỗ hàm song ánh f từ tập các số tự nhiên đến tập S có thể được biểu diễn qua các số hạng của dãy $a_1, a_2, ..., a_n, ...$ ở đây $a_1 = f(1)$, $a_2 = f(2), ..., a_n = f(n), ...$ Ví dụ, tập các số nguyên dương lẻ có thể được liệt kê thành dãy $a_1, a_2, ... a_n, ...$ với $a_n = 2n - 1$.

Bây giờ chúng ta sẽ cho ví dụ về một tập không đếm được.

Ví dụ 12. Chứng minh rằng tập các số thực là không đếm được.

Giải : Để chứng minh tập các số thực là không đếm được, ta giả sử rằng nó là đếm được và sẽ đi tới mâu thuẫn. Như vậy, khi đó tập con tất cả các số thực nằm trong khoảng 0 và 1 cũng sẽ là đếm được (vì tập con của một tập đếm được cũng là đếm được, xem Bài tập 20 ở cuối Tiết này). Với giả thiết đó, các số thực trong khoảng 0, 1 có thể được liệt kê theo một thứ tự nào đó, ví dụ r_1, r_2, r_3 ... Giả sử biểu diễn thập phân của các số đó là :

$$\begin{aligned} r_1 &= 0, d_{11}\ d_{12}\ d_{13}\ d_{14} \quad \ldots \\ r_2 &= 0, d_{21}\ d_{22}\ d_{23}\ d_{24} \quad \ldots \\ r_3 &= 0, d_{31}\ d_{32}\ d_{33}\ d_{34} \quad \ldots \\ r_4 &= 0, d_{41}\ d_{42}\ d_{43}\ d_{44} \quad \ldots \\ &\vdots \end{aligned}$$

Ở đây $d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (Ví dụ, nếu $r_1 = 0, 23794102...$, chúng ta có $d_{11} = 2$, $d_{12} = 3$, $d_{13} = 7$, v.v.). Sau đó, ta lập một số thực mới với biểu diễn thập phân $r = 0, d_1\ d_2\ d_3\ d_4$ ..., với các chữ số thập phân được xác định theo qui tắc sau :

$$d_i = \begin{cases} 4 \text{ nếu } d_{ii} \neq 4 \\ 5 \text{ nếu } d_{ii} = 4 \end{cases}$$

(Ví dụ , giả sử rằng $r_1 = 0, 23794102$ ..., $r_2 = 0,44590138$ ..., $r_3 = 0,09118764$ ..., $r_4 = 0,80553900$ ... v.v ... Khi đó ta có $r = 0, d_1d_2d_3d_4$ ... $= 0,4544...$ ở đây $d_1 = 4$ vì $d_{11} \neq 4$; $d_2 = 5$ vì $d_{22} = 4$; $d_3 = 4$ vì $d_{33} \neq 4$; $d_4 = 4$ vì $d_{44} \neq 4$ v.v...).

Mỗi một số thực đều có phần thập phân xác định duy nhất. Khi đó số thực r sẽ không bằng bất cứ số nào trong dãy r_1, r_2, r_3 ... vì phần thập phân của r khác với phần thập phân của r_i ở vị trí thứ i bên phải dấu thập phân, đối với mọi i.

Vì có một số thực r nằm trong khoảng giữa 0 và 1 không có mặt trong bảng liệt kê, nên giả thiết rằng tập hợp tất cả các số thực giữa 0 và 1 có thể liệt kê được là sai. Do đó, tập hợp các số thực nằm giữa 0 và 1 là không thể liệt kê được, do đó tập các số thực nằm trong khoảng giữa 0 và 1 là không đếm được. Bất kỳ tập nào có tập con không đếm được cũng sẽ là không đếm được (xem Bài tập 23 ở cuối tiết này). Từ đó suy ra các số thực là không đếm được.

BÀI TẬP

1. Tìm các số hạng sau của dãy $\{a_n\}$, ở đây $a_n = 2.(-3)^n + 5^n$

a) a_0 b) a_1

c) a_4 d) a_5

2. Xác định số hạng a_8 của dãy $\{a_n\}$ nếu a_n bằng :

a) 2^{n-1} b) 7

c) $1 + (-1)^n$ d) $-(-2)^n$

3. Xác định các số hạng a_0, a_1, a_2 và a_3 của dãy $\{a_n\}$ với a_n bằng

a) $2^n + 1$ b) $(n + 1)^{n+1}$

c) $\lfloor \frac{n}{2} \rfloor$ d) $\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil$

4. Xác định a_0, a_1, a_2 và a_3 của dãy $\{a_n\}$ với a_n bằng :

a) $(-2)^n$ b) 3

c) $7 + 4^n$ d) $2^n + (-2)^n$

5. Tính các tổng sau :

a) $\sum_{k=1}^{5} (k + 1)$ b) $\sum_{j=0}^{4} (-2)^j$

c) $\sum_{i=1}^{10} 3$ d) $\sum_{j=0}^{8} (2^{j+1} - 2^j)$

6. Tính giá trị của các tổng sau, ở đây $S = \{1, 3, 5, 7\}$

a) $\sum_{j \in S} j$ b) $\sum_{j \in S} j^2$

c) $\sum_{j \in S} \frac{1}{j}$ d) $\sum_{j \in S} 1$

7. Tính tổng của các cấp số nhân sau :

a) $\sum_{j=0}^{8} 3.2^j$ b) $\sum_{j=1}^{8} 2^j$

c) $\sum_{j=2}^{8} (-3)^j$ d) $\sum_{j=0}^{8} 2.(-3)^j$

8. Tìm giá trị các tổng sau :

a) $\sum_{j=0}^{8} (1 + (-1)^j)$ b) $\sum_{j=0}^{8} (3^j - 2^j)$

c) $\sum_{j=0}^{8} (2.3^j + 3.2^j)$ d) $\sum_{j=0}^{8} (2^{j+1} - 2^j)$

9. Tính các tổng kép sau :

a) $\sum_{i=1}^{2} \sum_{j=1}^{3} (i + j)$ b) $\sum_{i=0}^{2} \sum_{j=0}^{3} (2i + 3j)$

c) $\sum_{i=1}^{3} \sum_{j=0}^{2} i$ d) $\sum_{i=0}^{2} \sum_{j=1}^{3} ij$

10. Tính các tổng kép sau :

a) $\sum_{i=1}^{3} \sum_{j=1}^{2} (i - j)$ b) $\sum_{i=0}^{3} \sum_{j=0}^{2} (3i + 2j)$

c) $\sum_{i=1}^{3} \sum_{j=0}^{2} j$ d) $\sum_{i=0}^{2} \sum_{j=0}^{3} i^2 j^3$

11. Chứng minh rằng $\sum_{j=1}^{n} (a_j - a_{j-1}) = a_n - a_o$, ở đây a_o, a_1, ... a_n là dãy các số thực. Loại tổng này được gọi là **viễn vọng.**

12. Dùng hằng đẳng thức $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$ và Bài tập 11, tính tổng

$$\sum_{k=1}^{n} \frac{1}{k(k+1)}$$

13. Lấy tổng hai vế hằng đẳng thức $k^2 - (k - 1)^2 = 2k - 1$ từ $k = 1$ đến $k = n$ và dùng Bài tập 11 để tìm :

a) công thức tính $\sum_{k=1}^{n} (2k - 1)$ (tổng n số lẻ đầu tiên)

b) công thức tính $\sum_{k=1}^{n} k$.

14*. Dùng kỹ thuật cho trong Bài tập 11, cùng với kết quả Bài tập 13b, tìm công thức tính $\sum_{k=1}^{n} k^2$.

Cũng có một ký hiệu đặc biệt cho tích. Tích $a_m a_{m+1} \ldots a_n$ *được ký hiệu bởi :*

$$\prod_{j=m}^{n} a_j$$

15. Xác định giá trị các tích sau :

a) $\prod_{i=0}^{10} i$ b) $\prod_{i=5}^{8} i$

c) $\prod_{i=1}^{100} (-1)^i$ d) $\prod_{i=1}^{10} 2$

Giá trị của **hàm giai thừa** *tại số nguyên dương n, được ký hiệu là n!, là tích của n số nguyên dương liên tiếp từ 1 đến n. Ta cũng qui ước rằng 0! = 1.*

16. Dùng ký hiệu tích để biểu diễn $n!$

17. Tính $\sum_{j=0}^{4} j!$

18. Tính $\prod_{i=0}^{4} j!$

19. Xác định xem các tập cho sau đây là đếm được hay không đếm được. Đối với các tập hợp đếm được hãy chỉ ra một hàm song ánh từ tập các số tự nhiên đến tập đó.

a) tập các số nguyên âm.

b) tập các số chẵn.

c) tập các số thực nằm giữa 0 và 1/2.

d) tập các số nguyên là bội của 7.

20*. Xác định xem các tập sau là đếm được hay không đếm được. Trong trường hợp đếm được, hãy chỉ ra một hàm song ánh từ tập các số tự nhiên đến tập đó.

a) tập các số nguyên không chia hết cho 3.

b) tập các số nguyên chia hết cho 5 nhưng không chia hết cho 7.

c) tập các số thực trong biểu diễn thập phân chỉ gồm các số 1.

d) tập các số thực trong biểu diễn thập phân chỉ gồm các số 1 hoặc số 9.

21. Nếu A là tập không đếm được và B là tập đếm được, $A - B$ có nhất thiết phải là không đếm được không?

22. Chứng minh rằng tập con của một tập đếm được cũng là đếm được.

23. Chứng minh rằng nếu A là tập không đếm được và $A \subseteq B$ thì B cũng là tập không đếm được.

24*. Chứng minh rằng hợp của hai tập đếm được cũng là đếm được.

25.** Chứng minh rằng hợp của một số đếm được các tập đếm được cũng là đếm được.

26*. Một số thực được gọi là **hữu tỉ** nếu nó có thể được viết dưới dạng thương số của hai số nguyên. Chứng minh rằng tập các số hữu tỷ nằm giữa 0 và 1 là đếm được. (Gợi ý : Liệt kê các phần tử của tập hợp này theo thứ tự tăng của $p + q$, ở đây p là tử số và q là mẫu số của phân số p/q ở dạng tối giản)

27*. Chứng tỏ rằng tập tất cả các xâu bit là đếm được.

28*. Chứng tỏ rằng tập hợp các số thực là nghiệm của phương trình bậc hai $ax^2 + bx + c = 0$ với a, b, c là các số nguyên, là đếm được.

29*. Chứng tỏ rằng tập hợp tất cả các chương trình máy tính trong một ngôn ngữ lập trình đặc biệt nào đó là đếm được. (Gợi ý : Một chương trình được viết trong một ngôn ngữ lập trình nào đó có thể được xem như một xâu ký tự lấy từ một bảng chữ cái hữu hạn).

30*. Chứng minh rằng tập các hàm từ các số nguyên dương tới tập {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} là không đếm được. (Gợi ý : hước đầu tiên là lập một hàm song ánh giữa tập các số thực nằm giữa 0 và 1 và một tập con các hàm đó, ví dụ bằng cách gán cho số thực 0, d_1d_2, $d_3 \ldots d_n \ldots$ hàm f với $f(n) = d_n$).

31*. Ta nói ràng một hàm là **tính được** nếu có một chương trình máy tính cho phép tlm được các giá trị của hàm đó. Dùng Bài tập 29 và 30 chứng minh rằng có các hàm là không tính được.

1.8. ĐỘ TĂNG CỦA HÀM

MỞ ĐẦU

Giả sử rằng một chương trình máy tính sắp thứ tự lại một bảng liệt kê những số nguyên trong đó các số nguyên được xếp theo thứ tự tăng dần. Một vấn đề quan trọng liên quan đến tính thực tiễn của chương trình này là máy tính phải mất bao lâu mới giải xong bài toán này. Sự phân tích cho thấy rằng thời gian được dùng để sắp lại một bảng liệt kê những số nguyên (những số này nhỏ hơn một cỡ nào đó đã được chỉ rõ) là nhỏ hơn $f(n)$ micro giây, với $f(n) = 100n\log n + 25n + 9$. Để phân tích tính thực tiễn của chương trình này, chúng ta cần phải hiểu hàm này tăng nhanh như thế nào khi n tăng. Trong tiết này chúng ta sẽ ôn lại một số phương pháp quan trọng được dùng để đánh giá độ tăng của các hàm số. Chúng ta sẽ đưa vào một khái niệm được dùng hết sức rộng rãi trong việc phân tích độ tăng của các hàm, đó là khái niệm O (tiếng Anh là hig O – nghĩa là chữ O lớn). Chúng ta cũng sẽ đưa ra một số kết quả tiện ích về độ tăng của các hàm khi dùng khái niệm này.

KHÁI NIỆM O (big-O)

Độ tăng của các hàm thường được mô tả bằng cách dùng một khái niệm đặc hiệt được định nghĩa như sau :

ĐỊNH NGHĨA 1. Cho f và g là hai hàm từ tập các số nguyên hoặc số thực đến tập các số thực. Ta nói $f(x)$ là $O(g(x))$ nếu tồn tại hai hằng số C và k sao cho :

$$|f(x)| \leqslant C|g(x)|$$

với mọi $x > k$.

Chú ý : Để chứng minh $f(x)$ là $O(g(x))$, ta chỉ cần tìm *một* cặp hằng số C và k sao cho $|f(x)| \leqslant C|g(x)|$ nếu $x > k$. Tuy nhiên một cặp C và

k thoả mãn điều kiện đó *không bao giờ* là duy nhất. Hơn thế nữa, nếu đã có một cặp như vậy tồn tại, thì sẽ có *vô số* các cặp như thế. Một cách đơn giản để thấy điều này là lưu ý rằng nếu C, k là một cặp như vậy thì cặp C', k' với $C < C'$ và $k < k'$ cũng sẽ thoả mãn định nghĩa trên, vì $|f(x)| \leq C|g(x)| \leq C'|g(x)|$ với mọi $x > k' > k$.

Ví dụ 1. Chứng minh rằng $f(x) = x^2 + 2x + 1$ là $O(x^2)$

Giải : Vì $0 \leq x^2 + 2x + 1 \leq x^2 + 2x^2 + x^2 = 4x^2$

với mọi $x > 1$, từ đó suy ra $f(x)$ là $O(x^2)$.

(Để áp dụng định nghĩa 1 ở trên, ở đây ta lấy $C = 4$ và $k = 1$. Ta cũng không cần phải sử dụng ở đây dấu giá trị tuyệt đối, vì tất cả các hàm trong các đẳng thức này đều là dương khi x dương).

Một cách giải khác là lưu ý rằng khi $x > 2$, suy ra $2 \leq x^2$. Do đó, nếu $x > 2$, ta có :

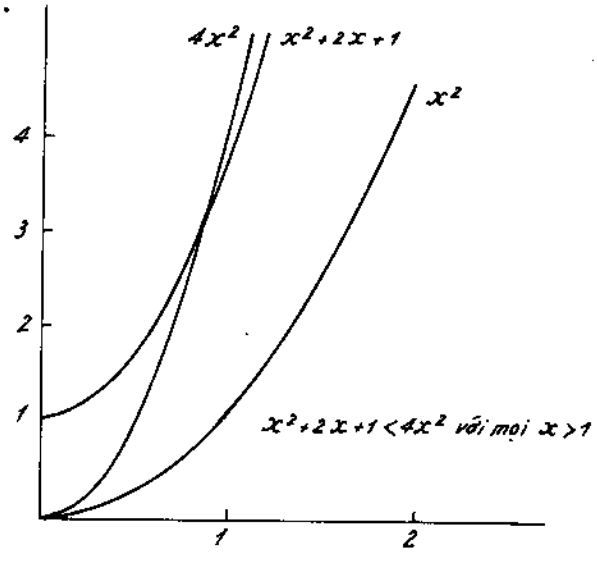
$$0 \leq x^2 + 2x + 1 \leq x^2 + x^2 + x^2 = 3x^2$$

(Chúng ta áp dụng định nghĩa ở đây với $C = 3$ và $k = 2$).

Cần thấy rằng trong mối quan hệ $f(x)$ là $O(x^2)$, x^2 có thể thay bằng một hàm có giá trị lớn hơn x^2, ví dụ $f(x)$ là $O(x^3)$, $f(x)$ là $O(x^2 + 2x + 7)$, v.v... Mặt khác, ta cũng có x^2 là $O(x^2 + 2x + 1)$, vì $x^2 < x^2 + 2x + 1$ với mọi $x \geq 1$.

Hình 1 minh hoạ $x^2 + 2x + 1$ là $O(x^2)$. ■

Chú ý rằng trong Ví dụ 1 ta có hai hàm, $f(x) = x^2 + 2x + 1$ và $g(x) = x^2$ sao cho $f(x)$ là $O(g(x))$ và



Hình 1. Hàm $x^2 + 2x + 1$ là $O(x^2)$

$g(x)$ là $O(f(x))$ (điều này suy ra từ bất đẳng thức $x^2 \leq x^2 + 2x + 1$, bất đẳng thức này đúng với mọi x không âm). Ta nói hai hàm $f(x)$ và $g(x)$ thoả mãn cả hai quan hệ big - O nói ở trên là có *cùng bậc* (xem các Bài tập 22 – 25).

Khái niệm big-O đã được dùng trong toán học đã gần một thế kỷ nay. Trong tin học, nó được sử dụng rộng rãi để phân tích các thuật toán, như chúng ta sẽ thấy ở Chương 2. Nhà toán học người Đức Paul Bachmann là người đầu tiên đưa ra khái niệm big-O vào năm 1892 trong một cuốn sách nổi tiếng về lý thuyết số. Ký hiệu big-O đôi khi còn gọi là **ký hiệu Landau**, theo tên của nhà toán học Đức Edmund Landau, người đã dùng ký hiệu này trong suốt các công trình của mình.

Khi $f(x)$ là $O(g(x))$ và $h(x)$ là hàm có giá trị tuyệt đối lớn hơn $g(x)$ đối với các giá trị đủ lớn của x, ta suy ra rằng $f(x)$ là $O(h(x))$. Nói cách khác, hàm $g(x)$ trong quan hệ $f(x)$ là $O(g(x))$ có thể được thay bằng một hàm có giá trị tuyệt đối lớn hơn. Để thấy điều đó, chú ý rằng, nếu

$$|f(x)| \leq C|g(x)| \qquad \text{với mọi } x > k$$

và nếu $\qquad |h(x)| > |g(x)| \qquad$ với mọi $x > k$, thì :

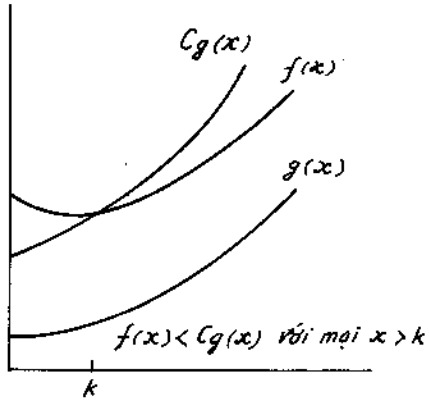
$$|f(x)| \leq C|h(x)| \qquad \text{với mọi } x > k.$$

Từ đó, $f(x)$ là $O(h(x))$.

Khi dùng khái niệm big-O, hàm g trong quan hệ $f(x)$ là $O(g(x))$ được chọn là nhỏ nhất có thể được (đôi khi lấy từ tập các hàm sơ cấp, như các hàm có dạng x^n với n là một số nguyên dương).

Trong những thảo luận dưới đây, ta sẽ đề cập chủ yếu tới các hàm chỉ nhận giá trị dương, nên ta sẽ bỏ các dấu giá trị tuyệt đối trong các biểu thức liên quan việc đánh giá big-O của các hàm. Hình 2 minh hoạ mối quan hệ $f(x)$ là $O(g(x))$.

Ví dụ sau đây minh hoạ khái niệm big-O được dùng để đánh giá độ tăng của các hàm như thế nào.



Hình 2. Hàm $f(x)$ là $O(g(x))$

Ví dụ 2. Chứng minh rằng $7x^2$ là $O(x^3)$.

Giải : Bất đẳng thức $7x^2 < x^3$ đúng với mọi $x > 7$. (Để thấy điều này chỉ cần chia hai vế bất đẳng thức đó cho x^2). Do đó, $7x^2$ là $O(x^3)$, khi lấy $C = 1$ và $k = 7$ trong định nghĩa của khái niệm big-O.

■

Ví dụ 3. Ví dụ 2 chứng tỏ rằng $7x^2$ là $O(x^3)$. Liệu có thể x^3 là $O(7x^2)$ không?

Giải : Để xác định xem x^3 có là $O(7x^2)$ không, cần phải xem có tồn tại các hằng số C và k sao cho $x^3 \leq C(7x^2)$ với mọi $x > k$ hay không. Bất đẳng thức trên tương đương với bất đẳng thức $x \leq 7C$ (điều này nhận được khi chia 2 vế của bất đẳng thức cho x^2). Không thể tồn tại một hằng số C nào như vậy vì x có thể lớn tuỳ ý. Vậy x^3 không là $O(7x^2)$.

Các đa thức thường được dùng để đánh giá độ tăng của các hàm. Thay vì phải phân tích độ tăng của các đa thức mỗi khi cần thiết, ta muốn có một kết quả có thể dùng được ngay để đánh giá độ tăng của một đa thức. Định lý sau cho phép làm được điều đó.

Định lý 1. Cho $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, ở đây a_0, a_1, $\ldots$, a_n là các số thực. Khi đó $f(x)$ là $O(x^n)$.

Chứng minh : Dùng bất đẳng thức tam giác, nếu $x > 1$, ta có

$$\begin{aligned} |f(x)| &= |a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0| \\ &\leq |a_n|x^n + |a_{n-1}|x^{n-1} + \ldots + |a_1|x + |a_0| \\ &= x^n\left(|a_n| + \frac{|a_{n-1}|}{x} + \ldots + \frac{|a_1|}{x^{n-1}} + \frac{|a_0|}{x^n}\right) \\ &\leq x^n(|a_n| + |a_{n-1}| + \ldots + |a_1| + |a_0|) \end{aligned}$$

Điều này chứng tỏ rằng

$$|f(x)| \leq Cx^n$$

ở đây $C = |a_n| + |a_{n-1}| + \ldots + |a_1| + |a_0|$, với mọi $x > 1$. Từ đó suy ra $f(x)$ là $O(x^n)$.

Dưới đây là một số ví dụ về các hàm có miền xác định là tập hợp các số nguyên đương.

là một số ví dụ về các hàm có miền xác định là tập hợp các số nguyên dương.

Ví dụ 4. Dùng khái niệm hig-O đánh giá tổng n số nguyên dương đầu tiên.

Giải : Vì mỗi số nguyên trong tổng n số nguyên dương đầu tiên đều không vượt quá n, suy ra :

$$1 + 2 + \ldots + n \leqslant n + n + \ldots + n = n^2$$

Từ bất đẳng thức này suy ra $1 + 2 + \ldots + n$ là $O(n^2)$, khi lấy $C = 1$, $k = 1$ trong định nghĩa của khái niệm big-O (Chú ý rằng hàm trong quan hệ big - O ở đây có miền xác định là tập các số nguyên dương). ■

Những ví dụ sau đây liên quan đến hàm giai thừa và hàm logarit. Việc đánh giá hig-O của các hàm này có vai trò quan trọng trong việc phân tích số các hước được dùng trong các thủ tục sắp xếp (sorting).

Ví dụ 5. Cho ước lượng hig-O của hàm giai thừa và hàm logarit của hàm giai thừa.

Chú ý hàm giai thừa tăng rất nhanh, ví dụ :

$$1! = 1 \ , \ 2! = 1.2 = 2 \ , \ 3! = 1.2.3 = 6$$

$$4! = 1.2.3.4 = 24 \ , \text{ nhưng } 20! = 2.432.902.008.176.640.000)$$

Giải : Vì mỗi số hạng trong tích của n ! đều không vượt quá n, ta có :

$$n! = 1.2.3... \ n \leqslant n.n.n \ ... \ n = n^n$$

Bất đẳng thức này chứng tỏ $n!$ là $O(n^n)$. Lấy logarit hai vế bất đẳng thức vừa tìm được ở trên, ta nhận được :

$$\log n! \leqslant \log n^n = n \log n$$

Suy ra $\log n!$ là $O(n \log n)$. ■

Ví dụ 6. Trong Tiết 3.2, ta sẽ chứng minh rằng : $n < 2^n$

với mọi n nguyên dương. Dùng bất đẳng thức đó chúng ta có thể kết luận rằng n là $O(2^n)$ (lấy $k = C = 1$ trong định nghĩa của khái niệm hig-O). Vì hàm logarit (cơ số 2) đồng biến, nên lấy logarit hai vế bất đẳng thức trên, ta có : $\log n < n$. Từ đó suy ra : $\log n$ là $O(n)$ (lại lấy $C = k = 1$ trong định nghĩa của big-O).

Nếu chúng ta dùng logarit cơ số b, với b khác 2, ta cũng có : $\log_b n$ là $O(n)$, vì :

$$\log_b n = \frac{\log n}{\log b} < \frac{n}{\log b}$$

với mọi n nguyên dương.

ĐỘ TĂNG CỦA TỔ HỢP CÁC HÀM

Nhiều thuật toán được tạo bởi hai hoặc nhiều thủ tục con tách rời nhau. Số các bước mà máy tính sử dụng để giải một bài toán với đầu vào (input) có qui mô xác định theo các thuật toán đó là tổng số bước cần thiết, vì vậy cần phải tìm những đánh giá big-O đối với số bước mà mỗi thủ tục con đã sử dụng, rồi sau đó tổ hợp các đánh giá đó lại.

Những đánh giá big-O đối với tổ hợp của các hàm có thể nhận được nếu ta lưu ý khi các đánh giá big-O khác nhau được tổ hợp với nhau. Đặc biệt, cần phải đánh giá độ tăng của tổng và tích của các hàm. Cụ thể, ta có thể nói gì nếu các đánh giá big-O của mỗi hàm đều đã biết? Giả sử $f_1(x)$ là $O(g(x))$ và $f_2(x)$ là $O(g_2(x))$. Theo định nghĩa của khái niệm big-O, khi đó tồn tại các hằng số C_1, C_2, k_1 và k_2 sao cho,

$$|f_1(x)| \leqslant C_1|g_1(x)| \quad \text{với mọi } x > k_1$$

và

$$|f_2(x)| \leqslant C_2|g_2(x)| \text{ với mọi } x > k_2$$

Để đánh giá tổng của $f_1(x)$ và $f_2(x)$, chú ý rằng :

$$|(f_1 + f_2)(x)| = |f_1(x) + f_2(x)| \leqslant |f_1(x)| + |f_2(x)|$$

(ở đây chúng ta đã dùng bất đẳng thức tam giác $|a + b| \leqslant |a| + |b|$).

Khi x lớn hơn cả k_1 lẫn k_2, ta suy ra các bất đẳng thức cho tổng của $|f_1(x)|$ và $|f_2(x)|$ như sau :

$$|f_1(x)| + |f_2(x)| \leqslant C_1|g_1(x)| + C_2|(g_2(x)|$$

$$\leqslant C_1|g(x)| + C_2|g(x)| = (C_1 + C_2)|g(x)| = C|g(x)|$$

ở đây $C = C_1 + C_2$ và $g(x) = \max(|g_1(x)|, |g_2(x)|)$, $\max(a, b)$ ký hiệu số lớn nhất trong hai số đó).

Bất đẳng thức trên chứng tỏ rằng $|(f_1 + f_2)(x)| \leqslant C|g(x)|$ với mọi $x > k$ ở đây $k = \max(k_1, k_2)$. Kết quả tiện ích này được phát biểu thành định lý sau :

Định lý 2. Cho $f_1(x)$ là $O(g_1(x))$ và $f_2(x)$ là $O(g_2(x))$. Khi đó $(f_1 + f_2)(x)$ là $O(\max(g_1(x), g_2(x)))$.

Thường chúng ta có những đánh giá big-O của f_1 và f_2 qua một hàm $g(x)$. Trong tình hình đó, Định lý 2 có thể được dùng để chứng minh rằng $(f_1 + f_2)(x)$ cũng là $O(g(x))$ vì $\max(g_1(x), g_2(x)) = g(x)$. Kết quả trên cho hệ quả sau :

Hệ quả 1. Cho $f_1(x)$ và $f_2(x)$, cả hai đều là $O(g(x))$. Khi đó $(f_1 + f_2)(x)$ là $O(g(x))$.

Theo cách tương tự ta có thể dẫn ra những đánh giá big-O đối với tích của hai hàm f_1 và f_2. Khi x lớn hơn $\max(k_1, k_2)$, suy ra :

$$\begin{aligned} |(f_1f_2)(x)| &= |f_1(x)||f_2(x)| \leq C_1|g_1(x)|C_2|g_2(x)| \\ &\leq C_1C_2|(g_1g_2)(x)| \leq C|(g_1g_2)(x)| \end{aligned}$$

Ở đây $C = C_1C_2$. Từ bất đẳng thức trên, suy ra $f_1(x)f_2(x)$ là $O(g_1g_2)$, vì tồn tại các hằng số C và k, cụ thể là $C = C_1C_2$ và $k = \max(k_1, k_2)$ sao cho $|(f_1f_2)(x)| \leq C|g_1(x)g_2(x)|$ với mọi $x > k$. Kết quả này được phát biểu thành định lý sau :

Định lý 3. Cho $f_1(x)$ là $O(g_1(x))$ và $f_2(x)$ là $O(g_2(x))$. Khi đó $(f_1f_2)(x)$ là $O(g_1(x)\ g_2(x))$.

Mục đích trong việc dùng khái niệm hig-O để đánh giá các hàm là chọn hàm g tăng tương đối chậm với $f(x)$ là $O(g(x))$. Ví dụ sau minh hoạ ta có thể dùng các Định lý 2 và 3 để làm điều đó như thế nào. Loại phân tích được cho trong các ví dụ này thường được dùng để phân tích thời gian giải các bài toán bằng các chương trình máy tính.

Ví dụ 7. Cho một đánh giá big-O đối với hàm

$$f(x) = 3n\log(n!) + (n^2 + 3)\log n \text{ với } n \text{ là số nguyên dương.}$$

Giải : Trước hết, ta đánh giá tích $3n \log (n\ !)$. Từ Ví dụ 5 ta biết rằng $\log (n\ !)$ là $O(n\log n)$. Dùng đánh giá này và lưu ý rằng $3n$ là $O(n)$, Định lý 3 sẽ cho ta $3n\log(n!)$ là $O(n^2\log n)$.

Tiếp theo, ta đánh giá tích $(n^2 + 3)\log n$. Vì $n^2 + 3 < 2n^2$ khi n > 2, suy ra $(n^2 + 3)$ là $O(n^2)$. Do đó, từ Định lý 3 suy ra : $(n^2 + 3)\log n$ là $O(n^2\log n)$. Dùng Định lý 2 kết hợp với hai đánh giá big-O vừa tìm được ở trên, ta được :

$$f(n) = 3n\log(n!) + n^2\log n \text{ là } O(n^2\log n)$$

■

Ví dụ 8. Cho một đánh giá big–O đối với

$$f(x) = (x + 1)\log(x^2 + 1) + 3x^2.$$

Giải : Trước hết, ta hãy đánh giá tích $(x + 1)\log(x^2 + 1)$.

Chú ý rằng $(x + 1)$ là $O(x)$. Hơn nữa, $x^2 + 1 \leq 2x^2$ khi $x > 1$. Từ đó,

$$\log(x^2 + 1) \leq \log(2x^2) = \log 2 + \log x^2$$

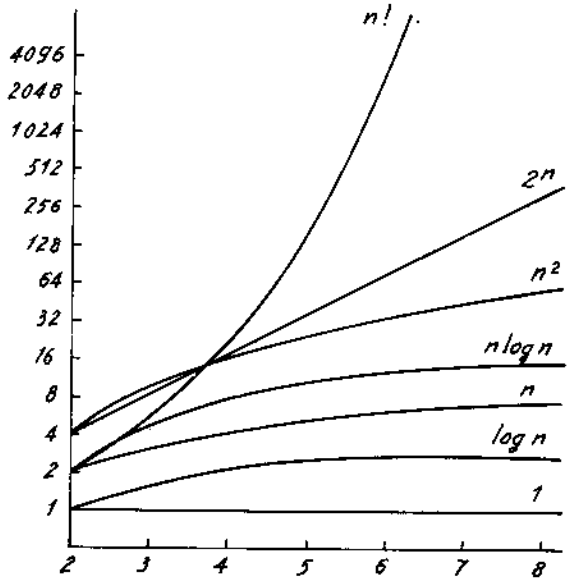
$$= \log 2 + 2\log x \leq 3\log x,$$

nếu $x > 2$. Điều này chứng tỏ rằng : $\log(x^2 + 1)$ là $O(\log x)$.

Từ Định lý 3 suy ra rằng $(x + 1)\log(x^2 + 1)$ là $O(x\log x)$. Vì $3x^2$ là $O(x^2)$, Định lý 2 cho ta $f(x)$ là $O(\max(x\log x, x^2))$. Vì $x\log x \leq x^2$ với mọi $x > 1$, suy ra $f(x)$ là $O(x^2)$.

Như đã nói ở trên, khái niệm big–O được dùng để đánh giá số các công đoạn cần thiết để giải một bài toán hằng một thủ tục hoặc một thuật toán xác định nào đó. Các hàm thường được dùng trong các đánh giá này là : 1, $\log n$, n, $n\log n$, n^2, 2^n và $n!$.

Dùng giải tích ta có thể chứng minh rằng mỗi hàm trong bảng liệt kê trên đều nhỏ hơn hàm đứng tiếp sau nó. Nhỏ hơn ở đây hiểu theo nghĩa tỷ số của một hàm và hàm đứng sau nó tiến tới 0 khi $x \to \infty$. Hình 3 cho đồ thị của các hàm kể ở trên. (Chú ý ở đây thang đối với giá trị của các hàm tăng gấp đôi đối với mỗi vạch kế tiếp trên đồ thị).



Hình 3. Biểu diễn độ tăng của các hàm thường được dùng trong đánh giá big–O.

BÀI TẬP

1. Các hàm sau có là $O(x)$ không?

a) $f(x) = 10$ b) $f(x) = 3x + 7$

c) $f(x) = x^2 + x + 1$ d) $f(x) = 5\log x$

e) $f(x) = \lfloor x \rfloor$ f) $f(x) = \lceil \frac{x}{2} \rceil$

2. Các hàm sau có là $O(x^2)$ không?

a) $f(x) = 17x + 11$ b) $f(x) = x^2 + 1000$

c) $f(x) = x\log x$ d) $f(x) = \frac{x^4}{2}$

e) $f(x) = 2^x$ f) $f(x) = \lfloor x \rfloor \lceil x \rceil$

3. Dùng định nghĩa, chứng minh rằng $x^4 + 9x^3 + 4x + 7$ là $O(x^4)$

4. Dùng định nghĩa chứng minh rằng $2^x + 17$ là $O(3^x)$.

5. Chứng minh rằng $\frac{x^2 + 1}{x + 1}$ là $O(x)$

6. Chứng minh rằng $\frac{x^3 + 2x}{2x + 1}$ là $O(x^2)$

7. Tìm một số nguyên n nhỏ nhất sao cho $f(x)$ là $O(x^n)$ đối với các hàm $f(x)$ sau :

a) $f(x) = 2x^3 + x^2\log x$ b) $f(x) = 2x^3 + (\log x)^4$

c) $f(x) = \frac{x^4 + x^2 + 1}{x^3 + 1}$ d) $f(x) = \frac{x^5 + 5\log x}{x^4 + 1}$

8. Cũng hỏi như Bài tập 7 cho các hàm $f(x)$ sau :

a) $f(x) = 2x^2 + x^3\log x$ b) $f(x) = 3x^5 + (\log x)^4$

c) $f(x) = \frac{x^4 + x^2 + 1}{x^4 + 1}$ d) $f(x) = \frac{x^3 + 5\log x}{x^4 + 1}$

9. Chứng minh $x^2 + 4x + 17$ là $O(x^3)$, nhưng x^3 không là $O(x^2 + 4x + 17)$.

10. Chứng minh x^3 là $O(x^4)$, nhưng x^4 không là $O(x^3)$.

11. Chứng minh rằng $3x^4 + 1$ là $O(x^4/2)$ và $x^4/2$ là $O(3x^4 + 1)$.

12. Chứng minh rằng $x\log x$ là $O(x^2)$, nhưng x^2 không là $O(x\log x)$

13. Chứng minh rằng 2^n là $O(3^n)$, nhưng 3^n không là $O(2^n)$.

14. Với các hàm $g(x)$ cho dưới đây, x^3 có là $O(g(x))$ không?

a) $g(x) = x^2$ b) $g(x) = x^3$

c) $g(x) = x^2 + x^3$ d) $g(x) = x^2 + x^4$

e) $g(x) = 3^x$ f) $g(x) = \dfrac{x^3}{2}$

15. Giải thích ý nghĩa của điều là : $f(x)$ là $O(1)$.

16. Chứng minh rằng nếu $f(x)$ là $O(x)$ thì $f(x)$ là $O(x^2)$.

17. Cho $f(x)$, $g(x)$ và $h(x)$ là các hàm sao cho $f(x)$ là $O(g(x))$ và $g(x)$ là $O(h(x))$. Chứng minh rằng $f(x)$ là $O(h(x))$.

18. Cho k là một số nguyên dương. Chứng minh rằng $1^k + 2^k + ... + n^k$ là $O(n^{k+1})$.

19. Hãy cho một đánh giá big-O tốt nhất có thể được đối với các hàm sau :

a) $(n^2 + 8)(n + 1)$ b) $(n\log n + n^2)(n^3 + 2)$

c) $(n! + 2^n)(n^3 + \log(n^2 + 1))$.

20. Cho một đánh giá big-O đối với các hàm cho dưới đây. Đối với các hàm $g(x)$ trong đánh giá $f(x)$ là $O(g(x))$. Hãy chọn các hàm đơn giản có bậc thấp nhất.

a) $(n^3 + n^2 \log n)(\log n + 1) + (17\log n + 19)(n^3 + 2)$

b) $(2^n + n^2)(n^3 + 3^n)$

c) $(n^n + n\,2^n + 5^n)(n! + 5^n)$.

21. Cho một đánh giá big-O đối với các hàm cho dưới đây. Đối với hàm $g(x)$ trong đánh giá $f(x)$ là $O(g(x))$ hãy chọn hàm đơn giản có bậc thấp nhất.

a) $n\log(n^2 + 1) + n^2\log n$

b) $(n\log n + 1)^2 + (\log n + 1)(n^2 + 1)$

c) $n^{2^n} + n^{n^2}$.

Cho $f(x)$ và $g(x)$ là các hàm từ tập các số thực hoặc tập các số nguyên dương đến tập các số thực. Ta viết $f(x)$ là $\Theta(g(x))$ khi tồn tại các số thực dương C_1 và C_2 và một số nguyên dương k sao cho :

$$C_1|g(x)| \leqslant |f(x)| \leqslant C_2|g(x)|$$

với mọi $x > k$.

22. a) Chứng minh rằng : $3x + 7$ là $\theta(\xi)$
h) Chứng minh rằng : $2x^2 + x - 7$ là $\theta(x^2)$
c) Chứng minh rằng : $\lfloor x + 1/2 \rfloor$ là $\theta(x)$
d) Chứng minh rằng : $\log(x^2 + 1)$ là $\theta(\log_2 x)$
e) Chứng minh rằng : $\log_{10} x$ là $\theta(\log_2 x)$

23. Chứng minh rằng $f(x)$ là $\Theta(g(x))$ nếu và chỉ nếu $f(x)$ là $O(g(x))$ và $g(x)$ là $O(f(x))$.

24. a) Chứng minh rằng $3x^2 + x + 1$ là $\theta(3x^2)$

b) Biểu diễn bằng hình vẽ mối quan hệ ở câu a), bằng cách dựng đồ thị của các hàm $3x^2 + x + 1$, $C_1.3x^2$ và $C_2.3x^2$; chỉ vị trí của k trên trục x với C_1, C_2 và k đã tìm được ở câu *a)*.

25. Biểu diễn mối quan hệ $f(x)$ là $\Theta(g(x))$ bằng hình vẽ. Cho đồ thị của các hàm $f(x)$, $C_1|g(x)|$ và $C_2|g(x)|$ cũng như hằng số k trên trục x.

26. Cho một đánh giá big–O đối với tích n số nguyên dương lẻ đầu tiên.

27. Chứng minh rằng nếu f và g là các hàm có giá trị thực sao cho $f(x)$ là $O(g(x))$, thì $f^k(x)$ là $O(g^k(x))$.
(Chú ý rằng $f^k(x) = f(x)^k$)

28. Chứng minh rằng nếu $f(x)$ là $O(\log_b x)$ với $b > 1$ thì $f(x)$ là $O(\log_a x)$ với $a > 1$.

29. Cho $f(x)$ là $O(g(x))$ với f và g là các hàm đơn điệu tăng và không giới nội. Chứng minh rằng $|f(x)|$ là $O(\log|g(x)|)$.

30. Cho $f(x)$ là $O(g(x))$. Từ đó có thể suy ra $2^{f(x)}$ là $O(2^{g(x)})$ không?

Các bài tập sau liên quan đến một loại khái niệm tiệm cận khác, được gọi là khái niệm **little-o** (chữ o nhỏ). *Vì khái niệm little-o dựa trên khái niệm giới hạn, nên để giải các bài tập này cần có kiến thức về giải tích. Ta nói $f(x)$ là $o(g(x))$, khi :*

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0$$

31. Chứng minh rằng

a) x^2 là $o(x^3)$ b) $x\log x$ là $o(x^2)$

c) x^2 là $o(2^x)$ d) $x^2 + x + 1$ không là $o(x^2)$

32. a) Chứng minh rằng nếu $f(x)$ và $g(x)$ là các hàm sao cho $f(x)$ là $o(g(x))$ và c là một hằng số, thì $cf(x)$ là $o(g(x))$.

b) Chứng minh rằng nếu $f_1(x)$, $f_2(x)$ và $g(x)$ là các hàm sao cho $f_1(x)$ là $o(g(x))$ và $f_2(x)$ là $o(g(x))$, thì $(f_1 + f_2)(x)$ là $o(g(x))$, với $(f_1 + f_2)(x) = f_1(x) + f_2(x)$.

33. Biểu diễn trên hình vẽ quan hệ $x\log x$ là $o(x^2)$ bằng cách vẽ đồ thị các hàm $x\log x$, x^2 và $x\log x/x^2$. Hãy giải thích xem bằng cách nào hình vẽ đó cho thấy $x\log x$ là $o(x^2)$.

34. Biểu diễn mối quan hệ $f(x)$ là $o(g(x))$ bằng hình vẽ. Vẽ phác đồ thị của các hàm $f(x)$, $g(x)$ và $f(x)/g(x)$.

35*. Cho $f(x)$ là $o(g(x))$. Từ đây có suy ra $2^{f(x)}$ là $o(x^{g(x)})$ không?

36*. Cho $f(x)$ là $o(g(x))$, liệu từ đó có suy ta $\log|f(x)|$ là $o(\log|g(x)|)$ không?

37. Hai câu của Bài tập này mô tả mối quan hệ giữa khái niệm big–O và little–o.

a) Chứng minh rằng nếu $f(x)$ và $g(x)$ là các hàm sao cho $f(x)$ là $o(g(x))$, thì $f(x)$ là $O(g(x))$.

b) Chứng tỏ rằng nếu $f(x)$ và $g(x)$ là các hàm sao cho $f(x)$ là $O(g(x))$, thì không nhất thiết suy ra $f(x)$ là $O(g(x))$.

38. Chứng minh rằng nếu $f(x)$ là một đa thức bậc n và $g(x)$ là một đa thức bậc m, với $m > n$) thì $f(x)$ là $o(g(x))$.

39. Chứng minh rằng nếu $f_1(x)$ là $O(g(x))$ và $f_2(x)$ là $o(g(x))$ thì $f_1(x) + f_2(x)$ là $O(g(x))$.

40. Cho H_n là **số điều hoà thứ** n

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

Chứng minh rằng H_n là $O(\log n)$. (*Gợi ý* : Trước hết chứng minh bất đẳng thức : $\sum_{j=2}^{n} \frac{1}{j} < \int_{1}^{n} \frac{1}{x} dx$ bằng cách chứng tỏ rằng tổng diện tích các

hình chữ nhật có chiều cao 1/j, chiều rộng từ $j - 1$ đến j với $j = 2, 3, \ldots n$ nhỏ hơn diện tích nằm dưới đường cong $1/x$ từ $x = 2$ đến $x = n$).

41*. Chứng minh rằng $n \log n$ là $O(\log n!)$.

42. Xác định xem $\log(n!)$ có là $O(n \log n)$ không? Giải thích.

CÂU HỎI ÔN TẬP

1. a) Định nghĩa phủ định của một mệnh đề.
   b) Tìm phủ định của mệnh đề "Đây là một khoá học buồn".
2. a) (Dùng bảng giá trị chân lý) định nghĩa các phép tuyển, hội, tuyển loại, kéo theo và tương đương của hai mệnh đề p và q.
   b) Xác định mệnh đề tuyển, hội, tuyển loại, kéo theo và tương đương của hai mệnh đề "Tôi sẽ đi xem phim tối nay" và "Tôi sẽ làm hết các bài tập toán rời rạc".
3. a) Nêu ít nhất năm cách viết khác nhau ra ngôn ngữ thông thường của mệnh đề kéo theo $p \rightarrow q$.
   b) Định nghĩa mệnh đề đảo và phản đảo của mệnh đề kéo theo.
   c) Phát biểu mệnh đề phản đảo của mệnh đề "Nếu ngày mai trời nắng, tôi sẽ đi chơi trong rừng".
4. a) Thế nào là hai mệnh đề tương đương logic?
   b) Nêu các cách để chứng minh hai mệnh đề phức hợp là tương đương logic.
   c) Chứng minh ít nhất bằng hai cách hai mệnh đề phức hợp $\neg p \vee (r \rightarrow \neg q)$ và $\neg p \vee \neg q \vee \neg r$ là tương đương logic.
5. (Xem lại các Bài tập ở tiết 1.2)
   a) Cho một bảng giá trị chân lý, hãy giải thích xem làm thế nào dùng dạng tuyển chính tắc lập được mệnh đề phức hợp có bảng giá trị chân lý đó.
   b) Hãy giải thích tại sao câu a chứng tỏ các toán tử $\wedge$, $\vee$ và $\neg$ là đầy đủ.
   c) Liệu có một toán tử sao cho tập hợp chỉ chứa toán tử đó là đầy đủ không?

6. Lượng từ tồn tại và phổ dụng của hàm mệnh đề $P(x)$ là gì? Xác định phủ định của chúng.

7. a) Cái gì là khác nhau giữa lượng từ $\exists x \forall y\ P(x, y)$ và $\forall y \exists x\ P(x, y)$, với $P(x, y)$ là một hàm mệnh đề?

b) Cho một ví dụ về hàm mệnh đề $P(x,y)$ sao cho $\exists x \forall y\ P(x,y)$ và $\forall y \exists x\ P(x, y)$ có các giá trị chân lý khác nhau.

8. a) Định nghĩa hợp, giao, hiệu, hiệu đối xứng của hai tập hợp.

b) Xác định hợp, giao, hiệu, hiệu đối xứng của tập các số nguyên dương và tập các số nguyên lẻ.

9. a) Thế nào là hai tập bằng nhau?

b) Nêu các cách để chứng minh hai tập bằng nhau.

c) Chứng minh ít nhất bằng hai cách khác nhau rằng tập $A - (B \cap C)$ và tập $(A - B) \cup (A - C)$ bằng nhau.

10. Giải thích mối liên hệ giữa tương đương logic và các hằng đẳng thức tập hợp.

11. a) Định nghĩa bàn số $|S|$ của một tập S.

b) Cho công thức tính $|A \cup B|$, trong đó A và B là hai tập hợp.

12. a) Định nghĩa tập lũy thừa của một tập S.

b) Khi nào tập rỗng thuộc tập lũy thừa của S.

c) Tập luỹ thừa của một tập S với n phần tử có bao nhiêu phần tử?

13. a) Định nghĩa miền xác định, miền giá trị và tập hợp ảnh của hàm f.

b) Cho $f(n)$ là một hàm từ tập các số nguyên đến tập các số nguyên sao cho $f(n) = n^2 + 1$. Tìm miền xác định, miền giá trị và tập hợp ảnh của hàm đó.

14. a) Thế nào là một hàm đơn ánh từ tập các số nguyên dương đến tập các số nguyên dương.

b) Thế nào là một hàm toàn ánh từ tập các số nguyên dương đến tập các số nguyên đương.

c) Cho một ví dụ về hàm vừa đơn ánh và toàn ánh từ tập các số nguyên đương đến tập các số nguyên dương.

d) Cho một ví dụ về hàm đơn ánh nhưng không toàn ánh từ tập các số nguyên đương đến tập các số nguyên dương.

e) Cho một ví dụ về hàm toàn ánh nhưng không đơn ánh từ tập các số nguyên dương đến tập các số nguyên dương.

f) Cho một ví dụ về hàm không đơn ánh, cũng không toàn ánh từ tập các số nguyên dương đến tập các số nguyên dương.

15. a) Định nghĩa hàm ngược của một hàm.

b) Khi nào một hàm có hàm ngược.

c) Hàm $f(n) = 10 - n$ từ tập các số nguyên đến tập các số nguyên có hàm ngược không? Nếu có, tìm hàm ngược đó.

16. a) Định nghĩa các hàm sàn và hàm trần từ tập các số thực đến tập các số nguyên.

b) Đối với số thực x nào $\lfloor x \rfloor = \lceil x \rceil$?

17. a) Dùng ký hiệu lấy tổng biểu diễn tổng các luỹ thừa của 2 từ 2^0 đến 2^n.

b) Tính giá trị của tổng ở câu a)

18. a) Thế nào là một tập đếm được? Cho một định nghĩa chính xác.

b) Tập các số nguyên âm có là đếm được không? Tại sao?

c) Tập các số hữu tỉ với mẫu số lớn hơn 3 có là đếm được không? Tại sao?

d) Tập các số thực nằm trong khoảng giữa 2 và 3 có là đếm được không? Tại sao?

19. a) Phát biểu định nghĩa quan hệ $f(n)$ là $O(g(n))$, với $f(n)$ và $g(n)$ là hai hàm từ tập các số nguyên dương tới tập các số thực.

b) Dùng định nghĩa chứng minh hoặc bác bỏ khẳng định sau :

"$n^2 + 18n + 107$ là $O(n^3)$".

c) Cũng hỏi như trên đối với :

"n^3 là $O(n^2 + 18n + 107)$"

20. a) Làm thế nào cho một đánh giá big–O đối với một hàm là tổng nhiều số hạng, mỗi số hạng lại là tích của một vài hàm?

b) Cho một đánh giá big–O đối với hàm

$$f(n) = (n! + 1)(2^n + 1) + (n^{n-2} + 8.n^{n-3})(n^3 + 2^n).$$

Đối với hàm $g(x)$ trong đánh giá $f(x)$ là $O(g(x))$ của bạn, hãy dùng một hàm đơn giản có bậc nhỏ nhất có thể được.

BÀI TẬP BỔ SUNG

1. Cho p là mệnh đề "Tôi sẽ làm hết các bài tập trong cuốn sách này" và q là mệnh đề "Tôi sẽ nhận được điểm A trong khoá học này". Hãy biểu diễn các mệnh đề sau qua p và q.

   a) Tôi sẽ nhận được điểm A trong khoá học này chỉ nếu tôi làm hết các bài tập trong cuốn sách này.

   b) Tôi sẽ nhận được điểm A trong khoá học này và tôi sẽ làm hết bài tập trong cuốn sách này.

   c) Hoặc là tôi không nhận được điểm A trong khoá học này hoặc là tôi sẽ không làm hết bài tập trong cuốn sách này.

   d) Để tôi nhận được điểm A trong khoá học này, cần và đủ là tôi phải làm hết các bài tập trong cuốn sách này.

2. Tìm bảng giá trị chân lý của mệnh đề :

   $$(p \vee q) \rightarrow (p \wedge \neg r)$$

3. Chứng minh rằng các mệnh đề sau là hằng đúng :

   a) $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ b) $((p \vee q) \wedge \neg p) \rightarrow q$

4. Tìm mệnh đề đảo và phản đảo của các mệnh đề kéo theo sau :

   a) Nếu hôm nay trời mưa tôi sẽ lái xe đi làm.

   b) Nếu $|x| = x$, thì $x \geq 0$

   c) Nếu n lớn hơn 3 thì n^2 lớn hơn 9.

5. Tìm mệnh đề phức hợp chứa các hiến mệnh đề p, q, r và s. Biết rằng mệnh đề phức hợp này là đúng khi chính xác ba trong số bốn biến mệnh đề trên là đúng và sai trong các trường hợp còn lại.

6. Cho $P(x)$ là câu : "sinh viên x biết giải tích" và $Q(y)$ là câu " lớp y có một sinh viên biết giải tích". Hãy biểu diễn các câu sau như các lượng từ của $P(x)$ và $Q(x)$:

   a) Một số sinh viên hiết giải tích.

   b) Không có sinh viên nào biết giải tích.

   c) Tất cả các lớp đều có một sinh viên biết giải tích.

   d) Tất cả sinh viên trong tất cả các lớp đều biết giải tích.

   e) Có ít nhất một lớp không có một sinh viên nào biết giải tích.

7. Cho $P(m,n)$ là câu "n chia hết cho m", ở đây không gian của cả hai biến là tập hợp các số nguyên. Xác định giá trị chân lý của các mệnh đề sau :

a) $P(4,5)$ b) $P(2,4)$

c) $\forall m \forall n\ P(m,n)$ d) $\exists m \forall n\ P(m,n)$

e) $\exists n \forall m\ P(m,n)$ f) $\forall n\ P(1,n)$.

8. Cho $P(x,y)$ là một hàm mệnh đề. Chứng tỏ rằng mệnh đề kéo theo

$$\exists x \forall y\ P(x,y) \rightarrow \forall y \exists x\ P(x,y)$$ là hằng đúng.

9. Cho $P(x)$ và $Q(x)$ là các hàm mệnh đề. Chứng tỏ

$$\exists x\ (P(x) \rightarrow Q(x)) \text{ và } \forall x\ P(x) \rightarrow \exists x\ Q(x)$$

luôn luôn có cùng giá trị chân lý.

