HỌC VIỆN NÔNG NGHIỆP VIỆT NAM
KHOA CÔNG NGHỆ THÔNG TIN

PGS.TS. NGUYỄN VĂN ĐỊNH

BÀI GIẢNG

CƠ SỞ MÃ HÓA THÔNG TIN

FUNDAMENTALS OF CODING

CHƯƠNG TRÌNH ĐỊNH HƯỚNG HỌC THUẬT

HÀ NỘI 2015

Notation

Dưới đây, chúng ta giới thiệu một số ký hiệu của lý thuyết tập hợp được sử dụng trong giáo trình này.

- Một tập hợp là một số các phần tử được chọn lọc theo một danh sách hoặc một số tính chất nào đó. Ta ký hiệu:

R : tập các số thực

Z : tập các số nguyên (gồm số 0, số nguyên âm và số nguyên dương)

F_n (hay Z_n): tập các số nguyên nhỏ hơn n, $F_n = \{0, 1, \ldots n - 1\}$. Chẳng hạn: $F_2 = \{0, 1\}$.

- Một đối tượng của một tập hợp gọi là một phần tử của tập hợp. Nếu x là phần tử của tập S thì ta viết ta viết $x \in S$ (đọc: x thuộc S), nếu trái lại, ta viết $x \notin S$. (đọc x không thuộc S). Chẳng hạn: ta có $x \in Z$ nhưng $½ \notin Z$.
- Hai tập hợp gọi là bằng nhau nếu chúng chứa các phần tử như nhau, chẳng hạn ta có $F_3 = \{0, 1, 2\}$, cũng có thể viết $F_3 = \{0, 2, 1\}$ hay $F_3 = \{2, 1, 0\}$
- Một tập hợp có thể không có phần tử nào, gọi là tập rỗng và ký hiệu là: $\varnothing$.
- Nếu S là một tập hợp và P là một hoặc một số tính chất nào đó mà các phần tử của S có thể có hoặc không, ta có thể xác định một tập hợp mới nhờ ký hiệu:

$$\{x \in S \mid P(x)\}$$

đó là tập các phần tử của S mà có tính chất P. Chẳng hạn, tập các số nguyên dương có thể được ký hiệu là $\{x \in Z \mid x > 0\}$. Tập tất cả các số chẵn có thể được ký hiệu là $\{ 2n \mid n \in Z \}$.

- Một tập hợp T được gọi là tập con của tập S, ký hiệu là $T \subseteq S$, nếu mọi phần tử của T là thuộc về S, khi đó ta nói T bị chứa trong S, hay S chứa T.
- Nếu A và B là 2 tập hợp, khi đó hợp của A và B là một tập hợp chứa các phần tử ít nhất thuộc về một tập A hoặc B. Ký hiệu:

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

- Giao của A và B là một tập hợp chứa các phần tử thuộc về cả A và B. Ký hiệu:

$A \cap B = \{ x \mid x \in A$ và $x \in B \}$

- Nếu A và B không có phần tử chung, tức là $A \cap B = \varnothing$, thì ta nói A và B là không giao nhau.
- Số phần tử của một tập hợp hữu hạn S, gọi là lực lượng của tập hợp đó (cardinality), ký hiệu là card(S), hay $| S |$. Chẳng hạn: với $Z_2 = \{0, 1\}$ thì $| Z_2 | = 2$, tương tự $| Z_3 | = 3$, $| Z_n | = n$.
- Tích Decac của 2 tập A và B, được ký hiệu là $A \times B$, là tập các cặp có thứ tự (a, b), với $a \in A$ và $b \in B$. Chú ý rằng $(a, b) \neq (b, a)$. Như vậy:

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

- Nếu A và B là các tập hữu hạn phần tử thì $| A \times B | = | A | . | B |$.
- Tích Decac của S với S được ký hiệu và xác định như sau:

$S^2 = \{(s_1, s_2) \mid s_1 \in S, s_2 \in S\}$

- Tổng quát, ta có tích Decac của n tập hợp $S_1, S_2, \ldots S_n$ được ký hiệu và xác định như sau:

$S_1 \times S_2 \times \ldots \times S_n = \{ (s_1, s_2, \ldots, s_n) \mid s_i \in S_i , i = 1, 2, \ldots, n \}$.

- Nếu $S_1 = S_2 = \ldots = S_n = S$, tích Decac trên có thể ký hiệu là S^n, đó là tập các n-bộ $(s_1, s_2, \ldots, s_n)$, với mọi $s_i \in S$, hiển nhiên khi đó $| S^n | = | S |^n$.
- Cuối cùng, chú ý rằng trong giáo trình này chúng ta có thể ký hiệu các n-bộ. hay vector n thành phần $(x_1, x_2, \ldots, x_n)$, bởi cách viết đơn giản là $x_1 x_2 \ldots x_n$.

Chương 1

TỔNG QUAN VỀ MÃ HÓA THÔNG TIN

1.1 CÁC KHÁI NIỆM CƠ BẢN VỀ MÃ HÓA THÔNG TIN

Mở đầu.

Claude Elwood Shannon (April 30, 1916 – February 24, 2001), một nhà toán học, một kỹ sư điện tử người Mỹ, ông cũng được biết đến như là "cha đẻ của lý thuyết thông tin". Trong thế chiến thứ II, Shannon có nhiều đóng góp cho quân đội Mỹ trong lĩnh vực phân tích và phá khóa mật mã. Năm 1948, Claude Shannon khi đó làm việc tại Bell Laboratories tại Mỹ, đã đưa ra Lý thuyết Mã hóa.

Hai năm sau đó, Richard Hamming, cũng tại Bell Labs, bắt đầu nghiên cứu mã sửa lỗi với tỷ lệ truyền tải thông tin hiệu quả hơn sự lặp lại đơn giản bằng cách biểu diễn một mã trong đó bốn bit dữ liệu được theo sau bởi ba bit kiểm tra cho phép không chỉ phát hiện mà còn sửa sai với một lỗi duy nhất.

Ý tưởng chính của Lý thuyết Mã hóa là thêm thông tin vào từng thông điệp mã trước khi gửi đi để bên nhận có thể tự phát hiện lỗi hoặc thậm chí tự sửa lỗi xảy ra trên đường truyền. Do đó, yêu cầu cơ bản nhất là giải mã duy nhất (unique decoding): bộ giải mã phải giải mã ra được đúng mã tự đã gửi, hoặc báo rằng không giải mã được.

Để thực hiện yêu cầu trên, trong mấy thập kỷ qua đã xuất hiện nhiều phương pháp giải mã khác nhau, gắn liền với các mã tương ứng như: mã tuần hoàn (Cyclic codes), mã lặp lại (Repetition codes), mã Reed-Solomon (Reed Solomon codes), mã BCH (BCH code), mã Reed-Muller…

Lý thuyết Mã hóa có rất nhiều ứng dụng trong thực tiễn. Một trong các ứng dụng của chúng là thiết kế các mã giúp việc đồng bộ hóa, như mã Đa truy nhập phân chia theo mã (Code Division Multiple Access- viết tắt là CDMA) bằng cách gắn mỗi điện thoại một từ mã đặc biệt để tiến hành giải mã. Mã nổi tiếng khác là mã Yêu cầu lặp lại tự động (Automatic Repeat reQuest- viết tắt là ARQ) bằng cách thêm các bit kiểm tra chẵn lẻ (gọi là bit dư thừa) vào các thông báo, khi máy thu phát hiện sự bất đồng nó sẽ yêu cầu máy phát truyền lại thông báo. Hầu hết các mạng diện rộng và các giao thức như SDLC(IBM), TCP(Internet), X25 (Quốc tế), TCP/IP.. đều sử dụng ARQ..

Đặc biệt, từ năm 1969 đến 1973 các tàu thăm dò sao Hỏa Mariner của NASA sử dụng một mã Reed-Muller mạnh mẽ có khả năng điều chỉnh 7 sai sót trong số 32 bit truyền, bao gồm 6 bit dữ liệu và 26 bit kiểm tra và tốc độ truyền dữ liệu hơn 16.000 bit trong mỗi giây. Đến năm 1989, tàu Voyager 2 đã vượt qua Hải vương tinh, ngôi sao xa nhất trong hệ Mặt trời, một đóng góp không nhỏ cho các thành công này là lý thuyết mã hóa.

Lý thuyết mã hóa không chỉ giúp giải quyết các vấn đề có tầm quan trọng của khoa học và cuộc sống trong thế giới thực, mà nó cũng đã làm phong phú nhiều lĩnh vực khác nhau của toán học, với những vấn đề mới cũng như những giải pháp mới.

1.1.1 Các khái niệm về thông tin và truyền tin

Trước hết ta xét vài thí dụ liên quan đến thông tin:

Thí dụ 1.1.

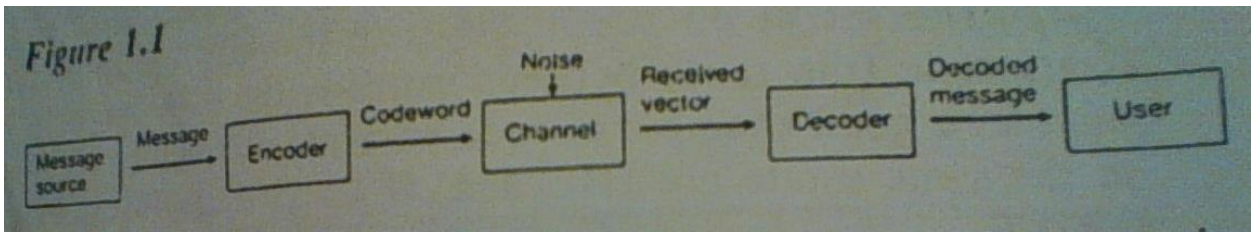
- Hai người nói chuyện với nhau: cái mà trao đổi giữa họ gọi là thông tin.
- Một người xem tivi, hoặc đọc báo, hoặc nghe radio: người đó đang nhận thông tin từ TV, báo , đài..
- Quá trình giảng dạy trên lớp: Giảng viên và sinh viên đang trao đổi thông tin
- Các máy tính tính nối mạng và trao đổi dữ liệu: chúng đang truyền thông tin qua kênh truyền…

