

C1: Tổng quan và Các khái niệm cơ bản

Lý thuyết thông tin

Biên soạn: Phạm Văn Sư

Bộ môn Xử lý tín hiệu và Truyền thông
Khoa Kỹ thuật Điện tử I
Học viện Công nghệ Bưu chính Viễn thông

ver. 22a



Mục tiêu của bài học

- Giới thiệu sơ lược về vai trò, lịch sử và hướng phát triển của môn khoa học Lý thuyết thông tin
 - Cung cấp các định nghĩa, khái niệm cơ bản nền tảng của Lý thuyết thông tin
 - Giới thiệu mô hình tổng quan của hệ thống truyền tin
 - Những khía cạnh đánh giá một hệ thống truyền tin



Notes

Notes

Các câu hỏi cần trả lời

- Môn khoa học Lý thuyết thông tin đóng vai trò gì với các môn khoa học khác?
- Những mốc thời gian cơ bản và những thành tựu của môn khoa học Lý thuyết thông tin cho đến nay?
- Hiện nay môn khoa học Lý thuyết thông tin được phát triển thế nào? theo những hướng nào? ví dụ minh họa các hướng này?
- Ba định nghĩa nền tảng của Lý thuyết thông tin là gì? T/c của chúng?
- Sơ đồ một hệ thống truyền tin cơ bản? Vai trò, chức năng và nguyên lý của các khôi trong sơ đồ?
- Để đánh giá một hệ thống truyền tin, chúng ta đánh giá theo các yếu tố nào?



Notes

C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

1 Sơ lược về môn Lý thuyết thông tin (LTTT)

- Vị trí và vai trò của Lý thuyết thông tin
- Lịch sử phát triển của môn LTTT
- Các bài toán thực tế của LTTT

2 Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

- Các khái niệm cơ bản
- Sơ đồ tổng quát của hệ thống truyền tin
- Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin
- Những tiêu chí đánh giá chất lượng một hệ thống thông tin



Notes

C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

1 Sơ lược về môn Lý thuyết thông tin (LTTT)

- Vị trí và vai trò của Lý thuyết thông tin
- Lịch sử phát triển của môn LTTT
- Các bài toán thực tế của LTTT

2 Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

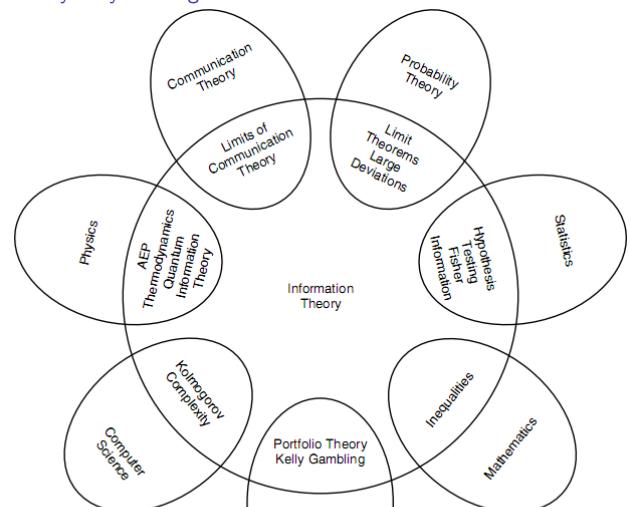
- Các khái niệm cơ bản
- Sơ đồ tổng quát của hệ thống truyền tin
- Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin
- Những tiêu chí đánh giá chất lượng một hệ thống thông tin



Notes

Sơ lược về môn Lý thuyết thông tin

Vị trí và vai trò của Lý thuyết thông tin



Notes

C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

1 Sơ lược về môn Lý thuyết thông tin (LTTT)

- Vị trí và vai trò của Lý thuyết thông tin
- Lịch sử phát triển của môn LTTT
- Các bài toán thực tế của LTTT

2 Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

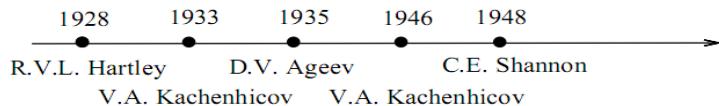
- Các khái niệm cơ bản
- Sơ đồ tổng quát của hệ thống truyền tin
- Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin
- Những tiêu chí đánh giá chất lượng một hệ thống thông tin



Notes

Sơ lược về môn Lý thuyết thông tin

Lịch sử phát triển của môn LTTT



Notes

C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

1 Sơ lược về môn Lý thuyết thông tin (LTTT)

- Vị trí và vai trò của Lý thuyết thông tin
- Lịch sử phát triển của môn LTTT
- Các bài toán thực tế của LTTT

2 Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

- Các khái niệm cơ bản
- Sơ đồ tổng quát của hệ thống truyền tin
- Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin
- Những tiêu chí đánh giá chất lượng một hệ thống thông tin



Notes

Sơ lược về môn Lý thuyết thông tin

Các bài toán thực tế của LTTT

- Nén dữ liệu (Data compression)
 - ▶ Giới hạn dưới của độ dài trung bình của các biểu diễn thông tin?
 - ▶ Với giới hạn "méo" cho trước, tốc độ mã hóa tối đa là bao nhiêu?
- Truyền dữ liệu (Data transmission)
 - ▶ Phương thức mã hóa kênh nào để phía thu có thể thu và giải mã với xác suất lỗi nhỏ nhất?
 - ▶ Một bộ mã hóa kênh tối ưu có thể đạt được cặp giá trị (R, p_e) ở đâu?
- Thông tin mạng (Network information theory)
 - ▶ Bài toán "Nén" và "Truyền" trong mạng gồm nhiều nguồn/người dùng?
- Suy luận (Inference)
 - ▶ Điều gì/kết cục gì sẽ xảy ra tiếp?
- Đánh bạc và đầu tư (Gambling and investment)
 - ▶ Giới hạn trên của "tốc độ nhân đôi" - cực đại tiệm cận lũy thừa của sự giàu có (tăng trưởng)?
- Tính toán độ phức tạp (Complexity theory)



Notes

C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

- Vị trí và vai trò của Lý thuyết thông tin
 - Lịch sử phát triển của môn LTTT
 - Các bài toán thực tế của LTTT

② Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản



C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

- Vị trí và vai trò của Lý thuyết thông tin
 - Lịch sử phát triển của môn LTTT
 - Các bài toán thực tế của LTTT

② Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

- Các khái niệm cơ bản
 - Sơ đồ tổng quát của hệ thống truyền tin
 - Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin
 - Những tiêu chí đánh giá chất lượng một hệ thống thông tin



Notes

Notes

Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

Các định nghĩa cơ bản (1)

Định nghĩa (Thông tin - Information)

Thông tin là những tính chất xác định của vật chất mà con người trực tiếp hoặc gián tiếp thông qua hệ thống kỹ thuật thu nhận được từ thế giới vật chất bên ngoài hoặc từ những quá trình xảy ra trong bản thân nó, nhằm mang lại sự hiểu biết về chúng.

- Khách quan
- Đa dạng

Định nghĩa (Tin - Message)

Tin là dạng vật chất cụ thể để biểu diễn hoặc thể hiện thông tin



- Tin liên tục
- Tin rời rạc

Notes

Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

Các định nghĩa cơ bản (2)

Định nghĩa (Tín hiệu - Signal)

Tín hiệu là các đại lượng vật lý biến thiên, phản ánh tin cần truyền.

- Sự biến đổi tham số riêng của quá trình vật lý mới là tín hiệu



Notes

C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

1 Sơ lược về môn Lý thuyết thông tin (LTTT)

- Vị trí và vai trò của Lý thuyết thông tin
- Lịch sử phát triển của môn LTTT
- Các bài toán thực tế của LTTT

2 Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

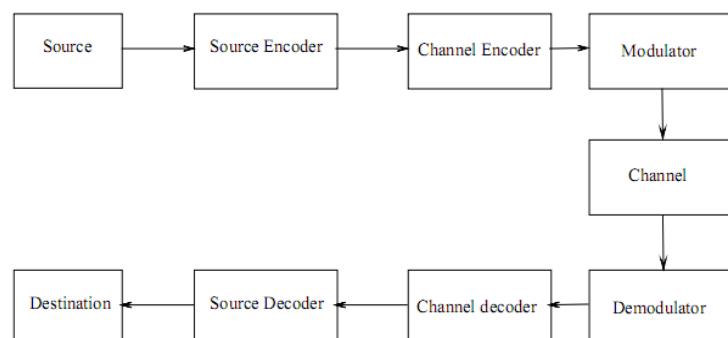
- Các khái niệm cơ bản
- **Sơ đồ tổng quát của hệ thống truyền tin**
- Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin
- Những tiêu chí đánh giá chất lượng một hệ thống thông tin



Notes

Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

Sơ đồ tổng quát của hệ thống truyền tin



Hình: Sơ đồ tổng quát hệ thống thông tin



Notes

Sơ đồ tổng quát của hệ thống truyền tin

Các khái niệm cơ bản (1)

Định nghĩa (Nguồn tin - Source)

Nguồn là nơi sản sinh ra tin.

- Đặc tính: Nguồn liên tục, nguồn rời rạc
- Tính chất: Thông kê, hàm ý

Định nghĩa (Máy phát - Transmitter)

Máy phát là thiết bị biến đổi tập tin thành tín hiệu tương ứng để truyền đi.

- Phép biến đổi phải đảm bảo tính song ánh (đơn trị 2 chiều)
- Tổng quát gồm: Mã hóa và điều chế



Notes

Sơ đồ tổng quát của hệ thống truyền tin

Các khái niệm cơ bản (2)

Định nghĩa (Kênh truyền tin - Channel)

Kênh truyền tin là tập hợp các môi trường vật lý trong đó tín hiệu được truyền đi từ nguồn đến nơi nhận tin.

- Kênh (channel) thường được hiểu là phần đường truyền tin từ phía phát đến phía thu.

Định nghĩa (Máy thu - Receiver)

Máy thu là thiết bị thu nhận tín hiệu và từ đó thiết lập lại thông tin.

- Máy thu thực hiện các phép biến đổi ngược máy phát.
- Tổng quát gồm: Giải điều chế và giải mã.



Notes

Sơ đồ tổng quát của hệ thống truyền tin

Các khái niệm cơ bản (3)

Định nghĩa (Nhận tin - Reception)

Là việc thu nhận thông tin nhằm sao lưu, biểu thị và xử lý tin.

Định nghĩa (Nhiễu - Noise)

Là các yếu tố có ảnh hưởng xấu đến việc thu nhận tin.



C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

1 Sơ lược về môn Lý thuyết thông tin (LTTT)

- Vị trí và vai trò của Lý thuyết thông tin
- Lịch sử phát triển của môn LTTT
- Các bài toán thực tế của LTTT

2 Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

- Các khái niệm cơ bản
- Sơ đồ tổng quát của hệ thống truyền tin
- Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin
- Những tiêu chí đánh giá chất lượng một hệ thống thông tin

Notes

Notes

Sơ đồ tổng quát của hệ thống truyền tin

Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin

- Định dạng và mã hóa nguồn - Sử dụng tối thiểu tài nguyên để biểu diễn tin một cách đầy đủ nhất: Lấy mẫu, lượng tử hóa, điều chế xung mã (PCM), PCM vi phân, mã Huffman, etc.
- Mã hóa kênh - Sử dụng tối thiểu tài nguyên để đảm bảo việc truyền nhận thông tin với lỗi ít nhất: mã hóa khối, mã hóa liên tục, etc.
- Điều chế - Truyền thông tin với tốc độ cao nhất, tốn ít năng lượng nhất: Điều chế dịch khóa pha (PSK), Điều chế dịch khóa tần (FSK), etc.
- Ghép kênh/đa truy nhập - Chia sẻ tài nguyên tốt nhất cho người dùng trong hệ thống: TDM/TDMA, CDMA, MC-CDMA, etc.
- Bảo mật - Đảm bảo tính bí mật, xác thực và toàn vẹn của tin trong quá trình truyền.



Notes

C1: Tổng quan và Các khái niệm cơ bản

Nội dung chính

1 Sơ lược về môn Lý thuyết thông tin (LTTT)

- Vị trí và vai trò của Lý thuyết thông tin
- Lịch sử phát triển của môn LTTT
- Các bài toán thực tế của LTTT

2 Sơ đồ tổng quát của hệ thống truyền tin và các khái niệm cơ bản

- Các khái niệm cơ bản
- Sơ đồ tổng quát của hệ thống truyền tin
- Sơ lược về các phương pháp xử lý thông tin trong hệ thống thông tin
- Những tiêu chí đánh giá chất lượng một hệ thống thông tin

Notes

Sơ đồ tổng quát của hệ thống truyền tin

Những tiêu chí đánh giá chất lượng một hệ thống thông tin

- Tính hiệu quả
 - ▶ Tốc độ truyền tin cao.
 - ▶ Truyền đồng thời nhiều tin khác nhau.
 - ▶ Chi phí cho một bít thông tin thấp.
 - Độ tin cậy cao.
 - ▶ Đảm bảo độ chính xác của việc nhận thông tin.
 - An toàn.
 - ▶ Bí mật (Confidentiality)
 - ▶ Xác thực (Authentication)
 - ▶ Toàn vẹn (Integrity)
 - ▶ Khả dụng (Availability)
 - Đảm bảo chất lượng dịch vụ (Quality of Service - QoS).



Notes

Notes

C2: Lý thuyết thông tin thống kê

Lý thuyết thông tin

Biên soạn: Phạm Văn Sư

Bộ môn Xử lý tín hiệu và Truyền thông
Khoa Kỹ thuật Điện tử I
Học viện Công nghệ Bưu chính Viễn thông

ver. 22a



Notes

Mục tiêu của bài học

- Công thức tính và đơn vị đo lường của thông tin
- Đánh giá lượng tin trung bình thống kê của nguồn
- Mối liên hệ về lượng tin giữa các nguồn thông tin
- Lượng thông tin trung bình truyền qua kênh



Notes

Các câu hỏi cần trả lời

- Một sự kiện xuất hiện sẽ mang lại một lượng tin bao nhiêu? Đơn vị lượng tin?
 - Lượng tin tiên nghiệm, hậu nghiệm, tương hỗ là gì? Ý nghĩa các đại lượng trong mô hình phát - thu? Giá trị và ý nghĩa của các đại lượng này trong hai trường hợp cực đoan của kênh?
 - Lượng thông tin trung bình thống kê của nguồn rời rạc không nhớ xác định thế nào? Tính chất? Áp dụng?
 - Mối quan hệ về lượng tin giữa các nguồn thông tin? Tính chất? Mối quan hệ giữa các đại lượng?
 - Lượng tin trung bình truyền qua kênh xác định thế nào?
 - Suy diễn các khái niệm tương tự cho nguồn liên tục?



Biên soạn: Phạm Văn Sư (PTIT)

C2: Lý thuyết thông tin thống kê

ver. 22a

3 / 48

Phần I

Lý thuyết thông tin thống kê cho nguồn rác



Biên soạn: Phạm Văn Sư (PTIT)

C2: Lý thuyết thông tin thống kê

ver. 22a

4 / 48

Notes

Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

1 Đo lường thông tin



C2: Lý thuyết thông tin thống kê

Nội dung chính

① Đo lường thông tin

- **Lượng tin riêng**
 - Lượng tin hậu nghiệm, lượng tin tương hỗ, hai trạng thái cực đoan của kênh
 - Entropy và các đại lượng liên quan của nguồn rời rạc
 - Entropy
 - Entropy của các trường sự kiện đồng thời
 - Entropy có điều kiện
 - Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
 - Tính chất và các mối quan hệ giữa các đại lượng



Notes

Notes

Đo lường thông tin

Lượng tin riêng: Ví dụ 1

Ví dụ

Chúng ta nhận được một bức thư.

- **TH1:** Đã biết hoặc đoán biết chắc chắn nội dung của bức thư → không có độ bất định: bức thư không mang lại thông tin.
- **TH2:** Không biết và có thể đoán biết không chắc chắn nội dung của bức thư → có độ bất định: bức thư mang lại một lượng thông tin.
- **TH3:** Không biết và không thể đoán biết không được nội dung của bức thư → độ bất định rất lớn: bức thư mang lại một lượng thông tin lớn.

⇒ Độ bất định: một đặc trưng quan trọng trong đo lường lượng thông tin.

- Lượng thông tin tỷ lệ thuận với độ bất định

⇒ Không có độ bất định: không có thông tin. ⇒ Lượng thông tin thu được bằng cách làm giảm độ bất định.



Đo lường thông tin

Lượng tin riêng: Ví dụ 2

Ví dụ

Một rổ đựng n bóng ($n = 1, 2, \dots$), các bóng được đánh nhãn từ 1 đến hết. Lấy ngẫu nhiên một bóng và quan sát nhãn của nó. Quan sát xác suất, độ bất định của sự kiện chúng ta lấy được một bóng có nhãn là "1".

n	Xác suất	Độ bất định
1	1	0
2	1/2	$\neq 0$
\vdots	\vdots	\vdots
∞	≈ 0	∞



Lượng thông tin: là một hàm giảm của xác suất xuất hiện của tin.

Notes

Notes

Đo lường thông tin

Lượng thông tin riêng: Định nghĩa

Nhận xét: Gọi x là một tin với xác suất xuất hiện $p(x)$, gọi $I(x)$ là đại lượng biểu diễn *lượng thông tin mà chúng ta thu được khi biết rằng x đã xảy ra (hoặc một cách tương đương, lượng độ bất định mất đi khi chúng ta biết x đã xảy ra)*

- ➊ $I(x)$: là một hàm của $p(x) \Rightarrow I(x) = I(p(x))$
 - ▶ $I(\cdot)$ là liên tục của $p(x)$ với $p(x) \in [0, 1]$; $I(p(x) = 1) = 0$.
 - ▶ $I(\cdot)$ là một hàm đơn điệu giảm theo $p(x)$.
 - ▶ $I(x) \geq 0$.
- ➋ Nếu x và y là hai tin độc lập thì $I(x \cap y) = I(x) + I(y)$
 - ▶ $I(p(x) \times p(y)) = I(p(x)) + I(p(y))$.

Dịnh nghĩa: Lượng thông tin riêng

Một tin (sự kiện) x với xác suất xuất hiện $p(x)$ thì việc nó xuất hiện sẽ mang lại lượng thông tin, hay còn gọi là lượng tin riêng/lượng thông tin tiên nghiệm, được xác định bởi:

$$I(x) \triangleq -\log(p(x))$$

Notes

Đo lường thông tin

Lượng thông tin riêng: Đơn vị

$$I(x_k) = -\log(p(x_k))$$

- Logarithm:
 - Cơ số 2: đơn vị [bit].
 - Cơ số $e = 2, 7 \dots$: đơn vị [nat].
 - Cơ số 10: đơn vị [hartley].

Ví dụ

Một bình đựng 2 viên bi màu đen và ba viên bi màu trắng. Thực hiện việc lấy ngẫu nhiên hai lần liên tiếp, mỗi lần một viên bi, bi đã được lấy không được bỏ lại bình. Gọi x là thông điệp cho chúng ta biết đã lấy được cả hai viên bi màu đen.

Tính lượng tin của thông điệp x .



Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

1 Đo lường thông tin

- Lượng tin riêng
- Lượng tin hậu nghiệm, lượng tin tương hổ, hai trạng thái cực đoan của kênh

2 Entropy và các đại lượng liên quan của nguồn rời rạc

- Entropy
- Entropy của các trường sự kiện đồng thời
- Entropy có điều kiện
- Entropy tương đối và Lượng thông tin tương hổ giữa các nguồn
- Tính chất và các mối quan hệ giữa các đại lượng

3 Lý thuyết thông tin thống kê cho nguồn liên tục

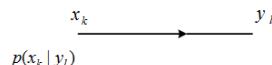
- Tín hiệu liên tục, Nguồn liên tục
- Entropy vi phân
- Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hổ giữa các nguồn liên tục



Notes

Đo lường thông tin

Lượng thông tin hậu nghiệm, lượng tin tương hổ, 2 trạng thái cực đoan của kênh



Biết đã nhận được tin $y_l \rightarrow$ tin x_k phát
đi với xác suất $p(x_k|y_l)$

- $I(x_k|y_l) \triangleq -\log(p(x_k|y_l))$: Lượng thông tin hậu nghiệm
 - ▶ Lượng tin riêng về x_k sau khi đã có (biết) y_l
- $I(x_k; y_l) \triangleq I(x_k) - I(x_k|y_l)$: Lượng thông tin chéo về x_k do y_l mang.
 - ▶ Lượng tin tương hổ giữa tin x_k và y_l
- $\Rightarrow I(x_k|y_l) = I(x_k) - I(x_k; y_l)$: Lượng thông tin tổn hao trên kênh.

Nhận xét:

- Kênh không có nhiễu: $I(x_k|y_l) = 0$; $I(x_k; y_l) = I(x_k)$
- Kênh bị đứt (bị nhiễu tuyệt đối): $I(x_k; y_l) = 0$, $I(x_k|y_l) = I(x_k)$.



Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

② Entropy và các đại lượng liên quan của nguồn rác



C2: Lý thuyết thông tin thống kê

Nội dung chính

② Entropy và các đại lượng liên quan của nguồn rác

- Entropy

- Entropy của các trường sự kiện đồng thời
 - Entropy có điều kiện
 - Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
 - Tính chất và các mối quan hệ giữa các đại lượng

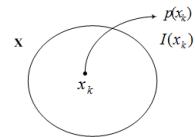


Notes

Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Entropy - Lượng tin trung bình thông kê của nguồn



X: nguồn rời rạc không nhớ (DMS) gồm các tin x_k xung khắc với xác suất xuất hiện $p(x_k)$

Định nghĩa (Entropy)

Entropy của nguồn rời rạc không nhớ X là trung bình thông kê của lượng thông tin riêng của các tin (phản tử) x_k (xung khắc) thuộc nguồn, ký hiệu là $H(X)$.

$$H(X) \triangleq E[I(x_k)] = \sum_{k=1}^N p(x_k)I(x_k) = -\sum_{k=1}^N p(x_k)\log(p(x_k)) \\ = E[-\log(p(x_k))]$$

- $H(X)$ còn được gọi là entropy một chiều của nguồn rời rạc.
- $H(X)$ có đơn vị của lượng thông tin (bit, nat, hartley).



Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

- ➊ Đo lường thông tin
 - Lượng tin riêng
 - Lượng tin hậu nghiệm, lượng tin tương hỗ, hai trạng thái cực đoan của kênh
- ➋ Entropy và các đại lượng liên quan của nguồn rời rạc

- Entropy
- Entropy của các trường sự kiện đồng thời
- Entropy có điều kiện
- Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
- Tính chất và các mối quan hệ giữa các đại lượng

- ➌ Lý thuyết thông tin thống kê cho nguồn liên tục

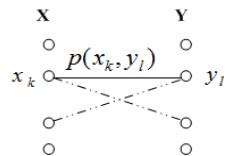
- Tín hiệu liên tục, Nguồn liên tục
- Entropy vi phân
- Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ giữa các nguồn liên tục



Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Entropy của các trường sự kiện đồng thời - Entropy hợp



Hình: Mô hình của cặp nguồn rời rạc X và Y

Định nghĩa (Entropy hợp)

Entropy hợp $H(X, Y)$ của một cặp nguồn rời rạc (X, Y) (còn gọi là Entropy của trường sự kiện đồng thời (X, Y)) với xác suất phân bố đồng thời của các tin x_k và y_l là $p(x_k, y_l)$ được cho bởi công thức:

$$\begin{aligned} H(X, Y) &\triangleq - \sum_{x_k \in X} \sum_{y_l \in Y} p(x_k, y_l) \log(p(x_k, y_l)) = - \sum_{k=1}^N \sum_{l=1}^M p(x_k, y_l) \log(p(x_k, y_l)) \\ &= E[-\log(p(x_k, y_l))]_{(x_k, y_l) \in (X, Y)} \end{aligned}$$

Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

1 Do lường thông tin

- Lượng tin riêng
- Lượng tin hậu nghiệm, lượng tin tương hỗ, hai trạng thái cực đoan của kênh

2 Entropy và các đại lượng liên quan của nguồn rời rạc

- Entropy
- Entropy của các trường sự kiện đồng thời
- Entropy có điều kiện
- Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
- Tính chất và các mối quan hệ giữa các đại lượng

3 Lý thuyết thông tin thống kê cho nguồn liên tục

- Tín hiệu liên tục, Nguồn liên tục
- Entropy vi phân
- Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương
giữa các nguồn liên tục



Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Entropy có điều kiện: Entropy có điều kiện từng phần (1/2)

Định nghĩa (Entropy có điều kiện từng phần - Partial Conditional Entropy)

Cho hai nguồn rời rạc X, Y . $H(X|Y = y_l)$ được gọi là Entropy có điều kiện từng phần, là Entropy có điều kiện về một nguồn tin này khi đã nhận được một tin nhất định của nguồn kia.

$$\begin{aligned} H(X|Y = y_l) &\triangleq E[I(x_k|Y = y_l)]_{x_k \in X|Y = y_l} \\ &= \sum_{x_k \in X} p(x_k|Y = y_l) I(x_k|Y = y_l) \\ &= - \sum_{x_k \in X} p(x_k|Y = y_l) \log(p(x_k|Y = y_l)) \\ &= - \sum_{k=1}^N p(x_k|y_l) \log(p(x_k|y_l)) \end{aligned}$$

$H(X|Y = y_l)$: lượng tin tổn hao trung bình của mỗi tin ở đầu phát khi đầu thu đã

Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Entropy có điều kiện: Entropy có điều kiện từng phần (2/2)

Định nghĩa (Entropy có điều kiện từng phần - Partial Conditional Entropy)

Cho hai nguồn rời rạc X, Y . $H(Y|X = x_k)$ được gọi là Entropy có điều kiện từng phần, là Entropy có điều kiện về một nguồn tin này khi đã phát đi một tin nhất định của nguồn kia.

$$\begin{aligned} H(Y|X = x_k) &\triangleq E[I(y_l|X = x_k)]_{y_l \in Y|X = x_k} \\ &= \sum_{y_l \in Y} p(y_l|X = x_k) I(y_l|X = x_k) \\ &= - \sum_{y_l \in Y} p(y_l|X = x_k) \log(p(y_l|X = x_k)) \\ &= - \sum_{l=1}^M p(y_l|x_k) \log(p(y_l|x_k)) \end{aligned}$$

$H(Y|X = x_k)$: lượng tin riêng trung bình chứa trong mỗi tin ở đầu thu khi đầu

Notes

Entropy và các đại lượng liên quan của nguồn rác

Entropy có điều kiện (1/2)

Định nghĩa (Entropy có điều kiện)

Với một cặp nguồn rời rạc (X, Y) có xác suất phân bố hợp $p(x_k, y_l)$, xác suất phân bố có điều kiện $p(x_k|y_l)$, Entropy có điều kiện $H(X|Y)$ được cho bởi công thức:

$$\begin{aligned}
H(X|Y) &\triangleq E[H(X|Y = y_l)]_{y_l \in Y} = \sum_{y_l \in Y} p(y_l) H(X|Y = y_l) \\
&= - \sum_{y_l \in Y} p(y_l) \sum_{x_k \in X} p(x_k|y_l) \log(p(x_k|y_l)) \\
&= - \sum_{k=1}^N \sum_{l=1}^M p(x_k, y_l) \log(p(x_k|y_l)) \\
&= E[-\log(p(X|Y))]_{p(x_k, y_l)}
\end{aligned}$$

$H(X|Y)$: lượng tin riêng tồn hao trung bình của mỗi tin ở đầu phát khi đầu thu đã thu được một tin nào đó.

Biên soạn: Phạm Văn Sư (PTIT)

C2: Lý thuyết thông tin thống kê

ver. 22a

22 / 48

Entropy và các đại lượng liên quan của nguồn rác

Entropy có điều kiện (2/2)

Định nghĩa (Entropy có điều kiện)

Với một cặp nguồn rời rạc (X, Y) có xác suất phân bố hợp $p(x_k, y_l)$, xác suất phân bố có điều kiện $p(x_k|y_l)$, Entropy có điều kiện $H(Y|X)$ được cho bởi công thức:

$$\begin{aligned}
H(Y|X) &\triangleq E[H(Y|X = x_k)]_{x_k \in X} = \sum_{x_k \in X} p(x_k) H(Y|X = x_k) \\
&= - \sum_{x_k \in X} p(x_k) \sum_{y_l \in Y} p(y_l|x_k) \log(p(y_l|x_k)) \\
&= - \sum_{k=1}^N \sum_{l=1}^M p(x_k, y_l) \log(p(y_l|x_k)) \\
&= E[-\log(p(Y|X))]_{p(x_k, y_l)}
\end{aligned}$$

$H(Y|X)$: lượng tin riêng trung bình chứa trong mỗi tin ở đầu thu khi đầu phát đã
phát đi một tin nào đó.

Biên soạn: Phạm Văn Sư (PTIT)

C2: Lý thuyết thông tin thống kê

ver. 22a

23 / 48

Notes

Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

1 Do lường thông tin

- Lượng tin riêng
- Lượng tin hậu nghiệm, lượng tin tương hỗ, hai trạng thái cực đoan của kênh

2 Entropy và các đại lượng liên quan của nguồn rời rạc

- Entropy
- Entropy của các trường sự kiện đồng thời
- Entropy có điều kiện
- Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
- Tính chất và các mối quan hệ giữa các đại lượng

3 Lý thuyết thông tin thống kê cho nguồn liên tục

- Tín hiệu liên tục, Nguồn liên tục
- Entropy vi phân
- Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ giữa các nguồn liên tục



Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Entropy tương đối và lượng thông tin tương hỗ giữa các nguồn: Entropy tương đối

Định nghĩa (Entropy tương đối - Relative Entropy)

Entropy tương đối, còn gọi là khoảng cách Kullback Leibler giữa hai phân bố rời rạc $p(x_k)$ và $q(x_k)$ của một nguồn rời rạc X được xác định bởi:

$$D(p||q) \triangleq \sum_{k=1}^N p(x_k) \log \left(\frac{p(x_k)}{q(x_k)} \right)$$

- Quy ước: $0 \log(\frac{0}{q}) = 0$; $p \log(\frac{p}{0}) = \infty$
- Tính chất:
 - ▶ $D(p||q) \geq 0$, $D(p||q) = 0$ nếu và chỉ nếu $p(x_k) = q(x_k)$
 - ▶ Tổng quát $D(p||q) \neq D(q||p)$
 - ▶ Không thỏa mãn $D(p||q) + D(q||r) \geq D(p||r) \Rightarrow$ không phải khoảng cách thông thường.



Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Entropy tương đối và lượng thông tin tương hỗ giữa các nguồn: Lượng thông tin tương hỗ giữa các nguồn

Định nghĩa (Lượng thông tin tương hỗ - Mutual Information)

Cho hai nguồn rời rạc X, Y có các xác suất phân bố hợp, phân bố riêng, và phân bố có điều kiện lần lượt là $p(x_k, y_l)$, $p_X(x_k) = p(x_k)$, $p_Y(y_l) = p(y_l)$, và $p(x_k|y_l)$. Lượng thông tin tương hỗ, còn gọi là lượng thông tin chéo trung bình của hai nguồn được xác định bởi:

$$\begin{aligned} I(X; Y) &\triangleq E[I(x_k; y_l)] = \sum_{k=1}^N \sum_{l=1}^M p(x_k, y_l) \log\left(\frac{p(x_k|y_l)}{p(x_k)}\right) \\ &= \sum_{k=1}^N \sum_{l=1}^M p(x_k, y_l) \log\left(\frac{p(x_k, y_l)}{p(x_k)p(y_l)}\right) \\ &= D(p(x_k, y_l)||p(x_k)p(y_l)) \end{aligned}$$

- $I(X; Y)$: lượng thông tin mà X cho biết về Y cũng như lượng thông tin Y cho biết về X .

Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

1 Do lường thông tin

- Lượng tin riêng
- Lượng tin hậu nghiệm, lượng tin tương hỗ, hai trạng thái cực đoan của kênh

2 Entropy và các đại lượng liên quan của nguồn rời rạc

- Entropy
- Entropy của các trường sự kiện đồng thời
- Entropy có điều kiện
- Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
- Tính chất và các mối quan hệ giữa các đại lượng

3 Lý thuyết thông tin thống kê cho nguồn liên tục

- Tín hiệu liên tục, Nguồn liên tục
- Entropy vi phân
- Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ giữa các nguồn liên tục

Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Tính chất và các mối quan hệ giữa các đại lượng: Các tính chất của Entropy, ví dụ minh họa

- $H(X) \geq 0$, $H(X) = 0$ khi và chỉ khi $p(x_k) = 1$ và $p(x_r) = 0$ ($\forall r \neq k$)
- $H(X) \leq \log |X| = \log(N)$, $H(X) = \log(N)$ khi và chỉ khi các x_k có phân bố xác suất đồng đều, $p(x_k) = 1/N \forall k$
- $H(X)$ là một hàm chỉ phụ thuộc vào đặc tính thống kê của nguồn
- $H_b(X) = (\log_b(a))H_a(X)$, $H_a(X)$: entropy được tính với cơ số a ; Quy ước: $H(X)$ cơ số 2.



Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Tính chất và các mối quan hệ giữa các đại lượng: Các tính chất của Entropy có điều kiện, Entropy hợp (1/2)

$$0 \leq H(X|Y) \leq H(X); 0 \leq H(Y|X) \leq H(Y)$$

- Đạt đẳng thức phía phải khi và chỉ khi X và Y là độc lập: kênh bị đứt.
- Đạt đẳng thức phía trái khi và chỉ khi kênh hoàn hảo.

Nếu X và Y độc lập

- $H(X|Y = y_l) = H(X); H(X|Y) = H(X).$
- $H(Y|X = x_k) = H(Y); H(Y|X) = H(Y).$

Trường hợp tổng quát $H(X|Y) \neq H(Y|X)$.

$$H(X, Y) = H(Y, X) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

$$H(X_1, X_2, \dots, X_n) = \sum_{i=1}^n H(X_i|X_{i-1}, X_{i-2}, \dots, X_1)$$

Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Tính chất và các mối quan hệ giữa các đại lượng: Các tính chất của Entropy có điều kiện, Entropy hợp (2/2)

$$H(X, Y) \leq H(X) + H(Y)$$

$$H(X_1, X_2, \dots, X_n) \leq \sum_{i=1}^n H(X_i)$$

- Xảy ra đẳng thức khi và chỉ khi X và Y độc lập: kênh bị đứt.

$$H(X, Y|Z) = H(X|Z) + H(Y|X, Z).$$

Cho nguồn rời rạc X , $g()$ là một hàm mô tả quan hệ toán học xác định, khi đó:

- $H(g(X)|X) = 0$
- $H(X|g(X)) \geq 0$
- $H(X) \geq H(g(X))$
 - ▶ Xảy ra đẳng thức khi và chỉ khi $g()$ là quan hệ toán học 1 – 1.

Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Tính chất và các mối quan hệ giữa các đại lượng: Các tính chất của lượng tin tương hỗ

$$0 \leq I(X; Y) \leq H(X), 0 \leq I(X; Y) \leq H(Y)$$

- Xảy ra đẳng thức bên phải khi và chỉ khi X và Y độc lập
- Xảy ra đẳng thức bên trái khi và chỉ khi kênh lý tưởng không nhiễu

$$I(X; Y) = I(Y; X)$$

- Lượng thông tin mà X cho biết về Y cũng bằng lượng thông tin mà Y cho biết về X .

$$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

- $I(X; Y)$: lượng giảm độ bất định trung bình của X do việc biết Y .

$$I(X; Y) = H(X) + H(Y) - H(X, Y)$$

CHỦ ĐỀ

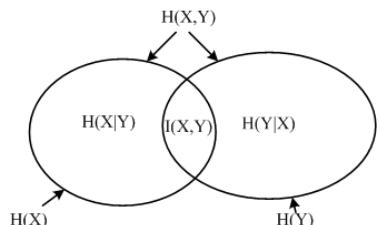
$$I(X; X) = H(X)$$

- $H(X)$: lượng thông tin riêng trung bình của X .

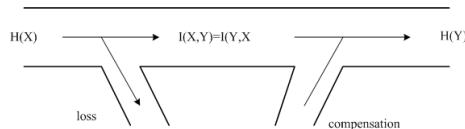
Notes

Entropy và các đại lượng liên quan của nguồn rời rạc

Tính chất và các mối quan hệ giữa các đại lượng: Biểu diễn mối liên hệ giữa các đại lượng



(a) Biểu đồ Venn



(b) Sơ đồ kênh



Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

1 Do lường thông tin

- Lượng tin riêng
- Lượng tin hậu nghiệm, lượng tin tương hỗ, hai trạng thái cực đoan của kênh

2 Entropy và các đại lượng liên quan của nguồn rời rạc

- Entropy
- Entropy của các trường sự kiện đồng thời
- Entropy có điều kiện
- Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
- Tính chất và các mối quan hệ giữa các đại lượng

3 Lý thuyết thông tin thống kê cho nguồn liên tục

- Tín hiệu liên tục, Nguồn liên tục
- Entropy vi phân
- Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ giữa các nguồn liên tục



Notes

Phần II

Lý thuyết thông tin thống kê cho nguồn liên tục



Biên soạn: Phạm Văn Sư (PTIT)

C2: Lý thuyết thông tin thống kê

ver. 22a

34 / 48

C2: Lý thuyết thông tin thống kê

Nội dung chính

③ Lý thuyết thông tin thống kê cho nguồn liên tục

- Tín hiệu liên tục, Nguồn liên tục
 - Entropy vi phân
 - Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương H các nguồn liên tục



Biên soạn: Phạm Văn Sư (PTIT)

C2: Lý thuyết thông tin thống kê

ver. 22a

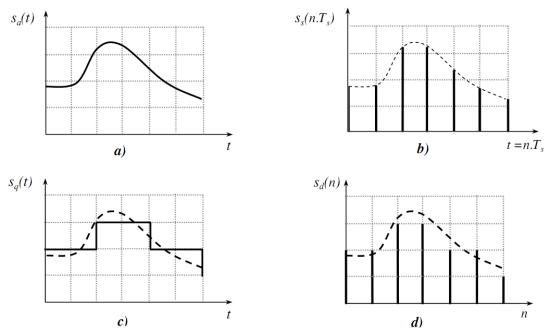
35 / 48

Notes

Notes

Tín hiệu liên tục, nguồn liên tục

Tín hiệu liên tục: Minh họa đồ thị các loại tín hiệu



Tín hiệu:

- Biểu diễn: hàm toán học của các biến độc lập
- Đặc trưng tín hiệu liên tục: Công suất phổ trung bình, bề rộng phổ



Notes

Tín hiệu liên tục, nguồn liên tục

Nguồn liên tục

Nguồn liên tục

Nguồn tin X phát ra các tin x có giá trị liên tục trong khoảng $x_{min} \div x_{max}$ với hàm mật độ phân bố xác suất $f(x)$

Mô hình toán học nguồn liên tục

- Biến ngẫu nhiên liên tục X với hàm mật độ phân bố xác suất $f(x)$



Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

1 Do lường thông tin

- Lượng tin riêng
- Lượng tin hậu nghiệm, lượng tin tương hỗ, hai trạng thái cực đoan của kênh

2 Entropy và các đại lượng liên quan của nguồn rời rạc

- Entropy
- Entropy của các trường sự kiện đồng thời
- Entropy có điều kiện
- Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
- Tính chất và các mối quan hệ giữa các đại lượng

3 Lý thuyết thông tin thống kê cho nguồn liên tục

- Tín hiệu liên tục, Nguồn liên tục
- **Entropy vi phân**
- Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ giữa các nguồn liên tục



Notes

Entropy vi phân

Định nghĩa (Entropy vi phân - Differential Entropy)

Entropy vi phân của một nguồn liên tục X có hàm mật độ phân bố xác suất $f(x)$ được xác định bởi:

$$h(X) \triangleq - \int_S f(x) \log(f(x)) dx$$

trong đó, S là miền xác định dương (support set: tập trên đó $f(x) \geq 0$) của X .

- $h(X)$ mặc định chỉ xét trên điều kiện các hàm liên tục, xác định và khả tích.
- $h(X) = h(f)$

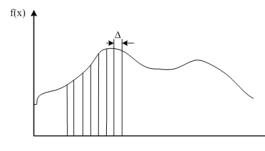
Ví dụ

Cho X là một nguồn liên tục có hàm mật độ phân bố xác suất đều (uniform distribution) trong đoạn $[a, b]$. Tính $h(X)$.

Notes

Entropy vi phân

Mối quan hệ giữa Entropy vi phân và Entropy rời rạc



- $X \rightarrow X^\Delta = \{x_i\}$
 $(i\Delta \leq X \leq (i+1)\Delta)$.
- $p(X^\Delta = x_i) = p(x_i) = f(x_i)\Delta = \int_{i\Delta}^{(i+1)\Delta} f(x)dx$

- $\rightarrow H(X^\Delta) = -\sum_{-\infty}^{\infty} f(x_i)\Delta \log(f(x_i)\Delta) = -\sum_{-\infty}^{\infty} \Delta f(x_i) \log(f(x_i)) + \log(1/\Delta)$

Định lý

Một nguồn liên tục X với hàm mật độ phân bố xác suất $f(x)$ khả tích theo tiêu chuẩn Riemann thì:

$$H(X^\Delta) + \log(\Delta) \rightarrow h(X) \text{ khi } \Delta \rightarrow 0$$

- Entropy của một nguồn rời rạc thu được từ nguồn liên tục X bằng phép
- lượng tử hóa sử dụng n bít có giá trị xấp xỉ bằng $h(X) + n$

Notes

Entropy vi phân

Mô hình Entropy của nguồn liên tục

$$\lim_{\Delta \rightarrow 0} \log\left(\frac{1}{\Delta}\right) \rightarrow \infty \Rightarrow H(X) \text{ lớn vô hạn.}$$

Ví dụ

Xét việc truyền thông tin từ nguồn liên tục X đến nguồn Y bằng dây dẫn lý tưởng (không tổn hao, không nhiễu). Tín hiệu phát $x(t)$ nhận các giá trị liên tục trong khoảng $[0, 1]$ (V). Ở đầu thu Y ta đặt một vòi kết lý tưởng (tập âm nội bằng 0, $Z_V = \infty$). Khi đó việc thu tín hiệu thỏa mãn $y(t) = x(t)$. Xem xét việc lượng tử hóa, và tính toán $H(X)$.

Lượng tử đều:

- 10 mức $\Delta = 0, 1: X^\Delta = \{x_i\}$
 $(i = 1, 10) \Rightarrow H(X^\Delta) = \log(10).$
- $\Delta = 0, 01 \Rightarrow H(X^\Delta) = \log(100).$
- $\Delta \rightarrow 0 \Rightarrow H(X^\Delta) \rightarrow H(X) \rightarrow \infty.$



Notes

Entropy vi phân

Một số tính chất

- $h(X)$ có thể âm, dương.
- $h(X)$ có giá trị hữu hạn.
- Với một hằng số c : $h(X + c) = h(X)$
- Với một hằng số $c \neq 0$: $h(cX) = h(X) + \log(|c|)$
 - ▶ $h(X)$ phụ thuộc vào thang tỷ lệ (đơn vị đo)

Định lý

Trong số những quá trình ngẫu nhiên (tín hiệu) có cùng công suất trung bình $P_x = \sigma^2$, quá trình (tín hiệu) có hàm mật độ phân bố chuẩn (phân bố Gausse) sẽ cho Entropy vi phân lớn nhất. Nói cách khác

$$h(X) \leq \log(\sqrt{2\pi e P_x})$$

- Trong số các tín hiệu nhiễu (tạp âm) có cùng công suất trung bình, tín hiệu nhiễu Gausse có tác hại lớn nhất với việc truyền tin.

Notes

C2: Lý thuyết thông tin thống kê

Nội dung chính

- ➊ Đo lường thông tin
 - Lượng tin riêng
 - Lượng tin hậu nghiệm, lượng tin tương hỗ, hai trạng thái cực đoan của kênh
- ➋ Entropy và các đại lượng liên quan của nguồn rời rạc
 - Entropy
 - Entropy của các trường sự kiện đồng thời
 - Entropy có điều kiện
 - Entropy tương đối và Lượng thông tin tương hỗ giữa các nguồn
 - Tính chất và các mối quan hệ giữa các đại lượng
- ➌ Lý thuyết thông tin thống kê cho nguồn liên tục
 - Tín hiệu liên tục, Nguồn liên tục
 - Entropy vi phân
 - Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ giữa các nguồn liên tục

Notes

Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ của các nguồn liên tục

Entropy vi phân hợp, Entropy vi phân có điều kiện

Định nghĩa (Entropy vi phân hợp)

Entropy vi phân hợp của cặp nguồn liên tục (X, Y) với hàm mật độ phân bố hợp (phân bố đồng thời) $f(x, y)$, được định nghĩa:

$$h(X, Y) \triangleq - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \log(f(x, y)) dx dy$$

Định nghĩa (Entropy vi phân có điều kiện)

Các Entropy vi phân có điều kiện của cặp nguồn liên tục (X, Y) với hàm mật độ phân bố hợp (phân bố đồng thời) $f(x, y)$, được định nghĩa:

$$h(X|Y) \triangleq - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \log(f(x|y)) dx dy$$

$$h(Y|X) \triangleq - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \log(f(y|x)) dx dy$$

Notes

Lượng thông tin tương hỗ của các nguồn liên tục

Định nghĩa (Entropy vi phân tương đối)

Xét một nguồn liên tục X , với nguồn X giả sử có hai phân bố $f(x)$ và $g(x)$.

Entropy vi phân tương đối hay còn gọi là khoảng cách Kullback Leibler được tính bằng công thức:

$$D(f(x)||g(x)) \triangleq \int_S f(x) \log\left(\frac{f(x)}{g(x)}\right) dx$$

- $D(f||g) < \infty$ iff miền xác định (support set) của $f()$ chứa miền của $g()$.
- Quy ước $0 \log \frac{0}{0} = 0$

Định nghĩa (Lượng thông tin tương hỗ)

Lượng thông tin tương hỗ $I(X; Y)$ giữa hai nguồn liên tục X và Y có xác suất phân bố hợp $f(x, y)$ được xác định bởi công thức:

$$I(X; Y) \triangleq \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \log\left(\frac{f(x, y)}{f(x)f(y)}\right) dx dy$$

Notes

Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ của các nguồn liên tục

Một số tính chất (1)

$$h(X, Y) = h(X) + h(Y|X) = h(Y) + h(X|Y)$$

$$h(X_1, X_2, \dots, X_n) = \sum_{i=1}^n h(X_i | X_{i-1}, \dots, X_1)$$

$$h(X|Y) \leq h(X); h(Y|X) \leq h(Y)$$

- Xảy ra đẳng thức khi và chỉ khi X và Y độc lập nhau.

$$h(X_1, X_2, \dots, X_n) \leq \sum_{i=1}^n h(X_i)$$

$$D(f(x)|g(x)) \geq 0$$

- Xảy ra đẳng thức iff $f() = g()$ trên gần toàn miền xác định.

LÝ THUYẾT THÔNG

Notes

Entropy vi phân hợp, Entropy vi phân có điều kiện, Lượng tin tương hỗ của các nguồn liên tục

Một số tính chất (2)

$$I(X; Y) = D(f(x, y)|f(x)f(y))$$

$$I(X; Y) \geq 0$$

- Xảy ra đẳng thức iff X và Y độc lập nhau.

$$I(X; Y) = I(Y; X)$$

$$I(X; Y) = h(X) - h(X|Y) = h(Y) - h(Y|X)$$

$$I(X^\Delta; Y^\Delta) \approx I(X; Y)$$

- $I(X; Y)$ là giới hạn của lượng thông tin tương hỗ giữa các nguồn rời rạc hóa (lượng tử hóa) tương ứng.

Notes

Kết thúc bài học



Biên soạn: Phạm Văn Sư (PTIT)

C2: Lý thuyết thông tin thống kê

ver. 22a

48 / 48

Notes

Notes

C2(cont.): Dung lượng kênh

Lý thuyết thông tin

Biên soạn: Phạm Văn Sư

Bộ môn Xử lý tín hiệu và Truyền thông
Khoa Kỹ thuật Điện tử I
Học viện Công nghệ Bưu chính Viễn thông

ver. 22a



Notes

Mục tiêu của bài học

- Trang bị một số khái niệm cơ bản về kênh truyền
- Cách xác định dung lượng của kênh
- Mối quan hệ giữa tốc độ dữ liệu và dung lượng kênh để đảm bảo truyền tin tin cậy



Notes

Các câu hỏi cần trả lời

- Tốc độ dữ liệu đầu vào kênh được đánh giá thế nào?
 - Thế nào là kênh giãn tin? kênh nén tin? kênh thông thường?
 - Thế nào là kênh rời rạc không nhớ? Kênh đôi xứng? Kênh đồng nhất?
 - Lượng tin trung bình truyền qua kênh rời rạc không nhớ?
 - Dung lượng của một kênh rời rạc không nhớ xác định bằng công thức nào?
Có tính chất gì? Cách xác định cho các bài toán cụ thể?
 - Thế nào là một kênh AWGN? Mô hình?
 - Lượng tin trung bình truyền qua kênh AWGN?
 - Dung lượng của một kênh AWGN được xác định thế nào? Dung lượng một kênh AWGN có băng thông hữu hạn?
 - Định lý mã hóa thứ hai của Shannon?



Biên soạn: Phạm Văn Sư (PTIT)

C2(cont.): Dung lượng kênh

ver. 22a

3 / 27

C2(cont.): Dung lượng kênh

Nội dung chính

1 Dung lượng kênh rác

- Khả năng phát của nguồn rời rạc
 - Kênh rời rạc và một số khái niệm
 - Dung lượng kênh rời rạc
 - Định lý mã hóa thứ hai của Shannon

- Kênh Gausse nhiễu trắng cộng - AWGN
 - Dung lượng của kênh AWGN



Biên soạn: Phạm Văn Sư (PTIT)

C2(cont.): Dung lượng kênh

ver. 22a

4 / 27

Notes

Notes

C2(cont.): Dung lượng kênh

Nội dung chính

1 Dung lượng kênh rác

- Khả năng phát của nguồn rời rạc
 - Kênh rời rạc và một số khái niệm
 - Dung lượng kênh rời rạc
 - Định lý mã hóa thứ hai của Shannon

- Kênh Gausse nhiễu trắng cộng - AWGN
 - Dung lượng của kênh AWGN



Tốc độ phát, khả năng phát của nguồn rác

Tốc độ phát, khả năng phát của nguồn rác

Định nghĩa (Tốc độ phát của nguồn rời rạc)

Tốc độ phát của một nguồn rời rạc được định nghĩa $v_n = \frac{1}{T_n}$

- T_n : độ rộng trung bình của mỗi xung phát.
 - v_p : số xung phát trong một đơn vị thời gian, v_p : đơn vị [baud]

Định nghĩa (Khả năng phát của nguồn rời rac)

Một nguồn rời rạc X có tốc độ phát $v_n = \frac{1}{T_n}$, khi đó khả năng phát của nguồn được xác định:

$$H'(X) = v_n H(X) = \frac{H(X)}{T_n}$$

- $H'(X)$: lượng thông tin trung bình do nguồn phát ra trong một đơn vị thời gian, Đơn vị [bit/s]
 - $H'(X)_{\max} = v_n \log(N) = \log(N)/T_p$

Notes

Notes

Tốc độ phát, khả năng phát của nguồn rời rạc

Độ dư thừa của nguồn

Dịnh nghĩa (Độ dư thừa của nguồn rời rạc)

Với một nguồn rời rạc X , một phép xử lý thông tin đạt được $H(X)$, khi đó độ dư thừa của nguồn được định nghĩa là:

$$D = \frac{H(X)_{\max} - H(X)}{H(X)_{\max}} = 1 - \frac{H(X)}{H(X)_{\max}} = 1 - \mu$$

- $\mu = \frac{H(X)}{H(X)_{\max}}$: là tỷ số nén tin.
- D đặc trưng cho hiệu suất, khả năng chống nhiễu và mật độ của tin
 - ▶ D lớn \Rightarrow hiệu suất thấp, khả năng chống nhiễu cao.



Notes

C2(cont.): Dung lượng kênh

Nội dung chính

1 Dung lượng kênh rời rạc

- Khả năng phát của nguồn rời rạc
- Kênh rời rạc và một số khái niệm
- Dung lượng kênh rời rạc
- Định lý mã hóa thứ hai của Shannon

2 Dung lượng kênh Gausse nhiễu trắng cộng

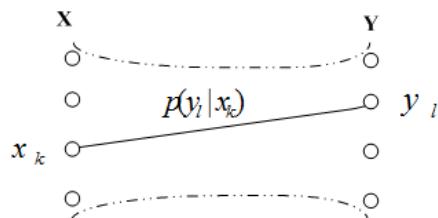
- Kênh Gausse nhiễu trắng cộng - AWGN
- Dung lượng của kênh AWGN



Notes

Kênh rời rạc và một số khái niệm

Đặc trưng của kênh rời rạc



Một kênh rời rạc hoàn toàn có thể đặc trưng bởi 3 tham số:

- Trường tin lối vào X (input), trường tin lối ra Y (output).
- Xác suất chuyển tin lối vào x_k thành tin lối ra y_l : $p(y_l|x_k)$.
- Tốc độ truyền tin của kênh v_k hay thời gian trung bình để truyền một dấu tin
 $T_k = \frac{1}{v_k}$.



Notes

Kênh rời rạc và một số khái niệm

Đặc trưng của kênh rời rạc - Một số khái niệm

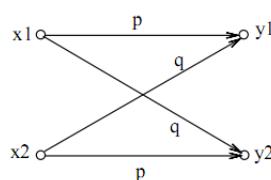
Định nghĩa (Kênh đồng nhất)

Xét một kênh rời rạc có xác suất chuyển $p(y_l|x_k)$.

- Nếu $p(y_l|x_k)$ không phụ thuộc vào thời gian t thì kênh được gọi là kênh đồng nhất; ngược lại gọi là kênh không đồng nhất.

Định nghĩa (Kênh đối xứng)

Xét một kênh rời rạc có xác suất chuyển $p(y_l|x_k)$. Nếu $p(y_l|x_k) = p = \text{const } \forall k, l$, $k \neq l$ và $p(y_l|x_k) = q = \text{const } \forall k = l$ thì kênh được gọi là đối xứng.



Hình: Mô hình kênh nhị phân đối xứng (BSC)

Notes

Kênh rời rạc và một số khái niệm

Đặc trưng của kênh rời rạc - Một số khái niệm (cont.)

Định nghĩa (Kênh không có nhớ)

Nếu $p(y_l|x_k)$ không phụ thuộc vào các tin (kí hiệu) phát/nhận trước đó thì kênh được gọi là kênh không có nhớ (memoryless):

$$p(y_l|x_k, x_{k-1}, \dots, x_1, y_{l-1}, \dots, y_1) = p(y_l|x_k)$$

- Nếu y_k tương ứng với tin phát $x_k \Rightarrow$

$$p(y_1, y_2, \dots, y_n|x_1, x_2, \dots, x_n) = \prod_{k=1}^n p(y_k|x_k)$$

Biểu diễn kênh:

- Giản đồ chuyển trên đó nhän các đường chuyển là các $p(y_l|x_k)$
- Các ma trận xác suất chuyển $P = [p_{kl}]$ với $p_{kl} = p(y_l|x_k)$

$$P = \begin{bmatrix} p(y_1|x_1) & p(y_2|x_1) & \dots & p(y_M|x_1) \\ p(y_1|x_2) & p(y_2|x_2) & \dots & p(y_M|x_2) \\ \vdots & \vdots & \ddots & \vdots \\ p(y_1|x_N) & p(y_2|x_N) & \dots & p(y_M|x_N) \end{bmatrix}$$



Notes

Kênh rời rạc và một số khái niệm

Lượng thông tin truyền qua kênh trong một đơn vị thời gian

Định nghĩa

Một kênh rời rạc có lượng tin truyền qua $I(X; Y)$ với tốc độ truyền tin v_k thì lượng thông tin truyền qua kênh trong một đơn vị thời gian là:

$$I'(X; Y) = v_k I(X; Y) = \frac{I(X; Y)}{T_k}$$

- $T_k > T_n$: kênh giãn tin
- $T_k = T_n$: kênh thông thường
- $T_k < T_n$: kênh nén tin



Notes

C2(cont.): Dung lượng kênh

Nội dung chính

1 Dung lượng kênh rời rạc

- Khả năng phát của nguồn rời rạc
- Kênh rời rạc và một số khái niệm
- Dung lượng kênh rời rạc
- Định lý mã hóa thứ hai của Shannon

2 Dung lượng kênh Gausse nhiễu trắng cộng

- Kênh Gausse nhiễu trắng cộng - AWGN
- Dung lượng của kênh AWGN



Notes

Dung lượng kênh rời rạc

Định nghĩa (Khả năng thông qua của kênh rời rạc)

Khả năng thông qua của kênh rời rạc là giá trị cực đại của lượng thông tin truyền qua kênh trong một đơn vị thời gian lấy theo mọi khả năng có thể của phân bố nguồn phát.

$$\begin{aligned} C' &= \max_{p(X)} I'(X; Y) = \max_X I'(X; Y) = v_k \max_X I(X; Y) \quad [\text{bit/s}] \\ &= v_k C \end{aligned}$$

- $C = \max_X I(X; Y)$: khả năng thông qua của kênh đối với mỗi dấu.
 - C : đơn vị [bit/lần truyền]
 - C : thường được sử dụng.

Tính chất:

- $C' \geq 0$, $C' = 0$ khi và chỉ khi X và Y hoàn toàn độc lập \Rightarrow kênh bị đứt
- $C' \leq v_k \log(N)$ (N là độ lớn của nguồn X)
- $C' \leq v_k \log(M)$ (M là độ lớn của nguồn Y)



Notes

C2(cont.): Dung lượng kênh

Nội dung chính

1 Dung lượng kênh rời rạc

- Khả năng phát của nguồn rời rạc
- Kênh rời rạc và một số khái niệm
- Dung lượng kênh rời rạc
- Dịnh lý mã hóa thứ hai của Shannon

2 Dung lượng kênh Gausse nhiễu trắng cộng

- Kênh Gausse nhiễu trắng cộng - AWGN
- Dung lượng của kênh AWGN



Notes

Định lý mã hóa thứ hai của Shannon

Định lý mã hóa thứ hai của Shannon

Định lý

Nếu khả năng phát $H'(X)$ của một nguồn rời rạc X nhỏ hơn khả năng thông qua của kênh ($H'(X) \leq C'$) thì tồn tại một phép mã hóa và giải mã sao cho việc truyền tin qua kênh có xác suất lỗi nhỏ tùy ý khi độ dài từ mã đủ lớn. Ngược lại thì không tồn tại một phép mã hóa nào như vậy.

Định lý

Nếu tốc độ dữ liệu cần truyền R truyền qua kênh có dung lượng C' thỏa mãn $R \leq C'$ thì tồn tại một phép mã hóa và giải mã sao cho việc truyền tin qua kênh có xác suất lỗi nhỏ tùy ý khi độ dài từ mã đủ lớn. Ngược lại thì không tồn tại một phép mã hóa nào như vậy.

- Nhận xét: Định lý chỉ ra tính tồn tại, không chỉ ra cách xây dựng



Notes

C2(cont.): Dung lượng kênh

Nội dung chính

- Khả năng phát của nguồn rời rạc
 - Kênh rời rạc và một số khái niệm
 - Dung lượng kênh rời rạc
 - Định lý mã hóa thứ hai của Shannon

② Dung lượng kênh Gausse nhiễu trắng cộng

- Kênh Gausse nhiễu trắng cộng - AWGN
 - Dung lượng của kênh AWGN



C2(cont.): Dung lượng kênh

Nội dung chính

- Khả năng phát của nguồn rời rạc
 - Kênh rời rạc và một số khái niệm
 - Dung lượng kênh rời rạc
 - Định lý mã hóa thứ hai của Shannon

② Dung lượng kênh Gausse nhiễu trắng cộng

- Kênh Gausse nhiễu trắng cộng - AWGN
 - Dung lượng của kênh AWGN



Notes

Notes

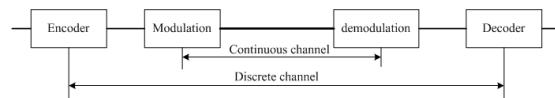
Kênh Gausse nhiễu trắng cộng - AWGN

Đặc trưng của kênh Gausse nhiễu cộng

Tham số đặc trưng của kênh liên tục:

- Trường dấu lối vào (input) và trường dấu lối ra (output).
 - Hàm chuyển, hàm mật độ phân bố xác suất để thu được $y(t)$ khi đã phát $x(t)$: $f(y(t)|x(t))$
 - Tốc độ truyền của kênh v_k

Kênh rời rạc chưa kênh liên tục:



Định lý

Khả năng thông qua của kênh liên tục không nhỏ hơn khả năng thông qua của kênh rời rạc chứa nó.

$$C_{liên\ tục} \geq C_{rời\ rac\ chúa\ liên\ tục}$$

Kênh Gausse nhiễu trắng cộng - AWGN

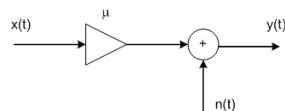
Mô hình của kênh Gausse nhiễu cộng

Định nghĩa (Kênh Gausse)

Kênh Gausse không đổi là một kênh liên tục có tập tin lỗi vào và tập tin lỗi ra liên hệ với nhau theo công thức:

$$v(t) = \mu x(t) + n(t)$$

trong đó: $\mu = \text{const}$; $n(t)$ là nhiễu cộng còn gọi là nhiễu trống có phân bố chuẩn $\mathcal{N}(\mu, \sigma^2)$.