10. Nếu $\forall y \exists x\ P(x,y)$ là đúng thì có nhất thiết suy ra $\exists x \forall y\ P(x,y)$ cũng là đúng không?

11. Nếu $\forall x \exists y\ P(x,y)$ là đúng thì có nhất thiết suy ra $\exists x \forall y\ P(x,y)$ là đúng không ?

12. Tìm phủ định của các mệnh đề sau :

a) Nếu hôm nay tuyết rơi, ngày mai tôi sẽ đi trượt tuyết.

b) Mọi người trong lớp đều hiểu phép qui nạp toán học.

c) Một số sinh viên lớp này không thích môn toán học rời rạc.

d) Trong tất cả các lớp học toán đều có một học sinh ngủ gật trong giờ học.

13. Dùng các lượng từ diễn đạt các câu sau : "Tất cả các sinh viên lớp này đều đã học một môn nào đó ở tất cả các khoa của Trường toán học".

14. Dùng các lượng từ diễn đạt câu sau : "Có một toà nhà ở khu ký túc xá của một trường đại học nào đó ở Mỹ trong đó các phòng đều quét sơn trắng"?

15. Cho A là tập hợp các từ tiếng Anh có chứa chữ cái x và cho B là tập hợp các từ tiếng Anh có chứa chữ cái q. Biểu diễn các tập sau như các tổ hợp của A và B.

a) Tập các từ tiếng Anh không chứa chữ cái x.

b) Tập các từ tiếng Anh chứa cả x lẫn q.

c) Tập các từ tiếng Anh chứa x nhưng không chứa q.

d) Tập các từ tiếng Anh không chứa x hoặc q.

e) Tập các từ tiếng Anh chứa x hoặc q nhưng không cả hai.

16. Chứng minh rằng nếu A là một tập con của B thì tập luỹ thừa của A cũng là tập con của tập luỹ thừa của B.

17. Cho A và B là hai tập hợp sao cho tập luỹ thừa của A là tập con của tập luỹ thừa của B. Từ đó có suy ra A là tập con của B không?

18. Cho **E** là tập các số chẵn và **O** là tập các số lẻ. Như thường lệ, **Z** – là tập hợp tất cả các số nguyên. Xác định các tập hợp sau :

a) $\mathbf{E} \cup \mathbf{O}$ b) $\mathbf{E} \cap \mathbf{O}$

c) $\mathbf{Z} - \mathbf{E}$ d) $\mathbf{Z} - \mathbf{O}$

19. Chứng minh rằng nếu A là một tập hợp nào đó và U là tập vũ trụ thì :

a) $A \cap \overline{A} = \varnothing$ b) $A \cup \overline{A} = U$

20. Chứng minh rằng nếu A và B là hai tập hợp thì :

a) $A = A \cap (A \cup B)$ b) $A = A \cup (A \cap B)$

21. Chứng minh rằng, nếu A và B là hai tập hợp thì :

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

22. Cho A và B là hai tập hợp. Chứng minh rằng $A \subseteq B$ nếu và chỉ nếu $A \cap B = A$.

23. Cho A, B, và C là các tập hợp. Chứng minh rằng $(A - B) - C$ không nhất thiết phải bằng $A - (B - C)$.

24. Cho A, B và C là các tập hợp. Đẳng thức

$(A - B) - C = (A - C) - B$ là đúng hay sai? Tại sao?

25. Cho A, B, C và D là các tập hợp, đẳng thức :
$(A - B) - (C - D) = (A - C) - (B - D)$ là đúng hay sai? Tại sao?

26. Chứng minh rằng nếu A và B là các tập hữu hạn, thì

$$|A \cap B| \leq |A \cup B|.$$

Khi nào có dấu bằng?

27. Cho A và B là hai tập hợp trong tập hợp vũ trụ hữu hạn U. Liệt kê các tập sau theo thứ tự tăng dần của bản số :

a) $|A|$, $|A \cup B|$, $|A \cap B|$, $|U|$, $|\varnothing|$

b) $|A - B|$, $|A \oplus B|$, $|A| + |B|$, $|A \cup B|$, $|\varnothing|$

28. Cho A và B là các tập con của tập vũ trụ hữu hạn U.

Chứng minh rằng :

$$|\overline{A} \cap \overline{B}| = |U| - |A| - |B| + |A \cap B|$$

29. Cho f và g là hàm từ $\{1, 2, 3, 4\}$ đến $\{a, b, c, d\}$ và từ $\{a, b, c, d\}$ đến $\{1, 2, 3, 4\}$ tương ứng, sao cho $f(1) = d$, $f(2) = c$, $f(3) = a$ và $f(4) = b$ và $g(a) = 2$, $g(b) = 1$, $g(c) = 3$, $g(d) = 2$.

a) f có phải đơn ánh không? g có đơn ánh không?

b) f có toàn ánh không? g có toàn ánh không?

c) f hoặc g có hàm ngược không? Nếu có, tìm hàm ngược đó.

30. Cho f là một hàm đơn ánh từ A đến B. Giả sử S và T là hai tập con của A. Chứng minh rằng : $f(S \cap T) = f(S) \cap f(T)$.

31. Cho một ví dụ cho thấy đẳng thức trong Bài tập 30 là không đúng nếu f không phải là một đơn ánh.

32. Chứng minh rằng $\lceil x + 1 \rceil = \lceil x \rceil + 1$ với mọi x là số thực.

33. Tính giá trị các đại lượng sau :

a) $\sum_{i=0}^{3} \left(\sum_{j=0}^{4} ij \right)$

b) $\prod_{j=1}^{4} \left(\sum_{i=0}^{3} j \right)$

c) $\sum_{i=1}^{5} \left(\sum_{j=0}^{i} 1 \right)$

d) $\prod_{i=1}^{3} \left(\prod_{j=0}^{i} j \right)$

34. Tập hợp các số vô tỷ nằm giữa 0 và 1 có đếm được không? Giải thích.

35.** Một số thực được gọi là **số đại số** nếu nó là nghiệm của một đa thức với hệ số nguyên. Chứng minh rằng tập hợp các số đại số là đếm được. (Gợi ý : dùng tính chất đa thức bậc n có nhiều nhất n nghiệm phân biệt).

36. Chứng minh rằng $8x^3 + 12x + 100\log x$ là $O(x^3)$.

37. Cho một đánh giá big–O đối với hàm $(x^2 + x(\log x)^3)(2^x + x^3)$

38. Tìm đánh giá big–O của $\sum_{j=1}^{n} j(j+1)$

***39.** Chứng minh rằng $n!$ không là $O(2^n)$

***40.** Chứng minh rằng n^n không là $O(n!)$

BÀI TẬP TRÊN MÁY TÍNH

Viết chương trình với Input và Output cho dưới đây

1. Cho bảng chân lý của các mệnh đề p và q. Tìm bảng giá trị chân lý của hội, tuyển, tuyển loại, kéo theo, và tương đương của các mệnh đề đó.

2. Cho hai xâu bit có chiều dài n, tìm AND bit, OR bit và XOR bit của hai xâu đó.

3. Cho giá trị chân lý của các mệnh đề p và q trong logic mờ, tìm giá trị chân lý của tuyển và hợp của hai mệnh đề đó (xem các Bài tập 23 – 25 trong tiết 1.1).

4. Cho hai tập con A, B của một tập hợp có n phần tử, dùng các xâu bit để tìm $\overline{A}$, $A \cup B$, $A \cap B$, $A - B$ và $A \oplus B$.

5. Cho hai đa tập A và B từ cùng một tập vũ trụ. Tìm $A \cup B$, $A \cap B$, $A - B$ và $A \oplus B$. (Xem phần chú thích ở trước Bài tập 47 của Tiết 1.5).

6. Cho các tập mờ A và B, tìm $\overline{A}$, $A \cup B$, và $A \cap B$ (Xem phần chú thích ở trước Bài tập 49 của Tiết 1.5).

7. Cho hàm f từ $\{1, 2, \ldots n\}$ đến tập các số nguyên, xác định xem f có phải là đơn ánh không?

8. Cho hàm f từ $\{1, 2, \ldots n\}$ đến chính nó, xác định xem f có phải là toàn ánh không?

9. Cho một song ánh từ $\{1, 2, \ldots n\}$ là chính nó, xác định f^{-1}.

10. Cho các số hạng của một dãy $a_1, a_2, \ldots a_n$, tính :

$$\sum_{j=1}^{n} a_j \quad \text{và} \quad \prod_{j=1}^{n} a_j$$

TÍNH TOÁN VÀ KHÁM PHÁ

Dùng các chương trình mà bạn đã viết, giải các bài tập sau :

1. Xác định số n lớn nhất sao cho $n!$ có ít hơn 100 chữ số thập phân? Ít hơn 1000 chữ số thập phân ?

2. Trong biểu diễn thập phân, $n!$ tận cùng bằng bao nhiêu số không, với n từ 1 đến 25? Bạn có thể đưa ra một công thức cho phép tính được số các số không tận cùng của $n!$ trong biểu diễn thập phân của nó không? (xem Tiết 2.3).

3. Tính số hàm đơn ánh từ một tập S đến tập T, với S và T là hai tập hữu hạn có bản số khác nhau. Bạn có thể đưa ra một công thức cho phép tính được số các hàm đó không? (Ta sẽ tìm được công thức này ở Chương 4).

4. Tính số hàm toàn ánh từ một tập S đến tập T với S và T là hai tập hữu hạn, có bản số khác nhau. Bạn có thể đưa ra một công thức tính số các hàm đó không? (Chúng ta sẽ tìm được một công thức như vậy ở Chương 5).

5. Biết rằng n^b là $O(d^n)$ với b và d là hai số dương và $d \geqslant 2$. Xác định các giá trị của các hằng số C và k sao cho $n^b \leqslant Cd^n$ với mọi $x > k$ đối với mỗi tập các giá trị sau : $b = 10$, $d = 2$; $b = 20$, $d = 3$; $b = 1000$, $d = 7$.

VIẾT TIỂU LUẬN

Dùng các tư liệu ở ngoài cuốn sách này, viết các tiểu luận trả lời những câu hỏi sau :

1. Hãy mô tả logic mờ được áp dụng như thế nào cho những ứng dụng thực tế. Hãy tham khảo một vài cuốn sách phổ biến mới xuất bản gần đây về logic mờ.

2. Hãy đọc một số tác phẩm của Lews Carroll về logic ký hiệu. Mô tả chi tiết một số mô hình mà ông đã dùng để biểu diễn các suy lý logic.

3. Lý thuyết tiên đề của tập hợp có thể được phát triển để tránh nghịch lý của Russell (xem Bài tập 24 của Tiết 1.4). Hãy bàn về vấn đề này.

4. Hãy tìm xem khái niệm hàm lần đầu tiên xuất hiện ở đâu và mô tả xem khái niệm này lần đầu tiên được dùng như thế nào?

5. Hãy giải thích xem tại sao sẽ rất tiện ích nếu ta có một bảng liệt kê đầy đủ các dãy đặc biệt các số nguyên. Nếu bạn tìm được một bảng liệt kê như vậy, thì các dãy được tổ chức như thế nào?

6. Mô tả khái niệm bản số được mở rộng tới các tập vô hạn như thế nào?

7. Tìm một định nghĩa về số siêu việt. Hãy giải thích rõ làm thế nào chứng minh được sự tồn tại của các số này và làm thế nào lập được các số đó. Các số nổi tiếng nào mà bạn đã biết là số siêu việt?

8. Tìm cách dẫn ra đầu tiên về khái niệm big-O của Bachmann. Giải thích xem ông và những người khác đã dùng khái niệm này như thế nào.

CHƯƠNG 2

NHỮNG KIẾN THỨC CƠ BẢN : THUẬT TOÁN, CÁC SỐ NGUYÊN VÀ MA TRẬN

Nhiều bài toán có thể được giải khi xem chúng như các trường hợp đặc biệt của một bài toán tổng quát. Ví dụ, xét bài toán xác định vị trí của số nguyên lớn nhất trong dãy 101, 12, 144, 212, 98. Đây là một trường hợp đặc biệt của bài toán xác định số nguyên lớn nhất trong một dãy các số nguyên. Để giải bài toán tổng quát này, ta cần phải cho một thuật toán chỉ rõ dãy các bước được sử dụng để giải bài toán tổng quát đó. Trong cuốn sách này, chúng ta sẽ nghiên cứu các thuật toán để giải nhiều loại bài toán khác nhau. Ví dụ, thuật toán để tìm ước số chung lớn nhất của hai số nguyên, để làm phát sinh mọi kiểu sắp thứ tự của một tập hữu hạn, để tìm một bảng liệt kê, và để tìm con đường ngắn nhất giữa hai đỉnh của một mạng. Một vấn đề quan trọng liên quan đến thuật toán là độ phức tạp tính toán của nó. Tức là, những tài nguyên nào của máy tính cần phải có khi dùng một thuật toán để giữ một bài toán có qui mô xác định. Trong chương này chúng ta sẽ minh họa sự phân tích độ phức tạp của các thuật toán.

Tập hợp các số nguyên đóng một vai trò cơ bản trong toán học rời rạc. Đặc biệt, khái niệm chia hết của các số nguyên là hết sức cơ bản đối với số học của máy tính. Trong chương này, chúng tôi cũng sẽ ôn lại một cách ngắn gọn một số khái niệm quan trọng của lý thuyết số – khoa học về các số nguyên và tính chất của chúng. Một số các thuật toán quan trọng liên quan đến các số nguyên cũng sẽ được nghiên cứu, kể cả thuật toán của Euclide dùng để xác định ước số chung lớn nhất đã được mô tả lần đầu tiên khoảng hàng ngàn năm trước đây. Các số nguyên có thể được biểu diễn bằng cách dùng một số nguyên lớn hơn 1 làm cơ số. Các khai triển nhị phân được dùng xuyên suốt trong tin học, chính là biểu diễn cơ số 2. Trong chương này, chúng ta cũng sẽ bàn về biểu diễn

cơ số b của các số nguyên và cho một thuật toán để tìm chúng. Các thuật toán cho số học các số nguyên – những thủ tục đầu tiên được gọi là thuật toán – cũng sẽ được bàn đến. Chương này cũng giới thiệu một số ứng dụng quan trọng của lý thuyết số như mã hóa thư từ, tạo các số giả ngẫu nhiên, và gán các vị trí của bộ nhớ cho các file máy tính.

Các ma trận được dùng trong toán học rời rạc để biểu diễn rất nhiều các cấu trúc rời rạc. Chương này cũng sẽ ôn lại một số kiến thức cơ bản về ma trận, số học của chúng cần thiết để biểu diễn các quan hệ và đồ thị. Số học các ma trận cũng sẽ được dùng trong rất nhiều thuật toán liên quan đến các cấu trúc này.

2.1. THUẬT TOÁN

MỞ ĐẦU

Có nhiều lớp bài toán tổng quát xuất hiện trong toán học rời rạc. Ví dụ : cho một dãy các số nguyên, tìm số lớn nhất ; cho tập hợp, liệt kê hết các tập con của nó; cho tập các số nguyên, xếp chúng theo thứ tự tăng dần; cho một mạng, tìm đường đi ngắn nhất giữa hai đỉnh của nó. Khi được giao cho một bài toán như vậy, thì việc đầu tiên phải làm là xây dựng một mô hình dịch bài toán đó thành ngữ cảnh toán học. Các cấu trúc rời rạc được dùng trong các mô hình này là tập hợp, dãy, và hàm – các cấu trúc đã được xét ở chương 1, cùng với các cấu trúc khác như hoán vị, quan hệ, đồ thị, cây, mạng và các máy hữu hạn trạng thái – những khái niệm sẽ được nghiên cứu ở các chương sau.

Lập được một mô hình toán học thích hợp chỉ là một phần của quá trình giải. Để hoàn tất quá trình giải, còn cần phải có một phương pháp dùng mô hình để giải bài toán tổng quát. Nói một cách lý tưởng, cái được đòi hỏi là một thủ tục, đó là dãy các bước dẫn tới đáp số mong muốn. Một dãy các bước như vậy, được gọi là một **thuật toán**.

ĐỊNH NGHĨA 1. *Thuật toán* là một thủ tục xác định dùng một số bước hữu hạn để giải một bài toán. Thuật ngữ "*Algorithm*" (thuật toán) là biến

tướng của tên nhà toán học Ả rập *al-Khowarizmi*, người đã viết cuốn sách về các chữ số Hindu – cơ sở của ký hiệu số thập phân hiện đại. Ban đầu, từ *algorism* được dùng để chỉ các qui tắc thực hiện các phép tính số học trên các số thập phân. Sau đó, *algorism* tiến hóa thành *algorithm* vào thế kỷ 19. Với sự quan tâm ngày càng tăng đối với các máy tính, khái niệm thuật toán đã được cho một ý nghĩa chung hơn, bao hàm cả các thủ tục xác định để giải các bài toán, chứ không phải chỉ là thủ tục để thực hiện các phép tính số học. (Chúng ta sẽ bàn về các thuật toán để thực hiện những phép tính số học đối với các số nguyên ở Tiết 2.4).

Trong cuốn sách này chúng ta sẽ xét các thuật toán để giải rất nhiều bài toán. Ở tiết này ta sẽ dùng thuật toán tìm số nguyên lớn nhất trong một dãy hữu hạn các số nguyên để minh họa một thuật toán và các tính chất của nó. Chúng ta cũng sẽ mô tả các thuật toán dùng để xác định vị trí của một phần tử đặc biệt nào đó trong một tập hợp hữu hạn. Trong các tiết sau, chúng ta sẽ xét tới các thủ tục tìm ước số chung lớn nhất của hai số nguyên, tìm đường đi ngắn nhất giữa hai điểm trong một mạng, cũng như phép nhân các ma trận v.v...

Ví dụ 1. Mô tả thuật toán tìm phần tử lớn nhất trong một dãy hữu hạn các số nguyên.

Mặc dù bài toán tìm phần tử lớn nhất trong một dãy hữu hạn các số nguyên tương đối tầm thường, nhưng nó cho ta một minh họa tốt cho khái niệm thuật toán. Hơn nữa, trong nhiều trường hợp cá biệt vẫn có nhu cầu phải xác định số nguyên lớn nhất trong một dãy hữu hạn các số nguyên. Ví dụ, một trường thường xuyên cần phải tìm điểm số cao nhất trong các cuộc thi đều có hàng ngàn sinh viên tham gia. Hoặc một tổ chức thể thao hàng tháng đều muốn biết hội viên có thành tích cao nhất của họ. Và chúng ta muốn xây dựng một thuật toán có thể được dùng bất cứ khi nào bài toán tìm phần tử lớn nhất trong dãy hữu hạn các số nguyên được đặt ra.

Chúng ta có thể chỉ rõ thủ tục để giải bài toán này bằng vài cách. Một cách đơn giản là dùng ngôn ngữ thông thường để mô tả các bước cần phải thực hiện. Dưới đây là một thủ tục như vậy :

Lời giải của ví dụ 1 : Chúng ta sẽ thực hiện các bước sau :

1. Đặt giá trị cực đại tạm thời bằng số nguyên đầu tiên trong dãy. (Cực đại tạm thời sẽ là số nguyên lớn nhất đã được kiểm tra ở một giai đoạn nào đó của thủ tục).

2. So sánh số nguyên tiếp sau với giá trị cực đại tạm thời, nếu nó lớn hơn giá trị cực đại tạm thời, thì đặt cực đại tạm thời bằng số nguyên đó.

3. Lặp lại bước trước nếu còn các số nguyên trong dãy.

4. Dừng khi không còn số nguyên nào nữa trong dãy. Cực đại tạm thời ở điểm này chính là số nguyên lớn nhất của dãy.

■

Một thuật toán cũng có thể được mô tả bằng cách dùng một ngôn ngữ máy tính nào đó. Tuy nhiên, một khi đã làm như vậy, thì chỉ những lệnh được phép trong ngôn ngữ đó mới có thể dùng được. Điều này thường làm cho sự mô tả các thuật toán trở nên rối rắm và khó hiểu. Hơn nữa,, vì nhiều ngôn ngữ lập trình đều được dùng rộng rãi, nên chọn một ngôn ngữ đặc biệt nào đó là điều người ta không muốn. Vì vậy, thay vì dùng một ngôn ngữ đặc biệt nào đó để mô tả một thuật toán, trong quyển sách này chúng ta sẽ dùng một dạng **giả mã**. Giả mã tạo ra bước trung gian giữa sự mô tả một thuật toán bằng ngôn ngữ thông thường và sự thực hiện thuật toán đó trong ngôn ngữ lập trình. Các bước của thuật toán được chỉ rõ bằng cách dùng các lệnh giống như trong các ngôn ngữ lập trình. Tuy nhiên, trong giả mã, các lệnh được dùng có thể có cả những phép toán xác định và các mệnh đề. Một chương trình máy tính có thể được tạo ra trong bất kỳ một ngôn ngữ máy tính nào bằng cách dùng mô tả giả mã như một điểm xuất phát.

Giả mã được dùng trong cuốn sách này tựa hồ trên ngôn ngữ lập trình Pascal. Tuy nhiên, cú pháp của Pascal cũng như cú pháp của các ngôn ngữ lập trình khác đều không được tuân theo ở đây. Hơn nữa, bất kỳ lệnh xác định nào đều có thể được dùng trong giả mã này.

Mô tả giả mã của thuật toán tìm số lớn nhất trong dãy hữu hạn các số nguyên như sau :

ALGORITHM 1. TÌM PHẦN TỬ LỚN NHẤT TRONG DÃY HỮU HẠN

```
procedure max (a1, a2, ..., an : integers)
max := a1
for i := 2 to n
    if max < ai then max := ai
{max là phần tử lớn nhất}
```

Thuật toán này trước hết gán số hạng đầu tiên a_1 của dãy cho biến *max*. Vòng lặp "for" được dùng để kiểm tra lần lượt các số hạng của dãy. Nếu một số hạng lớn hơn giá trị hiện thời của max, thì nó được gán làm giá trị mới của max.

Các thuật toán có một số tính chất chung. Sẽ rất hữu ích khi mô tả các thuật toán nếu ta ghi nhớ các tính chất đó trong đầu. Các tính chất đó là :

- *Đầu vào* (Input) : Một thuật toán có các giá trị đầu vào từ một tập đã được chỉ rõ.
- *Đầu ra* (Output) : Từ mỗi tập các giá trị đầu vào, thuật toán sẽ tạo ra các giá trị đầu ra. Các giá trị đầu ra chính là nghiệm của bài toán.
- *Tính xác định* : Các bước của một thuật toán phải được xác định một cách chính xác.
- *Tính hữu hạn* : Một thuật toán cần phải tạo ra các giá trị đầu ra mong muốn sau một số hữu hạn (nhưng có thể rất lớn) các bước đối với mọi tập đầu vào.
- *Tính hiệu quả* : Mỗi bước của thuật toán cần phải thực hiện được một cách chính xác và trong một khoảng thời gian hữu hạn.
- *Tính tổng quát* : Thủ tục cần phải áp dụng được cho mọi bài toán có dạng mong muốn, chứ không phải chỉ cho một tập đặc biệt các giá trị đầu vào.

Ví dụ 2. Chứng tỏ rằng Algorithm 1 để tìm phần tử lớn nhất trong một dãy hữu hạn các số nguyên hội đủ những tính chất trên.

Giải : Đầu vào của Thuật toán 1 là một dãy các số nguyên. Đầu ra là số lớn nhất trong dãy đó. Mỗi một bước của thuật toán trên đều được xác định một cách chính xác, vì chỉ có phép gán, một vòng lặp hữu hạn và các mệnh đề kéo theo. Thuật toán dùng một số hữu hạn bước vì nó kết thúc sau khi tất cả các số nguyên của dãy đã được kiểm tra. Thuật toán này có thể được thực hiện trong một khoảng thời gian hữu hạn, vì mỗi bước chỉ là sự so sánh hoặc gán. Cuối cùng, Thuật toán 1 là tổng quát vì nó có thể được dùng để tìm số cực đại của dãy các số nguyên hữu hạn bất kỳ. ■

THUẬT TOÁN TÌM KIẾM

Bài toán xác định vị trí của một phần tử trong một bảng liệt kê sắp thứ tự thường gặp trong nhiều trường hợp khác nhau. Ví dụ, chương trình kiểm tra chính tả của các từ tìm kiếm các từ này trong một cuốn từ điển, mà từ điển chẳng qua cũng là một bảng liệt kê sắp thứ tự của các từ. Các bài toán thuộc loại này được gọi là các **bài toán tìm kiếm**. Trong tiết này ta sẽ xem xét một số thuật toán tìm kiếm. Và ta sẽ nghiên cứu số các bước được dùng bởi mỗi thuật toán đó trong Tiết 2.2.

Bài toán tìm kiếm tổng quát được mô tả như sau : xác định vị trí của phần tử x trong một bảng liệt kê các phần tử phân biệt a_1, a_2, ..., a_n hoặc xác định rằng nó không có mặt trong bảng liệt kê đó. Lời giải của bài toán trên là vị trí của số hạng của bảng liệt kê có giá trị bằng x (tức là, i sẽ là nghiệm nếu $x = a_i$, và là 0 nếu x không có mặt trong bảng liệt kê).

Thuật toán đầu tiên mà chúng tôi giới thiệu có tên là thuật toán **tìm kiếm tuyến tính** hay **tìm kiếm tuần tự**. Nó bắt đầu bằng việc so sánh x với a_1. Khi $x = a_1$, nghiệm là vị trí của a_1, tức là 1. Khi $x \neq a_1$, so sánh x với a_2. Nếu $x = a_2$, nghiệm là vị trí của a_2, tức là 2. Khi $x \neq a_2$ so sánh x với a_3. Tiếp tục quá trình này bằng cách tuần tự so sánh x với mỗi một số hạng của bảng liệt kê cho tới khi tìm được số hạng bằng x, khi đó nghiệm là vị trí của số hạng đó. Nếu toàn bảng liệt kê đã được kiểm tra mà không xác định được vị trí của x, thì nghiệm là 0. Giả mã đối với thuật toán tìm kiếm tuyến tính được cho trong Algorithm 2.

ALGORITHM 2. THUẬT TOÁN TÌM KIẾM TUYẾN TÍNH

procedure tìm kiếm tuyến tính (x : integer, a_1, a_2, ..., a_n : các số nguyên phân biệt)

i : = 1

while ($i \leq n$ and $x \neq a_i$)

    i : = i + 1

if $i \leq n$ **then** location : = i

else location : = 0

{location là chỉ số dưới của số hạng bằng x hoặc là 0 nếu không tìm được x}

Bây giờ ta xét một thuật toán tìm kiếm khác. Thuật toán này có thể được dùng khi bảng liệt kê có các số hạng được sắp theo thứ tự tăng dần (ví dụ : nếu các số hạng là các số, thì chúng được sắp từ số nhỏ nhất đến số lớn nhất ; hoặc nếu chúng là các từ thì chúng được sắp theo thứ tự bảng chữ cái v.v...). Thuật toán thứ hai này được gọi là thuật toán **tìm kiếm nhị phân**. Nó được tiến hành bằng cách so sánh phần tử cần xác định vị trí với số hạng ở giữa bảng liệt kê. Sau đó bảng này được tách làm hai bảng kê con nhỏ hơn có kích thước như nhau, hoặc một trong hai bảng con ít hơn bảng con kia một số hạng. Sự tìm kiếm tiếp tục bằng cách hạn chế tìm kiếm ở một bảng kê con thích hợp dựa trên việc so sánh phần tử cần xác định vị trí với số hạng giữa bảng kê. Trong tiết sau, ta sẽ chứng minh rằng thuật toán tìm kiếm nhị phân hiệu quả hơn nhiều so với thuật toán tìm kiếm tuyến tính. Ví dụ dưới đây minh họa sự tìm kiếm nhị phân.

Ví dụ 3. Để tìm số 19 trong bảng liệt kê

1, 2, 3, 5, 6, 7, 8, 10, 12, 13, 15, 16, 18, 19, 20, 22

ta tách bảng liệt kê gồm 16 số hạng này thành hai bảng liệt kê nhỏ hơn, mỗi bảng có 8 số hạng, cụ thể là :

1, 2, 3, 5, 6, 7, 8, 10 và 12, 13, 15, 16, 18, 19, 20, 22.

Sau đó ta so sánh 19 với số hạng cuối cùng của bảng con thứ nhất. Vì 10 < 19, việc tìm kiếm 19 chỉ giới hạn trong bảng liệt kê con thứ 2 từ số hạng thứ 9 đến thứ 16 trong bảng liệt kê ban đầu. Tiếp theo, ta lại tách bảng kê con gồm 8 số hạng này làm hai bảng con, mỗi bảng có 4 số hạng, cụ thể là

12, 13, 15, 16 và 18, 19, 20, 22.

Vì 16 < 19 (so 19 với số hạng cuối cùng của bảng con đầu tiên), việc tìm kiếm lại được giới hạn chỉ trong bảng con thứ hai, từ số hạng thứ 13 đến số hạng thứ 16 của bảng liệt kê ban đầu. Bảng liệt kê 18, 19, 20, 22 lại được tách làm hai, cụ thể là :

18, 19 và 20, 22

Vì 19 không lớn hơn số hạng lớn nhất của bảng con thứ nhất – cũng là 19 – nên việc tìm kiếm giới hạn chỉ ở bảng con thứ nhất gồm các số 18, 19, là số hạng thứ 13 và 14 của bảng ban đầu. Tiếp theo, bảng con chứa 2 số hạng này lại được tách làm hai, mỗi bảng có một số hạng 18 và 19. Vì 18 < 19, sự tìm kiếm giới hạn chỉ trong bảng con thứ 2 – bảng liệt kê chỉ chứa số hạng thứ 14 của bảng liệt kê ban đầu, số hạng đó là số 19. Bây giờ sự tìm kiếm đã thu hẹp về chỉ còn một số hạng,

so sánh tiếp cho thấy 19 là số hạng thứ 14 của bảng liệt kê ban đầu. ■

Bây giờ chúng ta có thể chỉ rõ các bước trong thuật toán tìm kiếm nhị phân.

Để tìm số nguyên x trong bảng liệt kê $a_1, a_2, \ldots a_n$, với $a_1 < a_2 < \ldots < a_n$, ta bắt đầu bằng việc so sánh x với số hạng a_m ở giữa của dãy, với $m = \lfloor \frac{n+1}{2} \rfloor$. (Cần nhớ lại rằng $\lfloor x \rfloor$ là số nguyên lớn nhất không quá x). Nếu $x > a_m$, việc tìm kiếm x giới hạn ở nửa thứ hai của dãy, gồm $a_{m+1}, a_{m+2}, \ldots a_n$. Nếu x không lớn hơn a_m, thì sự tìm kiếm giới hạn trong nửa đầu của dãy gồm $a_1, a_2, \ldots a_m$.

Bây giờ sự tìm kiếm chỉ giới hạn trong bảng kê có không hơn $\lceil \frac{n}{2} \rceil$ phần tử. Dùng chính thủ tục này, so sánh x với số hạng ở giữa của bảng liệt kê được hạn chế. Sau đó lại hạn chế việc tìm kiếm ở nửa thứ nhất hoặc nửa thứ hai của bảng liệt kê. Lặp lại quá trình này cho tới khi nhận được một bảng liệt kê chỉ có một số hạng. Sau đó, chỉ còn xác định số hạng này có phải là x hay không. Giả mã cho thuật toán tìm kiếm nhị phân được cho trong Algorithm 3.

ALGORITHM 3. THUẬT TOÁN TÌM KIẾM NHỊ PHÂN

procedure tìm kiếm nhị phân (x : integer, $a_1, a_2 \ldots a_n$: integers tăng dần)
$i := 1$ (i là điểm mút trái của khoảng tìm kiếm)
$j := n$ {j là điểm mút phải của khoảng tìm kiếm)
while $i < j$
begin
$m := \lfloor \frac{i + j}{2} \rfloor$
if $x > a_m$ **then** $i := m + 1$
else $j := m$
end
if $x = a_i$ **then** location : = i
else location : = 0.
{location là chỉ số dưới của số hạng bằng x hoặc 0 nếu không tìm thấy x}

Algorithm 3 tiến hành bằng cách thu hẹp liên tiếp phần cần tìm kiếm của dãy. Ở bất kỳ giai đoạn nào, chỉ có các số hạng bắt đầu với a_i hoặc kết thúc với a_j là được xem xét. Nói cách khác, i và j là các chỉ số nhỏ nhất và lớn nhất của các số hạng còn lại, tương ứng. Algorithm 3 tiếp tục thu hẹp phần của dãy cần phải tìm kiếm cho tới khi chỉ còn lại một phần tử của dãy. Khi đã làm đến đó, sự so sánh sẽ cho thấy số hạng đó có là x hay không.

BÀI TẬP

1. Liệt kê tất cả các bước mà Algorithm 1 đã dùng để tìm số cực đại của bảng liệt kê 1, 8, 12, 9, 11, 2, 14, 5, 10, 4.

2. Các thủ tục sau có và thiếu những đặc điểm gì của một thuật toán

   a) **procedure** gấp đôi (*n* : positive integer – nguyên dương)

      while $n \geq 0$

      $n := 2n$

   b) **procedure** chia (*n* : positive integer)

      while $n \geq 0$

      begin

         $m := 1/n$

         $n := n - 1$

      end

   c) **procedure** tổng (*n* : positive integer)

      sum : = 0

      while $i < 10$

      sum : = sum + 1

   e) **procedure** chọn (*a*, *b* : integer)

      x : = hoặc *a* hoặc *b*.

3. Lập một thuật toán tính tổng tất cả các số nguyên trong một hàng.

4. Lập thuật toán tính x^n với x là một số thực và n là một số nguyên. (*Gợi ý* : trước hết cho một thủ tục tính x^n với n là một số nguyên

không âm bằng cách nhân liên tiếp với x, bắt đầu với 1. Sau đó mở rộng thủ tục này và dùng tính chất $x^{-n} = 1/x^n$ để tính x^n với n âm).

5. Lập thuật toán trao đổi các giá trị của các biến x và y bằng cách chỉ dùng phép gán. Số tối thiểu các lệnh gán để làm việc đó là bao nhiêu?

6. Mô tả thuật toán chỉ dùng lệnh gán để thay bộ ba số (x, y, z) thành (y, z, x). Số lệnh gán tối thiểu cần dùng là bao nhiêu?

7. Liệt kê tất cả các bước cần tiến hành để tìm kiếm số 9 trong dãy 1, 3, 4, 5, 6, 8, 9, 11 khi dùng :

   a) thuật toán tìm kiếm tuyến tính .

   b) thuật toán tìm kiếm nhị phân.

8. Liệt kê tất cả các bước cần tiến hành để tìm số 7 trong dãy cho trong Bài tập 7.

9. Mô tả thuật toán chèn một số nguyên x vào vị trí thích hợp trong dãy các số nguyên $a_1, a_2 \ldots a_n$ xếp theo thứ tự tăng dần.

10. Mô tả thuật toán tìm số nguyên nhỏ nhất trong một dãy hữu hạn các số tự nhiên.

11. Tìm thuật toán xác định vị trí gặp đầu tiên của phần tử lớn nhất trong bảng liệt kê các số nguyên, trong đó các số nguyên không nhất thiết phải khác nhau.

12. Mô tả thuật toán xác định vị trí gặp cuối cùng của phần tử nhỏ nhất trong một bảng liệt kê các số nguyên, trong đó các số này không nhất thiết phải khác nhau.

13. Mô tả thuật toán tìm số cực đại, số trung tâm, số trung bình và số cực tiểu của tập gồm ba số nguyên. (Số **trung tâm** của tập các số nguyên là số ở giữa của bảng liệt kê khi các số nguyên đó được liệt kê theo thứ tự tăng dần. Số **trung bình** của tập các số nguyên là tổng các số nguyên đó chia cho số các số nguyên trong tập).

14. Mô tả thuật toán tìm cả số lớn nhất lẫn bé nhất trong dãy hữu hạn các số nguyên

15. Mô tả thuật toán xếp ba số hạng đầu tiên của một dãy các số nguyên có chiều dài tùy ý theo thứ tự tăng dần.

16. Mô tả thuật toán tìm từ dài nhất trong một câu tiếng Anh, (ở đây từ là một xâu các chữ cái, còn câu là một bảng liệt kê các từ cách nhau một khoảng trống).

17. Mô tả thuật toán xác định một hàm từ một tập hữu hạn này đến một tập hữu hạn khác có là toàn ánh hay không?

18. Mô tả thuật toán xác định một hàm từ tập hữu hạn này đến tập hữu hạn khác có là đơn ánh hay không ?

19. Mô tả thuật toán đếm số các số 1 trong một xâu bit bằng cách kiểm tra mỗi bit của xâu để xác định nó có là bit 1 hay không.

20. Thay đổi Algorithm 3 sao cho thủ tục tìm kiếm nhị phân so sánh x với a_m ở mỗi giai đoạn của thuật toán và thuật toán kết thúc nếu $x = a_m$. Phiên bản này của thuật toán đó có ưu điểm gì?

21. **Thuật toán tìm kiếm tam phân** xác định vị trí của một phần tử trong một bảng liệt kê các số nguyên theo thứ tự tăng dần bằng cách tách liên tiếp bảng liệt kê đó thành ba bảng liệt kê con có kích thước bằng nhau (hoặc gần bằng nhau nhất có thể được) và giới hạn việc tìm kiếm trong một bảng liệt kê con thích hợp. Chỉ rõ các bước của thuật toán đó.

22. Chỉ rõ các bước của một thuật toán xác định vị trí của một phần tử trong một bảng liệt kê các số nguyên sắp theo thứ tự tăng dần bằng cách tách liên tiếp bảng liệt kê thành bốn bảng liệt kê con có chiều dài bằng nhau (hoặc gần bằng nhau nhất có thể được) và giới hạn việc tìm kiếm chỉ trong một bảng liệt kê con thích hợp.

23. **Kiểu** (mode) của một bảng liệt kê các số nguyên là phần tử ít nhất xuất hiện thường xuyên như các phần tử khác. Hãy lập một thuật toán tìm kiểu trong một dãy các số nguyên không giảm.

24. Lập thuật toán tìm tất cả các kiểu (xem định nghĩa của kiểu trong Bài tập 23) trong một bảng liệt kê các số nguyên không giảm.

25. Lập thuật toán tìm trong một dãy các số nguyên số hạng đầu tiên bằng một số hạng nào đó đứng trước nó trong dãy.

26. Lập thuật toán tìm trong một dãy các số nguyên tất cả các số hạng lớn hơn tổng tất cả các số hạng đứng trước nó trong dãy.

27. Lập thuật toán tìm trong dãy các số nguyên dương số hạng đầu tiên nhỏ hơn số hạng đứng ngay trước nó trong dãy.

2.2. ĐỘ PHỨC TẠP CỦA THUẬT TOÁN

MỞ ĐẦU

Khi nào một thuật toán cho lời giải thỏa đáng đối với một bài toán ? Trước hết, nó phải luôn cho đáp số đúng. Làm thế nào chứng minh được điều đó? Vấn đề này ta sẽ xem xét ở chương 3. Thứ hai, thuật toán phải hiệu quả. Vấn đề này ta sẽ xét dưới đây.

Hiệu quả của một thuật toán được phân tích như thế nào? Một thước đo hiệu quả đó là thời gian mà máy tính sử dụng để giải bài toán theo thuật toán đang xét, khi các giá trị đầu vào có một kích thước xác định. Một thước đo thứ hai đó là dung lượng bộ nhớ đòi hỏi để thực hiện thuật toán khi các giá trị đầu vào có kích thước xác định.

Các vấn đề như thế liên quan đến độ **phức tạp tính toán** của một thuật toán. Sự phân tích thời gian cần thiết để giải một bài toán có kích thước đặc biệt nào đó liên quan đến **độ phức tạp thời gian** của thuật toán. Sự phân tích bộ nhớ cần thiết của máy tính liên quan với **độ phức tạp không gian** của thuật toán. Việc xem xét độ phức tạp thời gian và không gian của một thuật toán là một vấn đề rất thiết yếu khi các thuật toán được thực hiện. Biết một thuật toán sẽ đưa ra đáp số trong một micrô giây, trong một phút hoặc trong một tỷ năm, hiển nhiên, là điều hết sức quan trọng. Tương tự như vậy, dung lượng bộ nhớ đòi hỏi phải là khả dụng để giải một bài toán, vì vậy độ phức tạp không gian cũng cần phải tính đến.

Sự xem xét độ phức tạp không gian gắn liền với các cấu trúc dữ liệu đặc biệt được dùng để thực hiện thuật toán. Vì các cấu trúc dữ liệu không được xét kỹ trong cuốn sách này, nên độ phức tạp không gian sẽ không được xem xét ở đây. Chúng ta sẽ chỉ tập trung xem xét độ phức tạp thời gian.

Độ phức tạp thời gian của một thuật toán có thể được biểu diễn qua số các phép toán được dùng bởi thuật toán đó khi các giá trị đầu vào có một kích thước xác định. Các phép toán được dùng để đo độ phức tạp thời gian có thể là phép so sánh các số nguyên, các phép cộng, trừ, nhân, chia các số nguyên hoặc bất kỳ một phép tính sơ cấp nào khác. Sở dĩ độ phức tạp thời gian được mô tả thông qua số các phép toán đòi hỏi thay vì thời gian thực của máy tính là bởi vì các máy tính khác nhau thực hiện các phép tính sơ cấp trong những khoảng thời gian khác nhau. Hơn nữa, phân tích tất cả các phép toán thành các phép tính bit sơ cấp mà máy tính sử dụng là điều rất phức tạp. Các máy tính nhanh nhất hiện có có thể thực hiện các phép toán bit sơ cấp (ví dụ cộng, nhân, chia hoặc trao đổi hai bit) chỉ trong 10^{-9} giây (1 nano giây), nhưng một máy tính cá nhân có thể đòi hỏi tới 10^{-6} giây ($1\mu s$), tức là 1000 lần lâu hơn để cùng làm một phép toán.

Chúng ta sẽ minh họa sự phân tích độ phức tạp thời gian của một thuật toán bằng cách xét Algorithm 1 ở Tiết 2.1.

Ví dụ 1. Mô tả độ phức tạp thời gian của Algorithm 1 ở tiết 2.1 - thuật toán tìm phần tử lớn nhất của một tập hợp.

Giải : Vì phép so sánh là phép toán sơ cấp được sử dụng trong thuật toán này, nên số các phép so sánh sẽ được dùng làm thước đo độ phức tạp thời gian của thuật toán đó.

Để tìm phần tử lớn nhất của tập hợp n phần tử được liệt kê theo thứ tự tùy ý, giá trị lớn nhất tạm thời trước hết được đặt bằng phần tử đầu tiên của bảng liệt kê đó. Sau đó, sau khi thực hiện một phép so sánh xác định rằng ta còn chưa đạt tới cuối bảng, giá trị lớn nhất tạm thời và số hạng thứ hai của bảng được so sánh, và cập nhật giá trị lớn nhất tạm thời bằng số hạng thứ hai, nếu nó lớn hơn. Thủ tục này cứ tiếp tục như thế : mỗi số hạng của dãy dùng hai phép so sánh, một để xác định ta còn chưa đạt đến cuối bảng và một để xác định có phải cập nhật giá trị lớn nhất tạm thời hay không. Vì hai phép so sánh này được dùng cho mỗi phần tử của bảng từ số hạng thứ hai tới số hạng thứ n và thêm một phép so sánh nữa để ra khỏi vòng lặp lại khi $i = n + 1$, nên ta có chính xác $2(n - 1) + 1 = 2n - 1$ phép so sánh sẽ được dùng mỗi khi thuật toán này được áp dụng. Từ đó, thuật toán tìm phần tử lớn nhất của tập n phần tử có độ phức tạp thời gian là $O(n)$ - được đo theo số các phép so sánh được sử dụng.

■

Tiếp theo ta sẽ phân tích độ phức tạp thời gian của thuật toán tìm kiếm.

Ví dụ 2. Mô tả độ phức tạp thời gian của thuật toán tìm kiếm tuyến tính.

Giải : Số các phép so sánh được dùng trong thuật toán này cũng sẽ được xem như thước đo độ phức tạp thời gian của nó. Ở mỗi một bước của vòng lặp trong thuật toán, có hai phép so sánh được thực hiện : một để xem đã tới cuối bảng chưa và một để so sánh phần tử x với một số hạng của bảng. Cuối cùng còn một phép so sánh nữa làm ở ngoài vòng lặp. Do đó, nếu $x = a_i$, thì đã có $2i + 1$ phép so sánh được sử dụng. Số phép so sánh nhiều nhất, $2n + 2$, đòi hỏi phải được sử dụng khi phần tử x không có mặt trong bảng. Trong trường hợp đó, $2n$ phép so sánh được dùng để xác định x không phải là a_i đối với $i = 1, 2, ..., n$; một phép so sánh nữa được dùng để ra khỏi vòng lặp và một phép so sánh nữa được làm ở ngoài vòng lặp. Như vậy khi x không có mặt trong bảng, tổng số các phép so sánh đã sử dụng là $2n + 2$. Từ đó, thuật toán tìm kiếm tuyến tính đòi hỏi tối đa là $O(n)$ phép so sánh.

■

Loại phân tích độ phức tạp được dùng trong Ví dụ 2 là sự phân tích **trong trường hợp xấu nhất.** Đó là trường hợp phải dùng tối đa các phép toán để giải bài toán theo thuật toán đang xét với đầu vào có kích thước xác định. Phép phân tích trường hợp xấu nhất cho chúng ta biết thuật toán sẽ cần thực hiện bao nhiêu phép toán để đảm bảo sẽ đưa ra lời giải.

Ví dụ 3. Mô tả độ phức tạp thời gian của thuật toán tìm kiếm nhị phân.

Giải : Để đơn giản, ta giả sử rằng có $n = 2^k$ phần tử trong bảng liệt kê $a_1, a_2, ..., a_n$, với k là một số nguyên không âm. Chú ý rằng $k = \log n$ (Nếu n- số các phần tử của bảng - không phải là lũy thừa của 2, ta có thể xem bảng là một phần của một bảng lớn hơn với 2^{k+1} phần tử, trong đó $2^k < n < 2^{k+1}$. Do đó, 2^{k+1} là lũy thừa nhỏ nhất của 2 lớn hơn n).

Ở mỗi giai đoạn của thuật toán, i và j- vị trí của số hạng đầu tiên và số hạng cuối cùng của bảng con hạn chế tìm kiếm ở giai đoạn đó được so sánh để xem bảng con này còn nhiều hơn một phần tử hay không. Nếu $i < j$, một phép so sánh sẽ được làm để xác định x có lớn hơn số hạng ở giữa của bảng con hạn chế hay không.

Ở giai đoạn đầu tiên, việc tìm kiếm được hạn chế trong một bảng có 2^{k-1} số hạng. Cho đến đây, đã dùng hai phép so sánh. Thủ tục này sẽ được tiếp tục, mỗi giai đoạn dùng hai phép so sánh để hạn chế việc tìm kiếm trong một hàng có số hạng chỉ còn một nửa. Nói một cách khác, hai phép so sánh đã được dùng ở giai đoạn đầu tiên của thuật toán, khi bảng liệt kê có 2^k phần tử, hai phép so sánh nữa khi sự tìm kiếm được qui về bảng liệt kê có 2^{k-1} phần tử ; rồi hai phép so sánh nữa khi sự tìm kiếm được qui về bảng liệt kê có 2^{k-2} phần tử, v.v... cho đến khi sự tìm kiếm qui về một bảng liệt kê có $2^1 = 2$ phần tử thì hai phép so sánh nữa sẽ được sử dụng. Cuối cùng, khi trong bảng chỉ còn một phần tử, một phép so sánh sẽ cho chúng ta biết rằng không còn một phần tử nào thêm nữa và một phép so sánh nữa cho biết số hạng đó có phải là x hay không.

Như vậy, cần phải có nhiều nhất $2k + 2 = 2\log n + 2$ phép so sánh để thực hiện phép tìm kiếm nhị phân, khi bảng tìm kiếm có 2^k phần tử. (Nếu n không phải là luỹ thừa của 2, bảng gốc sẽ được mở rộng tới bảng có 2^{k+1} phần tử, với $k = \lfloor \log n \rfloor$ và sự tìm kiếm đòi hỏi phải thực hiện $2\lceil \log n \rceil + 2$ phép so sánh). Do đó, thuật toán tìm kiếm nhị phân đòi hỏi tối đa $O(\log n)$ phép so sánh. Từ sự phân tích ở trên suy ra rằng thuật toán tìm kiếm nhị phân, ngay cả trong trường hợp xấu nhất, cũng hiệu quả hơn thuật toán tìm kiếm tuyến tính. ■

Một loại phân tích độ phức tạp quan trọng khác, ngoài sự phân tích trong trường hợp xấu nhất, là sự phân tích được gọi là sự phân tích **trong trường hợp trung bình**. Trong loại phân tích này, ta phải tìm số trung bình các phép toán được dùng để giải bài toán trên toàn bộ các giá trị đầu vào có kích thước đã cho. Sự phân tích độ phức tạp trong trường hợp trung bình thường phức tạp hơn nhiều so với sự phân tích trong trường hợp xấu nhất. Tuy nhiên, sự phân tích trong trường hợp trung bình đối với thuật toán tìm kiếm tuyến tính có thể thực hiện không mấy khó khăn như trong Ví dụ 4 dưới đây.

Ví dụ 4. Mô tả sự phân tích trong trường hợp trung bình của thuật toán tìm kiếm tuyến tính, với giả thiết rằng phần tử x có mặt trong bảng liệt kê.

Giải : Có n kiểu đầu vào khả dĩ khi biết trước x có mặt trong bảng liệt kê. Nếu x là số hạng đầu tiên của bảng liệt kê, cần phải làm ba phép so sánh : một để xác định đã đến cuối bảng hay chưa, một để so sánh x với số hạng đầu tiên, và một ở ngoài vòng lặp. Nếu x là số hạng thứ hai trong bảng, thì cần phải làm 2 phép so sánh nữa, vì vậy ta đã sử dụng tổng cộng 5 phép so sánh. Nói chung, nếu x là phần tử thứ i của

bằng, thì mỗi một bước trong số i bước, ta cần phải dùng 2 phép so sánh và thêm một phép so sánh ở ngoài vòng lặp nữa, sao cho cần phải làm tổng cộng $2i + 1$ phép so sánh. Vì thế, số trung bình các phép so sánh đã được sử dụng là :

$$\frac{3 + 5 + 7 + \ldots + (2n + 1)}{n} = \frac{2(1 + 2 + 3 + \ldots + n) + n}{n}$$

Trong Tiết 3.2 ta sẽ chứng minh rằng :

$$1 + 2 + \ldots + n = \frac{n(n + 1)}{2}$$

Từ đó, số trung bình các phép so sánh được dùng bởi thuật toán tìm kiếm tuyến tính (khi biết trước x có mặt trong bảng) là :

$$\frac{2\left[\frac{n(n + 1)}{2}\right]}{n} + 1 = n + 2$$

tức là $O(n)$.

Chú ý. Trong sự phân tích trình bày ở trên ta đã giả thiết rằng x có mặt trong bảng liệt kê cần tìm kiếm và khả năng nó ở bất kỳ vị trí nào trong bảng là như nhau. Ta cũng có thể tiến hành phân tích trong trường hợp trung bình đối với thuật toán trên khi x có thể không có mặt trong bảng (xem Bài tập 13 ở cuối tiết này).

■

Bảng 1 giới thiệu một số thuật ngữ thường dùng để mô tả độ phức tạp thời gian của một thuật toán. Ví dụ, một thuật toán được nói là có **độ phức tạp hàm mũ**, nếu độ phức tạp thời gian của nó là $D(b^n)$, với $b > 1$, được đo qua một loại phép toán đặc biệt nào đó. Tương tự, một thuật toán có độ phức tạp thời gian là $D(n^b)$ được nói là có **độ phức tạp đa thức**. Thuật toán tìm kiếm tuyến tính có **độ phức tạp tuyến tính** (trong trường hợp xấu nhất hoặc trung hình) và thuật toán tìm kiếm nhị phân có **độ phức tạp logarit** (trong trường hợp xấu nhất), được đo qua các phép so sánh được sử dụng.

Đánh giá big-O của độ phức tạp thời gian của một thuật toán cho biết thời gian đòi hỏi để giải một bài toán thay đổi như thế nào khi kích thước đầu vào tăng. Thực tế, đánh giá tốt nhất (tức là với hàm nhỏ nhất) có thể được chứng minh rằng đã được sử dụng. Tuy nhiên, đánh giá big-O của độ phức tạp thời gian không thể được phiên trực tiếp thành lượng thời gian mà máy tính đã sử dụng. Một nguyên nhân là ở chỗ đánh giá big-O $f(n)$ là $O(g(n))$, với $f(n)$ là độ phức tạp thời gian của thuật

toán, có nghĩa là $f(n) \leq C(g(n))$ với mọi $x > k$, ở đây C và k là các hằng số. Vì vậy nếu không biết C và k trong bất đẳng thức trên, sự đánh giá này không thể được dùng để xác định giới hạn trên của số các phép toán được dùng. Hơn nữa, như đã nhận xét ở trên, thời gian đòi hỏi để thực hiện một phép toán còn phụ thuộc vào loại phép toán và máy tính sử dụng.

Tuy nhiên, thời gian đòi hỏi bởi một thuật toán để giải một bài toán có kích thước đã cho có thể xác định được nếu tất cả các phép toán được qui về các phép toán bit được sử dụng bởi máy tính. Bảng 2 cho thấy thời gian cần thiết để giải các bài toán có kích thước khác nhau theo thuật toán dùng số các phép tính bit đã được chỉ ra ở hàng thứ 3 cột hai đến bảy trong bảng. Thời gian lớn hơn 100^{100} năm được chỉ bằng các dấu sao (*). Khi lập bảng này, mỗi một phép toán bit được giả sử là mất 10^{-9} giây – thời gian đòi hỏi bởi một máy tính nhanh nhất hiện nay. Trong tương lai, thời gian này có thể sẽ giảm, khi những máy tính nhanh hơn được tạo ra.

BẢNG 1. Các thuật ngữ thường dùng cho độ phức tạp của một thuật toán

Độ phức tạp	*Thuật ngữ*
$O(1)$	Độ phức tạp hằng số
$O(\log n)$	Độ phức tạp logarit
$O(n)$	Độ phức tạp tuyến tính
$O(n \log n)$	Độ phức tạp $n \log n$
$O(n^b)$	Độ phức tạp đa thức
$O(b^n)$, $b > 1$	Độ phức tạp hàm mũ
$O(n!)$	Độ phức tạp giai thừa

Một điều quan trọng cần phải biết là máy tính phải cần bao lâu để giải xong một bài toán. Ví dụ, nếu một thuật toán đòi hỏi 10 giờ, thì có thể còn đáng chi phí thời gian máy tính (và tiền bạc nữa) đòi hỏi để giải bài toán đó. Nhưng nếu một thuật toán đòi hỏi 10 tỷ năm để giải một bài toán, thì thực hiện thuật toán đó sẽ là một điều phi lý. Một trong những hiện tượng lý thú nhất của công nghệ hiện đại là sự tăng ghê gớm của tốc độ và lượng bộ nhớ trong máy tính. Một nhân tố quan trọng khác làm giảm thời gian cần thiết để giải một bài toán là sự **xử lý song song** – đây là kỹ thuật thực hiện đồng thời các dãy phép tính. Do sự tăng tốc độ tính toán, và dung lượng bộ nhớ mấy tính, cũng như nhờ việc dùng các thuật toán lợi dụng được ưu thế của kỹ thuật xử lý song

song, các bài toán năm năm trước đây được xem là không thể giải được, thì bây giờ có thể giải bình thường và sau năm năm nữa câu nói này chắc vẫn còn đúng.