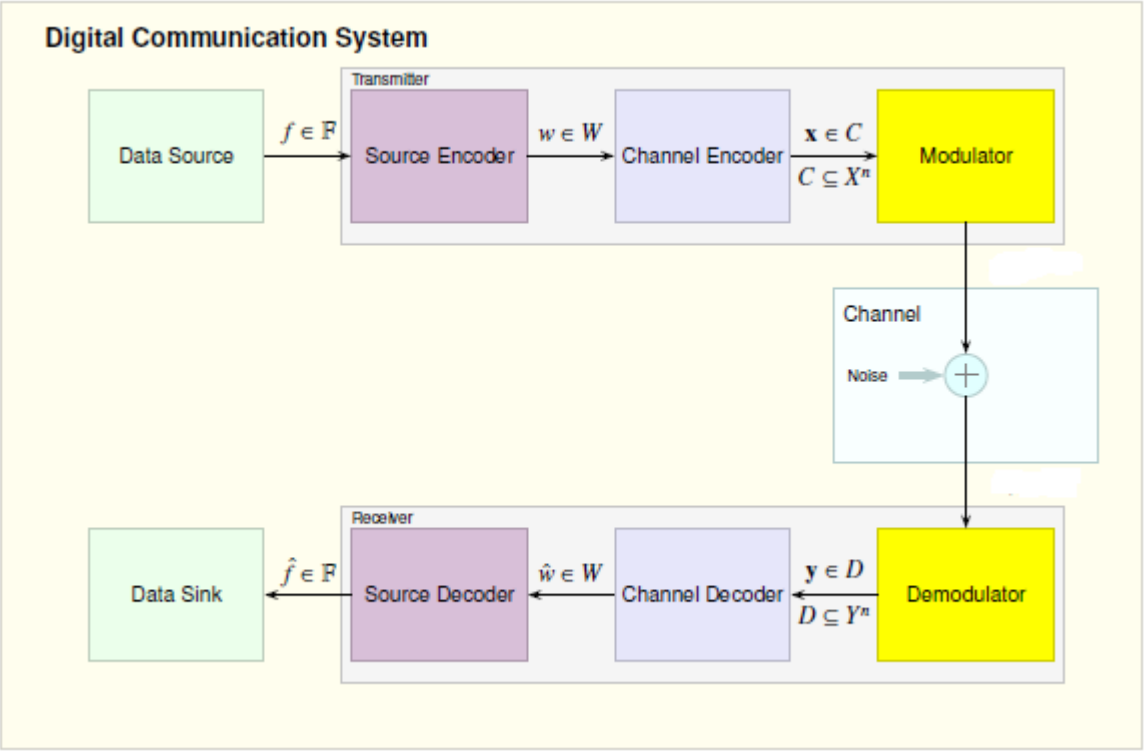
Từ đó có thể đưa ra khái niệm về thông tin như sau:

Định nghĩa 1.1.

- *Thông tin* (information) là tri thức được truyền từ đối tượng này đến đối tượng khác dưới dạng thông điệp (các xâu ký tự), âm thanh, hình ảnh…
- *Vật chất chứa thông tin* là các thông điệp, âm thanh, hình ảnh dùng để thể hiện và truyền tải thông tin.
- *Kênh thông tin* (channel) là nơi hình thành, truyền hay lưu trữ thông tin, còn gọi là môi trường chứa thông tin hay kênh thông tin.
- *Sự truyền tin* (transmission) là sự dịch chuyển thông tin từ điểm này đến điểm khác trong một môi trường xác định. Thiết bị truyền tin gọi là "*Transmitter*".
- *Nguồn tin* (source) là tập hợp các thông tin được truyền đi trong kênh thông tin.
- *Nhiễu (noise)* là các thông tin không mong muốn trong môi trường truyền tin gây sai lệch cho thông tin được truyền tải. (tín hiệu nhiễu , tiếng ồn, ảnh bị nhòe, biến dạng…).
- *Nơi nhận tin* (sink) là nơi tiếp nhận thông tin từ kênh truyền. Do tác động của nhiễu nên thông tin nhận được thường không giống thông tin ban đầu, vì vậy nơi nhận tin phải có khả năng phát hiện sai và sửa sai. Ngoài ra, nơi nhận tin còn phải giải nén hay giải mã các bản tin đã được nén hay bảo mật thông tin trước khi truyền. Thiết bị nhận tin gọi là "*Receiver*".

  Hình 1.1 dưới đây mô tả một hệ thống truyền tin kỹ thuật số (Digital Communication System)





Hình 1.1. Sơ đồ một hệ thống truyền tin

1.1.2 Các khái niệm về mã hóa thông tin

Trong các hệ thống truyền tin kỹ thuật số (Digital Communication System), các bản tin (thông điệp, âm thanh, hình ảnh…) được số hóa dưới dạng tập các xâu ký tự, ta coi mỗi tin là một xâu ký tự. Các tin nguồn sẽ được ánh xạ thành dạng biểu diễn khác nhằm mục đích bảo mật và để thuận tiện khi truyền phát đi. Việc ánh xạ đó gọi là sự mã hóa (encoding). Nơi nhận tin sẽ dùng ánh xạ ngược lại, để có nội dung của thông điệp ban đầu từ các tin nhận được, việc ánh xạ ngược lại được gọi là sự giải mã (decoding). Cả hai quá trình trên gọi chung là *mã hóa thông tin (coding).*

Thí dụ 1.2.

Xét một nguồn tin trên bảng chữ cái A = {*a, b, c, d*}. Chúng ta có thể thiết lập một ánh xạ song ánh f từ A vào tập các xâu trên bảng chữ cái {0, 1} như sau:

$$f : \{a \rightarrow 00,\ b \rightarrow 01,\ c \rightarrow 10,\ d \rightarrow 11\}$$

Do f là song ánh, tồn tại ánh xạ ngược f^{-1} là:

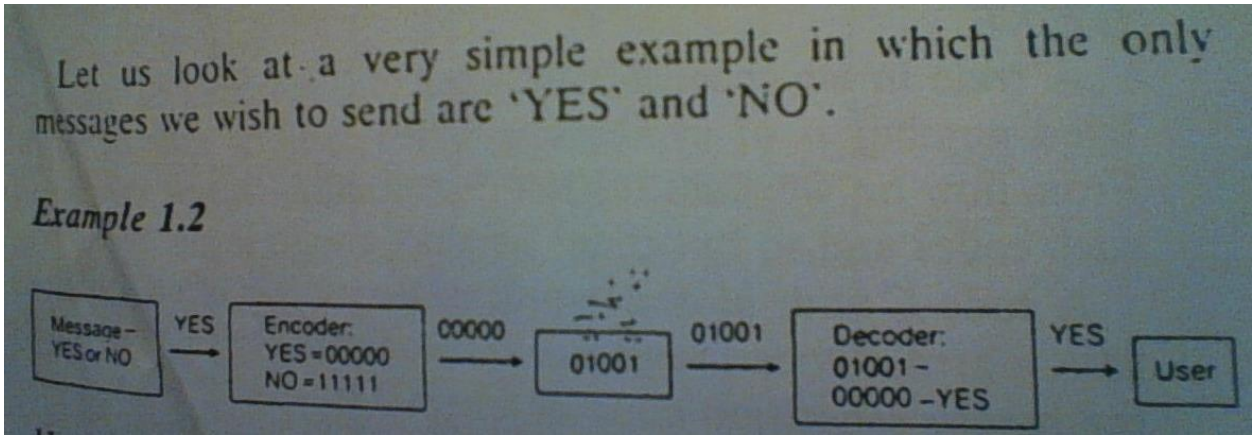
$$f^{-1} : \{00 \rightarrow a,\ 01 \rightarrow b, 10 \rightarrow c,\ 11 \rightarrow d\}$$

Để phát đi một tin nguồn là xâu '*baba*' chúng ta phát đi xâu '01000100'. Giả sử kênh truyền không có nhiễu, khi đó bên nhận nhận được xâu này, dùng ánh xạ ngược thì xác định được tin ban đầu bên phát đã phát đi là '*baba*'. Như vậy, ta đã thực hiện việc mã hóa thông tin trong quá trình phát và nhận bản tin nói trên.

Khi kênh truyền có nhiễu thì việc giải mã phức tạp hơn, trước hết bộ giả mã phải tìm cách xác định được từ mã đã gửi đi một cách hợp lý nhất, sau đó mới suy ra thông điệp ban đầu.

Với kênh truyền có nhiễu thì quá trình giải mã chủ yếu là làm thế nào để xác định được đúng từ mã đã gửi. Đó cũng là mục tiêu chính của lý thuyết mã hóa.

Xét thí dụ sau cho quá trình mã hóa trên một kênh truyền có nhiễu:



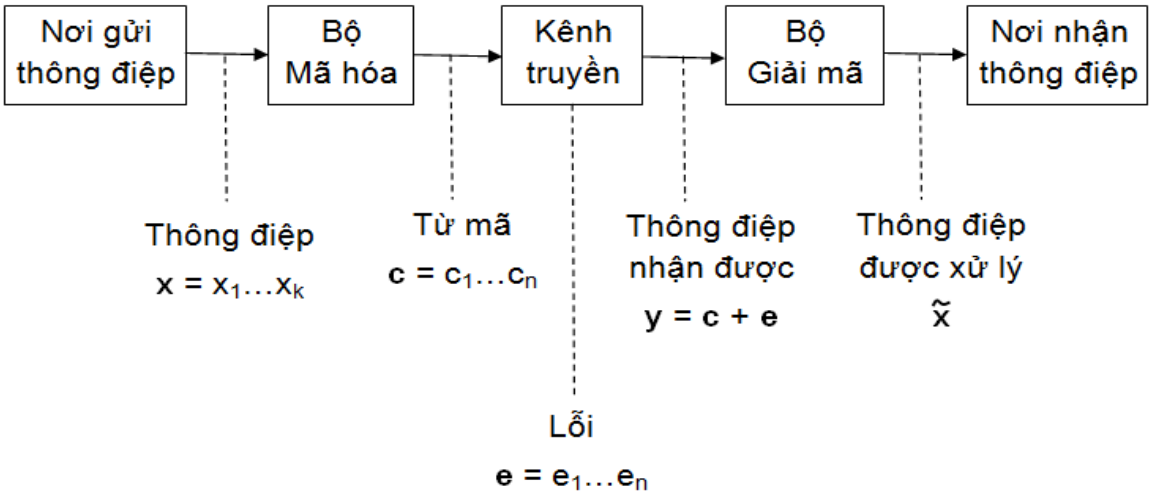
Ta có các khái niệm liên quan đến quá trình mã hóa thông tin.

Định nghĩa 1.2.

- Bảng ký hiệu dùng để biểu diễn các tin nguồn gọi là bảng ký hiệu nguồn (hay bảng chữ cái nguồn); bảng ký hiệu dùng để biểu diễn các tin mã hóa gọi là *bảng ký hiệu mã.(hay bảng chữ cái mã).* Số các ký hiệu trong bảng ký hiệu mã gọi là *cơ số mã*, thường ký hiệu là *q*. (chẳng hạn mã dùng bảng ký hiệu {0, 1} gọi là mã có cơ số q = 2, còn gọi là mã nhị phân).
- *Mã hóa* (Encoding) là quá trình dùng các ký hiệu mã để biểu diễn các tin nguồn. Quá trình ngược với quá trình mã hóa gọi là giải mã (Decoding).
- *Từ mã* (Code-word) là xâu ký hiệu mã biểu diễn cho một tin nguồn. Tập tất cả các từ mã tương ứng với các tin của một bản tin nguồn (thông điệp) gọi là mã (code) hay bộ mã, thường ký hiệu là C.
- *Mã khối* là khái niệm để chỉ cả một bản tin hay một khối tin của nguồn được mã hóa, thay vì mã hóa mỗi tin của nguồn.
- *Chiều dài từ mã* là số ký hiệu có trong một từ mã.