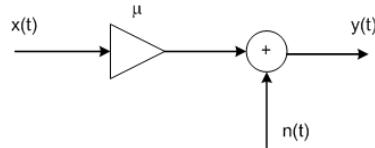
- $x(t) \sim X$, $y(t) \sim Y$, và $n(t) \sim N$: $N \sim \mathcal{N}(0, \sigma_n^2)$
 - $x(t)$ và $n(t)$ độc lập nhau.
 - $\rightarrow \sigma_y^2 = \mu^2 \sigma_x^2 + \sigma_n^2$ hay tương đương $P_y = \mu^2 P_x + P_n$



Notes

Kênh Gausse nhiễu trắng cộng - AWGN

Lượng thông tin tương hối qua kênh AWGN



- $y(t) = \mu x(t) + n(t)$
- Giả sử: $n(t) \sim \mathcal{N}(0, \sigma_n^2)$, $x(t)$ và $y(t)$ cũng có phân bố chuẩn

- $I(X; Y) = h(Y) - h(Y|X)$
- $h(Y) = \log \sqrt{2\pi e P_y}$ trong đó $P_y = \mu^2 P_x + P_n$
- $h(Y|X) = - \int \int f(x, y) \log(f(y|x)) dx dy$
 - ▶ $\Pr\{y \in dy | x\} = \Pr\{n \in dn\} \rightarrow f(y|x) dy = f(n) dn \rightarrow f(y|x) = f(n) \frac{dn}{dy} = f(n) \frac{1}{\frac{dy}{dn}} = f(n)$
 - ▶ $\Rightarrow h(Y|X) = \log \sqrt{2\pi e P_n}$
- $\Rightarrow I(X; Y) = \frac{1}{2} \log \left(1 + \frac{P_x}{P_n} \right)$



Notes

C2(cont.): Dung lượng kênh

Nội dung chính

1 Dung lượng kênh rời rạc

- Khả năng phát của nguồn rời rạc
- Kênh rời rạc và một số khái niệm
- Dung lượng kênh rời rạc
- Định lý mã hóa thứ hai của Shannon

2 Dung lượng kênh Gausse nhiễu trắng cộng

- Kênh Gausse nhiễu trắng cộng - AWGN
- Dung lượng của kênh AWGN



Notes

Dung lượng kênh AWGN

Định nghĩa (Dung lượng của kênh liên tục)

Khả năng thông qua của kênh liên tục, còn gọi là dung lượng kênh liên tục, là giá trị cực đại của lượng thông tin truyền qua kênh trong một đơn vị thời gian lấy theo mọi khả năng có thể của phân bố nguồn phát trong đó kể đến giới hạn công suất phát.

$$C' = v_k \max_{f(x): E\{x^2(t)\} \leq P} I(X; Y) = v_k \max_{X: E\{x^2(t)\} \leq P} I(X; Y)$$

$$C = \max_{f(x): E\{x^2(t)\} \leq P} I(X; Y) = \max_{X: E\{x^2(t)\} \leq P} I(X; Y)$$

- $v_k = \frac{1}{\Delta t}$ với Δt là thời gian rời rạc hóa.

Định lý (Dung lượng của kênh Gausse nhiễu cộng)

Kênh AWGN với giới hạn công suất phát P và công suất nhiễu N có dung lượng:

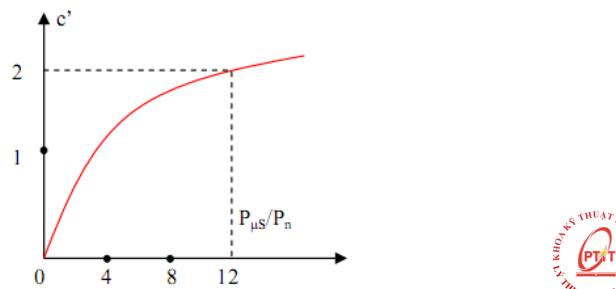
$$C' = \frac{v_k}{2} \log \left(1 + \frac{\mu^2 P}{P_n} \right) \quad C = \frac{1}{2} \log \left(1 + \frac{\mu^2 P}{P_n} \right)$$

Notes

Dung lượng kênh AWGN

Một số nhận xét

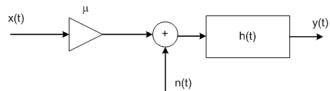
- $\mu^2 P / P_n = S/N$ gọi là tỷ số công suất trung bình của tín hiệu trên tạp âm (SNR)
- $S/N \rightarrow 0 \Rightarrow C' \rightarrow 0$: S/N rất bé thì có thể coi như kênh bị đứt.
- Để tăng C' thì cần tăng S/N , tuy nhiên việc tăng này bị giới hạn do C' rơi vào tình trạng bão hòa.



Notes

Dung lượng kênh AWGN

Kênh có băng thông hạn chế



- $y(t) = (\mu x(t) + n(t)) * h(t)$
- Kênh AWGN với mật độ phổ công suất nhiễu hai phía $N_0/2$ [W/Hz].
- $h(t)$: đáp ứng xung của một mạch lọc thông dải lý tưởng có băng tần W [Hz]. \rightarrow Tốc độ lấy mẫu $\geq \frac{1}{2W}$

Định lý (Dung lượng của kênh AWGN băng tần hữu hạn)

Dung lượng của kênh AWGN với băng tần hữu hạn W và giới hạn công suất phát P_x có nhiều với mật độ phổ công suất hai phía $N_0/2$ được xác định:

$$C' = W \log \left(1 + \frac{\mu^2 P_x}{N_0 W} \right) [\text{bps}]$$

Notes

Dung lượng kênh AWGN

Kênh có băng tần hạn chế - Khảo sát ảnh hưởng của băng tần

- $W \rightarrow 0 \Rightarrow C' \rightarrow 0$
- Nếu $W \uparrow$, thì $C' \uparrow$.
 - ▶ **Chú ý:** $W \uparrow \rightarrow P_n = WN_0 \uparrow \rightarrow SNR \downarrow$
- $W \rightarrow \infty$, $C \rightarrow C'_\infty = \frac{\mu^2 P_x}{N_0} \log_2 e < \infty$.
 - ▶ Thông tin vũ trụ thường với băng tần rất rộng.
- $0 \leq C' \leq C'_\infty$.
 - ▶ **Chú ý:** Tạp âm nhiệt luôn tồn tại.

Định lý (Định lý mã hóa thứ hai của Shannon)

Các nguồn tin rời rạc có thể mã hóa và truyền theo kênh liên tục với xác suất sai bé tùy ý khi giải mã các tín hiệu nhận được nếu khả năng phát của nguồn nhỏ hơn khả năng thông qua của kênh. Ngược lại, không thể thực hiện được phép mã hóa và giải mã với sai số bé tùy ý.

Chú ý: $\lim_{x \rightarrow 0} (1+x)^{1/x} = e$



Notes

Kết thúc phần dung lượng kênh



Biên soạn: Phạm Văn Sư (PTIT)

C2(cont.): Dung lượng kênh

ver. 22a

27 / 27

Notes

Notes

C3: Mã hóa nguồn - Nén dữ liệu

Lý thuyết thông tin

Biên soạn: Phạm Văn Sư

Bộ môn Xử lý tín hiệu và Truyền thông
Khoa Kỹ thuật Điện tử I
Học viện Công nghệ Bưu chính Viễn thông

ver. 22a



Notes

Mục tiêu của bài học

- Trang bị một số khái niệm cơ bản về mã hóa, mã hóa nguồn
- Mã hóa tối ưu cho nguồn
- Một số thuật toán mã hóa nguồn phổ biến



Notes

Các câu hỏi cần trả lời

- Mã hóa là gì? Bộ mã là gì? Các thông số cơ bản của một bộ mã?
 - Thế nào là mã không suy biến? mã có khả năng giải mã duy nhất? mã có tính prefix?
 - Bài toán mã hóa tối ưu? Cách để xây dựng được bộ mã tối ưu?
 - Định lý mã hóa thứ nhất của Shannon?
 - Mã hóa khôi tin có ưu điểm gì so với mã hóa đơn lẻ từng tin?
 - Những điểm cơ bản nhất về các thuật toán mã hóa: Shannon, Shannon-Fano, Shannon-Fano-Elias, mã hóa số học, LZW?
 - Cách thức thực hiện mã hóa và giải mã cho các phương thức mã hóa : Shannon, Shannon-Fano, Shannon-Fano-Elias, mã hóa số học, LZW?



C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- 1 Tổng quan về mã hóa nguồn - Nén dữ liệu
 - 2 Các định nghĩa và khái niệm cơ bản mã hóa
 - 3 Nguyên tắc mã hóa tối ưu
 - 4 Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
 - 5 Kết thúc



Notes

Notes

Tổng quan về mã hóa nguồn

Mục tiêu và phân loại

Mục tiêu của mã hóa nguồn

Thực hiện tìm kiếm các phương thức biểu diễn dữ liệu nhỏ gọn nhất có thể

Nguyên lý của mã hóa nguồn

Loại bỏ các thông tin dư thừa hoặc các thông tin dư thừa và các thông tin không cần thiết.

- Theo quan điểm bảo toàn thông tin:

- Nén không tổn hao (lossless data compression)
- Nén có tổn hao (lossy data compression)

- Theo đặc tính thay đổi:

- Mã thích nghi (adaptive)
- Mã không thích nghi (nonadaptive)

- Theo phương pháp:

- RLE (run length encoding)
- Mã hóa thống kê
- Mã hóa từ điển
- Mã hóa chuyển đổi

- Theo mô hình n-user:

- Tập trung
- Phân tán



Notes

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- Tổng quan về mã hóa nguồn - Nén dữ liệu
- Các định nghĩa và khái niệm cơ bản mã hóa
- Nguyên tắc mã hóa tối ưu
- Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
- Kết thúc

Notes



Các định nghĩa và khái niệm cơ bản mã hóa

Mã hóa

Cho nguồn rời rạc X với các tin x_k có xác suất phân bố $p(x_k)$. Một bộ dâu (chữ mã) M với các dâu (chữ mã) $\{m_1, m_2, \dots, m_q\}$.

Định nghĩa (Mã hóa)

Mã hóa là một phép ánh xạ $1 - 1$ từ tập các tin rời rạc x_k lên tập các từ mã là tổ hợp có thể của các dâu (các chữ mã) m_k

$$f : x_k \longmapsto m_k^{l_k}$$

- l_k là độ dài từ mã thứ k : số dâu mã tạo thành từ mã $m_k^{l_k}$.
- $m_k^{l_k}$ gọi là từ mã.
 - ▶ $m_k^{l_k}$ thường là các phần tử của một cấu trúc đại số
 - ▶ Các dâu mã thường được chọn từ một trường F nào đó
- Bộ mã: tập hợp các từ mã, là sản phẩm của phép mã hóa.



Notes

Các định nghĩa và khái niệm cơ bản mã hóa

Các thông số cơ bản của bộ mã

- Độ dài từ mã: l_k là độ dài từ mã thứ k ; $l_k = const \forall k$ gọi là mã đều, ngược lại gọi là mã không đều.
- Độ dài trung bình: là trung bình thống kê của độ dài các từ mã:
$$\bar{l} = \sum_{k=1}^N p(x_k)l_k$$
- Cơ số mã: số các dâu (chữ mã) khác nhau được sử dụng trong bộ mã.
- Bộ mã mà tất cả các tổ hợp dâu mã là từ mã của tập tin tương ứng gọi là bộ mã đầy, ngược lại gọi là mã không đầy (mã vơi).
- Tính hiệu quả của phép mã hóa: $\eta = \frac{\bar{l}_{min}}{\bar{l}} = \frac{H(X)}{\bar{l}} \rightarrow \eta \leq 1$. Bộ mã hiệu quả khi $\eta \rightarrow 1$.
- Độ chật giải mã: là số dâu (chữ mã) nhận được cần thiết trước khi có thể thực hiện được việc giải mã.
- Phương sai độ dài trung bình của bộ mã $\sigma_l^2 = \sum_{k=1}^N p(x_k)(l_k - \bar{l})^2$



Notes

Các định nghĩa và khái niệm cơ bản mã hóa

Khái niệm các bộ mã (1)

Định nghĩa (Mã không suy biến (không dị thường))

Một bộ mã được gọi là *không suy biến (non-singular)* nếu mọi tin x_k của nguồn X ánh xạ thành các từ mã khác nhau của bộ mã.

$$x_k \neq x_l \Rightarrow m_k^{l_k} \neq m_l^{l_l}$$

- Đảm bảo cho việc mô tả không bị nhập nhằng giữa các tin sau khi mã hóa

Định nghĩa (Từ mã mở rộng)

Một từ mã mở rộng là việc ánh xạ một chuỗi hữu hạn các tin thành các từ mã liên tiếp nhau.

$$x_1 x_2 \dots \mapsto m_1^{l_1} m_2^{l_2} \dots$$

Định nghĩa (Bộ mã có khả năng giải mã một cách duy nhất)

Một bộ mã được gọi là bộ mã có khả năng giải mã được một cách duy nhất nếu từ mã mở rộng của nó là một từ mã không suy biến.

Notes

Các định nghĩa và khái niệm cơ bản mã hóa

Khái niệm các bộ mã (2)

Định nghĩa (Bộ mã có tính prefix)

Một bộ mã được gọi là bộ mã có tính prefix hay còn gọi mã có khả năng giải mã tức thời nếu không có bất cứ từ mã nào là phần tiền tố (prefix) của một từ mã khác trong bộ mã.

- Một bộ mã prefix là bộ mã có khả năng tự phân tách được.

Định lý (Bất đẳng thức Kraft)

Với bất cứ bộ mã prefix nào trên tập dấu (chữ mã) M có kích thước (cơ số) q thì tập độ dài các từ mã có thể l_1, l_2, \dots, l_N phải thỏa mãn bất đẳng thức:

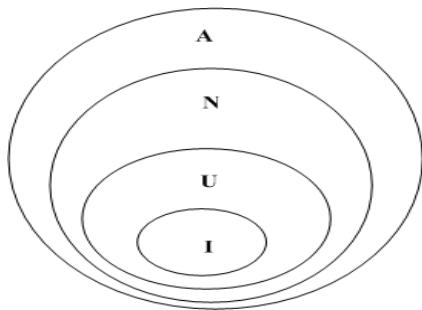
$$\sum_{k=1}^N q^{-l_k} \leq 1$$

Ngược lại, với một tập các độ dài từ mã cho trước thỏa mãn bất đẳng thức này thì tồn tại một bộ mã prefix nhận tập độ dài này làm độ dài các từ mã.

Notes

Các định nghĩa và khái niệm cơ bản mã hóa

Lược đồ Venn biểu diễn các bộ mã



Hình: Phân loại các lớp các mã (I) Mã giải mã tức thì (U) Mã có khả năng giải mã duy nhất (N) Mã không suy biến (A) Tất cả các mã

- Một bộ mã có khả năng giải mã một cách duy nhất chưa chắc là một bộ mã có tính prefix.

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- ① Tổng quan về mã hóa nguồn - Nén dữ liệu
 - ② Các định nghĩa và khái niệm cơ bản mã hóa
 - ③ Nguyên tắc mã hóa tối ưu
 - ④ Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
 - ⑤ Kết thúc

Notes

Notes

Nguyên tắc mã hóa tối ưu

Ví dụ, nguyên tắc mã hóa tối ưu

Ví dụ

Giả sử có bộ mã $\mathcal{C} = \{0, 10, 110, 111\}$. Cho một đoạn văn bản sau:
"aaaaabbbcccd". Thực hiện việc mã hóa theo các phương án sau:

- ① Phương án 1 $a \leftrightarrow 111, b \leftrightarrow 110, c \leftrightarrow 10$ và $d \leftrightarrow 0$
- ② Phương án 2 $d \leftrightarrow 111, c \leftrightarrow 110, b \leftrightarrow 10$ và $a \leftrightarrow 0$

Tìm biểu diễn tương ứng của đoạn văn bản và so sánh các bản mã thu được.

Nguyên tắc

Gán các từ mã có độ dài ngắn cho các tin có xác suất xuất hiện lớn, và các từ mã có độ dài lớn cho các tin có xác suất xuất hiện nhỏ.



Notes

Nguyên tắc mã hóa tối ưu

Mã hóa tối ưu, Bài toán mã hóa tối ưu

Định nghĩa (Phép mã hóa tối ưu)

Một phép mã hóa được gọi là tiết kiệm (hay còn gọi là tối ưu) nếu nó đạt được độ dài trung bình từ mã cực tiểu \bar{l}_{min}

Bài toán mã hóa tối ưu

$$\min \bar{l} = \sum_k p(x_k)l_k$$

$$\text{sao cho } \sum_{k=1}^N q^{-l_k} \leq 1$$

$\Rightarrow l_k^* = -\log_q(p(x_k))$. Trường hợp tổng quát $l_k^* \notin \mathbb{Z}^+$



Notes

Nguyên tắc mã hóa tối ưu

Đánh giá độ dài trung bình của mã tối ưu

Định lý

Độ dài trung bình từ mã \bar{I} của bất cứ bộ mã có khả năng giải mã tức thì cơ sở q nào biểu diễn một nguồn rời rạc X cũng lớn hơn hoặc bằng với entropy $H_q(X)$ của nguồn, nói cách khác:

$$\bar{I} \geq H_q(X)$$

xảy ra đẳng thức khi và chỉ khi $q^{-l_k} = p(x_k)$

- Phân bố thỏa mãn đẳng thức trên gọi là q-adic

Định lý

Gọi tập $I_1^*, I_2^*, \dots, I_N^*$ là tập các độ dài từ mã tối ưu của phép mã hóa cơ số q cho nguồn rời rạc có phân bố p trên tập dấu mã M . Khi đó độ dài trung bình từ mã của bộ mã tối ưu \bar{I}^* thỏa mãn bất đẳng thức kẹp:

$$H_q(X) \leq \bar{I}^* < H_q(X) + 1$$

Notes

Nguyên tắc mã hóa tối ưu

Mã khồi dữ liệu

- Dãy n ký hiệu (tin) từ nguồn rời rạc X , mỗi tin x_k được lấy với xác suất phân bố độc lập tương đồng (i.i.d) $p(x_k)$.
- Gọi $I(x_1, x_2, \dots, x_n)$ là độ dài từ mã tương ứng với dãy (x_1, x_2, \dots, x_n) .
- Định nghĩa L_n là độ dài trung bình từ mã với mỗi ký hiệu, nói cách khác:

$$L_n = \frac{1}{n} \sum p(x_1, x_2, \dots, x_n) I(x_1, x_2, \dots, x_n) = \frac{1}{n} E[I(X_1, X_2, \dots, X_n)]$$

Định lý

Độ dài trung bình từ mã với mỗi ký hiệu khi thực hiện mã hóa khôi đồng thời thỏa mãn bất đẳng thức

$$H(X) \leq L_n < H(X) + \frac{1}{n}$$

- $n \rightarrow \infty \Rightarrow L_n \rightarrow H(X)$



Notes

Nguyên tắc mã hóa tối ưu

Mã hóa với đặc trưng thống kê xấp xỉ

Định lý

Dộ dài trung bình bộ mã biểu diễn một nguồn có hàm mật độ phân bố $p(x)$ với các độ dài từ mã được sử dụng $l_k = \lceil \log \frac{1}{q(x_k)} \rceil$ thỏa mãn

$$H(p) + D(p||q) \leq E[I_k]_p < H(p) + D(p||q) + 1$$

- → Nếu chúng ta sử dụng phân bố sai trong quá trình thiết kế mã, thì chúng ta phải trả giá $D(p||q)$ trong độ dài từ mã trung bình mô tả nguồn.



C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- ① Tổng quan về mã hóa nguồn - Nén dữ liệu
 - ② Các định nghĩa và khái niệm cơ bản mã hóa
 - ③ Nguyên tắc mã hóa tối ưu
 - ④ Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
 - ⑤ Kết thúc



Notes

Notes

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- ① Tổng quan về mã hóa nguồn - Nén dữ liệu
- ② Các định nghĩa và khái niệm cơ bản mã hóa
- ③ Nguyên tắc mã hóa tối ưu
- ④ Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
- ⑤ Kết thúc



Notes

Một số phương pháp mã hóa nguồn phổ biến

Mã Shannon

Nguyên tắc chọn độ dài từ mã

Với một tin x_k có $p(x_k)$ cho trước, mã Shannon có độ dài từ mã xác định bởi công thức:

$$l_k = \lceil \log_2 \frac{1}{p(x_k)} \rceil \quad (\forall x_k \in X)$$



Thuật toán

- ❶ Sắp xếp các tin theo thứ tự xác suất phân bố giảm dần.
- ❷ Chọn các từ mã có độ dài thích hợp theo thứ tự và tránh việc chọn các từ mã vi phạm tính prefix.

Notes

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- ① Tổng quan về mã hóa nguồn - Nén dữ liệu
- ② Các định nghĩa và khái niệm cơ bản mã hóa
- ③ Nguyên tắc mã hóa tối ưu
- ④ Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
- ⑤ Kết thúc



Notes

Một số phương pháp mã hóa nguồn phổ biến

Mã Shannon-Fano

- Thuật toán đơn giản xây dựng bộ mã có tính prefix.
- Thuật toán tạo bộ mã không đều khá hiệu quả (tính toán đơn giản).
- Thuộc lớp thuật toán cận tối ưu (suboptimal).
 - ▶ Không luôn luôn tạo ra bộ mã tối ưu.
- Ít phổ biến.

Thuật toán Shannon-Fano

- ① Sắp xếp các tin theo thứ tự xác suất (tần suất) từ cao đến thấp từ phía trái sang phía phải.
- ② Chia dãy đó thành hai phần sao cho các phần có tổng xác suất xấp xỉ bằng nhau.
- ③ Gán nhãn cho phần nửa trái một bít 0, và nhóm bên phải bít 1.
- ④ Lặp lại các bước 3 và 4 cho mỗi nửa bằng cách chia nhóm nhỏ và gán nhãn bít cho đến tận khi các nhóm chỉ còn một nút tương ứng với lá của cây mã.
- ⑤ Từ mã thu được bằng cách duyệt từ gốc đến các nút lá tương ứng.

Notes

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- ① Tổng quan về mã hóa nguồn - Nén dữ liệu
- ② Các định nghĩa và khái niệm cơ bản mã hóa
- ③ Nguyên tắc mã hóa tối ưu
- ④ Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - **Mã Huffman**
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
- ⑤ Kết thúc



Notes

Một số phương pháp mã hóa nguồn phổ biến

Mã Huffman: Tổng quan

- Thuộc lớp mã hóa Entropy, mã hóa nén dữ liệu không tổn hao (lossless data compression)
- Là lớp mã với độ dài từ mã thay đổi (variable-length code)
- Bộ mã thu được là bộ mã có tính prefix.
- Yêu cầu phân bố của nguồn phải biết trước.
- Thuộc dạng thuật toán "Greedy".
- Là thuật toán mã hóa tối ưu.

Định lý

Mã hóa Huffman là mã hóa tối ưu. Nói cách khác, gọi \bar{I}_H là độ dài trung bình từ mã của bộ mã Huffman cho nguồn rời rạc X , \bar{I} là độ dài trung bình từ mã của bộ mã tạo được bởi một phương pháp nào đó, khi đó chúng ta có:

$$\bar{I}_H \leq \bar{I}$$

Notes

Một số phương pháp mã hóa nguồn phổ biến

Mã Huffman: Bài toán mã hóa

Nhập vào: $X = \{x_k\}$ với các xác suất phân bố $p(x_k)$ tương ứng.

$$X = \{x_k\} = \begin{pmatrix} x_1 & x_2 & \dots & x_N \\ p(x_1) & p(x_2) & \dots & p(x_n) \end{pmatrix}$$

In ra: Các từ mã nhị phân $m_k^{l_k}$ tương ứng với tin x_k



Notes

Một số phương pháp mã hóa nguồn phổ biến

Mã Huffman: Thuật toán mã hóa

- ❶ Khởi động danh sách cây nhị phân có một nút chứa các trọng số là xác suất phân bố tương ứng của các tin x_k , sắp xếp theo thứ tự tăng dần từ trái sang phải.
- ❷ Thực hiện lặp các bước sau đến khi thu được một nút duy nhất.
 - ❶ Tìm hai cây T' và T'' trong danh sách các nút gốc có trọng lượng tối thiểu p' và p'' . Thay thế chúng bằng một cây có nút gốc có trọng lượng bằng $p' + p''$ và các cây con là T' và T'' .
 - ❷ Đánh nhãn 0 và 1 trên các nhánh từ gốc mới đến các cây T' và T'' .
 - ❸ Sắp xếp các nút theo thứ tự tăng dần của trọng xác suất.
- ❸ Duyệt từ gốc cuối cùng đến nút lá với các bít là các nhãn ta được từ mã tương ứng với các tin.



Notes

Một số phương pháp mã hóa nguồn phổ biến

Mã Huffman: Nhận xét

- Phép mã hóa tối ưu Huffman: tập các từ mã cho bộ mã tối ưu là không duy nhất. Nói cách khác, có thể có nhiều hơn một tập các độ dài cho cùng độ dài trung bình:
 - ▶ Việc gán nhãn "0" và "1" là tùy ý.
 - ▶ Việc sắp xếp các phân bố xác suất hợp (cây thay thế) có thể thực hiện: xếp "trội" nhất, hoặc xếp "chìm" nhất
 - Việc xếp xác suất phân bố "trội" nhất sẽ cho bộ mã có phương sai độ dài từ mã nhỏ nhất (gần bộ mã đều nhất)

Mã Huffman thỏa mãn mã tối ưu:

- ❶ Nếu $p(x_k) > p(x_l)$ thì $l_k < l_l$.
 - ❷ Hai từ mă có độ dài nhất có cùng độ dài.
 - ❸ Hai từ mă có độ dài nhất chỉ khác nhau một bít ở vị trí cuối cùng, và hai từ mă này tương ứng với hai tin (ký hiệu) có xác suất xuất hiện thấp nhất. (VẤN ĐỀ DỊCH TỰ)
PTT

Mã Huffman cũng thỏa mãn giới hạn $\bar{I}_k \leq H(X) + 1$

Một số phương pháp mã hóa nguồn phổ biến

Mã Huffman: Bài toán giải mã, Thuật toán giải mã

Nhập vào: Chuỗi bít thông tin

In ra: Dãy tin tương ứng

- Khởi động, đặt con trỏ P chỉ đến gốc (root) của cây mã hóa Huffman. Gán con trỏ bít b rỗng.
 - Lặp các bước sau đến khi kết thúc chuỗi bít thông tin
 - Gán b bằng bít tiếp theo của chuỗi. Nếu $b = 0$ dịch con trỏ P theo nhánh có nhãn 0, nếu ngược lại, dịch con trỏ P theo nhánh có nhãn 1.
 - Nếu P đã chỉ đến nút lá thì ghi ra tin tương ứng với từ mã. Khởi động lại con trỏ chỉ đến gốc



Notes

Notes

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- ① Tổng quan về mã hóa nguồn - Nén dữ liệu
- ② Các định nghĩa và khái niệm cơ bản mã hóa
- ③ Nguyên tắc mã hóa tối ưu
- ④ Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
- ⑤ Kết thúc



Notes

Một số phương pháp mã hóa nguồn phổ biến

Mã hóa Shannon-Fano-Elias

- ① Sử dụng hàm mật độ phân bố tích lũy để thực hiện mã hóa.
- ② Định nghĩa hàm mật độ phân bố tích lũy cải tiến:

$$\bar{F}(x) = \sum_{a < x_k} p(a) + \frac{1}{2} p(x_k)$$

- ▶ $\bar{F}(a) \neq \bar{F}(b)$ nếu $a \neq b$.
- ▶ → có thể sử dụng $\bar{F}(x)$ như là một mã cho x_k .

- ③ Cắt $\bar{F}(x)$ còn l_k bít, ký hiệu là $\lfloor \bar{F} \rfloor_{l_k}$.
- ④ Nếu $l_k = \lceil \log_2 \frac{1}{p(x_k)} \rceil + 1$ thì:

$$\frac{1}{2^{l_k}} < \frac{p(x_k)}{2} = \bar{F}(x) - F(x-1)$$

- ▶ → l_k bít là đủ để có thể mô tả x_k



Notes

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- 1 Tổng quan về mã hóa nguồn - Nén dữ liệu
 - 2 Các định nghĩa và khái niệm cơ bản mã hóa
 - 3 Nguyên tắc mã hóa tối ưu
 - 4 Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - **Thuật toán mã hóa số học - Arithmetic Coding**
 - Thuật toán mã hóa Lempel-Ziv
 - 5 Kết thúc



Một số phương pháp mã hóa nguồn phổ biến

Mã hóa số học

- Thuộc lớp mã hóa không đều.
 - Thuộc lớp mã hóa Entropy.
 - Thuộc lớp mã hóa không tổn hao.
 - Được sử dụng rộng rãi trong thực tế và trong các trình tiện ích nén dữ liệu thương mại.
 - Thực hiện việc mã hóa một nhóm dữ liệu.
 - Là một mở rộng trực tiếp của phương pháp mã hóa Shannon-Fano-Elias.
 - Ý tưởng quan trọng là tính toán và sử dụng hàm phân bố xác suất của X^n .