BẢNG 2. Thời gian máy tính được dùng bởi một thuật toán

Kích thước của bài toán	*Các phép tính bit được sử dụng*					
n	log *n*	*n*	*n*log *n*	n^2	2^n	*n!*
10	3.10^{-9} s	10^{-8} s	3.10^{-8} s	10^{-7} s	10^{-6} s	3.10^{-3} s
10^2	7.10^{-9} s	10^{-7} s	7.10^{-7} s	10^{-5} s	4.10^{13} năm	*
10^3	$1,0.10^{-8}$ s	10^{-6} s	1.10^{-5} s	10^{-3} s	*	*
10^4	$1,3.10^{-8}$ s	10^{-5} s	1.10^{-4} s	10^{-1} s	*	*
10^5	$1,7.10^{-8}$ s	10^{-4} s	2.10^{-3} s	10s	*	*
10^6	2.10^{-8} s	10^{-3} s	2.10^{-2} s	17 phút	*	*

BÀI TẬP

1. Có bao nhiêu phép so sánh được dùng trong thuật toán trong Bài tập 10, Tiết 2.1 để tìm số tự nhiên nhỏ nhất trong dãy n số tự nhiên?

2. Viết thuật toán sắp 4 số hạng đầu tiên của một dãy có chiều dài tùy ý theo thứ tự tăng dần. Chứng minh rằng thuật toán này có độ phức tạp thời gian là $O(1)$ được tính qua số các phép so sánh được sử dụng.

3. Giả sử một phần tử đã biết có mặt trong số bốn số hạng đầu tiên của một bảng liệt kê gồm 32 số hạng. Hỏi thuật toán tìm kiếm tuyến tính hay thuật toán tìm kiếm nhị phân tìm ra vị trí của phần tử đó nhanh hơn.

4. Xác định số các phép nhân được dùng để tính x^{2^k} bắt đầu với x rồi liên tiếp bình phương (để tìm x^2, x^4, v.v...). Cách này có hiệu quả hơn cách nhân x với chính nó một số lần thích hợp không?

5. Cho đánh giá big-O đối với số các phép so sánh được dùng bởi một thuật toán để xác định số các số 1 trong một xâu bit bằng cách kiểm tra từng bit của xâu, để xác định nó có là bit 1 không. (Xem Bài tập 19, Tiết 2.1)

6*. a) Chứng minh rằng thuật toán sau xác định số các bit 1 trong một xâu bit S.

---

procedure đếm bit (S : xâu bit)
count : = 0
while $S \neq 0$
begin
    count : = *count* + 1
    S : = $S \wedge (S - 1)$
end {*count* là số các số 1 trong S}

Ở đây $S - 1$ là xâu bit nhận được bằng cách thay bit 1 ở bên phải cùng thành bit 0 và tất cả các bit 0 ở bên phải nó thành bit 1. (Nhớ rằng $S \wedge (S - 1)$ là AND bit của S và $S - 1$).

b) Cần phải thực hiện bao nhiêu phép AND bit để tìm số các bit 1 trong một xâu bit?

7. Thuật toán thông thường để đánh giá một đa thức

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

tại $x = c$ có thể được thể hiện trong giả mã sau :

---

procedure đa thức (c, a_0, a_1 ... a_n : real number)
power : = 1
y : = a_0
for i : = 1 **to** n
begin
    power : = *power* * c
    y : = $y + a_i$ * power.
end $\{y = a_n c^n + a_{n-1}c^{n-1} + \ldots + a_1 c + a_0\}$

Ở đây giá trị cuối cùng của y chính là giá trị của đa thức tại $x = c$.

a) Đánh giá $3x^2 + x + 1$ ở $x = 2$ bằng cách thực hiện từng bước của thuật toán trên.

b) Có chính xác bao nhiêu phép nhân và phép cộng đã được sử dụng để đánh giá đa thức bậc n tại $x = c$? (không kể các phép cộng được dùng để tăng biến của vòng lặp).

8. Có một thuật toán (qua các phép nhân và phép cộng) hiệu quả hơn thuật toán thông thường ở trên dùng để đánh giá một đa thức. Thuật toán đó gọi là **phương pháp Horner**. Giả mã sau cho thấy cách dùng phương pháp đó để xác định giá trị của đa thức

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \text{ tại } x = c.$$

---

procedure *Horner* (c, a_0, a_1, ... a_n : real number)
$y := a_n$
for $i := 1$ **to** n
$y := y * c + a_{n-i}$
$\{y = a_n c^n + a_{n-1}c^{n-1} + \ldots + a_1 c + a_0\}$

---

a) Đánh giá $3x^2 + x + 1$ tại $x = 2$ bằng cách thực hiện từng bước của thuật toán trên.

b) Có chính xác bao nhiêu phép nhân và phép cộng đã được sử dụng bởi thuật toán đó để đánh giá một đa thức bậc n ở $x = c$? (không kể các phép cộng được dùng để tăng biến vòng lặp).

9. Một bài toán lớn cỡ như thế nào có thể giải trong một giây nếu dùng một thuật toán đòi hỏi phải thực hiện $f(n)$ phép tính bit, với mỗi phép tính bit được thực hiện trong 10^{-9}s và $f(n)$ có các giá trị sau :

a) $\log n$? b) n ? c) $n \log n$?

d) n^2 ? e) 2^n ? f) $n!$?

10. Một thuật toán cần bao nhiêu thời gian để giải một bài toán có kích thước n, nếu thuật toán đó dùng $2n^2 + 2^n$ phép toán bit, mỗi một phép mất 10^{-9}s, với các giá trị sau của n ?

a) 10 b) 20 c) 50 d) 100.

11. Một thuật toán dùng 2^{50} phép toán bit sẽ cần bao nhiêu thời gian, nếu mỗi phép toán bit mất một khoảng thời gian sau :

a) 10^{-6}s b) 10^{-9}s c) 10^{-12}s.

12. Xác định số phép so sánh ít nhất. (hay hiệu, suất, trong trường hợp tốt nhất).

a) Dòi hỏi để xác định số lớn nhất trong một dãy các số nguyên khi dùng Algorithm 1 của tiết 2.1.

b) Được sử dụng để xác định vị trí của một phần tử trong một dãy n số hạng khi dùng thuật toán tìm kiếm tuyến tính.

c) Được dùng để xác định vị trí một phần tử trong dãy n số hạng khi dùng thuật toán tìm kiếm nhị phân.

13. Phân tích độ phức tạp thời gian trong trường hợp trung bình của thuật toán tìm kiếm tuyến tính, nếu biết chính xác một nửa thời gian phần tử x không có mặt trong dãy và khả năng x ở bất cứ vị trí nào trong dãy là như nhau.

14. Một thuật toán được gọi là **tối ưu** để giải một bài toán đối với một phép toán xác định, nếu như không có một thuật toán nào khác giải được bài toán ấy mà chỉ dùng số các phép toán đó ít hơn.

a) Chứng minh rằng Algorithm 1 ở Tiết 2.1 là thuật toán tối ưu đối với số các phép so sánh các số nguyên (Chú ý: các phép so sánh được dùng để "kế toán" trong vòng lặp không liên quan gì đến đây).

b) Thuật toán tìm kiếm tuyến tính đối với số các phép so sánh các số nguyên có là tối ưu không? (không kể các phép so sánh được dùng để "kế toán" trong vòng lặp).

15. Mô tả độ phức tạp thời gian trong trường hợp xấu nhất được đo qua các phép so sánh của thuật toán tìm kiếm tam phân được cho trong Bài tập 21 của Tiết 2.1.

16. Mô tả độ phức tạp thời gian trong trường hợp xấu nhất, được đo qua các phép so sánh của thuật toán tìm kiếm được mô tả trong Bài tập 22 của Tiết 2.1.

17. Phân tích độ phức tạp thời gian trong trường hợp xấu nhất của thuật toán mà bạn đã lập ở Bài tập 23 của Tiết 2.1 để xác định kiểu của một bảng liệt kê các số nguyên theo thứ tự không giảm.

18. Cũng hỏi như trên đối với thuật toán mà bạn đã lập ở Bài tập 24 của Tiết 2.1.

19. Cũng hỏi như trên đối với thuật toán bạn đã lập ở Bài tập 25 của Tiết 2.1.

20. Cũng hỏi như trên đối với thuật toán mà bạn đã lập ở Bài tập 26 của Tiết 2.1.

21. Cũng hỏi như trên đối với thuật toán mà bạn đã lập ở Bài tập 27 của Tiết 2.1.

2.3. CÁC SỐ NGUYÊN VÀ PHÉP CHIA

MỞ ĐẦU

Phần của toán học rời rạc có liên quan đến các số nguyên và tính chất của chúng thuộc một ngành của toán học có tên là **lý thuyết số**. Tiết này là mở đầu cho phần nhập môn gồm ba tiết của lý thuyết số. Trong tiết này chúng ta sẽ ôn lại một số khái niệm cơ bản của lý thuyết số như : tính chia hết, ước số chung lớn nhất và số học đồng dư. Trong Tiết 2.4 ta sẽ mô tả một số thuật toán quan trọng lấy từ lý thuyết số, liên hệ các tư liệu trong Tiết 2.1 và 2.2 về thuật toán và độ phức tạp của chúng với những khái niệm được đưa vào ở tiết này. Ví dụ, chúng ta sẽ đưa ra thuật toán tìm ước số chung lớn nhất của hai số nguyên dương và thuật toán thực hiện số học của máy tính bằng cách dùng khai triển nhị phân.

Những ý tưởng mà chúng ta sẽ phát triển trong tiết này đều dựa trên khái niệm về tính chia hết. Và một khái niệm quan trọng dựa trên tính chia hết là khái niệm số nguyên tố. Số nguyên tố là một số nguyên lớn hơn 1 và chỉ chia hết cho 1 và chính nó. Xác định một số nguyên có là nguyên tố hay không là điều rất quan trọng trong những ứng dụng đối với ngành mật mã. Một định lý quan trọng của lý thuyết số - Định lý cơ bản của số học - khẳng định rằng tất cả các số nguyên dương đều có thể biểu diễn một cách duy nhất dưới dạng tích của các số nguyên tố. Việc phân tích các số nguyên ra thừa số nguyên tố có vai trò quan trọng trong mật mã. Phép chia một số nguyên cho một số nguyên dương khác cho thương số và số dư. Làm việc với các số dư sẽ dẫn tới số học

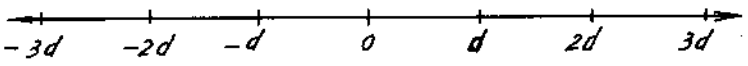
đồng dư được dùng xuyên suốt trong tin học. Trong tiết này chúng ta sẽ xét ba ứng dụng của số học đồng dư : sự sinh các số giả ngẫu nhiên, sự gán các vị trí bộ nhớ cho các file và mã và giải mã các thư tín.

PHÉP CHIA

Khi một số nguyên được chia cho một số nguyên thứ hai khác không, thương số có thể là một số nguyên hoặc không. Ví dụ, 12/3 = 4 là một số nguyên, trong khi 11/4 = 2,75 lại không là một số nguyên. Điều này dẫn tới định nghĩa sau :

ĐỊNH NGHĨA 1. Nếu a và b là hai số nguyên với $a \neq 0$, ta nói b chia hết cho a nếu có một số nguyên c sao cho $b = ac$. Khi b chia hết cho a, ta cũng nói a là một ước số của b và b là bội của a. Ký hiệu $a \mid b$ là chỉ b chia hết cho a và $a \nmid b$ để chỉ b không chia hết cho a.

Hình 1 cho đường thẳng số chỉ rõ số nguyên chia hết cho số nguyên dương d.



Hình 1. Các số nguyên chia hết cho số nguyên dương d.

Ví dụ 1. Xác định xem $3 \mid 7$ và $3 \mid 12$ có đúng không?

Giải : Ta có $3 \nmid 7$ vì 7/3 không phải là một số nguyên. Trái lại $3 \mid 12$ vì 12/3 = 4 là một số nguyên.

■

Ví dụ 2. Cho n và d là hai số nguyên dương. Có bao nhiêu số nguyên dương không vượt quá n chia hết cho d?

Giải : Các số nguyên dương chia hết cho d là tất cả các số nguyên dương có dạng dk, với k cũng là một số nguyên dương. Do đó, số các số nguyên dương chia hết cho d và không vượt quá n sẽ bằng số các số nguyên k với $0 < kd \leq n$ hay $0 < k \leq \frac{n}{d}$. Vì vậy có $\lfloor \frac{n}{d} \rfloor$ số nguyên dương không vượt quá n chia hết cho d.

■

Một số tính chất cơ bản của tính chia hết được cho trong Định lý 1.

Định lý 1. Cho a, b, c là các số nguyên. Khi đó :

1) Nếu $a|b$ và $a|c$ thì $a|(b + c)$;

2) Nếu $a|b$ thì $a|bc$ với mọi số nguyên c ;

3) Nếu $a|b$ và $b|c$ thì $a|c$.

Chứng minh: Giả sử $a|b$ và $a|c$. Khi đó, theo định nghĩa của tính chia hết, suy ra có tồn tại các số nguyên s và t với $b = as$ và $c = at$.

Do đó, $$b + c = as + at = a(s + t)$$

Vì vậy, $b + c$ chia hết cho a. Phần 1 của định lý được chứng minh. việc chứng minh các phần 2 và 3 của định lý xin dành lại cho độc giả như một bài tập.

■

Mọi số nguyên dương lớn hơn một đều chia hết ít nhất cho hai số nguyên, vì mọi số nguyên dương đều chia hết cho 1 và chính nó. Các số nguyên dương chỉ có chính xác hai ước số nguyên dương khác nhau đó được gọi là **số nguyên tố**.

ĐỊNH NGHĨA 2. Số nguyên dương p lớn hơn 1 được gọi là số *nguyên tố* nếu nó chỉ có các ước số dương là 1 và p. Các số nguyên dương lớn hơn 1 và không phải là số nguyên tố được gọi là *hợp số*.

Ví dụ 3. Số 7 là số nguyên tố vì nó chỉ có các ước số dương là 1 và 7, trong khi 9 là một hợp số vì nó chia hết cho 3.

Số nguyên tố là các viên gạch xây nên các số nguyên dương, như định lý cơ bản của số học dưới đây chứng tỏ. Sự chứng minh định lý này sẽ được cho trong Tiết 3.2.

Định lý 2. **Định lý cơ bản của số học.** Mọi số nguyên dương đều có thể được viết duy nhất dưới dạng tích của các số nguyên tố. Trong đó các số nguyên tố được viết theo thứ tự tăng dần.

Ví dụ dưới đây minh họa sự phân tích một số nguyên ra thừa số nguyên tố.

Ví dụ 4. Sự phân tích 100, 641, 999 và 1024 ra thừa số nguyên tố cho :

$$100 = 2.2.5.5. = 2^2 5^2$$

$$641 = 641.$$

$999 = 3.3.3.37 = 3^3.37$

và $1024 = 2.2.2.2.2.2.2.2.2.2 = 2^{10}$.

Việc xác định một số đã cho là số nguyên tố thường đóng một vai trò quan trọng. Ví dụ, trong ngành mật mã các số nguyên tố lớn nhất được dùng trong một số phương pháp để mã các bức thư bí mật. Một thủ tục để chứng minh một số nguyên là số nguyên tố được dựa trên nhận xét sau:

Định lý 3: Nếu n là một hợp số, thì n có ước số nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$.

Chứng minh: Nếu n là một hợp số, nó sẽ có một thừa số a với $1 < a < n$. Do đó, $n = a.b$ với a, b đều là các số nguyên dương lớn hơn 1. Ta cũng thấy rằng $a \leq \sqrt{n}$ và $b \leq \sqrt{n}$, vì nếu không $ab > \sqrt{n}.\sqrt{n} = n$. Vì vậy, n có ước số nguyên dương không vượt quá $\sqrt{n}$. Ước số này hoặc là số nguyên tố hoặc theo định lý cơ bản của số học có ước số là số nguyên tố. Trong mọi trường hợp, n có ước số nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$.

Từ Định lý 3 suy ra rằng một số nguyên là số nguyên tố nếu nó không chia hết cho một số nguyên tố nào nhỏ hơn hoặc bằng căn bậc hai của nó. Trong ví dụ sau, nhận xét đó đã được sử dụng để chứng minh số 101 là số nguyên tố.

Ví dụ 5. Chứng minh rằng số 101 là số nguyên tố. Các số nguyên tố không vượt quá $\sqrt{101}$ có cả thảy là 2, 3, 5 và 7. Vì 101 không chia hết cho 2, 3, 5 và 7 (tức là thương của 101 và các số đó không phải là một số nguyên), từ đó suy ra 101 là một số nguyên tố. ■

Vì tất cả các số nguyên đều có thể phân tích ra các thừa số nguyên tố, nên sẽ rất hữu ích nếu có một thủ tục tìm sự phân tích đó. Ta hãy xét bài toán phân tích số n ra thừa số nguyên tố. Hãy bắt đầu bằng việc chia n cho các số nguyên tố liên tiếp xuất phát từ số nguyên tố nhỏ nhất, tức là 2. Nếu n có một thừa số nguyên tố, thì theo Định lý 3 thừa số nguyên tố p không vượt qua $\sqrt{n}$ sẽ được tìm thấy. Do vậy, nếu không tìm được một thừa số nguyên tố nào không vượt quá $\sqrt{n}$, thì n sẽ là số nguyên tố. Tóm lại, nếu tìm được thừa số nguyên tố p, thì hãy tiếp tục phân tích n/p. Chú ý rằng n/p không thể có các thừa số nguyên tố nhỏ hơn p. Như vậy, nếu n/p không có các thừa số nguyên tố lớn hơn hoặc bằng p và không

vượt quá căn bậc hai của nó, thì n/p lại là một số nguyên tố. Trái lại, nếu nó có một thừa số nguyên tố q, thì lại tiếp tục phân tích $n(pq)$. Thủ tục này cứ tiếp tục cho tới khi phép phân tích quy về một số nguyên tố. Thủ tục này được minh họa trong ví dụ dưới đây.

Ví dụ 6: Phân tích 7007 ra thừa số nguyên tố.

Giải: Để phân tích 7007 ra thừa số nguyên tố, trước hết ra hãy thực hiện các phép chia 7007 cho các số nguyên tố liên tiếp, bắt đầu từ 2. Ta thấy 7007 không chia hết cho 2, 3, và 5. Tuy nhiên 7007 chia hết cho 7, với $7007/7 = 1001$. Tiếp sau, là chia 1001 cho các số nguyên tố liên tiếp bắt đầu từ 7. Ta ngay lập tức thấy rằng 1001 cũng lại chia hết cho 7 vì $1001/7 = 143$. Tiếp tục chia cho các số nguyên liên tiếp, bắt đầu từ 7. Mặc dù 143 không chia hết cho 7, nhưng nó chia hết cho 11 và $143/11 = 13$. Vì 13 là số nguyên tố nên thủ tục kết thúc ở đây.

Từ đó: $$7007 = 7.7.11.13 = 7^2.11.13$$

Dùng phép chia tầm thường và Định lý 3 ta đã nhận được các thủ tục để phân tích một số nguyên ra thừa số nguyên tố và kiểm tra tính nguyên tố của một số nguyên. Tuy nhiên, các thủ tục này chưa phải là những thuật toán hiệu quả nhất được biết cho các nhiệm vụ đó. Gần đây việc phân tích ra thừa số nguyên tố và kiểm tra tính nguyên tố của một số trở lên quan trọng trong những ứng dụng của lý thuyết số đối với ngành mật mã. Điều này dẫn tới sự quan tâm rất to lớn đối với việc phát triển các thuật toán hiệu quả cho các nhiệm vụ đó. Độc giả có thể tham khảo thêm về vấn đề này trong các tài liệu được giới thiệu ở cuối quyển sách này.

THUẬT TOÁN CHIA

Chúng ta thấy rằng một số nguyên có thể chia hết hoặc không chia hết cho một số nguyên khác. Tuy nhiên, khi một số nguyên được chia cho một số nguyên dương, luôn có một thương và một số dư, như thuật toán chia dưới đây cho thấy.

ĐỊNH LÝ 4. Thuật toán chia. Cho a là một số nguyên và d là một số nguyên dương. Khi đó tồn tại các số q và r duy nhất, với $0 \leq r < d$, sao cho $a = dq + r$.

Chú ý : Định lý 4 không thực sự là một thuật toán. (Tại sao không?). Tuy nhiên, chúng ta vẫn dùng tên truyền thống đó của nó.

ĐỊNH NGHĨA 3. Trong đẳng thức được cho trong thuật toán chia, d được gọi là *số chia*, a được gọi là *số bị chia*, q được gọi là *thương số* và r được gọi là *số dư*.

Hai ví dụ sau minh họa cho thuật toán chia.

Ví dụ 7. Xác định thương số và số dư khi chia 101 cho 11.

Giải : Ta có : $101 = 11.9 + 2$

Vậy, thương số của phép chia 101 cho 11 là 9 và số dư là 2. ■

Ví dụ 8. Xác định thương số và số dư của phép chia (−11) cho 3?

Giải : Ta có : $-11 = 3(-4) + 1$

Do đó, thương số của phép chia (−11) cho 3 là − 4 và số dư là 1. Chú ý rằng số dư không thể âm, do đó số dư trong ví dụ trên không thể là (− 2), mặc dù :

$$(-11) = 3\ (-3) - 2$$

vì $r = -2$ không thỏa mãn $0 < r < 3$. ■

Chú ý rằng số nguyên a chia hết cho số nguyên d nếu và chỉ nếu số dư bằng 0

ƯỚC SỐ CHUNG LỚN NHẤT, BỘI SỐ CHUNG NHỎ NHẤT

Số nguyên lớn nhất đều được chia hết bởi hai số nguyên được gọi là **ước số chung lớn nhất** của hai số nguyên đó.

ĐỊNH NGHĨA 4. Cho a *và* b là hai số nguyên khác không, số nguyên d lớn nhất sao cho $d \mid a$ và $d \mid b$ được gọi là *ước số chung lớn nhất* của a và b. Ước số chung lớn nhất của a và b được ký hiệu là ƯCLN(a, b).

Ước số chung lớn nhất của hai số nguyên khác không tồn tại bởi vì các ước số chung của chúng là hữu hạn. Một cách để tìm ước số chung lớn nhất của hai số nguyên là tìm tất cả các ước số chung dương của cả hai số rồi chọn lấy ước số chung lớn nhất. Điều này được làm trong các ví dụ dưới đây. Một thuật toán hiệu quả hơn để tìm ước số chung lớn nhất sẽ được cho sau.

Ví dụ 9. Tìm ước số chung lớn nhất của 24 và 36.

Giải : Các ước số chung dương của 24 và 36 là 1, 2, 3, 4, 6 và 12.

Vậy ƯCLN(24, 36) = 12. ■

Ví dụ 10. Tìm ước số chung lớn nhất của 17 và 22?

Giải : Các ước số chung của 17 và 22 không có một ước số chung dương nào ngoài 1. Vậy ƯCLN(17, 22) = 1. ■

Vì chỉ ra hai số nguyên không có các ước số chung dương nào ngoài 1 cũng là một điều quan trọng, nên ta có định nghĩa sau.

ĐỊNH NGHĨA 5. Các số nguyên a và b được gọi là *nguyên tố cùng nhau* nếu ước số chung lớn nhất của chúng bằng 1.

Ví dụ 11. Từ Ví dụ 10 suy ra 17 và 22 là nguyên tố cùng nhau, vì ƯCLN(17, 22) = 1. ■

Vì ta cũng thường cần phải chỉ rõ không có hai số nguyên nào trong tập các số nguyên có ước số chung lớn nhất lớn hơn 1, ta có định nghĩa sau :

ĐỊNH NGHĨA 6. Các số nguyên $a_1, a_2, \ldots, a_n$, được gọi là đôi một nguyên tố cùng nhau nếu ƯCLN$(a_i, a_j) = 1$ với mọi $1 \leqslant i, j \leqslant n$.

Ví dụ 12. Hãy xác định xem các số nguyên 10, 17 và 21 có đôi một nguyên tố cùng nhau không? Cũng hỏi như trên đối với 10, 19 và 24.

Giải : Vì ƯCLN(10, 17) = 1, ƯCLN(10, 21) = 1 và ƯCLN(17, 21) = 1, nên ta kết luận rằng 10, 17 và 21 là đôi một nguyên tố cùng nhau.

Vì ƯCLN(10, 24) = 2 > 1, ta thấy rằng 10, 19, và 24 không đôi một nguyên tố cùng nhau. ■

Một cách khác để tìm ước số chung lớn nhất của hai số nguyên là dùng các phân tích của chúng ra thừa số nguyên tố. Giả sử a và b là hai số nguyên khác không, được phân tích ra thừa số nguyên tố như sau :

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \text{ và } b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$$

ở đây mỗi số mũ là số nguyên không âm và tất cả các số nguyên tố xuất hiện trong phép phân tích ra thừa số nguyên tố của a hoặc b đều được đưa vào phép phân tích của a và b với số mũ zero, nếu cần. Khi đó ƯCLN(a, b) được cho bởi :

$$\text{ƯCLN}(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)}$$

Ở đây $\min(x, y)$ là số nhỏ nhất trong hai số x và y. Để chứng minh công thức tính ƯCLN(a,b) ở trên là đúng ta chỉ cần chứng tỏ rằng cả a và b đều chia hết cho số nguyên ở vế phải và không có số nguyên nào lớn hơn có tính chất đó. Thực vậy, a và b đều chia hết cho số nguyên đó vì lũy thừa của mỗi số nguyên tố trong phân tích ra thừa số nguyên tố của nó đều không vượt quá lũy thừa của số nguyên tố đó trong phân tích ra thừa số nguyên tố của a cũng như của b. Hơn nữa, a và b không thể chia hết cho số nguyên nào lớn hơn, vì số mũ của các số nguyên tố trong phân tích này không thể tăng và cũng không thể đưa thêm các số nguyên tố khác vào.

Ví dụ 13. Vì các phân tích của 120 và 500 ra thừa số nguyên tố là : $120 = 2^3.3.5$ và $500 = 2^2.5^3$, nên ước số chung lớn nhất của chúng là :

$$\text{ƯCLN}(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2.3^0.5^1 = 20.$$

■

Phép phân tích ra thừa số nguyên tố cũng có thể được dùng để tìm **bội số chung nhỏ nhất** của hai số nguyên.

ĐỊNH NGHĨA 7. Bội số chung nhỏ nhất của hai số nguyên a và b là số nguyên dương nhỏ nhất chia hết cho cả a lẫn b. Bội số chung nhỏ nhất của hai số nguyên a, b được ký hiệu là BCNN(a,b).

Bội số chung nhỏ nhất tồn tại vì tập các số nguyên chia hết cho a và b là không rỗng và tất cả các tập không rỗng của các số nguyên dương đều có phần tử nhỏ nhất (điều này sẽ được xét kỹ ở Chương 3). Giả sử rằng phân tích ra thừa số nguyên tố của a và b như cho ở trên. Khi đó bội số chung nhỏ nhất của a và b được cho bởi :

$$\text{BCNN}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}$$

với $\max(x,y)$ là số lớn nhất trong hai số x và y. Công thức này đúng bởi vì một bội số chung của a và b ít nhất phải có $\max(a_i, b_i)$ các thừa số nguyên tố p_i và bội số chung nhỏ nhất không có các thừa số nguyên tố nào khác với các thừa số nguyên tố của a và b.

Ví dụ 4. Xác định bội số chung nhỏ nhất của $2^3 3^5 7^2$ và $2^4 3^3$.

Giải: Ta có :

$$\text{BCNN}\,(2^3 3^5 7^2,\ 2^4 3^3) = 2^{\max(3,4)}\ 3^{\max(5,3)}\ 7^{\max(2,0)} = 2^4 3^5 . 7^2$$

■

Định lý sau cho mối quan hệ giữa ước số chung lớn nhất và bội số chung nhỏ nhất của hai số nguyên. Nó có thể được chứng minh bằng cách dùng hai công thức đã được dẫn ra ở trên đối với hai đại lượng đó. Phần chứng minh này xin dành lại cho độc giả như một bài tập.

ĐỊNH LÝ 5. Cho a và b là hai số nguyên dương. Khi đó

$$ab = \text{ƯCLN}\,(a,\ b).\text{BCNN}\,(a,b).$$

SỐ HỌC ĐỒNG DƯ

Trong một số tình huống, chúng ta chỉ cần quan tâm tới số dư của một số nguyên khi chia nó cho một số nguyên dương xác định nào đó. Ví dụ, khi chúng ta hỏi sau đây 50 giờ nữa sẽ là mấy giờ (theo đồng hồ 24 giờ), là chúng ta chỉ quan tâm tới số dư khi lấy 50 cộng với số giờ hiện thời và chia cho 24. Vì chúng ta thường phải quan tâm chỉ tới số dư như vậy, nên ta có một số ký hiệu đặc biệt cho nó.

ĐỊNH NGHĨA 8. Cho a là một số nguyên và m là một số nguyên dương. Khi đó ta ký hiệu a **mod** m là số dư khi chia a cho m.

Từ định nghĩa của số dư, ta suy ra rằng a **mod** m là số nguyên r sao cho : $a = qm + r$ và $0 \leqslant r < m$.

Ví dụ 15. Ta thấy

$$17\ \textbf{mod}\ 5 = 2,\ -133\ \textbf{mod}\ 9 = 2 \text{ và } 2001\ \textbf{mod}\ 101 = 82$$

■

Chúng ta cũng có ký hiệu để chỉ ra rằng hai số nguyên a và b có cùng số dư khi chia chúng cho một số nguyên dương m.

ĐỊNH NGHĨA 9. Nếu a và b là hai số nguyên và m là một số nguyên dương, thì a được gọi là đồng dư với b theo modun m nếu $a - b$ chia hết cho m. Chúng ta sẽ dùng ký hiệu $a \equiv b (\text{mod}\ m)$ để chỉ rằng a đồng dư với b theo modun m. Nếu a và b không đồng dư theo modun m, ta viết $a \not\equiv b\ (\text{mod}\ m)$.

Chú ý rằng $a \equiv b\ (\text{mod}\, m)$ nếu và chỉ nếu $a\ \textbf{mod}\, m = b\ \textbf{mod}\ m$.

Ví dụ 16. Xác định xem 17 có đồng dư với 5 theo modun 6 không? Cũng hỏi như vậy đối với 24 và 14?

Giải : Vì $17 - 5 = 12$ chia hết cho 6, nên $17 \equiv 5 \pmod 6$. Tuy nhiên, vì $24 - 14 = 10$ không chia hết cho 6 nên $24 \not\equiv 14 \pmod 6$.

■

Nhà toán học vĩ đại người Đức Friedrich Gauss đã phát triển khái niệm đồng dư vào cuối thế kỷ 19. Khái niệm đồng dư đóng một vai trò rất quan trọng trong sự phát triển của lý thuyết số. Định lý sau cho một cách rất tiện ích để làm việc với các đồng dư.

ĐỊNH LÝ 6. Cho m là một số nguyên dương. Các số nguyên a và b đồng dư theo modun m nếu và chỉ nếu tồn tại một số nguyên k sao cho $a = b + km$.

Chứng minh : Nếu $a \equiv b \pmod m$, thì $m \mid (a - b)$. Điều này có nghĩa là tồn tại một số nguyên k sao cho $a - b = km$, tức là $a = b + km$. Ngược lại, nếu tồn tại một số nguyên k sao cho $a = b + km$, thì $km = a - b$, tức $(a - b)$ chia hết cho m, nghĩa là $a \equiv b \pmod m$.

■

Định lý sau cho các phép cộng và nhân của các đồng dư.

ĐỊNH LÝ 7. Cho m là một số nguyên dương. *Nếu* $a \equiv b \pmod m$ và $c \equiv d \pmod m$ thì :

$$a + c \equiv b + d \pmod m$$

và

$$ac \equiv bd \pmod m$$

Chứng minh: Vì $a \equiv b \pmod m$ và $c \equiv d \pmod m$, nên tồn tại các số nguyên s và t sao cho $b = a + sm$ và $d = c + tm$. Từ đó,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

và

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$$

Do đó,

$$a + c \equiv b + d \pmod m$$

và

$$ac \equiv bd \pmod m$$

■

Ví dụ 17. Vì $7 \equiv 2 \pmod 5$ và $11 \equiv 1 \pmod 5$, từ Định lý 7 suy ra :

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$$

và

$$77 = 7.11 \equiv 2.1 = 2 \pmod 5.$$

■

CÁC ỨNG DỤNG CỦA ĐỒNG DƯ

Lý thuyết số có những ứng dụng trong rất nhiều lĩnh vực. Trong tiết này ta sẽ giới thiệu ba ứng dụng của nó, đó là việc dùng các đồng dư để gán các vị trí của bộ nhớ cho các file ; sự tạo các số giả ngẫu nhiên và hệ thống mật mã dựa trên số học đồng dư.

Ví dụ 18. *Các hàm băm.* Máy tính trung tâm ở trường bạn đều lưu giữ hồ sơ của mỗi sinh viên. Vấn đề đặt ra là các ô nhớ được gán như thế nào để hồ sơ của các sinh viên có thể truy cập được nhanh? Lời giải của bài toán này là cần phải dùng một **hàm băm** được chọn thích hợp. Mỗi hồ sơ được nhận dạng bằng cách dùng một **chìa khóa** tương ứng với một hồ sơ sinb viên duy nhất. Ví dụ, hồ sơ sinh viên thường được nhận dạng hằng cách dùng số của thẻ bảo hiểm xã hội của sinh viên đó như là *chìa khóa*. Hàm băm $h(k)$ gán ô nhớ $h(k)$ cho hồ sơ có chìa khóa là k. Thực tế, người ta có thể sử dụng nhiều hàm băm khác nhau. Một trong số các hàm băm thường dùng nhất là hàm :

$$h(k) = k \textbf{ mod } m.$$

Ở đây m là số các ô nhớ khả dụng.

Các hàm băm cần phải dễ dàng đánh giá để các hồ sơ được truy cập nhanh. Hàm băm $h(k) = k$ **mod** m đáp ứng được yêu cầu đó ; để tìm $h(k)$ ta chỉ cần tính số dư trong phép chia k cho m. Hơn nữa, hàm băm cần phải là toàn ánh để cho tất cả các ô nhớ đều có thể sử dụng. Hàm $h(k) = k$ **mod** m cũng thoả mãn tính chất này.

Ví dụ, khi $m = 111$, hồ sơ của sinh viên có số thẻ Bảo hiểm xã hội 064212848 sẽ được gán cho ô nhớ 14, vì

$$h(064212848) = 064212848 \textbf{ mod } 111 = 14.$$

Tương tự, vì $h(037149212) = 037149212$ **mod** $111 = 65$,

nên hồ sơ của sinh viên có số thẻ bảo hiểm xã hội là 037149212 sẽ được gán cho ô nhớ 65.

Vì hàm băm không phải là đơn ánh (do chìa khóa khả dĩ nhiều hơn số ô nhớ), nên có thể có hơn một hồ sơ được gán cho một ô nhớ. Khi xảy

ra điều này, người ta nói có sự **xung đột**. Một cách để giải quyết xung đột là gán cho ô nhớ còn tự do đầu tiên ngay sau ô nhớ đã được gán trước bởi hàm băm. Ví dụ, ngay sau khi làm hai phép gán cho hai hồ sơ ở trên, chúng ta sẽ gán ô nhớ 15 cho hồ sơ của sinh viên có số thẻ bảo hiểm xã hội là 107 405 723. Để hiểu tại sao, ta hãy chú ý rằng hàm $h(k)$ ánh xạ số thẻ Bảo hiểm này với ô nhớ 14, vì $h(107\ 405\ 723) = 107\ 405\ 723$ **mod** $111 = 14$, nhưng ô nhớ này đã bị chiếm bởi hồ sơ của sinh viên với số thẻ Bảo hiểm xã hội 064 212 848 rồi. Tuy nhiên, ô nhớ 15, ô nhớ đầu tiên sau ô nhớ 14 còn là tự do.

Còn có nhiều cách phức tạp hơn để giải quyết sự xung đột một cách có hiệu quả hơn phương pháp đơn giản vừa nêu ở trên. Các phương pháp đó được bàn tới trong các tài liệu tham khảo về các hàm băm được cho ở cuối cuốn sách này.

Ví dụ 19. *Các số giả ngẫu nhiên.* Các số được chọn một cách ngẫu nhiên thường cần thiết cho các mô phỏng trên máy tính. Có nhiều phương pháp để tạo ra các số có những tính chất của các số được chọn ngẫu nhiên. Vì các số được sinh ra bởi các phương pháp có hệ thống không thực sự là ngẫu nhiên, nên chúng được gọi là các **số giả ngẫu nhiên**.

Thủ tục thường dùng nhất để tạo các số giả ngẫu nhiên đó là **phương pháp đồng dư tuyến tính**. Chúng ta chọn 4 số nguyên, đó là **modun** m, **nhân tử** a, **số gia** c và **số hạt giống** x_0, với $2 \leqslant a \leqslant m$, $0 \leqslant c < m$ và $0 \leqslant x_0 < m$. Chúng ta sẽ tạo ra dãy các số giả ngẫu nhiên $\{x_n\}$ với $0 \leqslant x_n < m$ với mọi n bằng cách dùng liên tiếp phép đồng dư

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

(Đây là một ví dụ về định nghĩa đệ qui sẽ được bàn tới ở Tiết 3.3. Trong tiết đó, chúng ta sẽ chứng minh rằng dãy được định nghĩa như thế là hoàn toàn xác định).

Rất nhiều thực nghiệm trên máy tính đòi hỏi phải tạo các số giả ngẫu nhiên nằm giữa 0 và 1. Để tạo các số như vậy, chúng ta chia các số được tạo ra theo phương pháp đồng dư tuyến tính cho modun m, tức là chúng ta dùng các số x_n/m.

Ví dụ, dãy các số giả ngẫu nhiên được sinh ra khi chọn $m = 9$, $a = 7$, $c = 4$ và $x_0 = 3$ có thể tìm được như sau :

$$x_1 = 7x_0 + 4 = 7.3 + 4 = 25 \textbf{ mod } 9 = 7,$$

$$x_2 = 7x_1 + 4 = 7.7 + 4 = 53 \textbf{ mod } 9 = 8,$$
$$x_3 = 7x_2 + 4 = 7.8 + 4 = 60 \textbf{ mod } 9 = 6,$$
$$x_4 = 7x_3 + 4 = 7.6 + 4 = 46 \textbf{ mod } 9 = 1,$$
$$x_5 = 7x_4 + 4 = 7.1 + 4 = 11 \textbf{ mod } 9 = 2,$$
$$x_6 = 7x_5 + 4 = 7.2 + 4 = 18 \textbf{ mod } 9 = 0,$$
$$x_7 = 7x_6 + 4 = 7.0 + 4 = 4 \textbf{ mod } 9 = 4,$$
$$x_8 = 7x_7 + 4 = 7.4 + 4 = 32 \textbf{ mod } 9 = 5,$$
$$x_9 = 7x_8 + 4 = 7.5 + 4 = 39 \textbf{ mod } 9 = 3.$$

Vì $x_9 = x_0$ và vì mỗi một số hạng chỉ phụ thuộc vào số hạng trước nó, nên dãy sau đã được sinh ra :

3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 12, 0, 4, 5, 3 ...

Dãy này chứa 9 phần tử khác nhau trước khi lặp lại. Đa số các máy tính đều dùng phương pháp đồng dư tuyến tính để tạo ra các số giả ngẫu nhiên. Và thường thường phương pháp này được sử dụng với số gia $c = 0$. Một "máy phát" các số giả ngẫu nhiên như vậy được gọi là **máy phát nhân thuần tuý**. Ví dụ, máy phát nhân thuần tuý với modun $m = 2^{31} - 1$ và nhân tử $a = 7^5 = 16.807$ thường được dùng rất rộng rãi. Với các giá trị này, người ta có thể chứng minh rằng sẽ có $2^{31} - 2$ số được phát ra trước khi bắt đầu lặp lại.

MẬT MÃ

Đồng dư có nhiều ứng dụng trong toán học rời rạc cũng như trong tin học. Những thảo luận về các ứng dụng này có thể tìm trong các tài liệu tham khảo được giới thiệu ở cuối cuốn sách này. Một trong những ứng dụng của phép đồng dư liên quan đến mật mã học, một lĩnh vực nghiên cứu các thư từ bí mật. Một trong số những người sử dụng mật mã được biết sớm nhất - đó là Julius Caesar (Xê-da). Ông đã làm cho các bức thư trở nên bí mật bằng cách dịch mỗi chữ cái đi ba chữ cái về phía trước trong bảng chữ cái (và ba chữ cái cuối cùng thành ba chữ cái đầu tiên). Ví dụ, theo sơ đồ đó, chữ B được chuyển thành chữ E và chữ X được chuyển thành chữ A. Đây là một ví dụ về sự **mã hóa**, tức là quá trình làm cho bức thư trở nên bí mật.

Để biểu diễn quá trình mã hóa của Caesar một cách toán học, trước hết ta thay mỗi chữ cái bằng một số nguyên từ 0 đến 25, dựa vào vị trí

của nó trong bảng chữ cái. Ví dụ, thay A bằng 0, K bằng 10, và $Z = 25$. Phương pháp mã hóa của Caesar có thể được biểu diễn bởi hàm f, hàm này gán cho số nguyên không âm p, $p \leq 25$, số nguyên $f(p)$ trong tập {0, 1, 2, ... 25} sao cho :

$$f(p) = (p + 3) \textbf{ mod } 26.$$

Như vậy, trong phiên bản mã hóa của hức thư, chữ cái được biểu diễn bởi p sẽ được thay bằng chữ cái được biểu diễn hởi $(p + 3)$ **mod** 26

Ví dụ 20. Dùng mật mã của Caesar chuyển bức thư "Meet You in the Park" (Gặp em ở công viên) thành bức thư bí mật.

Giải : Trước hết, thay các chữ cái trong bức thư gốc thành các số, ta được :

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Bây giờ thay các số p đó bằng $f(p) = (p + 3)$ **mod** 26, ta được :

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13

Dịch trở lại các chữ cái, ta được bức thư đã mã hóa "PHHW BRX LQ WKH SDUN".

■

Để phục hồi lại hức thư gốc đã được mã hóa theo mật mã của Caesar, ta cần phải dùng hàm ngược f^{-1} của f. Chú ý rằng hàm f^{-1} ánh xạ số nguyên p từ tập hợp {0, 1, 2, ... 25) tới $f^{-1}(p) = (p-3)$ **mod** 26. Nói một cách khác, để tìm lại bức thư gốc mỗi một chữ cái lùi lại ba chữ trong bảng chữ cái, với ba chữ cái đầu tiên chuyển thành ba chữ cái cuối cùng tương ứng của bảng chữ cái. Quá trình phục hồi lại bức thư gốc từ bức thư đã được mã hóa được gọi là **giải mã**.

Có nhiều cách để tổng quát hóa mật mã của Caesar. Ví dụ, thay vì dịch mỗi chữ cái đi ba chữ cái, ta có thể dịch mỗi chữ cái đi k chữ cái, tức là

$$f(p) = (p + k) \textbf{ mod } 26$$

Một mật mã như thế được gọi là **mật mã dịch**. Chú ý rằng đối với loại mật mã này, sự giải mã được thực hiện bằng cách dùng :

$$f^{-1}(p) = (p - k) \textbf{ mod } 26.$$

Rõ ràng, phương pháp của Caesar và mật mã dịch không có độ an toàn cao. Có nhiều cách để nâng cao độ an toàn của phương pháp này. Một trong những cách đó, là dùng hàm có dạng :

$$f(p) = (ap + b) \textbf{ mod } 26$$

Ở đây a, b là các số nguyên được chọn sao cho f là một song ánh. Điều này sẽ cung cấp cho ta một số các hệ thống mật mã khả dĩ. Ví dụ sau minh họa việc dùng một trong số các hệ thống đó.

Ví dụ 21. Chữ cái nào sẽ thay thế cho chữ K khi ta dùng hàm $f(p) = (7p + 3) \bmod 26$ để mã hóa?

Giải . Trước hết, lưu ý rằng 10 biểu diễn chữ cái K. Khi đó, dùng hàm mã hóa đã cho, suy ra $f(10) = (7.10 + 3) \bmod 26 = 21$. Vì 21 biểu diễn chữ cái V, nên K sẽ được thay bằng chữ cái V trong bức thư mã hóa.

Phương pháp mã hóa của Caesar và tổng quát hóa của phương pháp đó tiến hành bằng cách thay mỗi chữ trong bảng chữ cái bằng một chữ cái khác thuộc bảng đó. Các phương pháp mã hóa thuộc loại này đều dễ bị khám phá bằng cách dựa vào tần xuất xuất hiện của các chữ cái trong bức thư. Các phương pháp mã hóa tinh xảo hơn dựa trên việc thay một khối chữ cái này bằng một khối chữ cái khác. Có một số kỹ thuật dựa trên số học đồng dư để mã hóa một khối các chữ cái. Sự thảo luận về các kỹ thuật này bạn đọc có thể tìm thấy trong các sách tham khảo được giới thiệu ở cuối cuốn sách này.

BÀI TẬP

1. Các số sau có chia hết cho 17 không

a) 68? b) 84? c) 357? d) 1001?

2. Chứng minh rằng nếu a là một số nguyên khác 0, thì

a) a chia hết cho 1 b) 0 chia hết cho a

3. Chứng minh phần 2 của Định lý 1.

4. Chứng minh phần 3 của Định lý 1.

5. Chứng minh rằng nếu $a|b$ và $b|a$, với a và b là các số nguyên, thì $a = b$ hoặc $a = -b$.

6. Chứng minh rằng nếu a, b, c, d là các số nguyên sao cho $a|c$ và $b|d$, thì $ab \mid cd$.

7. Chứng minh rằng nếu a, b và c là các số nguyên sao cho $ac|bc$, thì $a|b$.

8. Các số nguyên sau có phải là số nguyên tố không?

a) 19 b) 27 c) 93

d) 101 e) 107 f) 113.

9. Hãy xác định thương số và số dư trong các trường hợp sau :

a) 19 chia cho 7 b) – 111 chia cho 11

c) 789 chia cho 23 d) 1001 chia cho 13

e) 0 chia cho 19 f) 3 chia cho 5

g) –1 chia cho 3 h) 4 chia cho 1.

10. Phân tích các số dưới đây ra thừa số nguyên tố.

a) 39 b) 81 c) 101

d) 143 e) 289 f) 899

11. Phân tích 10! ra thừa số nguyên tố.

***12.** 100! tận cùng bằng bao nhiêu số không?

***13.** Một **số vô tỷ** là một số thực x không thể viết được dưới dạng tỷ số của hai số nguyên. Hãy chứng minh rằng $\log_2 3$ là một số vô tỷ.

14. Tìm các số nguyên dương nhỏ hơn 12 nguyên tố cùng nhau với 12?

15. Các tập nào cho dưới đây là đôi một nguyên tố cùng nhau?

a) (11, 15, 19) b) (14, 15, 21)

c) (12, 17, 31, 37) d) (7, 8, 9, 11).

16. Một số nguyên dương được gọi là **hoàn hảo**, nếu nó bằng tổng các ước số của nó (trừ ước là chính số đó).

b) Chứng minh 6 và 28 là các số hoàn hảo.

b) Chứng minh rằng $2^{p-1}(2^p - 1)$ là một số hoàn hảo nếu (2^p-1) là số nguyên tố.

17. Cho m là một số nguyên dương. Chứng minh rằng $a \equiv b \pmod m$ nếu $a \bmod m = b \bmod m$.

18. Cho m là một số nguyên dương. Chứng minh rằng $a \bmod m = b \bmod m$ nếu $a \equiv b \pmod m$.

19. Chứng minh rằng nếu $2^n - 1$ là số nguyên tố, thì n là số nguyên tố (Gợi ý : dùng hằng đẳng thức :

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1)).$$

20. Trong các số nguyên cho dưới đây, số nào là số nguyên tố

a) $2^7 - 1$ b) $2^9 - 1$

c) $2^{11} - 1$ d) $2^{13} - 1$.

21. Giá trị của **hàm Euler** ϕ tại số nguyên dương n được định nghĩa là số các số nguyên dương nhỏ hơn hoặc bằng n và nguyên tố cùng nhau với n. Tìm

a) $\phi(4)$ b) $\phi(10)$ c) $\phi(13)$.

22. Chứng minh rằng n là số nguyên tố nếu và chỉ nếu $\phi(n) = n - 1$.

23. Xác định giá trị của $\phi(p^k)$ với p là số nguyên tố và k là một số nguyên dương.

24. Xác định ước số chung lớn nhất của các cặp số nguyên sau :

a) $2^2.3^3.5^5$ và $2^5.3^3.5^2$ b) 2.3.5.7.11.13 và $2^{11}.3^9.11.17^{14}$.

c) 17 và 17^{17}. d) $2^2.7$. và $5^3.13$.

e) 0 và 5. f) 2.3.5.7 và 2.3.5.7.

25. Chứng minh rằng nếu n và k là các số nguyên dương, thì

$$\lceil \frac{n}{k} \rceil = \lfloor \frac{n-1}{k} \rfloor + 1.$$

26. Chứng minh rằng nếu a là một số nguyên và d là số nguyên dương lớn hơn 1, thì thương và số dư nhận được trong phép chia a cho d tương ứng là $\lfloor \frac{a}{d} \rfloor$ và $a - d \lfloor \frac{a}{d} \rfloor$.

27. Tính các đại lượng sau :

a) 13 **mod** 3 b) −97 **mod** 11

b) 155 **mod** 19 d)−221 **mod** 23

28. Liệt kê năm số nguyên đồng dư với 4 theo môđun 12.

29. Các số nguyên nào dưới đây đồng dư với 5 theo môđun 17.

a) 80 ? b) 103 ? c) −29 ? d) −122 ?

30. Nếu tích của hai số nguyên là $2^7\ 3^8\ 5^2\ 7^{11}$ và ước số chung lớn nhất của chúng là $2^3\ 3^4\ 5$ thì bội số chung nhỏ nhất của chúng bằng bao nhiêu?

31. Chứng minh rằng nếu a, b là các số nguyên dương, thì ab = ƯCLN(a,b). BCNN(a, b). (Gợi ý : Dùng phân tích a,b ra thừa số nguyên tố và các công thức tính ƯCLN(a,b) và BCNN(a, b) qua các phân tích đó).

32. Chứng minh rằng nếu $a \equiv b \pmod m$ và $c \equiv d \pmod m$ trong đó a, b, c, d và m là các số nguyên với $m \geq 2$, thì

$$a - c \equiv b - d \pmod m.$$

33. Chứng minh rằng nếu $n|m$ với n và m là các số nguyên dương lớn hơn 1 và nếu $a \equiv b \pmod m$ trong đó a, b là các số nguyên, thì $a \equiv b \pmod n$.

34. Chứng minh rằng nếu a, b, c và m là các số nguyên sao cho $m \geq 2$, $c > 0$ và $a \equiv b \pmod m$, thì $ac \equiv bc \pmod{mc}$.

35. Chứng minh rằng $ac \equiv bc \pmod m$ trong đó a, b, c và m là các số nguyên với m ≥ 2, không nhất thiết phải kéo theo $a \equiv b \pmod m$.

36. Chứng minh rằng nếu a, b và m là các số nguyên sao cho $m \geq 2$ và $a \equiv b \pmod m$ thì ƯCLN(a,m) = ƯCLN(b, m).

37. Chứng minh rằng nếu a, b, k và m là các số nguyên sao cho $k \geq 1$, $m \geq 2$ và $a \equiv b \pmod m$, thì $a^k \equiv b^k \pmod m$ với mọi $k \geq 1$.

38. Ô nhớ nào sẽ được gán bởi hàm băm $h(k) = k$ **mod** 101 cho hồ sơ của sinh viên có số thẻ Bảo hiểm xã hội là.

a) 104578690 b) 432222187

c) 372201919 d) 501338753

39. Một bãi đỗ xe có 31 chỗ dành cho khách. Được đánh số từ 0 đến 30. Các xe của khách được gán cho chỗ đỗ bằng cách dùng một hàm băm $h(k) = k$ **mod** 31 với k là số tạo bởi ba chữ số đầu trên biển đăng ký xe của khách.

a) Xác định chỗ đỗ của xe, nếu ba chữ số đầu trên biển đăng ký của nó là :

317, 918, 007, 100, 111, 310.

b) Mô tả thủ tục mà khách cần phải phải theo để tìm ra chỗ đỗ xe còn trống khi chỗ đỗ theo qui ước của họ đã bị chiếm.

40. Xác định dãy các số giả ngẫu nhiên được sinh ra bằng cách dùng "máy phát" đồng dư tuyến tính.

$$x_{n+1} = (4x_n + 1) \textbf{ mod } 7 \text{ với số hạt giống } x_0 = 3.$$

41. Cũng hỏi như trên với :

$$x_{n+1} = 3x_n \textbf{ mod } 11 \text{ và số hạt giống } x_0 = 2.$$

42. Viết một thuật toán dưới dạng giả mã để tạo ra một dãy các số giả ngẫu nhiên, bằng cách dùng máy phát đồng dư tuyến tính.

43. Mã hóa bức thư "DO NOT PASS GO" bằng cách dịch các chữ ra số bằng hàm mã hóa $f(p)$ cho dưới đây, rồi sau đó dịch các số đó trở lại thành chữ cái.

a) $f(p) = (p + 3)$ **mod** 26 (mật mã Caesar)
b) $f(p) = (p + 13)$ **mod** 26.
c) $f(p) = (3p + 7)$ **mod** 26.

44. Giải mã các bức thư đã được mã hóa bằng mật mã Caesar sau :

a) EOXH MHDQV
b) WHVW WRGDB
C) HDW GLP VXP.

2.4. SỐ NGUYÊN VÀ THUẬT TOÁN

MỞ ĐẦU

Như đã nhắc tới trong Tiết 2.1, thuật ngữ algorithm (thuật toán) ban đầu được dùng để chỉ các thủ tục thực hiện những phép tính số học đối với các số nguyên viết ở biểu diễn thập phân. Các thuật toán đó đã được sửa để dùng cho biểu diễn nhị phân là cơ sở cho số học của máy tính. Chúng cho những minh họa tốt đối với khái niệm thuật toán và độ phức tạp của thuật toán. Vì những lý do ấy mà trong tiết này chúng ta sẽ xét các thuật toán đó.