Mọi hệ thống truyền tin (Communication System) trong thế giới thực đều bị cản trở bởi nhiễu (noise) và do đó dễ bị sai sót trong việc truyền tải thông tin. Claude Shannon [1] đã đặt nền móng cho việc dùng các phương pháp mã hóa trong các hệ thống thông tin liên lạc sao cho các lỗi xảy ra trong truyền tin có thể được giảm xuống với xác suất nhỏ tùy ý. Những phương pháp này dựa trên cơ sở của lý thuyết mã hóa thông tin.

Hình 1.2 trình bày mô hình hệ thống truyền tin (Communication System) có ứng dụng lý thuyết mã hóa để xử lý thông tin.



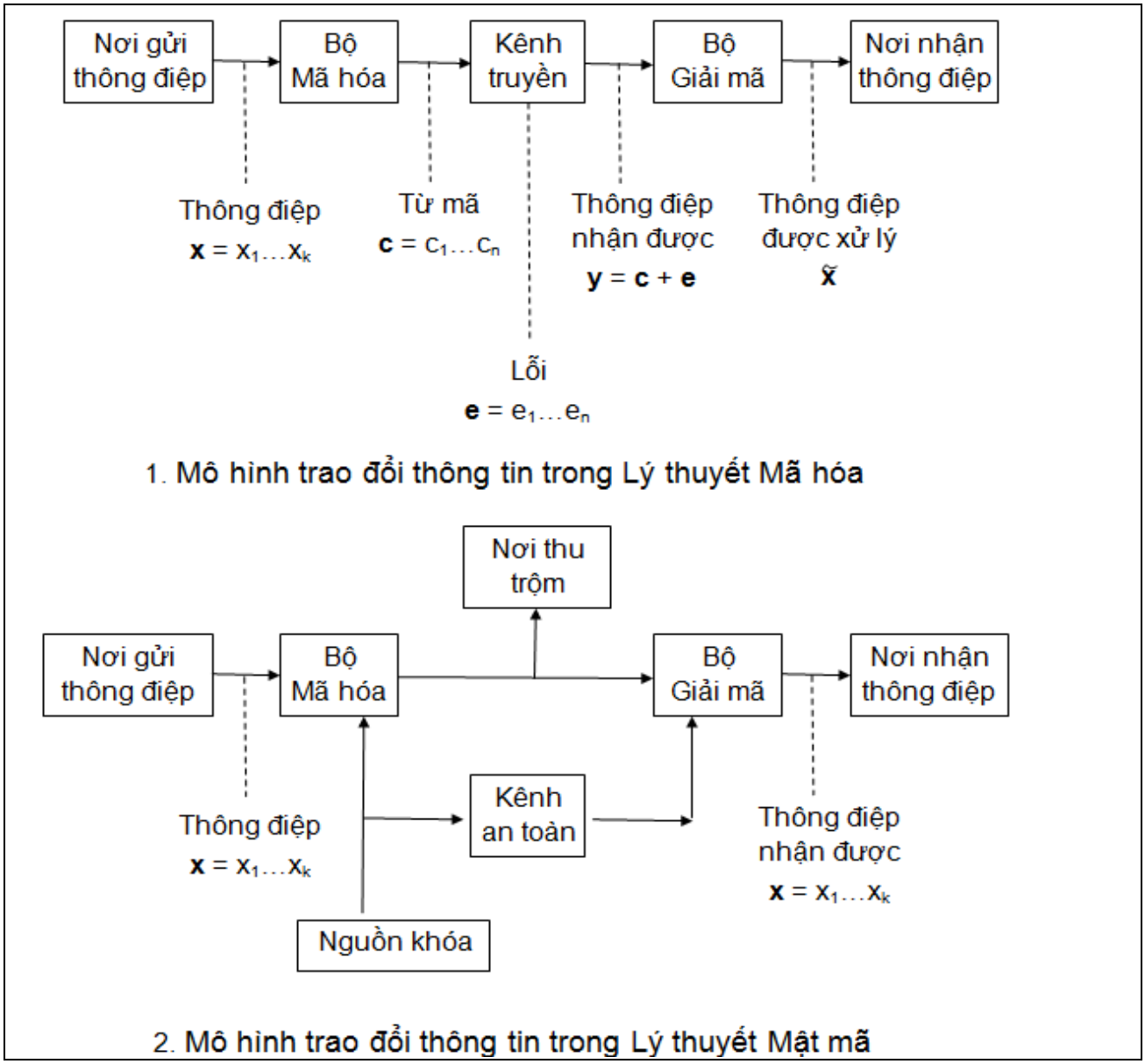
Hình 1.2. Mô hình trao đổi thông tin trong Lý thuyết Mã hóa

Như vậy Lý thuyết mã hóa là một ngành của Tin học nhằm nghiên cứu các phương pháp mã hóa thông tin trong quá trình truyền tin để giải quyết tình trạng lỗi xảy ra trên đường truyền, đồng thời cũng đưa ra các các phương pháp đặc biệt để có thể phát hiện lỗi và sửa sai các lỗi, xử lý các đặc tính của mã và có nhiều ứng dụng quan trọng trong việc truyền tin, lưu trữ và khôi phục dữ liệu, và nhiều ứng dụng khác trong khoa học máy tính.

1.1.3 Sự khác nhau giữa lý thuyết mã hóa và lý thuyết mật mã

Lý thuyết Mã hóa là một ngành của Tin học liên quan đến truyền dữ liệu qua các kênh bị nhiễu và phục hồi các thông điệp được gửi đi. Một cách khái quát, Lý thuyết Mã hóa làm cho thông điệp trở nên ít sai sót và dễ đọc hơn, trong khi đó Lý thuyết Mật mã là cũng một ngành của Tin học nhưng liên quan đến một kỹ thuật làm cho việc đọc thông điệp trở nên khó khăn.

Điều này được thể hiện khi so sánh hai mô hình trao đổi thông tin trong Lý thuyết Mã hóa và Lý thuyết Mật mã sau:



Hình 1.3. Sự khác nhau giữa Lý thuyết Mã hóa và Lý thuyết Mật mã

1.2 MỘT SỐ CƠ SỞ TOÁN HỌC CỦA LÝ THUYẾT MÃ HÓA

Toán học đóng vai trò rất quan trọng trong việc xây dựng và phát triển Tin học, nhất là trong lý thuyết mã hóa. Trong phần này, chúng ta sẽ nhắc lại một số khái niệm cơ sở và một số kết quả của Toán học có liên quan tới việc trình bày nội dung Lý thuyết mã hóa.

1.2.1 Các phép toán logic mệnh đề và các phép toán bit

Các quy tắc của logic cho ý nghĩa chính xác của các mệnh đề và được sử dụng để phân biệt giữa các lập luận đúng và không đúng. Cùng với tầm quan trọng của nó trong việc hiểu biết về suy luận toán học, logic học còn nhiều ứng dụng trong Tin học, nhất là trong lý thuyết mã hóa.

Mệnh đề

Mệnh đề là cơ sở để xây dựng môn logic mệnh đề.

Một mệnh đề là một câu, một phát biểu (*statement*) đúng hoặc sai, chứ không thể vừa đúng vừa sai.

Thí dụ 1.3 Xét các câu sau:

- Hà nội là thủ đô của Việt Nam.
- $3 \geq 4$.
- x-2 = 5.

Câu 1 là mệnh đề đúng.

Câu 2 là mệnh đề sai.

Câu 3 không phải là mệnh đề vì biến x chưa được gán một giá trị cụ thể nên nó chẳng đúng cũng chẳng sai.

Trong chương này, các chữ các như p, q, r, s…được dùng để ký hiệu mệnh đề, cũng như dùng để ký hiệu các biến mệnh đề (là biến nhận giá trị là mệnh đề).

Giá trị chân lý của một mệnh đề p : ký hiệu là V(p). V(p) = T (True-đúng) nếu p là mệnh đề đúng (trong máy tính được biểu diễn bằng số 1), V(p) = F (False-sai) nếu p là mệnh đề sai (trong máy tính được biểu diễn bằng số 0).

Các phép toán logic mệnh đề

Các mệnh đề như trên gọi là các mệnh đề đơn hay mệnh đề sơ cấp. Nhờ các phép toán logic mệnh đề, từ các mệnh đề ban đầu có thể tạo ra các mệnh đề mới gọi là các mệnh đề phức hợp (hay mệnh đề phức). Quy tắc xác định các mệnh đề phức dựa trên quy tắc xác định giá trị chân lý của chúng, từ các giá trị chân lý của các mệnh đề ban đầu.

Ta có các phép toán logic mệnh đề sau:

Định nghĩa 1.3

Giả sử p, q là các mệnh đề, khi đó ta có các mệnh đề phức hợp nhận được từ p và q qua các phép toán logic mệnh đề:

1. *'hội của p và q'* (hay '*p và q*', '*p AND q*') ký hiệu '$p \wedge q$', là một mệnh đề chỉ đúng khi cả p và q cùng đúng, và sai trong các trường hợp còn lại.
2. *'tuyển của p và q'* (hay '*p hoặc q*', '*p OR q*') ký hiệu '$p \vee q$', là một mệnh đề chỉ sai khi cả p và q cùng sai, và đúng trong các trường hợp còn lại.
3. *'tuyển loại của p và q'* (hay '*p tuyển loại q*', '*p XOR q*') ký hiệu '$p \oplus q$', là một mệnh đề đúng khi p và q nhận giá trị khác nhau, và sai khi p và q nhận cùng giá trị.
4. '*phủ định p*' (hay '*không phải p'*, '*NOT p'*) ký hiệu '$\neg p$' , là một mệnh đề đúng khi p sai và ngược lại
5. *'p kéo theo q'* ký hiệu '$p \rightarrow q$', là một mệnh đề chỉ sai khi p đúng và q sai, và đúng trong các trường hợp còn lại.
6. *'p tương đương q'* ký hiệu '$p \leftrightarrow q$', là một mệnh đề đúng khi p và q nhận cùng giá trị, sai trong trường hợp khi p và q nhận giá trị khác nhau.