Notes

Notes

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- ① Tổng quan về mã hóa nguồn - Nén dữ liệu
- ② Các định nghĩa và khái niệm cơ bản mã hóa
- ③ Nguyên tắc mã hóa tối ưu
- ④ Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
- ⑤ Kết thúc



Notes

Một số phương pháp mã hóa nguồn phổ biến

Thuật toán mã Lempel-Ziv-Welch: Tổng quan

- Thuộc lớp mã hóa không tổn hao.
- Thuộc lớp mã hóa thuật toán từ điển.
- Không yêu cầu phải biết trước phân bố của nguồn, thuật toán thích nghi.
- Ứng dụng rộng rãi trong thực tế, là cơ sở của nhiều trình tiện ích nén dữ liệu thương mại.

Mã hóa Huffman	Mã hóa LZ
Yêu cầu biết phân bố của nguồn	Không cần biết phân bố của nguồn
Bảng mã được chọn trước	Bảng mã được tạo trong quá trình
Phương thức mã độ dài cố định-thay đổi	Phương thức độ dài thay đổi-cố định

Bảng: So sánh giữa mã hóa Huffman và mã hóa LZ. © GIT



Notes

Một số phương pháp mã hóa nguồn phổ biến

Thuật toán mã Lempel-Ziv-Welch: Thuật toán mã hóa

Thuật toán mã hóa Lempel-Ziv

- ❶ Cho trước chuỗi $\mathcal{X} = x_1x_2 \dots x_n$ (n rất lớn).
- ❷ Khởi động bảng từ mã cơ bản khởi đầu.
- ❸ Tìm kiếm trong chuỗi nguồn đã cho cụm mào đầu dài nhất có mặt trong bảng từ mã. Nói cách khác, tìm kiếm w dài nhất mà $\mathcal{X} = (w, \mathcal{X}')$.
- ❹ Cập nhật bảng mã với từ mã mới được tạo thành từ (w, x_k) , với x_k là ký hiệu tiếp theo trong chuỗi đầu vào.



Notes

C3: Mã hóa nguồn - Nén dữ liệu

Nội dung chính

- ❶ Tổng quan về mã hóa nguồn - Nén dữ liệu
- ❷ Các định nghĩa và khái niệm cơ bản mã hóa
- ❸ Nguyên tắc mã hóa tối ưu
- ❹ Một số phương pháp mã hóa nguồn phổ biến
 - Mã Shannon
 - Mã Shannon-Fano
 - Mã Huffman
 - Thuật toán mã hóa Shannon-Fano-Elias
 - Thuật toán mã hóa số học - Arithmetic Coding
 - Thuật toán mã hóa Lempel-Ziv
- ❺ Kết thúc



Notes

Kết thúc phần mã hóa nguồn



Biên soạn: Phạm Văn Sư (PTIT)

C3: Mã hóa nguồn - Nén dữ liệu

ver. 22a

37 / 37

Notes

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1: Mã khối tuyến tính)

Lý thuyết thông tin

Biên soạn: Phạm Văn Sư

Bộ môn Xử lý tín hiệu và Truyền thông
Khoa Kỹ thuật Điện tử I
Học viện Công nghệ Bưu chính Viễn thông

ver. 22a



Notes

Mục tiêu của bài học

- Trang bị một số khái niệm cơ bản về mã hóa kênh
- Mã khối tuyến tính
- Mã vòng tuyến tính



Notes

Các câu hỏi cần trả lời

- Các tham số đánh giá mã hóa kênh?
 - Khoảng cách mã Hamming tối thiểu? Có vai trò gì trong việc đánh giá khả năng phát hiện lỗi và sửa lỗi của bộ mã?
 - Mã khôi tuyển tính? Ma trận sinh và ma trận kiểm tra của mã khôi tuyển tính? Mã khôi tuyển tính hệ thống?
 - Bài toán thiết kế mã khôi tuyển tính?
 - Mã vòng (mã cyclic, mã xyclic) tuyển tính? Đa thức sinh và đa thức kiểm tra của mã vòng tuyển tính? Mã vòng tuyển tính hệ thống?



C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1)

Nội dung chính

- ① Các định nghĩa và khái niệm cơ bản
 - ② Mã khồi tuyển tính
 - Mã khồi tuyển tính
 - Mã khồi tuyển tính dạng hệ thống
 - ③ Dánh giá mã khồi nhị phân tuyển tính trên kênh BSC
 - ④ Các vấn đề khi thiết kế mã khồi tuyển tính
 - ⑤ Kết thúc

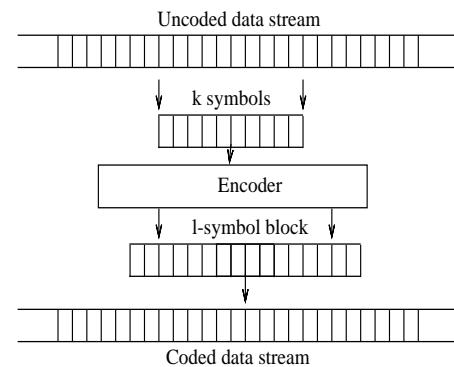


Notes

Notes

Một số định nghĩa và khái niệm cơ bản

Mã hóa khôi



Hình: Quá trình mã hóa khôi



Một số định nghĩa và khái niệm cơ bản

Véc-tơ mă

Định nghĩa (Véc-tơ mă)

Một bộ mã $\mathcal{C} = \{c_0, c_1, \dots, c_{M-1}\}$ chứa các từ mã có độ dài l , mỗi từ mã $c_k = (c_{k,0}, c_{k,1}, \dots, c_{k,l-1})$ với các dấu mã $c_{k,i} \in GF(q)$ ($i = \overline{0, l-1}$).

- \mathbb{C} : bộ mã cơ số q
 - c_k được gọi là từ mã, véc-tơ mã
 - M là số từ mã của bộ mã \mathbb{C} .

Khởi thông tin đầu vào là tập $\{m_i\}$, trong đó $m_i = (m_{i,0}, m_{i,1}, \dots, m_{i,k-1})$ với $m_{i,j} \in GF(q)$. Tập $\{m_i\}$ tạo thành một không gian véc-tơ trên $GF(q)$.

- Nếu các khối thông tin có cùng độ dài k thì số từ mã của bộ mã \mathcal{C} phải thỏa mãn $M = q^k$.
 - Nếu các khối tin có độ dài thay đổi thì M không có dạng trên.
 - ▶ Các bộ mã hóa loại này khó thực thi hơn.



Notes

Một số định nghĩa và khái niệm cơ bản

Độ dư thừa mã, Tỷ số mã, Trọng số mã

Định nghĩa (Độ dư thừa của bộ mã)

Dộ dư thừa của bộ mã \mathfrak{C} được định nghĩa là $r = l - \log_q(M)$.

- Nếu $M = 2^k$ thì $r = l - k$.

Định nghĩa (Tỷ số mã hóa)

Tỷ số mã hóa R được định nghĩa: $R = \frac{\log_q(M)}{I}$

- Nếu $M = 2^k$ thì $R = k/l$

Định nghĩa (Trọng số của từ mã/cấu trúc lõi)

Trong số của một từ mã c hoặc của một cấu trúc lỗi e là số dấu mã khác 0 trong c hoặc e. Kí hiệu là $w(c)$ hoặc $w(e)$



- $0 \leq w(c) \leq l$

Một số định nghĩa và khái niệm cơ bản

Khoảng cách mã Hamming

Định nghĩa (Khoảng cách mã Hamming)

Khoảng cách Hamming giữa hai từ mã c_1 và c_2 là tổng số vị trí tương ứng trong hai từ mã mà dấu mã khác nhau.

$$d_{Hamming}(c_1, c_2) = d(c_1, c_2) = |\{i | c_{1,i} \neq c_{2,i}, i = 0, 1, \dots, l - 1\}|$$

- $d(c_1, c_2) = d(c_2, c_1)$.
 - $0 \leq d(c_1, c_2) \leq l$.
 - $d(c_1, c_2) + d(c_2, c_3) \geq d(c_1, c_3)$ (Bất đẳng thức tam giác).

Định nghĩa (Khoảng cách Hamming tối thiểu)

Khoảng cách mã tối thiểu, hay khoảng cách Hamming tối thiểu của một bộ mã khồi \mathcal{C} là khoảng cách Hamming tối thiểu giữa tất cả các cặp từ mã phân biệt trong bộ mã.

$$d_{min} = d_0 = \min_{\forall c_1, c_2 \in C, c_1 \neq c_2} d(c_1, c_2)$$

Notes

Notes

Một số định nghĩa và khái niệm cơ bản

Khả năng phát hiện và sửa lỗi của mã

Định lý (Khả năng phát hiện lỗi của bộ mã)

Một bộ mã có khoảng cách mã tối thiểu d_{min} có khả năng phát hiện tất cả các cấu trúc lỗi có trọng nhô hơn hoặc bằng $(d_{min} - 1)$.

- Chú ý: Một số bộ mã có thể phát hiện được các cấu trúc lỗi có trọng $\geq d_{min}$

Định lý (Khả năng sửa lỗi của bộ mã)

Một bộ mã có khoảng cách mã tối thiểu d_{min} có khả năng sửa được tất cả các cấu trúc lỗi có trọng nhô hơn hoặc bằng $\lfloor \frac{d_{min}-1}{2} \rfloor^a$.

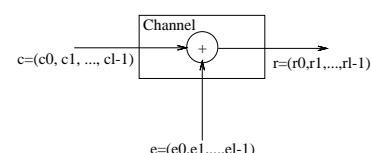
^a $\lfloor x \rfloor$ là phần nguyên lớn nhất nhỏ hơn hoặc bằng x

- Chú ý: Một số bộ mã có thể sửa được các cấu trúc lỗi có trọng $\lfloor \frac{d_{min}-1}{2} \rfloor + 1$ hoặc lớn hơn.

Notes

Một số định nghĩa và khái niệm cơ bản

Mô hình mã truyền dẫn trong kênh có nhiễu



Hình: Mô hình kênh nhiễu cộng

- c: từ mã phát, e: cấu trúc lỗi,
 $r = c + e$: véc-tơ thu.
 - Nếu không có lỗi thì véc-tơ thu là một từ mã hợp lệ.
- Định dạng điều chế, mức công suất phát, và mức nhiễu trên kênh quyết định xảy ra một cấu trúc lỗi trong q^l cấu trúc lỗi có thể.

- Máy thu thực hiện việc xem xét véc-tơ thu có phải là từ mã hợp lệ hay không: quá trình phát hiện lỗi.
- Khi máy thu phát hiện lỗi:
 - Yêu cầu phát lại: thông qua ARQ
 - HOẶC Đánh dấu từ mã lỗi: với các ứng dụng real-time (voice, video,...)
 - HOẶC Sửa lỗi: FEC.

Notes



C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1)

Nội dung chính

- ① Các định nghĩa và khái niệm cơ bản
 - ② Mã khối tuyến tính
 - Mã khối tuyến tính
 - Mã khối tuyến tính dạng hệ thống
 - ③ Dánh giá mã khối nhị phân tuyến tính trên kênh BSC
 - ④ Các vấn đề khi thiết kế mã khối tuyến tính
 - ⑤ Kết thúc



C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1)

Nội dung chính

- ① Các định nghĩa và khái niệm cơ bản
 - ② Mã khối tuyến tính
 - Mã khối tuyến tính
 - Mã khối tuyến tính dạng hệ thống
 - ③ Dánh giá mã khối nhị phân tuyến tính trên kênh BSC
 - ④ Các vấn đề khi thiết kế mã khối tuyến tính
 - ⑤ Kết thúc



Notes

Notes

Mã khôi tuyển tính

Định nghĩa

Định nghĩa (Mã khôi tuyển tính)

Xét một bộ mã khồi \mathcal{C} gồm các từ mã độ dài l $\{c_k = (c_{k,0}, c_{k,1}, \dots, c_{k,l-1})\}$ với các dấu mã thuộc $GF(q)$. Bộ mã \mathcal{C} là một bộ mã khồi tuyến tính cơ số q nếu và chỉ nếu \mathcal{C} tao thành một không gian vec-tơ con trên $GF(q)$.

Định nghĩa (Chiều của một bộ mã khối)

Chiều của một bộ mã khối là chiều của không gian véc-tơ tương ứng.

- Ký hiệu: $\mathfrak{C}(l, k)$ hoặc $\mathfrak{C}(l, k, d_0)$.
 - ① Tổ hợp tuyển tính của một tập các từ mã bất kỳ là một từ mã $\Rightarrow \mathfrak{C}$ luôn chứa từ mã toàn 0
 - ② Khoảng cách mã tối thiểu của bộ mã khói tuyển tính bằng trọng số của một từ mã có trọng số nhỏ nhất khác từ mã toàn không.
 - ③ Các cấu trúc lỗi không thể phát hiện được của bộ mã độc lập với từ mã phát và luôn chứa tập tất cả các từ mã không toàn 0.

Biên soạn: Phạm Văn Sư (PTIT)

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1: Mã kh

ver. 22a

13 / 30

Mã khôi tuyển tính

Mã trân sinh của mã khối tuyển tính

Gọi $\{g_0, g_1, \dots, g_{k-1}\}$ là cơ sở của các từ mã trong bộ mã $\mathfrak{C}(l, k)$.

Mã trân sinh $G(k \times l)$ của bộ mã được thành lập như sau:

$$G = \begin{pmatrix} g_0 \\ g_1 \\ \dots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \dots & g_{0,l-1} \\ g_{1,0} & g_{1,1} & \dots & g_{1,l-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \dots & g_{k-1,l-1} \end{pmatrix}$$

Gọi $a = (a_0, a_1, \dots, a_{k-1})$ là khối dữ liệu đầu vào (bản tin) cần mã hóa.

Từ mã thu được từ phép mã hóa:

$$\begin{aligned} c &= aG = [a_0, a_1, \dots, a_{k-1}]G \\ &= a_0g_0 + a_1g_1 + \dots + a_{k-1}g_{k-1} \end{aligned}$$



Notes

Notes

Mã khởi tuyển tính

Ma trận kiểm tra tính chẵn lẻ

Với \mathfrak{C} , tồn tại \mathfrak{C}^\perp là không gian véc-tơ đối ngẫu $(l - k)$ chiều.

Gọi $\{h_0, h_1, \dots, h_{l-k-1}\}$ là cơ sở của \mathfrak{C}^\perp . \Rightarrow Ma trận sinh $H(l-k \times l)$ của \mathfrak{C}^\perp :

$$H = \begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_{l-k-1} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,l-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,l-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{l-k-1,0} & h_{l-k-1,1} & \cdots & h_{l-k-1,l-1} \end{pmatrix}$$

- H là ma trận kiểm tra chẵn lẻ của mă C
 - $GH^T = 0$.

Định lý

Một véc-tơ c là một từ mã thuộc \mathcal{C} nếu và chỉ nếu $cH^T = 0$



- $cH^T = 0$ gọi là biểu thức kiểm tra chẵn lẻ.

Mã khôi tuyển tính

Ma trận kiểm tra tính chẵn lẻ và khoảng cách mã

Định lý

Giả sử bộ mã \mathbb{C} có ma trận kiểm tra \mathbf{H} chẵn lẻ. Khoảng cách mã tối thiểu của bộ mã \mathbb{C} bằng số cột tối thiểu khác 0 của \mathbf{H} mà tổ hợp tuyến tính không tầm thường của chúng bằng 0.

Định lý (Giới hạn Singleton)

Với bộ mã khởi truyền tính $\mathcal{C}(l, k)$, khoảng cách mã tối thiểu thỏa mãn bất đẳng thức:

$$d_{min} \leq l - k + 1$$



Notes

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1)

Nội dung chính

- 1 Các định nghĩa và khái niệm cơ bản
 - 2 Mã khối tuyến tính
 - Mã khối tuyến tính
 - Mã khối tuyến tính dạng hệ thống
 - 3 Dánh giá mã khối nhị phân tuyến tính trên kênh BSC
 - 4 Các vấn đề khi thiết kế mã khối tuyến tính
 - 5 Kết thúc



Mã khôi tuyển tính

Mã khôi tuyển tính hệ thống

Định nghĩa (Mã khôi tuyển tính hệ thống)

Mã khôi tuyển tính hệ thống $\mathcal{C}(l, k)$ thực hiện việc ánh xạ bản tin (khối dữ liệu) độ dài k thành một véc-tơ/tử mã độ dài l sao cho trong số l bít có thể chỉ ra k bít bản tin và số còn lại $l - k$ bít kiểm tra tính chẵn lẻ.

Giả sử từ mã xây dựng mã có dạng $c = [p_1 \quad | \quad a]$

- a : khối thông tin (bản tin) độ dài k ; p_1 : khối bít kiểm tra độ dài $l - k$

G phương pháp khử Gausse

$$G = [P \quad | \quad I_k]$$

- $P_{(k \times I-k)}$: ma trận tạo dấu kiểm tra
 - $I_k - \cdot \cdot \cdot$: ma trận đơn vị

$$\Rightarrow H = [I_n \quad | \quad -P^T]$$

$$\bullet \Rightarrow CH^T = 0$$

Chú ý: Nếu xét $c = [a \quad | \quad p_1]$

- $G = [I_k \quad | \quad P]$
 - $\Rightarrow H = [-P^T \quad | \quad I_{l-k}]$



Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1)

Nội dung chính

1 Các định nghĩa và khái niệm cơ bản

2 Mã khối tuyến tính

- Mã khối tuyến tính
- Mã khối tuyến tính dạng hệ thống

3 Dánh giá mã khối nhị phân tuyến tính trên kênh BSC

4 Các vấn đề khi thiết kế mã khối tuyến tính

5 Kết thúc



Notes

Dánh giá mã khối nhị phân tuyến tính trên kênh BSC

Ví dụ

Ví dụ

Xét bộ mã nhị phân đều chiều dài 1 (ví dụ bộ mã nhị phân đều chiều dài 2: $\mathcal{C} = \{(00), (01), (11), (10)\}$). Giả sử kết quả mã hóa được truyền qua kênh nhị phân rời rạc đối xứng không nhớ (BSC) có xác suất thu sai p_0 , các bít được phát đi độc lập nhau, và xác suất phát đi bít 0 và bít 1 tương đương nhau.

- ① Tính xác suất thu được một từ mã đúng.
- ② Giả sử xác suất sai cho phép đối với việc thu các từ mã là p_a , tìm điều kiện đối với p_0 để có thể sử dụng được bộ mã cho việc thông tin qua kênh.



Notes

Dánh giá mã khối nhị phân tuyến tính trên kênh BSC

Dánh giá khả năng phát hiện lỗi

Cho $\mathcal{C}(I, k, d_{min})$ truyền qua kênh BSC có xác suất chuyền sai p .

- $P_u(E)$: xác suất véc-tơ thu có lỗi mà không phát hiện được.
- $P_e(E)$: xác suất véc-tơ thu có lỗi.
- $P_d(E)$: xác suất véc-tơ thu có lỗi được phát hiện.

$$P_u(E) \leq \sum_{j=d_{min}}^I \binom{I}{j} p^j (1-p)^{I-j} = 1 - \sum_{j=0}^{d_{min}-1} \binom{I}{j} p^j (1-p)^{I-j}$$

$$P_u(E) = \sum_{j=d_{min}}^I A_j p^j (1-p)^{I-j}$$

$$P_e(E) = \sum_{j=1}^I \binom{I}{j} p^j (1-p)^{I-j} = 1 - (1-p)^I$$

$$P_d(E) = P_e(E) - P_u(E) = 1 - (1-p)^I - P_u(E)$$



Notes

Dánh giá mã khối nhị phân tuyến tính trên kênh BSC

Dánh giá khả năng phát hiện lỗi (cont.)

- P_{ub} : tỷ lệ bít lỗi không được phát hiện
 - ▶ \triangleq xác suất bít thông tin nhận được bị lỗi trong một từ mã bị tác động bởi cấu trúc lỗi không phát hiện được
 - ▶ $P_u(E) \geq P_{ub}(E) \geq \frac{1}{k} P_u(E)$
- P_{db} : tỷ lệ bít lỗi được phát hiện
 - ▶ \triangleq xác suất bít thông tin nhận được bị lỗi trong một từ mã bị tác động bởi cấu trúc lỗi có thể phát hiện được.
 - ▶ $P_d(E) \geq P_{db}(E) \geq \frac{1}{k} P_d(E)$
- Nếu biết phân bố trọng của bộ mã, P_{ub} có thể tính một cách chính xác:

$$P_{ub} = \sum_{j=d_{min}}^I \frac{B_j}{k} p^j (1-p)^{I-j}$$

trong đó B_j là tổng trọng của các khối tin tương ứng với tất cả các từ mã có trọng là j .



Notes

Đánh giá mã khôi phục phân tán tính trên kênh BSC

Đánh giá khả năng sửa lỗi

Cho $\mathfrak{C}(l, k, d_{min})$ truyền qua kênh BSC có xác suất chuyển sai p .

Xét bộ giải mã có độ dài giới hạn.

- $P(E)$: xác suất giải mã sai

$$P(E) \leq \sum_{j=\lfloor \frac{d_{\min}}{2} - 1 \rfloor + 1}^l \binom{l}{j} p^j (1-p)^{l-j} = 1 - \sum_{j=0}^{\lfloor \frac{d_{\min}-1}{2} \rfloor} \binom{l}{j} p^j (1-p)^{l-j}$$

Đảng thức xảy ra chỉ khi mà là hoàn hảo.

- $P(F)$: xác suất giải mã thất bại

$$P(F) \leq 1 - \sum_{j=0}^{\lfloor \frac{d\min - 1}{2} \rfloor} \binom{l}{j} p^j (1-p)^{l-j}$$



Đánh giá mã khôi phục phân tán tính trên kênh BSC

Dánh giá khả năng sửa lỗi (cont')

Xét $\mathfrak{C}(l, k, d_{min})$ với phân bố trọng số đã biết $\{A_i\}$

$P_k^j \triangleq$ xác suất một véc-tơ thu có khoảng cách Hamming chính xác là k so với một từ mã có trọng là j .

$$P_k^j = \sum_{r=0}^k \binom{j}{k-r} \binom{l-j}{r} p^{j-k+2r} (1-p)^{l-j+k-2r}$$

$$P(E) = \sum_{i=d_{min}}^l A_j \sum_{k=0}^{\lfloor \frac{d_{min}-1}{2} \rfloor} P_k^j$$

$$P(F) = 1 - \sum_{i=0}^{\lfloor \frac{d_{min}-1}{2} \rfloor} \binom{i}{j} p^j (1-p)^{i-j} - P(E)$$



Notes

Notes

Dánh giá mã khối nhị phân tuyến tính trên kênh BSC

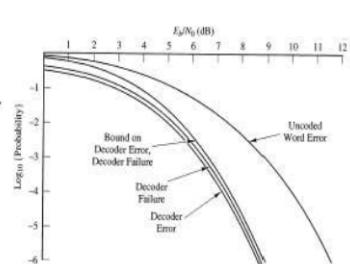
Dánh giá khả năng sửa lỗi (cont')

- Nếu biết được mối quan hệ giữa trọng số của các khối tin và trọng số các từ mã tương ứng

$$\Rightarrow B_j$$

- \Rightarrow

$$BER = P_b(E) = \frac{1}{k} \sum_{j=d_{min}}^l B_j \sum_{k=0}^{\lfloor \frac{d_{min}-1}{2} \rfloor} P_k^j$$



Chú ý: Thường, thông tin $\{B_j\}$ không khả thi.

- \Rightarrow Chủ yếu dựa vào các đánh giá biên

$$P(E) \geq P_b(E) \geq \frac{1}{k} P(E)$$



Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1)

Nội dung chính

1 Các định nghĩa và khái niệm cơ bản

2 Mã khối tuyến tính

- Mã khối tuyến tính
- Mã khối tuyến tính dạng hệ thống

3 Dánh giá mã khối nhị phân tuyến tính trên kênh BSC

4 Các vấn đề khi thiết kế mã khối tuyến tính

5 Kết thúc



Notes

Các vấn đề khi thiết kế mã khối tuyến tính

Thiết kế mã khối tuyến tính tối ưu

Khi thiết kế, ta mong muốn có được bộ mã có độ dư thừa nhỏ nhất có thể, nhưng lại có khả năng phát hiện và sửa lỗi lớn nhất có thể.

Trường hợp 1

Với k và d_{min} cho trước, xây dựng bộ mã có độ dư thừa tối thiểu: $\min\{l\}$.

Độ dài từ mã của bộ mã thỏa mãn giới hạn Griesmer:

$$l \geq \sum_{i=0}^{k-1} \lceil \frac{d_{min}}{2^i} \rceil$$

$\lceil x \rceil$: phần nguyên nhỏ nhất lớn hơn hoặc bằng x .



Notes

Các vấn đề khi thiết kế mã khối tuyến tính

Thiết kế mã khối tuyến tính tối ưu (cont')

Trường hợp 2

Với l và k cho trước, xây dựng bộ mã có khả năng phát hiện và sửa sai lớn nhất: $\max\{d_{min}\}$.

Khoảng cách Hamming tối thiểu của bộ mã thỏa mãn giới hạn Plotkin:

$$d_{min} \leq \frac{l \times 2^{k-1}}{2^k - 1}$$

Trường hợp 3

Với l và khả năng sửa sai t cho trước, xây dựng bộ mã có độ dư thừa nhỏ nhất: $\max\{k\}$.

Mối liên hệ giữa l , k và t thỏa mãn giới hạn Hamming:

$$2^{l-k} \geq \sum_{i=0}^t \binom{l}{i}$$

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 1)

Nội dung chính



Kết thúc phần mã khởi tuyến tính



Notes

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2: Mã vòng tuyến tính)

Biên soạn: Phạm Văn Sư

Bộ môn Xử lý tín hiệu và Truyền thông
Khoa Kỹ thuật Điện tử I
Học viện Công nghệ Bưu chính Viễn thông

ver 22a



Mục tiêu của bài học

- Tiếp tục trang bị một số khái niệm cơ bản về mã hóa kênh
 - Mã vòng (mã cyclic, mã xyclic) tuyến tính



Notes

Notes

Các câu hỏi cần trả lời

- Vành đa thức đồng dư?
 - Đa thức sinh, đa thức kiểm tra của mã vòng tuyến tính?
 - Mã vòng tuyến tính hệ thống? Thuật toán lập mã cho mã vòng tuyến tính hệ thống?
 - Các phương pháp giải mã cơ bản cho mã vòng tuyến tính?



Biên soạn: Phạm Văn Sư (PTIT)

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2: Mã vò

ver 22a

3 / 36

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1 Đa thức mă và các phép biến đổi

- Mã vòng tuyển tính
 - Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyển tính dạng hệ thống

- Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra

- Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng

5 Kết thúc



Biên soạn: Phạm Văn Sư (PTIT)

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2: Mã và

ver 22a

4 / 36

Notes

Notes

Đa thức mă và các phép biến đổi

Đa thức mă

Véc-tơ mă $c = (c_0, c_1, \dots, c_{l-1})$ có thể biểu diễn ở dạng đa thức:

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{l-1} x^{l-1}$$

Nhận xét:

- Mỗi véc-tơ mã/từ mã có chiều dài / tương ứng với một đa thức bậc nhỏ hơn hoặc bằng $l - 1$.
 - Mỗi quan hệ giữa véc-tơ mã với biểu diễn đa thức đảm bảo $1 - 1$.
 - $c(x)$ gọi là đa thức mã. Khái niệm từ mã/véc-tơ mã và đa thức mã có thể được dùng thay thế nhau.
 - $c \in \mathcal{C}(l, k) \Leftrightarrow c(x) \in GF(q)[x]/(x^l - 1)$



Đa thức mă và các phép biến đổi

Phép cộng đa thức, Phép nhân đa thức

- Xét các đa thức $f(x), g(x)$ trên $GF(q)[x]/(x^l - 1)$

Phép công đa thức

$$f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_{l-1}x^{l-1}$$

$$g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_{l-1}x^{l-1}$$

$$\Rightarrow f(x) + g(x) = (f_0 + g_0) + (f_1 + g_1)x + \cdots + (f_{l-1} + g_{l-1})x^{l-1}$$

Phép nhân đa thức

$$f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_{l-1}x^{l-1} = \sum_{i=0}^{l-1} f_i x^i$$

$$g(x) \equiv g_0 + g_1 x + g_2 x^2 + \cdots + g_{l-1} x^{l-1} = \sum_{j=0}^{l-1} g_j x^j$$

$$g(x) = g_0 + g_1 x + g_2 x^2 + \dots + g_{l-1} x^{l-1} - \sum_{j=0}^{l-1} g_j x^j$$

$$\equiv f(x) \times g(x) \equiv (\sum_{i=0}^{l-1} f_i x^i)(\sum_{j=0}^{l-1} g_j x^j) \text{ modulo } (x^l - 1)$$



Notes

Notes

Đa thức mã và các phép biến đổi

Phép dịch vòng

Trên $GF(q)[x]/(x^l - 1)$, cho $f(x) = \sum_{i=0}^{l-1} f_i x^i \longleftrightarrow a = (f_0, f_1, \dots, f_{l-1})$

Xét $g(x) = x.f(x) \longleftrightarrow b = (f_{l-1}, f_0, f_1, \dots, f_{l-2})$ (chú ý: mod $x^l - 1$)

- b thu được bằng cách dịch vòng về phía phải của a một cấp/nhịp/vòng.
- Kí hiệu $g(x) = f^{(1)}(x)$.
- \Rightarrow Nhân x^i với $f(x)$ thu được một véc-tơ là kết quả dịch vòng phải của véc-tơ ban đầu đi i nhịp/cấp: $f^{(i)}(x)$.

Xét $g(x) = \frac{f(x)}{x} \longleftrightarrow b = (f_1, f_2, f_3, \dots, f_{l-1}, f_0)$ (chú ý: mod $x^l - 1$)

- b thu được bằng cách dịch vòng về phía trái của a một cấp/vòng.
- \Rightarrow Chia $f(x)$ cho x^i thu được một véc-tơ là kết quả dịch vòng trái của véc-tơ ban đầu đi i nhịp/cấp.

PTIT
PHÁT TRIỂN
VÀ THƯƠNG MẠI
TRỰC TUYẾN

Notes

Đa thức mã và các phép biến đổi

Đa thức đối ngẫu

Định nghĩa

Cho đa thức $f(x)$ bậc k : $f(x) = f_0 + f_1 x + f_2 x^2 + \dots + f_k x^k$.