Ngoài các thuật toán được dùng trong số học, còn có nhiều thuật toán quan trọng liên quan đến các số nguyên. Chúng ta sẽ bắt đầu việc thảo luận về các số nguyên và thuật toán bằng thuật toán Euclid. Đây là một trong những thuật toán tiện ích nhất và có lẽ cũng là lâu đời nhất trong toán học. Chúng ta cũng sẽ mô tả thuật toán tìm khai triển cơ số b của một số nguyên với cơ số b bất kỳ.

THUẬT TOÁN EUCLID

Phương pháp mô tả trong Tiết 2.3 để tính ước số chung lớn nhất của hai số bằng cách dùng phân tích các số nguyên đó ra thừa số nguyên tố là không hiệu quả. Lý do là ở chỗ thời gian phải tiêu tốn cho sự phân tích đó. Chúng ta sẽ cho dưới đây một phương pháp hiệu quả hơn để tìm ước số chung lớn nhất, phương pháp đó được gọi là **thuật toán Euclid**. Thuật toán này đã được biết từ thời cổ đại. Nó mang tên nhà toán học cổ Hy lạp Euclid, người đã mô tả thuật toán này trong cuốn sách "Những yếu tố" nổi tiếng của ông.

Trước khi mô tả thuật toán Euclid, chúng ta hãy xem nó được sử dụng như thế nào để tìm ƯCLN(91, 287). Trước hết, người ta lấy số lớn, tức 287, chia cho số nhỏ, tức 91, và được :

$$287 = 91.3 + 14.$$

Bất kỳ một ước số chung nào của 287 và 91 cũng là ước số của 287 - 91.3 = 14. Và cũng như vậy, bất kỳ một ước số chung nào của 91 và 14 cũng là ước số của 287 = 91.3 + 14. Do đó, ước số chung lớn nhất của 287 và 91 cũng chính là ước số chung lớn nhất của 91 và 14. Điều này có nghĩa là bài toán tìm ƯCLN(287, 91) được qui về bài toán tìm ƯCLN(91, 14). Tiếp theo, chia 91 cho 14, ta được :

$$91 = 14.6 + 7.$$

Vì bất kỳ ước số chung nào của 91 và 14 cũng là ước số của 91 - 14.6 = 7 và bất kỳ ước số chung nào của 14 và 7 cũng là ước số của 91, suy ra ƯCLN(91, 14) = ƯCLN(14, 7)

Tiếp tục bằng cách chia 14 cho 7, ta được :

$$14 = 7.2$$

Vì 14 chia hết cho 7, suy ra ƯCLN(14, 7) = 7 và vì ƯCLN(287, 91) = ƯCLN(91, 14) = ƯCLN (14,7) = 7, vả bài toán ban đầu đặt ra đã giải xong.

Bây giờ chúng ta sẽ mô tả thuật toán Euclid tổng quát. Chúng ta sẽ dùng các phép chia liên tiếp để qui bài toán tìm ước số chung lớn nhất của hai số nguyên dương về chính bài toán đó nhưng với hai số nguyên nhỏ hơn, cho tới khi một trong hai số nguyên là zêro.

Thuật toán Euclid dựa trên kết quả sau về các ước số chung lớn nhất và thuật toán chia.

Bổ đề 1. Cho $a = bq + r$, trong đó a, b, q và r là các số nguyên.

Khi đó $$\text{ƯCLN}(a, b) = \text{ƯCLN}(b, r).$$

Chứng minh : Nếu chúng ta có thể chứng minh được rằng các ước số chung của cặp a và b cũng chính là các ước số chung của cặp b và r, thì tức là ta đã chứng minh được ƯCLN(a, b) = ƯCLN(b, r), vì cả hai cặp này cần phải có *cùng* ước số chung lớn nhất.

Giả sử d là một ước số chung của a và b. Từ đó suy ra $a - bq = r$ chia hết cho d (theo Định lý 1, Tiết 2.3). Do đó, mọi ước số chung của a và b đều là ước số chung của b và r.

Tương tự, giả sử d là ước số chung của b và r. Khi đó $bq + r = a$ cũng chia hết cho d. Do đó, mọi ước số chung của b và r cũng là ước số chung của a và b

Do đó, $$\text{ƯCLN}(a, b) = \text{ƯCLN}(b, r)$$

■

Giả sử rằng a và b là hai số nguyên dương với $a \geq b$. Giả sử $r_0 = a$ và $r_1 = b$. Bằng cách áp dụng liên tiếp thuật toán chia, ta tìm được :

$$r_0 = r_1q_1 + r_2 \qquad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_2 + r_3 \qquad 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_n.$$

Cuối cùng, số dư zêrô sẽ xuất hiện trong dãy các phép chia liên tiếp, vì dãy các số dư $a = r_0 > r_1 > r_2 > \ldots \geq 0$ không thể chứa quá a số hạng được. Hơn nữa, từ Bổ đề 1 suy ra :

$$\text{ƯCLN}(a, b) = \text{UCLN}(r_0, r_1) = \text{UCLN}(r_1, r_2) = \ldots$$

$$= \text{ƯCLN}(r_{n-2}, r_{n-1}) = \text{UCLN}(r_{n-1}, r_n) = \text{ƯCLN}(r_n, 0) = r_n$$

Do đó, ước số chung lớn nhất là số dư khác không cuối cùng trong dãy các phép chia.

Ví dụ 1. Dùng thuật toán Euclid tìm ƯCLN(414, 662)

Giải : Dùng liên tiếp thuật toán chia, ta được :

$$662 = 414.1 + 248$$
$$414 = 248.1 + 166$$
$$248 = 166.1 + 82$$
$$166 = 82.2 + 2$$
$$82 = 2.41$$

Do đó, ƯCLN(414, 662) = 2, vì 2 là số dư khác không cuối cùng. ■

Thuật toán Euclid được viết dưới dạng giả mã như sau :

ALGORITHM 1. THUẬT TOÁN EUCLID

```
procedure ƯCLN(a,b : positive integers)
x := a
y := b
while y ≠ 0
begin
    r := x mod y
    x := y
    y := r
end {ƯCLN(a,b) là x}
```

Trong Algorithm 1, các giá trị ban đầu của x và y tương ứng là a và b. Ở mỗi giai đoạn của thủ tục, x được thay bằng y và y được thay bằng x **mod** y, tức là số dư r trong phép chia của x cho y. Quá trình này được lặp lại chừng nào $y \neq 0$. Thuật toán sẽ ngừng khi $y = 0$ và giá

trị của x ở điểm này, đó là số dư khác không cuối cùng trong thủ tục, cũng chính là ước số chung lớn nhất của a và b.

Chúng ta sẽ nghiên cứu độ phức tạp thời gian của thuật toán Euclid trong Tiết 3.3 của Chương 3 và sẽ chứng tỏ rằng số các phép chia đòi hỏi để tìm ước số chung lớn nhất của a và b với $a \geq b$ là $O(\log b)$.

BIỂU DIỄN CÁC SỐ NGUYÊN

Trong cuộc sống hàng ngày chúng ta dùng ký hiệu thập phân để biểu diễn các số nguyên. Ví dụ, 965 được dùng để ký hiệu : $9.10^2 + 6.10 + 5$. Tuy nhiên, trong nhiều trường hợp việc dùng các cơ số khác 10 sẽ thuận tiện hơn. Đặc biệt, các máy tính thường dùng ký hiệu nhị phân (với cơ số là 2) khi thực hiện các phép tính số học và ký hiệu bát phân (cơ số 8) khi biểu diễn các ký tự như các chữ cái và con số. Thực tế, ta có thể dùng một số nguyên dương hất kỳ lớn hơn 1 làm cơ số để biểu diễn các số nguyên. Điều này được phát biểu trong định lý sau :

Định lý 1. Cho b là một số nguyên dương lớn hơn 1. Khi đó nếu n là một số nguyên dương, thì nó có thể được biểu diễn một cách duy nhất dưới dạng :

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0,$$

Ở đây k là một số nguyên không âm, $a_0, a_1, a_2 \ldots a_k$ là các số nguyên không âm nhỏ hơn b và $a_k \neq 0$.

Bạn đọc có thể tìm chứng minh của định lý trên trong các tài liệu tham khảo được giới thiệu ở cuốn sách này. Biểu diễn của n được cho trong Định lý 1 được gọi là **khai triển cơ số b của n**, nó được ký hiệu là $(a_k\ a_{k-1} \ldots a_1\ a_0)_b$. Ví dụ, $(245)_8$ hiểu diễn số

$$2.8^2 + 4.8 + 5 = 165.$$

Việc chọn 2 làm cơ số cho ta *khai triển nhị phân* của các số nguyên. Trong ký hiệu nhị phân mỗi số hoặc là 0 hoặc là 1. Nói cách khác, khai triển nhị phân của một số nguyên chính là một xâu bit. Các khai triển nhị phân (và các khai triển có liên quan là biến thể của khai triển nhị phân) được dùng bởi các máy tính để biểu diễn và làm các phép tính số học đối với các số nguyên.

Ví dụ 2. Xác định khai triển thập phân của số nguyên có khai triển nhị phân là $(101011111)_2$.

Giải : Ta có

$$(101011111)_2 = 2^8 + 2^6 + 2^4 + 2^3 + 2^2 + 2 + 1 = 351$$

■

Mười sáu là một cơ số khác cũng thường được dùng trong tin học. Khai triển cơ số 16 của một số nguyên được gọi là **khai triển thập lục phân**. Những khai triển này đòi hỏi phải có mười sáu chữ số khác nhau. Thường các chữ số thập lục phân được dùng là : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *A*, *B*, *C*, *D*, *E* và *F*, trong đó các chữ cái từ *A* đến *F* là biểu diễn các chữ số tương ứng với các số từ 10 đến 15 (trong ký hiệu thập phân).

Ví dụ 3. Xác định khai triển thập phân của số nguyên có khai triển thập lục phân là $(2AE0B)_{16}$?

Giải : Ta có :

$$(2AE0B)_{16} = 2.16^4 + 10.16^3 + 14.16^2 + 0.16 + 11 = (175627)_{10}.$$

■

Vì một chữ số thập lục phân được biểu diễn bằng cách dùng bốn bit, nên các **byte** – tức các xâu bit có chiều dài là 8 có thể được biểu diễn bởi hai chữ số thập lục phân. Ví dụ,

$$(11100101)_2 = (E5)_{16} \text{ vì } (1110)_2 = (E)_{16} \text{ và } (0101)_2 = (5)_{16}$$

Bây giờ chúng ta sẽ mô tả thuật toán xây dựng khai triển cơ số b của số nguyên n bất kỳ. Trước hết ta chia n cho b để được thương và số dư, tức là :

$$n = bq_0 + a_0 \qquad 0 \leqslant a_0 < b.$$

Số dư a_0 chính là chữ số đứng bên phải cùng trong khai triển cơ số b của n. Tiếp theo chia q_0 cho b, ta được

$$q_0 = bq_1 + a_1 \qquad 0 \leqslant a_1 < \text{h}$$

Ta thấy a_1 chính là chữ số thứ hai tính từ bên phải trong khai triển cơ số b của n. Tiếp tục quá trình này, bằng cách liên tiếp chia các thương cho b ta sẽ được các chữ số tiếp theo trong khai triển cơ số b của n là các số dư tương ứng. Quá trình này sẽ kết thúc khi ta nhận được một thương bằng 0.

Ví dụ 4. Tìm khai triển cơ số 8 của $(12345)_{10}$.

Giải : Trước hết, chia 12345 cho 8 ta được :

$$12345 = 8.1543 + 1.$$

Liên tiếp chia các thương tìm được cho 8, ta có :

$1543 = 8.192 + 7$

$192 = 8.24 + 0$

$24 = 8.3 + 0$

$3 = 8.0 + 3.$

Vì các số dư chính là các chữ số của khai triển cơ số 8 của 12345, ta suy ra rằng

$$(12345)_{10} = (30071)_8.$$

Giả mã dưới đây biểu diễn thuật toán tìm khai triển cơ số b

$(a_{k-1} \ldots a_1\ a_0)_b$ của số nguyên n.

ALGORITHM 2. XÂY DỰNG KHAI TRIỂN CƠ SỐ b.

procedure *khai triển cơ số b* (n : positive integers)

$q := n$

$k := 0$

while $q \neq 0$

begin

$a_k := q$ **mod** b

$q := \lfloor \frac{q}{b} \rfloor$

$k := k + 1$

end {khai triển cơ số b của n là $(a_{k-1} \ldots a_1\ a_0)_b$}

Trong Algorithm 2, q biểu diễn thương nhận được bởi các phép chia liên tiếp cho b, bắt đầu với $q = n$. Các chữ số trong khai triển cơ số b của n là các số dư tương ứng của các phép chia đó và được cho bởi q **mod** b. Thuật toán sẽ kết thúc khi $q = 0$.

THUẬT TOÁN CHO CÁC PHÉP TÍNH SỐ NGUYÊN

Các thuật toán thực hiện các phép tính với những số nguyên khi dùng các khai triển nhị phân của chúng là cực kỳ quan trọng trong số học của máy tính. Chúng ta sẽ mô tả ở đây các thuật toán cộng và nhân hai số nguyên trong biểu diễn nhị phân. Chúng ta cũng sẽ phân tích độ phức tạp tính toán của các thuật toán này thông qua số các phép toán bit thực sự được dùng. Trong suốt mục này, giả sử rằng khai triển nhị phân của a và b là :

$$a = (a_{n-1}\, a_{n-2} \ldots a_1 a_0)_2 \text{ và } b = (b_{n-1}\, b_{n-2} \ldots b_1\, b_0)_2,$$

sao cho a và b đều có n bit (đặt các bit 0 ở đầu mỗi khai triển đó, nếu cần).

Xét bài toán cộng hai số nguyên viết ở dạng nhị phân. Thủ tục thực hiện phép cộng có thể dựa trên phương pháp thông thường dùng để cộng các số bằng giấy và bút. Phương pháp này tiến hành bằng cách cộng cặp chữ số nhị phân với nhau, có nhớ, nếu xảy ra, để tính tổng của hai số nguyên. Dưới đây, ta sẽ mô tả chi tiết thủ tục này.

Để cộng a và b, trước hết cộng hai bit ở phải cùng của chúng, tức là ;

$$a_0 + b_0 = c_0.2 + s_0.$$

Ở đây s_0 là bit phải cùng trong khai triển nhị phân của $a + b$, c_0 là số **nhớ**, nó có thể bằng 0 hoặc 1. Sau đó ta cộng hai bit tiếp theo và số nhớ

$$a_1 + b_1 + c_0 = c_1.2 + s_1$$

Ở đây s_1 là bit tiếp theo (tính từ bên phải) trong khai triển nhị phân của $a + b$ và c_1 là số nhớ. Tiếp tục quá trình này bằng cách cộng các bit tương ứng trong hai khai triển nhị phân và số nhớ để xác định bit tiếp sau tính từ bên phải trong khai triển nhị phân của tổng $a + b$. Ở giai đoạn cuối cùng, cộng a_{n-1}, b_{n-1} và c_{n-2} để nhận được $c_{n-1}.2+s_{n-1}$. Bit đứng đầu của tổng là $s_n = c_{n-1}$. Kết quả, thủ tục này tạo ra được khai triển nhị phân của tổng, cụ thể là $a + b = (s_n\, s_{n-1}\, s_{n-2} \ldots s_1\, s_0)_2$.

Ví dụ 5. Cộng $a = (1110)_2$ và $b = (1011)_2$.

Giải : Theo thủ tục được chỉ rõ trong thuật toán, trước hết chú ý rằng :

$$a_0 + b_0 = 0 + 1 = 0.2 + 1$$

Vì vậy $c_0 = 0$ và $s_0 = 1$.

Sau đó, vì $a_1 + b_1 + c_0 = 1 + 1 + 0 = 1.2 + 0$

suy ra $c_1 = 1$, và $s_1 = 0$.

Tiếp theo, $a_2 + b_2 + c_1 = 1 + 0 + 1 = 1.2 + 0$,

sao cho $c_2 = 1$ và $s_2 = 0$.

Cuối cùng, vì $a_3 + b_3 + c_2 = 1 + 1 + 1 = 1.2 + 1$.

suy ra $c_3 = 1$ và $s_3 = 1$. Điều này có nghĩa là $s_4 = c_3 = 1$. Do đó, $s = a + b = (11001)_2$. Phép cộng này được thể hiện trên Hình 1.

```
  11
1110
1011
-----
11001
```

Hình 1. Cộng $(1110)_2$ và $(1011)_2$

Thuật toán cộng có thể được mô tả hằng cách dùng giả mã như sau.

ALGORITHM 3. PHÉP CỘNG CÁC SỐ NGUYÊN

procedure *cộng* (a, b : positive integers)
{Khai triển nhị phân của a và b tương ứng là $(a_{n-1}\ a_{n-2}\ \ldots\ a_1 a_0)_2$ và $(b_{n-1}\ b_{n-2}\ \ldots\ b_1\ b_0)_2$}
$c := 0$
for $j := 0$ **to** $n-1$
begin
$d := \lfloor (a_j + b_j + c)/2 \rfloor$
$s_j := a_j + b_j + c - 2d$
$c := d$
end
$s_n := c$
{khai triển nhị phân của tổng là $(s_n s_{n-1} \ldots s_1 s_0)_2$}

Tiếp theo, chúng ta sẽ phân tích số các phép cộng bit được dùng bởi Algorithm 3

Ví dụ 6. Có bao nhiêu phép cộng bit được đòi hỏi để dùng Algorithm 3 tính tổng tổng của hai số nguyên n bit (hoặc nhỏ hơn) trong biểu diễn nhị phân của chúng?

Giải : Tổng hai số nguyên được tính bằng cách cộng liên tiếp các cặp bit và khi cần phải cộng cả số nhớ nữa. Cộng một cặp bit và số nhớ đòi ba hoặc ít hơn phép cộng các bít. Như vậy tổng số các phép cộng bit được sử dụng nhỏ hơn ba lần số bit trong khai triển nhị phân. Do đó, số các phép cộng bit được dùng bởi Algorithm 3 để cộng hai số nguyên n bit là $O(n)$.

■

Tiếp theo, ta sẽ xét phép nhân của hai số nguyên n bit a và b. Thuật toán thông thường (được dùng khi nhân tay) tiến hành như sau. Dùng định luật phân phối, ta thấy rằng :

$$ab = a \sum_{j=0}^{n-1} b_j 2^j = \sum_{j=0}^{n-1} a(b_j 2^j)$$

Chúng ta có thể tính ab bằng cách dùng phương trình trên. Trước hết, chúng ta thấy rằng $ab_j = a$ nếu $b_j = 1$ và $ab_j = 0$ **nếu** $b_j = 0$. Mỗi lần chúng ta nhân một số hạng với 2 là chúng ta dịch khai triển nhị phân của nó một chỗ về phía trái bằng cách thêm một số không vào cuối khai triển nhị phân của nó. Do đó, chúng ta có thể nhận được $(ab_j)2^j$ bằng cách **dịch** khai triển nhị phân của ab_j đi j chỗ về phía trái, tức là thêm j số không vào cuối khai triển nhị phân của nó. Cuối cùng, ta sẽ nhận được tích ab bằng cách cộng n số nguyên $ab_j 2^j$ với $j = 0, 1, \ldots n - 1$.

Ví dụ dưới đây minh họa cách dùng thuật toán trên.

Ví dụ 7. Tìm tích của $a = (110)_2$ và $b = (101)_2$.

Giải : Trước hết chú ý rằng :

$$ab_0.2^0 = (110)_2.1.2^0 = (110)_2.$$

$$ab_1 2^1 = (110)_2.0.2^1 = (0000)_2$$

và $$ab_2.2^2 = (110)_2.1.2^2 = (11000)_2.$$

Để tìm tích, hãy cộng $(110)_2$, $(0000)_2$ và $(11000)_2$. Thực hiện các phép cộng này (dùng Algorithm 3, đưa vào cả các bit 0 ban đầu, nếu cần) cho thấy rằng $ab = (11110)_2$. Phép nhân được thể hiện trên Hình 2.

■

```
  110
  101
-----
  110
0 00
11 0
-----
11 110
```

Hình 2. Nhân $(110)_2$ với $(101)_2$.

Thủ tục trên được mô tả bằng giả mã sau:

ALGORITHM 4 Nhân các số nguyên.

procedure *nhân* (*a*, *b* : positive integers)

{Khai triển nhị phân của a và b tương ứng là $(a_{n-1}a_{n-2} \dots a_1a_0)_2$ và $(b_{n-1}\ b_{n-2} \dots b_1b_0)_2$}

for j : = 0 **to** n − 1

begin

if b_j = 1 **then** c_j : = a được dịch đi j chỗ

else c_j : = 0

end

{c_0, c_1 ..., c_{n-1} là các tích riêng phần }

p : = 0

for j : = 0 **to** n − 1

p : = p + c_j

{p là giá trị của tích ab}

Tiếp theo, ta sẽ xác định số các phép cộng bit và dịch bit được dùng bởi Algorithm 4 để nhân hai số nguyên.

Ví dụ 8. Có bao nhiêu phép cộng bit và dịch bit được dùng để nhân hai số nguyên a và b theo thuật toán Algorithm 4?

Giải : Algorithm 4 tính tích của hai số nguyên a và b bằng cách cộng các tính riêng phần c_0, c_1, c_2 ... và c_{n-1}. Khi b_j = 1, ta tính tích riêng phần c_j bằng cách dịch khai triển nhị phân của a đi j bit. Khi b_j = 0 thì không cần có dịch chuyển nào vì c_j = 0. Do đó, để tìm tất cả n số nguyên $ab_j\ 2^j$ với j = 0, 1, ... n −1, đòi hỏi tối đa :

$$0 + 1 + 2 + \dots + n - 1$$

phép dịch chỗ. Vì thế, theo Ví dụ 4 ở Tiết 1.8 số các dịch chuyển chỗ đòi hỏi là $O(n^2)$.

Để cộng các số nguyên ab_j từ $j = 0$ đến $n - 1$ đòi hỏi phải cộng một số nguyên n bit, một số nguyên $(n + 1)$ bit, ... và một số nguyên $2n$ bit. Từ Ví dụ 8 ta biết rằng mỗi phép cộng đó đòi hỏi $O(n)$ phép cộng bit. Do đó, có tất cả $O(n^2)$ phép cộng bit được đòi hỏi cho n phép cộng các tích riêng phần.

Điều đáng ngạc nhiên là có những thuật toán hiệu quả hơn thuật toán thông thường nhân hai số nguyên. Một thuật toán như vậy chỉ dùng $O(n^{1,585})$ các phép toán bit để nhân các số n bit sẽ được mô tả ở Chương 5.

BÀI TẬP

1. Dùng thuật toán Euclid tìm

a) ƯCLN (12, 18)

b) ƯCLN (111, 201)

c) ƯCLN (1001, 1331)

d) ƯCLN (12345, 54321)

2. Cũng hỏi như trên :

a) ƯCLN (1,5)

b) ƯCLN (100, 101)

c) ƯCLN (123, 277)

d) ƯCLN (1529, 14039)

e) ƯCLN(1529, 14038)

f) ƯCLN (11111, 111111)

3. Để tìm ƯCLN(34, 21) theo thuật toán Euclid, cần phải làm bao nhiêu phép chia?

4. Cũng hỏi như trên đối với ƯCLN (34, 55)?

5. Chuyển từ biểu diễn thập phân sang biểu diễn nhị phân của các số nguyên sau :

a) 231 b) 4532 c) 97644.

6. Cũng hỏi như trên đối với các số nguyên sau :

a) 321 b) 1023 c) 100632.

7. Chuyển từ biểu diễn nhị phân sang biểu diễn thập phân của các số nguyên sau :

a) 11111

b) 10000 00001

c) 10101 0101

d) 11010 01000 10000

8. Cũng hỏi như trên đối với các số nguyên sau :

a) 11011

b) 10101 10101

c) 11101 11110

d) 11111 00000 11111

9. Tìm một phương pháp đơn giản để chuyển từ biểu diễn thập lục phân về biểu diễn nhị phân của các số nguyên.

10. Tìm một phương pháp đơn giản để chuyển từ biểu diễn nhị phân về biểu diễn thập phân lục phân.

11. Chuyển từ biểu diễn thập lục phân về biểu diễn nhị phân của các số nguyên sau :

a) 80E b) 135AB

c) ABBA d) DEFACED.

12. Chuyển từ biểu diễn nhị phân về biểu diễn thập lục phân của các số nguyên sau :

a) 111 10111 b) 10 10101 01010 c) 11101 11011 10111

13. Chứng minh rằng tất cả các số nguyên dương đều có thể biểu diễn một cách duy nhất dưới dạng tổng các lũy thừa phân biệt của 2 (*Gợi ý* : xét khai triển nhị phân của các số nguyên).

14. Có thể chứng minh rằng mọi số nguyên đều có thể biểu diễn duy nhất dưới dạng

$$l_k 3^k + l_{k-1} 3^{k-1} + \ldots + l_1 .3 + l_0$$

với l_j bằng -1, 0 hoặc 1 và $j = 0, 1, 2 \ldots k$.

Khai triển loại này được gọi là **khai triển tam phân cân bằng**

Hãy tìm khai triển tam phân cân bằng của

a) 5, b) 13 c) 37 d) 79

15. Chứng minh rằng một số nguyên dương chia hết cho 3 nếu và chỉ nếu tổng các chữ số thập phân của nó chia hết 3.

16. Chứng minh rằng một số nguyên dương chia hết cho 11 nếu và chỉ nếu hiệu của tổng các chữ số thập phân của nó ở các vị trí chẵn và tổng các chữ số thập phân của nó ở các vị trí lẻ chia hết cho 11.

17. Chứng tỏ rằng một số nguyên dương chia hết cho 3 nếu và chỉ nếu hiệu của tổng các chữ số nhị phân của nó ở vị trí chẵn và tổng các chữ số nhị phân của nó ở vị trí lẻ chia hết cho 3.

Biểu diễn **bù đối với một** *của các số nguyên được dùng để đơn giản hóa số học của máy tính. Để biểu diễn các số nguyên dương và âm với giá trị tuyệt đối nhỏ hơn 2^n, cần dùng cả thảy n + 1 bit. Bit bên trái cùng được dùng để biểu thị dấu. Một bit 0 ở vị trí này được dùng để chỉ số nguyên dương, còn bit 1 ở vị trí này được dùng để chỉ số nguyên âm. Đối với các số nguyên dương các bit còn lại đồng nhất với khai triển nhị phân của số nguyên đó. Đối với các số âm, các bit còn lại nhận được bằng cách trước hết tìm khai triển nhị phân của giá trị tuyệt đối của số nguyên đó, sau đó lấy phần bù của từng bit trong đó với phần bù của 1 là 0 và phần bù của 0 là 1.*

18. Tìm biểu diễn bù đối với một của các số nguyên sau bằng cách dùng các xâu bit có chiều dài 6

a) 22 b) 31 c) −7 d) −19

19. Các biểu diễn hù đối với một có chiều dài 5 sau đây biểu diễn các số nguyên nào?

a) 11001 b) 01101 c) 10001 d) 11111

20. Biểu diễn bù đối với một của số − *m* nhận được từ biểu diễn bù đối với một của *m* như thế nào, nếu dùng các xâu bit có chiều dài *n*?

21. Làm thế nào nhận được biểu diễn bù đối với một của tổng hai số nguyên từ biểu diễn bù đối với một của từng số nguyên đó ?

22. Cũng hỏi như trên đối với hiệu của hai số nguyên.

23. Đôi khi các số nguyên được mã hóa bằng cách dùng khai triển nhị phân 4–chữ số để biểu diễn một chữ số thập phân. Điều này tạo ra dạng **thập phân mã hóa nhị phân** của các số nguyên. Ví dụ, số 791 được mã hóa theo cách đó trở thành 011110010001. Hỏi phải cần bao nhiêu bit để hiểu diễn một số có *n* chữ số thập phân khi dùng loại mã hóa này?

Khai triển Cantor là tổng có dạng :

$$a_n n! + a_{n-1}(n-1)! + \ldots + a_2 2! + a_1 1!$$

với a_i *là một số nguyên thoả mãn* $0 \leqslant a_i \leqslant i$ *và* $i = 1, 2, \ldots n$.

24. Tìm các khai triển Cantor của :

a) 2 b) 7 c) 19

d) 87 e) 1000 f) 1 000 000

25*. Mô tả một thuật toán tìm khai triển Cantor của một số nguyên.

26*. Mô tả thuật toán cộng hai số nguyên từ khai triển Cantor của chúng.

27. Cộng $(10111)_2$ và $(11010)_2$ bằng cách thực hiện từng bước của thuật toán cộng được cho trong phần lý thuyết của tiết này.

28. Nhân $(1110)_2$ và $(1010)_2$ bằng cách thực hiện từng bước thuật toán nhân cho trong phần lý thuyết của tiết này.

29. Mô tả thuật toán tính hiệu của hai khai triển nhị phân.

30. Đánh giá số các phép toán bit được dùng để trừ hai khai triển nhị phân.

31. Lập một thuật toán để xác định $a > b$, $a = b$ hay $a < b$ đối với hai số nguyên a và b ở dạng khai triển nhị phân

32. Thuật toán so sánh ở Bài tập 31 dùng bao nhiêu phép toán bit khi số lớn hơn trong hai số a và b có n bit trong khai triển nhị phân của nó.

33. Đánh giá độ phức tạp của Algorithm 2 để tìm khai triển cơ số b của số nguyên n qua số các phép chia được dùng.

2.5. MA TRẬN

MỞ ĐẦU

Các ma trận được dùng suốt trong toán học rời rạc để biểu diễn mối quan hệ giữa các phần tử trong một tập hợp. Trong các chương sau, chúng ta sẽ dùng các ma trận trong một số rất lớn các mô hình. Ví dụ, các ma trận sẽ được dùng trong các mạng thông tin và các hệ thống giao thông vận tải. Nhiều thuật toán sẽ được phát triển để dùng các mô hình ma trận đó. Tiết này sẽ ôn lại một số kiến thức về số học các ma trận sẽ được dùng trong các thuật toán đó.

ĐỊNH NGHĨA 1. *Ma trận* là một hảng số hình chữ nhật. Một ma trận có m hàng và n cột được gọi là ma trận $m \times n$. Một ma trận có số hàng bằng số cột được gọi là một ma trận *vuông*. Hai ma trận là bằng nhau nếu chúng nó cùng số hàng và số cột và các phần tử tương ứng ở tất cả các vị trí đều bằng nhau.

Ví dụ 1 Ma trận

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$$

là ma trận 3×2.

■

Bây giờ chúng ta sẽ đưa ra một số thuật ngữ về ma trận. Các chữ cái hoa và đậm sẽ được dùng để ký hiệu các ma trận.

ĐỊNH NGHĨA 2. Cho

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

Hàng thứ i của là ma trận $1 \times n$ $[a_{i1}, a_{i2} \ldots a_{in}]$.

Cột thứ j của A là ma trận $n \times 1$

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \cdot \\ \cdot \\ \cdot \\ a_{nj} \end{bmatrix}$$

Phần tử thứ (i, j) của $\mathbf{A}$ là phần tử a_{ij}, tức là số nằm ở hàng thứ i và cột thứ j của $\mathbf{A}$. Một ký hiệu ngắn gọn và thuận tiện của ma trận $\mathbf{A}$ là viết $\mathbf{A} = [a_{ij}]$, ký hiệu đó cho biết $\mathbf{A}$ là một ma trận có phần tử thứ (i, j) *là* a_{ij}.

SỐ HỌC MA TRẬN

Bây giờ chúng ta sẽ xét các phép toán cơ bản của số học ma trận, bắt đầu bằng định nghĩa phép cộng các ma trận.

ĐỊNH NGHĨA 3. cho $\mathbf{A} = [a_{ij}]$ và $\mathbf{B} = [b_{ij}]$ là các ma trận $m \times n$. Tổng của **A** và **B**, được ký hiệu là $\mathbf{A} + \mathbf{B}$ là ma trận $m \times n$ có phần tử thứ (i, j) là $a_{ij} + b_{ij}$. Nói cách khác, $\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}]$.

Tổng của hai ma trận có cùng kích thước nhận được bằng cách cộng các phần tử ở những vị trí tương ứng. Các ma trận có kích thước khác nhau không thể cộng được với nhau, vì tổng của hai ma trận chỉ được xác định khi cả hai ma trận có cùng số hàng và cùng số cột.

Ví dụ 2. Ta có :

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{bmatrix}$$

■

Bây giờ chúng ta sẽ xét phép nhân các ma trận. Tích của hai ma trận chỉ được xác định khi số cột của ma trận thứ nhất bằng số hàng của ma trận thứ hai.

ĐỊNH NGHĨA 4. Cho **A** là ma trận $m \times k$ và **B** là ma trận $k \times n$. Tích của **A** và **B**, được ký hiệu là **AB**, là ma trận $m \times n$ với phần tử thứ (i, j) bằng tổng các tích của các phần tử tương ứng từ hàng thứ i *của* **A** *và cột thứ* j *của* **B**. Nói cách khác, nếu $\mathbf{AB} = [c_{ij}]$, thì

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{ik}b_{kj} = \sum_{t=1}^{k} a_{it}b_{tj}$$

Trong Hình 1 hàng tô đậm của **A** và cột tô đậm của **B** được dùng để tính phần tử c_{ij} của **AB**. Tích của hai ma trận không xác định khi số hàng của ma trận thứ nhất và số cột của ma trận thứ hai không như nhau.

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1k} \\ a_{21} & a_{22} & \ldots & a_{2k} \\ \vdots & & & \vdots \\ a_{i1} & a_{i2} & \ldots & a_{ik} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1j} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2j} & \ldots & b_{2n} \\ \vdots & & & \vdots & & \vdots \\ b_{k1} & b_{k2} & \ldots & b_{kj} & \ldots & b_{kn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \vdots & & & \vdots \\ & & c_{ij} & \\ \vdots & & & \vdots \\ c_{m1} & c_{m2} & \ldots & c_{mn} \end{bmatrix}$$

Hình 1. Tích của $\mathbf{A} = [a_{ij}]$ và $\mathbf{B} = [b_{ij}]$.

Dưới đây là một số ví dụ về tích hai ma trận.

Ví dụ 3. Cho

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \quad \text{và} \quad \mathbf{B} = \begin{bmatrix} 2 & 4 \\ 1 & 1 \\ 3 & 0 \end{bmatrix}$$

Tìm **AB**.

Giải : Vì **A** là ma trận 4×3 và **B** là ma trận 3×2 nên tích **AB** là xác định và là ma trận 4×2. Để tìm các phần tử của **AB**, các phần tử tương ứng của các hàng của **A** và các cột của **B** ban đầu được nhân với nhau rồi sau đó các tích đó sẽ được cộng lại. Ví dụ, phần tử ở vị trí (3,1) của **AB** là tổng các tính của các phần tử ở hàng thứ 3 của **A** và cột thứ 1 của **B**, cụ thể là $3.2 + 1.1 + 0.3 = 7$. Khi tất cả các phần tử của **AB** đã được tính, ta được :

$$\mathbf{AB} = \begin{bmatrix} 14 & 4 \\ 8 & 9 \\ 7 & 13 \\ 8 & 2 \end{bmatrix}$$

■

Phép nhân ma trận không có tính chất giao hoán. Tức là, nếu **A** và **B** là hai ma trận, thì không nhất thiết **AB** phải bằng **BA**. Thực tế, có thể chỉ một trong hai tích đó là xác định. Ví dụ, nếu **A** là ma trận 2×3 và **B** là ma trận 3×4, khi đó **AB** là xác định và là ma trận 2×4, tuy nhiên ma trận **BA** là không xác định vì không thể nhân ma trận 3×4 với ma trận 2×3.

Nói chung, giả sử **A** là ma trận $m \times n$ và **B** là ma trận $r \times s$. Khi đó **AB** là xác định chỉ khi $n = r$ và **BA** là xác định chỉ khi $s = m$. Hơn nữa, thậm chí khi **AB** và **BA** đều xác định, thì chúng cũng sẽ không cùng kích thước trừ trường hợp $m = n = r = s$. Do đó, nếu cả hai **AB** và **BA** xác định và có cùng kích thước, thì cả **A** và **B** đều phải là các ma trận vuông và có cùng kích thước. Hơn thế nữa, thậm chí nếu cả **A** và **B** đều là các ma trận $n \times n$, thì **AB** và **BA** cũng không nhất thiết phải bằng nhau, như ví dụ dưới đây cho thấy :

Ví dụ 4. Cho $\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ và $\mathbf{B} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

Hỏi **AB** có bằng **BA** không?

Giải : Ta tìm được

$$\mathbf{AB} = \begin{bmatrix} 3 & 2 \\ 5 & 3 \end{bmatrix} \text{ và } \mathbf{BA} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$$

Vậy $\mathbf{AB} \neq \mathbf{BA}$.

■

CÁC THUẬT TOÁN NHÂN MA TRẬN

Định nghĩa của tích hai ma trận dẫn tới thuật toán tính tích của hai ma trận. Giả sử rằng $\mathbf{C} = [c_{ij}]$ là ma trận $m \times n$ là tích của ma trận $m \times k$ $\mathbf{A} = [a_{ij}]$ và ma trận $k \times n$ $\mathbf{B} = [b_{ij}]$. Thuật toán dựa trên định nghĩa nhân ma trận được biểu diễn dưới dạng giả mã như sau :

ALGORITHM 1. NHÂN MA TRẬN

```
procedure nhân ma trận (A, B : ma trận)
for i := 1 to m
begin
    for j := 1 to n
    begin
        cij := 0
        for q := 1 to k
        cij := cij + aiqbqj
    end
end {C = [cij] là tích của A và B}
```

Bây giờ chúng ta sẽ xác định độ phức tạp của thuật toán này qua số các phép nhân và phép cộng được dùng.

Ví dụ 5. Có bao nhiêu phép cộng và phép nhân các số nguyên được dùng trong Algorithm 1 để nhân hai ma trận có các phần tử là các số nguyên?

Giải : Trong tích của **A** và **B** có n^2 phần tử. Để tìm mỗi phần tử đòi hỏi cả thảy n phép nhân và n phép cộng. Vậy tổng cộng có n^3 phép nhân và n^3 phép cộng đã được sử dụng.

■

Điều đáng ngạc nhiên là vẫn có các thuật toán hiệu quả hơn Algorithm 1. Như ví dụ 5 cho thấy, việc nhân hai ma trận $n \times n$ trực tiếp theo định nghĩa đòi hỏi phải có $O(n^3)$ phép nhân và phép cộng. Dùng các thuật toán khác, hai ma trận $n \times n$ có thể được nhân mà chỉ cần dùng $O(n^{\sqrt{7}})$ phép nhân và phép cộng (chi tiết về các thuật toán này có thể tìm trong các sách tham khảo được giới thiệu ở cuối cuốn sách này).

Có một bài toán quan trọng khác liên quan đến độ phức tạp của phép nhân ma trận. Đó là : tích $\mathbf{A}_1\ \mathbf{A}_2\ \ldots\ \mathbf{A}_n$ cần được tính như thế nào để phải dùng một số ít nhất các phép nhân số nguyên, trong đó $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ tương ứng là các ma trận $m_1 \times m_2$, $m_2 \times m_3$, ... $m_n \times m_{n+1}$ và có các phần tử đều là số nguyên? (Vì phép nhân ma trận có tính kết hợp, như Bài tập 13 ở cuối tiết này cho thấy, nên trình tự nhân trước hay sau không quan trọng). Trước khi nghiên cứu vấn đề này, cần chú ý rằng $m_1\ m_2\ m_3$ phép nhân các số nguyên được dùng để nhân ma trận $m_1 \times m_2$ và ma trận $m_2 \times m_3$ theo Algorithm 1. (Xem Bài tập 23 ở cuối tiết này). Ví dụ sau minh họa bài toán về độ phức tạp này.

Ví dụ 6. Cho $\mathbf{A}_1$, $\mathbf{A}_2$ và $\mathbf{A}_3$ tương ứng là các ma trận 30×20, 20×40 và 40×10 với các phần tử đều là số số nguyên. Hỏi phải nhân $\mathbf{A}_1$, $\mathbf{A}_2$ và $\mathbf{A}_3$ theo trình tự như thế nào để số các phép nhân là ít nhất?

Giải : Có hai cách tính tích $\mathbf{A}_1\mathbf{A}_2\mathbf{A}_3$. Đó là $\mathbf{A}_1(\mathbf{A}_2\mathbf{A}_3)$ và $(\mathbf{A}_1\mathbf{A}_2)\mathbf{A}_3$.

Nếu thực hiện nhân $\mathbf{A}_2$ và $\mathbf{A}_3$ trước, sẽ có tổng cộng $20.\ 40.\ 10 = 8000$ phép nhân đã được sử dụng để nhận được ma trận 20×10 $\mathbf{A}_2\mathbf{A}_3$. Sau đó nhân $\mathbf{A}_1$ với $\mathbf{A}_2\mathbf{A}_3$ đòi hỏi phải thực hiện $30.20.10 = 6000$ phép nhân nữa. Như vậy tổng cộng cần thực hiện $8000 + 6000 = 14000$ phép nhân. Mặt khác, nếu thực hiện nhân $\mathbf{A}_1$ và $\mathbf{A}_2$ trước, thì cần thực hiện $30.20.40 = 24000$ phép nhân để nhận được ma trận 30×40 $\mathbf{A}_1\mathbf{A}_2$. Sau đó, nhân $\mathbf{A}_1\mathbf{A}_2$ và $\mathbf{A}_3$ đòi hỏi phải thực hiện $30 \times 40 \times 10 = 12\,000$ phép nhân nữa. Từ đó, tổng cộng cần thực hiện $24\,000 + 12\,000 = 36\,000$ phép nhân.

Như vậy, nhân theo phương pháp thứ nhất chắc chắn sẽ hiệu quả hơn.

■

Các thuật toán xác định cách có hiệu quả nhất để nhân n ma trận có thể tìm trong các sách tham khảo được giới thiệu ở cuối sách này.

CHUYỂN VỊ VÀ LŨY THỪA CÁC MA TRẬN

Bây giờ chúng ta đưa vào một ma trận quan trọng có các phần tử chỉ là 0 và 1 .

ĐỊNH NGHĨA 5. Ma trận đồng nhất (hay còn gọi là ma trận đơn vị - ND) bậc n là ma trận $n \times n$ $\mathbf{I}_n = [\delta_{ij}]$, với $\delta_{ij} = 1$ nếu $i = j$ và $\delta_{ij} = 0$ nếu $i \neq j$. Do đó

$$\mathbf{I}_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Nhân một ma trận với ma trận đơn vị kích thước thích hợp không làm thay đổi ma trận đó. Nói cách khác, khi $\mathbf{A}$ là ma trận $m \times n$, ta có :

$$\mathbf{A}\mathbf{I}_n = \mathbf{I}_m\mathbf{A} = \mathbf{A}$$

Người ta cũng có thể định nghĩa lũy thừa của các ma trận vuông khi $\mathbf{A}$ là một ma trận $n \times n$, ta có :

$$\mathbf{A}^0 = \mathbf{I}_n, \quad \mathbf{A}^r = \underbrace{\mathbf{AAA} \dots \mathbf{A}}_{\text{n lần}}$$

Phép toán chuyển hàng thành cột và cột thành hàng của một ma trận vuông cũng được sử dụng trong nhiều thuật toán.

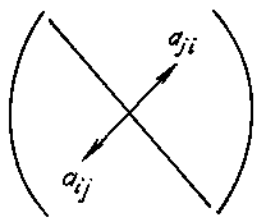
ĐỊNH NGHĨA 6. Cho $\mathbf{A} = [a_{ij}]$ là ma trận $m \times n$. *Chuyển vị* của $\mathbf{A}$, được ký hiệu là $\mathbf{A}^t$, là ma trận $n \times m$ nhận được bằng cách trao đổi các hàng và cột của ma trận $\mathbf{A}$ cho nhau. Nói cách khác, nếu $\mathbf{A}^t = [b_{ij}]$, thì $b_{ij} = a_{ji}$ với $i = 1, 2, \dots m$.

Ví dụ 7. Chuyển vị của ma trận $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ là ma trận $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$. ■

Các ma trận không đổi khi trao đổi các hàng và cột của nó cho nhau thường đóng vai trò quan trọng.

ĐỊNH NGHĨA 7. Ma trận vuông **A** được gọi là *đối xứng* nếu $\mathbf{A} = \mathbf{A}^t$. Như vậy, $\mathbf{A} = [a_{ij}]$ là đối xứng nếu $a_{ij} = a_{ji}$ với mọi i và j ; $0 \leqslant i \leqslant n$ và $0 \leqslant j \leqslant n$.

Chú ý rằng một ma trận là đối xứng nếu và chỉ nếu nó là ma trận vuông và đối xứng qua đường chéo chính của nó. Phép đối xứng này được minh họa trên Hình 2.



Hình 2. Ma trận đối xứng.

Ví dụ 8. Ma trận :

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$ là đối xứng

CÁC MA TRẬN ZÊRÔ - MỘT

Các ma trận có các phần tử là 0 hoặc 1 được gọi là các **ma trận zêrô-một**. Các ma trận zêrô-một thường được dùng để biểu diễn các cấu trúc rời rạc như chúng ta sẽ thấy trong các Chương 6 và 7. Các thuật toán dùng các cấu trúc này dựa trên số học Boole cho các ma trận zêrô-một. Số học này lại dựa trên các phép toán Boole $\vee$ và $\wedge$ thực hiện trên các cặp bit và được định nghĩa hởi :

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{nếu } b_1 = b_2 = 1 \\ 0 & \text{các trường hợp còn lại.} \end{cases}$$

$$b_1 \vee b_2 = \begin{cases} 0 & \text{nếu } b_1 = 0 \text{ hoặc } b_2 = 0 \\ 1 & \text{các trường hợp còn lại.} \end{cases}$$

ĐỊNH NGHĨA 8. Cho $\mathbf{A} = [a_{ij}]$ và $\mathbf{B} = [b_{ij}]$ là các ma trận zêrô-một $m \times n$. Khi đó *hợp* của **A** và **B**, được ký hiệu là $\mathbf{A} \vee \mathbf{B}$ là ma trận zêrô-một với phần tử ở vị trí (i, j) là $a_{ij} \vee b_{ij}$. *Giao* của **A** và **B**, được ký hiệu là $\mathbf{A} \wedge \mathbf{B}$, là ma trận zêrô - một với phần tử ở vị trí (i, j) là $a_{ij} \wedge b_{ij}$.

Ví dụ 9. Tìm hợp và giao của các các ma trận zêrô - một sau :

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \text{ và } \mathbf{B} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Giải : Hợp của **A** và **B** là :

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1\vee0 & 0\vee1 & 1\vee0 \\ 0\vee1 & 1\vee1 & 0\vee0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Giao của **A** và **B**

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1\wedge0 & 0\wedge1 & 1\wedge0 \\ 0\wedge1 & 1\wedge1 & 0\wedge0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Bây giờ ta định nghĩa tích Boole của hai ma trận.

ĐỊNH NGHĨA 9. Cho $\mathbf{A} = [a_{ij}]$ là ma trận zêrô – một $m\times k$ và $\mathbf{B} = [b_{ij}]$ là ma trận zêrô – một $k\times n$. Khi đó tích Boole của **A** và **B**, được ký hiệu là $\mathbf{A}\odot\mathbf{B}$ là ma trận $m\times n$ với phần tử ở vị trí (i, j) $[c_{ij}]$ là :

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \ldots \vee (a_{ik} \wedge b_{kj})$$

Chú ý rằng tích Boole của **A** và **B** nhận được bằng cách tương tự với tích thông thường của hai ma trận đó, nhưng với phép cộng được thay bằng phép $\vee$ và với phép nhân được thay bằng phép $\wedge$. Dưới đây là ví dụ về tích Boole của các ma trận.

Ví dụ 10. Tìm tích Boole của **A** và **B**, với

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ và } \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Giải : Tích Bool $\mathbf{A}\odot\mathbf{B}$ được cho bởi :

$$\mathbf{A}\odot\mathbf{B} = \begin{bmatrix} (1\wedge1)\vee(0\wedge0) & (1\wedge1)\vee(0\wedge1) & (1\wedge0)\vee(0\wedge1) \\ (0\wedge1)\vee(1\wedge0) & (0\wedge1)\vee(1\wedge1) & (0\wedge0)\vee(1\wedge1) \\ (1\wedge1)\vee(0\wedge0) & (1\wedge1)\vee(0\wedge1) & (1\wedge0)\vee(0\wedge1) \end{bmatrix}$$

$$= \begin{bmatrix} 1\vee0 & 1\vee0 & 0\vee0 \\ 0\vee0 & 0\vee1 & 0\vee1 \\ 1\vee0 & 1\vee0 & 0\vee0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

■

Algorithm 2 dưới dạng giả mã sau đây mô tả thuật toán tính tích Boole của 2 ma trận

ALGORITHM 2. TÍCH BOOLE

procedure tích Boole (**A**, **B** : các ma trận zêrô – một)

for $i := 1$ **to** m

begin

```
for j := 1 to n
    begin
        c_ij := 0
        for q := 1 to k
            c_ij := c_ij ∨ (a_iq ∧ b_qj)
    end
end {C = [c_ij] là tích Boole của A và B}
```

Chúng ta cũng có thể định nghĩa lũy thừa Boole của các ma trận zêrô – một vuông. Các lũy thừa này sẽ được dùng trong các nghiên cứu sau này của chúng ta về các đường trong đồ thị, các đường này được dùng, chẳng hạn, để mô hình các đường liên lạc trong các mạng máy tính.

ĐỊNH NGHĨA 10. Cho $\mathbf{A}$ là ma trận zêrô – một vuông và r là một số nguyên dương. Lũy thừa Boole bậc r của $\mathbf{A}$ được ký hiệu là $\mathbf{A}^{[r]}$ với

$$\mathbf{A}^{[r]} = \mathbf{A} \odot \mathbf{A} \odot \ \ldots \ \odot \mathbf{A}$$
$$\qquad\qquad\qquad\qquad\quad r \text{ lần}$$

($\mathbf{A}^{[r]}$ là hoàn toàn xác định vì tích Boole có tính chất kết hợp).

Chúng ta cũng có thể định nghĩa $\mathbf{A}^{[0]}$ là $\mathbf{I}_n$.

Ví dụ 11. Cho

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Tìm $\mathbf{A}^{[n]}$ với mọi n nguyên dương.

Giải : Ta thấy ngay rằng :

$$\mathbf{A}^{[2]} = \mathbf{A} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Ta cũng tìm được :

$$\mathbf{A}^{[3]} = \mathbf{A}^{[2]} \odot \mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \text{ và}$$

$$\mathbf{A}^{[4]} = \mathbf{A}^{[3]} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Tính thêm một lần nữa, ta được :

$$\mathbf{A}^{[5]} = \mathbf{A}^{[4]} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Độc giả bây giờ có thể thấy rằng $\mathbf{A}^{[n]} = \mathbf{A}^{[5]}$ với mọi n nguyên dương không nhỏ hơn 5.

■

Số các phép toán bit được dùng để tìm tích Boole của hai ma trận $n \times n$ cũng dễ dàng xác định được.

Ví dụ 2. Có bao nhiêu phép toán bit được dùng để tính $\mathbf{A} \odot \mathbf{B}$ với $\mathbf{A}$, $\mathbf{B}$ là các ma trận zêrô – một $n \times n$.

Giải. Có n^2 phần tử trong $\mathbf{A} \odot \mathbf{B}$. Dùng Algorithm 2, tổng cộng có n phép toán *OR* và n phép *AND* được dùng để tìm 1 phần tử của $\mathbf{A} \odot \mathbf{B}$. Vậy phải dùng $2n$ phép toán bit để tìm mỗi phần tử. Do đó khi dùng Algorithm 2, cần phải dùng $2n^3$ phép toán bit để tính $\mathbf{A} \odot \mathbf{B}$.

■

BÀI TẬP

1. Cho

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 2 & 0 & 4 & 6 \\ 1 & 1 & 3 & 7 \end{bmatrix}$$

a) Xác định kích thước của $\mathbf{A}$.

b) Xác định cột thứ 3 của $\mathbf{A}$.

c) Xác định dòng thứ 2 của $\mathbf{A}$.

d) Xác định phần tử ở vị trí (3,2) của $\mathbf{A}$.

e) Xác định $\mathbf{A}^t$.

2. Tìm $\mathbf{A} + \mathbf{B}$ với

a) $\mathbf{A} = \begin{bmatrix} 1 & 0 & 4 \\ -1 & 2 & 2 \\ 0 & -2 & -3 \end{bmatrix}$ và $\mathbf{B} = \begin{bmatrix} -1 & 3 & 2 \\ 2 & 2 & -3 \\ 2 & -3 & 0 \end{bmatrix}$

b) $\mathbf{A} = \begin{bmatrix} -1 & 0 & 5 & 6 \\ 4 & -3 & 5 & -2 \end{bmatrix}$ và $\mathbf{B} = \begin{bmatrix} -3 & 9 & -3 & 4 \\ 0 & -2 & -1 & 2 \end{bmatrix}$

3. Tìm **AB**, nếu

a) $\mathbf{A} = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$ và $\mathbf{B} = \begin{bmatrix} 0 & 4 \\ 1 & 3 \end{bmatrix}$

b) $\mathbf{A} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \\ 2 & 3 \end{bmatrix}$ và $\mathbf{B} = \begin{bmatrix} 3 & -2 & -1 \\ 1 & 0 & 2 \end{bmatrix}$

4. Tìm tích **AB**, với

a) $\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & -1 \\ -1 & 1 & 0 \end{bmatrix}$ và $\mathbf{B} = \begin{bmatrix} 0 & 1 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$

a) $\mathbf{A} = \begin{bmatrix} 1 & -3 & 0 \\ 1 & 2 & 2 \\ 2 & 1 & -1 \end{bmatrix}$ và $\mathbf{B} = \begin{bmatrix} 1 & -1 & 2 & 3 \\ -1 & 0 & 3 & -1 \\ -3 & -2 & 0 & 2 \end{bmatrix}$

5. Tìm ma trận **A** sao cho :

$$\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \mathbf{A} = \begin{bmatrix} 3 & 0 \\ 1 & 2 \end{bmatrix}$$

(*Gợi ý* : để tìm **A** bạn sẽ phải giải một hệ phương trình tuyến tính)

6. Tìm **A** sao cho

$$\begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 1 \\ 4 & 0 & 3 \end{bmatrix} \mathbf{A} = \begin{bmatrix} 7 & 1 & 3 \\ 1 & 0 & 3 \\ -1 & -3 & 7 \end{bmatrix}$$

7. Cho **A** là ma trận $m \times n$ và **O** là ma trận $m \times n$ với tất cả các phần tử đều là số zêrô. Chứng minh rằng :

$$\mathbf{A} = \mathbf{O} + \mathbf{A} = \mathbf{A} + \mathbf{O}$$

8. Chứng minh rằng phép cộng các ma trận có tính chất giao hoán, tức là, chứng minh rằng nếu **A** và **B** đều là các ma trận $m \times n$ thì $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$.