Tóm tắt bảng giá trị chân lý của các mệnh đề phức hợp với các toán $\wedge$, $\vee$, $\oplus$, $\neg$, $\rightarrow$, $\leftrightarrow$ trên như sau:

Giá trị các mệnh đề đơn		Giá trị chân lý các mệnh đề phức qua các phép toán					
p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$\neg p$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	F	F	T	T
T	F	F	T	T	F	F	F
F	T	F	T	T	T	T	F
F	F	F	F	F	T	T	T

Hình 1.4. *Bảng giá trị chân lý của các phép toán logic mệnh đề*

Đôi khi để đơn giản, ta có thể thay các giá trị 1/0 tương ứng cho T/F trong bảng 1.4 để nhận được bảng giá trị chân lý của các phép toán logic mệnh đề với các giá trị chân lý của các mệnh đề là 1 hoặc 0.

Các phép toán bit

Các thông tin được biểu diễn trong máy tính bằng các bit, mỗi bit có hai giá trị khả dĩ là 0 và 1. Vì vậy các mã nhị phân trên bảng ký hiệu mã {0, 1} được dùng khá phổ biến trong lý thuyết mã hóa thông tin. Các tính toán với các mã nhị phân thường dùng các phép toán trên các bit và trên các xâu bit. Khi thay các giá trị chân lý của các mệnh đề là 1 hoặc 0 tương ứng cho T hoặc F, ta có thể tính được giá trị các phép toán AND, OR, XOR trực tiếp với các bit nhận giá trị 1 hoặc 0. Khi đó ta có các phép toán AND .bit, OR .bit và XOR .bit được xác định như sau:

=OR	0	1	AND	0	1	XOR	0	1
0	0	1	0	0	0	0	0	1
1	1	1	1	0	1	1	1	0

Hình 1.5*. Các phép toán bit*

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

Có thể mở rộng các phép toán bit đối với *hai xâu bit có cùng độ dài*, bằng cách áp dụng các phép toán OR.bit, AND.bit, XOR.bit đối với các bit ở vị trí tương ứng trong hai xâu trên.

Thí dụ 1.4: ***next T5 18/1/18.*** Tìm OR bit, AND bit, XOR bit đối với hai xâu 10011011 và 01100111.

Ta có:

```
10011011
01100111
--------
11111111    OR bit
00000011    AND bit
11111100    XOR bit
```

◄

Định nghĩa 1.4.

Phép toán XOR .bit còn gọi là '*phép cộng bit*' (+ . bit, ký hiệu ⊕), phép toán AND .bit còn gọi là '*phép nhân bit*' (x . bit, ký hiệu ⊗).

Thí dụ 1.5 Tìm + .bit, x .bit đối với hai xâu 10011011 và 01100111.

Ta có:

```
10011011
01100111
--------
11111100      + bit
00000011      . bit
```

◄

1.2.2 Số học đồng dư

Số học đồng dư

Định nghĩa 1.5

- Cho a là một số nguyên và m là một số nguyên dương. Khi đó, ta ký hiệu a **mod** m (hay a modulo m) là một phép toán cho kết quả là số dư khi chia a cho m.
- 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 modulo m, ký hiệu a ≡ b (**mod** m), nếu a-b chia hết cho m. Ta dùng ký hiệu a ≢ b để chỉ a và b không đồng dư theo modulo m.

Nhận xét:

1. Từ định nghĩa của số dư ta suy ra a **mod** m là số nguyên r sao cho: a = qm + r, với 0 ≤ r < m và q là một số nguyên.

2. a ≡ b nếu và chỉ nếu a **mod** m = b **mod** m .

Thí dụ 1.6 : Xác định 15 có đồng dư với 7 và 6 có đồng dư với 3 theo modulo 2 hay không?

Giải : Vì 15-7 = 8 chia hết cho 2 nên 15 ≡ 7 (**mod** 2).

Tuy nhiên, vì 6-3 = 3 không chia hết cho 2 nên 6 ≢ 3 (**mod** 2). ◄

Liên quan đến khái niệm đồng dư, ta có hai định lý sau

Định lý 1.1: Cho m là một số nguyên dương. Các số nguyên a và b đồng dư theo modulo m nếu và chỉ nếu tồn tại một số nguyên *k* sao cho $a = b + k.m$

Định lý 1.2

*Cho m là một số nguyên dương, Nếu a ≡ b (**mod** m) và c ≡ d (**mod** m) thì*
*a + c ≡ b + d (**mod** m) và ac ≡ bd (**mod** m)*

Ví dụ 1.7: Dễ thấy rằng 15 ≡ 7 (**mod** 2) và 6 ≡ 4 (**mod** 2) , theo Định lý 1.2 thì:

15 + 6 ≡ (7 + 4) (**mod** 2), hay 21 ≡ 11(mod 2)

Cũng theo định lý 1.2 thì: 15.6 ≡ 7.4 (**mod** 2), hay là 90 ≡ 28 (mod 2)

Phép cộng và phép nhân modulo m

Định nghĩa 1.6

Cho số nguyên dương m, xét tập số nguyên M = {0, 1, … , m – 1}, phép cộng modulo m (ký hiệu ⊕) và phép nhân modulo m (ký hiệu ⊗) trên M được xác định như sau:

- ∀ a, b ∈ M thì a ⊕ b = (a + b) mod m
- ∀ a, b ∈ M thì a ⊗ b = (a . b) mod m

Thí dụ1.8

Với m = 2, khi đó trên tập số M = {0, 1},

- ta có phép cộng modulo 2 xác định như sau:

∀ a, b ∈ {0, 1} thì a ⊕ b = (a + b) mod 2. Ta có các kết quả sau:

0 ⊕ 0 = 0 mod 2 = 0

0 ⊕ 1 = 1 mod 2 = 1

1 ⊕ 0 = 1 mod 2 = 1

1 ⊕ 1 = 2 mod 2 = 0

- ta có phép nhân modulo 2 xác định như sau:

∀ a, b ∈ {0, 1} thì a ⊗ b = (a . b) mod 2. Ta có các kết quả sau:

0 ⊗ 0 = 0 mod 2 = 0

0 ⊗ 1 = 0 mod 2 = 0

1 ⊗ 0 = 0 mod 2 = 0

1 ⊗ 1 = 1 mod 2 = 1

Chú ý:. Kết quả phép cộng modulo 2 chính là phép XOR bit, còn phép nhân modulo 2 chính là phép AND bit (xem 2.1.1). Do đó phép cộng bit (+.bit) còn gọi là phép cộng modulo 2, và phép nhân bit (x.bit) còn gọi là phép nhân modulo 2, là các phép toán được dùng trong các tính toán trên các xâu bit.

1.2.3 Tập hợp và ánh xạ

Mô tả tập hợp

Nếu số phần tử của tập hợp là hữu hạn và không quá lớn ta có thể đặc tả tập hợp bằng cách liệt kê tất cả các phần tử của nó giữa hai dấu ngoặc nhọn { }, các phần tử trong tập hợp được viết cách nhau bởi dấu phảy ‘ , ' và không quan tâm đế thứ tự các phần tử của một tập hợp.

Nếu phần tử x là thuộc tập hợp A, ta viết x∈ A (đọc x thuộc A), nếu trái lại, ta viết x∉ A. (đọc x không thuộc A).

Các chữ cái in hoa thường được dùng để đặt tên cho tập hợp.

Hai tập hợp bằng nhau là hai tập hợp có các phần tử như nhau, chẳng hạn, tập hợp A = {1, 2, 3, 4, 5} là bằng tập hợp B, với B = {2, 1, 4, 3, 5}, và ta viết A = B.

Thí dụ 1.9 Gọi D là tập hợp các ngày trong tuần, khi đó ta có thể biểu diễn D bằng cách liệt kê các phần tử của nó:

D = {*Mon, Tues, Wed, Thurs, Fri, Sat, Sun*}

Ta có Mon$\in$ D, Fri$\in$ D, nhưng September$\notin$ D.

Ngoài ra, tập hợp: {*Sat, Tues, Wed, Mon,Thurs, Fri, Sun*} cũng bằng tập hợp D.

Nếu một tập hợp chứa một số khá lớn các phần tử, hoặc là vô hạn các phần tử, người ta có thể không liệt kê tất cả các phần tử của tập hợp, mà dùng cách đặc tả tập hợp theo một số tính chất đặc trưng của các phần tử của nó.

Thí dụ 1.10: Có thể cho tập hợp theo các cách sau :

D = {x | x là một ngày trong tuần }, D là tập các ngày của một tuần lễ,

C = {z | z = a + ib, với a, b$\in$ R, $i^2 = -1$}, C là tập hợp số phức,

X = {x | x > 5}, X là tập các số thực có giá trị lớn hơn 5.

Ta nói tập hợp A là tập hợp con của tập hợp B và ký hiệu là A $\subseteq$ B, nếu mọi phần tử của A cũng là phần tử của B.

Ta nói tập hợp A là tập hợp con thực sự của tập hợp B và ký hiệu là A $\subset$ B, nếu A là tập hợp con của B, và trong B có ít nhất một phần tử không thuộc A.

Trái lại, nếu A có dù chỉ một phần tử mà không phải là phần tử của B thì A không phải là tập hợp con của tập hợp B.

- Nếu A $\subseteq$ B thì ta nói A bị chứa trong B, hay B chứa A.
- Nếu A $\subset$ B thì ta nói A bị chứa thực sự trong B, hay B thực sự chứa A.
- Hai tập hợp A và B gọi là bằng nhau khi và chỉ khi A $\subseteq$ B và B $\subseteq$ A, và viết A = B.

Phương pháp chứng minh hai tập hợp bằng nhau

Để chứng minh 2 tập bằng nhau, A = B, ta sẽ chứng minh hai bao hàm thức A $\subseteq$ B và B $\subseteq$ A.

Để chứng minh A $\subseteq$ B ta cần chỉ ra rằng: với phần tử bất kỳ x$\in$ A thì cũng có x$\in$ B, với bao hàm thức ngược lại B $\subseteq$ A cũng chứng minh tương tự. (xem thí dụ 1.5)

Một trường hợp đặc biệt của tập hợp là *"tập hợp rỗng",* tập hợp này không chứa bất kỳ phần tử nào, và được ký hiệu là Ø, hay { }. Tập hợp rỗng được xem như tập con của mọi tập hợp.

Tập hợp tất cả các tập hợp con của tập hợp A gọi là tập hợp lũy thừa của A, ký hiệu 2^A.

Người ta ký hiệu | A | là số phần tử của A, còn gọi là lực lượng của tập hợp A.

Rõ ràng ta có $|2^A| = 2^{|A|}$.

Thí dụ 1.11 :

a/. {1, 2, 3, 4} $\subseteq$ {2, 1, 4, 5, 3}

b/. {1, 2, 3, 4, 5} = {5, 1, 2, 3, 4}

c/. Cho A = {1, 2, 3} thì tập hợp lũy thừa của A là

2^A = {Ø, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}}

Ta có $|2^A| = 2^{|A|} = 2^3 = 8$ phần tử

Trong giáo trình này, từ nay về sau, để cho ngắn gọn, ta dùng từ "tập" để thay cho "tập hợp".