Đa thức đối ngẫu của $f(x)$, kí hiệu là $f^*(x)$ được định nghĩa là:

$$f^*(x) = x^k \times f(x^{-1}) = f_k + f_{k-1} x + f_{k-2} x^2 + \dots + f_1 x^{k-1} + f_0 x^k$$

- Nếu $f^*(x) = f(x)$ thì $f(x)$ là đa thức tự đối ngẫu.



Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

② Mă vòng tuyển tính

- Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống

- Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra

- Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng

5 Kết thúc



C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

② Mã vòng tuyển tính

- Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống

- Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra

- Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng

5 Kết thúc



Notes

Notes

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Định nghĩa

Định nghĩa

Một mã khối tuyến tính $\mathcal{C}(l, k)$ được gọi là mã vòng tuyến tính nếu với mọi từ mã $c = (c_0, c_1, \dots, c_{l-1}) \in \mathcal{C}$ thì kết quả của mỗi dịch vòng từ mã c cũng sẽ thu được một véc-tơ cũng là một từ mã thuộc \mathcal{C} .

Cho $a(x) \in GF(q)[x]/(x^l - 1)$, $c(x) \in \mathcal{C}$

$\Rightarrow a(x)c(x)$ là tổ hợp tuyến tính của các dịch vòng của $c(x)$

$\Rightarrow a(x)c(x) \in \mathcal{C} \quad \forall a(x) \in GF(q)[x]/(x^l - 1), c(x) \in \mathcal{C}$



Notes

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Một số tính chất, Đa thức sinh

Định lý

Bộ mã \mathcal{C} là một bộ mã vòng tuyến tính cơ số q có chiều dài từ mã l nếu và chỉ nếu các đa thức mã của \mathcal{C} tạo thành một ideal trên $GF(q)[x]/(x^l - 1)$.

- Trong tập tất cả các đa thức mã của \mathcal{C} , có một đa thức monic duy nhất $g(x)$ với bậc tối thiểu $r = l - k < l$. $g(x)$ được gọi là đa thức sinh của bộ mã \mathcal{C} .
- Mọi đa thức mã $c(x) \in \mathcal{C}$ tồn tại duy nhất một biểu diễn $c(x) = a(x)g(x)$, trong đó $g(x)$ là đa thức sinh, $a(x)$ là đa thức bậc $\leq l - r = k$ trên $GF(q)[x]$.
- Đa thức sinh $g(x)$ của bộ mã \mathcal{C} là một thừa số của $x^l - 1$ trên $GF(q)[x]$.

Định lý

Nếu $g(x)$ có bậc $r = l - k$ và là một thừa số của $x^l - 1$ thì $g(x)$ là một đa thức sinh của mã vòng tuyến tính $\mathcal{C}(l, k)$.

Notes

Mã vòng tuyển tính

Một số định nghĩa và khái niệm: Đa thức kiểm tra, Mã vòng đối ngẫu

Định nghĩa

Một bộ mã vòng tuyến tính $\mathfrak{C}(l, k)$ có đa thức sinh $g(x)$. Một đa thức $h(x) \neq 0$ được gọi là đa thức kiểm tra của $\mathfrak{C}(l, k)$ nếu $g(x) \times h(x) = x^l - 1 \equiv 0 \pmod{x^l - 1}$

- $\deg(h(x)) = k$
 - $h(x) = \frac{x^k - 1}{g(x)}$

Định lý

$\mathfrak{C}(I, k)$ là một mã vòng tuyến tính với đa thức sinh $g(x)$. Khi đó, mã đối ngẫu \mathfrak{C}^\perp cũng là một mã vòng tuyến tính $(I, I - k)$ và được sinh ra từ đa thức sinh $h^*(x) = x^k h(x^{-1})$ với $h(x) = \frac{(x^l - 1)}{g(x)}$.

Biên soạn: Phạm Văn Sư (PTIT)

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2: Mã vò

ver 22a

13 / 36

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

- 1 Da thức mã và các phép biến đổi
 - 2 Mã vòng tuyến tính
 - Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống
 - 3 Mạch nguyên lý mã hóa mã vòng
 - Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra
 - 4 Các phương pháp giải mã vòng
 - Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
 - 5 Kết thúc



Biên soạn: Phạm Văn Sư (PTIT)

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2: Mã và

ver. 22a

14 / 36

Notes

Notes

Mã vòng tuyển tính

Một số định nghĩa và khái niệm: Ma trận sinh của mã vòng

Một bộ mã vòng tuyến tính $\mathcal{C}(l, k)$ với đa thức sinh

$$g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_{l-k}x^{l-k} \text{ có ma trận sinh xác định bởi:}$$

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{l-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{l-k-1} & g_{l-k} & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{l-k-2} & g_{l-k-1} & g_{l-k} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & g_{l-k} \end{bmatrix}$$

- G có kích thước $k \times l$
 - G không có dạng hệ thống



Mã vòng tuyển tính

Một số định nghĩa và khái niệm: Ma trận kiểm tra của mã vòng

Trên $GF(q)$, xét bộ mã vòng tuyến tính $\mathcal{C}(l, k)$ với đa thức sinh $g(x)$. Tồn tại một đa thức $h(x)$ bậc $k = l - r$ thỏa mãn $g(x)h(x) = x^l - 1$, hay $h(x)g(x) \equiv 0 \pmod{x^l - 1}$. $h(x)$ được gọi là đa thức kiểm tra của mã $\mathcal{C}(l, k)$.

Xét một bộ mã vòng tuyến tính $\mathcal{C}(l, k)$ với đa thức kiểm tra $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_kx^k$, ma trận kiểm tra của nó được xác định bởi:

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_1 & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_k & \dots & h_2 & h_1 & h_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & h_0 \end{bmatrix}$$

- H có kích thước $I - k \times I$
 - $G H^T \equiv 0$



Notes

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

② Mă vòng tuyển tính

- Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mảng vòng
 - Mảng vòng tuyến tính dạng hệ thống

- Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra

- Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng

5 Kết thúc



Mã vòng tuyển tính dạng hệ thống

Thuật toán chia = Thuật toán bốn bước = Thuật toán tạo từ mã dạng hệ thống từ đa thức sinh

Từ mã dang hệ thống c = [p | a]

Bài toán

Nhập vào: $\mathcal{C}(l, k)$, $g(x)$, khôi tin cần mã hóa $a = (a_0, a_1, \dots, a_{k-1})$.

In ra: Từ mã dạng hệ thống tương ứng c

Thuật toán

- Mô tả khối tin bằng biểu diễn đa thức tương ứng $a(x)$.
 - Tính $a^{(l-k)}(x) = x^{l-k}a(x)$.
 - Chia $x^{l-k}a(x)$ cho đa thức sinh $g(x)$ của bộ mã, thu được phần dư $p(x)$.
 - Thành lập đa thức mã $c(x) = p(x) + x^{l-k}a(x)$. In ra từ mã tương ứng với đa thức mã $c(x)$.



Notes

Notes

Mã vòng tuyển tính dạng hệ thống

Thuật toán nhân = Thuật toán tạo từ mã dạng hệ thống từ đa thức kiểm tra

- Hoàn toàn có thể xây dựng được mã vòng tuyên tính dạng hệ thống từ đa thức (ma trận) kiểm tra.

Xây dựng mã hệ thống từ đa thức kiểm tra

- ❶ Từ khôi tin vào (tương ứng đa thức tin) ta có: $c_{l-k} = a_0, c_{l-k+1} = a_1, \dots, c_{l-1} = a_{k-1}$.
 - ❷ Tính toán $c_0, c_1, \dots, c_{l-k-1}$ từ công thức:

$$c_{l-k-i} = \sum_{i=0}^{k-1} h_j c_{l-j-i} \quad (1 \leq i \leq l-k)$$

- ③ Từ mã tương ứng dạng hệ thống $c = (c_0, c_1, c_2, \dots, c_{l-k-1}, a_0, \dots, a_{k-1})$.



Mã vòng tuyển tính dạng hệ thống

Ma trận sinh, ma trận kiểm tra dạng hệ thống

G phương pháp khử Gausse $\xrightarrow{}$ G dạng hệ thống

- Nếu $G = [P \quad | \quad I_k] \Rightarrow H = [I_{l-k} \quad | \quad P^T]$
 - Nếu $G = [I_k \quad | \quad P] \Rightarrow H = [P^T \quad | \quad I_{l-k}]$



Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

- ① **Đa thức mã và các phép biến đổi**
 - ② **Mã vòng tuyến tính**
 - Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống
 - ③ **Mạch nguyên lý mã hóa mã vòng**
 - Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra
 - ④ **Các phương pháp giải mã vòng**
 - Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
 - ⑤ **Kết thúc**



C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

- ① **Đa thức mã và các phép biến đổi**
 - ② **Mã vòng tuyến tính**
 - Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống
 - ③ **Mạch nguyên lý mã hóa mã vòng**
 - Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra
 - ④ **Các phương pháp giải mã vòng**
 - Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
 - ⑤ **Kết thúc**

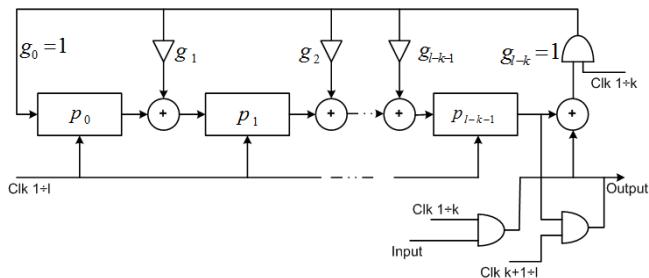


Notes

Notes

Mã vòng tuyến tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức sinh - Sơ đồ mạch nguyên lý



Hình: Mạch thực hiện mã hóa mã vòng dạng tuyến tính dựa trên đa thức sinh



Notes

Mã vòng tuyến tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức sinh - Nguyên lý hoạt động

- ➊ Đầu tiên, nội dung các thanh ghi được xóa về 0.
- ➋ k nhịp đầu tiên, véc-tơ tin (a) được dịch trực tiếp ra đầu ra và đồng thời được dịch vào mạch để tính các bít kiểm tra. Sau k nhịp, nội dung các thanh ghi là các bít kiểm tra.
- ➌ $I - k$ nhịp tiếp theo, mạch thực hiện dịch nội dung các bít kiểm tra trong thanh ghi ra đầu ra.
- ➍ Quá trình mã hóa kết thúc khi toàn bộ khối bít kiểm tra được dịch ra ngoài.



Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi

2. Mã vòng tuyến tính

- Một số định nghĩa và khái niệm
- Ma trận sinh và ma trận kiểm tra của mã vòng
- Mã vòng tuyến tính dạng hệ thống

3. Mạch nguyên lý mã hóa mã vòng

- Xây dựng từ đa thức sinh
- Xây dựng từ đa thức kiểm tra

4. Các phương pháp giải mã vòng

- Phương pháp giải mã ngưỡng
- Phương pháp bẫy lỗi - Thuật toán chia dịch vòng

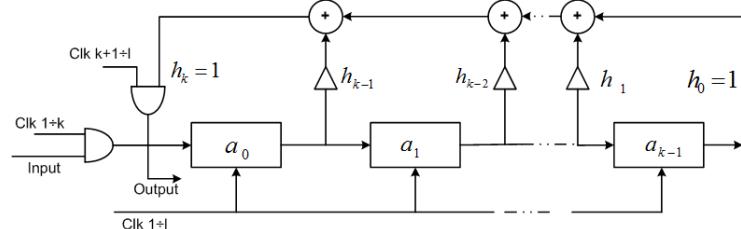
5. Kết thúc



Notes

Mã vòng tuyến tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức kiểm tra - Mạch nguyên lý



Hình: Sơ đồ mạch mã hóa mã vòng dạng hệ thống dựa trên đa thức kiểm tra



Notes

Mã vòng tuyển tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức kiểm tra - Nguyên lý hoạt động

- ➊ Đầu tiên, nội dung các thanh ghi thông tin được xóa về 0.
 - ➋ k nhịp đầu tiên, khôi thông tin được dịch vào các thanh ghi đồng thời dịch ra đầu ra. Sau k nhịp, nội dung các thanh ghi là nội dung của khôi tin.
 - ➌ $l - k$ nhịp tiếp theo, các c_{l-k-i} ($i = \overline{1, l - k}$) được tính và được chuyển vào thanh ghi đồng thời chuyển ra đầu ra.
 - ➍ Quá trình mã hóa kết thúc sau khi $l - k$ bít kiểm tra được lập xong.



C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

- ① Da thức mã và các phép biến đổi
 - ② Mã vòng tuyến tính
 - Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống
 - ③ Mạch nguyên lý mã hóa mã vòng
 - Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra
 - ④ Các phương pháp giải mã vòng
 - Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
 - ⑤ Kết thúc



Notes

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

- ① **Đa thức mã và các phép biến đổi**
 - ② **Mã vòng tuyến tính**
 - Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống
 - ③ **Mạch nguyên lý mã hóa mã vòng**
 - Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra
 - ④ **Các phương pháp giải mã vòng**
 - Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
 - ⑤ **Kết thúc**

Biên soạn: Phạm Văn Sư (PTIT)

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2: Mã vò

ver 22a

14

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Hệ tổng kiểm tra

$$c \in \mathfrak{C}, w \in \mathfrak{C}^\perp A \triangleq wr = we$$

A: một tổng kiểm tra.

$$A = w_0 e_0 + w_1 e_1 + \cdots + w_{l-1} e_{l-1}$$

- bít lỗi e_k được kiểm tra bằng tổng kiểm tra A nếu $w_k = 1$.

Định nghĩa (Hệ tổng kiểm tra trực giao)

Một hệ gồm J tổng kiểm tra được gọi là hệ tổng kiểm tra trực giao với vị trí bít lỗi e_{j-1} nếu:

- ① Tất cả các hệ số của e_{l-1} trong hệ J tổng kiểm tra bằng 1.
 - ② Với $k \neq l - 1$ chỉ có nhiều nhất một véc-tơ trong hệ tổng kiểm tra mà hệ số của e_k bằng 1.

$$\Rightarrow A_k = e_{l-1} + \sum_{i \neq l-1} w_i e_i$$



Notes

Notes

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Thuật toán một bước

Giải mã ngưỡng dựa trên hệ tổng kiểm tra trực giao

Bít lỗi e_{l-1} được quyết định là 1 nếu có phần lớn các véc-tơ trong tổng kiểm tra trực giao bằng 1. Ngược lại thì bít lỗi e_{l-1} được quyết định là 0.

- Bộ giải mã hoạt động đúng khi véc-tơ lỗi có trọng $\leq \lfloor J/2 \rfloor$.
- Nếu có thể tạo hệ J tổng kiểm tra trực giao cho e_{l-1} thì cũng có thể tạo hệ J tổng kiểm tra trực giao cho các vị trí bít lỗi e_k ($k \neq l-1$) nào đó.
- Nếu J là số tổng kiểm tra trực giao cực đại có thể lập được cho e_{l-1} (hoặc bất kỳ e_k nào đó), phương pháp giải mã nêu trên có thể sửa được các cấu trúc lỗi có trọng $\leq \lfloor J/2 \rfloor$. $t_{ML} = \lfloor J/2 \rfloor$: khả năng sửa lỗi của bộ giải mã ngưỡng.
- Phép giải mã này được gọi là hiệu quả với bộ mã $\mathcal{C}(l, k, d_0)$ chỉ nếu $t_{ML} = \lfloor J/2 \rfloor$ bằng hoặc xấp xỉ bằng $t = \lfloor (d_0 - 1)/2 \rfloor$.



Notes

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Hệ tổng kiểm tra có khả năng trực giao

Định nghĩa (Bộ mã vòng có khả năng trực giao đầy đủ)

Một bộ mã vòng $\mathcal{C}(l, k, d_0)$ gọi là có khả năng trực giao đầy đủ một bước nếu và chỉ nếu nó có thể tạo được hệ $J = d_0 - 1$ tổng kiểm tra trực giao với một vị trí bít lỗi nào đó.

- $J < l - k$.
- Không phải mọi mã vòng $\mathcal{C}(l, k, d_0)$ đều là có khả năng trực giao đầy đủ.

Định nghĩa (Hệ tổng kiểm tra có khả năng trực giao)

Một tập gồm J tổng kiểm tra A_1, A_2, \dots, A_J là hệ tổng kiểm tra trực giao với tập M vị trí bít lỗi $E = \{e_{i_1}, e_{i_2}, \dots, e_{i_M}\}$ ($0 \leq i_1 < i_2 < \dots < i_M < l$) nếu:

- ➊ Mọi vị trí bít lỗi e_{i_j} của E đều được kiểm tra bởi mọi tổng kiểm tra A_j ($1 \leq j \leq J$), và
- ➋ Không có bất cứ vị trí lỗi nào khác được kiểm tra ở nhiều hơn 1 tổng kiểm tra.

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

2 Mă vòng tuyển tính

- Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống

- Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra

4 Các phương pháp giải mã vòng

- Phương pháp giải mã ngược
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng

5 Kết thúc



Các phương pháp giải mã vòng

Phương pháp bẫy lỗi - Thuật toán chia dịch vòng: Thuật toán

Nhập vào: Véc-tơ thu $r(x)$ và thông số bộ mã $\mathfrak{C}(l, k)$ như đa thức sinh $g(x)$ và d_{min} , kí hiệu $\mathfrak{C}(l, k, d_{min})$.

In ra Từ mã đã được sửa sai.

Bước 1: Với $j = 0, \dots, l - 1$

- ① Tính $s_i(x)$ là phần dư của phép chia $x^i r(x)$ [hoặc $\frac{r(x)}{x^i}$] cho $g(x)$.
 - ② Tính trọng của $s_i(x)$: $w(s_i(x))$.
 - ③ Nếu $w(s_i(x)) \leq t = \lfloor \frac{d_{\min}-1}{2} \rfloor$ chuyển đến **Bước 2**.
 - ④ Nếu $w(s_i(x)) > t$ tăng i lên 1 đơn vị.
 - ⑤ Nếu $i = l$ chuyển đến **Bước 3**.

Bước 2 Đa thức mã được sửa bởi: $\hat{r}(x) = \frac{x^i r(x) + s_i(x)}{x^i}$ [hoặc $\hat{r}(x) = x^i \{ \frac{r(x)}{x^i} + s_i(x) \}$] In ra từ mã đã được sửa lỗi tương ứng. Kết thúc.

Bước 3 Thông báo không sửa được lỗi (số lỗi vượt quá khả năng sửa lỗi). Kết thúc.

Notes

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

- ① **Đa thức mã và các phép biến đổi**
 - ② **Mã vòng tuyến tính**
 - Một số định nghĩa và khái niệm
 - Ma trận sinh và ma trận kiểm tra của mã vòng
 - Mã vòng tuyến tính dạng hệ thống
 - ③ **Mạch nguyên lý mã hóa mã vòng**
 - Xây dựng từ đa thức sinh
 - Xây dựng từ đa thức kiểm tra
 - ④ **Các phương pháp giải mã vòng**
 - Phương pháp giải mã ngưỡng
 - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
 - ⑤ **Kết thúc**



Kết thúc phần mã vòng



Notes

Notes

Lý thuyết thông tin



Phần 4 Cyclic coding

- Cơ sở toán học
- Mã hóa
- Giải mã

dinhnq@ptit.edu.vn

Vành đa thức $Z_2[x]/x^n + 1$

Tập các đa thức $f(x) = \sum_{i=0}^{n-1} f_i x^i \quad f_i \in GF(2)$

với hai phép toán: cộng và nhân đa thức theo modulo $X^n + 1$

tạo nên một vành đa thức, ký hiệu vành này là $Z_2[x]/x^n + 1$

Cộng và nhân đa thức theo modulo $X^n + 1$ như thế nào?

Xét hai đa thức thuộc vành: $a(x) = \sum_{i=0}^{n-1} a_i x^i \quad b(x) = \sum_{i=0}^{n-1} b_i x^i$

Phép cộng: $a(x) + b(x) = c(x) = \sum_{i=0}^{n-1} (a_i + b_i)x^i$

with $a_i + b_i$ is add in $GF(2)$

Nếu ta coi mỗi đa thức $f(x)$ là một véctơ trong không gian tuyến tính V_n

$$f(x) = f_0 + f_1 x + \dots + f_{n-1} x^{n-1} \Leftrightarrow f = (f_0, f_1, \dots, f_{n-1})$$

thì phép cộng đa thức hoàn toàn tương tự như phép cộng véctơ.

Vành đa thức $Z_2[x]/x^n + 1$ (tt)

Phép nhân đa thức

Phép nhân 2 đa thức được thực hiện theo mod $X^n + 1$ (tức là coi $X^n = 1 (=x^0)$).

(Để đảm bảo $c(X)$ vẫn là một đa thức có bậc $\leq n - 1$ thuộc R)

$$c(X) = a(X) \cdot b(X) = \left(\sum_{i=0}^{n-1} a_i x^i \right) \cdot \left(\sum_{i=0}^{n-1} b_i x^i \right) \text{mod } X^n + 1$$

Chú ý: Tích của hai đa thức được thực hiện trên cơ sở tích của hai đơn
thức $a_i x^i$ và $b_j x^j$ theo nguyên tắc:

- $x^i \cdot x^j = x^{(i+j)} \text{mod } n$
- $a_i b_j$ là phép nhân mod trên trường F

Phép dịch vòng trên vành đa thức $Z_2[x]/x^n + 1$

Xét đa thức thuộc vành: $a(X) = \sum_{i=0}^{n-1} a_i x^i \leftrightarrow a = (a_0, a_1, a_2, \dots, a_{n-1})$

Khi đó: $b(X) = x \cdot a(X) = x \cdot \left(\sum_{i=0}^{n-1} a_i x^i \right) \leftrightarrow b = (a_{n-1}, a_0, a_1, \dots, a_{n-2})$

Tổng quát: $c(X) = x^j \cdot a(X) = x^j \cdot \left(\sum_{i=0}^{n-1} a_i x^i \right) \leftrightarrow c = (a_{n-j}, a_{n-j+1}, \dots, a_{n-j-1})$

Hệ quả: $d(X) = \frac{a(X)}{x} = x^{-1} a(X) = \frac{x^n a(X)}{x} = x^{n-1} a(X)$

Đa thức bất khả quy

Định nghĩa: Đa thức $a(x)$ được gọi là bất khả quy nếu nó chỉ chia hết cho 1 và cho chính nó. Như vậy đa thức này không thể phân tích thành tích các đa thức có bậc nhỏ hơn.

Chú ý 1: Một số đa thức bất khả quy

$$\text{Bậc 1: } 1 + x$$

$$\text{Bậc 2: } 1 + x + x^2$$

$$\text{Bậc 3: } 1 + x + x^3; \quad 1 + x^2 + x^3$$

$$\text{Bậc 4: } 1 + x + x^4; \quad 1 + x^3 + x^4; \quad 1 + x + x^2 + x^3 + x^4;$$

Chú ý 2:

- Trọng số của đa thức = trọng số của vector biểu diễn đa thức đó.
- Đa thức bất khả quy (ngoại trừ $1+x$) là đa thức có trọng số lẻ và có số hạng tự do bằng 1, (tức nó chứa một số lẻ các đơn thức).

Phân tích của nhị thức x^n+1

Định lý: Nếu $2^m-1=n$, thì đa thức $X^n + 1$ được phân tích thành tích của tất cả các đa thức bất khả quy có bậc m và ước của m.

Xét x^7+1 : m = 3, n = 7: Trong số 8 đa thức bậc 3 chỉ có 2 đa thức sau là các đa thức bất khả quy, đó là $x^3 + x + 1$ và $x^3 + x^2 + 1$. Như vậy:

$$X^7 + 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$$

Câu hỏi:

Chứng minh rằng: $(x^n + 1) \div (x + 1) \quad \forall n \geq 1$

Ideal của Vành đa thức $Z_2[x]/x^n + 1$

Định nghĩa: Ideal I của vành đa thức $Z_2[x]/X^n + 1$ gồm tập các đa thức là

bội của một đa thức $g(X) = \sum_{i=0}^r g_i x^i$ thỏa mãn:

- $g(X) | X^n + 1$ (tức $g(X)$ là ước của $X^n + 1$)
- Với $\forall a(X) \in I, a(X) \neq 0$ ta có: $\deg g(X) = r = \min \deg a(X)$

Ký hiệu Ideal của vành đa thức là $I = \langle g(X) \rangle$

Mã Cyclic

Một mã cyclic (n,k) sinh bởi $g(x) = g_0 + g_1x + \dots + g_rx^r$

chính là một ideal $I=\langle g(x) \rangle$ của $Z_2[x]/x^n + 1$

$g(x)$: generator polynomial, order $r=n-k$

Câu hỏi:

Điều kiện để $g(x)$ là đa thức sinh của mã cyclic (n,k)?

- Ở dạng general, đa thức mã của một bộ mã Cyclic(n,k) là tích của đa thức sinh $g(x)$ với đa thức thông tin $a(x)$

Số mã cyclic trên vành đa thức $Z_2[x]/x^n + 1$

- Để tìm được tất cả các mã trong vành $Z_2[x]/x^n + 1$ ta phải thực hiện phân tích nhị thức $x^n + 1$ thành tích của các đa thức bất khả quy

Gọi số các đa thức bất khả quy trong phân tích của $x^n + 1$ là a , khi đó số các Ideal (tức số bộ mã) trong vành được xác định theo biểu thức:
 $|I| = 2^a - 1$.

Ví dụ: Xét vành $Z_2[x]/x^7 + 1$:

	$g(x)$	$C(n, k)$	d_0	Note
1	1	(7, 7)	1	no parity code
2	$1 + x$	(7, 6)	2	Single parity-check code
3	$1+x+x^3$	(7, 4)	3	Hamming code
4	$1+x^2+x^3$	(7, 4)	3	Hamming code
5	$1+x+x^2+x^4$	(7, 3)	4	
6	$1+x^2+x^3+x^4$	(7, 3)	4	
7	$1+x+x^2+x^3+x^4+x^5+x^6$	(7, 1)	7	repetition code

Generator matrix / parity-check matrix

- Ở dạng general, mã cyclic (n,k) sinh bởi $g(x)$ có:

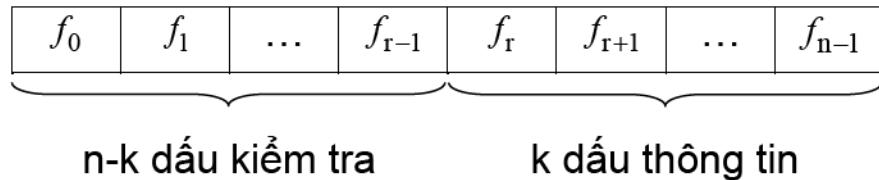
$$G = \begin{pmatrix} g(x) \\ x.g(x) \\ \dots \\ x^{k-1}g(x) \end{pmatrix} \quad H = \begin{pmatrix} h^*(X) \\ x.h^*(X) \\ \dots \\ x^{r-1}.h^*(X) \end{pmatrix}$$

Trong đó đa thức kiểm tra: $h(x) = \frac{x^n + 1}{g(x)}$

Đa thức đối ngẫu (reciprocal) của $h(x)$: $h^*(x) = x^{\deg h(x)} h(x^{-1})$

Linear Systematic (n,k) code :

- Từ mã dạng hệ thống



- Mã dạng hệ thống sử dụng G và H dạng hệ thống:

$$\diamond \quad G_{\text{sys}} = [P_{k,r} : I_{k,k}]$$

$$\diamond \quad H_{\text{sys}} = [I_{r,r} : P_{r,k}^T]$$

Mã hóa cyclic hệ thống theo phương pháp chia

Thuật toán tạo từ mã hệ thống

VÀO: $C(n,k)$, $g(x)$

Message $a = (a_0, a_1, \dots, a_{k-1}) \quad a \in A$

RA: Codeword dạng hệ thống

BƯỚC 1: Mô tả message a thành đa thức thông tin

$$a(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1} \quad \deg a(x) \leq k-1$$

BƯỚC 2: Nâng bậc $a(x)$ để dịch chuyển lên vùng bit cao

$$[x^{n-k} a(x)] = a_0 x^{n-k} + a_1 x^{n-k+1} + \dots + a_{k-1} x^{n-1}$$

BƯỚC 3: Tính $r(x) = [x^{n-k} a(x)] \bmod g(x) = r_0 + r_1 x + \dots + r_{n-k-1} x^{n-k-1}$

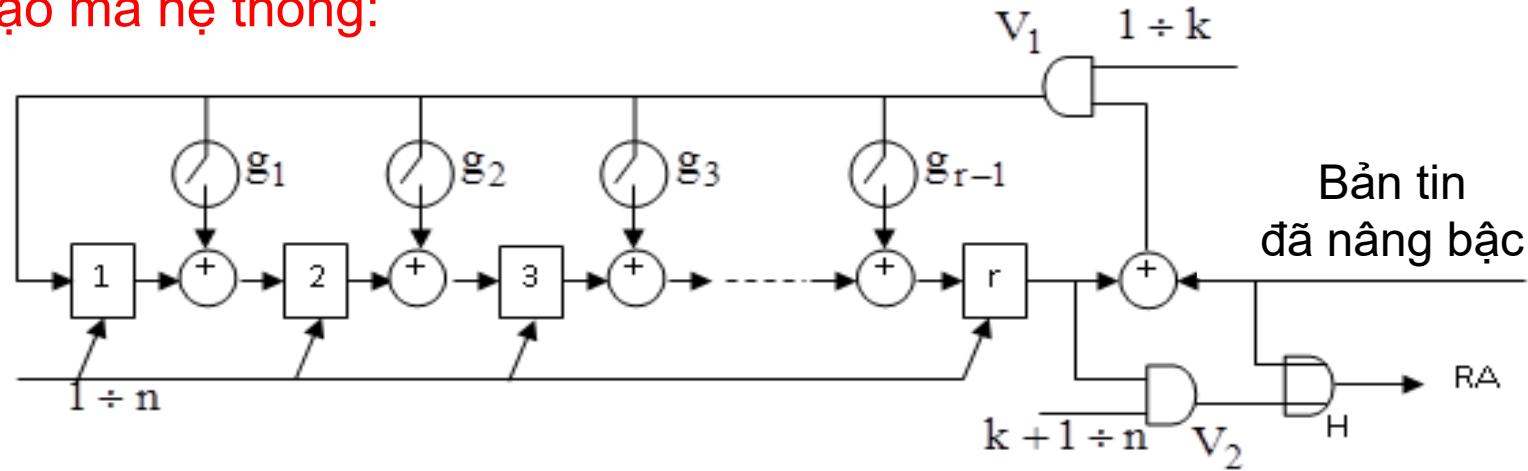
BƯỚC 4: Xác lập đa thức mã ra $f(x) = r(x) + x^{n-k} a(x)$

$$= \underbrace{r_0 + r_1 x + \dots + r_{n-k-1} x^{n-k-1}}_{r(x)} + \underbrace{a_0 x^{n-k} + a_1 x^{n-k+1} + \dots + a_{k-1} x^{n-1}}_{x^{n-k} a(x)}$$

tương ứng với codeword $f = (\underbrace{f_0, f_1, \dots, f_{n-k-1}}_{r(x)}, \underbrace{f_{n-k}, \dots, f_{n-1}}_{x^{n-k} a(x)})$