9. Chứng minh rằng phép cộng các ma trận có tính chất kết hợp, tức là, chứng minh rằng nếu **A**, **B** và **C** đều là các ma trận $m \times n$, thì

$$\mathbf{A} + (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) + \mathbf{C}$$

10. Cho **A** là ma trận 3×4, **B** là ma trận 4×5 và **C** là ma trận 4×4. Xác định xem các tích cho dưới đây tích nào xác định và tìm kích thước của các tích xác định đó :

a) **AB** b) **AB** c) **AC**

d) **CA** e) **BC** f) **CB**

11. Bạn biết gì về kích thước của hai ma trận **A** và **B**, nếu như cả hai tích **AB** và **BA** đều xác định?

12. Trong bài tập này ta sẽ chứng minh rằng phép nhân ma trận có tính chất phân phối đối với phép cộng?

a) Cho **A** và **B** là các ma trận $m \times k$ và C là ma trận $k \times n$. Chứng minh rằng $(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$

b) Giả sử dòng **C** là ma trận $m \times k$ và **A** và **B** là các ma trận $k \times n$. Chứng minh rằng $\mathbf{C}(\mathbf{A} + \mathbf{B}) = \mathbf{CA} + \mathbf{CB}$

13. Trong bài tập này ta sẽ chứng minh phép nhân ma trận có tính chất kết hợp. Giả sử **A** là ma trận $m \times p$, **B** là ma trận $p \times k$ và **C** là ma trận $k \times n$. Chứng minh rằng **A(BC)** = **A(BC)**.

14. Ma trận $n \times n$ $\mathbf{A} = [a_{ij}]$ được gọi là **ma trận chéo** nếu $a_{ij} = 0$ khi $i \neq j$. Chứng minh rằng tích của hai ma trận chéo $n \times n$ cũng là một ma trận chéo. Cho một qui tắc đơn giản để tính ma trận tích.

15. Cho $\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

Tìm công thức để tính $\mathbf{A}^n$ với n là một số nguyên dương.

16. Chứng minh rằng $(\mathbf{A}^t)^t = \mathbf{A}$.

17. Cho **A** và **B** là các ma trận $n \times n$ chứng minh rằng

a) $(\mathbf{A} + \mathbf{B})^t = \mathbf{A}^t + \mathbf{B}^t$

b) $(\mathbf{AB})^t = \mathbf{B}^t.\mathbf{A}^t$.

Nếu **A** *và* **B** *là các ma trận* $n \times n$ *và* $\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n$, *thì* **B** *được gọi là* **ma trận nghịch đảo** *của* **A** *(thuật ngữ này phù hợp vì ma trận* **B** *thỏa mãn tính chất đó là duy nhất) và* **A** *được gọi là ma trận* **khả nghịch**. *Ký hiệu* $\mathbf{B} = \mathbf{A}^{-1}$ *để chỉ rằng* **B** *là nghịch đảo của* **A**.

18. Chứng tỏ rằng

$$\begin{bmatrix} 2 & 3 & -1 \\ 1 & 2 & 1 \\ -1 & -1 & 3 \end{bmatrix}$$

là nghịch đảo của

$$\begin{bmatrix} 7 & -8 & 5 \\ -4 & 5 & -3 \\ 1 & -1 & 1 \end{bmatrix}$$

19. Cho **A** là ma trận 2×2 với

$$\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Chứng minh rằng nếu $ad - bc \neq 0$ thì

$$\mathbf{A}^{-1} = \begin{bmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{bmatrix}$$

20. Cho $\mathbf{A} = \begin{bmatrix} -1 & 2 \\ 1 & 3 \end{bmatrix}$

a) Tìm $\mathbf{A}^{-1}$ (*Gợi ý* : dùng Bài tập 19)

b) Tìm $\mathbf{A}^3$

c) Tìm $(\mathbf{A}^{-1})^3$

d) Dùng đáp số của bạn cho câu (b) và (c) chứng tỏ rằng $(\mathbf{A}^{-1})^3$ là nghịch đảo của $\mathbf{A}^3$.

21. Cho **A** là một ma trận khả nghịch. Chứng minh rằng $(\mathbf{A}^n)^{-1} = (\mathbf{A}^{-1})^n$ với mọi n là số nguyên dương.

22. Cho **A** là một ma trận. Chứng minh rằng ma trận $\mathbf{AA}^t$ là ma trận đối xứng. (*Gợi ý* : chứng minh ma trận này bằng ma trận chuyển vị của nó với sự giúp đỡ của Bài tập 17b).

23. Chứng minh rằng thuật toán thông thường dùng $m_1\ m_2\ m_3$ phép nhân để tính tích của ma trận $m_1 \times m_2$ **A** và ma trận $m_2 \times m_3$ **B**.

24. Cho biết cách có hiệu quả nhất để nhân các ma trận $\mathbf{A}_1$, $\mathbf{A}_2$ và $\mathbf{A}_3$ có kích thước tương ứng bằng :

a) 20×50 ; 50×10 ; 10×40 ?

b) 10×5 ; 5×50 ; 50×1 ?

25. Nêu cách hiệu quả nhất thể thực hiện phép nhân các ma trận $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$ và $\mathbf{A}_4$ nếu kích thước của chúng tương ứng hằng 10×2 ; 2×5; 5×20, và 20×3?

26 a) Chứng minh rằng hệ phương trình tuyến tính :

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\
\cdot \qquad\qquad \ldots \qquad\qquad \cdot \\
\cdot \qquad\qquad \ldots \qquad\qquad \cdot \\
\cdot \qquad\qquad \ldots \qquad\qquad \cdot \\
a_{n1}x_1 + q_{n2}x_2 + \ldots + a_{nn}x_n &= b_n
\end{aligned}$$

với các biến x_1, x_2 ... x_n có thể biểu diễn dưới dạng $\mathbf{AX} = \mathbf{B}$ với $\mathbf{A} = [a_{ij}]$; **X** là ma trận cột $n\times1$ với x_i là phần tử ở hàng thứ i ; và **B** là ma trận cột $n\times1$ với b_i là phần tử ở hàng thứ i.

b) Chứng minh rằng nếu $\mathbf{A} = [a_{ij}]$ là khả nghịch (như đã được định nghĩa ở trước Bài tập 18), thì nghiệm của hệ ở câu (a) có thể tìm được bằng cách dùng phương trình : $\mathbf{X} = \mathbf{A}^{-1}\mathbf{B}$.

27. Sử dụng các kết quả của Bài tập 18 và 26, giải hệ sau :

$$\begin{aligned}
7x_1 - 8x_2 + 5x_3 &= 5 \\
-4x_1 + 5x_2 - 3x_3 &= -3 \\
x_1 - x_2 + x_3 &= 0
\end{aligned}$$

28. Cho

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ và } \mathbf{B} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Tìm a) $\mathbf{A} \vee \mathbf{B}$ b) $\mathbf{A} \wedge \mathbf{B}$ c) $\mathbf{A} \odot \mathbf{B}$.

29. Cho

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ và } \mathbf{B} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Tìm

a) $\mathbf{A} \vee \mathbf{B}$; b) $\mathbf{A} \wedge \mathbf{B}$; c) $\mathbf{A} \odot \mathbf{B}$

30. Tìm tích Boole của **A** và **B** với

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \text{ và } \mathbf{B} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

31. Cho

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Tìm

a) $\mathbf{A}^{[2]}$; b) $\mathbf{A}^{[3]}$; c) $\mathbf{A} \vee \mathbf{A}^{[2]} \vee \mathbf{A}^{[3]}$

32. Cho **A** là một ma trận zêrô – một. Chứng minh rằng ;

a) $\mathbf{A} \vee \mathbf{A} = \mathbf{A}$; b) $\mathbf{A} \wedge \mathbf{A} = \mathbf{A}$

33. Trong bài tập này ta sẽ chứng minh các phép giao và hợp có tính chất giao hoán. Giả sử **A** và **B** là các ma trận zêrô–một $m \times n$. Chứng minh rằng

a) $\mathbf{A} \vee \mathbf{B} = \mathbf{B} \vee \mathbf{A}$ h) $\mathbf{A} \wedge \mathbf{B} = \mathbf{B} \wedge \mathbf{A}$.

34. Trong bài tập này ta sẽ chứng minb các phép giao và hợp có tính chất kết hợp. Cho **A**, **B** và **C** là các ma trận zêrô–một $m \times n$. Chứng minh rằng

a) $\mathbf{A} \vee (\mathbf{B} \vee \mathbf{C}) = (\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C}$

b) $\mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C}) = (\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C}$

35. Trong bài tập này ta sẽ chứng minh luật phân phối của phép giao đối với phép hợp và pbép hợp đối với giao. Giả sử **A**, **B**, và **C** là các ma trận zêrô–một $m \times n$. Chứng minh rằng

a) $\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) = (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C})$

b) $\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) = (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$

36. Cho **A** là ma trận zêrô–một $m \times n$ và **I** là ma trận đơn vị $n \times n$. Chứng minh rằng **A** . **I** = **I** . **A** = **A**.

37. Trong bài tập này ta sẽ chứng minh tích Boole có tính kết hợp. Cho **A** là ma trận zêrô–một $m \times p$, **B** là ma trận zêrô – một $p \times k$ và **C** là ma trận zêrô–một $k \times n$. Chứng minh rằng

$$\mathbf{A} \odot (\mathbf{B} \odot \mathbf{C}) = (\mathbf{A} \odot \mathbf{B}) \odot \mathbf{C}.$$

CÂU HỎI ÔN TẬP

1. a) Định nghĩa thuật ngữ *thuật toán*.

b) Nêu những cách khác nhau mô tả một thuật toán

c) Nêu sự khác nhau giữa một thuật toán để giải một bài toán và một chương trình máy tính để giải bài toán đó.

2. a) Dùng ngôn ngữ thông thường mô tả thuật toán tìm số lớn nhất, số lớn thứ hai và số lớn thứ ba của một bảng liệt kê gồm n số nguyên.

b) Biểu diễn thuật toán đó bằng giả mã.

c) Thuật toán trên dùng bao nhiêu phép so sánh.

3. a) Độ phức tạp thời gian trong trường hợp xấu nhất, trong trường hợp trung bình và trong trường hợp tốt nhất (tính qua các phép so sánh) có ý nghĩa gì đối với thuật toán tìm số nhỏ nhất trong bảng liệt kê gồm n số nguyên.

b) Xác định độ phức tạp thời gian trong trường hợp xấu nhất, trong trường hợp trung bình và trong trường hợp tốt nhất của các phép so sánh của thuật toán tìm số nhỏ nhất trong bảng liệt kê gồm các số nguyên bằng cách so sánh các số nguyên với số nguyên bé nhất đã tìm được đến lúc này?

4. a) Mô tả thuật toán tìm kiếm tuyến tính và thuật toán tìm kiếm nhị phân để tìm một số nguyên trong một bảng liệt kê các số nguyên sắp theo thứ tự tăng dần.

b) So sánh độ phức tạp thời gian trong trường hợp xấu nhất của hai thuật toán đó.

c) Một trong hai thuật toán đó có luôn luôn nhanh hơn thuật toán kia không?

5. Phát biểu Định lý cơ bản của số học.

6. a) Mô tả thủ tục phân tích một số ra thừa số nguyên tố.

b) Dùng thủ tục đó phân tích số 80.707 ra thừa số nguyên tố.

7. a) Định nghĩa ước số chung lớn nhất của hai số nguyên.

b) Mô tả ít nhất ba cách khác nhau để tìm ước số chung lớn nhất của hai số nguyên. Khi nào mỗi phương pháp tỏ ra tốt nhất.

c) Tìm ước số chung lớn nhất của 1.234.567 và 7.654.321.

d) Tìm ước số chung lớn nhất của $2^3 3^5 5^7 7^9 11$ và $2^9 3^7 5^5 7^3 13$.

8. a) Nói a và b đồng dư theo modun 7 có nghĩa là gì?

b) Các cặp nào trong số các số nguyên −11, −8, −7, −1, 0, 3, và 17 là đồng dư theo modun 7?

c) Chứng minh rằng nếu a và b đồng dư theo modun 7 thì $10a + 13$ và $-4b - 20$ cũng đồng dư theo môđun 7.

9. Mô tả thủ tục chuyển khai triển thập phân của một số nguyên sang khai triển thập lục phân của số đó.

10. a) Làm thế nào có thể tìm được một tổ hợp tuyến tính (với hệ số nguyên) của hai số nguyên bằng ước số chung lớn nhất của chúng?

b) Biểu diễn ƯCLN(84, 119) như một tổ hợp tuyến tính của 84 và 119.

11. Định nghĩa tích của hai ma trận **A** và **B**. Khi nào tích này là xác định?

12. a) Có bao nhiêu cách khác nhau để tính tích $\mathbf{A}_1\mathbf{A}_2\mathbf{A}_3\mathbf{A}_4$ bằng cách nhân liên tiếp các cặp ma trận? Khi nào tích này là xác định?

b) Giả sử rằng $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$ và $\mathbf{A}_4$, tương ứng có kích thước là 10×20, 20×5, 5×10 và 10×5. Tích $\mathbf{A}_1\mathbf{A}_2\mathbf{A}_3\mathbf{A}_4$ cần phải tính như thế nào để số phép nhân các phần tử phải dùng là ít nhất.

BÀI TẬP BỔ SUNG

1 a) Mô tả thuật toán xác định vị trí lần gặp cuối cùng của số lớn nhất trong một bảng liệt kê các số nguyên.

b) Đánh giá số các phép so sánh đã được dùng.

2. a) Mô tả thuật toán tìm phần tử lớn thứ nhất và lớn thứ hai trong một bảng liệt kê các số nguyên.

b) Đánh giá số các phép so sánh đã được dùng.

3. a) Cho một thuật toán để xác định một xâu bit có chứa hai số zêrô đứng liền nhau hay không.

b) Thuật toán đó đã dùng bao nhiêu phép so sánh?

4. a) Giả sử một bảng liệt kê các số nguyên được sắp theo thứ tự từ số lớn nhất đến số nhỏ nhất, và một số nguyên có thể xuất hiện lặp lại trong bảng liệt kê đó. Tìm thuật toán xác định vị trí tất cả các lần xuất hiện của số nguyên x nào đó trong bảng liệt kê đó.

b) Đánh giá số phép so sánh đã được sử dụng.

5. Tìm 4 số đồng dư với 5 theo modun 17.

6. Chứng minh rằng nếu a và d là các số dương, thì tồn tại các số nguyên q và r sao cho $a = dq + r$ với $-d/2 \leqslant r \leqslant d/2$.

***7** Chứng minh rằng nếu $ac \equiv bc \pmod m$ thì $a \equiv b \pmod{m/d}$, với $d = \text{ƯCLN}(m, c)$

***8.** Có bao nhiêu số 0 ở cuối khai triển nhị phân của 100_{10} ! ?

9. Dùng thuật toán Euclid, tìm ƯCLN(10.223, 33.341).

10. Để tìm ƯCLN(144, 233) bằng thuật toán Euclid, cần phải làm bao nhiêu phép chia?

11. Tìm ƯCLN$(2n + 1, 3n + 2)$ với n là một số nguyên dương (*Gợi ý* : dùng thuật toán Euclid).

12. a) Chứng tỏ rằng nếu a và b là các số nguyên dương với $a \geqslant b$, thì ƯCLN$(a, b) = a$ nếu $a = b$; ƯCLN$(a, b) = 2\text{ƯCLN}\left(\frac{a}{2}, \frac{b}{2}\right)$ nếu a và b là số chẵn ; ƯCLN$(a, b) = \text{ƯCLN}\left(\frac{a}{2}, b\right)$ nếu a là chẵn b là lẻ ; và ƯCLN$(a, b) = \text{ƯCLN}(a - b, b)$ nếu cả a và b đều lẻ.

b) Giải thích rõ dùng câu (*a*) như thế nào để xây dựng một thuật toán tính ước số chung lớn nhất của hai số nguyên mà chỉ dùng các phép so sánh, các phép trừ và xê dịch các khai triển nhị phân chứ không dùng phép chia.

c) Tìm ƯCLN(1202, 4848) bằng thuật toán đó.

13. Chứng minh rằng một số nguyên chia hết cho 9 nếu và chỉ nếu tổng các chữ số trong biểu diễn thập phân của nó chia hết cho 9.

14. a) Xây dựng một thuật toán tính x^n **mod** m, trong đó x là một số nguyên, m và n là các số nguyên dương, bằng cách dùng khai triển nhị phân của n. (Gợi ý : Thực hiện liên tiếp các phép bình phương để nhận được x **mod** m, x^2 **mod** m, x^4 **mod** m v.v... Sau đó nhân các luỹ thừa thích hợp có dạng x^{2^k} **mod** m để nhận được những x^n **mod** m).

b) Đánh giá số các phép nhân được sử dụng trong thuật toán đó.

Một tập hợp các số nguyên được gọi là **nguyên tố cùng nhau** *nếu ước số chung lớn nhất của các số nguyên đó bằng 1.*

15. Các tập số nguyên sau đây có phải là nguyên tố cùng nhau không

a) 8, 10, 12 b) 12, 15, 25

c) 15, 21, 28 c) 21, 24, 28, 32

16. Tìm một tập hợp gồm bốn số nguyên là tập nguyên tố cùng nhau, sao cho không có hai số nào trong chúng là nguyên tố cùng nhau.

17. a) Giả sử một bức thư được mã hoá bằng cách dùng hàm $f(p) = (ap + b)$ **mod** 26 sao cho ƯCLN(a, 26) = 1. Xác định hàm có thể dùng để giải mã bức thư đó ?

b) Phiên bản mã hóa của một bức thư như sau : LJMKG MGMXF QEXMW. Nếu nó được mã hóa bằng cách dùng hàm $f(p) = (7p + 10)$ **mod** 26, thì bức thư gốc là như thế nào?

18. Chứng minh rằng hệ các phương trình đồng dư : $x \equiv 2 (\text{mod } 6)$ và $x \equiv 3 (\text{mod } 9)$ không có nghiệm.

19. Tìm nghiệm của hệ phương trình đồng dư sau : $x \equiv 4 (\text{mod } 6)$ và $x \equiv 13 (\text{mod } 15)$

***20** a) Chứng minh rằng hệ phương trình đồng dư : $x \equiv a_1 (\text{mod } m_1)$, và $x \equiv a_2 (\text{mod } m_2)$ có nghiệm nếu và chỉ nếu ƯCLN$(m_1, m_2) | a_1 - a_2$.

b) Chứng minh rằng nghiệm của câu a) là duy nhất theo modun BCNN(m_1, m_2).

21. Tìm $\mathbf{A}^n$, nếu $\mathbf{A}$ là $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

22. Chứng minh rằng nếu $\mathbf{A} = c\mathbf{I}$, với c là một số thực và $\mathbf{I}$ là ma trận đơn vị $n \times n$, thì $\mathbf{AB} = \mathbf{BA}$ với $\mathbf{B}$ là ma trận $n \times n$ bất kỳ.

23. Chứng minh rằng nếu $\mathbf{A}$ là ma trận 2×2 sao cho $\mathbf{AB} = \mathbf{BA}$ với $\mathbf{B}$ là ma trận 2×2 bất kỳ thì $\mathbf{A} = c\mathbf{I}$, trong đó c là một số thực và $\mathbf{I}$ là ma trận đơn vị 2×2.

Một ma trận $n \times n$ được gọi là có dạng **tam giác trên** *nếu $a_{ij} = 0$ với mọi $i > j$.*

24. Từ định nghĩa của tích ma trận, hãy lập một thuật toán tính tích của ma trận có dạng tam giác trên, trong đó bỏ qua các tích tự động bằng zêrô.

25. Cho mô tả giả mã của thuật toán ở Bài tập 24.

26. Có bao nhiêu phép nhân các phần tử đã được sử dụng trong thuật toán Bài tập 25.

27. Chứng minh rằng nếu $\mathbf{A}$ và $\mathbf{B}$ là các ma trận khả nghịch và $\mathbf{AB}$ tồn tại, thì $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$.

28. Xác định trình tự tốt nhất để tính tích $\mathbf{ABCD}$, nếu $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ là các ma trận có kích thước tương ứng là : 30×10; 10×40; 40×50 ; và 50×30 ? Giả sử rằng số phép nhân các phần tử được dùng để tích tính của một ma trận $p \times q$ với ma trận $q \times r$ là pqr.

29. Cho $\mathbf{A}$ là ma trận $n \times n$ và $\mathbf{O}$ là ma trận $n \times n$ chỉ gồm các số không. Chứng minh các hệ thức sau :

a) $\mathbf{A} \odot \mathbf{O} = \mathbf{O} \odot \mathbf{A} = \mathbf{O}$

b) $\mathbf{A} \vee \mathbf{O} = \mathbf{O} \vee \mathbf{A} = \mathbf{A}$

c) $\mathbf{A} \wedge \mathbf{O} = \mathbf{O} \wedge \mathbf{A} = \mathbf{O}$

BÀI TẬP LÀM TRÊN MÁY TÍNH

Viết các chương trình với Input và Output sau :

1. Cho bảng liệt kê gồm n số nguyên, tìm số nguyên lớn nhất trong bảng đó.

2. Cho bảng liệt kê gồm n số nguyên, tìm nơi xuất hiện đầu tiên và cuối cùng của số lớn nhất trong bảng đó.

3. Cho một bảng liệt kê gồm n số nguyên phân biệt, dùng thuật toán tìm kiếm tuyến tính, xác định vị trí của một số nguyên trong bảng.

4. Cho một hảng liệt kê sắp thứ tự gồm n số nguyên phân biệt. Dùng thuật toán tìm kiếm nhị phân xác định vị trí của một số nguyên trong bảng đó.

5. Cho một bảng liệt kê sắp thứ tự gồm n số nguyên và một số nguyên x. Xác định số các phép so sánh được dùng để xác định vị trí của số nguyên x trong bảng theo thuật toán tìm kiếm nhị phân.

6. Cho một số nguyên dương. Xác định xem số đó có phải là số nguyên tố không.

7. Cho một bức thư, hãy mã hóa nó theo mật mã Caesar và cho một bức thư đã được mã hóa theo mật mã Caesar, hãy giải mã bức thư đó.

8. Cho hai số nguyên dương. Dùng thuật toán Euclid tìm ước số chung lớn nhất của chúng.

9. Cho hai số nguyên đương, tìm bội số chung nhỏ nhất của chúng.

***10.** Cho một số nguyên dương, phân tích số đó ra thừa số nguyên tố.

11. Cho một số nguyên dương a và một số nguyên đương b lớn hơn 1. Tìm khai triển cơ số b của số nguyên a.

12. Cho một số nguyên đương, tìm khai triển Cantor của số nguyên đó (Xem phần chú thích ở trước Bài tập 24 của Tiết 2.4).

13. Cho một số nguyên dương n, một môđun m, một nhân tử a, một số gia c và hạt giống x_0, với $0 \leqslant a < m$, $0 \leqslant c < m$, hãy tạo dãy n số giả ngẫu nhiên bằng cách dùng "máy phát' đồng dư tuyến tính $x_{n+1} = (ax_n + c) \bmod m$.

14. Cho các số nguyên đương a và b, tìm các số nguyên s và t sao cho $sa + tb = \text{ƯCLN}(a, b)$.

15. Cho ma trận $m \times k$ **A** và ma trận $k \times n$ **B**, tìm **AB**

***16.** Cho ma trận vuông **A** và số nguyên dương n. Tìm $\mathbf{A}^n$.

17. Cho một ma trận vuông, xác định xem ma trận đó có là đối xứng hay không.

18. Cho ma trận $n_1 \times n_2$ **A**, ma trận $n_2 \times n_3$ **B**, ma trận $n_3 \times n_4$ **C**, và ma trận $n_4 \times n_5$ **D** với tất cả các phần tử là số nguyên, tìm trình tự nhân có hiệu quả nhất bốn ma trận trên (qua số các phép nhân và cộng các số nguyên).

19. Cho hai ma trận Boole $m \times n$. Tìm giao và hợp của chúng.

20. Cho ma trận Boole $m \times k$ **A** và ma trận Boole $k \times n$ **B**. Tìm tích Boole của **A** và **B**.

21. Cho ma trận Boole vuông **A** và một số nguyên dương n, tìm $\mathbf{A}^{[n]}$.

TÍNH TOÁN VÀ KHÁM PHÁ

Dùng các chương trình mà bạn đã viết làm các bài tập sau

1. Xác định xem $2^p - 1$ có phải là số nguyên tố không đối với mỗi số nguyên tố p không vượt quá 100.

2. Chứng tỏ rằng $n^2 + n + 41$ là số nguyên tố với mọi số nguyên n sao cho $0 \leq n \leq 39$, nhưng không là số nguyên tố khi $n = 40$. Một đa thức của n với các hệ số nguyên và bậc lớn hơn zêrô có luôn nhận giá trị là số nguyên tố đối với mọi n nguyên đương?

3. Tìm các số nguyên tố có đạng $n^2 + 1$ nhiều nhất có thể được. Người ta vẫn còn chưa biết các số nguyên tố dạng này có nhiều vô hạn hay không.

4. Tìm 10 số nguyên tố khác nhau mỗi số có 100 chữ số.

5. Có bao nhiêu số nguyên tố nhỏ hơn 1.000.000, nhỏ hơn 10.000.000 và nhỏ hơn 100.000.000? Bạn có thể đưa ra một ước lượng về số các số nguyên tố nhỏ hơn một số nguyên đương x nào đó không?

6. Tìm một thừa số nguyên tố của 10 số lẻ, mỗi số gồm 20 chữ số khác nhau được chọn một cách ngẫu nhiên. Đối với mỗi một số, việc tìm đó mất bao lâu? Cũng hỏi như trên đối với 10 số lẻ, mỗi số có 30 chữ số? 10 số lẻ, mỗi số có 40 chữ số, v.v..., bạn cứ tiếp tục chừng nào còn có thể.

7. Tìm tất cả các số giả nguyên tố, tức là các hợp số n sao cho $2^{n-1} \equiv 1 \pmod{n}$, với n không vượt quá 10.000.

VIẾT TIỂU LUẬN

Dùng các tư liệu ở ngoài cuốn sách này viết các tiểu luận trả lời những câu hỏi sau :

1. Khảo sát lịch sử của từ thuật toán (algorithm) và mô tả cách dùng từ này trong các văn bản đầu tiên.

2. Mô tả thuật ngữ "thuật toán song song ". có nghĩa là gì? Giải thích xem giả mã được dùng trong cuốn sách này làm thế nào có thể mở rộng để dùng cho cả các thuật toán song song.

3. Giải thích xem độ phức tạp của các thuật toán song song có thể đo như thế nào? Cho một số ví dụ để minh họa khái niệm này và chứng tỏ một thuật toán song song có thể làm việc nhanh hơn một thuật toán không hoạt động song song như thế nào?

4. Các số nguyên tố nhỏ hơn một lũy thừa nguyên của 2 một đơn vị được gọi là các số nguyên tố Mersenne. Hiện nay người ta đã biết bao nhiêu số nguyên tố Mersenne? Mỗi số trong 10 số Mersenne lớn nhất được tìm ra khi nào, do ai tìm ra và dùng loại máy tính nào? Số nguyên tố lớn nhất được biết hiện nay có phải là số Mersenne không?

5. Hãy giải thích những trắc nghiệm tính nguyên tố theo kiểu xác suất đã được sử dụng như thế nào trên thực tế để tạo các số cực lớn mà hầu chắc chắn là số nguyên tố. Các trắc nghiệm như vậy liệu có những mặt hạn chế tiềm tàng nào không?

6. *Số Carmichael* là một số nguyên, nó cũng là một số giả nguyên tố đối với tất cả các cơ số nguyên tố cùng nhau với số nguyên đó. Vấn đề có tồn tại một số vô hạn các số Carmichael đã được giải quyết mới đây sau hơn 75 năm để ngỏ. Hãy giải thích rõ số Carmichael là gì? Cho những ví dụ về các số đó, và mô tả các điểm mấu chốt trong chứng minh có tồn tại vô số các số đó.

7. Tổng kết tình trạng hiện nay của các thuật toán phân tích thừa số qua độ phức tạp của chúng, kích thước của các số hiện nay có thể phân tích được. Theo bạn thì khi nào có thể phân tích được các số có 200 chữ số?

8. Mô tả các thuật toán hiện đang được dùng trong các máy tính hiện đại để cộng, trừ, nhân và chia các số nguyên dương.

9. Mô tả lịch sử của Định lý số dư Trung hoa. Mô tả một số bài toán liên quan đã được đặt ra trong các văn bản bằng tiếng Trung hoa và Hindu và định lý số dư Trung hoa áp dụng như thế nào cho các bài toán đó?

10. Khi nào các số trong một dãy mới thực sự là các số ngẫu nhiên chứ không phải giả ngẫu nhiên? Những hạn chế nào sẽ được bộc lộ trong các mô phỏng và thực nghiệm dùng các số giả ngẫu nhiên? Các số giả ngẫu nhiên có thể có những tính chất gì mà các số ngẫu nhiên không có.

11. Chứng tỏ phép đồng dư có thể được dùng để nói được ngày trong tuần ở bất kỳ ngày nào đã cho.

13. Mô tả một số thuật toán được dùng để nhân các số nguyên lớn một cách có hiệu quả.

14. Mô tả một số thuật toán được dùng để nhân các ma trận lớn một cách có hiệu quả ?

CHƯƠNG 3

SUY LUẬN TOÁN HỌC

Để hiểu các tác phẩm toán học, chúng ta cần phải biết cái gì tạo nên những lập luận toán học đúng đắn, các chứng minh. Học toán mỗi người cần hình thành những tư duy toán học chứ không phải đọc một bài bình luận. Rõ ràng, điều đó đòi hỏi phải hiểu các kỹ thuật thường dùng để xây dựng các chứng minh. Mục đích của chương này là cung cấp cho bạn những cái tạo nên các suy luận toán học đúng đắn và những công cụ cần thiết để xây dựng các suy luận đó.

Nhiều mệnh đề toán học khẳng định một tính chất nào đó là đúng cho tất cả các số nguyên dương. Ví dụ, với mọi số nguyên dương n ta có : $n! < n^n$, $n^3 - n$ chia hết cho 3, tổng n số nguyên dương đầu tiên bằng $n(n + 1)/2$. Mục đích chính của chương này cũng như của cuốn sách này là làm cho các bạn sinh viên hiểu sâu sắc phương pháp quy nạp toán học. Chính nhờ phương pháp này mà ta có thể chứng minh được rất nhiều kết quả loại như vừa kể trên.

Trong các chương trước ta đã định nghĩa dưới dạng tường minh các tập hợp, các dãy, các hàm. Tức là chúng ta mô tả tập hợp bằng cách liệt kê các phần tử của nó, hoặc là cho một số tính chất đặc trưng của các phần tử này.

Chúng ta cho các công thức biểu diễn các số hạng của một dãy hay các giá trị của một hàm. Có một cách rất quan trọng khác để định nghĩa các đối tượng này là dựa trên quy nạp toán học. Để định nghĩa các dãy hay các hàm người ta định rõ giá trị của một vài số hạng đầu tiên, sau đó đưa ra quy tắc tìm các giá trị của các số hạng sau qua các giá trị đã biết đó. Ví dụ, có thể xác định được dãy số $\{2^n\}$ bằng cách cho $a_1 = 2$ và $a_{n+1} = 2a_n$ với $n = 1, 2, 3 \ldots$ Cũng có thể xác định một tập hợp bằng cách liệt kê một vài phần tử của nó, và cho các quy tắc

xây dựng các phần tử khác từ những phần tử đã biết của tập hợp. Các định nghĩa như vậy được gọi là các *định nghĩa bằng đệ quy*, chúng rất hay được sử dụng trong toán học rời rạc và trong tin học.

Khi một thủ tục được xây dựng để giải một bài toán nào đó, thông thường nó giải đúng bài toán này. Chính việc thử để thấy với các dữ liệu vào đúng thủ tục cho ta các kết quả đúng cũng không khẳng định được thủ tục này *luôn luôn* đúng. Tính đúng đắn của một thủ tục chỉ có thể đảm bảo bằng cách chứng minh rằng nó luôn tạo ra các kết quả đúng. Mục cuối của chương này trình bày sơ lược về các kỹ thuật kiểm chứng chương trình. Đó là kỹ thuật hình thức để kiểm tra tính đúng đắn của các thủ tục. Việc kiểm chứng chương trình là cơ sở để tiến tới chứng minh sự đúng đắn của các chương trình bằng máy.

3.1. CÁC PHƯƠNG PHÁP CHỨNG MINH

MỞ ĐẦU

Hai vấn đề quan trọng xuất hiện trong toán học là : (1) Khi nào một suy luận toán học là đúng? (2) Có thể dùng các phương pháp nào để xây dựng các suy luận toán học? Trong mục này chúng ta sẽ trả lời các câu hỏi này bằng cách mô tả những dạng khác nhau của suy luận toán học đúng và không đúng.

Định lý là một phát biểu có thể chỉ ra được là đúng. Chúng ta thể hiện một định lý là đúng bằng một dãy các mệnh đề tạo thành một suy luận, mà ta gọi là **sự chứng minh**. Để xây dựng các chứng minh cần có các phương pháp rút ra những mệnh đề mới từ những mệnh đề cũ. Những mệnh đề dùng khi chứng minh có thể bao gồm các **tiên đề** hoặc **định đề** (những giả thiết cơ sở của các cấu trúc toán học), những giả thiết của định lý cần chứng minh, và những định lý đã được chứng minh từ trước. Các **quy tắc suy luận** đó là các cách rút ra các kết luận từ những điều khẳng định khác, chúng liên kết các bước của một chứng minh lại với nhau.

Trong tiết này chúng ta sẽ mô tả các quy tắc suy luận. Điều này sẽ làm sáng tỏ cái gì tạo thành một chứng minh đúng đắn. Một số dạng suy luận sai thường gặp được gọi là các nguỵ hiện, cũng sẽ được bàn đến. Sau đó, chúng ta sẽ đề cập tới những phương pháp chứng minh định lý thường gặp.

Chú ý: Các thuật ngữ *bổ đề* hay *hệ quả* được dùng để hiểu thị một dạng nào đó của định lý. **Bổ đề** là một định lý đơn giản được dùng trong chứng minh một định lý khác. Những chứng minh phức tạp thường dễ hiểu hơn khi sử dụng một số các bổ đề đã được chứng minh từ trước. Còn hệ quả là các mệnh đề được suy ra từ một định lý đã được chứng minh.

Các phương pháp chứng minh là rất quan trọng không chỉ bởi vì chúng thường xuyên được dùng để chứng minh các định lý toán học mà còn vì chúng được áp dụng nhiều trong tin học. Chẳng hạn, đó là sự kiểm tra tính đúng đắn của một chương trình trên máy hay việc khẳng định sự an toàn của một hệ điều hành, xây dựng các luật suy diễn trong lĩnh vực trí tuệ nhân tạo v.v.

Do vậy, nắm vững các kỹ thuật chứng minh là vô cùng cốt yếu trong cả toán học và tin học.

CÁC QUY TẮC SUY LUẬN

Hằng đúng $(p \wedge (p \rightarrow q)) \rightarrow q$ là cơ sở của quy tắc suy luận có tên là **Modus ponens** hay **luật tách rời.** Hằng đúng này được viết như sau :

$$\begin{array}{l} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$$

Khi dùng ký hiệu này, các giả thiết được viết trên các hàng còn kết luận viết ở hàng dưới dấu gạch ngang. (Ký hiệu $\therefore$ có nghĩa là "vậy thì"). Luật tách rời phát biểu rằng nếu cả mệnh đề kéo theo và các giả thiết của nó là đúng thì kết luận của mệnh đề này là đúng.

Ví dụ 1. Giả sử mệnh đề kéo theo "nếu hôm nay tuyết rơi, thì chúng ta sẽ đi trượt tuyết" và giả thiết của nó " hôm nay tuyết rơi " là đúng. Khi đó, theo luật tách rời, "chúng ta sẽ đi trượt tuyết" là đúng.

■

Ví dụ 2. Mệnh đề kéo theo "nếu n chia hết cho 3, khi đó n^2 chia hết cho 9" là đúng. Do vậy, nếu n chia hết cho 3, thì theo luật tách rời ta suy ra n^2 chia hết cho 9.

■

Bảng 1 liệt kê một số quy tắc suy diễn quan trọng. Việc kiểm nghiệm chúng có thể tìm thấy trong một số bài tập ở Tiết 1.2. Ở đây chúng ta sẽ đưa ra một số chứng minh có dùng các quy tắc suy diễn này.

BẢNG 1. Các quy tắc suy luận

Quy tắc suy luận	Hằng đúng	Tên gọi
$\dfrac{p}{\therefore p \vee q}$	$p \to (p \vee q)$	Luật cộng
$\dfrac{p \wedge q}{\therefore p}$	$(p \wedge q) \to p$	Luật rút gọn
$\dfrac{\begin{array}{l}p \\ p \to q\end{array}}{\therefore q}$	$[(p \wedge (p \to q)] \to q$	Modus ponens
$\dfrac{\begin{array}{l}\neg q \\ p \to q\end{array}}{\therefore \neg p}$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens
$\dfrac{\begin{array}{l}p \to q \\ q \to r\end{array}}{\therefore p \to r}$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Tam đoạn luận giả định
$\dfrac{\begin{array}{l}p \vee q \\ \neg p\end{array}}{\therefore q}$	$[(p \vee q) \wedge \neg p] \to q$	Tam đoạn luận tuyển

Ví dụ 3. Quy tắc suy luận nào là cơ sở của suy diễn sau : "Bây giờ trời quá băng giá. Vậy thì bây giờ hoặc là trời quá băng giá hoặc trời đang mưa"?

Giải : Giả sử p là mệnh đề "Bây giờ trời quá băng giá" và q là mệnh đề "hây giờ trời đang mưa". Khi đó suy diễn trên có dạng

$$\frac{p}{\therefore p \vee q}$$

tức là đã sử dụng quy tắc cộng.

■

Ví dụ 4. Quy tắc suy luận nào là cơ sở của suy diễn sau : "Bây giờ trời quá băng giá và đang mưa. Vậy thì bây giờ trời quá băng giá"?

Giải : Giả sử p là mệnh đề "Bây giờ trời quá băng giá" và q là mệnh đề "bây giờ trời đang mưa". Khi đó suy diễn trên có dạng

$$\frac{p \wedge q}{\therefore p}$$

vậy là ta đã sử dụng quy tắc rút gọn.

■

Ví dụ 5. Quy tắc suy luận nào là cơ sở của suy diễn sau.

"Nếu hôm nay trời mưa thì hôm nay chúng ta sẽ không đi chơi ngoài trời. Nếu hôm nay chúng ta không đi chơi ngoài trời thì ngày mai chúng ta sẽ đi chơi ngoài trời. Vậy thì, nếu hôm nay trời mưa thì ngày mai chúng ta sẽ đi chơi ngoài trời".

Giải : Giả sử p là mệnh đề "hôm nay trời mưa", và q là mệnh đề "hôm nay chúng ta sẽ không đi chơi ngoài trời", còn r là mệnh đề "ngày mai chúng ta sẽ đi chơi ngoài trời". Khi đó suy diễn trên có dạng quy tắc tam đoạn luận giả định :

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

■

Những suy luận có dùng các quy tắc suy diễn gọi là *suy luận có cơ sở*. Khi tất cả các luận đề dùng trong một suy luận có cơ sở là đúng thì sẽ dẫn tới một kết luận đúng. Tuy nhiên, một suy luận có cơ sở có thể dẫn đến một kết luận sai nếu một trong các mệnh đề dùng trong suy diễn là sai. Ví dụ :

"Nếu 101 chia hết cho 3 thì 101^2 chia hết cho 9. 101 chia hết cho 3, vậy thì 101^2 chia hết cho 9".

Cách chứng minh trên là có cơ sở vì đã dùng luật tách rời. Tuy vậy, kết luận của suy diễn này là sai vì $101^2 = 10\ 201$ không chia hết cho 9. Sở dĩ ta có kết luận sai vì đã sử dụng mệnh đề sai "101 chia hết cho 3".

NGỤY BIỆN

Có một số ngụy biện rất hay gặp trong các chứng minh sai. Chúng giống như các quy tắc suy luận nhưng không dựa trên các hằng đúng mà chỉ

là các tiếp liên. Bây giờ chúng ta sẽ chỉ ra sự khác nhau giữa suy luận đúng và suy luận sai.

Mệnh đề $[(p \rightarrow q) \wedge q] \rightarrow p$ không là hằng đúng vì nó sai khi p sai và q đúng. Tuy nhiên có nhiều chứng minh sai đã xem nó như hằng đúng. Loại suy luận sai điển hình này gọi là **ngộ nhận kết luận.**

Ví dụ 6. Suy diễn dưới đây có cơ sở hay không?

Nếu bạn giải mọi bài tập trong cuốn sách này, khi đó bạn sẽ nắm vững toán học rời rạc. Bạn đã nắm vững toán học rời rạc.

Vậy thì bạn đã giải mọi bài tập trong cuốn sách này

Giải : Giả sử p là mệnh đề "bạn đã giải mọi bài tập trong cuốn sách này", còn q là mệnh đề "bạn đã nắm vững toán học rời rạc". Khi đó cách suy diễn trên có dạng : *nếu* $p \rightarrow q$ *và* q *thì có* p. Đó là ví dụ về cách suy luận sai vì dùng nguỵ lý ngộ nhận kết luận. Thật vậy, hoàn toàn có thể là bạn học toán rời rạc bằng nhiều cách khác mà không nhất thiết phải làm đầy đủ các bài tập của cuốn sách này (tự đọc sách, nghe các bài giảng, làm một số mà không phải là tất cả các bài tập của cuốn sách này, v.v.).

■

Ví dụ 7. Giả sử p là mệnh đề "$n \equiv 1 \pmod 3$", và q là mệnh đề "$n^2 \equiv 1 \pmod 3$". Mệnh đề kéo theo "nếu $n \equiv 1 \pmod 3$, thì $n^2 \equiv 1 \pmod 3$" có dạng $p \rightarrow q$ là đúng. Nếu q là đúng tức là $n^2 \equiv 1 \pmod 3$, thì có thể suy ra p là đúng, tức là $n \equiv 1 \pmod 3$ không ?

Giải: Không thể kết luận p đúng được bởi vì có thể $n \equiv 2 \pmod 3$. Chứng minh sai vì dùng nguỵ lý ngộ nhận kết luận.

■

Mệnh đề $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ không phải là hằng đúng, vì nó sai khi p sai và q đúng. Nhiều chứng minh sai vì đã sử dụng mệnh đề này như một luật suy diễn. Suy luận phi lý kiểu này gọi là **nguỵ biện phủ nhận giả thiết.**

Ví dụ 8. Cho p và q như trong Ví dụ 6. Nếu mệnh đề kéo theo $p \rightarrow q$ là đúng và nếu $\neg p$ là đúng có thể kết luận $\neg q$ là đúng không? Nói cách khác có thể khẳng định rằng bạn không nắm vững môn toán rời rạc nếu bạn không làm mọi bài tập trong cuốn sách này, cho dù thừa nhận nếu

bạn làm tất cả các bài tập trong cuốn sách này thì bạn sẽ nắm vững toán rời rạc ?

Giải: Điều khẳng định đó là sai vì bạn có thể nắm vững môn toán rời rạc ngay cả khi bạn không làm mọi bài tập trong cuốn sách này.

Cách suy diễn sai này có dạng $p \rightarrow q$ và $\neg p$ kéo theo $\neg q$. Đó là một ví dụ về nguỵ hiện phủ nhận giả thiết.

■

Ví dụ 9. Giả sử p và q như trong Ví dụ 7. Có thể cho rằng nếu $\neg p$ là đúng khi đó $\neg q$ là đúng vì $p \rightarrow q$ là đúng không? Nói cách khác, có thể kết luận $n^2 \not\equiv 1 \pmod 3$ nếu $n \not\equiv 1 \pmod 3$, vì "nếu $n \equiv 1 \pmod 3$" kéo theo $n^2 \equiv 1 \pmod 3$" không ?

Giải: Không thể kết luận $n^2 \not\equiv 1 \pmod 3$ nếu $n \not\equiv 1 \pmod 3$, vì $n^2 \equiv 1 \pmod 3$ khi $n \equiv 2 \pmod 3$. Đây là một ví dụ nữa về nguỵ biện phủ định giả thiết.

■

Nhiều chứng minh sai vì đã dựa trên nguỵ biện **dùng ngay câu hỏi** (begging the question). Nguỵ biện này xuất hiện khi một hay nhiều bước chứng minh dựa trên sự đúng đắn của một mệnh đề đang cần phải chứng minh. Nói cách khác nguỵ biện này xuất hiện khi chứng minh một mệnh đề lại sử dụng chính nó, hoặc là một mệnh đề tương đương với nó. Vì vậy nguỵ biện này cũng được gọi là lý luận quẩn.

Ví dụ 10. Suy luận sau đây có đúng không?

Nếu n^2 là một số chẵn thì n cũng là một số chẵn. Thật vậy, vì n^2 là chẵn nên $n^2 = 2k$ với k là một số nguyên nào đó. Giả sử $k = 2l$ với l là một số nguyên nào đó. Điều này chứng tỏ n là số chẵn.

Giải: Suy luận trên là sai. Phát hiểu "giả sử $k = 2l$ với l là một số nguyên nào đó" xuất hiện trong chứng minh mà không đưa ra lý lẽ nào chứng tỏ nó là đúng. Đây là lý luận quẩn vì phát biểu này cũng tương đương với mệnh đề đang phải chứng minh, tức là n chẵn. Ở đây kết quả hiển nhiên là đúng (n chẵn), chỉ có cách chứng minh là sai.

■

CÁC PHƯƠNG PHÁP CHỨNG MINH ĐỊNH LÝ

Chúng ta đã chứng minh một số định lý trong chương 1 và 2. Bây giờ chúng ta hiểu rõ hơn về phương pháp luận xây dựng các chứng minh.

Dưới đây chúng ta sẽ mô tả cách chứng minh các kiểu mệnh đề.

Bởi vì rất nhiều định lý là các mệnh đề kéo theo, nên các kỹ thuật chứng minh kéo theo là rất quan trọng. Nhớ lại rằng $p \rightarrow q$ là đúng trừ khi p đúng nhưng q sai. Và lưu ý là, để chứng minh mệnh đề $p \rightarrow q$ chỉ cần chỉ ra q là đúng nếu p đúng chứ *ít khi* phải chứng minh q là đúng. Sau đây ta sẽ bàn tới những kỹ thuật chứng minh phép kéo theo.

Giả sử rằng giả thiết p của phép kéo theo $p \rightarrow q$ là sai. Khi đó phép kéo theo là đúng vì mệnh đề có hai dạng $\mathbf{F} \rightarrow \mathbf{T}$ và $\mathbf{F} \rightarrow \mathbf{F}$ và tức là mệnh đề đúng. Do vậy, nếu có thể chỉ ra p là sai khi đó phép kéo theo $p \rightarrow q$ được chứng minh. Một chứng minh như vậy gọi là **chứng minh rỗng**. Chứng minh rỗng thường được dùng để thiết lập các trường hợp đặc biệt của các định lý phát biểu rằng phép kéo theo là đúng cho tất cả các số nguyên dương (tức là các định lý dạng $\forall n\ P(n)$ trong đó $P(n)$ là một hàm mệnh đề). Kỹ thuật chứng minh các định lý kiểu này sẽ được thảo luận trong Tiết 3.2.

Ví dụ 11. Chỉ ra rằng mệnh đề $P(0)$ là đúng trong đó $P(n)$ là hàm mệnh đề "Nếu $n > 1$ thì $n^2 > n$".

Giải: Dễ thấy $P(0)$ là mệnh đề kéo theo "Nếu $0 > 1$ thì $0^2 > 0$". Vì giả thiết $0 > 1$ sai, nên mệnh đề kéo theo $P(0)$ tự động đúng. ■

Chú ý. Kết luận của phép kéo theo $0^2 > 0$ là sai. Nhưng không vì thế mà mệnh đề $P(0)$ là sai, vì theo định nghĩa, mệnh đề kéo theo mặc nhiên được coi là đúng nếu giả thiết của nó là sai.

Giả sử rằng kết luận q của phép kéo theo $p \rightarrow q$ là đúng. Khi đó $p \rightarrow q$ là đúng vì nó có dạng $\mathbf{T} \rightarrow \mathbf{T}$ hoặc $\mathbf{F} \rightarrow \mathbf{T}$ đều là đúng cả. Do vậy nếu có thể chỉ ra được q là đúng thì mệnh đề $p \rightarrow q$ được chứng minh. Đó là cách **chứng minh tầm thường**. Những chứng minh tầm thường lại rất quan trọng khi cần chứng minh các trường hợp đặc biệt của các định lý (xem phần cách chứng minh từng trường hợp) và trong quy nạp toán học, một kỹ thuật chứng minh được đề cập trong Tiết 3.2.

Ví dụ 12. Gọi $P(n)$ là mệnh đề "Nếu a và b là hai số nguyên dương và $a \geq b$, thì $a^n \geq b^n$ ". Hãy chỉ ra rằng $P(0)$ là đúng.

Giải: Mệnh đề $P(0)$ là "nếu $a \geq b$, thì $a^0 \geq b^0$ "Vì $a^0 = b^0 = 1$ nên kết luận của $P(0)$ là đúng. Do đó, $P(0)$ là đúng. Đây là ví dụ về một

chứng minh tầm thường. Lưu ý giả thiết của mệnh đề "$a \geq b$" là không cần cho chứng minh này.

■

Mệnh đề kéo theo $p \rightarrow q$ có thể được chứng minh bằng cách chỉ ra rằng nếu p đúng thì q cũng phải đúng. Điều đó chứng tỏ tổ hợp p đúng và q sai không bao giờ xảy ra. Chứng minh kiểu này gọi là **chứng minh trực tiếp**.

Để thực hiện một chứng minh như thế ta giả sử p là đúng rồi sử dụng các quy tắc suy luận và các định lý đã được chứng minh để chỉ ra q cũng phải đúng.

Ví dụ 13. Hãy chứng minh trực tiếp định lý "Nếu n là số lẻ thì n^2 cũng lẻ".

Giải: Giả sử rằng giả thiết của mệnh đề kéo theo này là đúng, tức là n là một số lẻ. Khi đó $n = 2k + 1$, với k là một số nguyên. Từ đó suy ra $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Do đó n^2 là một số lẻ.

■

Vì mệnh đề kéo theo $p \rightarrow q$ tương đương với mệnh đề phản đảo của nó $\neg q \rightarrow \neg p$, nên phép kéo theo $p \rightarrow q$ sẽ được chứng minh bằng cách chỉ ra rằng $\neg q \rightarrow \neg p$ là đúng. Mệnh đề kéo theo này thường được chứng minh trực tiếp nhưng cũng có thể sử dụng hất kỳ kỹ thuật chứng minh nào. Chứng minh kiểu này gọi là **chứng minh gián tiếp**.

Ví dụ 14. Hãy chứng minh gián tiếp định lý "Nếu $3n + 2$ là một số lẻ thì n cũng lẻ".

Giải: Giả sử ngược lại kết luận của phép kéo theo là sai, tức là n chẵn. Khi đó $n = 2k$ với k là số nguyên nào đó. Từ đó suy ra rằng $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$ nên $3n + 2$ là một số chẵn. Vì phủ định kết luận của phép kéo theo dẫn đến giả thiết của nó sai, nên mệnh đề kéo theo ban đầu là đúng.

■

Giả sử có thể tìm được mâu thuẫn q sao cho $\neg p \rightarrow q$ là đúng, tức là $\neg p \rightarrow \mathbf{F}$ là đúng. Khi đó mệnh đề $\neg p$ phải là sai. Do đó p là đúng. Kỹ thuật chứng minh kiểu này được dùng khi có thể tìm được mâu thuẫn dạng $r \wedge \neg r$, tức là ra mệnh đề kéo theo $\neg p \rightarrow (r \wedge \neg r)$ là đúng. Đó là cách **chứng minh bằng phản chứng.**

Ví dụ 15. Chứng minh rằng $\sqrt{2}$ là số vô tỷ.

Giải: Gọi p là mệnh đề "$\sqrt{2}$ là số vô tỷ". Giả sử ngược lại $\neg p$ là đúng, khi đó $\sqrt{2}$ là số hữu tỷ. Ta sẽ chỉ ra điều này dẫn tới mâu thuẫn. Vì $\sqrt{2}$ là số hữu tỷ nên tồn tại a và b nguyên sao cho $\sqrt{2} = a/b$, trong đó a, b không có ước chung (phân số a/b là tối giản). Bình phương hai vế đẳng thức này ta được :

$$2 = \frac{a^2}{b^2} \text{ . Vì thế } 2b^2 = a^2.$$

Điều này có nghĩa a^2 là số chẵn và do vậy cả a cũng là số chẵn. Đặt $a = 2c$ với c là số nguyên nào đó. Do đó $2b^2 = 4c^2$ hay $b^2 = 2c^2$. Vậy b^2 và b là các số chẵn.

Ta đã chứng tỏ là $\neg p$ kéo theo $\sqrt{2} = a/b$, trong đó a, b là các số nguyên không có ước chung và đều chia hết cho 2. Điều này mâu thuẫn vì chúng ta đã chỉ ra rằng $\neg p$ kéo theo cả r và $\neg r$ với r là mệnh đề "a và b là các số nguyên không có ước chung". Vì thế, $\neg p$ là sai, hay p : "$\sqrt{2}$ là số vô tỷ" là đúng.

■

Chứng minh gián tiếp mệnh đề kéo theo có thể làm như chứng minh bằng phản chứng. Trong chứng minh gián tiếp ta chỉ ra $p \rightarrow q$ là đúng bằng cách chứng minh trực tiếp $\neg q \rightarrow \neg p$ là đúng. Để viết lại chứng minh gián tiếp như chứng minh bằng phản chứng, ta giả sử p và $\neg q$ là đúng. Khi đó ta chứng minh trực tiếp $\neg q \rightarrow \neg p$ là đúng, do vậy $\neg p$ là đúng. Tức là dẫn tới mâu thuẫn $p \wedge \neg p$. Ví dụ 16 sẽ minh họa những điều vừa nói ở trên.