Các phép toán trên tập hợp

Các tập hợp được xét ở đây được xem như là các tập con của một tập vũ trụ X nào đó. Các phép toán cho trên tập hợp là:

a. Phần bù của tập hợp A trong X, ký hiệu $\overline{A}$, là tập các phần tử của X mà không thuộc A.

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

b. Hợp của A và B, ký hiệu $A \cup B$, là tập các phần tử hoặc thuộc A, hoặc thuộc B, hoặc thuộc cả A và B.

$$A \cup B = \{x \mid x \in A \text{ hoặc } x \in B\}$$

c. Giao của A và B, ký hiệu $A \cap B$, là tập hợp các phần tử đồng thời thuộc cả A và B.

$$A \cap B = \{x \mid x \in A \text{ và } x \in B\}$$

d. Hiệu của A và B, ký hiệu $A \setminus B$ (hoặc $A - B$), là tập các phần tử thuộc A mà không thuộc B

$$A \setminus B = \{x \mid x \in A \text{ và } x \notin B\}$$

Có thể chứng minh được các tính chất sau của các phép toán trên tập hợp

- Giao hoán

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

- Kết hợp

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

- Phân bố

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

- Đối ngẫu (công thức Demorgan)

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Tích Descartes của các tập hợp

Tích Descartes (tích Đề các) của hai tập A và B là một phép ghép hai tập để được tập hợp mới, ký hiệu $A \times B$:

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

Có thể mở rộng tích Descartes cho nhiều tập hợp:

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

Có thể dùng ký hiệu lũy thừa để chỉ tích Descartes của cùng một tập hợp:

$$A^k = A \times A \times \ldots \times A \text{ (k lần)}$$

Thí dụ 1.12 : Cho R là tập số thực, biểu diễn các điểm trên đường thẳng, khi đó:

$R^2 = \{(x, y) \mid x \in R, y \in R\}$ biểu diễn các điểm trên mặt phẳng,

$R^3 = \{(x, y, z) \mid x \in R, y \in R, z \in R\}$ biểu diễn các điểm trong không gian,

Thí dụ 1.13 : Chứng minh công thức Demorgan thứ nhất: $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Ta cần chứng minh hai bao hàm thức : $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ và $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$.

▪ Chứng minh $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ (a) :

Giả sử x là phần tử bất kỳ mà $x \in \overline{A \cup B}$, khi đó $x \notin A \cup B$, suy ra $x \notin A$ và $x \notin B$, vậy $x \in \overline{A} \cap \overline{B}$. Bao hàm thức (a) được chứng minh.

▪ Với bao hàm thức $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$ (b) ta cũng chứng minh tương tự.

Từ (a) và (b) suy ra $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Các bạn sinh viên tự chứng minh công thức Demorgan thứ hai như là một bài tập.

Tập lũy thừa của một tập hợp.

Định nghĩa 1.7: Cho tập hợp A, tập lũy thừa của A, ký hiệu P(A), là tập tất cả các tập con của A.

Thí dụ 1.14: Tìm tập lũy thừa của tập {1,3,5}.

Giải : Ta có P({1,3,5}) = {Ø,{1},{3},{5},{1,3},{1,5},{3,5},{1,3,5}}. ◄

Nhận xét :

Nếu tập A có n phần tử thì tập P(A) sẽ có 2^n phần tử.

Ánh xạ trên các tập hợp

Giữa các tập hợp có thể có sự tương ứng giữa một (nhiều) phần tử của một (nhiều) tập hợp này với các phần tử của (các) tập hợp khác, khi đó ta có một ánh xạ giữa các tập hợp đó.

Định nghĩa 1.8

Cho hai tập hợp A và B, nếu có một quy tắc f cho tương ứng mỗi phần tử $x \in A$ với một phần tử duy nhất $y \in B$ thì ta nói có một ánh xạ f từ A vào B, và ký hiệu là f: $A \to B$

▪ Phần tử $y \in$ B mà tương ứng với phần tử $x \in$ A được gọi là ảnh của *x* qua ánh xạ *f*, thường được ký hiệu là *y = f(x).*

▪ Tập tất cả những giá trị $y \in$ B là ảnh của *x* nào đó trong A, gọi là ảnh của A qua ánh xạ *f*, được ký hiệu và xác định như sau:

$$f(A) = \{y \in B \mid \text{có } x \in A \text{ để } y = f(x)\}$$

Từ định nghĩa ánh xạ trên đây, chú ý rằng ánh xạ *f* phải thỏa mãn hai tính chất:

(i) Mọi phần tử $x \in$ A đều có tương ứng với một phần tử $y \in$ B. Tập A còn được gọi là miền xác định của ánh xạ *f*. (không thể có phần tử nào của A không có tương ứng vào B)

(ii) Có thể có hai phần tử khác nhau của A cùng tương ứng với một phần tử của B, nhưng một phần tử của A thì không thể tương ứng với hai phần tử khác nhau của B.

Nếu vi phạm một trong 2 tính chất trên thì phép tương ứng *f* không phải là một ánh xạ.

Định nghĩa 1.9

Cho ánh xạ *f* từ A vào B, khi đó:

a/. Ánh xạ *f: A→ B được gọi là đơn ánh nếu ảnh của các phần tử khác nhau là khác nhau.*

Nói cách khác: ánh xạ f gọi là đơn ánh nếu với mọi $x_1, x_2 \in A$, *mà* $x_1 \neq x_2$, *thì* $f(x_1) \neq f(x_2)$

b/. Ánh xạ *f: A→ B được gọi là toàn ánh nếu f(A) = B.*

Nói cách khác: ánh xạ f gọi là toàn ánh nếu với bất kỳ $y \in B$, *có ít nhất một phần tử* $x \in A$ *tương ứng với y, tức là có* $x \in A$ *sao cho* $y = f(x)$.

c/. Ánh xạ *f: A→ B gọi là song ánh nếu f vừa là đơn ánh vừa là toàn ánh.*

Chú ý:

1. Nếu *f: A→ B* là một ánh xạ song ánh, thì tồn tại ánh xạ ngược từ B vào A, ký hiệu f^{-1}*: B→ A,* ứng mỗi phần tử $y \in B$ với một phần tử $x \in A$ mà $y = f(x)$.

Ánh xạ ngược f^{-1}*: B→ A* cũng là một song ánh và chỉ ánh xạ song ánh mới có ánh xạ ngược

2. Ánh xạ đơn ánh còn được gọi là 'ánh xạ 1 – 1'; ánh xạ toàn ánh còn gọi là 'ánh xạ lên' và ánh xạ song ánh còn gọi là ánh xạ '1 – 1' và 'lên'.

3. Ánh xạ *f: A→ B* cũng được gọi là một hàm từ A vào B. Khi các tập A, B là các tập con của tập số thực R, thì các ánh xạ được gọi là các hàm số.

Thí dụ1.15: Gọi A là tập các sinh viên trong 1 lớp, B = {0, 1, 2,…, 100},

a/. Phép tương ứng *f* ứng mỗi sinh viên với 1 giá trị trong B là điểm thi môn tiếng Anh của sinh viên đó (thang điểm 100, không có điểm lẻ). Rõ ràng *f* là một ánh xạ từ A vào B, vì với mỗi sinh viên đều có điểm thỏa mãn tính chất (i), và một sinh viên chỉ có một điểm duy nhất (thỏa mãn tính chất (ii) của ánh xạ).

b/. Phép tương ứng ngược lại từ B vào A không phải là ánh xạ, vì có thể với một giá trị trong B ứng với nhiều sinh viên cùng nhận giá trị đó là điểm (phá vỡ tính chất (ii) của ánh xạ. Ngoài ra, có thể có những giá trị của B không có sinh viên nào có điểm như vậy (phá vỡ tính chất (i) của ánh xạ). Phép tương ứng phá vỡ ít nhất một trong hai tính chất trên thì không phải là ánh xạ.

c/. Nếu gọi C là tập các mã sinh viên của lớp, thì tương ứng g mỗi sinh viên với mã SV của mình sẽ là một ánh xạ vừa có tính đơn ánh, vừa có tính toàn ánh, vậy g là một ánh xạ song ánh từ A vào C. Ta có ánh xạ ngược từ tập mã sinh viên C vào tập sinh viên A: g^{-1}*: C→ A.* Rõ ràng ánh xạ g^{-1} cũng là một song ánh.

Các bạn sinh viên có thể tìm thêm các thí dụ về các loại ánh xạ.

1.2.4 Các cấu trúc đại số.

Cho một tập hợp không rỗng A các phần tử. Một quy tắc '$*$' cho phép từ hai phần tử bất kỳ của A tạo nên một phần tử mới cũng thuộc A, tức là:

$$\forall a, b \in A \text{ thì } a * b \in A$$

được gọi là một luật hợp thành trên A (hay một phép toán trân A). Phép toán '$*$' có thể thỏa mãn một số tính chất, chẳng hạn tính giao hoán, tính kết hợp…

Tập A khác rỗng, trên đó có trang bị một hay nhiều luật hợp thành (phép toán), với những tính chất xác định tạo nên một *cấu trúc đại số*.

Một vài chú ý về tên gọi và ký hiệu: Các cấu trúc đại số thường sử dụng các luật hợp thành cộng (còn gọi là phép cộng, ký hiệu '+') và luật hợp thành nhân (còn gọi là phép nhân, ký hiệu '.') trên tập A, đó là các phép toán cho phép từ hai phần tử của A tạo ra phần tử mới cũng thuộc A , thỏa mãn một số tính chất nào đó. Với mỗi phép '+' hay phép nhân '.', tên gọi của một số tính chất có thể thay đổi cho phù hợp thói quen sử dụng. Chẳng hạn, với phép cộng thì phần tử trung hòa được gọi là *phần tử không* '0', còn với phép nhân thì phần tử trung hòa được gọi là *phần tử đơn vị* '1'. *Phần tử đối* (ký hiệu '*-x*') trong phép cộng khi chuyển qua phép nhân gọi là *phần tử nghịch đảo* (ký hiệu ' *1/x* ' hay ' x^{-1} ')

Có 3 cấu trúc đại số quan trọng trong toán học, đó là : Cấu trúc Nhóm, Vành và Trường, đặc biệt là các trường hữu hạn GF(q) có nhiều ứng dụng trong cơ sở mã hóa thông tin.

Cấu trúc Nhóm

Nhóm là cấu trúc đầu tiên có nhiều ứng dụng, và là cơ sở để xây dựng các cấu trúc vành và trường.

Định nghĩa 1.10.