Mã hóa cyclic hệ thống theo phương pháp chia (tt)

-Bộ tạo mã hệ thống:



Mã hóa cyclic hệ thống theo phương pháp nhân

Thuật toán tạo từ mã hệ thống

VÀO: $C(n,k)$, $g(x)$

Message $a \in (\text{Áo } 2^k \text{ message}), \quad a = (a_0, a_1, \dots, a_{k-1})$

RA: Codeword dạng hệ thống $f = (\underbrace{f_0, f_1, \dots, f_{n-k-1}}_{\text{bit bit}}, \underbrace{f_{n-k}, \dots, f_{n-1}}_{\text{bit bit}})$

BƯỚC 1: Tính $h(x) = \frac{x^n + 1}{g(x)} = \sum_{j=0}^k h_j x^j$

BƯỚC 2: Lập công thức các dấu mã vùng bit cao

$$f_{n-k} = a_0, f_{n-k+1} = a_1, \dots, f_{n-1} = a_{k-1}$$

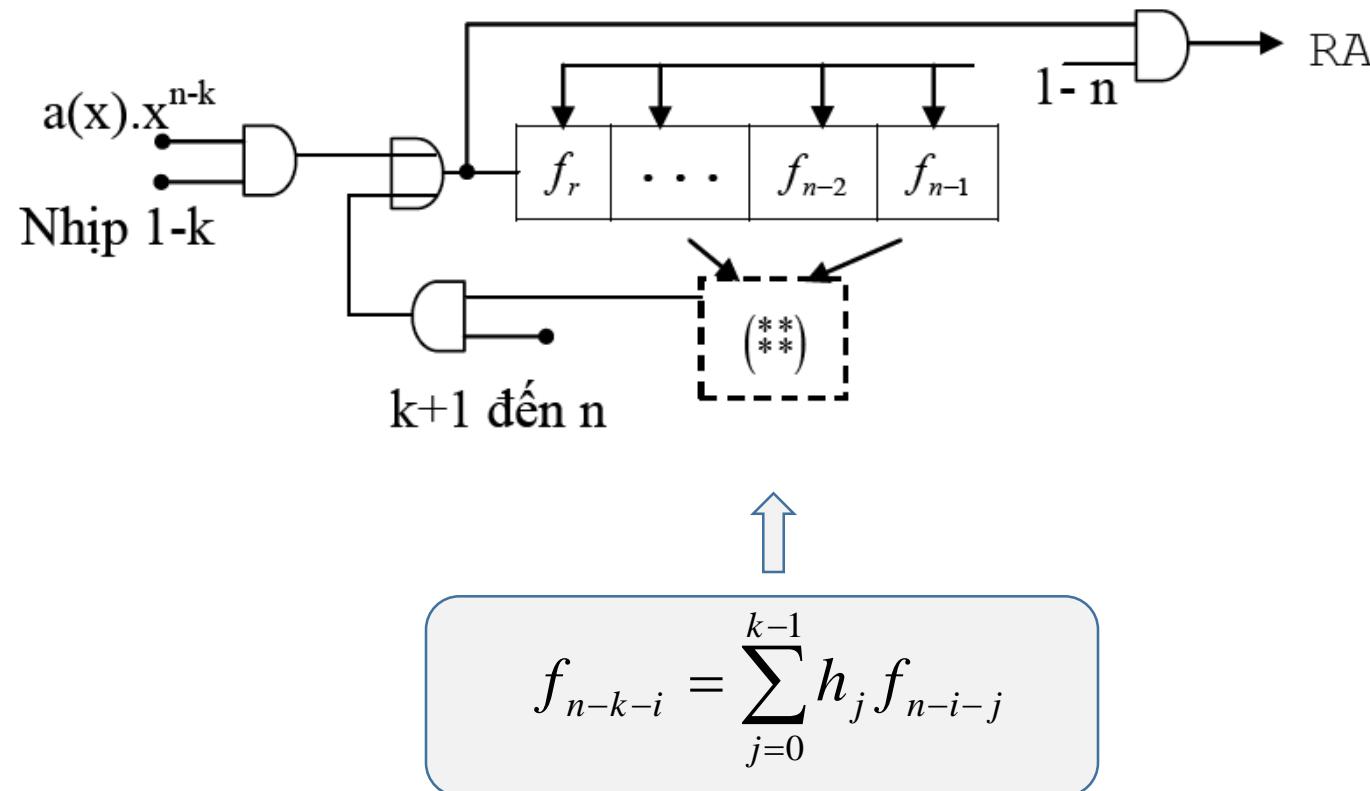
BƯỚC 3: Lập công thức các dấu mã vùng bit thấp

$$f_{n-k-i} = \sum_{j=0}^{k-1} h_j f_{n-i-j} \quad 1 \leq i \leq n - k$$

BƯỚC 4: Xác lập giá trị codeword theo bản tin vào

Mã hóa cyclic hệ thống theo phương pháp nhân (...)

-Bộ tạo mã hệ thống:

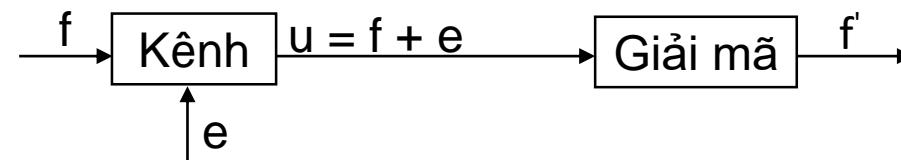


Giải mã ngưỡng

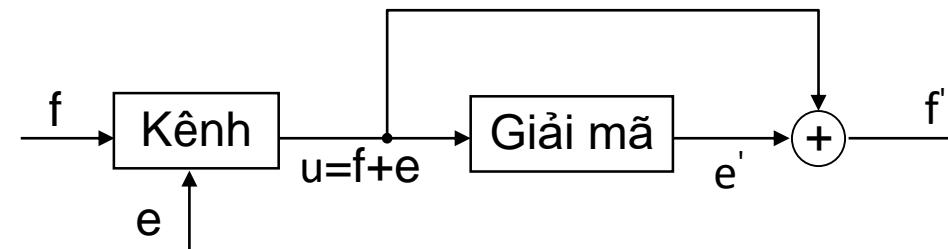
a. Thủ tục giải mã

Mọi phương pháp giải mã đều có thể tiến hành theo một trong hai thủ tục giải mã sau:

-Thủ tục 1: Dẫn ra từ mã gốc f từ vector u .



-Thủ tục 2: Dẫn ra vécto sai e từ u .



$$u + e' = [f + e] + e' = f + [e + e']$$

$$\text{if } e = e' \text{ then } e + e' = 0, \Rightarrow f' = f$$

Giải mã ngưỡng (...)

b. Syndrom của vector mã nhận được

Gọi vector tới đầu vào máy thu là: $u = (u_0 u_1 \dots u_{n-1})$

Syndrom của u: $S(u) = u.H^T$

Khai triển: $S(u) = (f + e)H^T = eH^T = S(e)$

Vậy $S(u)$ đặc trưng cho cấu trúc lỗi trong vector u

-Quá trình giải mã dựa trên việc phân tích trạng thái của $S(u)$ được gọi là giải mã theo syndrom (hội chứng).

- Hiển nhiên là khi không có sai ($e \equiv 0$) ta có: $S(u) = S(e) = 0$
- Khi có sai: $S(u) = S(e) \neq 0$

Giải mã ngưỡng (...)

Các tổng kiểm tra trong S(u)

$$S(u) = u \cdot H^T = \begin{pmatrix} s_0 & s_1 & \dots & s_{n-k-1} \end{pmatrix}$$

- Mỗi thành phần của $S(u)$ sẽ mô tả một mối quan hệ nào đó giữa các dấu mã, và được gọi là một tổng kiểm tra.

Tập r tổng kiểm tra trong $S(u)$ tạo nên hệ tổng kiểm tra. Mỗi tổng kiểm tra trong hệ sẽ chứa một thông tin nhất định về dấu cần giải mã u_i , thông tin đó có thể nhiều, ít hoặc bằng không. Ngoài ra mỗi tổng kiểm tra này còn chứa thông tin về các dấu mã u_j khác.

Giải mã ngưỡng (...)

c. Hệ tổng kiểm tra trực giao

Để dễ giải cho u_i hiển nhiên rằng ta cần xây dựng một hệ tổng kiểm tra chứa nhiều thông tin nhất về u_i . Trên cơ sở đó ta đưa ra khái niệm hệ tổng kiểm tra trực giao sau:

Định nghĩa: Hệ J tổng kiểm tra được gọi là trực giao với dấu mã u_i nếu:

- Mỗi tổng kiểm tra trong hệ đều chứa u_i .
- Dấu mã u_j ($j \neq i$) chỉ nằm tối đa trong một tổng kiểm tra

Giải mã ngưỡng (...)

d. Thủ tục giải mã ngưỡng dựa trên hệ tổng kiểm tra trực giao

B1: Tính H

B2: Tính syndrom theo công thức $S(u)=u \cdot H^T$

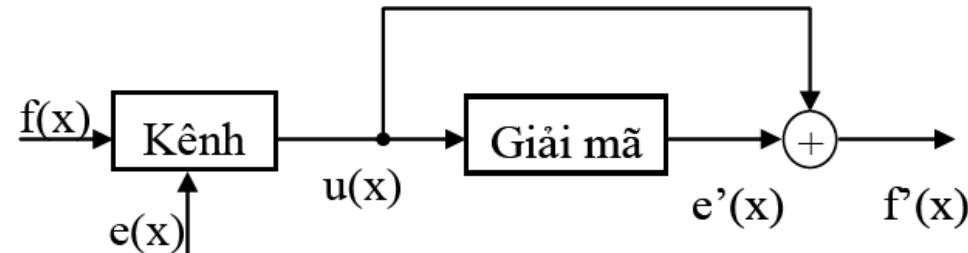
B3: Lập hệ J tổng kiểm tra trực giao với dấu mã u_i , kiểm tra $J=d_0-1$

B4: Lập sơ đồ bộ giải mã theo đa số

B5: Lập bảng hoạt động giải mã vector u thành từ mã f

B6: Kiểm tra f có phải là từ mã hợp lệ ?

Ví dụ 1: Xét mã $(7, 3, 4)$ có $g(x) = 1 + x + x^2 + x^4$.



$$h(X) = \frac{x^7 + 1}{g(X)} = x^3 + x + 1, \quad h^*(X) = 1 + x^2 + x^3$$

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

Từ mã nhận được: $u = (u_0 u_1 u_2 u_3 u_4 u_5 u_6)$

Tính syndrom: $uH^T = S(u) = (s_0 s_1 s_2 s_3)$

$$= (u_0 u_1 \dots u_6) \begin{pmatrix} 1000 \\ 0100 \\ 1010 \\ 1101 \\ 0110 \\ 0011 \\ 0001 \end{pmatrix}$$


Hệ 4 tổng kiểm tra:

$$s_0 = u_0 + u_2 + u_3$$

$$s_1 = u_1 + u_3 + u_4$$

$$s_2 = u_2 + u_4 + u_5$$

$$s_3 = u_3 + u_5 + u_6$$

Hệ tổng kiểm tra trực giao với dấu mă u_3

$$s_0 = u_0 + u_2 + u_3$$

$$s_1 = u_1 + u_3 + u_4$$

$$s_3 = u_3 + u_5 + u_6$$

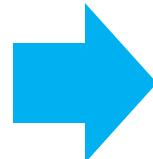
Do $J = d_0 - 1$, nên ta có thể sửa được sai bởi phương pháp giải mă đa số.

Do tính chất dịch vòng, nên để thuận tiện cho dãy bít ra theo trật tự, ta có thể dịch vòng hệ tổng kiểm tra trên đi 3 vị trí sang phải). Hệ tổng kiểm tra trực giao với dấu mã u_6

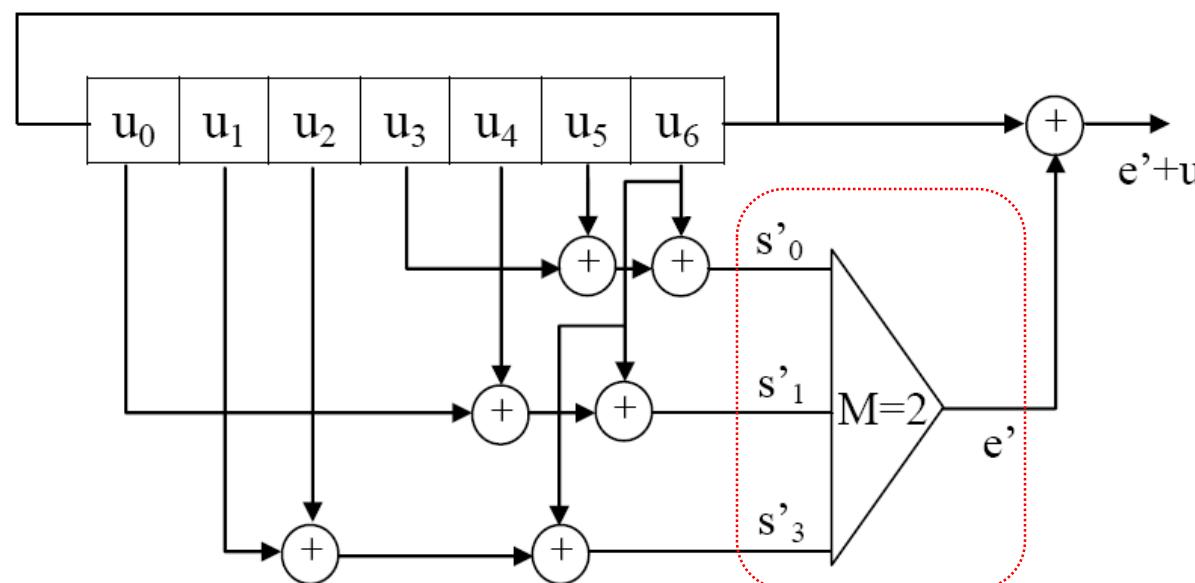
$$s_0 = u_0 + u_2 + u_3$$

$$s_1 = u_1 + u_3 + u_4$$

$$s_3 = u_3 + u_5 + u_6$$



$$\left\{ \begin{array}{l} s'_0 = u_6 + u_3 + u_5 \\ s'_1 = u_6 + u_0 + u_4 \\ s'_3 = u_6 + u_1 + u_2 \end{array} \right.$$



Quá trình giải mã từ mā u nhận được có dạng: 0 0 1 1 1 1 1

(Hay $u(x) = x^6 + x^5 + x^4 + x^3 + x^2$)

Nhịp	Trạng thái các ô nhớ							s'_0	s'_1	s'_2	e'	Ra	Dấu mā ra
	u_0	u_1	u_2	u_3	u_4	u_5	u_6						
7	0	0	1	1	1	1	1						
8	1	0	0	1	1	1	1	1	0	0	0	1	f'6
9	1	1	0	0	1	1	1	1	1	1	1	0	f'5
10	1	1	1	0	0	1	1	0	1	0	0	1	f'4
11	1	1	1	1	0	0	1	0	0	1	0	1	f'3
12	1	1	1	1	1	0	0	0	0	1	0	1	f'2
13	0	1	1	1	1	1	0	1	0	0	0	0	f'1
14	0	0	1	1	1	1	1	0	1	0	0	0	f'0

$$u = 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1$$

$$e = 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0$$

$$0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1$$

Sai ở vị trí x^5 đã được sửa

Từ mā đã giải mā $\hat{f}(x) = x^6 + x^4 + x^3 + x^2$

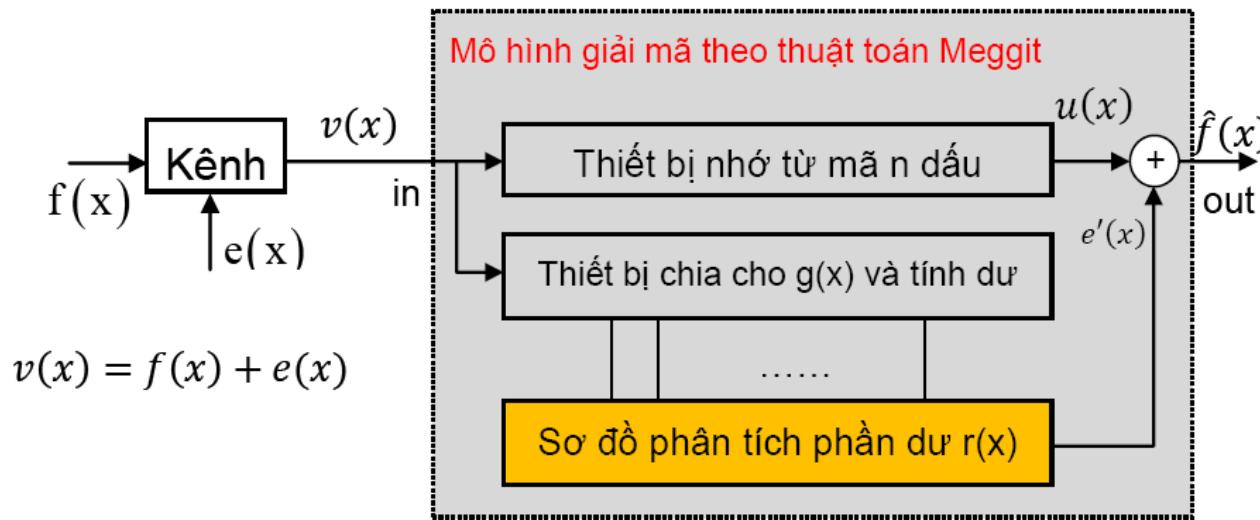
-Kiểm tra lại:

$$\begin{array}{r}
 x^6 + x^4 + x^3 + x^2 \\
 - x^6 + x^4 + x^3 + x^2 \\
 \hline
 0
 \end{array}
 \left| \begin{array}{r}
 x^4 + x^2 + x + 1 \\
 \hline
 x^2
 \end{array} \right.$$

Lưu ý rằng $d_0=4$, nên chỉ sửa được một lỗi.

Giải mã theo thuật toán Meggitt

Giả sử $f(x)$ là một từ mã của một bộ mã cyclic $V_{-}(n,k)$ có đa thức sinh $g(x)$



Do $f(x):g(x)$. khi đó phép chia: $\frac{v(x)}{g(x)} = \frac{f(x)}{g(x)} + \frac{e(x)}{g(x)}$ Phần dư $r(x)$

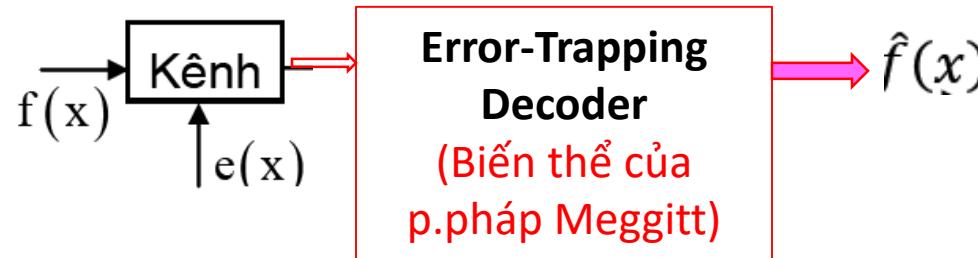
Chú ý: do $g(x)$ có bậc r , nên $r(x)$ có bậc $\leq r-1$

Phần dư $r(x)$ đặc trưng cho $e(x)$

Bằng cách phân tích $r(x)$ ta có thể tìm được $e(x)$. Sơ đồ phân tích $r(x)$ là một sơ đồ logic tổng hợp, đây là một thành phần quan trọng trong sơ đồ giải mã theo thuật toán Meggit.

Error trapping decoding

- Phương pháp Meggitt thực tế có mạch giải mã khá phức tạp. Nếu giới hạn lại một số điều kiện thì có thể cho ra một biến thể giải mã đơn giản.



Nếu có thể dịch vòng (bẫy) lỗi về chỉ nằm trong vùng $n-k$ dấu mã đầu tiên, khi đó có thể xác định $e(x)$.

- Dấu hiệu lỗi bị bẫy thành công:** là ngay khi $w(r(x)) \leq t$.

Thuật toán chia dịch vòng (Error trapping decoding)

Thuật toán (dịch phải)

VÀO: - Từ mã nhận được $v(x)$
- Mã $V_{-}(n,k)$ có $g(x)$, có d_0 .

RA: - Từ mã $\hat{f}(x)$

For $i := 0$ to $(n-1)$ do

(1) Chia $v(x).x^i$ cho $g(x)$ để tìm phần dư $r_i(x)$.

(2) Tính $w(r_i(x))$.

- Nếu $w(r_i(x)) \leq t = \left\lceil \frac{d_0 - 1}{2} \right\rceil$ thì $\hat{f}(x) = \frac{v(x).x^i + r_i(x)}{x^i}$ và stop.

- Nếu $w(r_i(x)) > t \Rightarrow i := i + 1$. Nếu $i + 1 = n$ thì thông báo

“không sửa được sai (Số sai vượt quá khả năng
sửa sai của bộ mã)” và stop.

Note: Có thể giải theo cách dịch trái (chia $v(x)$ cho x^i).

Giải mã theo thuật toán chia dịch vòng (...)

Thí dụ: mã cyclic (7, 3, 4) với đa thức sinh $g(x) = 1 + x + x^2 + x^4$

Giả sử từ mã nhận được $v(x) = x + x^2 + x^3 + x^5 + x^6 \leftrightarrow 0111011$

Ta sử dụng thuật toán chia dịch vòng để tìm lại từ mã đã phát:

i = 0

(1) Chia $v(x) \cdot x^0$ cho $g(x)$ để tìm phần dư $r_0(x)$.

$$\begin{array}{r} x^6 + x^5 \quad + x^3 + x^2 + x \\ x^6 \quad + x^4 + x^3 + x^2 \\ \hline x^5 + x^4 \quad + x \\ x^5 \quad + x^3 + x^2 + x \\ \hline x^4 + x^3 + x^2 \\ x^4 \quad + x^2 + x + 1 \\ \hline r_0(x) = x^3 + x + 1 \end{array}$$

(2) $w(r_0(x)) = 3 > \left[\frac{4-1}{2} \right] = 1$ Không thỏa mãn điều kiện

i = 1:

(1) Chia $x \cdot v(x)$ cho $g(x)$ để tìm phần dư $r_1(x)$.

$$\begin{array}{r} x^6 + x^4 + x^3 + x^2 + 1 \\ \hline x^6 + x^4 + x^3 + x^2 \\ \hline r_1(x) = 1 \end{array}$$

(2) $w(r_1(x)) = 1 = t$

Từ mã ra: $\hat{f}(X) = \frac{x \cdot v(x) + r_1(x)}{x} = x^5 + x^3 + x^2 + x$

Vậy sai ở vị trí x^6 đã được sửa $v = 0111011 \rightarrow f = 0111010$

Giải theo cách dịch trái cũng sẽ cho cùng kết quả.

Tài liệu tham khảo

- ✓ John Proakis & Masoud Salehi, **Digital Communication**, 2007
- ✓ Shu Lin, **Error Control Coding-Fundamentals and Applications**, Prentice Hall, 2004
- ✓ Simon Haykin, **Communication Systems**, 4rd edition, John Wiley & Sons, 2001.



Lý thuyết thông tin

Phần 2

Lý thuyết thông tin thống kê

- Đo lường thông tin
- Nguồn & kênh rời rạc
- Nguồn & kênh liên tục



dinhptit@gmail.com



A. Đo lường thông tin

Khái niệm

- Để đánh giá tin: (1) Độ bất định (uncertainty), (2) Hàm ý của tin.
- Đối với hệ thống truyền tin, chỉ có độ bất định của tin là có ảnh hưởng.
 - Độ bất định của tin quyết định tới tần suất chiếm dụng hệ thống. Độ bất định của tin càng cao thì sự xuất hiện của nó càng hiếm. Vì vậy, hệ thống truyền tin muốn hiệu quả cần xử lý với các tin khác nhau nếu độ bất định của chúng khác nhau.
 - Việc giảm độ bất định của một tin giữa trước khi nhận tin (độ bất định tiên nghiệm) và sau khi nhận tin (độ bất định hậu nghiệm) chính là **lượng tin** nhận được.



Nguyên tắc đo lường thông tin

- Độ lớn của tin là độ bất định của tin
- Phép đo phải đảm bảo tính tuyến tính

Cụ thể: Xét nguồn tin $A = \{a_1, a_2, \dots, a_s\}$ với $p(a_i)$, $i = 1, \dots, S$; $\sum p(a_i) = 1$.

- **Độ bất định của một dấu của nguồn (lượng tin riêng):**

$$I(a_i) = \log \frac{1}{p(a_i)} = -\log p(a_i)$$

- **Đơn vị đo**

- Nếu là cơ số e, thì $I(a_i) = -\ln[p(a_i)]$ [đơn vị tự nhiên, natural, nat]
- Nếu là cơ số 2, thì $I(a_i) = -\log_2[p(a_i)]$ [đơn vị nhị phân, bit]
- Nếu là cơ số 10, thì $I(a_i) = -\lg[p(a_i)]$ [đơn vị thập phân, hartley]

- **Chú ý:** 1 nat = 1,443 bit. 1 hart = 3,322 bit



Entropy của nguồn rời rạc không nhớ (DMS)

Xét nguồn tin $A = \{a_1, a_2, \dots, a_s\}$ với $p(a_i)$, $i = 1, \dots, S$; $\sum p(a_i) = 1$.

- **Độ bất định trung bình trong mỗi dấu của nguồn:** là trung bình thống kê (kỳ vọng, expected value) của lượng tin riêng của mỗi dấu

$$I(A) = \sum_{i=1}^S p(a_i)I(a_i) = -\sum_{i=1}^S p(a_i)\log p(a_i) \equiv H(A)$$

$H(A)$: Entropy của A (bit/symbol)

- **Note:** $H(A) \equiv H_1(A)$ Entropy tiên nghiệm; Entropy ko điều kiện.



Tính chất của entropy của nguồn rời rạc

- Tính chất 1:

$$H_1(A) \geq 0$$

Dấu “=“ chỉ xảy ra khi tồn tại một symbol có xs bằng 1.

- Tính chất 2: Một nguồn A rời rạc gồm s dấu thì:

$$H_1(A) \leq \log s \equiv H_0(A)$$

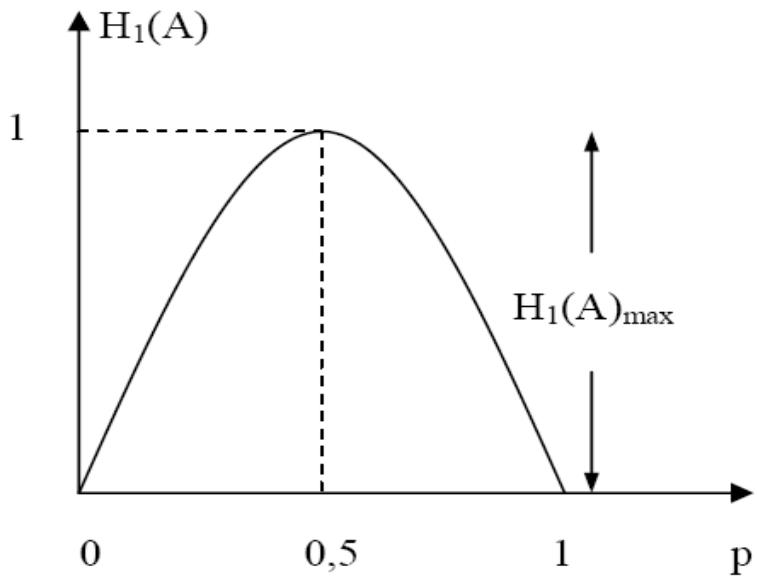
Dấu “=“ chỉ xảy ra khi các symbol của nguồn đồng xác suất.
Tức entropy đạt max, ký hiệu $H_0(A)$.

Khảo sát entropy của nguồn nhị phân

- Nguồn rời rạc nhị phân là nguồn chỉ có hai dấu:

$$A = \begin{pmatrix} a_1 & a_2 \\ p & 1-p \end{pmatrix}$$

$$H_1(A) = -\sum_{i=1}^2 p(a_i) \log p(a_i) = -p \log p - (1-p) \log(1-p) = f(p)$$





Thông tin tương hỗ

- **Lượng tin tương hỗ** giữa x_k và y_l (**Lượng tin chéo**):

$$I(x_k; y_l) = \log \frac{p(x_k | y_l)}{p(x_k)}$$

- **Tính chất:**

- $I(x_k; y_l) = I(x_k) - I(x_k | y_l)$

Lượng tin nhận được = Độ bất định tiên nghiệm – độ bất định hậu nghiệm

- $-\infty \leq I(x_k; y_l) \leq I(x_k), I(y_l)$

- $I(x_k; y_l) = I(y_l; x_k) = \log \frac{p(y_l | x_k)}{p(y_l)}$

□ X và Y độc lập (kênh vô dụng, kênh đứt):

- Khi đó việc thu được y_l không mang thông tin gì về các x_k (tức chúng là các biến cố độc lập). Dẫn đến độ bất định hậu nghiệm ko giảm:

$$p(x_k | y_l) = p(x_k) \quad \forall k$$

→ Lượng tin truyền qua kênh: $I(x_k; y_l) = 0$

□ Truyền tin không nhiễu (kênh lý tưởng):

Nếu y_l là phiên bản thu đúng của x_k thì phát x_k chắc chắn nhận được y_l (ánh xạ 1:1):

$$p(x_k | y_l) = 1$$

→ $I(x_k / y_l) = 0$: lượng thông tin tổn hao trong kênh bằng 0.