Ví dụ 16. Hãy chứng minh bằng phản chứng định lý "Nếu $3n + 2$ là lẻ thì n lẻ".

Giải: Ta giả sử $3n + 2$ là lẻ và n không lẻ, tức là n chẵn. Tiến hành từng bước như trong bài giải của Ví dụ 14, ta có thể chỉ ra nếu n chẵn thì $3n + 2$ cũng chẵn. Điều này mâu thuẫn với giả thiết $3n + 2$ là lẻ. Định lý được chứng minh.

Để chứng minh mệnh đề có dạng $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$ người ta dùng hằng đúng.

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

như một quy tắc suy luận. Điều này chứng tỏ rằng mệnh đề kéo theo ban đầu có giả thiết là tuyển của các mệnh đề p_1, p_2 ..., p_n có thể được

chứng minh bằng cách chứng minh mỗi một trong n mệnh đề kéo theo $p_i \to q$ với $i = 1, 2, ..., n$ một cách riêng rẽ. Cách chứng minh như trên gọi là **chứng minh từng trường hợp**. Đôi khi để chứng minh $p \to q$ là đúng, thay cho p ta dùng mệnh đề tuyển $(p_1 \vee p_2 \vee ... \vee p_n)$ tương đương với p lại thuận tiện hơn. Xét ví dụ sau.

Ví dụ 17. Hãy chứng minh mệnh đề "Nếu số nguyên n không chia hết cho 3 thì $n^2 \equiv 1 \pmod 3$".

Giải: Gọi p là mệnh đề "n không chia hết cho 3" và q là "$n^2 \equiv 1 \pmod 3$". Khi đó p tương với $p_1 \vee p_2$ trong đó p_1 là "$n \equiv 1 \pmod 3$" và p_2 là "$n \equiv 2 \pmod 3$". Từ đó, để chứng tỏ $(p \to q)$ ta sẽ chứng minh $(p_1 \to q)$ và $(p_2 \to q)$. Dễ dàng chứng minh hai mệnh đề kéo theo sau này.

Đầu tiên, giả sử p_1 là đúng, tức là $n = 3k + 1$ với k là một số nguyên nào đó.. Do đó

$$n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1,$$

tức là $n^2 \equiv 1 \pmod 3$ hay $(p_1 \to q)$ là đúng.

Tiếp theo giả sử p_2 là đúng, tức là $n = 3k + 2$ với k là một số nguyên nào đó. Do đó

$$n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$$

tức là $n^2 \equiv 1 \pmod 3$ hay $(p_2 \to q)$ là đúng.

Vì cả hai $(p_1 \to q)$ và $(p_2 \to q)$ là đúng nên ta kết luận $(p_1 \vee p_2) \to q$ là đúng. Hơn thế nữa, vì p tương đương với $p_1 \vee p_2$ nên suy ra mệnh đề $p \to q$ là đúng. ■

Để chứng minh một định lý có dạng quan hệ tương đương, tức là nó có dạng $(p \leftrightarrow q)$, trong đó p và q là hai mệnh đề, ta sử dụng hằng đúng

$$(p \leftrightarrow q) \leftrightarrow [(p \to q) \wedge (q \to p)].$$

Tức là mệnh đề "p nếu và chỉ nếu q" là đúng nếu cả hai mệnh đề kéo theo "nếu p thì q" và "nếu q thì p" được chứng minh.

Ví dụ 18. Hãy chứng minh định lý "n là số lẻ nếu và chỉ nếu n^2 là lẻ".

Giải: Định lý này có dạng "p nếu và chỉ nếu q", trong đó p là "n là số lẻ", còn q là "n^2 là số lẻ". Để chứng minh định lý này, ta cần chỉ ra $p \to q$ và $q \to p$ là đúng.

Chúng ta đã biết (Ví dụ 13) $p \rightarrow q$ là đúng. Ta sẽ chứng minh gián tiếp rằng $q \rightarrow p$. Giả sử kết luận là sai, tức là n là chẵn. Đặt $n = 2k$, với k là một số nguyên nào đó. Khi đó $n^2 = 4\ k^2 = 2(2k^2)$, tức n^2 là chẵn. Mâu thuẫn với giả thiết n^2 là lẻ. Do vậy ta đã chứng minh được $q \rightarrow p$ là đúng.

Vì cả hai $(p \rightarrow q)$ và $(q \rightarrow p)$ đã được chứng minh là đúng, nên mệnh đề tương đương với chúng $(p \leftrightarrow q)$ là đúng. ■

Đôi khi một định lý biểu đạt nhiều mệnh đề là tương đương. Định lý này được viết như sau :

$$p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n,$$

hay các mệnh đề p_1, p_2 ..., p_n có cùng giá trị chân lý. Một cách chứng minh các mệnh đề này tương đương lẫn nhau là dùng hằng đúng :

$$[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots \wedge (p_n \rightarrow p_1)].$$

Điều này chứng tỏ rằng nếu các mệnh đề kéo theo $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, ..., $p_n \rightarrow p_1$ có thể chỉ ra được là đúng, thì các mệnh đề p_1, p_2, ..., p_n là tương đương.

Ví dụ 19. Hãy chứng minh rằng nếu n là một số nguyên, thì ba mệnh đề sau là tương đương.

p_1 : n **mod** 3 = 1 hoặc n **mod** 3 = 2,

p_2 : n không chia hết cho 3.

p_3 : $n^2 \equiv 1 \pmod 3$

Giải: Để chứng minh ba mệnh đề này tương đương chúng ta phải chứng minh các mệnh đề kéo theo $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$ và $p_3 \rightarrow p_1$ là đúng.

Ta sẽ chứng minh trực tiếp $p_1 \rightarrow p_2$ là đúng. Giả sử n **mod** 3 = 1 hoặc 2, tức là n chia cho 3 dư 1 hoặc dư 2. Nói cách khác n không chia hết cho 3. Vậy $p_1 \rightarrow p_2$ là đúng.

Chúng ta đã chỉ ra $p_2 \rightarrow p_3$ là đúng trong Ví dụ 17.

Chúng ta sẽ chứng minh gián tiếp $p_3 \rightarrow p_1$ là đúng. Giả sử kết luận là sai, tức là n **mod** 3 không bằng 1 hoặc 2, vậy n **mod** 3 = 0. Điều này có nghĩa là n chia hết cho 3 hay $n = 3k$ với k là một số nguyên nào

đó. Từ đó suy ra $n^2 = 9k^2 = 3(3k^2)$ hay $n^2 \equiv 0 \pmod 3$. Do vậy p_3 là sai. hay mệnh đề $p_3 \rightarrow p_1$ là đúng. Bài toán đã được chứng minh.

■

ĐỊNH LÝ VÀ LƯỢNG TỪ

Nhiều định lý được phát biểu như là các mệnh đề có chứa lượng từ. Người ta dùng nhiều cách khác nhau để chứng minh các định lý có dạng các lượng từ như thế. Chúng ta sẽ mô tả một vài loại quan trọng nhất.

Nhiều định lý là các khẳng định sự tồn tại của các đối tượng thuộc một loại nào đó. Một định lý loại này là mệnh đề có dạng $\exists x P(x)$ với P là vị ngữ. Chứng minh mệnh đề dạng $\exists x P(x)$ gọi là **chứng minh tồn tại**. Có một vài cách chứng minh định lý loại này. Đôi khi một chứng minh tồn tại của mệnh đề $\exists x P(x)$ được hoàn tất bằng cách tìm được một phần tử a sao cho $P(a)$ đúng. Cách chứng minh tồn tại như vậy gọi là chứng minh **kiến thiết**. Có cách chứng minh khác gọi là chứng minh tồn tại không kiến thiết, tức là chúng ta không tìm phần tử a sao cho $P(a)$ đúng mà chứng minh rằng $\exists x P(x)$ là đúng bằng một cách khác. Một phương pháp thông thường để xây dựng một chứng minh tồn tại không kiến thiết là chứng minh bằng phản chứng và chỉ ra rằng phủ định lượng từ tồn tại dẫn tới mâu thuẫn. Ví dụ sau sẽ minh họa khái niệm chứng minh tồn tại kiến thiết.

Ví dụ 20. *Chứng minh tồn tại kiến thiết.*

Chỉ ra rằng với mọi n nguyên dương, tồn tại n số nguyên dương liên tiếp là hợp số. Điều này có nghĩa là phải chứng minh: $\forall n\ \exists x$ ($x + i$ là hợp số với $i = 1, 2, ..., n$).

Giải: Giả sử

$$x = (n + 1)! + 1.$$

Ta thấy $x + i = (n + 1)! + (i + 1)$ với $i = 1, 2, ..., n$ chia hết cho $(i + 1)$. Vì vậy $x + 1, x + 2, ..., x + n$ là n hợp số liên tiếp. Trong cách chứng minh này ta đã chỉ ra số x để cho $P(x)$ đúng. Đó là cách chứng minh kiến thiết.

■

Ví dụ 21. *Chứng minh tồn tại không kiến thiết.*

Chỉ ra rằng với mọi số nguyên dương n tồn tại một số nguyên tố lớn hơn n. Bài này đòi hỏi chứng minh một lượng từ tồn tại là $\exists x\, Q(x)$, trong đó $Q(x)$ là mệnh đề "x là nguyên tố và x lớn hơn n". Bài toán được xét trong tập hợp các số nguyên dương.

Giải: Giả sử n là một số nguyên dương. Để chỉ ra có một số nguyên tố lớn hơn n ta nghiên cứu số nguyên $n! + 1$. Vì mọi số nguyên đều có ít nhất một ước số nguyên tố, nên có ít nhất một số nguyên tố là ước của $n! + 1$. (Có thể $n! + 1$ cũng là số nguyên tố). Ta thấy rằng khi chia $n! + 1$ cho các số nguyên nhỏ hơn hay bằng n đều dư 1, nên mọi ước nguyên tố của $n! + 1$ đều lớn hơn n. Đó chính là điều cần chứng minh. Chứng minh này là cách chứng minh tồn tại không kiến thiết vì không tìm ra được số nguyên tố lớn hơn n mà đơn giản chỉ khẳng định là nó phải có.

■

Giả sử mệnh đề dạng $\forall x\, P(x)$ là sai. Chúng ta chứng tỏ điều này bằng cách nào? Nhớ lại rằng các mệnh đề $\neg\, \forall x\, P(x)$ và $\exists x \neg P(x)$ là tương đương. Điều này có nghĩa là nếu ta tìm được một phần tử a sao cho $P(a)$ sai thì chúng ta chỉ ra được $\exists x \neg P(x)$ là đúng hay $\forall x\, P(x)$ là sai. Phần tử a sao cho $P(a)$ sai gọi là **một phản ví dụ**. Nếu tìm được dù chỉ một phản ví dụ cũng đủ chứng tỏ $\forall x\, P(x)$ là sai.

Ví dụ 22. Chứng tỏ rằng khẳng định "Tất cả các số nguyên tố đều lẻ" là sai.

Giải: Mệnh đề "Tất cả các số nguyên tố đều lẻ" là một lượng từ phổ dụng, tức là $\forall x O(x)$, trong đó $O(x)$ là mệnh đề "x là lẻ" và không gian đang xét là tập các số nguyên tố. Chú ý rằng $x = 2$ là một phản ví dụ, vì 2 là số nguyên tố nhưng là số chẵn. Vì thế mệnh đề "Tất cả các số nguyên tố đều lẻ" là sai.

■

Hãy nhớ rằng dù có cho rất nhiều ví dụ minh chứng một định lý là đúng cũng không thể khẳng định sự đúng đắn của định lý dạng $\forall x P(x)$ trừ khi các ví dụ này phủ hết mọi giá trị của không gian. Ví dụ, việc chỉ ra rằng $x^2 - x + 41$ là nguyên tố với những $x = 0, 1, 2 \ldots, 40$ cũng không thể khẳng định rằng đa thức này luôn nhận giá trị nguyên tố khi x là các số nguyên không âm. Dễ thấy khi $x = 41$ thì giá trị của đa thức là hợp số.

Cuối cùng, trong cuốn sách này chúng tôi tuân theo những quy ước chuẩn của toán học là một mệnh đề với các biến tự do được giả thiết là lượng tử phổ dụng khi nghiên cứu giá trị chân lý của nó. Ví dụ, trong Ví dụ 2 khi nói mệnh đề kéo theo "nếu n chia hết cho 3 thì n^2 chia hết cho 9" là đúng, ta ngầm hiểu là lượng hóa "với mọi số nguyên n, nếu n chia hết cho 3 thì n^2 chia hết cho 9" là đúng. Ta cũng ngầm giả thiết là ở đây không gian là tập các số nguyên dương.

VÀI LỜI BÌNH LUẬN

Chúng ta đã mô tả các phương pháp khác nhau để chứng minh định lý. Độc giả có thể nhận thấy rằng ở đây không đưa ra một thuật toán nào để chứng minh định lý. Không tồn tại một thủ tục như vậy.

Có nhiều định lý chúng ta có thể dễ dàng chứng minh nhờ các giả thiết, các định nghĩa của các thành phần của nó. Nhưng cũng có nhiều định lý nếu không sử dụng một cách thông minh các chứng minh gián tiếp, chứng minh bằng phản chứng, hay một vài kỹ thuật chứng minh khác thì chứng minh chúng sẽ rất vất vả. Xây dựng các chứng minh là một nghệ thuật có thể học được chỉ bằng cách thử tấn công bằng nhiều cách khác nhau.

Tuy vậy, cơ nhiêu mệnh đề dường như là các định lý vẫn cứ ngoan cố chống lại những cố gắng không mệt mỏi của các nhà toán học từ mấy trăm năm nay. Ví dụ, mệnh đề "mọi số nguyên dương chẵn lớn hơn 4 là tổng của hai số nguyên tố" vẫn chưa được chứng minh là đúng và cũng chưa tìm được một phản ví dụ nào. Mệnh đề này mang tên là bài toán *Goldbach*. Đây là một trong nhiều khẳng định trong toán học chưa được chứng minh.

BÀI TẬP

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

   a) Alice giỏi môn toán. Do đó Alice giỏi môn toán hoặc môn tin.

   b) Jerry giỏi môn toán và môn tin. Do vậy Jerry giỏi môn toán.

   c) Nếu trời mưa thì bể bơi sẽ đóng cửa. Trời mưa, do đó bể bơi đóng cửa.

   d) Nếu hôm nay tuyết rơi thì trường đại học sẽ đóng cửa. Hôm nay trường đại học không đóng cửa. Do vậy hôm nay đã không có tuyết rơi.

e) Nếu tôi đi bơi thì tôi sẽ phơi nắng được nhiều. Nếu tôi phơi nắng nhiều thì tôi rám nắng. Do đó nếu tôi đi bơi thì tôi rám nắng.

2. Quy tắc suy luận nào được dùng trong mỗi một lập luận sau :

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

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

c) Linda là vận động viên bơi tuyệt vời. Nếu Linda là vận động viên bơi tuyệt vời, khi đó cô ta có thể làm việc như một người cứu hộ ở bể bơi. Do đó Linda có thể làm việc như một người cứu hộ ở bể bơi.

d) Steve sẽ làm việc ở một công ty tin học vào mùa hè này. Do đó mùa hè này anh ta sẽ làm việc ở một công ty tin học hoặc là một kẻ lang thang ngoài bãi biển.

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

3. Xác định xem mỗi suy luận sau là có cơ sở không. Nếu một suy luận là có cơ sở thì nó đùng quy tắc suy luận nào. Nếu không hãy chỉ ra nguỵ hiện nào đã được sử dụng.

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

b) $\log_2 3$ là vô tỷ nếu nó không là tỷ số của hai số nguyên. Do đó, vì $\log_2 3$ không thể viết dưới dạng a/b với a và b là hai số nguyên, nếu nó là vô tỷ.

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

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

e) Nếu n là một số thực và $n > 2$, khi đó $n^2 > 4$. Giả sử $n \leqslant 2$. Khi đó $n^2 \leqslant 4$.

4. Suy luận sau đây là chứng minh không chính xác của định lý "Nếu n^2 không chia hết cho 3 thì n không chia hết cho 3". Nguyên nhân là do dùng suy luận quẩn. Sai lầm ở đâu ?

> Nếu n^2 là không chia hết cho 3, khi đó n^2 không bằng $3k$ với k là một số nguyên nào đó. Vì thế n không bằng $3l$ với một số nguyên l nào đó. Kết luận, n không chia hết cho 3.

5. Hãy chứng minh mệnh đề $P(0)$, trong đó $P(n)$ là mệnh đề "Nếu n là số nguyên dương lớn hơn 1, khi đó $n^2 > n$". Bạn đã dùng kiểu chứng minh nào?

6. Hãy chứng minh mệnh đề $P(1)$, trong đó $P(n)$ là mệnh đề "Nếu n là số nguyên dương khi đó $n^2 \geq n$". Bạn đã dùng kiểu chứng minh nào?

7. Giả sử $P(n)$ là mệnh đề "Nếu a và b là các số thực dương, khi đó $(a + b)^n \geq a^n + b^n$. Chứng minh $P(1)$ là đúng. Bạn đã dùng kiểu chứng minh nào?

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

   a) chứng minh trực tiếp

   b) chứng minh gián tiếp

   c) chứng minh bằng phản chứng.

9. Hãy chứng minh tổng hai số nguyên lẻ là một số chẵn

10. Chứng minh tổng hai số hữu tỷ là số hữu tỷ.

11. Chứng minh tổng một số hữu tỷ với một số vô tỷ là một số vô tỷ bằng phản chứng.

12. Chứng minh rằng tích của hai số hữu tỷ là một số hữu tỷ.

13. Chứng minh hoặc bác bỏ rằng tích hai số vô tỷ là một số vô tỷ.

14. Chứng minh hoặc bác bỏ rằng tích một số hữu tỷ khác không và một số vô tỷ là số vô tỷ.

15*. Chứng minh hoặc bác bỏ rằng $n^2 - n + 41$ là nguyên tố khi n là số nguyên dương.

16. Chứng minh hoặc bác bỏ rằng $2^n + 1$ là nguyên tố với mọi n nguyên không âm.

17. Chỉ ra rằng $\sqrt[3]{3}$ là vô tỷ.

18*. Chỉ ra rằng $\sqrt{n}$ là vô tỷ nếu n là số nguyên dương không chính phương.

19 Chứng minh rằng x và y là hai số thực khi đó

$$\max(x, y) + \min(x, y) = x + y$$

(*Gợi ý* : Sử dụng chứng minh từng trường hợp, với hai trường hợp tương ứng là $x \geq y$ và $x < y$).

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

21. Chứng minh rằng nếu x và y là hai số thực khi đó $|x| + |y| \geq |x + y|$, (trong đó $|x|$ là giá trị tuyệt đối của x).

22. Chứng minh rằng nếu n là số nguyên dương khi đó n là chẵn nếu và chỉ nếu $7n + 4$ là chẵn.

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

24. Chứng minh rằng $m^2 = n^2$ nếu và chỉ nếu $m = n$ hoặc $m = -n$.

25.* Cho p là một số nguyên tố. Chứng minh rằng $a^2 \equiv b^2 \pmod p$ nếu và chỉ nếu $a \equiv b \pmod p$ hoặc là $a \equiv -b \pmod p$.

26. Hãy chứng minh hoặc bác bỏ rằng $n^2 - 1$ là hợp số với n nguyên dương lớn hơn 1.

27. Hãy chứng minh hoặc bác bỏ rằng nếu m và n là các số nguyên dương sao cho $mn = 1$ khi đó hoặc là $m = 1$ và $n = 1$ hoặc là $m = -1$ và $n = -1$.

28. Hãy chứng minh hoặc bác bỏ rằng a **mod** $m + b$ **mod** $m = (a + b)$ **mod** m, với m là số nguyên dương.

29. Hãy chứng minh hoặc bác bỏ rằng mọi số nguyên dương có thể được viết dưới dạng tổng các bình phương của hai số nguyên.

30. Chứng minh rằng nếu n là một số nguyên dương sao cho tổng các ước của nó bằng $n + 1$, thì n là số nguyên tố. Bạn đã dùng kiểu chứng minh nào?

31. Chứng minh rằng ít nhất một trong các số thực $a_1, a_2, \ldots a_n$ lớn hơn hay bằng trung bình cộng của các số này. Bạn đã dùng kiểu chứng minh nào?

32*. Dùng Bài tập 31 chỉ ra rằng nếu 10 số nguyên dương đầu tiên được đặt xung quanh một vòng tròn, theo một thứ tự bất kỳ, thì sẽ tồn tại 3 số nguyên đứng liền nhau có tổng lớn hơn hay bằng 17.

33. Chứng minh rằng nếu n là một số nguyên, bốn mệnh đề sau là tương đương :

- n là chẵn
- $n + 1$ là lẻ
- $3n + 1$ là lẻ
- $3n$ là chẵn.

34. Chứng minh rằng nếu n là một số nguyên, ba mệnh đề sau là tương đương :

- n chia hết cho 5
- n^2 chia hết cho 5
- $n^2 \not\equiv \pm 1 \pmod 5$.

35. Chứng minh hoặc bác bỏ rằng có ba số nguyên dương lẻ liên tiếp là các số nguyên tố, tức là các số nguyên tố lẻ dạng p, $p + 2$ và $p + 4$.

36. Chứng minh hoặc bác bỏ rằng với n là một số nguyên dương đã cho khi đó tồn tại n số nguyên dương lẻ liên tiếp là các số nguyên tố.

37. Quy tắc suy luận nào đã dùng để khẳng định kết luận trong suy luận của Lewis Carroll trong Ví dụ 14 của Tiết 1.3?

38. Quy tắc suy luận nào đã dùng để khẳng định kết luận trong suy luận của Lewis Carroll trong Ví dụ 15 của Mục 1.3?

39. Hãy đưa ra một chứng minh kiến thiết của mệnh đề "Với mọi số nguyên dương n tồn tại một số nguyên chia hết cho nhiều hơn n số nguyên tố.

40. Tìm phản ví dụ cho mệnh đề "với mọi số nguyên tố n, $n + 2$ cũng là số nguyên tố".

41*. Chứng minh rằng có vô hạn các số nguyên tố đồng dư với 3 theo modun 4. Chứng minh của bạn thuộc loại kiến thiết hay không kiến thiết. (*Gợi ý* : Một phương pháp là giả sử rằng chỉ có một số hữu hạn các số nguyên tố $p_1, p_2, ..., p_n$. Gọi $q = 4p_1p_2 ... p_n + 3$. Chứng tỏ rằng q có ước nguyên tố đồng dư với 3 theo môđun 4 không nằm trong các số nguyên tố $p_1, p_2, ..., p_n$).

42. Chứng minh hoặc bác bỏ rằng nếu $p_1, p_2, ..., p_n$ là các số nguyên tố nhỏ nhất thì $p_1p_2 ... p_n + 1$ là một số nguyên tố.

43. Chứng minh rằng các mệnh đề p_1, p_2, p_3, p_4 và p_5 có thể chỉ ra là tương đương nhau nếu chứng minh được rằng các mệnh đề kéo theo

$$p_1 \rightarrow p_4,\ p_3 \rightarrow p_1,\ p_4 \rightarrow p_2,\ p_2 \rightarrow p_5 \text{ và } p_5 \rightarrow p_3 \text{ là đúng.}$$

44. Chứng minh hay bác bỏ rằng nếu a và b là các số hữu tỷ khi đó a^b cũng là hữu tỷ.

45. Chứng minh rằng có các số vô tỷ a và b sao cho a^b là hữu tỷ. Chứng minh của bạn thuộc loại kiến thiết hay không kiến thiết? (*Gợi ý*: Cho $a = \sqrt{2}$ và $b = \sqrt{2}$. Chỉ ra rằng a^b hoặc $(a^b)^b$ là hữu tỷ).

46. Chứng minh bàn cờ 8×8 có thể phủ hoàn toàn bằng các quân domino (1×2 ô).

47*. Chứng minh rằng không thể phủ hoàn toàn bàn cờ 8×8 bằng các quân domino nếu hai ô ở các góc đối diện bị cắt bỏ.

48*. Bài toán Logic, lấy từ WFF'N PROOF - Trò chơi Logic, có hai giả thiết :

1. "Môn logic là khó hoặc không có nhiều sinh viên thích môn logic"
2. "Nếu môn toán là dễ thì logic là không khó".

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

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

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

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

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

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

49*. Hãy xác định xem suy luận sau đây có cơ sở hay không: "Nếu một siêu nhân có khả năng và muốn ngăn cản một tội ác thì anh ta sẽ làm điều đó. Nếu một siêu nhân không có khả năng ngăn cản một tội ác thì anh ta là người bất lực. Nếu anh ta không muốn ngăn cản tội ác anh ta sẽ là một người xấu bụng. Một siêu nhân không ngăn cản tội ác. Nếu siêu nhân tồn tại thì anh ta hoặc là bất lực hoặc là xấu hụng. Do đó siêu nhân không tồn tại".

3.2. QUY NẠP TOÁN HỌC

MỞ ĐẦU

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

$$1 = 1.$$

$$1 + 3 = 4.$$

$$1 + 3 + 5 = 9.$$

$$1 + 3 + 5 + 7 = 16.$$

$$1 + 3 + 5 + 9 + 11 = 25.$$

Từ các kết quả này ta dự đoán tổng n số nguyên lẻ đầu tiên là n^2. Nhưng chúng ta cần có phương pháp *chứng minh* dự đoán trên là *đúng*, nếu thực tế đúng như vậy.

Quy nạp toán học là một kỹ thuật chứng minh cực kỳ quan trọng. Người ta thường dùng nó để chứng minh những điều khẳng định kiểu như trên. Như chúng ta sẽ thấy trong tiết này và trong các chương sau, quy nạp toán học rất hay được sử dụng để chứng minh các kết quả về những đối

tượng rời rạc thuộc nhiều kiểu khác nhau. Chẳng hạn, chứng minh độ phức tạp của thuật toán, tính không đúng đắn của một số loại chương trình, các định lý về đồ thị và cây, cũng như một lớp rất rộng các đẳng thức và các bất đẳng thức.

Trong tiết này chúng ta sẽ mô tả cách dùng phương pháp quy nạp toán học và sẽ lý giải vì sao quy nạp toán học là một kỹ thuật chứng minh có cơ sở chặt chẽ. Nhưng chúng ta cũng cần nhớ rằng quy nạp toán học dùng chỉ để chứng minh các kết quả nhận được bằng một cách nào đó chứ không là công cụ để phát hiện ra các công thức hay định lý.

TÍNH ĐƯỢC SẮP TỐT

Tính đúng đắn của quy nạp toán học được suy ra từ tiên đề sau đây về tập các số nguyên.

Tính được sắp tốt : Mọi tập không rỗng các số nguyên không âm luôn có phần tử nhỏ nhất.

Tính được sắp tốt thường được dùng trực tiếp trong các chứng minh.

Ví dụ 1. Dùng tính chất được sắp tốt hãy chứng minh thuật toán chia như sau. Nếu a là một số nguyên và d là một số nguyên dương khi đó tồn tại duy nhất các số nguyên q và r sao cho $0 \leqslant r < d$ và $a = dq + r$.

Giải: Giả sử S là tập các số nguyên không âm dạng $a - dq$ trong đó q là một số nguyên. Tập này không rỗng vì $-dq$ có thể lớn tùy ý bằng cách chọn q âm có trị tuyệt đối đủ lớn. Theo tính được sắp tốt S có số nhỏ nhất là $r = a - dq_0$. Rõ ràng $r < d$, vì nếu ngược lại ta xét số $a - d(q_0 + 1) = (a - dq_0) - d = r - d \geqslant 0$ tức là $a - d(q_0 + 1)$ thuộc tập S mà lại nhỏ hơn r. Đó là điều vô lý. Do vậy có các số nguyên q, r sao cho $a = dq + r$ và $0 \leqslant r < d$. Chúng tôi để lại phần chứng minh tính duy nhất của q và r cho độc giả tự làm như một bài tập.

■

QUY NẠP TOÁN HỌC

Nhiều định lý phát biểu rằng $P(n)$ là đúng với mọi n nguyên dương, trong đó $P(n)$ là một hàm mệnh đề. Quy nạp toán học là một kỹ thuật chứng minh các định lý thuộc loại như thế. Nói cách khác quy nạp toán học

thường được sử dụng để chứng minh các mệnh đề dạng $\forall n P(n)$ trong đó n là một số nguyên dương tùy ý.

Qúa trình chứng minh $P(n)$ là đúng với mọi số nguyên dương n bao gồm hai bước :

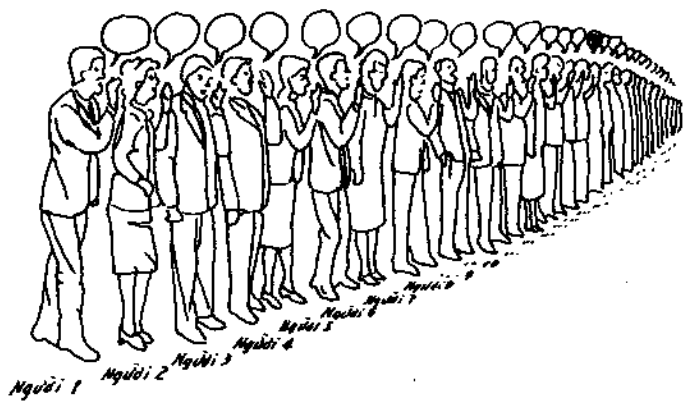
1. *Bước cơ sở* : Chỉ ra mệnh đề $P(1)$ là đúng.
2. *Bước quy nạp* : Chứng minh phép kéo theo $P(n) \rightarrow P(n + 1)$ là đúng với mọi số nguyên dương n, trong đó người ta gọi $P(n)$ là **giả thiết quy nạp.**

Khi hoàn thành cả hai bước chúng ta đã chứng minh $P(n)$ là đúng với mọi n nguyên dương, tức là chúng ta đã chứng minh $P(n)$ là đúng.

Theo cách viết của các quy tắc suy luận thì kỹ thuật chứng minh này có dạng như sau :

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

Vì quy nạp toán học là kỹ thuật chứng minh rất quan trọng, nên chúng ta cần giải thích kỹ thuật từng bước chứng minh. Trước tiên là phải chỉ ra là $P(1)$ đúng. Điều này có nghĩa là chỉ ra một trường hợp riêng của mệnh đề $P(n)$ khi $n = 1$ là đúng. Sau đó cần phải chỉ ra với mọi n nguyên dương tùy ý, mệnh đề $P(n) \rightarrow P(n + 1)$ là đúng, có nghĩa là $P(n + 1)$ không thể sai khi $P(n)$ đúng. Điều này cũng có thể thực hiện được bằng cách giả sử $P(n)$ là đúng và chỉ ra *với giả thiết quy nạp đó* $P(n + 1)$ cũng đúng.

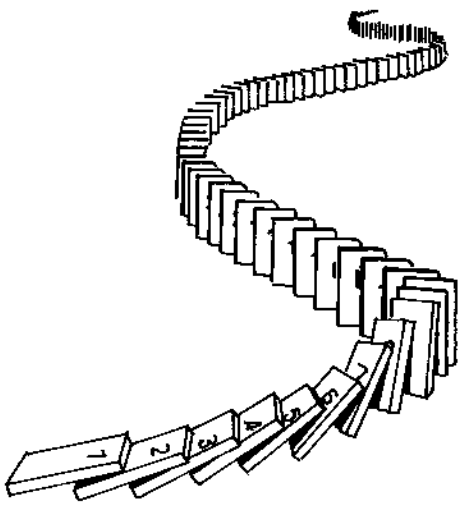


Hình 1. Hàng người tiết lộ bí mật.

Chú ý: Trong khi chứng minh bằng quy nạp toán học, ta không giả sử $P(n)$ đúng với mọi n nguyên dương! Mà chúng ta chỉ chứng tỏ rằng giả sử $P(n)$ là đúng thì khi đó $P(n + 1)$ cũng đúng, như vậy quy nạp toán học không phải là cách suy lý quẩn.

Khi sử dụng quy nạp toán học để chứng minh định lý, trước tiên ta chỉ ra $P(1)$ là đúng. Sau đó ta biết $P(2)$ là đúng, vì $P(1)$ suy ra $P(2)$. Tiếp theo $P(3)$ đúng vì $P(2)$ suy ra $P(3)$. Cứ tiếp tục như vậy ta có $P(k)$ đúng với mọi k nguyên dương tùy ý.

Có một vài cách minh họa phương pháp quy nạp toán học có thể giúp bạn dễ nhớ cách hoạt động của nguyên lý này. Giả sử có một hàng người (Hình 1), người thứ nhất, người thứ hai, người thứ ba, ...Tiếp theo ta giả sử có một tin mật và giả sử rằng nếu một người biết tin này là tức anh ta sẽ tiết lộ cho người đứng sau mình. Gọi $P(n)$ là mệnh đề "người n biết tin mật này". Khi đó nếu người thứ nhất biết tin mật này thì $P(1)$ là đúng, sau đó $P(2)$ cũng đúng vì người thứ nhất nói cho người thứ hai, người hai lại nói cho người thứ ba, tức là $P(3)$ đúng v.v. Cứ như vậy, theo quy nạp toán học, mọi người trong hàng đều biết điều bí mật. Một cách minh họa khác là một dãy quân cờ đôminô có nhãn là 1,



Hình 2. Cách minh họa phép quy nạp toán học bằng quân bài đôminô.

2, 3, ... đang đứng trên mặt bàn. Giả sử $P(n)$ là mệnh đề "quân đôminô n bị đổ". Nếu quân 1 bị đổ, tức là $P(1)$ đúng, và nếu quân n đổ thì quân $(n + 1)$ cũng đổ, tức là nếu $P(n) \rightarrow P(n + 1)$ là đúng, thì khi đó tất cả các quân đôminô đều bị đổ. Điều này được minh họa trên Hình 2.

Tại sao quy nạp toán học là phương pháp chứng minh có cơ sở vững chắc. Nguyên do là vì tập các số nguyên không âm có tính được sắp tốt. Giả sử ta biết $P(1)$ là đúng và giả sử mệnh đề $P(n) \rightarrow P(n + 1)$ là đúng với mọi số nguyên dương n. Để chứng minh $P(n)$ là đúng với mọi số nguyên dương n, ta giả sử ngược lại có ít nhất một số nguyên dương sao cho $P(n)$ là sai. Khi đó tập S bao gồm các số nguyên dương n mà $P(n)$ sai là không rỗng. Theo tiên đề được sắp tốt, S có phần tử nhỏ nhất, giả sử là k. Vì $P(1)$ đúng nên k khác 1, hơn thế nữa $k > 1$. Do $0 < k - 1 < k$ nên $k - 1$ không thuộc S, tức là $P(k - 1)$ đúng. Nhưng vì mệnh đề $P(k - 1) \rightarrow P(k)$ là đúng, ta suy ra $P(k)$ là đúng. Điều này vô lý vì k thuộc S. Do vậy, $P(n)$ là đúng với mọi n nguyên dương.

CÁC VÍ DỤ

Chúng ta sẽ minh họa cách dùng quy nạp toán học để chứng minh các định lý thông qua các ví dụ. Tuy nhiên các bài toán này có thể được chứng minh bằng các phương pháp khác.

Ví dụ 2. Bằng quy nạp toán học hãy chứng minh rằng tổng n số nguyên dương lẻ đầu tiên là n^2.

Giải: Gọi $P(n)$ là mệnh đề "tổng n số nguyên dương lẻ đầu tiên là n^2". Đầu tiên ta cần làm bước cơ sở, tức là phải chỉ ra $P(1)$ là đúng. Sau đó phải chứng minh hước quy nạp, tức là cần chỉ ra $P(n + 1)$ là đúng nếu giả sử $P(n)$ là đúng.

BƯỚC CƠ SỞ : $P(1)$ hiển nhiên là đúng vì $1 = 1^2$

BƯỚC QUY NẠP : Giả sử $P(n)$ đúng, tức là với mọi n nguyên dương lẻ ta có

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

Ta phải chỉ ra $P(n + 1)$ là đúng, tức là :

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

Do giả thiết quy nạp ta suy ra :

$$1 + 3 + 5 + \ldots + (2n - 1) + (2n + 1)$$
$$= [1 + 3 + 5 + \ldots + (2n - 1)] + (2n + 1)$$
$$= n^2 + (2n + 1) = (n + 1)^2.$$

Đẳng thức này chứng tỏ $P(n + 1)$ được suy ra từ $P(n)$.

Vì $P(1)$ là đúng và vì mệnh đề kéo theo $P(n) \rightarrow P(n + 1)$ là đúng với mọi n nguyên dương, nguyên lý quy nạp toán học chỉ ra rằng $P(n)$ đúng với mọi n nguyên dương.

■

Ví dụ 3. Bằng quy nạp toán học chứng minh bất đẳng thức $n < 2^n$ với mọi n nguyên dương.

Giải: Giả sử $P(n)$ là mệnh đề "$n < 2^n$ ".

BƯỚC CƠ SỞ : $P(1)$ là đúng vì $1 < 2^1 = 2$.

BƯỚC QUY NẠP : Giả sử $P(n)$ là đúng với mọi n nguyên dương, tức là $n < 2^n$. Ta cần chứng minh $P(n + 1)$ đúng, tức là cần chứng minh $n + 1 < 2^{n+1}$.

Thật vậy, cộng 1 vào hai vế của giả thiết quy nạp và lưu ý rằng $1 \leqslant 2^n$, ta có :

$$1 + n < 1 + 2^n < 2^n + 2^n = 2^{(n+1)}.$$

Theo quy nạp toán học, ta khẳng định $n < 2^n$ đúng với mọi n nguyên dương.

■

Bây giờ chúng ta dùng quy nạp toán học để chứng minh một định lý về tính chia hết của số nguyên.

Ví dụ 4. Chứng minh rằng $n^3 - n$ chia hết cho 3 với mọi n nguyên dương.

Giải: Gọi $P(n)$ là mệnh đề "$n^3 - n$ chia hết cho 3"

BƯỚC CƠ SỞ. $P(1)$ là đúng vì $1^3 - 1 = 0$ chia hết cho 3.

BƯỚC QUY NẠP. Giả sử $P(n)$ đúng, tức là $n^3 - n$ chia hết cho 3. Ta cần chứng minh $P(n + 1)$ đúng. Thật vậy, biểu thức

$$(n + 1)^3 - (n + 1) = (n^3 + 3n^2 + 3n + 1) - (n + 1)$$
$$= (n^3 - n) + 3(n^2 + n)$$

chia hết cho 3 vì số hạng thứ nhất chia hết cho 3 theo giả thiết quy nạp, còn số hạng sau là 3 lần của một số nguyên. Bước quy nạp được hoàn thành. Theo nguyên lý quy nạp toán học, $n^3 - n$ chia hết cho 3 với mọi n nguyên dương.

■

Đôi khi chúng ta cần chỉ ra $P(n)$ đúng với $n = k, k + 1, k + 2, \ldots$ trong đó k là một số nguyên khác 1. Khi chứng minh bằng quy nạp toán học ta cần thay đổi một chút ở bước cơ sở.

Ví dụ 5. Dùng quy nạp toán học chứng tỏ rằng

$$1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1, \text{ với mọi } n \text{ nguyên không âm.}$$

Giải: Giả sử $P(n)$ là mệnh đề "công thức này đúng với mọi n nguyên không âm"

BƯỚC CƠ SỞ. $P(0)$ đúng vì $2^0 = 1 = 2^1 - 1$.

BƯỚC QUY NẠP. Giả sử $P(n)$ đúng, tức là

$$1 + 2 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1.$$

Sử dụng giả thiết quy nạp dễ thấy rằng

$$1 + 2 + 2^2 + \ldots + 2^n + 2^{n+1} = (1 + 2 + 2^2 + \ldots + 2^n) + 2^{n+1}$$
$$= 2^{n+1} - 1 + 2^{n+1} = 2^{n+2} - 1.$$

Đẳng thức này chứng tỏ $P(n + 1)$ là đúng. Hay công thức này đúng với mọi n nguyên không âm.

■

Như ví dụ 5 đã minh họa, để dùng quy nạp toán học chứng minh $P(n)$ đúng với $n = k, k + 1, k + 2, \ldots$ trong đó k khác 1, chúng ta phải chỉ ra $P(k)$ là đúng (bước cơ sở) và sau đó chỉ ra mệnh đề kéo theo $P(n) \rightarrow P(n + 1)$ đúng với $n = k, k + 1, k + 2, \ldots$ (bước quy nạp). Lưu ý là k có thể dương, âm hay bằng không (xem Bài tập 62).

Công thức trong Ví dụ 5 là trường hợp riêng của công thức tính tổng các số hạng của cấp số nhân $a, ar, ar^2, \ldots, ar^n, \ldots$ trong đó a và r là các số thực. Ví dụ dãy số trong Ví dụ 5 là cấp số nhân với $a = 1$ và $r = 2$. Cũng như vậy, dãy $3, 15, 75, \ldots, 3.5^n, \ldots$ là cấp số nhân với $a = 3$ và $r = 5$.

Ví dụ 6. *Tổng các số hạng của cấp số nhân.* Dùng quy nạp toán học chứng minh công thức sau đây đối với tổng một số hữu hạn các số hạng của cấp số nhân :

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \ldots + ar^n = \frac{ar^{n+1} - a}{r - 1} .$$

trong đó $r \neq 1$.

Giải: Giả sử $P(n)$ là mệnh đề "tổng $(n + 1)$ số hạng đầu tiên của cấp số nhân được cho theo công thức trên".

BƯỚC CƠ SỞ. $P(0)$ là đúng vì $a = \frac{ar - a}{r - 1}$

BƯỚC QUY NẠP. Giả sử $P(n)$ là đúng, tức là :

$$a + ar + ar^2 + \ldots + ar^n = \frac{ar^{n+1} - a}{r - 1}$$

Để chứng minh từ đây có thể suy ra được $P(n+1)$ đúng, cộng ar^{n+1} vào hai vế của đẳng thức trên, ta nhận được :

$$a + ar + ar^2 + \ldots + ar^n + ar^{n+1} = \frac{ar^{n+1} - a}{r - 1} + ar^{n+1}$$

$$= \frac{ar^{n+1} - a}{r - 1} + \frac{ar^{n+2} - ar^{n+1}}{r - 1} = \frac{ar^{n+2} - a}{r - 1} .$$

Điều này chứng tỏ nếu $P(n)$ đúng thì $P(n + 1)$ cũng đúng. Vậy công thức trên là đúng với mọi n nguyên.

■

Một bất đẳng thức quan trọng đối với tổng các nghịch đảo của các số nguyên dương sẽ được chứng minh trong ví dụ sau.

Ví dụ 7. Bất đẳng thức đối với các số điều hòa. Các *số điều hòa* H_k, $k = 1, 2, 3 \ldots$ được định nghĩa như sau :

$$H_k = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{k}$$

Ví dụ,

$$H_4 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12}$$

Dùng quy nạp chứng minh rằng : $H_{2^n} \geq 1 + \frac{n}{2}$ trong đó n là số nguyên không âm.

Giải: Giả sử $P(n)$ là mệnh đề "$H_{2^n} \geq 1 + \frac{n}{2}$".

BƯỚC CƠ SỞ. $P(0)$ là đúng vì $H_{2^0} = H_1 = 1 \geq 1 + \frac{0}{2}$.

BƯỚC QUY NẠP. Giả sử $P(n)$ đúng, tức là ta có $H_{2^n} \geq 1 + \frac{n}{2}$. Để chứng minh $P(n+1)$ đúng, ta thực hiện các phép hiến đổi như sau :

$$H_{2^{n+1}} = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^n} + \frac{1}{2^n + 1} + \ldots + \frac{1}{2^{n+1}} =$$

$$= H_{2^n} + \frac{1}{2^n + 1} + \ldots + \frac{1}{2^{n+1}} \geq \left(1 + \frac{n}{2}\right) + \frac{1}{2^n + 1} + \ldots + \frac{1}{2^{n+1}}$$

(do giả thiết quy nạp)

$$\geq \left(1 + \frac{n}{2}\right) + 2^n \cdot \frac{1}{2^{n+1}}$$

(vì có 2^n số hạng mỗi số không nhỏ hơn $\frac{1}{2^{n+1}}$)

$$= \left(1 + \frac{n}{2}\right) + \frac{1}{2} = 1 + \frac{n+1}{2}$$

Đó là điều cần chứng minh. Như vậy bất đẳng thức về các số điều hòa đúng với mọi số nguyên không âm.

■

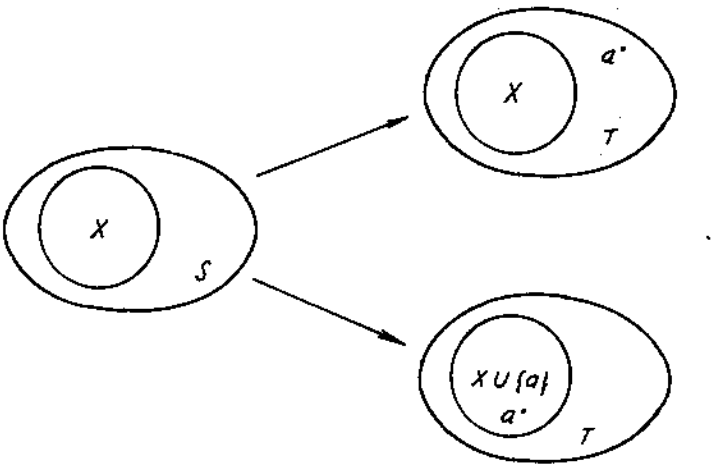
Ví dụ 8. *Số tập con của một tập hữu hạn.* Dùng quy nạp toán học chỉ ra rằng, nếu S là một tập có n phần tử, thì S có 2^n tập con.

Giải: Gọi $P(n)$ là mệnh đề "tập n phần tử có 2^n tập con"

BƯỚC CƠ SỞ. $P(0)$ là đúng, vì tập rỗng có $2^0 = 1$ tập con, đó là chính nó.

BƯỚC QUY NẠP. Giả sử $P(n)$ là đúng, tức là tập n phần tử có 2^n tập con. Ta cần phải chứng minh $P(n + 1)$ cũng đúng.

Thật vậy, giả sử T là tập có $(n + 1)$ phần tử. Khi đó có thể viết $T = S \cup \{a\}$, trong đó a là một phần tử của T và $S = T - \{a\}$. Rõ ràng ứng với mỗi tập con X của S ta có thể tạo ra được đúng hai tập con của T đó là X và $X \cup \{a\}$. Theo giả thiết quy nạp, tập S có 2^n tập con, vậy tập T có $2.2^n = 2^{n+1}$ tập con. Đây chính là điều cần chứng minh. ■



Hình 3. Sinh các tập con của tập hợp với $n + 1$ phần tử. Ở đây $T = S \cup \{a\}$.

Ví dụ 9. Chứng minh rằng nếu n là một số nguyên dương thì

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

Giải: Gọi $P(n)$ là mệnh đề "tổng n số nguyên dương đầu tiên bằng $\frac{n(n+1)}{2}$".

BƯỚC CƠ SỞ. Rõ ràng $P(1)$ là đúng, vì $1 = \frac{1(1+1)}{2}$.

BƯỚC QUY NẠP. Giả sử $P(n)$ là đúng, tức là

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

Với giả thiết này ta phải chỉ ra $P(n + 1)$ đúng. Thật vậy, ta có

$$1 + 2 + 3 + ... + n + (n + 1) = [1 + 2 + 3 + ... + n] + (n + 1)$$
$$= \frac{n(n + 1)}{2} + (n + 1) = \frac{(n + 1)(n + 2)}{2}.$$

Đẳng thức này chứng tỏ $P(n + 1)$ đúng nếu $P(n)$ đúng.

Vậy tổng n số nguyên dương đầu tiên bằng $\frac{n(n + 1)}{2}$.

■

Ví dụ 10. Bằng quy nạp chỉ ra rằng $2^n < n!$ với mọi số nguyên $n \geq 4$.

Giải: Giả sử $P(n)$ là mệnh đề $2^n < n!$.

BƯỚC CƠ SỞ. Rõ ràng $P(4)$ là đúng vì $2^4 = 16 < 4! = 24$.

BƯỚC QUY NẠP. Giả sử $P(n)$ là đúng, tức là $2^n < n!$. Để chứng minh $P(n + 1)$ đúng ta nhân cả hai vế bất đẳng trên với 2, ta có :

$$2.2^n < 2.n! < (n + 1)n! = (n + 1)!$$

Đó là điều cần chứng minh.

■

Ví dụ 11. Bằng quy nạp toán học chứng minh định luật De Morgan tổng quát :

$$\overline{\bigcap_{k=1}^{n} A_k} = \bigcup_{k=1}^{n} \overline{A_k}$$

trong đó $A_1, A_2 ... A_n$ là các tập con của tập vũ trụ U và $n \geq 2$.

Giải: Giả sử $P(n)$ là đẳng thức cần chứng minh.

BƯỚC CƠ SỞ. Rõ ràng $P(2)$ là đúng vì $\overline{A_1 \cap A_2} = \overline{A}_1 \cup \overline{A}_2$ chính là định luật De Morgan mà ta đã chứng minh trong Tiết 1.5.

BƯỚC QUY NẠP. Giả sử $P(n)$ là đúng, tức là

$$\overline{\bigcap_{k=1}^{n} A_k} = \bigcup_{k=1}^{n} \overline{A_k}$$

Để chứng minh $P(n + 1)$ đúng, ta giả sử $A_1, A_2, ..., A_n, A_{n+1}$ là các tập con của tập vũ trụ U. Khi đó sử dụng giả thiết quy nạp ta có :

$$\overline{\bigcap_{k=1}^{n+1} A_k} = \overline{\left(\bigcap_{k=1}^{n} A_k\right) \cap A_{n+1}} = \overline{\left(\bigcap_{k=1}^{n} A_k\right)} \cup \overline{A_{n+1}}$$

$$= \left(\bigcup_{k=1}^{n} \overline{A_k}\right) \cup \overline{A_{n+1}} = \bigcup_{k=1}^{n+1} \overline{A_k}$$

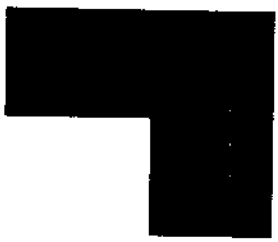
Đây chính là điều cần chứng minh.

■

Ví dụ 12. Giả sử n là một số nguyên dương. Một bàn cờ hình vuông mỗi chiều bằng 2^n đơn vị và bị hỏ đi một ô vuông. Chỉ ra rằng có thể lát bàn cờ đó bằng các miếng hình chữ L (gồm 3 hình vuông đơn vị), như ở Hình 4.

Giải: Gọi $P(n)$ là mệnh đề "có thể lát bàn cờ đó bằng các miếng hình chữ L".

BƯỚC CƠ SỞ. Rõ ràng $P(1)$ là đúng như Hình 5 chỉ ra.

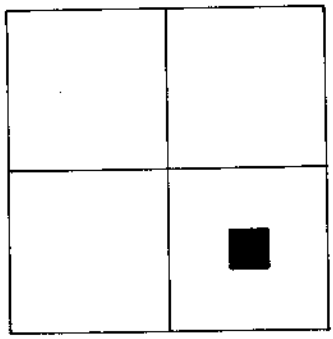


Hình 4. Miếng hình L.

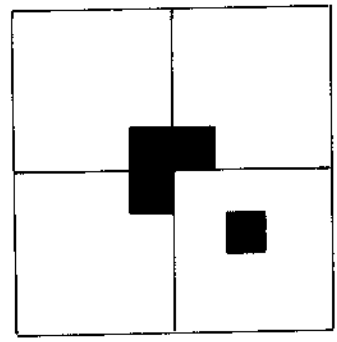
BƯỚC QUY NẠP. Giả sử $P(n)$ đúng, tức là mọi bàn cờ hình vuông mỗi chiều bằng 2^n đơn vị và bị khuyết một ô vuông đều có thể lát bằng các miếng hình chữ L. Ta phải chứng minh điều này cũng đúng với $(n + 1)$, tức

Hình 5. Lát bàn cờ 2×2 bỏ đi một ô vuông.

là $P(n + 1)$ đúng. Thật vậy, ta chia hình vuông có mỗi cạnh bằng 2^{n+1} thành 4 hình vuông mỗi cạnh 2^n (Hình 6). Một trong bốn hình vuông này bị khuyết một ô vuông, theo giả thiết quy nạp ta có thể lát nó bằng các miếng hình chữ L. Với ba hình còn lại ta đặt một miếng chữ L như



Hình 6. Chia bàn cờ $2^{n+1} \times 2^{n+1}$ thành bốn bàn cờ $2^n \times 2^n$



Hình 7. Lát bàn cờ $2^{n+1} \times 2^{n+1}$ bỏ đi một ô vuông.

trên Hình 7, khi đó ta nhận được ba hình vuông cạnh 2^n và cũng bị khuyết một ô vuông, theo giả thiết quy nạp chúng có thể lát bằng cách miếng hình chữ L. Tóm lại có thể lát được hình vuông cạnh 2^{n+1} bị khuyết một ô vuông bằng các miếng hình chữ L.

NGUYÊN LÝ THỨ HAI CỦA QUY NẠP TOÁN HỌC

Một dạng khác của quy nạp toán học cũng thường được dùng trong khi chứng minh. Với dạng này trong bước cơ sở ta cũng làm như trước đây, nhưng trong bước quy nạp có hơi khác một chút. Giả sử $P(k)$ đúng với $k = 1, 2, 3, ..., n$ ta phải chứng minh $P(n + 1)$ đúng. Đó chính là **nguyên lý thứ hai của quy nạp toán học.** Tóm lại để chứng minh $P(n)$ đúng với mọi n nguyên dương ta phải tiến hành hai bước :

1. BƯỚC CƠ SỞ. Chỉ ra mệnh đề $P(1)$ là đúng.

2. BƯỚC QUY NẠP. Chứng tỏ $[P(1) \wedge P(2) \wedge ... \wedge P(n)] \rightarrow P(n+1)$ là đúng với mọi n nguyên dương.

Hai dạng khác nhau này của quy nạp toán học là tương đương. Sau đây là những ví dụ áp dụng dạng thứ hai của quy nạp.

Ví dụ 13. Chỉ ra rằng nếu n là một số nguyên lớn hơn 1, khi đó n có thể viết dưới dạng tích của các số nguyên tố.

Giải: Gọi $P(n)$ là mệnh đề "n có thể viết dưới dạng tích của các số nguyên tố".

BƯỚC CƠ SỞ. $P(2)$ là đúng vì 2 là tích của chính nó.