Nhóm là một tập hợp A, trên đó có một phép toán, ký hiệu là phép ' + ', thỏa mãn các tiên đề:

(1) Tính kết hợp: $\forall a, b, c \in A$ *thì* $a + (b + c) = (a + b) + c$

(2) Tồn tại phần tử $0 \in A$ *sao cho* $\forall a \in A$ *thì* $a + 0 = 0 + a$. *Phần tử 0 là duy nhất trong A.*

(3) Tồn tại phần tử đối: $\forall a \in A$ *thì có phần tử đối* $-a \in A$ *sao cho* $a + (-a) = (-a) + a = 0$. *Với mỗi* $a \in A$, *phần tử đối* $-a$ *là duy nhất.*

- Nhóm A với phép cộng '+' ký hiệu là (A, +). Nếu phép cộng có tính giao hoán thì nhóm A gọi là *nhóm giao hoán* hay *nhóm Abel*.

Thí dụ 1.16

1. Tập các số nguyên Z với phép cộng các số thông thường là một nhóm Abel.
2. Cho A là tập các số hữu tỷ khác không: A = Q\{0}, phép toán hai ngôi là phép nhân thông thường '.', khi đó dễ thấy A là nhóm Abel.
3. Tập A = {0, 1} với phép cộng modulo 2 (phép cộng.bit) là một nhóm Abel.

Thật vậy, có thể thấy ràng A với phép cộng .bit thỏa mãn 3 tiên đề trên:

- Tiên đề kết hợp: rõ ràng $\forall a, b, c \in A$ thì $a + (b + c) = (a + b) + c$.

- Phần tử không là 0: $\forall 0, 1 \in A$ thì $0 + 0 = 0, 1 + 0 = 1$

- Tồn tại phần tử đối: dễ thấy phần tử đối của 0 là 0 do $0 \oplus 0 = 0$, đối của 1 là 1, do $1 \oplus 1 = 0$.

Vậy $(A, \oplus)$ là một nhóm Abel.

4. Tập A = {1, 2, …, p-1} với phép nhân modulo p là một nhóm Abel.

Cấu trúc Vành

Vành là một cấu trúc đại số phức tạp hơn cấu trúc nhóm, có thể coi vành là một nhóm với phép cộng có tính hoán và bổ xung thêm một phép toán nhân có tính kết hợp và có tính phân phối với phép cộng.

Ta có định nghĩa cụ thể sau:

Định nghĩa 1.11

Vành là một tập A không rỗng, trên đó có hai phép toán cộng ' + ' và nhân '.' thỏa mãn các tiên đề sau:

(1) với phép cộng thì (A, +) là một nhóm Abel.

(2) phép nhân có tính kết hợp: $\forall a, b, c \in A$ thì $a .(b .c) = (a .b) .c$

(3) phép nhân có tính phân phối đối với phép cộng: $\forall a, b, c \in A$ thì $a.(b + c) = a.b + a.c$

- Vành A với 2 phép toán '+' và '.' được ký hiệu là (A, + , .).

Chú ý:

1. Phần tử không của nhóm (A, +) cũng gọi là phần tử không của vành;
2. Nếu phép nhân có tính giao hoán thì A gọi là vành giao hoán.
3. Nếu phép nhân có phần tử đơn vị thì vành (A, +, .) gọi là vành có đơn vị. Phần tử đơn vị của phép nhân cũng gọi là phần tử đơn vị của vành.

Thí dụ 1.17

1. Tập các số nguyên Z, tập các số hữu tỷ Q, tập số thực R với phép cộng và phép nhân thông thường là các vành giao hoán có đơn vị.
2. Tập A = {0, 1, 2, 3, 4, 5} với phép cộng và phép nhân modulo 6: *$\forall a, b \in A$ thì $a \oplus b = (a + b) \pmod 6$, $a \otimes b = (a .b) \pmod 6$* . Dễ thấy rằng với hai phép toán này thì (A, $\oplus$, $\otimes$) là vành giao hoán có đơn vị, và gọi là vành các đồng dư theo modulo 6.
3. Tập A = {0, 1} với phép cộng và phép nhân modulo 2: *$\forall a, b \in A$ thì $a \oplus b = (a + b) \bmod 2$, $a \otimes b = (a .b) \bmod 2$* . Dễ thấy rằng với hai phép toán này thì (A, $\oplus$, $\otimes$) là vành giao hoán có đơn vị, và gọi là vành các đồng dư theo modulo 2. Chú ý rằng các phép cộng và nhân theo modulo 2 chính là các phép cộng.bit và nhân.bit đã biết.

Định nghĩa 1.12:

Cho vành (A, + , .), nếu phép nhân có tính chất: $a .b = 0$ thì hoặc $a = 0$ hoặc $b = 0$, thì vành (A , +, .) được gọi là vành nguyên

Chú ý :

1. Nếu có a.b = 0 với $a \neq 0$, $b \neq 0$ thì a và b gọi là các ước của 0, khi đó vành (A, + , .) gọi là vành có ước của 0. Như vậy vành nguyên (A, + , .) là vành không có ước của không.
2. Trong vành nguyên ta có: điều kiện cần và đủ để một tích bằng 0 là một trong hai nhân tử bằng 0.

Thí dụ 1.18

1. Vành các số nguyên Z, vành các số hữu tỷ Q, vành các số thực R (với phép cộng và phép nhân thông thường) là các vành không có ước của 0. Đó là các vành nguyên.
2. Vành các đồng dư theo modulo 6 trong thí dụ 1.17 (2) là vành có ước của 0, vì với $2 \neq 0$, $3 \neq 0$ nhưng $2 \otimes 3 = 0$. Vành này không phải vành nguyên
3. Vành các đồng dư theo modulo 2 trong thí dụ 1.17 (3) là vành không có ước của 0. Vành này là một vành nguyên.
4. Với *p* là số nguyên tố thì mọi vành các đồng dư theo modulo *p* là vành nguyên.

Cấu trúc Trường

Định nghĩa 1.13

Trường là một tập A không rỗng, trên đó có hai phép toán cộng ' + ' và nhân ' . ' thỏa mãn các tiên đề sau:

(1) (A, +, .) là một vành giao hoán có đơn vị.

(2) $\forall a \in A$, $a \neq 0$ thì đều có phần tử nghịch đảo a^{-1} (hay 1/a)

- Trường A với 2 phép toán '+' và '.' được ký hiệu là (A, + , .).

Nhận xét

1. Trường là một vành nguyên
2. Một trường gồm tối thiểu 2 phần tử: phần tử không của phép cộng và phần tử đơn vị của phép nhân
3. Nếu F là một trường thì a.0 = 0.a = 0, $\forall a \in F$.
4. Nếu có $a.b = a.c$ với $a \neq 0$ thì suy ra $b = c$

Từ các định nghĩa nhóm, vành, trường trên đây, ta có thể định nghĩa trực tiếp cho cấu trúc trường như sau:

Định nghĩa 1.13*

Trường là một tập A không rỗng, trên đó có hai phép toán cộng ' + ' và nhân ' . ' thỏa mãn các tiên đề sau:

(1) P hép cộng (+) có tính kết hợp và giao hoán, có phần tử không, có phần tử đối.

(2) Phép nhân (.) có tính kết hợp và giao hoán, có tính phân phối với phép cộng, có phần tử đơn vị.

(3) $\forall a \in A$, $a \neq 0$ thì đều có phần tử nghịch đảo a^{-1} (hay 1/a)

- Trường A với 2 phép toán '+' và '.' được ký hiệu là (A, + , .).

Thí dụ 1.19

1. Tập các số hữu tỷ Q, tập số thực R với phép cộng và phép nhân thông thường là các trường.
2. Nếu p là một số nguyên tố, tập F = $\{0, 1, ..., p - 1\}$ với các phép cộng và phép nhân modulo p là một trường, gọi là trường các đồng dư theo modulo p.
3. Tập F = {0, 1} với phép cộng .bit và phép nhân .bit (các phép cộng và nhân modulo 2, ký hiệu $\oplus$, $\otimes$) là một trường

Định nghĩa 1.14

Trường (F, +, .) có số phần tử | F | = q hữu hạn gọi là trường hữu hạn hay trường Galois, được ký hiệu là trường GF(q) hay F_q.

Đối với các trường Galois ta có định lý quan trọng sau:

Định lý 1.3

Mọi trường F hữu hạn thì số phần tử của nó phải có dạng : | F | = p^m, với p là số nguyên tố, và m là số nguyên dương

- Nói cách khác, các trường Galois đều có dạng $GF(p^m)$ trong đó p là một số nguyên tố còn m là một số nguyên dương.

Thí dụ 1.20

1. Theo định lý trên, với p là một số nguyên tố, $m = 1$, khi đó trường các đồng dư theo modulo p: F = {*0, 1, …, p – 1* } với các phép cộng và phép nhân modulo p là một trường Galois, ký hiệu *GF(p)* hay F_p.
2. Với $p = 2$, $m = 1$, tập F = {0, 1} với phép cộng.bit và phép nhân.bit (các phép cộng và nhân modulo 2, ký hiệu ⊕ , ⊗) là một trường Galois, ký hiệu *GF(2)* hay F_2.

Trường F_2 được ứng dụng nhiều trong lý thuyết mã hóa.

1.2.5 Đại số tuyến tính.

Ma trận:

Là bảng số gồm m hàng và n cột.

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots\dots\dots\dots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Ma trận **A** *gồm m hàng và n cột* được ký hiệu là **A** = $[a_{ij}]_{m \times n}$ trong đó a_{ij} chỉ phần tử nằm ở hàng thứ i, cột j của ma trận A.
Nếu ma trận có số hàng và số cột bằng n thì gọi là *Ma trận vuông cấp n, ký hiệu* A_n ,

Ôn lại các phép toán trên ma trận

- Cộng 2 ma trận cùng cấp: $A_{m.n} + B_{m.n} = C_{m.n}$ với các phần tử bằng tổng các phần tử tương ứng của A và B
- Nhân ma trận với 1 số : $k.A_{m.n}$ là ma trận cùng cấp, chứa các phần tử của A được nhân với k.
- Nhân 2 ma trận: $A_{m.n} . B_{n.p} = C_{m.p}$, với các phần tử $c_{ij} = a_{i1}.b_{1j} + a_{i2}.b_{2j} + a_{in}.b_{nj}$

  (i = 1,2, ..m ; j = 1, 2, ..p)
- Chuyển vị ma trận $A_{m.n}$ được ma trận $A^T_{n.m}$ với các hang của A là các cột của A^T.

Ma trận đơn vị cấp n, ký hiệu I_n

Có dạng :

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \dots\dots\dots & & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Tính chất của ma trận vuông I_n:

- Với mọi ma trận vuông A cấp n thì: $I_nA = A.I_n = A$
- Với mọi ma trận $A_{m \times n}$ thì: $A.I_n = A$
- Với mọi ma trận $B_{n \times m}$ thì: $I_n.B = B$

Ký hiệu ghép ma trận: Giả sử G là ma trận cấp $m \times k$ có k cột đầu làm nên ma trận đơn vị cấp k (I_k) , n-k cột cuối của G làm nên ma trận A ma trận cấp $m \times (n-k)$ ta có thể biểu diễn G dưới dạng $G = [I_k \mid A]$

Chẳng hạn với ma trận G cấp 3 x 5

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Khi đó $G = [\, I_3 \mid A]$ với

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

Ma trận không/một (ma trận bit)

- Các phép toán bit trên các ma trận bit.