- Lượng tin truyền qua kênh max đúng bằng lượng tin riêng tiên nghiệm của x_k (self-information):

$$I(x_k; y_l) = I(x_k; x_k) = I(x_k)$$

- Trường biến cố đồng thời (A,B) có thể biểu diễn dưới hai dạng:

- Dạng bảng

	a_1	a_2	a_s	
b_1	$p(a_1, b_1)$	$p(a_2, b_1)$				$p(a_s, b_1)$	
b_2	$p(a_1, b_2)$	$p(a_2, b_2)$				$p(a_s, b_{12})$	
...							
b_t	$p(a_1, b_t)$	$p(a_2, b_t)$				$p(a_s, b_t)$	

- Dạng trường

$$(A, B) = \begin{pmatrix} a_1, b_1 & a_1, b_2 & \dots & a_i, b_j & \dots & a_s, b_t \\ p(a_1, b_1) & p(a_1, b_2) & \dots & p(a_i, b_j) & \dots & p(a_s, b_t) \end{pmatrix}$$



Entropie của trường biến cố đồng thời

$$H(A, B) \stackrel{\Delta}{=} E[\log \frac{1}{p(a_i, b_j)}] = -\sum_{i=1}^s \sum_{j=1}^t p(a_i, b_j) \cdot \log p(a_i, b_j)$$

- **Tính chất:** $H(A, B) \leq H(A) + H(B)$

- Trường hợp riêng: Nếu A độc lập với B, thì:

$$p(a_i, b_j) = p(a_i)p(b_j) \quad \Longrightarrow \quad H(A, B) = H(A) + H(B)$$

- Mở rộng: Nếu n trường độc lập thống kê với nhau thì:

$$H(X_1, X_2, \dots, X_n) = \sum_{k=1}^n H(X_k)$$



Entropy có điều kiện (conditional entropy)

- Entropie của A khi đã rõ một dấu b_j của B là lượng tin trung bình hậu nghiệm của A khi đã rõ một dấu b_j

$$H(A|b_j) \stackrel{\Delta}{=} E[I(a_i|b_j)]_{a_i \in A} = \sum_{i=1}^s p(a_i|b_j) I(a_i|b_j) = -\sum_{i=1}^s p(a_i|b_j) \log p(a_i|b_j)$$

(Partial conditional entropy)

- Tương tự:

$$H(B|a_i) = -\sum_{j=1}^t p(b_j|a_i) \log p(b_j|a_i)$$

Entropy có điều kiện (tt)

- **Entropie của trường sự kiện A khi đã rõ trường sự kiện B** được xác định bởi kỳ vọng của các $H(A|b_j)$.

$$\begin{aligned} H(A|B) &\stackrel{\Delta}{=} E[H(A|b_j)]_{b_j \in B} = \sum_{j=1}^t p(b_j)H(A|b_j) \\ &= -\sum_{i=1}^s \sum_{j=1}^t p(a_i, b_j) \log p(a_i|b_j) = -\sum_{i=1}^s \sum_{j=1}^t p(b_j)p(a_i|b_j) \log p(a_i|b_j) \end{aligned}$$

- Ý nghĩa:
 - $H(A|B)$ là lượng thông tin tổn hao trung bình của mỗi dấu ở đầu phát khi đầu thu đã thu được một dấu bất kỳ (Hay lượng tin chưa biết về A khi nhận được B) do nhiễu phá hủy.



Entropy có điều kiện (tt)

- **Tương tự:**

$$\begin{aligned} H(B|A) &\stackrel{\Delta}{=} E[H(B|a_i)]_{a_i \in A} = \sum_{i=1}^s p(a_i)H(B|a_i) \\ &= -\sum_{i=1}^s \sum_{j=1}^t p(b_j, a_i) \log p(b_j|a_i) = -\sum_{i=1}^s \sum_{j=1}^t p(a_i)p(b_j|a_i) \log p(b_j|a_i) \end{aligned}$$

Ý nghĩa: $H(B/A)$ là lượng thông tin riêng trung bình chứa trong mỗi dấu ở đầu thu khi đầu phát đã phát đi một dấu bất kỳ (Lượng tin chưa biết về B khi A đã phát đi).

- **Chú ý:** $H(A/B) \neq H(B/A)$



Mối quan hệ của các Entropy

- **Tính chất 1:** Chain rule (luật xâu chuỗi)

$$H(B, A) = H(A, B) = H(A) + H(B / A) = H(B) + H(A / B)$$

- **Tính chất 2:**

$$0 \leq H(A|B) \leq H(A)$$

$$0 \leq H(B|A) \leq H(B)$$

- $H(A/B)=0, H(B/A)=0$: khi A và B là đồng nhất (kênh hoàn hảo, không nhiễu).
- $H(A/B) = H(A), H(B/A) = H(B)$: khi A và B là độc lập (kênh bị đứt).
- **Tính chất 3:** Cho DMS $X=\{x_k\}$, $k=1, N$. Một hàm toán học $f(X)$ mô tả mối quan hệ xác định của f và X . Khi đó:

$$H(f(X)|X) = 0$$

$$H(X|f(X)) \geq 0; \quad H(X) \geq H(f(X))$$

- Dấu “=” xảy ra chỉ khi $f(X)$ là quan hệ ánh xạ 1-1.



Lượng thông tin tương hỗ trung bình

- Lượng tin tương hỗ trung bình về tập phát A do tập thu B mang lại.

$$I(A;B) \stackrel{\Delta}{=} E[I(a_i; b_j)] = \sum_{a_i \in A} \sum_{b_j \in B} p(a_i, b_j) \log \frac{p(a_i | b_j)}{p(a_i)}$$

- Ý nghĩa:

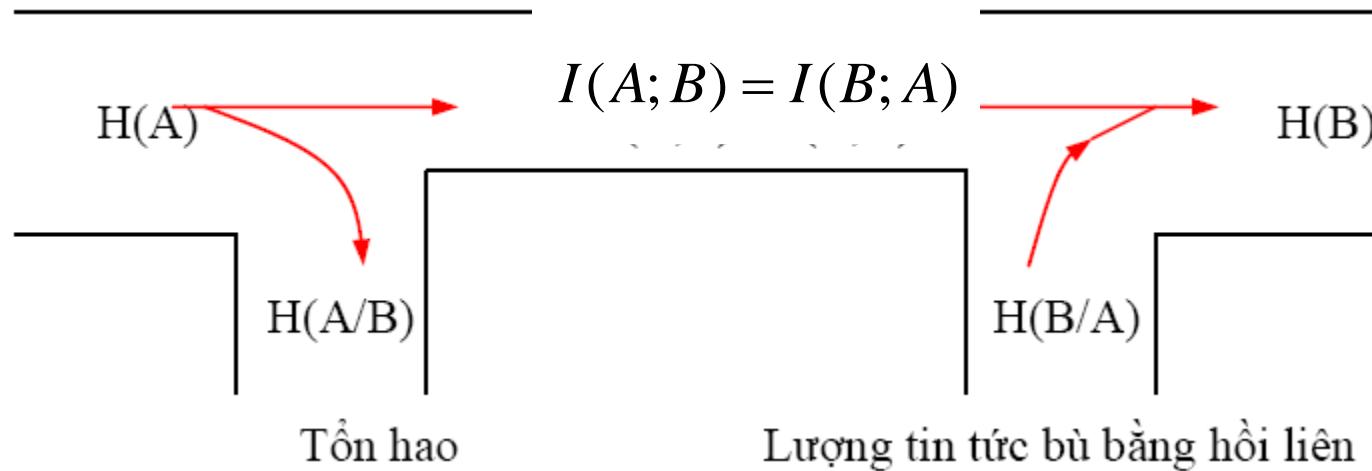
- $I(A;B)$: Đo lượng tin thu được về một biến ngẫu nhiên A thông qua giá trị của một biến ngẫu nhiên B.
- Nó là lượng thông tin trung bình được truyền qua kênh có nhiễu (lượng tin không bị nhiễu phá hủy)

- Tính chất 1:** $I(A; B) \geq 0$ $I(A; B) = 0$ khi A độc lập với B, kênh bị đứt.
- Tính chất 2:** $I(A; A) = H(A)$
- Tính chất 3:** $I(A; B) = I(B; A)$
- Tính chất 4:** $I(A; B) \leq H(A) \Rightarrow I(A; B) = H(A) = H(B)$ khi kênh không nhiễu.
- Tính chất 5:**

$$\begin{aligned}I(A; B) &= H(A) - H(A|B) = H(B) - H(B|A) = H(A) + H(B) - H(A, B) \\&\Rightarrow H(A, B) = H(B) + H(A|B) = H(A) + H(B|A)\end{aligned}$$

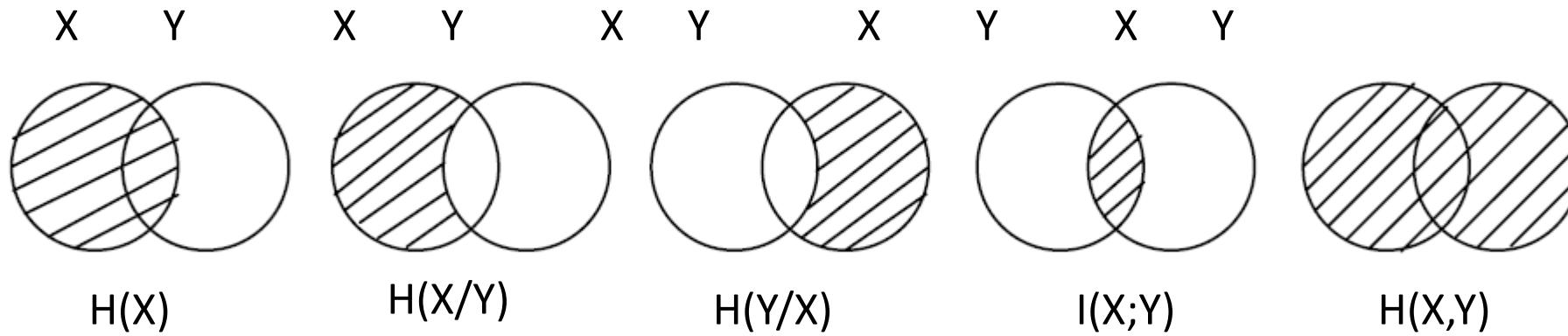
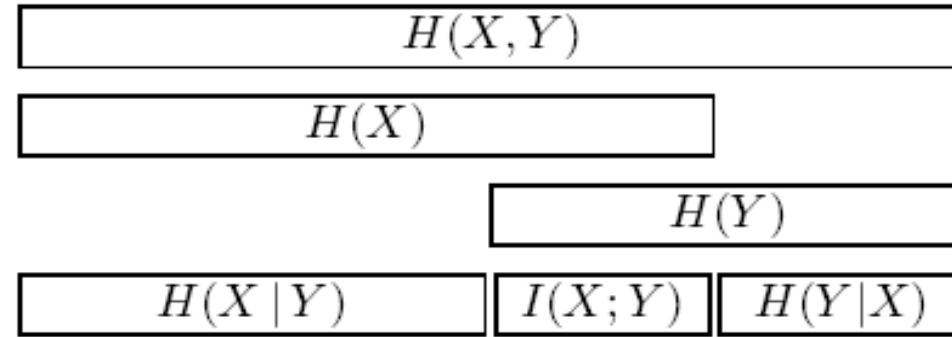


Mô hình kênh





Lược đồ Venn





B. Các tham số đặc trưng cho Nguồn và kênh ròi rạc

dinhptit@gmail.com

- **Tốc độ baud của nguồn rời rạc (tốc độ truyền tín hiệu):** số symbol nguồn phát ra trong một đơn vị thời gian. (Một symbol có thể là biểu diễn của mức biên độ, tần số hoặc pha... của tín hiệu).

$$v_n \stackrel{\Delta}{=} \frac{1}{T_n} \quad [Baud]$$

T_n : Thời hạn trung bình của mỗi dấu của nguồn phát.

- **Tốc độ bit /Khả năng phát của nguồn rời rạc (tốc độ truyền thông tin):** Là lượng tin trung bình do nguồn phát ra trong một đơn vị thời gian.

$$R_n \stackrel{\Delta}{=} v_n H(A) = \frac{H(A)}{T_n} \quad [bps]$$

R_n đạt max khi $H(A)$ max = $H_0(A) = \log S$

- **Độ thừa (redundancy) của nguồn rời rạc:** $D = 1 - \mu$

$$\mu = \frac{H(A)}{H_0(A)} \quad \text{he so nen tin}$$

- Tập các xác suất chuyển: $p(b_j / a_i)$
- Khả năng thông qua của kênh **C'** (hoặc dung lượng kênh **C**).
- Biểu diễn kênh rời rạc
 - Giản đồ kênh
 - Hoặc ma trận chuyển: $P = [p(b_j | a_i)] = \begin{bmatrix} p(b_1 | a_1) & \dots & \dots & p(b_t | a_1) \\ \dots & \dots & \dots & \dots \\ p(b_1 | a_s) & \dots & \dots & p(b_t | a_s) \end{bmatrix}$
 - Nếu một kênh có $p(b_j | a_i) \neq 0$ ($\forall i, j$): gọi là kênh đồng nhất (hay bất biến);
Ngược lại kênh không đồng nhất;
 - Nếu một kênh có $p(b_j | a_i) \neq 0$ vào dấu đã phát trước nó: gọi là kênh không nhớ (Discrete memoryless channels); ngược lại kênh có nhớ (Discrete channels with memory)



Tốc độ bit của kênh

•**Định nghĩa:** Tốc độ bit của kênh là lượng thông tin trung bình truyền qua kênh trong một đơn vị thời gian:

$$R_k = v_k I(A; B) \quad [\text{bps}]$$

v_K : Tốc độ baud của kênh (dấu/s). Biểu thị số dấu được truyền qua kênh trong một đơn vị thời gian.

$$v_K = \frac{1}{T_K}$$

T_K : thời gian trung bình để truyền một dấu qua kênh

Nếu kênh giãn tin: $T_K > T_n$

Nếu kênh nén tin: $T_K < T_n$

Thông thường: $T_K = T_n$

- **Khả năng thông qua của kênh rời rạc:** là giá trị cực đại của R_k (ứng với một phân bố tối ưu của các xác suất tiên nghiệm $p(a_i)$, $\forall a_i \in A$).

$$C' = \max_A R_k = v_k \max_A I(A; B) = v_k C \quad [\text{bit/s}]$$

Với: $C = \max_A I(A; B) \quad [\text{bit/symbol}]$

C: Dung lượng kênh : Channel capacity (khả năng thông qua của kênh với mỗi dấu).

→ C' đánh giá năng lực tải tin tối đa của một kênh.

- **Tính chất:**

$$0 \leq C \leq \log S$$

$C = 0$ khi A và B độc lập (kênh đứt, Useless channel)



Khả năng thông qua của kênh rời rạc (tt)

- **Độ thừa của kênh :** $D_k = 1 - \eta_k$
 $\eta_k = \frac{R_k}{C}$ Hiệu suất sử dụng kênh
 - → Hiệu suất sử dụng kênh phụ thuộc tính chất thống kê của nguồn.
 - Thông thường độ thừa của kênh được lợi dụng để xây dựng mã chống nhiễu kênh.
 - **Định lý mã hóa thứ hai của Shannon đối với kênh rời rạc :**
 - Nếu khả năng phát R_n của nguồn bé hơn khả năng thông qua của kênh: ($R_n < C'$) thì tồn tại một phép mã hoá và giải mã sao cho việc truyền tin có xác suất lỗi bé tuỳ ý khi độ dài từ mã đủ lớn. Nếu $R_n > C'$ thì không tồn tại phép mã hoá và giải mã như vậy.
- Nhận xét:** Định lý chỉ ra sự tồn tại, không chỉ ra cách thiết lập mã cụ thể nào.



Một số loại kênh rác đặc biệt

- Kênh đối xứng (symmetric channel):
- Lossless channel (Kênh không tổn hao):
- Deterministic channel (Kênh đơn định):
- Noiseless channel: Kênh không nhiễu (Kênh hoàn hảo)
- Useless channel: Kênh vô dụng (kênh đứt)



C. Nguồn & kênh liên tục không nhớ

dinhptit@gmail.com



Nguồn liên tục

- **Nguồn liên tục:**

Lực lượng của nguồn là vô hạn

- **Mô hình nguồn liên tục S:**

- Nguồn liên tục S là một biến ngẫu nhiên, phát ra những tin s có thể nhận các giá trị liên tục trong khoảng $s_{\min} \div s_{\max}$ với hàm mật độ phân bố xác suất *probability density function* $W_1(s)$.

- **Entropie (differential entropy) của nguồn S:**

$$h(S) \stackrel{\Delta}{=} \int_{-\infty}^{+\infty} W_1(s) \log \frac{1}{W_1(s)} ds$$

Chú ý:

- ✓ $h(S)$ có thể nhận các giá trị dương, âm (hữu hạn).
- ✓ $h(S)$ còn gọi là entropy tương đối

Entropy của nguồn ngẫu nhiên X có phân bố chuẩn

- Xét nguồn ngẫu nhiên $X=\{x(t)\}$, có phân bố chuẩn (Gaussian distribution), tức có hàm mật độ phân bố xác suất:

$$W_1(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(x-\mu)^2}{2\sigma^2}\right\}$$

$\mu = E(X)$ kỳ vọng của X.

$E(X^2) = \sigma^2$ phuơng sai của X (Công suất của X)

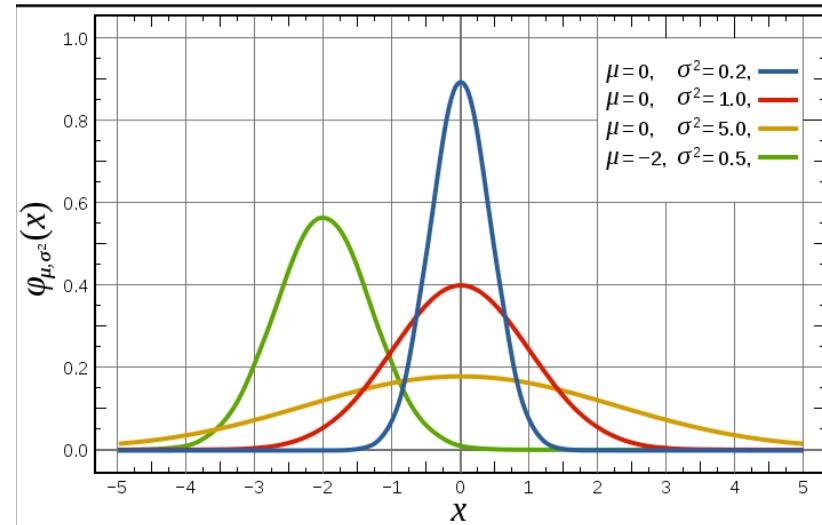
→ Entropie vi phân của X: $h(X) = \frac{1}{2} \log 2\pi e \sigma^2 = \log \sqrt{2\pi e \sigma^2}$ bit

- Định lý:** Let X be a random variable with mean μ and variance σ^2 .

$$\rightarrow h(X) \leq \log \sqrt{2\pi e \sigma^2}$$

“=“ only when X has a gaussian distribution

$$X \approx N(\mu, \sigma^2)$$



Entropy của nguồn ngẫu nhiên có phân bố đều

- Uniform distribution: $X \sim U(a, b)$

$$W(X) = \begin{cases} \frac{1}{b-a} & \text{for } x \in (a, b) \\ 0 & \text{elsewhere} \end{cases}$$



$$h(X) = - \int_a^b \frac{1}{b-a} \log \frac{1}{b-a} dx = \log(b-a)$$

– Note that $h(X) < 0$ if $(b-a) < 1$

- Định lý:**

Xét X trong một khoảng hữu hạn (a, b) , với: $\int_a^b W_1(x) dx = 1$

Thì: $h(X) \leq \log(b-a)$

“=” chỉ xảy ra khi X có phân bố đều.

- For the exponential distribution:

$$W(x) = \begin{cases} \lambda e^{-\lambda x} & \text{for } x \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

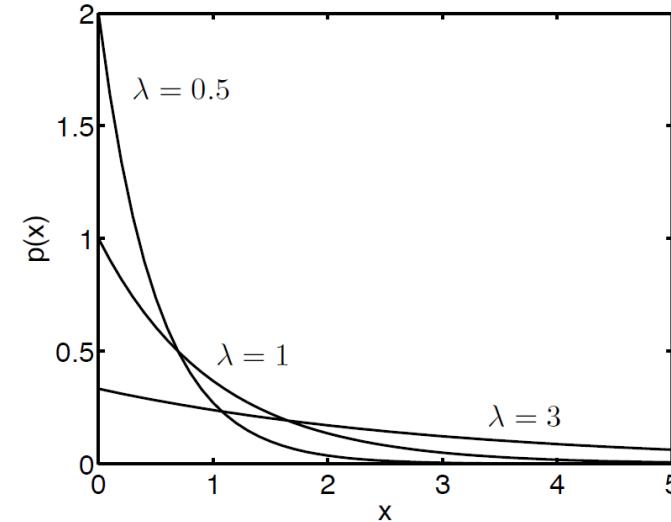
the differential entropy for this exponential distribution:

$$h(X) = \log \frac{e}{\lambda}$$

- Định lý:**

Trong số tất cả các đại lượng ngẫu nhiên X liên tục dương có cùng kỳ vọng m:

$$\int_0^{\infty} W_1(x) dx = 1 \quad \text{và} \quad \int_0^{\infty} x W_1(x) dx = m$$



Đại lượng ngẫu nhiên phân bố luật hàm mũ có entropy lớn nhất.



Entropy của trường sự kiện đồng thời

- Entropy vi phân của trường biến cố liên tục đồng thời của S và U.

$$h(S, U) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(s, u) \log[W(s, u)] ds du$$

Về mặt hình thức, so với nguồn rời rạc, $h(S, U)$ đóng vai trò của $H(A, B)$

- Tính chất:

$$h(U, S) = h(S, U) = h(S) + h(U|S) = h(U) + h(S|U)$$

$$h(U|S) \leq h(U); \quad h(S|U) \leq h(S) \quad \text{Đáu = khi } S, U \text{ độc lập.}$$



Entropy có điều kiện

- Entropie vi phân có điều kiện của nguồn S khi đã biết nguồn U.

$$h(S|U) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(s,u) \log[W(s|u)] ds du$$

Về mặt hình thức, so với nguồn rời rạc, $h(S|U)$ đóng vai trò của $H(A|B)$.



Lượng tin tương hỗ

- Lượng tin tương hỗ giữa các nguồn liên tục S và U:

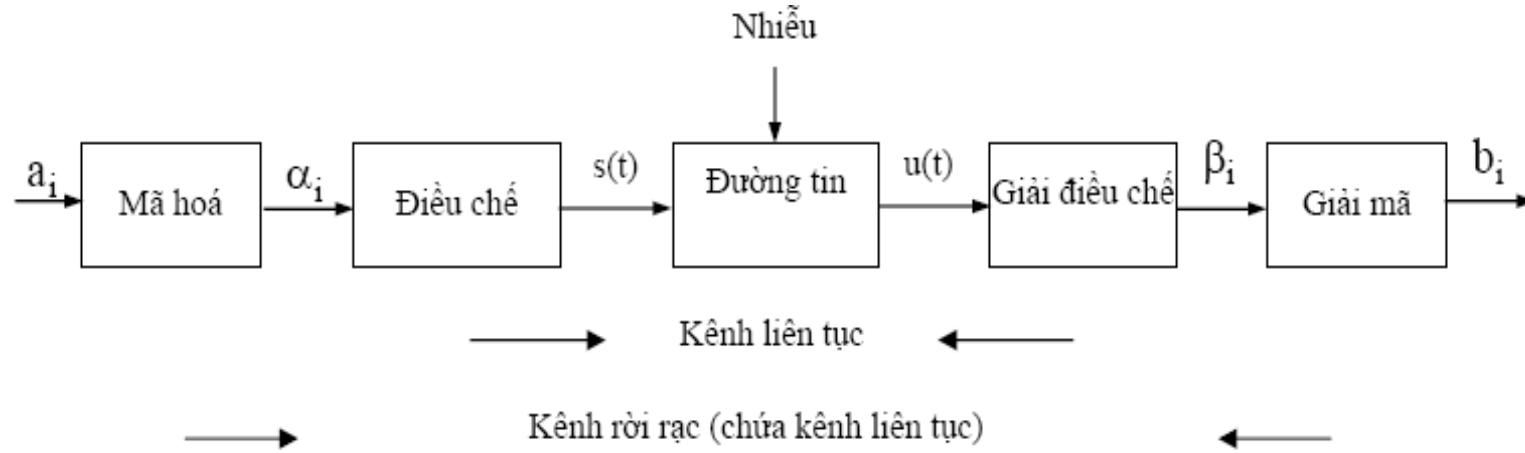
$$I(S;U) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(s,u) \log \left[\frac{W(s,u)}{W(s)W(u)} \right] dsdu$$

- Một số tính chất

$$I(S;U) = I(U;S) = h(U) - h(U|S) = h(S) - h(S|U)$$

$I(S;U) \geq 0$ Dấu = là khi S độc lập với U

Nếu kênh không nhiễu thì $I(S;U) \rightarrow$ vô cùng.



- Các đặc trưng của kênh liên tục:**

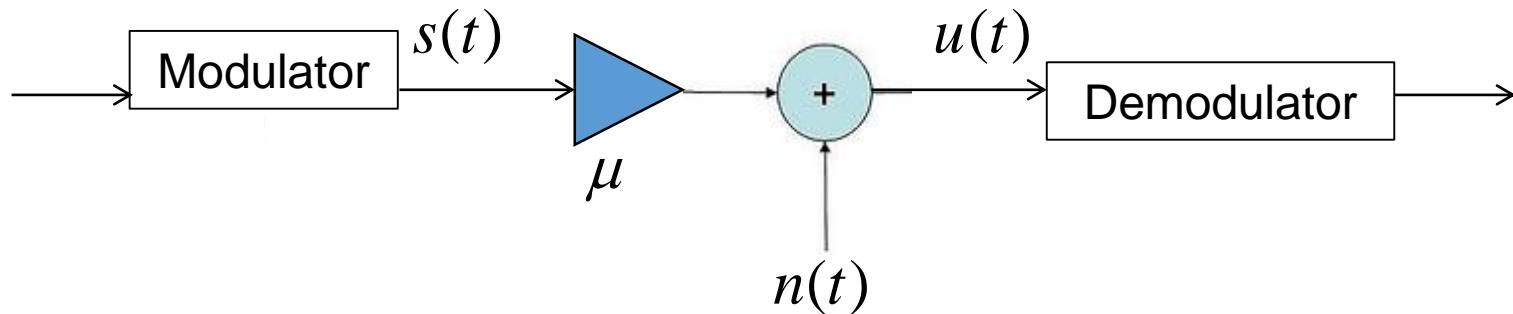
- Trường dấu lối vào (sau bộ điều chế): $S = \{s(t), w_1(s)\}$
- Trường dấu lối ra (trước bộ giải điều chế): $U = \{u(t), w_1(u)\}$
- Hàm mật độ phân bố để xuất hiện $U_j(t)$ khi đã phát $s_i(t)$: $W(U_j(t)/s_i(t))$
- Khả năng thông qua của kênh.

- Tính chất kênh liên tục trong kênh rời rạc:**

Khả năng thông qua của kênh liên tục không nhỏ hơn khả năng thông qua của kênh rời rạc chứa nó:

$$C'_{lt} \geq C'_{rr \text{ chua kenh lien tuc}}$$

$$u(t) = \mu \cdot s(t) + n(t) \quad \mu = \text{const}, (\notin t).$$



AWGN Channel

n(t) AWGN- Additive white Gaussian Noise: nhiễu cộng, mật độ phổ công suất không đổi rộng vô hạn (tập âm trắng), biên độ ngẫu nhiên có phân bố chuẩn.



Khả năng thông qua của kênh AWGN

Là giá trị cực đại của lượng tin truyền qua kênh AWGN trong một đơn vị thời gian, lấy theo mọi khả năng có thể có của phân bố xác suất nguồn phát, trong đó có tính đến giới hạn công suất phát và công suất tạp nhiễu.

$$C' = v_k \cdot \max I(U; S)$$

v_k Tốc độ truyền tin của kênh

- Dung lượng kênh AWGN: $C = \max I(U; S)$

Khả năng thông qua của kênh AWGN (tt)

- Nếu tín hiệu là hàm liên tục theo thời gian liên tục, khả năng thông qua của kênh AWGN với băng tần hữu hạn F và giới hạn công suất trung bình tín hiệu hữu ích nhận được $P_{\mu s}$, có nhiễu với mật độ phô công suất hai phía $N_0/2$ được xác định bởi:

$$C' = F \log \left(1 + \frac{\mu^2 P_s}{N_0 F} \right) = F \cdot \log(1 + \text{SNR}) \quad \text{bps}$$

- F: BW của kênh
 - P_n : là công suất trung bình của nhiễu trong giải F.
 - $P_n = N_0 \cdot F$: với trường hợp nhiễu tạp âm trắng.
 - N_0 : Mật độ phô công suất của nhiễu cộng.
- Nếu $F \rightarrow \infty$, tức là khi giải thông của kênh là vô hạn:

$$C_\infty = \lim_{F \rightarrow \infty} C' = (\log_2 e) \left(\frac{\mu^2 P_s}{N_0} \right) = 1,443 \cdot \frac{P_{\mu s}}{N_0} \quad \text{bps}$$



Định lý mã hoá thứ hai của Shannon đối với kênh liên tục

Các nguồn tin rác có thể mã hoá và truyền theo kênh liên tục với xác suất sai bé tuỳ ý khi giải mã các tín hiệu nhận được nếu khả năng phát R_n của nguồn nhỏ hơn khả năng thông qua của kênh.

Ngược lại, không thể thực hiện được mã hoá và giải mã với xác suất sai bé tuỳ ý được.