BƯỚC QUY NẠP. Giả sử $P(k)$ là đúng với $k = 1, 2, 3, \ldots n$. Ta phải chứng minh $P(n + 1)$ là đúng. Thật vậy, nếu $(n+1)$ là số nguyên tố thì hiển nhiên $P(n + 1)$ là đúng. Nếu $(n+1)$ là hợp số thì nó có thể viết như sau $n + 1 = a.b$, trong đó $2 \leqslant a \leqslant b < n + 1$. Theo giả thiết quy nạp a và b lại có thể viết thành tích của các số nguyên tố. Như vậy nếu $n + 1$ là hợp số thì nó cũng có thể được viết dưới dạng tích của các số nguyên tố.

■

Ví dụ 14. Chứng tỏ mọi bưu phí bằng hay lớn hơn 12 xu đều có thể tạo ra bằng các con tem 4 hay 5 xu.

Giải: Giả sử $P(n)$ là mệnh đề "mọi bưu phí n xu ($n \geqslant 12$) đều có thể tạo ra bằng các con tem 4 hay 5 xu".

BƯỚC CƠ SỞ. $P(12)$ là đúng vì có thể dùng 3 con tem 4 xu.

BƯỚC QUY NẠP. Giả sử $P(n)$ đúng. Nếu có ít nhất một con tem 4 xu thì ta chỉ việc đổi con tem này bằng tem 5 xu thì sẽ tạo được bưu phí $n + 1$ xu. Nếu không có con tem 4 xu nào, tức là cước phí n xu tạo nên chỉ bằng các con tem 5 xu. Vì $n \geqslant 12$ nên ít nhất ta đã dùng 3 con tem 5 xu. Thay 3 con tem này bằng 4 con tem 4 xu, ta sẽ tạo được cước phí $n + 1$ xu.

Bây giờ chúng ta sẽ chứng minh bằng *dạng thứ hai của quy nạp toán học.*

BƯỚC CƠ SỞ. Dễ kiểm tra rằng $P(12)$, $P(13)$, $P(13)$, $P(14)$, $P(15)$ là đúng.
BƯỚC QUY NẠP. Giả sử $n \geqslant 15$ và $P(k)$ là đúng với $12 \leqslant k \leqslant n$. Để tạo ra bưu phí $n + 1$ xu ta dùng các con tem đã tạo ra bưu phí $n-3$ xu và thêm một tem 4 xu nữa. Vậy là chúng ta đã hoàn tất bước quy nạp và kết thúc chứng minh.

Chú ý: Ví dụ 14 chỉ ra có thể dùng dạng thứ hai của quy nạp toán học trong các trường hợp khi mà trong bước quy nạp phải giả sử mệnh đề đúng với một loạt các giá trị của n. Lược đồ áp dụng nguyên lý quy nạp bây giờ cơ dạng như sau. Chỉ ra rằng $P(k)$, $P(k+1)$, $P(k+2)$, ..., $P(l)$ là đúng (bước cơ sở), sau đó chỉ ra $[P(k) \wedge P(k+1) \wedge P(k+2) \wedge \ldots \wedge P(n)] \rightarrow P(n+1)$

là đúng với mọi số nguyên $n \geq 1$ (bước quy nạp). Chẳng hạn, ở bước cơ sở của Ví dụ 14 cần phải chỉ ra $P(12)$, $P(13)$, $P(14)$, $P(15)$ là đúng vì trong bước quy nạp ta phải chứng tỏ

$$[P(12) \wedge P(13) \wedge P(14) \wedge \ldots \wedge P(n)] \rightarrow P(n+1)$$

là đúng với mọi số nguyên $n \geq 15$.

Chúng ta sẽ thảo luận hai áp dụng quan trọng của quy nạp toán học trong tiết tới. Đó là dùng quy nạp để định nghĩa một dãy số khi không biết công thức tường minh của các số hạng, và sau đó là chứng minh tính đúng đắn của một chương trình.

BÀI TẬP

1. Hãy tìm công thức tính tổng n số nguyên chẵn đầu tiên.

2. Dùng quy nạp toán học chứng minh công thức tìm được trong Bài tập trên.

3. Dùng quy nạp toán học chứng minh rằng

$$3.5 + 3.5^2 + \ldots + 3.5^n = \frac{3(5^{n+1} - 1)}{4},$$

với n là số nguyên không âm.

4. Dùng quy nạp toán học chứng minh rằng

$$2 - 2.7 + 2.7^2 - \ldots + 2(-7)^n = \frac{1 - (-7)^{n+1}}{4},$$

với n là số nguyên không âm.

5. Tìm công thức tính tổng $\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n}$ bằng cách quan sát các giá trị của biểu thức này với các giá trị nhỏ của n. Dùng quy nạp toán học để chứng minh kết quả của bạn.

6. Tìm công thức tính tổng $\frac{1}{1.2} + \frac{1}{2.3} + \ldots + \frac{1}{n(n+1)}$ bằng cách quan sát các giá trị của biểu thức này với các giá trị nhỏ của n. Dùng quy nạp toán học để chứng minh kết quả của bạn.

7. Chỉ ra rằng $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$, với n nguyên dương.

8. Chỉ ra rằng $1^3 + 2^3 + \ldots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$, với n nguyên dương.

9. Chỉ ra rằng

$$1^2 + 3^2 + \ldots + (2n+1)^2 = \frac{(n+1)(2n+1)(2n+3)}{3},$$

với n nguyên không âm.

10. Chứng minh rằng $1.1! + 2.2! + \ldots + n.n! = (n+1)! - 1$, với n nguyên dương.

11*. Bằng quy nạp toán học hãy chứng minh **bất đẳng thức Bernoulli :** "Nếu $h > -1$ thì $1 + nh \leqslant (1+h)^n$, với mọi n nguyên không âm".

12. Chứng minh rằng $3^n \leqslant n!$ với mọi n nguyên lớn hơn 6.

13. Chứng minh rằng $2^n \geqslant n^2$ với mọi n nguyên lớn hơn 4.

14. Chứng minh bằng quy nạp rằng $n! \leqslant n^n$ với mọi n nguyên lớn hơn 1.

15. Chứng minh bằng quy nạp rằng

$$1.2 + 2.3 + \ldots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

với mọi n nguyên dương.

16. Chứng minh bằng quy nạp rằng

$$1.2.3 + 2.3.4 + \ldots + n(n+1)(n+2) = \frac{n(n+1)(n+2)(n+3)}{4}$$

với mọi n nguyên dương.

17. Chứng minh rằng

$$1^2 - 2^2 + 3^2 - \ldots + (-1)^{n-1} n^2 = \frac{(-1)^n n(n+1)}{2}$$

với mọi n nguyên dương.

18. Chứng minh rằng :

$$1 + \frac{1}{4} + \frac{1}{9} + \ldots + \frac{1}{n^2} < 2 - \frac{1}{n},$$

với mọi n nguyên lớn hơn 1.

19. Chỉ ra rằng với bất cứ bưu phí nào là một số nguyên lớn hơn 7 xu cũng có thể tạo được chỉ bằng hai loại tem 3 xu và 5 xu.

20. Chứng minh bằng quy nạp rằng $n^3 + 2n$ chia hết cho 3 với n nguyên không âm.

21. Chứng minh bằng quy nạp rằng $n^5 - n$ chia hết cho 5 với n nguyên không âm.

22. Chứng minh bằng quy nạp rằng $n^3 - n$ chia hết cho 6 với n nguyên không âm.

23*. Chứng minh bằng quy nạp rằng $n^2 - n$ chia hết cho 8 với n nguyên dương lẻ.

24. Chứng minh bằng quy nạp rằng $n^2 - 7n + 12$ là không âm với n nguyên lớn hơn 3.

25. Chứng minh bằng quy nạp rằng tập hợp n phần tử có $n(n - 1)/2$ tập con chứa đúng 2 phần tử trong đó n là số nguyên lớn hơn hay bằng 2.

26*. Chứng minh bằng quy nạp rằng tập hợp n phần tử có $n(n-1)(n-2)/6$ tập con chứa đúng 3 phần tử trong đó n là số nguyên lớn hơn hay bằng 3.

27. Sử dụng quy nạp toán học chứng minh :

$$\sum_{j=1}^{n} j^4 = \frac{n(n + 1)(2n + 1)(3n^2 + 3n - 1)}{30},$$

với n nguyên dương.

28. Với giá trị n nguyên không âm nào ta có $n^2 \leqslant n!$? Hãy chứng minh điều khẳng định của bạn bằng quy nạp toán học.

29. Với giá trị n nguyên không âm nào ta có $2n + 3 \leqslant 2^n$? Hãy chứng minh điều khẳng định của bạn bằng quy nạp toán học.

30. Sử dụng quy nạp toán học chứng minh :

$$\frac{1}{2n} \leqslant \frac{1.3.5 \ldots (2n - 1)}{2.4 \ldots 2n}$$

với n nguyên dương.

31. a) Với các con tem loại 5 xu và 6 xu có thể tạo được các bưu phí nào?

b) Chứng minh câu trả lời của bạn trong phần a) bằng quy nạp toán học.

c) Chứng minh câu trả lời của bạn trong phần a) bằng nguyên lý thứ hai của quy nạp toán học.

32. Chỉ dùng đồng 10 xu và đồng 25 xu có thể tạo được các khoản tiền là bao nhiêu? Hãy chứng minh câu trả lời của bạn bằng quy nạp toán học.

33. Máy trả tiền tự động ở ngân hàng chỉ có loại tiền 20 và loại 50 đôla. Máy có thể trả được các khoản tiền là bao nhiêu, nếu số lượng các tờ giấy bạc thuộc hai loại trên là không hạn chế. Hãy chứng minh câu trả lời của bạn bằng quy nạp toán học.

34. Giả sử rằng

$$A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

trong đó a và b là các số thực. Chứng minh rằng

$$A^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix},$$

với n là số nguyên dương tùy ý.

35. Giả sử **A** và **B** là các ma trận vuông có tính chất $\mathbf{AB} = \mathbf{BA}$. Chỉ ra rằng $\mathbf{AB}^n = \mathbf{B}^n\mathbf{A}$, với n là số nguyên dương tùy ý.

36. Giả sử m là một số nguyên dương. Dùng phương pháp qui nạp toán học chứng minh rằng a và b là hai số nguyên sao cho $a \equiv b \pmod m$, khi đó $a^k \equiv b^k \pmod m$ với k là nguyên không âm.

37. Dùng quy nạp toán học chứng minh rằng nếu $A_1, A_2, \ldots A_n$ và B là các tập hợp thì

$$(A_1 \cup A_2 \cup \ldots \cup A_n) \cap B$$

$$= (A_1 \cap B) \cup (A_2 \cap B) \cup \ldots \cup (A_n \cap B).$$

38. Chứng minh rằng nếu $A_1, A_2, \ldots A_n$ và $B_1, B_2, \ldots B_n$ là các tập hợp sao cho $A_i \subseteq B_i$ $(i = 1, 2, \ldots, n)$ khi đó :

a) $\bigcup_{i=1}^{n} A_i \subseteq \bigcup_{i=1}^{n} B_i$ b) $\bigcap_{i=1}^{n} A_i \subseteq \bigcap_{i=1}^{n} B_i$.

39. Dùng quy nạp toán học chứng minh rằng nếu A_1, A_2, ... A_n là các tập con của tập vũ trụ U thì

$$\overline{\bigcup_{k=1}^{n} A_k} = \bigcap_{k=1}^{n} \overline{A_k} .$$

40. Dùng quy nạp toán học chứng minh rằng :
$\neg(p_1 \vee p_2 \vee \ldots \vee p_n)$ là tương đương với $\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n$, trong đó p_1, p_2, ... p_2, ... p_n là các mệnh đề.

41*. Chứng minh rằng

$$[(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots \wedge (p_{n-1} \rightarrow p_n)]$$

$$\rightarrow [(p_1 \wedge p_2 \wedge \ldots \wedge P_{n-1}) \rightarrow p_n)]$$

là một hằng đúng với p_1, p_2, ... p_n là các mệnh đề.

42. Dùng công thức cho tổng các số hạng của một cấp số nhân hãy tính các tổng sau :

a) $4 + 4.3 + 4.3^2 + \ldots + 4.3^8$

b) $3 + 3.2^2 + 3.2^4 + \ldots + 3.2^{10}$

c) $1 - 2 + 2^2 - 2^3 + \ldots + (-1)^n 2^n$.

43. Sai lầm ở đâu trong "chứng minh" tất cả các con ngựa đều cùng màu như sau :

> Cho $P(n)$ là mệnh đề tất cả các con ngựa trong một tập n con ngựa là cùng màu. Rõ ràng $P(1)$ là đúng. Bây giờ giả sử $P(n)$ là đúng, tức là các con ngựa trong một tập bất kỳ có n con là cùng màu. Xét $n + 1$ con ngựa tùy ý, và đánh số các con ngựa đó là 1, 2, ..., n, $n + 1$. Dễ thấy n con ngựa đầu tiên và n con ngựa cuối cùng phải là cùng màu. Vì tập n con ngựa đầu tiên và tập n con ngựa cuối cùng là gối lên nhau, nên tất cả $n + 1$ con ngựa là cùng màu. Điều này chứng tỏ $P(n + 1)$ là đúng và chúng ta hoàn tất chứng minh bằng quy nạp.

44*. Tìm sai lầm trong "chứng minh" $a^n = 1$ với mọi n nguyên không âm, và a là số thực khác không cho dưới đây :

BƯỚC CƠ SỞ. $a^0 = 1$ là đúng, theo định nghĩa của hàm mũ.

BƯỚC QUY NẠP. Giả sử $a^k = 1$ với mọi nguyên không âm và nhỏ hơn n. Khi đó :

$$a^{n+1} = \frac{a^n . a^n}{a^{n-1}} = \frac{1.1}{1} = 1.$$

45*. Chứng minh rằng dạng thứ hai của quy nạp toán học là phương pháp có cơ sở bằng cách chỉ ra rằng nó được suy ra từ tính được sắp tốt.

46. Chứng minh rằng một biến thể sau đây của quy nạp toán học là phương pháp có cơ sở để chứng minh $P(n)$ là đúng với mọi n nguyên dương.

BƯỚC CƠ SỞ. $P(1)$ và $P(2)$ là đúng.

BƯỚC QUY NẠP. Với mọi số nguyên dương n, nếu $P(n)$ và $P(n + 1)$ cả hai đều đúng thì $P(n + 2)$ là đúng.

Trong các Bài 47 và 48, H_n ký hiệu số điều hòa thứ n.

47*. Dùng quy nạp toán học chứng minh $H_{2^n} \leq 1 + n$ với mọi n nguyên không âm.

48*. Dùng quy nạp toán học chứng minh

$$H_1 + H_2 + \ldots + H_n = (n + 1)H_n - n.$$

49*. Chứng minh rằng :

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{n}} > 2(\sqrt{n+1} - 1)$$

50*. Chứng minh rằng n đường thẳng chia mặt phẳng thành $(n^2 + n + 2)/2$ miền nếu không có hai đường thẳng nào song song và không có ba đường nào có chung một điểm.

51**. Giả sử $a_1, a_2, \ldots, a_n$ là các số thực dương hãy chứng minh bằng quy nạp :

$$\frac{a_1 + a_2 + \ldots + a_n}{n} \geq (a_1\ a_2\ \ldots\ a_n)^{1/n}.$$

52*. Dùng quy nạp toán học chứng minh rằng $4^{n+1} + 5^{2n-1}$ chia hết cho 21 với mọi n nguyên dương.

53. Dùng quy nạp toán học chứng minh Bổ đề 2 của Tiết 2.5 nói rằng p là số nguyên tố và $p \mid a_1a_2 \ldots a_n$ trong đó a_i là các số nguyên ($i = 1, 2, \ldots n$), khi đó $p \mid a_i$ với một i nguyên nào đó.

54*. Tính chất được sắp tốt có thể dùng để chứng minh rằng hai số nguyên dương a và b có chỉ một ước chung lớn nhất. Gọi S là tập các số nguyên dương dạng $as + bt$, trong đó s, t là các số nguyên.

a) Chỉ ra rằng S không rỗng.

b) Dùng tính chất được sắp tốt để chứng minh rằng S có phần tử nhỏ nhất c.

c) Chỉ ra rằng nếu d là ước chung của a và b khi đó d là ước của c.

d) Chỉ ra rằng $c \mid a$ và $c \mid b$ (*Gợi ý* : Trước tiên giả sử rằng c không là ước của a. Khi đó $a = qc + r$ trong đó $0 \leqslant r < c$. Chỉ ra rằng $r \in S$, mâu thuẫn với cách chọn c).

e) Từ c) và d) kết luận rằng tồn tại ước chung lớn nhất của a và b. Cuối cùng cần chỉ ra ước chung lớn nhất này là duy nhất.

55*. Chứng minh rằng nếu $a_1\ a_2 \ldots a_n$ là n số thực phân biệt, khi đó cần đúng $(n - 1)$ phép nhân để tính tích của n số này bất kể dấu ngoặc đơn được chèn như thế nào vào trong tích đó. (*Gợi ý* : dùng nguyên lý thứ hai của qui nạp toán học và xét phép nhân cuối cùng).

56. Bằng các miếng hình chữ L hãy lát một bàn cờ 4×4 khuyết một ô vuông ở góc trên bên trái.

57. Bằng các miếng lát hình chữ L hãy lát một bàn cờ 8×8 có một ô vuông ở góc trên bên trái bị cắt bỏ.

58. Chứng minh hoặc bác bỏ khẳng định rằng tất cả các bàn cờ có dạng cho dưới đây đều có thể được phủ hoàn toàn khi sử dụng các miếng hình chữ L, với n là số nguyên dương.

a) 3×2^n, b) 6×2^n

c) $3^n \times 3^n$, d) $6^n \times 6^n$

59*. Chứng minh rằng một bàn cờ ba chiều $2^n \times 2^n \times 2^n$ có một khối lập phương $1 \times 1 \times 1$ bị cắt bỏ có thể được lấp đầy bằng các khối lập phương $2 \times 2 \times 2$ bị khuyết một khối lập phương $1 \times 1 \times 1$.

60*. Chỉ ra rằng một bàn cờ $n \times n$ khuyết một hình vuông có thể được phủ hoàn toàn khi dùng các miếng lát hình chữ L nếu $n > 5$, n lẻ và không chia hết cho 3.

61. Cho a là một số nguyên và b là một số nguyên dương. Chỉ ra rằng các số nguyên q và r sao cho $a = dq + r$ trong đó $0 \leq r < d$, là duy nhất. (Sự tồn tại đã được chứng minh trong Ví dụ 1).

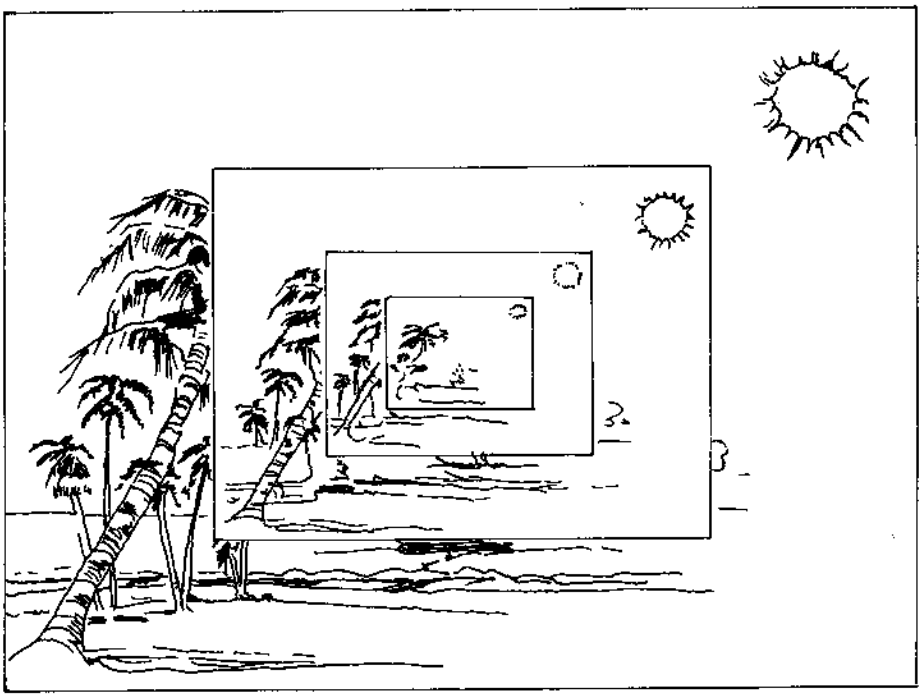
62. Dùng nguyên lý quy nạp toán học chỉ ra rằng $P(n)$ là đúng với $n = k + 1$, $k + 2$ ... với k nguyên, nếu $P(k)$ là đúng và mệnh đề kéo theo $P(n) \rightarrow P(n + 1)$ là đúng với mọi n nguyên dương và $n \geq k$.

3.3. ĐỊNH NGHĨA BẰNG ĐỆ QUY

MỞ ĐẦU

Đôi khi chúng ra rất khó định nghĩa một đối tượng một cách tường minh. Nhưng có thể dễ dàng định nghĩa đối tượng này qua chính nó. Kỹ thuật này được gọi là **đệ quy (hồi quy)**. Ví dụ, bức tranh trên Hình 1 được tạo ra bằng đệ quy. Trước tiên, cho bức tranh gốc. Sau đó lần lượt tại tâm của nó đặt chồng lên những bức tranh như thế nhưng nhỏ hơn.

Chúng ta có thể dùng đệ quy để định nghĩa các dãy số, các hàm số, và các tập hợp. Trước đây để định nghĩa một dãy số ta cho công thức tường minh của các số hạng của nó. Chẳng hạn, $a_n = 2^n$ với $n = 0, 1, 2, ...$ Nhưng cũng có thể định nghĩa dãy số này bằng cách cho số hạng đầu tiên của dãy $a_0 = 1$, và cho quy tắc tìm một số hạng của dãy qua một số hạng trước nó, ví dụ, $a_{n+1} = 2a_n$ với $n = 0, 1, 2, ...$



Hình 1. Bức tranh định nghĩa bằng đệ quy.

CÁC HÀM ĐƯỢC ĐỊNH NGHĨA BẰNG ĐỆ QUY

Để định nghĩa một hàm xác định trên tập các số nguyên không âm, chúng ta cho :

1. Giá trị của hàm tại $n = 0$.
2. Công thức tính giá trị của nó tại số nguyên n từ các giá trị của nó tại các số nguyên nhỏ hơn.

Định nghĩa như thế được gọi là **định nghĩa đệ quy** hay **định nghĩa quy nạp**.

Ví dụ 1. Giả sử f được định nghĩa bằng đệ quy như sau :

$$f(0) = 3, \quad f(n + 1) = 2f(n) + 3.$$

Hãy tìm $f(1)$, $f(2)$, $f(3)$, và $f(4)$.

Giải: Từ định nghĩa đệ quy ta suy ra :

$f(1) = 2f(0) + 3 = 2.3 + 3 = 9.$

$f(2) = 2f(1) + 3 = 2.9 + 3 = 21.$

$f(3) = 2f(2) + 3 = 2.21 + 3 = 45,$

$f(4) = 2\ f(3) + 3 = 2.45 + 3 = 93.$

■

Có nhiều hàm được định nghĩa bằng đệ quy. Chẳng hạn hàm giai thừa trong ví dụ sau.

Ví dụ 2. Hãy cho định nghĩa đệ quy của hàm giai thừa $F(n) = n\ !$.

Giải: Dễ thấy $f(0) = 1$.

Vì $(n + 1)\ ! = 1.2.3...n(n + 1) = n!(n + 1)$, nên ta có công thức $F(n + 1) = (n + 1)! = (n + 1).F(n)$ với mọi n nguyên dương.

■

Để xác định giá trị của hàm giai thừa, chẳng hạn $F(5) = 5!$, ta phải sử dụng công thức đệ quy nhiều lần.

$$F(5) = 5.F(4) = 5.4F(3) = 5.4.3F(2) = 5.4.3.2F(2) = 5.4.3.2F(1)$$

$$= 5.4.3.2.1F(0) = 5.4.3.2.1.1 = 120.$$

Ví dụ 3. Hãy cho định nghĩa đệ quy của hàm $F(n) = a^n$ trong đó a là một số thực khác không và n là nguyên không âm.

Giải: Ta cho $F(0) = a^0 = 1$.

Vì $a^{n+1} = a\ a^n$ nên $F(n + 1) = aF(n)$.

■

Ví dụ 4. Hãy cho định nghĩa đệ quy của hàm

$$F(n) = \sum_{k=0}^{n} a_k$$

Giải: Phần đầu của định nghĩa đệ quy là :

$$F(0) = \sum_{k=0}^{0} a_k = a_0$$

Phần thứ hai của định nghĩa đệ quy là :

$$F(n + 1) = \sum_{k=0}^{n+1} a_k = \left[\sum_{k=0}^{n} a_k\right] + a_{n+1} = F(n) + a_{n+1}$$

■

Trong một số định nghĩa hàm bằng đệ quy, người ta cho giá trị của hàm tại k số nguyên dương đầu tiên và cho quy tắc tính giá trị của hàm tại số nguyên lớn hơn từ k giá trị này. Theo nguyên lý thứ hai của qui nạp toán học thì cách định nghĩa này tạo ra các hàm hoàn toàn xác định (xem Bài tập 45 ở cuối tiết này).

Ví dụ 5. Dãy Fibonacci. Dãy số f_0, f_1, f_2 ... được định nghĩa hằng đệ quy như sau : $f_0 = 0$, $f_1 = 1$, và $f_n = f_{n-1} + f_{n-2}$ trong đó $n = 2, 3, 4, ...$ Hãy tính các số hạng f_2, f_3, f_4, f_5, f_6.

Giải: Trong phần đầu của định nghĩa cho $f_0 = 0$, $f_1 = 1$ nên ta suy ra :

$$f_2 = f_0 + f_1 = 0 + 1 = 1,$$
$$f_3 = f_2 + f_1 = 1 + 1 = 2,$$
$$f_4 = f_3 + f_2 = 2 + 1 = 3,$$
$$f_5 = f_4 + f_3 = 3 + 2 = 5,$$
$$f_6 = f_5 + f_4 = 5 + 3 = 8.$$

■

Chúng ta dùng định nghĩa đệ quy để chứng minh rất nhiều tính chất của dãy số này, như trong ví dụ sau.

Ví dụ 6. Chỉ ra rằng $f_n > \alpha^{n-2}$, trong đó $\alpha = \dfrac{(1+\sqrt{5})}{2}$ với $n \geq 3$.

Giải: Gọi $P(n)$ là mệnh đề "$f_n > \alpha^{n-2}$".

Rõ ràng : $\alpha < 2 = f_3$, $\alpha^2 = \dfrac{3+\sqrt{5}}{2} < 3 = f_4$,

tức là $P(3)$ và $P(4)$ là đúng. Bây giờ giả sử $P(k)$ là đúng với mọi k nguyên sao cho $3 \leq k \leq n$, trong đó $n \geq 4$. Ta cần chỉ ra $P(n + 1)$ đúng. Thật vậy, vì α nghiệm của phương trình $x^2 - x - 1 = 0$, nên suy ra $\alpha^2 = \alpha + 1$. Do đó

$$\alpha^{n-1} = \alpha^2.\alpha^{n-3} = (\alpha + 1).\alpha^{n-3} = \alpha.\alpha^{n-3} + \alpha^{n-3} = \alpha^{n-2} + \alpha^{n-3}$$

Theo giả thiết quy nạp nếu $n \geq 5$ ta suy ra

$$f_{n-1} > \alpha^{n-3}; \quad f_n > \alpha^{n-2}.$$

do vậy $f_{n+1} = f_n + f_{n-1} > \alpha^{n-2} + \alpha^{n-3} = \alpha^{n-1}$. Đó là điều cần chứng minh.

■

Bây giờ ta chỉ ra rằng thuật toán Euclid sử dụng $O(\log b)$ phép chia để tìm ƯCLN của hai số nguyên dương a và b, trong đó $a \geq b$.

ĐỊNH LÝ 1. *Định lý Lamé.*

Giả sử a, b là hai số nguyên dương, trong đó $a \geq b$. Khi đó số phép chia dùng trong thuật toán Euclid để tìm ƯCLN(a, b) sẽ nhỏ hơn hay bằng năm lần số các chữ số của b trong hệ thập phân.

Chứng minh: Giả sử a và b là hai số nguyên dương và $a \geq b$. Khi dùng thuật toán Euclid để tìm ƯCLN(a, b), ta sẽ nhận được dãy các đẳng thức sau ($a = r_0$, và $b = r_1$) :

$$r_0 = r_1 q_1 + r_2 ; \qquad 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3 ; \qquad 0 \leq r_3 < r_2$$

...

...

...

$$r_{n-2} = r_{n-1} q_{n-1} + r_n ; \; 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n ;$$

Như vậy để tìm r_n = ƯCLN(a, b) ta dùng n phép chia. Các thương q_1, q_2, ..., q_{n-1} luôn lớn hơn hay bằng 1, còn $q_n \geq 2$ vì $r_n < r_{n-1}$. Từ đó suy ra :

$$r_n \geq 1 = f_2,$$

$$r_{n-1} \geq 2r_n \geq 2 f_2 = f_3$$

$$r_{n-2} \geq r_{n-1} + r_n \geq f_3 + f_2 = f_4$$

...

$$r_2 \geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n$$

$$b = r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}.$$

Từ đó suy ra nếu n là số phép chia trong thuật toán tìm ƯCLN(a, b) thì $b \geqslant f_{n+1}$. Từ Ví dụ 6 ta có $f_{n+1} > \alpha^{n-1}$ với $n > 2$, trong đó

$$\alpha = \frac{(1+\sqrt{5})}{2}$$

Do vậy $b > \alpha^{n-1}$. Cuối cùng ta được :

$$\log_{10} b > (n-1)\log_{10}\alpha > \frac{n-1}{5} .$$

(vì $\log_{10}\alpha \sim 0.208 > \frac{1}{5}$).

Hay $n - 1 < 5.\log_{10} b$. Giả sử b là số nguyên có k chữ số, khi đó $b < 10^k$ và $\log_{10} b < k$. Do vậy $n - 1 < 5.k$, hay $n \leqslant 5k$. Đó là điều cần chứng minh.

Vì $$k = \lfloor \log_{10} b \rfloor + 1 \leqslant \log_{10} b + 1,$$

nên $$n \leqslant 5k \leqslant 5(\log_{10} b + 1) = O(\log b).$$

Vậy thuật toán Euclid để tìm ƯCLN(a, b) với mọi $a > b$ đã sử dụng $O(\log b)$ phép chia.

CÁC TẬP HỢP ĐƯỢC ĐỊNH NGHĨA BẰNG ĐỆ QUY

Các tập hợp thường được định nghĩa bằng đệ quy. Trước tiên người ta đưa ra tập xuất phát. Sau đó là quy tắc tạo các phần tử mới từ các phần tử đã biết của tập. Những tập được mô tả bằng cách như vậy được được gọi là các tập được định nghĩa tốt, các định lý về chúng có thể chứng minh bằng cách sử dụng định nghĩa đệ quy của chúng.

Ví dụ 7. Giả sử S được định nghĩa bằng đệ quy như sau :

$3 \in S$;

$x + y \in S$ nếu $x \in S$ và $y \in S$;

Hãy chỉ ra rằng S là tập các số nguyên chia hết cho 3.

Giải: Gọi A là tập các số nguyên đương chia hết cho 3. Để chứng minh $A = S$ ta sẽ chứng minh rằng A là một tập con của S và S là tập con của A. Để chứng minh A là tập con của S, ta giả sử $P(n)$ là mệnh đề "$3n$ thuộc tập S". $P(1)$ đúng vì theo định nghĩa của S "$3.1 = 3 \in S$".

Giả sử $P(n)$ đúng, tức là $3n \in S$. Vì $3 \in$ và $3n \in S$ nên theo định nghĩa $3 + 3n = 3(n + 1) \in S$. Điều này có nghĩa là $P(n + 1)$ đúng. Theo quy nạp toán học mọi số có dạng $3n$, với n nguyên dương, thuộc S, hay nói cách khác A là tập con của S.

Ngược lại, $3 \in S$, hiển nhiên 3 chia hết cho 3 nên $\in A$. Tiếp theo ta chứng minh tất cả các phần tử của S sinh ra do phần thứ hai của định nghĩa, cũng thuộc A. Giả sử x , y là hai phần tử của S, cũng là hai phần tử của A. Theo định nghĩa của S thì $x + y$ cũng là một phần tử của S, và vì x và y đều chia hết cho 3 nên $x + y$ cũng chia hết cho 3, tức là $x + y \in A$. Vậy S là tập con của A.

■

Định nghĩa tập hợp trong Ví dụ 7 là một định nghĩa đệ quy rất điển hình. Đầu tiên tập xuất phát được đưa ra. Tiếp theo là quy tắc tạo các phần tử mới từ các phần tử đã biết của tập. Sự ngầm định trong định nghĩa đệ quy này là không có phần tử nào thuộc tập đang định nghĩa, trừ phần tử đầu tiên được liệt kê trong tập đầu hoặc nó có thể được tạo ra theo quy tắc xây dựng phần tử mới.

Một trong các ứng dụng thường gặp nhất của định nghĩa đệ quy cho các tập hợp là để định nghĩa các **biểu thức được tạo đúng quy tắc** trong các hệ khác nhau. Xét ví dụ sau.

Ví dụ 8. Ta xét các biểu thức gồm các biến, các số và các toán tử cộng +, trừ −, nhân *, chia / và lũy thừa ↑ được kết hợp với nhau theo một quy tắc nào đó. Khi đó một biểu thức (được tạo) đúng quy tắc được định nghĩa như sau :

1. x là biểu thức đúng quy tắc nếu x là một số hay một biến,
2. $(f + g)$, $(f - g)$, $(f * g)$, (f / g) và $(f \uparrow g)$ là các biểu thức đúng quy tắc nếu f, g là các biểu thức đúng quy tắc.

Chẳng hạn, do x và 3 là các biểu thức đúng quy tắc, nên theo định nghĩa trên $(x + 3)$, $(x - 3)$, $(x * 3)$, $(x / 3)$ và $(x \uparrow 3)$ là các biểu thức đúng quy tắc. Tiếp theo, vì y cũng là biểu thức đúng quy tắc nên $((x + 3) + y)$, $(y - (x * 3))$ cũng là đúng qui tắc. v.v. (Lưu ý (3/0) cũng là biểu thức đúng quy tắc, vì ở đây ta chỉ quan tâm tới cú pháp).

Ví dụ 9. Các biểu thức cho mệnh đề phức hợp gồm các **T, F,** các biến mệnh đề và các toán tử $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ được định nghĩa như sau :

1. **T, F** và p, trong đó p là một biến mệnh đề, là các biểu thức đúng qui tắc.

2. $(\neg p)$, $(p \vee q)$, $(p \wedge q)$, $(p \rightarrow q)$, $(p \leftrightarrow q)$ là các biểu thức đúng nếu p và q là các biểu thức đúng quy tắc.

Chẳng hạn, nếu p, q và r là các biến mệnh đề, khi đó dùng định nghĩa đệ quy nhiều lần dễ dàng chỉ ra rằng các biểu thức

$(p \vee q)$, $(r \wedge \mathbf{T})$ and $((p \vee q) \rightarrow (r \wedge \mathbf{T}))$ là đúng quy tắc.

■

Định nghĩa đệ quy thường được dùng khi nghiên cứu các xâu ký tự. Trong Chương 1, ta đã định nghĩa **xâu** là một dãy các ký tự thuộc bộ chữ cái $\sum$. Tập hợp các xâu ứng với bộ chữ cái $\sum$ được ký hiệu bởi $\sum^*$. Hai xâu có thể kết hợp với nhau theo phép **ghép**. Ghép các xâu x và y cho xy là xâu tạo nên bằng cách viết tiếp xâu y vào xâu x. Ví dụ, cho $x = abra$, $y = cadabra$, khi đó $xy = abracadabra$. Khi chứng minh các kết quả về xâu người ta thường dùng định nghĩa đệ quy.

Ví dụ 10. *Định nghĩa đệ quy của tập các xâu*

Giả sử $\sum^*$ là tập các xâu trên bộ chữ cái $\sum$. Khi đó $\sum^*$ được định nghĩa bằng đệ quy như sau :

- $\lambda \in \sum^*$, trong đó λ là một xâu rỗng (không có phần tử nào) ;
- $wx \in \sum^*$ nếu $w \in \sum^*$ và $x \in \sum$.

Phần đầu của định nghĩa nói rằng xâu rỗng thuộc $\sum^*$. Phần sau khẳng định một xâu mới tạo nên bằng cách ghép một ký tự của $\sum$ với một xâu của $\sum^*$ cũng thuộc $\sum^*$.

■

Độ dài của xâu, tức số ký tự trong xâu, cũng được định nghĩa bằng đệ quy.

Ví dụ 11. Hãy định nghĩa bằng đệ quy độ dài của xâu w.

Giải: Ta ký hiệu độ dài của w là $l(w)$. Khi đó định nghĩa đệ quy của $l(w)$ như sau :

- $l(\lambda) = 0$, trong đó λ là xâu rỗng :
- $l(wx) = l(w) + 1$ nếu $w \in \sum^*$ và $x \in \sum$.

■

Ví dụ 12. Sử dụng quy nạp toán học chứng minh

$$l(xy) = l(x) + l(y),$$

trong đó x và y là các xâu thuộc $\sum^*$.

Giải: Gọi $P(y)$ là mệnh đề $l(xy) = l(x) + l(y)$ với x, y thuộc $\sum^*$.

BƯỚC CƠ SỞ. Dễ kiểm tra rằng $P(\lambda)$ là đúng vì

$$l(x\lambda) = l(x) + 0 = l(x) + l(\lambda) \text{ với mọi xâu } x.$$

BƯỚC QUY NẠP. Giả sử $P(y)$ là đúng, ta phải chứng minh $P(ya)$ đúng với mọi $a \in \sum$ tức là $l(xya) = l(x) + l(ya)$. Theo định nghĩa độ dài của xâu ta có

$$l(xya) = l(xy) + 1 \text{ và } l(ya) = l(y) + 1.$$

Theo giả thiết của phép qui nạp $l(xy) = l(x) + l(y)$

ta có $l(xya) = l(x) + l(y) + 1 = l(x) + l(ya)$

Đó là điều cần chứng minh.

BÀI TẬP

1. Hãy tìm $f(1)$, $f(2)$, $f(3)$, và $f(4)$, nếu $f(n)$ được định nghĩa bằng đệ quy với $f(0) = 1$ và với $n = 0, 1, 2, \ldots$

   a) $f(n + 1) = f(n) + 2$.

   b) $f(n + 1) = 3f(n)$.

   c) $f(n + 1) = 2^{f(n)}$

   d) $f(n + 1) = (f(n))^2 + f(n) + 1$.

2. Hãy tìm $f(1)$, $f(2)$, $f(3)$, $f(4)$ và $f(5)$, nếu $f(n)$ được định nghĩa đệ quy với $f(0) = 3$ và với $n = 0, 1, 2, \ldots$

   a) $f(n + 1) = -2f(n)$.

   b) $f(n + 1) = 3f(n) + 7$.

   c) $f(n + 1) = (f(n))^2 - 2f(n) - 2$.

   d) $f(n + 1) = 3^{f(n)/3}$.

3. Hãy tìm $f(2)$, $f(3)$, $f(4)$ và $f(5)$ nếu $f(n)$ được định nghĩa bằng đệ quy với $f(0) = -1$, $f(1) = 2$ và với $n = 1, 2, \ldots$

   a) $f(n + 1) = f(n) + 3f(n - 1)$.

   b) $f(n + 1) = f(n)^2 f(n - 1)$.

   c) $f(n + 1) = 3f(n)^2 - 4f(n - 1)^2$.

   d) $f(n + 1) = f(n - 1)/f(n)$.

4. Hãy tìm $f(2)$, $f(3)$, $f(4)$ và $f(5)$, nếu $f(n)$ được định nghĩa bằng đệ quy với $f(0) = f(1) = 1$ và với $n = 0, 1, 2, \ldots$

a) $f(n + 1) = f(n) - f(n - 1)$.

b) $f(n + 1) = f(n)f(n - 1)$.

c) $f(n + 1) = f(n)^2 + f(n - 1)^3$.

d) $f(n + 1) = f(n) / f(n - 1)$.

5. Hãy cho định nghĩa đệ quy của dãy $\{a_n\}$, $n = 1, 2 \ldots$ nếu

a) $a_n = 6n$; b) $a_n = 2n + 1$;

c) $a_n = 10^n$; d) $a_n = 5$.

6. Hãy định nghĩa đệ quy của dãy $\{a_n\}$, $n = 1, 2, \ldots$ nếu

a) $a_n = 4n - 2$; b) $a_n = 1 + (-1)^n$;

c) $a_n = n(n + 1)$; d) $a_n = n^2$.

7. Cho F là hàm sao cho $F(n)$ là tổng của n số nguyên dương đầu tiên. Hãy đưa ra định nghĩa đệ quy của $F(n)$.

8. Hãy đưa ra định nghĩa đệ quy của $S_m(n)$ là tổng của số nguyên m và số nguyên không âm n.

9. Hãy đưa ra định nghĩa đệ quy của $P_m(n)$ là tích của số nguyên m và số nguyên không âm n.

Trong các Bài tập từ 10 - 17, f_n là số Fibonacci thứ n.

10. Chứng minh rằng $f_1^2 + f_2^2 + \ldots + f_n^2 = f_n f_{n+1}$, với n nguyên dương.

11. Chứng minh rằng $f_1 + f_3 + \ldots + f_{2n-1} = f_{2n}$, với n nguyên dương.

12*. Chứng minh rằng $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$, với n nguyên dương.

13*. Chỉ ra rằng $f_0 f_1 + f_1 f_2 + \ldots + f_{2n-1} f_{2n} = f_{2n}^2$, với n nguyên dương.

14*. Chỉ ra rằng $f_0 - f_1 + f_2 - \ldots - f_{2n-1} + f_{2n} = f_{2n-1} - 1$, với n nguyên dương.

15. Xác định số phép chia cần dùng trong thuật toán Euclid tìm ƯCLN của các số Fibonacci f_n và f_{n+1} với n nguyên dương. Dùng quy nạp kiểm tra kết quả của bạn.

16. Cho

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Chứng tỏ rằng $\mathbf{A}^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$

với mọi n nguyên dương.

17. Bằng cách tính định thức hai vế của phương trình trong Bài tập 16, chứng minh đẳng thức trong Bài 12.

18*. Hãy đưa ra định nghĩa đệ quy của hàm max và min sao cho $\max(a_1, a_2, \ldots a_n)$ và $\min(a_1, a_2, \ldots a_n)$ tương ứng là số lớn nhất và bé nhất của n số $a_1, a_2, \ldots a_n$.

19*. Cho $a_1, a_2, \ldots a_n$ và $b_1, b_2, \ldots b_n$ là các số thực. Dùng định nghĩa đệ quy mà bạn đã đưa ra trong Bài tập 18, chứng minh :

a) $\max(-a_1, -a_2, \ldots, -a_n) = -\min(a_1, a_2, \ldots, a_n)$.

b) $\max(a_1+b_1, a_2+b_2, \ldots, a_n+b_n) \leqslant \max(a_1, a_2, \ldots, a_n) + \max(b_1, b_2, \ldots b_n)$.

c) $\min(a_1+b_1, a_2+b_2, \ldots, a_n+b_n) \geqslant \min(a_1, a_2, \ldots, a_n) + \min(b_1, b_2, \ldots b_n)$.

20. Gọi S là tập được định nghĩa như sau :
$1 \in S$, và $s + t \in S$, nếu $s \in S$ và $t \in S$.
Chứng minh rằng S là tập các số nguyên dương.

21. Hãy cho định nghĩa đệ quy của tập các số nguyên dương là bội của 5.

22. Cho định nghĩa đệ quy của :

a) tập các số nguyên lẻ.

b) tập các lũy thừa nguyên dương của 3.

c) tập các đa thức với hệ số nguyên.

23. Cho định nghĩa đệ quy của :

a) tập các số nguyên dương chẵn.

b) tập các số nguyên dương đồng dư với 2 theo modun 3.

c) tập các số nguyên dương không chia hết cho 5.

24. Chứng tỏ rằng một biểu thức đúng quy tắc bất kỳ gồm các số, các biến, và các toán tử $\{+, -, *, /, \uparrow\}$ sẽ chứa cùng một số dấu mở ngoặc và dấu đóng ngoặc.

25. Hãy định nghĩa một biểu thức đúng quy tắc của các tập hợp, các biến biểu diễn tập hợp, và các toán tử $\{\bar{}, \cup, \cap, -\}$.

Đảo *của một xâu là một xâu gồm các ký tự của xâu ban đầu nhưng với thứ tự ngược lại. Ta ký hiệu xâu đảo của xâu w là xâu w^R.*

26. Tìm xâu đảo của các xâu sau đây :

a) 0101
b) 11011
c) 10001 00101 11

27. Hãy đưa ra định nghĩa xâu đảo bằng đệ quy. (*Gợi ý* : Trước tiên định nghĩa đảo của xâu rỗng. Sau đó viết xâu w độ dài $n + 1$ dưới dạng xy, với x là xâu độ dài n và biểu diễn xâu đảo w qua x^R và y).

28*. Hãy cho một chứng minh đệ quy rằng $(w_1w_2)^R = w_2^R w_1^R$.

29. Hãy định nghĩa bằng đệ quy w^i trong đó i là một số nguyên không âm (với w^i biểu diễn phép ghép i bản sao của xâu w).

30*. Hãy định nghĩa bằng đệ quy tập các xâu nhị phân thuận nghịch độc.

31. Khi nào một xâu thuộc vào tập A gồm các xâu nhị phân và được định nghĩa như sau :
$\lambda \in A$, $0x1 \in A$ nếu $x \in A$, trong đó λ là một xâu rỗng?

32*. Định nghĩa bằng đệ quy tập các xâu nhị phân nhiều bit 0 hơn bit 1.

33. Dùng Bài tập 29 và quy nạp toán học để chỉ ra rằng $l(w^i) = i.l(w)$, trong đó w là một xâu và i là một số nguyên không âm.

34*. Chỉ ra rằng $(w^R)^i = (w^i)^R$ trong đó w là một xâu, i là một số nguyên không âm, tức là chứng minh rằng lũy thừa bậc i của một xâu đảo của một xâu là xâu đảo của xâu lũy thừa bậc i.

35*. Một **phân hoạch** của số nguyên dương n là một cách viết n như là tổng của các số nguyên dương. Ví dụ, $7 = 3 + 2 + 1 + 1$ là một phân hoạch của 7. Cho P_m bằng số các phân hoạch khác nhau của m, trong đó không kể tới thứ tự của các số hạng trong tổng và $P_{m,n}$ là số các biểu diễn khác nhau của m thành tổng của các số nguyên dương không vượt quá n.

a) Chỉ ra rằng $P_{m,m} = P_m$.

b) Chỉ ra rằng định nghĩa đệ quy sau đây cho $P_{m,n}$ là đúng.

$$P_{m,n} = \begin{cases} 1 & \text{if } m = 1 \\ 1 & \text{if } n = 1 \\ P_{n,m} & \text{if } m < n \\ 1 + P_{m,m-1} & \text{if } m = n > 1 \\ P_{m,n-1} + P_{m-n,n} & \text{if } m > n > 1 \end{cases}$$

c) Tìm số phân hoạch của 5 và 6 bằng cách sử dụng định nghĩa đệ quy trên.

Ta sẽ nghiên cứu định nghĩa đệ quy sau đây của hàm **Akermann**. *Hàm này đóng một vai trò quan trọng trong lý thuyết hàm đệ quy và trong nghiên cứu độ phức tạp của một một số thuật toán có chứa hợp của tập hợp.*

$$A(m, n) = \begin{cases} 2n & \text{if } m = 0 \\ 0 & \text{if } m \geq 1 \text{ và } n = 0 \\ 2 & \text{if } m \geq 1 \text{ và } n = 1 \\ A(m-1, A(m, n-1)) & \text{if } m \geq 1 \text{ và } n \geq 2. \end{cases}$$

Các Bài tập từ 36 đến 43 sử dụng định nghĩa này của hàm *Akermann*.

36. Tính các giá trị :

a) $A(1,0)$ b) $A(0,1)$

c) $A(1,1)$ d) $A(2,2)$.

37. Chỉ ra rằng $A(m, 2) = 4$ với mọi $m \geq 1$.

38. Chỉ ra rằng $A(1, n) = 2^n$ với mọi $n \geq 1$.

39. Tính

a) $A(2, 3)$

b*) $A(3, 3)$

40*. Tìm $A(3,4)$.

41.** Chứng minh rằng $A(m, n + 1) > A(m,n)$, với mọi m, n nguyên không âm.

42*. Chứng minh rằng $A(m + 1, n) \geqslant A(m, n)$, với mọi m, n nguyên không âm.

43. Chứng minh rằng $A(i, j) \geqslant j$ với mọi i, j nguyên không âm.

44. Giả sử hàm F được định nghĩa bằng cách cho $F(0)$ và một quy tắc để tính $F(n + 1)$ từ $F(n)$. Dùng quy nạp toán học chứng minh rằng F là một hàm được định nghĩa tốt.

45. Giả sử hàm F được định nghĩa bằng cách cho $F(0)$ và một quy tắc để tính $F(n + 1)$ từ các giá trị $F(k)$, với $k = 0, 1, 2, \ldots, n$. Dùng nguyên lý thứ hai quy nạp toán học chứng minh rằng F là một hàm được định nghĩa tốt.

3.4. CÁC THUẬT TOÁN ĐỆ QUY

MỞ ĐẦU

Đôi khi chúng ta có thể quy việc giải bài toán với tập các dữ liệu đầu vào xác định về việc giải cùng bài toán đó nhưng với các giá trị đầu vào nhỏ hơn. Ví dụ, bài toán tìm ƯCLN của hai số a, b với $b > a$, có thể rút gọn về bài toán tìm ƯCLN của hai số nhỏ hơn, b **mod** a và a vì ƯCLN(b **mod** a, a) = ƯCLN(a, b). Khi việc rút gọn như vậy thực hiện được thì lời giải bài toán ban đầu có thể tìm được bằng một dãy các phép rút gọn cho tới những trường hợp mà ta có thể dễ dàng nhận được lời giải của bài toán. Ví dụ, trong bài toán tìm ƯCLN(a, b), việc rút gọn sẽ tiếp tục cho tới khi số nhỏ hơn trong hai số bằng không, vì ƯCLN(0, a) = a với $a > 0$.

Chúng ta sẽ thấy rằng các thuật toán rút gọn liên tiếp bài toán ban đầu tới bài toán có dữ liệu đầu vào nhỏ hơn, được áp dụng trong một lớp rất rộng các bài toán.

ĐỊNH NGHĨA 1. Một thuật toán được gọi là *đệ quy* nếu nó giải bài toán bằng cách rút gọn liên tiếp bài toán ban đầu tới bài toán cũng như vậy nhưng có dữ liệu đầu vào nhỏ hơn.

Ví dụ 1. Tìm thuật toán đệ quy tính giá trị a^n với a là số thực khác không và n là số nguyên không âm.

Giải: Ta xây dựng thuật toán đệ quy nhờ định nghĩa đệ quy của a^n, đó là $a^{n+1} = a.a^n$ với $n > 0$ và khi $n = 0$ thì $a^0 = 1$. Vậy để tính a^n ta quy về các trường hợp có số mũ n nhỏ hơn, cho tới khi $n = 0$. Xem Thuật toán 1 sau đây :

■

THUẬT TOÁN 1. THUẬT TOÁN ĐỆ QUY TÍNH a^n.

procedure *power* (*a* : số thực khác không; *n* : số nguyên không âm)

if *n* = 0 **then** *power*(a, *n*) := 1

else power(*a.n*) := *a* * *power*(*a*, *n* − 1)

Ví dụ 2. Tìm thuật toán đệ quy tính ƯCLN của hai số nguyên a, b không âm và $a < b$.

Giải: Vì ƯCLN(*a, b*) = ƯCLN(*b* **mod** *a*, *a*) và điều kiện ƯCLN(0, *b*) = *b* nên ta có thể xây dựng thuật toán tìm ƯCLN như sau

■

THUẬT TOÁN 2 THUẬT TOÁN ĐỆ QUY TÍNH ƯCLN(*a, b*).

procedure *ƯCLN (a, b : các số nguyên không âm, a < b)*

if *a* = 0 **then** *ƯCLN (a, b)* := *b*

else *ƯCLN (a, b)* : = *ƯCLN (b* **mod** *a, a)*

Ví dụ 3. Hãy biểu diễn thuật toán tìm kiếm tuyến tính như một thủ tục đệ quy.

Giải: Để tìm x trong dãy tìm kiếm $a_1, a_2, \ldots a_n$ trong bước thứ i của thuật toán ta so sánh x với a_i. Nếu x bằng a_i thì i là vị trí cần tìm, ngược lại thì việc tìm kiếm được quy về dãy có số phần tử ít hơn, cụ thể là dãy $a_{i+1}, \ldots, a_n$. Thuật toán tìm kiếm có dạng thủ tục đệ quy như sau.

Cho *search*(*i*, *j*, *x*) là thủ tục tìm số x trong dãy a_i, a_{i+1}, ..., a_j. Dữ liệu đầu vào là bộ ba (1, *n*, *x*). thủ tục sẽ dừng khi số hạng đầu tiên của dãy còn lại là x hoặc là khi dãy còn lại chỉ có một phần tử khác x. Nếu x không là số hạng đầu tiên và còn có các số hạng khác thì lại áp dụng thủ tục này, nhưng dãy tìm kiếm ít hơn một phần tử nhận được bằng cách xóa đi phần tử đầu tiên của dãy tìm kiếm ở hước vừa qua.

THUẬT TOÁN 3. THUẬT TOÁN ĐỆ QUY TÌM KIẾM TUYẾN TÍNH.

procedure *search (i, j, x)*

if $a_i = x$ **then** vị trí := *i*

else if *i* = *j* **then** vị trí := 0

else *search (i + 1, j, x)*

■

Ví dụ 4. Hãy xây dựng phiên bản đệ quy của thuật toán tìm kiếm nhị phân.

Giải. Giả sử ta muốn định vị x trong dãy a_1, a_2 ..., a_n bằng tìm kiếm nhị phân. Trước tiên ta so sánh x với số hạng giữa, $a_{\lfloor (n+1)/2 \rfloor}$. Nếu chúng bằng nhau thì thuật toán kết thúc, nếu không ta chuyển sang tìm kiếm trong dãy ngắn hơn, nửa đầu của dãy nếu x nhỏ hơn giá trị giữa của dãy xuất phát, nửa sau nếu ngược lại. Như vậy ta rút gọn việc giải bài toán tìm kiếm về việc giải cũng bài toán đó nhưng trong dãy tìm kiếm có độ dài lần lượt giảm đi một nửa. Ta có thuật toán 4.