Thí dụ 1.20

Cộng 2 ma trận bit: (quy tắc cộng 2 ma trận thông thường, với phép +.bit)

Nhân 2 ma trận bit: (quy tắc nhân 2 ma trận thông thường, với phép toán là +.bit và x.bit

1. Cho

$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{và } \mathbf{B} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Tìm AB theo các phép tính modulo2.

Giải :

Ta có:

$$\mathbf{AB} = \begin{pmatrix} 1.1+0.1 & 1.0+0.1 & 1.1+0.0 \\ 1.1+1.1 & 1.0+1.1 & 1.1+1.0 \\ 0.1+1.1 & 0.0+1.1 & 0.1+1.0 \\ 1.1+1.1 & 1.0+1.1 & 1.1+1.0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Không gian vector n chiều trên trường só thực R

Các bạn sinh viên đã học Đại số tuyến tính, cần ôn lại và nắm vững các khái niệm sau:

- *Ôn lại định nghĩa không gian vector*

Các phép toán:

1. Cộng các vector
2. Nhân vector với 1 số
3. Tổ hợp tuyến tính của một hệ vector

- *Định nghĩa không gian con*
- *Hệ vector độc lập tuyến tính*
- *Cơ sở và số chiều của một không gian*
- *Không gian n chiều trên trường số thực:* $R^n = \{(x_1, x_2, \ldots, x_n) | \ x_i \in \mathrm{R}\}$
- *Tích vô hướng các vector: với* $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$*là các vector trên trường F, tích vô hướng của x và y ký hiệu là một giá trị trên F, ký hiệu là (x, y) hay x.y*:

$$x.\mathrm{y} = \sum_{i=1}^{n} x_i y_i$$

  Hai vector n chiều *x, y* gọi là trực giao nếu tích vô hướng **(**x,y**)** = 0

- *Hai không gian con trực giao: Hai không gian U và V là trực giao với nhau nếu một vector bất kỳ của không gian này là trực giao với một vector của không gian kia và ngược lại. Tức là U trực giao với V khi và chỉ khi* $\forall u \in U$, $\forall v \in V$ *thì tích vô hướng (u, v) = 0.*
- ***Không gian n chiều trên trường GF(q)*** *:*

  ký hiệu là $F_q^n = \{(x_1, x_2, \ldots, x_n) | \ x_i \in \{0, 1, \ldots q-1\}\}$

Trên trường GF(2), $F_2^n = \{(x_1, x_2, \ldots, x_n) | \ x_i \in \{0, 1\}\}$, mỗi vector của F_2^n là một bộ n ký hiệu 0 hoặc 1, đó là 1 từ mã nhị phân có độ dài n. Tập hợp tất cả các từ mã nhị phân độ dài n làm thành không gian n chiều F_2^n. Một bộ mã nhị phân C là một tập con của F_2^n, nếu C là không gian con có số chiều k < n thì C sẽ là một mã tuyến tính.

Tương tự, trên trường GF(3): $F_3^n = \{(x_1, x_2, \ldots, x_n) | \ x_i \in \{0, 1, 2\}\}$ là mỗi vector của F_3^n là một bộ n ký hiệu 0, 1 hoặc 2, đó là 1 từ mã tam phân có độ dài n. Tập hợp tất cả các từ mã tam phân độ dài n làm thành không gian n chiều F_3^n. Một bộ mã tam phân C là một tập con của F_3^n, nếu C là không gian con có số chiều k < n thì C sẽ là một mã tuyến tính

- Khái niệm độc lập tuyến tính và phụ thuộc tuyến tính trên các không gian vector F_q^n *trên trường GF(q)*

Định nghĩa 1.15

Tập vector $\{u_1, u_2, \ldots, u_n\}$ *trong không gian* F_q^n *là phụ thuộc tuyến tính khi và chỉ khi tồn tại các hằng số không cùng bằng không* $k_1, k_2, \ldots, k_n \in F_q = \{0, 1, \ldots q-1\}$*, sao cho ta có:*

$$k_1u_1 + k_2u_2 + \ldots + k_nu_n = (0, 0, \ldots, 0) \quad (*)$$

Trái lại, nếu đẳng thức (*) *chỉ xảy ra với mọi giá trị* $k_i = 0$*, thì tập vector U là độc lập tuyến tính.*

- *Ôn lại: Cách xác định một hệ vector độc lập tuyến tính/phụ thuộc tuyến tính, cách giải hệ*

phương trình tuyến tính, điều kiện hệ thuần nhất có nghiệm khác không….

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

Trong đó, $x_1, x_2, \ldots, x_n$ là n biến số. Ta đã biết cách giải hệ phương trình này trên trường số thực..

Trong trường F_2, ta cũng có hệ phương trình tuyến tính tương tự hệ trên, với chú ý rằng trong đó $a_{ij}, b_i \in F_2 = \{0, 1\}$, nghiệm của hệ là các giá trị $x_j \in \{0, 1\}$, $(1 \le i \le m, 1 \le j \le n,)$

Hệ phương trình trên có thể được viết theo dạng phương trình ma trận: $A\mathbf{x} = \mathbf{b}$, trong đó **A** là ma trận bit cấp $m \times n$, chứa các hệ số a_{ij}, **b** là ma trận cột chứa *m* hằng số b_i, chú ý rằng a_{ij} và b_i chỉ nhận giá trị 0 hoặc 1, **x** là vector cột *n* chiều, chứa các biến x_j. Tức là:

$$\begin{pmatrix} a_{11} & a_{12} \ldots\ldots & a_{1n} \\ a_{21} & a_{22} \ldots\ldots & a_{2n} \\ \ldots\ldots\ldots & & \\ a_{m1} & a_{m2} \ldots\ldots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \\ b_m \end{pmatrix}$$

Thí dụ về việc giải một hệ hệ phương trình tuyến tính trên trường F_2:

$$\begin{cases} x + y = 1 & (1) \\ x + z = 0 & (2) \\ x + y + z = 1 & (3) \end{cases}$$

Cộng pt (3) với (1) → z = 0

Thay vào (2) → x = 0

Thay x = 0 vào (1) → y = 1

Vậy ngiệm của hệ : $\begin{cases} x = 0 \\ y = 1 \\ z = 0 \end{cases}$

Hệ này cũng có thể viết dưới dạng ma trận $A\mathbf{x} = \mathbf{b}$, với A, b là các ma trận bit. (sv tự viết lại).

Thí dụ 1.21. *Cho hệ vector U trong không gian F_2^4 (các xâu nhị phân độ dài 4):*

$U=\{u_1 = (0, 1, 1,0), u_2 = (0, 0, 1, 1), u_3 = (0, 1, 0, 1)\}$. Xét sự độc lập tuyến tính của hệ vector U.

Giải: xét hệ thức dạng (*) trong định nghĩa 1.15: $k_1u_1 + k_2u_2 + k_3u_3 = 0000$, với $k_i \in F_2 = \{0, 1\}$.

Ta có hệ phương trình :

$$\begin{cases} 0k_1 + 0k_2 + 0k_3 = 0 \\ 1k_1 + 0k_2 + 1k_3 = 0 \\ 1k_1 + 1k_2 + 0k_3 = 0 \\ 0k_1 + 1k_2 + 1k_3 = 0 \end{cases}$$

Nếu hệ chỉ có nghiệm $k_1 = k_2 = k_3 = 0$ thì theo định nghĩa 1.15, hệ vector U là độc lập tuyến tính. Nhưng có thể thấy hệ trên có nghiệm $k_1 = k_2 = k_3 = 1$, tức là tồn tại ít nhất một $k_i \neq 0$ để đẳng thức (*) trong định nghĩa 1.15 xảy ra, nên hệ vector U là phụ thuộc tuyến tính.

Cách khác để xét sự độc lập tuyến tính của hệ vector U là: Có thể thấy rằng $u_3 = u_1 + u_2$, tức là trong U có một vector biểu diễn qua các vector còn lại, vậy hệ U là phụ thuộc tuyến tính.

Dễ thấy rằng hai vector bất kỳ của U đều độc lập tuyến tính.

Nếu thêm vào hệ U bất kỳ vector nào khác 0000 thì hệ mới cũng phụ thuộc tuyến tính.

Chú ý rằng mọi hệ có chứa vector không (xâu toàn ký hiệu '0') thì luôn phụ thuộc tuyến tính.

1.2.6. Các khái niệm về xác suất

Giải tích tổ hợp

Dưới đây là một số khái niệm thường dùng khi tính các xác suất, tính số lượng các mẫu, tính số các từ mã...

Chỉnh hợp: chỉnh hợp chập *k* của *n* phần tử là một mẫu có thứ tự gồm *k* phần tử lấy từ *n* phần tử.

Số các chỉnh hợp chập *k* của *n* phần tử: $A(n, k) = n.\ (n-1).(n-2).\ \ldots\ .(n-k+1)$

Chỉnh hợp lặp: chỉnh hợp lặp chập *k* của *n* phần tử là một mẫu có thứ tự, có lặp lại gồm *k* phần từ lấy ra từ *n* phần tử

Số các chỉnh hợp lặp chập k của n phần tử: $\overline{A}(n,k) = n^k$

Hoán vị: Mỗi cách xắp xếp khác nhau của n phần tử gọi là 1 hoán vị của n phần tử

Số các hoán vị của n phần tử: $P_n = n\ !$

Tổ hợp: tổ hợp chập *k* của *n* phần tử là một mẫu không có thứ tự gồm *k* phần từ lấy từ *n* phần tử.

Số các tổ hợp chập *k* của n phần tử: $C(n, k) = \dfrac{n.(n-1).(n-2).....(n-k+1)}{k!}$

Phép thử và sự kiện

Phép thử: một thí nghiệm, thực hiện một hoặc một nhóm điều kiện nào đó

Sự kiện: phép thử có thể có một hoặc nhiều kết quả, mỗi kết quả là 1 sự kiện (sơ cấp) liên kết với phép thủ đó. Tập Ω các sự kiện sơ cấp ứng với một phép thử gọi là không gian mẫu các sự kiện.

Sự kiện tất yếu: là sự kiện chắc chắn xảy ra khi thực hiện phép thử, thường được ký hiệu là Ω.

Sự kiến bất khả: là sự kiện không thể xảy ra khi thực hiện phép thử, thường được ký hiệu là ∅.

Sự kiến ngẫu nhiên: là sự kiện có thể xảy ra, hoặc không thể xảy ra khi thực hiện phép thử.

Hợp (hay tổng) của hai sự kiện A và B: là sự kiện được coi là xảy ra khi ít nhất 1 trong 2 sự kiện A hoặc B xảy ra, ký hiệu là A ∪ B hoặc A + B.

Giao (hay tích) của hai sự kiện A và B: là sự kiện coi là xảy ra khi ít nhất 1 trong 2 sự kiện A hoặc B xảy ra, ký hiệu là A ∩ B hoặc A.B.

Hai sự kiện A, B gọi là hai sự kiện xung khắc: nếu chúng không thể cùng xảy ra khi thực hiện phép thử.

Hai sự kiện A, B gọi là hai sự kiện đối lập: nếu chúng là xung khắc, và hợp của chúng là sự kiện tất yếu. (tức là nếu xảy ra sự kiện này thì không xảy ra sự kiện kia, và ngược lại)

Hai sự kiện A, B gọi là hai sự kiện độc lập: nếu sự xuất hiện (hay không xuất hiện) của sự kiện này không liên quan đến sự xuất hiện của sự kiện kia. (tức là sự xuất hiện của hai sự kiện là độc lập với nhau)

Định nghĩa xác suất bằng hệ tiên đề Kolmogorov

Giả sử ta có một tập Ω các sự kiện sơ cấp ứng với một phép thử nào đó, một σ-đại số các sự kiện F của các tập con của Ω, và một hàm P ánh xạ mỗi thành viên của F tới một giá trị là số thực. Các thành viên của F, nghĩa là các tập con $A \subseteq \Omega$, cũng được gọi là các "sự kiện".

Định nghĩa 1.16

Xác suất P của sự kiện A nào đó, ký hiệu P(A), thỏa mãn các tiên đề sau (gọi là hệ tiên đề Kolmogorov):

(1) $0 \le P(A) \le 1, \forall A \in F$

(2) $P(\Omega) = 1$.

(3) Nếu các sự kiện A_i *(i = 1, 2, ...n) là xung khắc từng đôi thì*

$$P(\bigcup_{i=1}^{n} A_i) = \sum_{i=1}^{n} P(A_i)$$

- Bộ ba (Ω , F , P) gọi là không gian xác suất

Định lý cộng xác suất

- Nếu A, B là các sự kiện xung khắc thì:

$$P(A \cup B) = P(A) + P(B)$$

- Nếu A, B là các sự kiện bất kỳ:

$$P(A \cup B) = P(A) + P(B) – P(A \cap B)$$

- Nếu A, B là các sự kiện độc lập:

$$P(A \cup B) = P(A) + P(B) – P(A).P(B)$$

- Nếu A, B là hai sự kiện đối lập:

$$P(A) = 1 – P(B), \text{ và}$$

$$P(B) = 1 – P(A)$$

Xác suất có điều kiện và định lý nhân xác suất

- *Xác suất không điều kiện*: Xác suất xảy ra sự kiện *A* của riêng nó, không phụ thuộc vào bất kỳ sự kiện khác gọi là xác suất không điều kiện của sự kiện A, hay đơn giản là xác suất của sự kiện A, kí hiệu là P(A).
- *Xác suất có điều kiện*: xác suất này được ký hiệu là P(A | B), và gọi là "xác suất của sự kiện A nếu sự kiện B đã xảy ra".
  - Nếu A và B là các sự kiện độc lập thì :

    $$P(A \mid B) = P(A) \text{ và } P(B \mid A) = P(B)$$

  - Nếu A và B không độc lập thì:

    $$P(A \mid B) = \frac{P(A \cap B)}{P(B)}; \; P(B \mid A) = \frac{P(A \cap B)}{P(A)}$$

Đôi khi có thể viết ngắn gọn P(A∩ B) = P(AB), khi đó xác suất của giao các sự kiện còn gọi là xác suất tích các sự kiện, được xác định bởi các quy tắc nhân xác suất sau dây:

- *Quy tắc nhân xác suất:*
  - Nếu A và B là các sự kiện độc lập thì : P(AB) = P(A). P(B),

Ngược lại nếu có P(AB) = P(A). P(B) thì A và B là các sự kiện độc lập.

- Nếu A và B không độc lập thì: $P(AB) = P(A).P(B \mid A)$

  $P(AB) = P(A \mid B).P(B)$

Thí dụ 1.22 Có bao nhiêu xâu bit nhị phân có độ dài 8.

Giải :

Xét tập hợp A = {0, 1}. Mỗi xâu bit độ dài 8 là một chỉnh hợp lặp chập 8 từ 2 phần tử của A. Vậy số xâu bit khác nhau có độ dài 8 là :

$$\overline{A}(2, 8) = 2^8 = 256$$ ◄

Thí dụ 1.24. Giả sử có một xâu bit độ dài 6 được gửi đi, xác suất để 1 bit bị nhận sai là p = 0.01. (tức là xác suất để gửi đi '0' lại nhận được '1' , và ngược lại). Tính xác suất để nhận được xâu bit y = 011000 khi xâu bit x = 000000 được gửi đi là bao nhiêu?

Giải :

Do xác suất nhận sai là p = 0.01 nên xác suất nhận đúng là 1-0.01 = 0.99. Đối với xâu bit 101000 nhận được khi xâu bit 000000 gửi đi thì bit thứ 2 và thứ 3 nhận được sai, các bit còn lại nhận được đúng. Do các sự kiện để xác suất các bit trong xâu nhận đúng và nhận sai là độc lập nhau, do đó theo quy tác nhân xác suất, ta có xác suất nhận được xâu bit y bằng tích các xác suất để nhận được từng bit, trong đó có 4 bit nhận đúng (xác suất là 0.99) và 2 bit nhận sai (xác suất là 0.01). Vậy xác suất cần tìm là:

$$(0.99)^4(0.01)^2 = 0.000096059601 \sim 96.10^{-6}$$ ◄

BÀI TẬP CHƯƠNG 1

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

a. 0111101; 0011011

b. 00001110; 01110001

c. 1010 01101; 010110110

2. Tìm các +.bit và x.bit của các cặp xâu bit ở bài tập trên.

3. Tính các biểu thức sau:

a. (10100101 OR 01011010) AND 00100110

b. (10100101 XOR 01011010) XOR 00100110

c. (10100101 XOR 01011010) AND 00100110

4. Cho hai tập hợp A = {0,1}, B = {0, 1, 2} và C = {x,y, z}.

a. Tính $A \times C$

b. Tinh $B \times C$

c. Tính A^2 ; A^3 ; $\{0, 1, 2\}^2$

5. Thực hiện các phép toán ma trận trên trường F_2:

a. Tính $\mathbf{A} \oplus \mathbf{B}$ (theo modulo 2)

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \text{ và } \mathbf{B} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

b. Tính $\mathbf{A} \otimes \mathbf{B}$ (theo modulo 2)

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \text{ và } \mathbf{B} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

6. Các phép tính $\oplus$ modulo 3 (để đơn giản, ký hiệu '+') và $\otimes$ modulo 3 (ký hiệu '.') được định nghĩa bởi bảng sau:

+	*0*	*1*	*2*	.	*0*	*1*	*2*
0	0	1	2	*0*	0	0	0
1	1	2	0	*1*	0	1	2
2	2	0	1	*2*	0	2	2

a. Tính $\mathbf{A} \oplus \mathbf{B}$ (theo modulo 3)

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 2 \\ 2 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \text{ và } \mathbf{B} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \\ 2 & 1 & 1 \end{pmatrix}$$

b. Tính $\mathbf{A} \otimes \mathbf{B}$ (theo modulo 3)

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 2 \\ 0 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix} \text{ và } \mathbf{B} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix}$$

c. Fập F = {0, 1, 2} với phép cộng mod 3 và nhân mod 3 như trên có phải là một trường không, tại sao?

7. Xây dựng bảng cộng và nhân modulo 5 tương tự bảng trong bài tập 6. Tập F = {0, 1, 2, 3, 4} với các phép cộng và nhân modulo 5 có phải là một trường không? Tại sao?

8. Xây dựng bảng cộng và nhân modulo 6 như trong bài tập 6. Tập F = {0, 1, 2, 3, 4, 5} với các phép cộng và nhân modulo 6 có phải là một trường không? Tại sao?

9. Trong không gian vector F_2^3 , xét sự phụ thuộc tuyến tính của các hệ vector:

a/. { 000, 001, 100, 101 }

b/. {001, 100, 101}

c/. {001, 100}

d./ {101, 010, 111}

10. Trong không gian vector F_2^4 , xét sự phụ thuộc tuyến tính của các hệ vector:

a/. {0000, 0011, 1100, 1111}

b/. {0011, 0101, 0110}

c/. {0011, 1111}

d/. {1100, 0011}

11. Trong không gian vector F_3^4 , xét sự phụ thuộc tuyến tính của các hệ vector:

a/. {0000, 1011, 0112, 2022, 0221, 1120, 2210, 1202, 2101}.

b/. {1011, 0112, 2022}.

c/. {2022, 0221, 1120}.

d/. {0112, 0221}

e/. {1011, 0112}

12. Một bản tin có 5 ký hiệu được truyền đi. Xác suất để mỗi ký hiệu được nhận đúng đều bằng nhau $p = 0.9$ (do kênh truyền có nhiễu)

a/. Nếu gọi A_i là sự kiện kí hiệu thứ *i* được nhận đúng ($i = 1, 2, 3, 4, 5$), các sự kiện A*i* là các sự kiện gì: các sự kiện xung khắc từng đôi; các sự kiện độc lập ?

b/. Gọi A là sự kiện có đúng hai ký hiệu nhận đúng. Tính xác suất của sự kiện A.

c/. Gọi B là sự kiện có đúng 2 ký hiệu nhận sai, tính xác suất của sự kiện B.

d/. Mô tả các sự kiện $A \cup B$ và $A \cap B$. Tính các xác suất $P(A \cup B)$ và $P(A \cap B)$.

e/. Gọi C là sự kiện có ít nhất 3 ký hiệu nhận đúng, sự kiện đối lập với sự kiện C là sự kiện gì? Tính xác suất P(C) và $P(\overline{C})$.

g/. Khi gửi đi một xâu x = 00000, có bao nhiêu xâu nhị phân độ dài 5 có thể nhận được?

h/. Khi gửi đi xâu x = 00000, tính xác suất để nhận được chính xâu x, xác suất để nhận được xâu y = 00100, và xác suất để nhận được xâu z = 00111. Khi gửi đi xâu x = 00000 thì xâu nào có nhiều khả năng nhận được nhất, tại sao.

13. Tìm các cặp vector trực giao trong các không gian sau:

a/. Trong không gian $\boldsymbol{F}_2^6$, cho x = 100101 ; y = 110011 và z = 111111, tìm các cặp vector trực giao.

b/. Trong không gian $\boldsymbol{F}_3^5$, cho u = 12020 ; v = 21211 và w = 12101, tìm các cặp vector trực giao.