THUẬT TOÁN 4. THUẬT TOÁN ĐỆ QUY TÌM KIẾM NHỊ PHÂN.

procedure *binary search (x, i, j)*

$m := \lfloor (i + j)/2 \rfloor$

if $x = a_m$ **then** vị trí := *m*

else if ($x < a_m$ *and* $i < m$) **then** *binary search (x, i, m − 1)*

else if ($x > a_m$ *and* $j > m$) **then** *binary search (x, m + 1, j)*

else vị trí := 0

ĐỆ QUY VÀ LẶP

Định nghĩa đệ quy biểu diễn giá trị của hàm tại một số nguyên qua giá trị của nó tại các số nguyên nhỏ hơn. Điều này có nghĩa là ta có thể xây dựng một thuật toán đệ quy tính giá trị của hàm được định nghĩa bằng đệ quy tại một điểm nguyên.

Ví dụ 5. Thủ tục đệ quy sau đây cho ta giá trị của n ! với n nguyên dương.

THUẬT TOÁN 5. THỦ TỤC ĐỆ QUY TÍNH GIAI THỪA.

procedure *factorial* (n : nguyên dương)

if $n = 1$ **then** *factorial(n)* := 1

else *factorial(n)* := n * *factorial*($n - 1$)

Có cách khác tính hàm giai thừa của một số nguyên từ định nghĩa đệ quy của nó. Thay cho việc lần lượt rút gọn việc tính toán cho các giá trị nhỏ hơn, chúng ta có thể xuất phát từ giá trị của hàm tại 1 và lần lượt áp dụng định nghĩa đệ quy để tìm giá trị của hàm tại các số nguyên lớn dần. Đó là **thủ tục lặp**. Nói cách khác để tìm $n!$ ta xuất phát từ $n! = 1$ (với $n = 1$), tiếp theo lần lượt nhân với các số nguyên cho tới khi bằng n. Xem Thuật toán 6.

THUẬT TOÁN 6. THỦ TỤC LẶP TÍNH GIAI THỪA.

procedure Iterative factorial (n : nguyên dương) ;

x := 1

for i := 1 **to** n

x := i * x

{x là $n!$}

Sau khi thi hành đoạn mã này giá trị của biến x là $n!$, ví dụ, sau khi đi qua vòng lặp 6 lần $x = 6! = 1.2.3.4.5.6 = 720$.

Thông thường để tính một dãy các giá trị được định nghĩa bằng đệ quy, nếu dùng phương pháp lặp thì số các phép tính sẽ ít hơn là dùng thuật toán đệ quy (trừ khi dùng các máy đệ quy chuyên dụng). Chúng ta sẽ xem xét bài toán tính các số hạng thứ n của dãy Fibonacci.

THUẬT TOÁN 7. THỦ TỤC ĐỆ QUY TÍNH CÁC SỐ FIBONACCI.

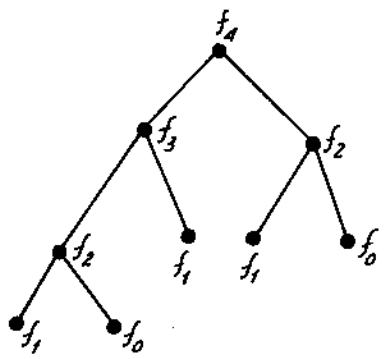
procedure *fibonacci* (n : nguyên không âm)

if $n = 0$ **then** *fibonacci*(0) := 0

else if $n = 1$ **then** *fibonacci*(1) := 1

else *fibonacci*(n) := *fibonacci*($n - 1$) + *fibonacci*($n - 2$)

Theo thuật toán này, để tìm f_n ta biểu diễn $f_n = f_{n-1} + f_{n-2}$. Sau đó thay thế cả hai số này bằng tổng của hai số Fibonacci bậc thấp hơn, cứ tiếp tục như vậy cho tới khi f_0 và f_1 xuất hiện thì được thay bằng các giá trị của chúng theo định nghĩa.



Hình 1. Ước lượng f_4 bằng đệ quy.

Mỗi giai đoạn đệ quy cho tới khi f_0 và f_1 xuất hiện, các số Fibonacci được tính hai lần. Chẳng hạn khi $n = 4$, trên Hình 1, giản đồ cây gồm có gốc với nhãn f_4, và các cành từ gốc được gán nhãn f_3 và f_2 vì chúng xuất hiện trong công thức đệ quy tính f_4. Mỗi nhánh này lại sinh ra hai nhánh con của cây. Sự phân nhánh sẽ kết thúc khi f_0 và f_1 được sinh ra. Độc giả có thể kiểm tra lại rằng để tìm f_n cần $(f_{n+1} - 1)$ phép cộng.

Bây giờ ta tính số các phép toán cần dùng để tính f_n khi sử dụng phương pháp lặp.

Thuật toán này khởi tạo x như $f_0 = 0$ và y như $f_1 = 1$. Khi vòng lặp được duyệt qua tổng của x và y được gán cho biến phụ z. Sau đó x được gán giá trị của y và y được gán giá trị của z. Vậy sau khi đi qua vòng lặp lần 1, ta có $x = f_1$ và $y = f_0 + f_1 = f_2$. Khi qua vòng lặp $n - 1$

lần thì $x = f_{n-1}$. Như vậy chỉ có $n-1$ phép cộng được dùng để tìm f_n khi $n > 1$.

THUẬT TOÁN 8. THỦ TỤC LẶP TÍNH CÁC SỐ FIBONACCI.

```
procedure Iterative fibonacci (n : nguyên không âm) ;
if n := 0 then y := 0
else
begin
    x := 0 ; y := 1
    for i := 1 to (n - 1)
    begin
        z := x + y
        x := y ; y := z
    end ;
end ; {y là số Fibonacci thứ n}
```

Chúng ta đã chỉ ra rằng số các phép toán dùng trong thuật toán đệ quy nhiều hơn khi dùng phương pháp lặp. Tuy nhiên đôi khi người ta vẫn thích dùng thủ tục đệ quy hơn ngay cả khi nó tỏ ra kém hiệu quả so với thủ tục lặp. Đặc biệt, có những bài toán chỉ có thể giải bằng thủ tục đệ quy mà không thể giải bằng thủ tục lặp.

BÀI TẬP

1. Hãy cho thuật toán đệ qui tính nx với mọi n nguyên dương và x nguyên.
2. Hãy cho thuật toán đệ qui tìm tổng n số nguyên dương đầu tiên.
3. Hãy cho thuật toán đệ qui tìm tổng n số nguyên dương lẻ đầu tiên.
4. Hãy cho thuật toán đệ qui tìm số cực đại của tập hữu hạn các số nguyên.
5. Hãy cho thuật toán đệ qui tìm số cực tiểu của tập hữu hạn các số nguyên.

6. Mô tả thuật toán đệ quy tìm x^n **mod** m với n, x, m là các số nguyên dương.

7. Hãy đưa ra thuật toán đệ quy tìm $n!$ **mod** m trong đó m, n là các số nguyên dương.

8. Hãy đưa ra thuật toán đệ quy tìm **mod** của một danh sách các số nguyên. (**mod** là một phần tử của danh sách ít nhất có tần xuất xuất hiện các như phần tử khác của danh sách.

9. Hãy nghĩ ra thuật toán đệ quy tìm ƯCLN của số nguyên không âm a, b ($a < b$) nếu dùng đẳng thức ƯCLN(a, b) = ƯCLN(a, $b - a$).

10. Hãy nghĩ ra thuật toán đệ quy tính a^{2^n} trong đó a là một số thực và n là một số nguyên dương. (*Gợi ý* : Dùng đẳng thức $a^{2^{n+1}} = (a^{2^n})^2$).

11. Hãy so sánh số các phép nhân dùng trong Thuật toán ở Bài tập 10 với số phép nhân dùng trong Thuật toán 1 để tính a^{2^n}?

12*. Dùng Thuật toán ở Bài tập 10 để nghĩ ra một thuật toán tính a^n với n nguyên không âm. (*Gợi ý* : Sử dụng biểu diễn nhị phân của n).

13*. Hãy so sánh số các phép nhân dùng trong Thuật toán ở Bài 12 với số phép nhân dùng trong Thuật toán 1 để tính a^n?

14. Bao nhiêu phép cộng được dùng bởi các thuật toán đệ quy và thuật toán lặp trong Thuật toán 7 và 8 để tìm số Fibonacii f_7.

15. Hãy nghĩ ra thuật toán đệ quy tìm số hạng thứ n của dãy được xác định như sau :
$a_0 = 1$, $a_1 = 2$ và $a_n = a_{n-1}a_{n-2}$ với $n = 2, 3, 4,...$

16. Hãy nghĩ ra Thuật toán lặp tìm số hạng thứ n của dãy được xác định trong Bài tập 15.

17. Thuật toán đệ quy hay thuật toán lặp tìm số hạng thú n của dãy trong Bài tập 15 là có hiệu quả hơn?

18. Hãy nghĩ ra thuật toán đệ quy tìm số hạng của dãy được xác định như sau : $a_0 = 1$, $a_1 = 2$, $a_2 = 3$ và $a_n = a_{n-1} + a_{n-2} + a_{n-3}$, với $n = 3, 4, 5, ...$

19. Hãy nghĩ ra thuật toán lặp tìm số hạng thứ n của dãy được xác định trong Bài tập 18.

20. Thuật toán đệ quy hay thuật toán lặp tìm dãy số trong Bài tập 18 là có hiệu quả hơn?

21. Hãy đưa ra thuật toán đệ quy và thuật toán lặp tìm số hạng thứ n của dãy được xác định như sau : $a_0 = 1$, $a_1 = 3$, $a_2 = 5$ và $a_n = a_{n-1}.(a_{n-2})^2.(a_{n-3})^3$, với $n = 4, 5, ...$
Thuật toán nào hiệu quả hơn?

22. Hãy nghĩ ra thuật toán đệ quy tìm số các phân hoạch của một số dương định nghĩa hằng đệ quy cho trong Bài tập 35 của Tiết 3.3.

23. Hãy đưa ra thuật toán đệ quy tìm xâu nghịch đảo của xâu nhị phân (Xem phần mở đầu của Bài tập 26 trong Tiết 3.3).

24. Hãy cho định nghĩa đệ quy tìm xâu w^i, là ghép của i bản sao của w, với w là xâu nhị phân.

25. Hãy cho thuật toán đệ quy tìm giá trị của hàm Akermann (*Gợi ý* : Xem phần ở đầu của Bài tập 36 trong Tiết 3.3).

3.5. TÍNH ĐÚNG ĐẮN CỦA CHƯƠNG TRÌNH

MỞ ĐẦU

Giả sử rằng chúng ta đã thiết kế được một thuật toán để giải một bài toán nào đó và đã viết chương trình để thể hiện nó. Liệu ta có thể tin chắc rằng chương trình có luôn luôn cho lời giải đúng hay không? Sau khi tất cả các sai sót về mặt cú pháp đã được loại bỏ, chúng ta có thể thử chương trình với các đầu vào mẫu. Nó không đúng nếu cho kết quả sai với đầu vào mẫu nào đó. Tuy nhiên, ngay cả khi chương trình cho kết quả đúng với tất cả đầu vào mẫu, nó vẫn có thể không luôn luôn tạo ra các câu trả lời đúng (trừ khi tất cả các đầu vào có thể đã được thử). Chúng ta cần phải chứng minh rằng chương trình *luôn luôn* cho đầu ra đúng.

Việc kiểm chứng chương trình, chứng minh tính đúng đắn của chương trình, dùng các quy tắc suy diễn và các kỹ thuật chứng minh đã được mô tả trong chương này, kể cả quy nạp toán học. Vì chương trình không đúng có thể dẫn tới các hiệu ứng rất tồi tệ, nên một số rất lớn các phương pháp luận đã được xây dựng để kiểm chứng chương trình. Đã có nhiều cố gắng giành cho việc chứng minh tự động chương trình sao cho nó có thể thực hiện được trên máy tính. Tuy nhiên, những kết quả đạt được theo hướng này còn rất hạn chế. Thật vậy, nhiều nhà toán học và lý thuyết máy tính đã khẳng định rằng sẽ không bao giờ thực hiện được việc tự động chứng minh tính đúng đắn của những chương trình phức tạp.

Một vài khái niệm và phương pháp thường dùng để chứng minh một chương trình là đúng đắn sẽ được bàn tới trong tiết này. Tuy nhiên, phương pháp luận đầy đủ của việc kiểm chứng chương trình sẽ không được trình bày trong cuốn sách này. Tiết này chỉ là phần nhập môn ngắn gọn vào lĩnh vực kiểm chứng chương trình, nó sẽ gắn các quy tắc suy luận, các kỹ thuật chứng minh và khái niệm thuật toán lại với nhau.

KIỂM CHỨNG CHƯƠNG TRÌNH

Một chương trình gọi là đúng đắn nếu với mọi đầu vào khả dĩ, nó cho đầu ra đúng. Việc chứng minh tính đúng đắn của chương trình gồm hai phần. Phần đầu chỉ ra rằng nếu chương trình kết thúc thì nhận được kết quả đúng. Phần này xác minh tính **đúng đắn bộ phận** của chương trình. Phần thứ hai chứng tỏ chương trình luôn luôn là kết thúc.

Để định rõ thế nào là một chương trình cho thông tin ra đúng người ta thường dùng hai mệnh đề sau. Thứ nhất là **khẳng định đầu**, nó đưa ra những tính chất mà thông tin đầu vào cần phải có. Mệnh đề thứ hai là **khẳng định cuối**, nó đưa ra những tính chất mà thông tin đầu ra cần phải có, tùy theo mục đích của chương trình. Khi kiểm tra chương trình cần phải chuẩn bị các khẳng định đầu và khẳng định cuối thích hợp.

ĐỊNH NGHĨA 1. Chương trình hay đoạn chương trình S được gọi là *đúng đắn bộ phận* đối với khẳng định đầu p và khẳng định cuối q, nếu p là đúng với các giá trị vào của S và nếu S kết thúc thì q là đúng với các giá trị ra của S. Ký hiệu $p\{S\}q$ có nghĩa là chương trình hay đoạn chương trình S là đúng đắn bộ phận đối với khẳng định đầu p và khẳng định cuối q.

Chú ý là khái niệm đúng đắn bộ phận không đề cập tới việc chương trình có kết thúc hay không. Nó chỉ nhằm kiểm tra xem chương trình có làm được cái mà nó định làm hay không, nếu nó kết thúc.

Ví dụ đơn giản sau đây minh họa các khái niệm khẳng định đầu và khẳng định cuối.

Ví dụ 1. Chỉ ra rằng đoạn chương trình

$y := 2$

$z := x + y$

là đúng đắn đối với khẳng định đầu p: $x = 1$ và khẳng định cuối q: $z = 3$.

Giải: Giả sử p đúng, tức là $x = 1$ lúc bắt đầu chương trình. Sau đó y được gán giá trị 2, còn z được gán tổng các giá trị của x và y, tức là 3. Vậy nếu S kết thúc thì q đúng. Theo định nghĩa, S là đúng đắn đối với khẳng định đầu p và khẳng định cuối q hay $p\{S\}q$ là đúng.

■

CÁC QUY TẮC SUY LUẬN

Một quy tắc suy luận rất có ích khi chứng minh một chương trình là đúng đó là phân chia nó thành dãy các đoạn chương trình (các chương trình con) và chứng minh mỗi đoạn chương trình là đúng.

Giả sử chương trình S được phân chia thành các đoạn chương trình S_1, S_2 và ta viết là $S = S_1 ; S_2$ với ý nghĩa S được tạo bởi S_1, tiếp theo là S_2. Giả sử tính đúng đắn của S_1 đối với khẳng định đầu p và khẳng định cuối q, và tính đúng đắn của S_2 đối với khẳng định đầu q và khẳng định cuối r đã được chứng minh. Từ đó suy ra nếu p đúng và S_1 được thi hành và kết thúc, thì q là đúng, và nếu q đúng và S_2 được thi hành và kết thúc, thì r là đúng. Như vậy, nếu p là đúng và $S = S_1 ; S_2$ được thi hành và kết thúc thì r là đúng. Quy tắc suy luận này có tên là **quy tắc hợp thành** có thể diễn đạt như sau :

$p\{S_1\}q$
$q\{S_2\}r$

$\therefore p\{S_1 ; S_2\}r$

Quy tắc suy luận này sẽ được sử dụng trong tiết này.

Chúng ta sẽ trình bày một số quy tắc suy luận nữa dùng cho các chương trình có chứa các câu lệnh điều kiện và các vòng lặp. Vì chương trình có thể phân chia thành các đoạn để chứng minh tính đúng đắn của nó, nên điều đó cho phép ta kiểm chứng được nhiều chương trình khác nhau.

CÂU LỆNH ĐIỀU KIỆN

Trước tiên, chúng ta sẽ trình bày những quy tắc suy luận đối với câu lệnh điều kiện. Giả sử một đoạn chương trình có dạng :

---

if *điều_kiện* **then**

S

---

trong đó S là một khối lệnh. Khối S sẽ được thi hành nếu *điều kiện* là đúng, và S sẽ không được thi hành và nếu *điều kiện* là sai. Để kiểm chứng tính đúng đắn của đoạn này đối với khẳng định cuối q ta phải làm hai việc. Đầu tiên phải chỉ ra khi p đúng và *điều kiện* đúng thì q đúng sau khi S kết thúc. Sau đó phải chứng minh rằng khi p đúng và *điều kiện* sai thì q đúng (vì trong trường hợp này S không thi hành).

Điều đó dẫn tới quy tắc suy luận sau :

$$(p \wedge \textit{điều kiện})\ \{S\}\ q$$
$$(p \wedge \neg \textit{điều kiện}) \rightarrow q$$

$$\therefore\ p\{\textbf{if } \textit{điều kiện } \textbf{then } S\}\ q$$

Ví dụ sau minh họa cách sử dụng quy tắc suy luận này.

Ví dụ 2. Hãy chứng tỏ đoạn chương trình

---

if $x > y$ **then**

$y := x$

---

là đúng đối với khẳng định đầu T và khẳng định cuối $y \geq x$.

Giải: Khi khẳng định đầu là đúng và có điều kiện $x > y$, thì y được gán giá trị của x, tức là $y := x$. Khẳng định cuối là đúng. Hơn nữa, khi khẳng định đầu đúng và điều kiện $x > y$ sai, tức là $y \geq x$, thì khẳng định cuối vẫn đúng. Vì thế, theo quy tắc suy luận cho đoạn chương trình kiểu này thì đoạn chương trình trên là đúng đối với khẳng định đầu p và khẳng định cuối q đã cho.

■

Tương tự, giả sử một đoạn chương trình có dạng

---

if *điều kiện* **then**

S_1

else

S_2

Nếu *điều kiện* là đúng thì S_1 được thi hành, nếu *điều kiện* là sai thì S_2 được thực hiện. Để kiểm chứng rằng đoạn chương trình là đúng đối với khẳng định đầu p và khẳng định cuối q ta phải làm hai việc. Trước tiên, phải chỉ ra khi p đúng và *điều kiện* đúng thì q đúng sau khi S_1 kết thúc. Sau đó phải chứng minh rằng khi p đúng và *điều kiện* sai thì q đúng sau khi S_2 được thực hiện. Ta có quy tắc suy luận sau đây.

$(p \wedge \textit{điều kiện})\ \{S_1\}q$

$(p \wedge \neg \textit{điều kiện})\ \{S_2\}q$

$\therefore\ p\{\textbf{if } \textit{điều kiện } \textbf{then } S_1 \textbf{ else } S_2\}q.$

Ví dụ sau minh họa cách sử dụng quy tắc suy luận này.

Ví dụ 3. Hãy chứng tỏ đoạn chương trình

---

if $x < 0$ **then**

$abs := -x$

else

$abs := x$

---

là đúng đối với khẳng định đầu T và khẳng định cuối $abs = |x|$.

Giải. Khi khẳng định đầu là đúng và có điều kiện $x < 0$, thì abs được gán $-x$, tức là $abs = -x = |x|$ khẳng định cuối là đúng. Hơn nữa, khi khẳng định đầu là đúng và điều kiện $x < 0$ là sai, tức là $x \geq 0$, khi đó abs được gán x, tức $abs = x = |x|$. Vì thế, theo quy tắc suy luận cho đoạn chương trình kiểu này thì đoạn chương trình trên là đúng đối với khẳng định đầu và khẳng định cuối đã cho.

BẤT BIẾN VÒNG LẶP

Tiếp theo chúng ta sẽ trình bày cách chứng minh tính đúng đắn của vòng lặp **while**. Để xây dựng quy tắc suy luận cho đoạn chương trình dạng.

---

while *điều_kiện*

S

---

hãy lưu ý rằng S được lặp đi lặp lại cho tới khi nào *điều kiện* trở nên sai. Ta gọi một điều khẳng định nào đó là **bất biến vòng lặp** nếu nó vẫn còn đúng sau mỗi lần S thi hành. Nói cách khác, nếu $(p \wedge \textit{điều kiện})\{S\}p$ là đúng thì p là một bất biến vòng lặp.

Giả sử p là bất biến vòng lặp. Từ đó suy ra p là đúng trước khi đoạn chương trình thực hiện, p và $\neg$*điều kiện* là đúng sau khi kết thúc. Quy tắc suy luận là :

$$\frac{(p \wedge \textit{điều kiện})\ \{S\}p}{\therefore\ p\{\textbf{while}\ \textit{điều kiện}\ S\}(\neg\textit{điều kiện} \wedge p).}$$

Ví dụ 4. Hãy dùng bất biến vòng lặp chứng tỏ đoạn chương trình

---

```
i := 1
factorial := 1
while i < n
  begin
     i := i + 1
     factorial := factorial * i
  end
```

---

kết thúc với *factorial* = $n!$, trong đó n là số nguyên dương. Giả sử p là mệnh đề "*factorial* := $i!$ và $i \leqslant n$". Chúng ta sẽ chứng minh p là một

bất biến vòng lặp bằng quy nạp toán học. Đầu tiên hãy nhớ rằng p là đúng trước khi vào lặp, vì $i = 1$, $factorial = 1 = 1!$ và $1 \leq n$. Giả sử p đúng và $i < n$ sau khi thực hiện vòng lặp và giả sử vòng **while** được thi hành một lần nữa. Trước tiên i tăng thêm một, như vậy vẫn còn nhỏ hơn hay bằng n. Do giả thiết quy nạp $factorial = (i - 1)!$ trước khi vào vòng lặp, nó sẽ được đặt bằng $(i - 1)!*i = i!$. Vì thế, p vẫn còn đúng. Do đó p là một bất biến vòng lặp.

Nói cách khác mệnh đề $[p \wedge (i < n)]\{S\}p$ là đúng. Từ đó suy ra khẳng định p **{while** $i < n$ $S\}$ $[(i \geq n) \wedge p]$ cũng đúng.

Vì vòng lặp kết thúc sau khi lặp $(n - 1)$ lần, khi đó $i = n$ và $factorial = n!$

Ví dụ cuối cùng này sẽ minh họa cách dùng các quy tắc suy luận khác nhau để kiểm chứng tính đúng đắn của một chương trình dài hơn.

Ví dụ 5. Ta sẽ kiểm tra sự đúng đắn của chương trình S tính tích hai số nguyên.

```
procedure multiply (m, n : integer)
S1 { if n < 0 then a := -n
   { else a := n
S2 { k := 0
   { x := 0
   { while k < a
   { begin
S3 {       x := x + m
   {       k := k + 1
   { end
S4 { if n < 0 then product := -x
   { else product := x
```

Chúng ta sẽ chứng minh sau khi S được thi hành thì *product* có giá trị là mn. Theo quy tắc hợp thành ta chia S thành bốn đoạn $S = S_1; S_2; S_3; S_4$ như đã chỉ ra trong đoạn chương trình S.

Gọi p là khẳng định đầu "m và n là các số nguyên". Khi đó có thể chỉ ra $p\{S_1\}q$ là đúng, với q là mệnh đề $p \wedge (a = |n|)$. Tiếp theo gọi r là mệnh đề $q \wedge (k = 0) \wedge (x = 0)$. Dễ kiểm tra rằng $q\{S_2\}r$ là đúng. Có thể chỉ ra "$x = mk$ và $k \leqslant a$" là một bất biến với vòng lặp trong S_3. Hơn nữa, dễ thấy rằng vòng lặp này sẽ kết thúc sau a bước lặp khi $k = a$, tức là $x = ma$ tại điểm này. Từ đó suy ra $r\{S_3\}s$ là đúng với s là mệnh đề "$x = ma$ và $a = |n|$". Cuối cùng có thể chỉ ra S_4 là đúng đối với khẳng định đầu s và khẳng định cuối t, trong đó t là mệnh đề "$product = mn$".

Kết hợp lại ta có tất cả $p\{S_1\}q$, $q\{S_2\}r$, $r\{S_3\}s$, $s\{S_4\}t$ là đúng, theo quy tắc hợp thành suy ra $p\{S\}t$ là đúng. Hơn nữa vì bốn đoạn đều kết thúc nên S cũng dừng. Vậy ta đã kiểm tra được tính đúng đắn của chương trình.

■

BÀI TẬP

1. Chứng minh đoạn chương trình :

   $y := 1,$
   $z := x + y$

   là đúng đắn đối với khẳng định đầu $x = 0$ và khẳng định cuối $z = 1$.

2. Hãy kiểm chứng đoạn chương trình :

   if $x < 0$ **then** $x := 0,$

   là đúng đắn đối với khẳng định đầu T và khẳng định cuối $x \geqslant 0$.

3. Hãy kiểm chứng đoạn chương trình :

   $x := 2$

   $z := x + y$

   if $y > 0$ **then** $z := z + 1$

   else $z := 0$

   là đúng đắn đối với khẳng định đầu $y = 3$ và khẳng định cuối $z = 6$.

4. Hãy kiểm chứng đoạn chương trình :

```
if x < y then min := x
else
    min := y
```

là đúng đắn đối với khẳng định đầu T và khẳng định cuối $(x \leq y \wedge min = x) \vee (x > y \wedge min = y)$.

5. Hãy nghĩ ra một quy tắc suy diễn để kiểm chứng tính đúng đắn bộ phận của các câu lệnh dạng :

```
if điều_kiện_1 then
    S1
else if điều_kiện_2 then
    S2
    .
    .
    .
else
    Sn
```

trong đó S_1, S_2,..., S_n là các khối lệnh.

6. Dùng quy tắc suy diễn đưa ra trong Bài tập 5 kiểm chứng tính đúng đắn của đoạn chương trình

```
if x < 0 then
    y := - 2|x|/x
else if x > 0 then
        y := 2|x|/ x
    else if x = 0 then y := 2.
```

với khẳng định đầu T và khẳng định cuối $y = 2$.

7. Dùng bất biến vòng lặp chứng minh đoạn chương trình sau đây tính lũy thừa bậc n với n nguyên dương của một số thực x là đúng đắn :

```
power := 1
i := 1
while i ≤ n
begin
```

```
        power := power * x
        i := i + 1
    end
```

8*. Chứng minh chương trình lập tính f_n cho trong Tiết 3.4 là đúng đắn.

9. Hãy giải trình mọi chi tiết trong chứng minh tính đúng đắn được cho trong Ví dụ 5.

10. Giả sử cả mệnh đề kéo theo $p_0 \to p_1$ và khẳng định chương trình $p_1\{S\}q$ là đúng. Chỉ ra rằng $p_0\{S\}q$ cũng đúng.

11. Giả sử cả $p\{S\}q_0$ và mệnh đề kéo theo $q_0 \to q_1$ là đúng. Chỉ ra rằng $p\{S\}q_1$ cũng đúng

12. Đoạn chương trình sau đây tính thương và số dư :

```
r := a
q := 0
while r ≥ d
begin
    r := r - d
    q := q + 1
end
```

Kiểm chứng rằng nó là đúng đắn bộ phận đối với khẳng định đầu "a và d là nguyên dương" và khẳng định cuối "q và r là nguyên sao cho $a = dq + r$ và $0 \leq r < d$".

13. Dùng bất biến vòng lặp chứng minh rằng Thuật toán Euclid (Thuật toán 1, trong Tiết 2.4) là đúng đắn bộ phận đối với khẳng định đầu "a và b là nguyên dương "và khẳng định cuối x = ƯCLN(a, b).

CÂU HỎI ÔN TẬP

1. a) Thế nào là chứng minh trực tiếp, gián tiếp, chứng minh bằng phản chứng của mệnh đề kéo theo $p \to q$.

b) Hãy đưa ra cách chứng minh trực tiếp, gián tiếp, chứng minh bằng phản chứng của mệnh đề "Nếu n chẵn, thì $n + 4$ chẵn".

2. a) Hãy mô tả một cách chứng minh mệnh đề $p \leftrightarrow q$.

b) Chứng minh mệnh đề "Số dương $3n + 2$ là lẻ nếu và chỉ nếu số dương $9n + 5$ là chẵn, với n nguyên".

3. Nếu ta chỉ ra được các mệnh đề kéo theo $p_4 \rightarrow p_2$, $p_3 \rightarrow p_1$ và $p_1 \rightarrow p_2$ là có cơ sở, thì có thể kết luận rằng các mệnh đề p_1, p_2, p_3 và p_4 là tương đương hay không ? Nếu không, hãy đưa ra một tập các mệnh đề kéo theo khác có thể được dùng để chứng minh rằng bốn mệnh đề đã cho là tương đương.

4. a) Giả sử mệnh đề dạng $\forall x P(x)$ là sai. Có thể chứng minh điều này bằng cách nào?

b) Chỉ ra rằng mệnh đề "Với mỗi số n nguyên dương, $n^2 + 1$ là số nguyên tố" là sai.

5. a) Chứng minh tồn tại kiến thiết và chứng minh tồn tại không kiến thiết có gì khác nhau?

b) Chứng minh với mọi số n nguyên dương tồn tại một số lớn hơn n không chia hết cho 3 hoặc 5. Bạn dùng cách chứng minh tồn tại kiến thiết hay không kiến thiết?

6. a) Hãy phát biểu tính được sắp tốt của tập các số nguyên dương.

b) Sử dụng tính chất này chỉ ra rằng mọi số nguyên dương có thể được viết dưới dạng tích của các số nguyên tố.

7. a) Có thể dùng quy nạp toán học để tìm công thức tính tổng n số hạng đầu tiên của một dãy hay không?

h) Có thể dùng quy nạp toán học để xác định xem công thức tính tổng n số hạng đầu tiên của một dãy số có đúng hay không?

8. a) Bất đẳng thức $11n + 17 \leqslant 2^n$ đúng với những giá trị nguyên dương nào của n?

b) Hãy chứng minh điều phỏng đoán của bạn trong phần a) bằng quy nạp toán học.

9. a) Những tổng bưu phí nào có thể tạo được khi chỉ dùng các loại tem 5 xu và 9 xu?

b) Hãy chứng minh điều phỏng đoán của bạn bằng quy nạp toán học.

c) Hãy chứng minh điều phỏng đoán của bạn bằng dạng thứ hai của quy nạp toán học.

d) Tìm cách chứng minh điều phỏng đoán của bạn bằng một cách khác với cách dùng trong phần h) và c).

10. Hãy đưa ra 3 ví dụ về cách chứng minh dùng dạng thứ hai của quy nạp toán học.

11. a) Hãy giải thích tại sao một hàm được định nghĩa tốt nếu nó được định nghĩa bằng đệ quy, tức là cho $f(1)$ và quy tắc để tìm $f(n)$ từ $f(n-1)$.

b) Hãy đưa ra một định nghĩa đệ quy của hàm $f(n) = (n+1)!$

12. a) Hãy đưa ra một định nghĩa đệ quy của các số Fibonacci.

b) Chỉ ra rằng $f_n > \alpha^{n-2}$ khi $n \geq 3$ trong đó f_n là số hạng thứ n của dãy Fibonacci và $\alpha = \dfrac{1+\sqrt{5}}{2}$.

13. a) Hãy giải thích tại sao dãy a_n được định nghĩa tốt nếu nó được định nghĩa bằng đệ quy khi cho a_1 và a_2 và cho quy tắc xác định a_n từ $a_1, a_2, \ldots, a_{n-1}$ với $n = 3, 4, 5, \ldots$

b) Tìm các giá trị của a_n nếu $a_1 = 1$, $a_2 = 2$ và $a_n = a_{n-1} + a_{n-2} + \ldots + a_1$ với $n = 3, 4, 5, \ldots$

14. Hãy đưa ra hai ví dụ về cách xây dựng bằng đệ quy các công thức được tạo đúng quy tắc từ tập các phần tử khác nhau và các toán tử.

15. a) Hãy đưa ra một định nghĩa đệ quy của độ dài của một xâu.

b) Dùng định nghĩa đệ quy từ phần a) chứng minh $l(xy) = l(x) + l(y)$.

16. a) Thuật toán đệ quy là gì?

b) Mô tả thuật toán đệ quy tính tổng n số hạng của một dãy.

17. Mô tả thuật toán đệ quy tính ƯCLN của hai số nguyên dương.

18. a) Khi thử một chương trình máy tính ta thấy được nó tạo ra các kết quả đúng từ các giá trị vào đúng. Điều đó có thể khẳng định là chương trình đã cho luôn cho các kết quả ra đúng không ?

b) Việc chứng tỏ rằng một chương trình máy tính là đúng đắn bộ phận đối với một khẳng định đầu và một khẳng định cuối có chứng tỏ rằng chương trình đó luôn luôn cho đầu ra đúng không? Nếu không thì còn cần điều kiện gì nữa ?

19. Kỹ thuật nào bạn có thể dùng để chỉ ra rằng chương trình rất dài là đúng đắn bộ phận đối với các khẳng định đầu và khẳng định cuối nào đó?

20. Bất biến vòng lặp là gì? Nó được dùng như thế nào?

BÀI TẬP BỔ SUNG

1. Chứng minh rằng tích của hai số lẻ là một số lẻ.

2. Chứng minh $\sqrt{5}$ là số vô tỷ.

3. Chứng minh hay phản bác rằng tổng của hai số vô tỷ là vô tỷ.

4. Chứng minh hay bác bỏ rằng $n^2 + n + 1$ là nguyên tố với mọi n là số nguyên dương..

5. Hãy xác định xem lý lẽ sau đây là có cơ sở không. Nếu n lớn hơn 5 thì n^2 lớn hơn 25. Do đó n là số nguyên với n^2 lớn hơn 25 sẽ suy ra $n > 5$.

6. Chứng minh rằng $n^4 - 1$ chia hết cho 5 khi n không chia hết cho 5. Dùng cách chứng minh từng trường hợp, với 4 trường hợp khác nhau tùy theo số dư của phép chia n cho 5.

7. Chứng minh $|xy| = |x||y|$ bằng cách chứng minh từng trường hợp.

8*. Chúng ta định nghĩa các **số Ulam** bằng cách đặt $u_1 = 1$ và $u_2 = 2$. Sau khi xác định được các số Ulam nhỏ hơn n, ta sẽ đặt n bằng số Ulam tiếp theo nếu nó có thể biểu diễn duy nhất thành tổng của hai số Ulam khác nhau. Ví dụ, $u_3 = 3$, $u_4 = 4$, $u_5 = 6$ và $u_6 = 8$.

   a) Tìm 20 số Ulam đầu tiên.

   b) Chứng minh có vô hạn số Ulam.

9. Hãy đưa ra cách chứng minh kiến thiết rằng có một đa thức $P(x)$ sao cho $P(x_1) = y_1$, $P(x_2) = y_2$, ..., $P(x_n) = y_n$, trong đó x_1, x_2, ..., x_n và y_1, y_2, ..., y_n là các số thực.

   (Gợi ý : Cho $P(x) = \sum_{i=1}^{n} \left(\prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \right) . y_i$).

10. Chỉ ra rằng
    $1^3 + 3^3 + 5^3 + ... + (2n + 1)^3 = (n + 1)^2 (2n^2 + 4n + 1)$
    với mọi n nguyên dương.

11. Chứng tỏ rằng $1.2^0 + 2.2^1 + 3.2^2 + ... + n.2^{n-1} = (n - 1).2^n + 1$, với n nguyên dương.

12. Chỉ ra rằng
    $$\frac{1}{1.3} + \frac{1}{3.5} + ... + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1},$$
    với mọi n nguyên dương.

13. Chỉ ra rằng

$$\frac{1}{1.4} + \frac{1}{1.7} + \ldots + \frac{1}{(3n-2)(3n+1)} = \frac{n}{3n+1},$$

với mọi n nguyên dương.

14. Dùng quy nạp toán học chứng minh $2^n > n^2 + n$, với mọi n nguyên dương lớn hơn 4.

15. Dùng quy nạp toán học chứng minh rằng $2^n > n^3$, với mọi n nguyên dương lớn hơn 9.

16. Tìm số nguyên N sao cho $2^n > n^4$, với mọi n nguyên dương lớn hơn N. Dũng quy nạp chứng minh kết quả của hạn là đúng.

17. Dùng quy nạp toán học chứng minh rằng $a - b$ là một nhân tử của $a^n - b^n$, với mọi n nguyên dương.

18. Dùng quy nạp toán học chứng minh rằng $n^3 + (n+1)^3 + (n+2)^3$ chia hết cho 9, với mọi n nguyên không âm.

19. Dùng quy nạp toán học chứng minh tổng $(n+1)$ số hạng đầu tiên của một cấp số cộng là

$$a + (a+d) + (a+2d) + \ldots + (a+nd) = \frac{(n+1)(2a+nd)}{2}$$

trong đó a và d là số thực.

20. Giả sử $a_j \equiv b_j \pmod m$ với $j = 1, 2, 3, \ldots m$. Chứng minh bằng quy nạp toán học rằng :

a) $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod m$

b) $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod m$

21*. Hãy xác định các số Fibonacci chẵn và dùng qui nạp chứng minh điều phỏng đoán của bạn.

22*. Hãy xác định số các Fibonacci chia hết cho 3 và dùng quy nạp chứng minh điều phỏng đoán của hạn.

23*. Chứng minh rằng $f_k f_n + f_{k+1} f_{n+1} = f_{n+k+1}$, với mọi số nguyên không âm n, trong đó k là số nguyên không âm còn f_i là số hạng thứ i của dãy Fibonacci.

Dãy Lucas *được xác định như sau* : $l_0 = 2$, $l_1 = 1$ *và* $l_n = l_{n-1} + l_{n-2}$ *với* $n = 2, 3, 4,...$

24. Chỉ ra rằng $f_n + f_{n+2} = l_{n+1}$ với mọi số nguyên không âm n, trong đó f_i và l_i là các số Fibonacci và số Lucas thứ i.

25. Chỉ ra rằng :

$l_0^2 + l_1^2 + ... + l_n^2 = l_n l_{n+1} + 2$ mọi n nguyên không âm và l_i là số Lucas thứ i.

26*. Dùng quy nạp toán học chỉ ra rằng tích của n số nguyên dương liên tiếp chia hết cho $n!$ (*Gợi ý* : Sử dụng hằng đẳng thức

$$\frac{m(m+1)...(m+n-1)}{n!} =$$

$$= \frac{(m-1)m(m+1)...(m+n-2)}{n!} + \frac{m(m+1)...(m+n-2)}{(n-1)!}\ ).$$

27. Dùng quy nạp toán học chỉ ra rằng $(\cos x + i \sin x)^n = \cos nx + i \sin nx$, với mọi n nguyên dương. (*Gợi ý* : Dùng các hằng đẳng thức

$\cos(a + b) = \cos a \cos b - \sin a \sin b$, và

$\sin(a + b) = \sin a \cos b + \sin b \cos a$.

28*. Dùng quy nạp toán học chỉ ra rằng

$$\sum_{j=1}^{n} \cos jx = \cos\frac{(n+1)x}{2} \sin\frac{nx}{2} \sin\frac{x}{2}$$

với mọi n nguyên dương và $\sin\frac{x}{2} \neq 0$.

Hàm McCarthy 91 *được định nghĩa theo quy tắc sau :*

$$M(n) = \begin{cases} n - 10 & \text{khi } n > 100 \\ M(M(n+11)) & \text{khi } n \leq 100 \end{cases}$$

với mọi n nguyên dương.

29. Bằng cách dùng liên tiếp quy tắc định nghĩa $M(n)$, tìm

a) $M(102)$ h) $M(101)$

c) M (99) d) $M(97)$

e) $M(87)$ f) $M(76)$.

30**. Chỉ ra rằng $M(n)$ là hàm được định nghĩa tốt từ tập các số nguyên dương sang tập các số nguyên dương.
(*Gợi ý* : Chứng minh rằng $M(n) = 91$ đối với mọi n nguyên dương và không lớn hơn 101).

31. Cách chứng minh như dưới đây đẳng thức :

$$\frac{1}{1.2} + \frac{1}{2.3} + \ldots + \frac{1}{(n-1)n} = \frac{3}{2} - \frac{1}{n}$$

với mọi n nguyên dương, có đúng không? Vì sao?

BƯỚC CƠ SỞ. Đẳng thức là đúng với $n = 1$ vì

$$\frac{1}{1.2} = \frac{3}{2} - \frac{1}{1}.$$

BƯỚC QUY NẠP. Giả sử đẳng thức đúng với n. Khi đó

$$\frac{1}{1.2} + \frac{1}{2.3} + \ldots + \frac{1}{(n-1)n} + \frac{1}{n(n+1)} = \frac{3}{2} - \frac{1}{n} + \left(\frac{1}{n} - \frac{1}{n+1}\right) = \frac{3}{2} - \frac{1}{n+1}$$

Vì thế kết quả là đúng với $n + 1$ nếu nó đúng với n. Đẳng thức trên được chứng minh.

32*. Một bộ trò chơi xếp hình được lắp vào với nhau bằng cách nối liên tiếp các chi tiết phù hợp vào một khối. Mỗi bước đi được thực hiện mỗi lần khi một chi tiết được thêm vào khối hay khi hai chi tiết được nối với nhau. Hãy dùng dạng thứ hai của quy nạp toán học chứng minh rằng: để lắp ráp được bộ đồ chơi xếp hình có n chi tiết cần đúng $n - 1$ bước đi, không quan tâm tới việc mỗi bước đi được thực hiện như thế nào.

33*. Chỉ ra rằng n đường tròn chia mặt phẳng thành $n^2 - n + 2$ miền nếu mọi cặp đường tròn cắt nhau tại đúng hai điểm và không có 3 đường tròn nào chứa một điểm chung.

34*. Chỉ ra rằng n mặt phẳng chia không gian 3 chiều thành $(n^3 + 5n + 6)/6$ miền nếu mọi bộ 3 mặt phẳng nào cũng có một điểm chung và không có 4 mặt phẳng chứa một điểm chung.

35*. Dùng tính chất được sắp tốt, chỉ ra rằng $\sqrt{2}$ là một số vô tỷ.
(*Gợi ý* : Giả sử $\sqrt{2}$ là hữu tỷ. Chỉ ra rằng tập các số dương có dạng $b\sqrt{2}$ có một phần tử a nhỏ nhất. Sau đó chỉ ra rằng $a\sqrt{2} - a$ là số dương nhỏ hơn có dạng này).

36. Một tập là được **sắp tốt** nếu mọi tập con không rỗng của nó có một phần tử bé nhất. Hãy xác định xem mỗi một trong các tập sau đây có là tập được sắp tốt không?

a) tập các số nguyên

b) tập các số nguyên lớn hơn – 100

c) tập các số hữu tỷ dương

d) tập các số hữu tỷ dương với mẫu số nhỏ hơn 100.

37*. Chỉ ra rằng có thể chứng minh tính được sắp tốt khi nguyên lý thứ hai của quy nạp toán học được dùng như một tiên đề.

38*. Chỉ ra rằng nguyên lý thứ nhất và thứ hai của quy nạp toán học là tương đương, tức là có thể chỉ ra mỗi nguyên lý là có cơ sở từ nguyên lý kia.

39. a) Chỉ ra rằng nếu $a_1, a_2, \ldots a_n$ là các số nguyên dương thì
$$\text{ƯCLN}(a_1, a_2, \ldots, a_n) = \text{ƯCLN}(a_1, a_2, \ldots, a_{n-2}, \text{ƯCLN}(a_{n-1}, a_n)).$$

b) Dùng phần a) cùng với thuật toán Euclid hãy viết một thuật toán đệ quy tính ƯCLN của n số nguyên dương.

40*. Hãy mô tả thuật toán đệ quy để viết ƯCLN của n số nguyên dương như một tổ hợp tuyến tính của n số nguyên này.

41. Hãy tìm dạng hiển của công thức cho $f(n)$ nếu $f(1) = 1$ và $f(n) = f(n-1) + 2n - 1$ với $n \geq 2$. Chứng minh kết quả của bạn bằng qui nạp toán học.

42.** Cho định nghĩa đệ quy của tập các xâu chứa các bit 0 hai lần nhiều hơn bit 1.

43. Cho S là tập các xâu nhị phân xác định theo đệ quy: $\lambda \in S$ và $0x \in S$, $x1 \in S$ nếu $x \in S$, trong đó λ là xâu rỗng.

a) Tìm tất cả các xâu của S có độ dài không vượt quá 5.

b) Cho mô tả dưới dạng hiển các phần tử của S.

44. Cho S là tập các xâu được xác định bằng đệ quy, $abc \in S$, $bac \in S$, $acb \in S$ và $abcx \in S$; $axbc \in S$, $xabc \in S$ nếu $x \in S$.

a) Tìm tất cả các phần tử của S có độ dài không lớn hơn 8.

b) Chỉ ra rằng mỗi phần tử của S có độ dài chia hết cho 3.

Giả sử B là tập các **xâu có dấu ngoặc cân bằng** được định nghĩa đệ quy như sau : $\lambda \in B$, trong đó λ là xâu rỗng, $(x) \in B$, $xy \in B$ nếu $x, y \in B$.

45. Hãy tìm các xâu dấu ngoặc cân bằng với bốn hoặc ít hơn các ký hiệu.

46. Sử dụng qui nạp chỉ ra rằng nếu x là xâu dấu ngoặc cân bằng thì số các dấu ngoặc trái trong x bằng số các dấu ngoặc phải.

Định nghĩa hàm N trên tập các xâu có dấu ngoặc bằng cách sau :

$$N(\lambda) = 0, \qquad N(() = 1, \qquad N()) = -1 ;$$

$$N(uv) = N(u) + N(v),$$

trong đó λ là xâu rỗng, u, v là các xâu. Có thể chỉ ra rằng N là hàm được xác định tốt.

47. Tìm

a) $N(())$ b) $N())))()(()$

c) $N((()(())$ d) $N(()((()))(()))$.

48.** Chỉ ra rằng xâu w gồm các dấu ngoặc là cân bằng nếu và chỉ nếu $N(w) = 0$ và $N(u) \geqslant 0$ với mọi u là tiền tố của w tức là $w = uv$.

49*. Cho thuật toán đệ quy để tìm tất cả các xâu có dấu ngoặc cân bằng chứa n hoặc ít hơn ký hiệu.

50. Hãy cho thuật toán đệ quy tìm ƯCLN của hai số nguyên không âm a và b với $a \leqslant b$, dựa trên các tính chất sau : ƯCLN$(a, b) = a$ nếu $a = b$, ƯCLN$(a, b) = 2$ƯCLN$\left(\frac{a}{2}, \frac{b}{2}\right)$ nếu a và b là chẵn, ƯCLN$(a, b) =$ ƯCLN$\left(\frac{a}{2}, b\right)$ nếu a là chẵn và b là lẻ và ƯCLN(a, b) = ƯCLN$(b - a, b)$ nếu a và b đều lẻ.

51. Hãy kiểm chứng đoạn chương trình

if $x > y$ **then**

$x := y$

với khẳng định đầu **T** và khẳng định cuối $x \leqslant y$.

52. Hãy soạn một quy tắc suy luận để kiểm chứng một chương trình đệ quy và sử dụng nó để kiểm chứng chương trình đệ quy tính giai thừa cho trong Tiết 3.4.

BÀI TẬP LÀM TRÊN MÁY TÍNH

Viết các chương trình với các input và output sau :

1. Cho cấp số nhân a, ar, ar^2, ..., ar^n tìm tổng các số hạng của nó.

2. Cho số nguyên không âm n, hãy tìm tổng n số nguyên dương nhỏ nhất.

3.** Cho một bàn cờ $2^n \times 2^n$ bị khuyết một ô, hãy đưa ra một cách lát bàn cờ này bằng những miếng hình chữ L.

4.** Hãy sinh ra tất cả các công thức được tạo đúng quy tắc, chứa các biến x, y, z và các toán tử $\{+, *, /, -\}$ với n hoặc ít hơn các ký hiệu.

5.** Hãy sinh ra tất cả các biểu thức mệnh đề được tạo đúng quy tắc, chứa n hoặc ít hơn các ký hiệu trong đó mỗi ký hiệu là **T**, **F**, một trong các biến mệnh đề p và q hoặc một toán tử trong số $\{\neg, \wedge, \vee, \leftrightarrow, \rightarrow\}$.

6. Cho một xâu, tìm xâu nghịch đảo của nó.

7. Cho số thực a và số nguyên dương n, hãy tìm a^n bằng đệ quy.

8. Cho số thực a và số nguyên đương n, hãy tìm a^{2^n} bằng đệ quy.

9*. Cho số thực a và số nguyên đương n, hãy tìm a^n bằng cách biểu diễn nhị phân của n và thuật toán đệ quy để tính a^{2^k}.

10. Cho hai số nguyên không đồng thời bằng không, hãy tìm ƯCLN bằng thuật toán đệ quy.

11. Cho một danh sách các số nguyên và một phần tử x, bãy định vị x trong danh sách này, bằng cách thực hiện đệ quy tìm kiếm tuyến tính.

12. Cho một danh sách các số nguyên và một phần tử x, hãy định vị x trong danh sách này, bằng cách thực hiện đệ quy tìm kiếm nhị phân.

13. Cho một số nguyên không âm n, hãy tìm số Fibonacci thứ n bằng phương pháp lặp.

14. Cho một số nguyên không âm n, hãy tìm số Fibonacci thứ n bằng phương pháp đệ quy.

15. Cho một số nguyên dương, hãy tìm số cách phân hoạch của số nguyên này (Xem Bài tập 35 của Tiết 3.3).

16. Cho các số dương m và n, hãy tìm $A(m, n)$, giá trị của hàm Ackermann tại cặp số (m, n). (Xem lời nói đầu trước Bài số 36, Tiết 3.3).

TÍNH TOÁN VÀ KHÁM PHÁ

Dùng các chương trình bạn đã viết để làm các bài tập sau :

1. Kiểm chứng phỏng đoán Goldbach nói rằng mọi số nguyên dương chẵn n là tổng của hai số nguyên tố, với $n \leqslant 10\ 000$.

2. Tìm thừa số nguyên tố nhỏ nhất của $n ! + 1$ với mọi n nguyên dương không lớn hơn 20.

3. Tìm tập nhỏ nhất của n hợp số liên tiếp với mỗi số dương n sao cho $n \leqslant 10$.

4. Một phỏng đoán chưa chứng minh được nói rằng có vô hạn số nguyên tố sinh đôi, tức là các số nguyên tố sai khác nhau 2 đơn vị. Bạn có thể tìm được bao nhiêu số nguyên tố sinh đôi?

5. Hãy tìm các số Fibonacci chia hết cho 5, cho 7, cho 11. Chứng minh phỏng đoán của bạn là đúng.

6. Tìm cách phủ các bàn cờ có kích thước 16×16, 32×32 và 64×64 khuyết một ô, bằng các miếng lát hình chữ L.

7. Hãy khảo sát xem bàn cờ $m \times n$ nào có thể phủ hoàn toàn bằng miếng lát hình chữ L. Bạn có thể đưa ra phỏng đoán rồi chứng minh.

8. Giả tbuyết $3x + 1$ nổi tiếng (*Giả thuyết Collatz*) phát biểu như sau : Dù bạn xuất phát từ giá trị nguyên x nào, khi tính lặp giá trị của $f(x)$, trong đó $f(x) = \dfrac{x}{2}$ nếu x chẵn và $f(x) = 3x + 1$ nếu x lẻ, thì ta luôn nhận được số nguyên 1. Hãy kiểm chứng giả thuyết đó với các số nguyên nhiều nbất có thể được.

9. Giá trị nào của hàm Akermann là đủ nhỏ để bạn có thể tính được?

10. Hãy so sánh hoặc là số các phép toán hoặc là thời gian cần thiết để tính các số Fibonacci bằng đệ quy và bằng phương pháp lặp.

VIẾT TIỂU LUẬN

Dùng các tư liệu ngoài cuốn sách này viết các tiểu luận trả lời những câu hỏi sau

1. Mô tả nguồn gốc của qui nạp toán học. Những ai đã sử dụng nó trước tiên và đã áp dụng vào các bài toán nào?

2. Trong thời gian gần đây có một số định lý quan trọng đã được chứng minh dựa trên sự tính toán rất nhanh của máy tính. Nói gì về cơ sở của các chứng minh như thế và kể lại những cuộc bàn cãi xung quanh cách chứng minh bằng tính toán trên máy.

3. Lập trình logic thao tác trên các mệnh đề có dùng các lượng từ, các vị ngữ, các liên từ logic và dùng các quy tắc suy diễn. Hãy giải thích các khái niệm cơ bản của lập trình logic và cách sử dụng nó trong lĩnh vực trí tuệ nhân tạo. Minh họa sự ứng dụng này bằng ngôn ngữ PROLOG.

4. "Chứng minh tự động các định lý" là nhiệm vụ dùng máy tính chứng minh định lý. Hãy thảo luận mục đích và các ứng dụng chứng minh tự động các định lý và sự tiến bộ đã đạt được trong lĩnh vực này.

5. Mô tả quy tắc cơ sở của WFF'N PROOF - Trò chơi logic biện đại - do Layman Allen đưa ra. Hãy cho một ví dụ về một trò chơi trong WFF'N PROOF.

6. Các miếng lát hình chữ L dùng trong các Bài tập của Tiết 3.2 là những ví dụ về các polymino do Golomb đưa ra năm 1954. Mô tả một vài bài toán và các kết quả liên quan tới bài toán lát bàn cờ bằng các poly mino.

7. Hãy bình luận về việc dùng các hàm Ackermann trong lý thuyết định nghĩa đệ quy và trong phân tích độ phức tạp của thuật toán cho hợp các tập hợp.

8. Mô tả một vài bài toán logic tìm thấy trong tác phẩm của Lewis Carroll và chỉ ra quy tắc suy diễn nào được dùng để giải các bài toán này.

9. Hãy bình luận một vài phương pháp luận dùng để chứng minh tính đúng đắn của chương trình và so sánh chúng với các phương pháp Hoare được mô tả trong Tiết 3.

10. Hãy giải thích cơ thể mở rộng ý tưởng và khái niệm tính đúng đắn của chương trình để chứng minh rằng các hệ điều hành là an toàn.