Tài liệu tham khảo

- David J. C. Mackay, **Information Theory, Inference, and Learning Algorithms**, Cambridge University Press, 2003
- McEliece R.J., **The theory of Information and coding**, Cambridge University Press, 1985
- John Proakis & Masoud Salehi, **Digital Communication**, 2007

Lý thuyết thông tin



Phần 3: Lý thuyết mã hóa

- Toán học nền tảng
- Mã tối ưu
- Mã khống chế lỗi

dinhptit@gmail.com

Toán học nền tảng

- ✓ Số học modular
- ✓ Các cấu trúc đại số:
- ✓ Nhóm
- ✓ Vành
- ✓ Trường
- ✓ Không gian tuyến tính V_n trên $GF(2)$



Các khái niệm

- **Phép Mã hóa f** là ánh xạ 1-1 mỗi dấu a_i thành từ mã $\alpha_i^{n_i}$

$$f : a_i \rightarrow \alpha_i^{n_i} \quad \alpha_i^{n_i} = (b_{i_1}, b_{i_2}, \dots, b_{i_{n_i}})$$

n_i : số dấu mã có trong codeword.

- Mã đều
- Mã không đều

- **Bộ Mã (code)** là tập các từ mã được dùng để mã hóa các dấu.

$$C = \{\alpha_i^{n_i}\}$$



Các khái niệm(cont)

- Độ chậm giải mã của bộ mã: Là số dấu mã nhận được cần thiết trước khi có thể thực hiện phân tách được từ mã.
 - Bộ mã được gọi là không suy biến (nonsingular) nếu mỗi tin của nguồn được mã hóa bằng một từ mã riêng biệt
 - Bộ mã phân tách được nếu giải mã là đơn trị (uniquely decodable code) .
 - Bộ mã có khả năng giải mã tức thời (Instantaneous code):
 - Là mã phân tách được, và
 - Sự giải mã được thực hiện ngay trong khi các dấu mã đang tới mà ko cần đợi tới khi kết thúc nhận bản tin.
- Bộ mã này phải có đặc tính prefix (không có bất cứ từ mã nào là tiền tố của từ mã khác).



Định lý Kraft (về chiều dài các từ mã của bộ mã prefix)

Xét một nguồn tin $X = \{x_1, x_2, \dots, x_s\}$.

Điều kiện cần và đủ để tồn tại bộ mã tức thời (prefix) với độ dài tương ứng $\{n_1, n_2, \dots, n_s\}$ để mã hóa X là:

$$\sum_{i=1}^s m^{-n_i} \leq 1$$

m là cơ số mã.



Độ thừa của một bộ mã đều (D):

Cho nguồn rời rạc A gồm **s** tin: $A = \{a_i; \overline{1,s}\}$.

Xét phép mã hóa $f: a_i \rightarrow \alpha_i^n ; \alpha_i^n \in V$.

Số từ mã (có độ dài n) có thể có: $N = m^n$. (m : cơ số mã)

Số từ mã được dùng: **s**

Định nghĩa: Độ thừa của một bộ mã đều:

$$D \stackrel{\Delta}{=} \frac{H_0(V) - H_0(A)}{H_0(V)} = 1 - \frac{H_0(A)}{H_0(V)} [\%]$$

Trong đó : $H_0(A) = \log s$, và $H_0(V) = \log N = n \log m$

- Nếu $s=N$: Mã không có độ thừa (mã đầy)
- Nếu $s < N$: Mã vơi (Sẽ có một số tổ hợp mã cấm ko dùng đến)



Khoảng cách mã (d)

Định nghĩa: Khoảng cách giữa hai từ mã bất kỳ α_i^n và α_j^n là số các dấu mã khác nhau tính theo cùng một vị trí giữa hai từ mã này, ký hiệu $d(\alpha_i^n, \alpha_j^n)$

Tính chất

- $d(\alpha_i^n, \alpha_j^n) = d(\alpha_j^n, \alpha_i^n)$
- $n \geq d(\alpha_i^n, \alpha_j^n) \geq 0$
- (Tính chất tam giác): $d(\alpha_i^n, \alpha_j^n) + d(\alpha_j^n, \alpha_k^n) \geq d(\alpha_i^n, \alpha_k^n)$

Định nghĩa: Khoảng cách Hamming d_0 của một bộ mã được xác định theo biểu thức sau:

$$d_0 \stackrel{\Delta}{=} \min_{\forall \alpha_i^n, \alpha_j^n} d(\alpha_i^n, \alpha_j^n)$$

Ở đây α_i^n và α_j^n Là các cặp từ mã phân biệt



Trọng số của một từ mã

Định nghĩa: Trọng số của một từ mã α_i^n (được k/hiệu là $W(\alpha_i^n)$) là số các dấu mã khác không trong từ mã.

Tính chất của trọng số:

- $0 \leq W(\alpha_i^n) \leq n$
- $d(\alpha_i^n, \alpha_j^n) = W(\alpha_i^n + \alpha_j^n)$



Khả năng khống chế lỗi của mã đều nhị phân

- Một mã đều nhị phân có khả năng phát hiện được lỗi nếu số lỗi không vượt quá $d_0 - 1$.
- Một mã đều nhị phân có khả năng sửa được lỗi nếu số lỗi không vượt quá $t = \left\lfloor \frac{d_0 - 1}{2} \right\rfloor$



Điều kiện sử dụng mã không có độ thừa trên BSC

Giả sử ta truyền từ mã đơn giản qua kênh đối xứng nhị phân không nhớ có xác suất thu sai một dấu là p_0 . Khi đó xác suất thu đúng một dấu tương ứng là $(1-p_0)$. Từ mã n dấu chỉ nhận đúng khi mọi dấu mã đều nhận đúng. Như vậy, xác suất thu đúng từ mã p_d là:

$$p_d = (1-p_0)^n$$

Xác suất thu sai của từ mã là:

$$p_s = 1 - p_d = 1 - (1-p_0)^n$$

Nếu xác suất thu sai cho phép một từ mã (n dấu) là p_{scp} , khi đó điều kiện sử dụng mã đơn giản trong kênh nhị phân đối xứng ko nhớ là:

$$p_s \leq p_{scp}$$

Với $p_0 \ll 1$, ta có công thức gần đúng sau:

$$(1-p_0)^n \approx 1 - np_0$$

Do đó: $p_s \approx np_0$

khi đó điều kiện sử dụng mã đơn giản trên BSC: $p_0 \leq \frac{p_{scp}}{n}$



Mã tối ưu

dinhptit@gmail.com

Mã hóa nguồn

Xét nguồn tin $A = \begin{pmatrix} a_i \\ p(a_i) \end{pmatrix}, i = \overline{1, S}$

Phép mã hóa nguồn $f : a_i \rightarrow \alpha_i^{n_i}$

- **Mục tiêu của mã nguồn**

Nén (giảm độ dài trung bình của từ mã)

- **Độ dài trung bình của bộ mã**

Là kỳ vọng của đại lượng ngẫu nhiên n_i .

$$\bar{n} = M[n_i] = \sum_{i=1}^s n_i p(a_i)$$

Định lý mã hóa nguồn của Shannon (Định lý mã hóa nguồn 1)

- Độ dài trung bình từ mã của bất kỳ bộ mã prefix nào dùng để mã hóa nguồn tin A cũng không thể để bé hơn n_0 , tức là:

$$\bar{n} \geq n_0$$

$$n_0 = \frac{H(A)}{\log m}$$

m: Cơ số mã.

Dấu “=” xảy ra khi: $m^{-n_i} = p(a_i)$

- Nguyên tắc mã nguồn là ưu tiên từ mã ngắn để mã hóa các tin có xác suất xuất hiện lớn.
- Hiệu quả của phép mã hóa nguồn: $\eta = \frac{n_0}{\bar{n}}$

Một số thuật toán mã nguồn

- **Thuật toán Shannon**

- Thuộc lớp mã entropy.

- **Thuật toán Shannon-Fano**

- Thuộc lớp mã entropy. Thuật toán đơn giản, Bộ mã có tính prefix
 - Không luôn tạo được mã tối ưu, Mã cận tối ưu (Suboptimal)

- **Thuật toán Shannon-Fano-Elias**

- Là tiền thân của mã hóa số học. Ít dùng vì có $H(x)+1 \leq LC(X) \leq H(X)+2$

- **Thuật toán số học**

- Thuộc lớp mã entropy, là sự mở rộng thuật toán Shannon-Fano-Elias.

- **Thuật toán Lempel-Ziv**

- Mã hóa từ điển. Thuật toán thích nghi. Không thuộc lớp entropy.
 - Không yêu cầu phải biết trước phân bố của nguồn.

- **Thuật toán Huffman**

Mã tối ưu

- **Yêu cầu của Optimal Codes**

- Bộ mã phải có khả năng giải mã tức thời (tính prefix).
- Độ dài trung bình từ mã phải đạt giá trị tối ưu ($\bar{n} = \bar{n}_{opt}$)

- **Bất đẳng thức kẹp (Định lý mã hóa nguồn 2)**

Độ dài trung bình của một bộ mã tối ưu thỏa mãn:

$$n_0 \leq \bar{n}_{opt} < n_0 + 1$$

Thuật toán Huffman

Đề xuất bởi David A. Huffman:



Đặc điểm

- Mã hóa entropy dựa trên tần suất xuất hiện
- Nén lossless;
- Variable-length code
- Bộ mã thu được là opt: (có tính prefix, và có $(\bar{n} = \bar{n}_{opt})$)

Nhược điểm

- Phải biết trước phân bố của nguồn
- Bộ mã ko phải là duy nhất, vì vậy phải gửi kèm cây mã (bảng mã) để phục vụ việc giải mã sau này.

Channel Error Control

dinhptit@gmail.com

Overview

❑ The need for Error Control

- **Ideal channel:** Sự truyền tin ko bị **corruption & error**.
- **Real channel:** BW, Noise, distortion & interference, gây ra lỗi

❑ Principles of Error Control

Phía phát: Tạo ra **redundant bits** vào chuỗi digit nhờ thuật toán, sao cho các lỗi sinh ra trên kênh có thể kiểm soát tại máy thu .

❑ Error Control Schemes

- ARQ schemes (Automatic Repeat request)
- FEC schemes (Forward Error Correction):
- Hybrid schemes

❑ Techniques for error detection

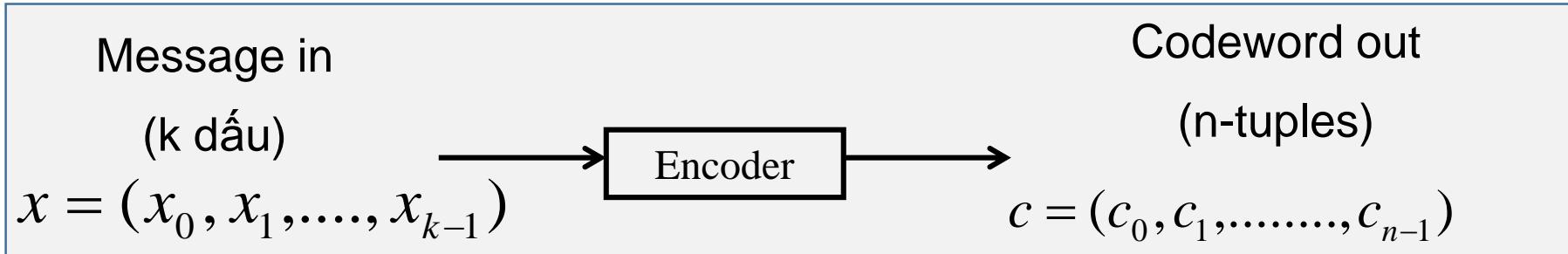
- Parity check
- Checksum
- Cyclic redundancy check (CRC)

Error-correcting codes (ECC)

- Linear block codes
 - ✓ Cyclic codes (e.g., Hamming codes is a subset)
 - ✓ Repetition codes
 - ✓ Polynomial codes (e.g., BCH codes)
 - ✓ Reed–Solomon codes
 - ✓ Low-density parity-check (LDPC) codes
- Convolutional codes
- Turbo codes

Mã khối (block codes)

- **Mã hóa khối:** là những thuật toán mã hóa hoạt động trên những khối thông tin vào có độ dài k xác định, tạo ra các từ mã có độ dài n xác định.



$\cdot x_i \in GF(q); c_j \in GF(q)$

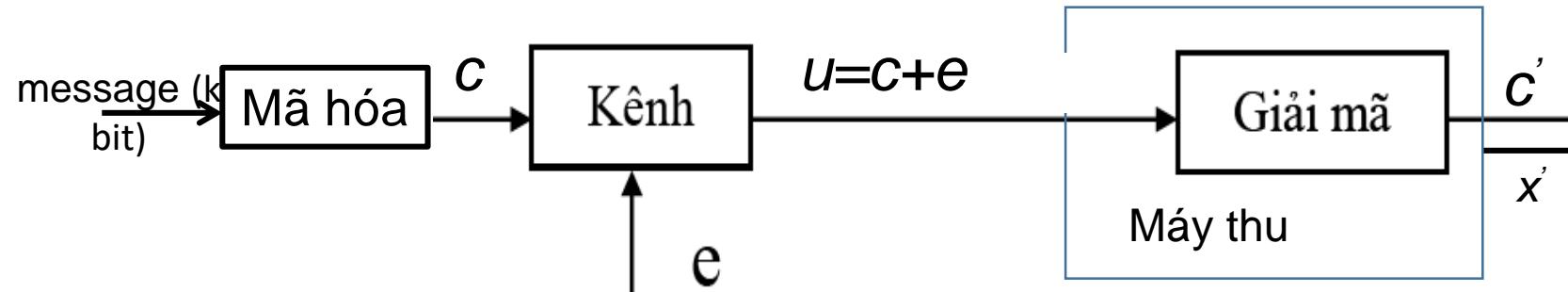
q : Cơ số mã, mặc định là 2.

- **Bộ mã khối C(n,k):** Là tập gồm 2^k từ mã n-tuples, được chọn trong số 2^n tổ hợp mã có thể có độ dài n.

- **Code rate :**

$$R_c = \frac{k}{n}$$

Mô hình kênh có nhiễu cộng:



$c = (c_0, c_1, \dots, c_{n-1})$: Từ mã phát (n -tuples), \in bộ mã $C(n,k)$

$u = (u_0, u_1, \dots, u_{n-1})$: Vector thu.

$e = (e_0, e_1, \dots, e_{n-1})$: Mẫu lỗi, \rightarrow có 2^n cấu trúc lỗi.

- Error pattern $e = u + c = (u_0 + c_0, u_1 + c_1, \dots, u_{n-1} + c_{n-1}) = (e_0, e_1, \dots, e_{n-1})$
where $e_i = 1$ for $u_i \neq c_i$, and $e_i = 0$ for $u_i = c_i$
- Máy thu không phát hiện ra có lỗi nếu vector thu **u** là một từ mã hợp lệ.

Khả năng khồng chế lỗi của mã khối

- Một bộ mã (n, k, d_0) có khả năng phát hiện được lỗi nếu cấu trúc lỗi có trọng số thỏa mãn:

$$w(e) \leq (d_0 - 1)$$

- Một bộ mã (n, k, d_0) có khả năng tự sửa được lỗi nếu cấu trúc lỗi có trọng số thỏa mãn:

$$w(e) \leq \left\lfloor \frac{d_0 - 1}{2} \right\rfloor$$

Mã khối tuyến tính (Linear block codes)

dinhptit@gmail.com

Mã khối tuyến tính (linear block code)

Định nghĩa: Mã khối tuyến tính $C(n,k)$ có chiều dài từ mã n , trong đó mỗi dấu mã là một dạng tuyến tính của k dấu thông tin.

$$c = (c_0 c_1 \dots c_{n-1}) \quad c_j = \sum_{i=1}^k a_i x_i \quad j = 0, \dots, n-1$$

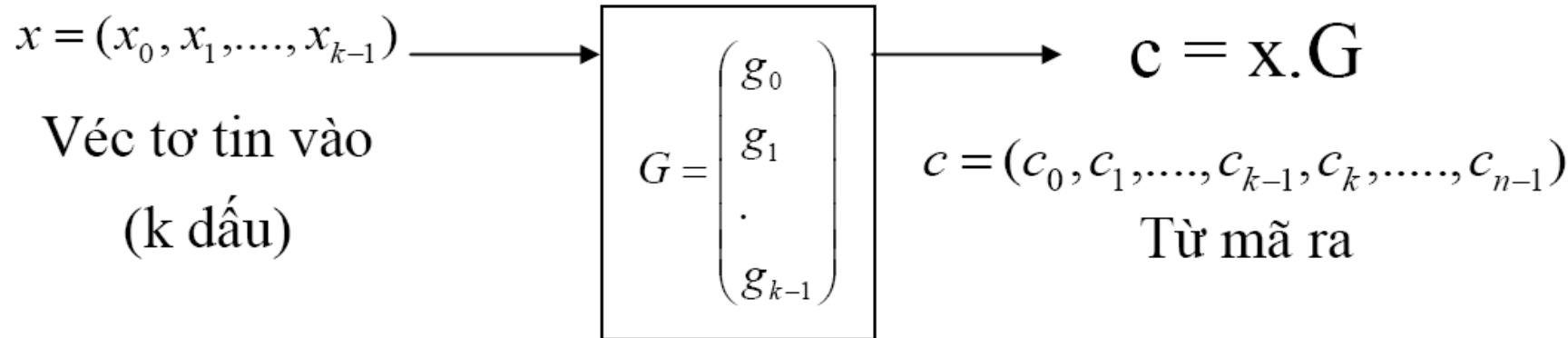
Định nghĩa: Mã tuyến tính (n,k) là không gian con tuyến tính k chiều (V_k) trong không gian tuyến tính n chiều (V_n).

□ Generator matrix của mã khối tuyến tính (n,k) :

$$G = \begin{pmatrix} g_0 \\ g_1 \\ \dots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \dots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \dots & g_{1,n-1} \\ \dots & \dots & \dots & \dots \\ g_{k-1,0} & g_{k-1,1} & \dots & g_{k-1,n-1} \end{pmatrix}$$

Mã khối tuyến tính (tt)

□ Mô hình tạo mã khối tuyến tính (n,k):



□ Ma trận kiểm tra

Mỗi mã $C(n,k)$, tồn tại mã đối ngẫu $C_d(n,n-k)$ với ma trận sinh H .

$$H = \begin{pmatrix} h_0 \\ h_1 \\ \dots \\ h_{n-k-1} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \dots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \dots & h_{1,n-1} \\ \dots & \dots & \dots & \dots \\ h_{n-k-1,0} & h_{n-k-1,1} & \dots & h_{n-k-1,n-1} \end{pmatrix}$$

H is called a *parity-check matrix* of C .

Mã hệ thống tuyến tính

Dạng thức 1:

Redundant checking part (n-k) digits	message part k digits
---	--------------------------

$$G_{sys} = \begin{pmatrix} g_0 \\ g_1 \\ \dots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} p_{0,0} & \dots & p_{0,n-k-1} & I_{0,n-k} & \dots & I_{0,n-1} \\ p_{1,0} & \dots & p_{1,n-k-1} & I_{1,n-k} & \dots & I_{1,n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ p_{k-1,0} & \dots & p_{k-1,n-k-1} & I_{k-1,n-k} & \dots & gI_{k-1,n-1} \end{pmatrix} = [PI_k]$$

Matrix $P_{k \times (n-k)}$
Matrix I_k

- Tương ứng các dấu mã kiểm tra và các dấu mã mang thông tin:

$$c_j = x_0 p_{0,j} + x_1 p_{1,j} + \dots + x_{k-1} p_{k-1,j} \quad 0 \leq j \leq n - k - 1$$

$$c_{n-k+i} = x_i \quad 0 \leq i \leq k-1$$

- Parity-check matrix in systematic form is: $H_{sys} = \begin{pmatrix} h_0 \\ h_1 \\ \dots \\ h_{n-k-1} \end{pmatrix} = [I_{n-k} P^T]$

Mã hệ thống tuyến tính (tt)

Dạng thức 2:

message part

k digits

Redundant checking part

(n-k) digits

- Generator matrix in systematic form is:

$$G_{sys} = \begin{pmatrix} g_0 \\ g_1 \\ \dots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} I_{0,0} & \dots & I_{0,k-1} & p_{0,k} & \dots & p_{0,n-1} \\ I_{1,0} & \dots & I_{1,k-1} & p_{1,k} & \dots & p_{1,n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ I_{k-1,0} & \dots & I_{k-1,k-1} & p_{k-1,k} & \dots & p_{k-1,n-1} \end{pmatrix} = [I_k P]$$

Ma trận I_k Ma trận $P_{k \times (n-k)}$

- Tương ứng các dấu mã mang thông tin và các dấu kiểm tra trong từ mã:

$$c_i = x_i \quad 0 \leq i \leq k-1; \quad c_j = x_0 p_{0,j} + x_1 p_{1,j} + \dots + x_{k-1} p_{k-1,j} \quad k \leq j \leq n-1$$

- Parity-check matrix in systematic form is:

$$H_{sys} = \begin{pmatrix} h_0 \\ h_1 \\ \dots \\ h_{n-k-1} \end{pmatrix} = [P^T I_{n-k}]$$

Các bài toán tối ưu của mã tuyến tính nhị phân

Khi xây dựng một mã tuyến tính (n, k, d_0) người ta mong muốn tìm được các mã có độ thừa nhỏ nhưng lại có khả năng khống chế sai lớn. Để đơn giản người ta thường xây dựng mã dựa trên các bài toán tối ưu sau:

Bài toán 1

Cho trước k và d_0 , tìm mã có độ dài với từ mã n nhỏ nhất.

Tương ứng với bài toán này ta có giới hạn Griesmer sau:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d_0}{2^i} \right\rceil$$

Ở đây $\lceil x \rceil$ chỉ số nguyên nhỏ nhất lớn hơn hoặc bằng x .

Ví dụ Cho $k = 4$, $d_0 = 3$

$$n \geq 3 + 2 + 1 + 1 = 7$$

Hay nói một cách khác mã $(7, 4, 3)$ là một mã tối ưu đạt được giới hạn Griesmer.

Các bài toán tối ưu của mã tuyến tính nhị phân (tt)

Bài toán 2

Cho n và k , tìm mã có d_0 là lớn nhất.

Tương ứng với bài toán này ta có giới hạn Plotkin sau:

$$d_0 \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$$

Ví dụ: Cho $k = 3$, $n = 7$

$$d_0 \leq \frac{7 \cdot 2^2}{2^3 - 1} = 4$$

Nói một cách khác mã $(7, 3, 4)$ là một mã tối ưu đạt được giới hạn Plotkin

Các bài toán tối ưu của mã tuyến tính nhị phân (tt)

Bài toán 3

Cho n và số sai khả sửa t xác định (hoặc cho n, d_0), tìm mã có số dấu thông tin k là lớn nhất (hay số dấu thừa $r = n - k$ là nhỏ nhất)

Tương ứng với bài toán này ta có giới hạn Hamming sau:

$$2^{n-k} \geq \sum_{i=0}^t C_n^i$$

Ví dụ Cho $n = 7$ và $t = 1$

$$2^r \geq \sum_{i=0}^1 C_7^i = C_7^0 + C_7^1 = 8$$

$$r \geq \log_2 8 = 3$$

$$\text{hay } k \leq 7 - 3 = 4$$

Như vậy mã $(7, 4, 3)$ là mã tối ưu đạt được giới hạn Hamming

Mã đạt được giới hạn Hamming còn được gọi là mã hoàn thiện

Tài liệu tham khảo

- ✓ John Proakis & Masoud Salehi, **Digital Communication**, 2007
- ✓ Shu Lin, **Error Control Coding-Fundamentals and Applications**, Prentice Hall, 2004
- ✓ Simon Haykin, **Communication Systems**, 4rd edition, John Wiley & Sons, 2001.



Bài tập và gợi ý giải môn học Lý thuyết thông tin

lý thuyết thông tin (Học viện Công nghệ Bưu chính Viễn thông)



Scan to open on Studocu

ĐÁP ÁN

Ngành đào tạo: ĐIỆN TỬ – VIỄN THÔNG

Hệ đào tạo : ĐẠI HỌC

Môn học : LÝ THUYẾT THÔNG TIN Mã số 411 LTT 340A Số ĐVHT: 4

PHẦN 1: LÝ THUYẾT THÔNG TIN

Câu 1: (1 điểm): Định nghĩa lượng thông tin riêng (độ bất định) của một biến ngẫu nhiên. Xác định các đơn vị đo

- Định nghĩa lượng thông tin riêng (độ bất định)

Lượng thông tin riêng là độ bất định tiềm năng chứa trong một biến cố ngẫu nhiên x_k .

Ký hiệu $I(x_k)$

$$I(x_k) = k \ln p(x_k)$$

- Các đơn vị đo

$$k = -1 \quad I(x_k) = -\ln p(x_k) \text{ (nat)}$$

$$k = -\frac{1}{\ln 2} \quad I(x_k) = -\log_2 p(x_k) \text{ (bít)}$$

$$k = -\frac{1}{\ln 10} \quad I(x_k) = -\lg p(x_k) \text{ (hart)}$$

$$1 \text{ nat} = 1,443 \text{ bít}$$

$$1 \text{ hart} = 3,322 \text{ bít}$$

Câu 2: (1 điểm) Định nghĩa entropy của nguồn rời rạc

Entropy của nguồn tin rời rạc A là trung bình thống kê của lượng thông tin riêng của các tin thuộc A

Ký hiệu: $H_1(A)$

$$H_1(A) = M \left[I(a_i) \right]$$

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_s \\ p(a_1) & p(a_2) & \dots & p(a_s) \end{pmatrix}$$

$$0 \leq p(a_i) \leq 1 \quad \sum_{i=1}^s p(a_i) = 1$$

$$H_1(A) = - \sum_{i=1}^{s'} p(a_i) \log p(a_i) \text{ (bít)}$$

Câu 3: (1 điểm) *Nêu các tính chất của entropy của nguồn rời rạc*

Các tính chất của $H_1(A)$

- Khi $p(a_k) = 1, p(a_i) = 0$ với $\forall i \neq k$ thì $H_1(A) = H_1(A)_{\min} = 0$
- Một nguồn tin rời rạc gồm s dấu đồng xác suất cho entropy cực đại. Ta có

$$H_1(A)_{\max} = \log s$$

- Entropy của nguồn rời rạc là một đại lượng giới hạn

$$0 \leq H_1(A) \leq \log s$$

Câu 4: (1 điểm) *Định nghĩa khả năng thông qua kênh rời rạc, nêu các tính chất?*

- Định nghĩa: Khả năng thông qua của kênh rời rạc là giá trị cực đại của lượng thông tin chéo trung bình truyền qua kênh trong một đơn vị thời gian lấy theo mọi khả năng có thể có của nguồn tin A.

$$C' = \max_A I'(A, B) = v_k \max_A I(A, B) \text{ (bps)}$$

- Các tính chất:

+ $C' \geq 0$

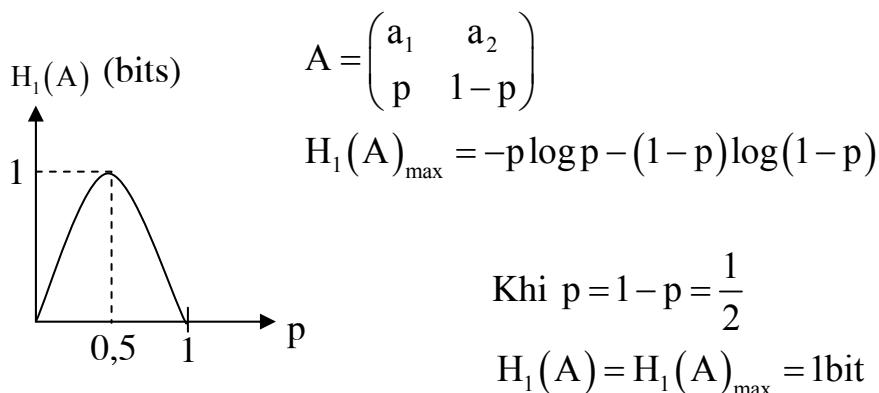
$C' = 0$ khi A và B là độc lập (kênh bị đứt)

+ $C' \leq v_k \log s$

$C' = v_k \log s$ khi kênh không nhiễu

Câu 5: (2 điểm) *Entropy của nguồn rời rạc nhị phân. Ý nghĩa của đơn vị đo bít?*

- Entropy của nguồn rời rạc nhị phân.



- Ý nghĩa: 1 bít là lượng thông tin riêng trung bình chứa trong một biến cố của một nguồn rời rạc 2 phân đồng xác suất.

Câu 6: (2 điểm) Xác định hai trạng thái cực đoan của kênh rời rạc.

- Kênh bị đứt:

Các nguồn tin A và B ở hai đầu thu và phát là độc lập.

$$p(a_i/b_j) = p(a_i)$$

$$p(b_j/a_i) = p(a_i)$$

$$p(a_i b_j) = p(a_i)p(b_j)$$

Ta có: $H(A/b_j) = H(A)$

$$H(A/B) = H(A)$$

Nhận xét: Lượng thông tin tổn hao trung bình đúng bằng entropy của nguồn. Kênh không thể truyền tin được

- Kênh không nhiễu:

$$A \equiv B$$

$$p(a_k/b_k) = 1$$

$$H(A/b_k) = 0$$

$$H(A/B) = 0$$

Nhận xét: Lượng thông tin tổn hao trên kênh bằng 0

Câu 7: (2 điểm) Entropy có điều kiện $H(A/B)$: định nghĩa và nêu các tính chất

- Định nghĩa: Entropy có điều kiện về 1 trường tin A khi đã rõ trường tin B được xác định theo công thức sau:

$$H(A/B) = - \sum_{i=1}^s \sum_{j=1}^t p(a_i b_j) \log p(a_i/b_j)$$

- Các tính chất:

- + $H(AB) = H(A) + H(B/A) = H(B) + H(A/B)$

- + $0 \leq H(A/B) \leq H(A)$

- + $H(AB) = H(A) + H(B)$

Câu 8: (2 điểm) Lượng thông tin chéo trung bình truyền qua kênh rời rạc: định nghĩa và tính chất

- Định nghĩa:

$$I(A, B) \stackrel{\Delta}{=} M[I(a_i, b_j)]$$

với $I(a_i, b_j) = \log \frac{p(a_i/b_j)}{p(a_i)}$

$$I(A, B) = \sum_{i=1}^s \sum_{j=1}^t p(a_i b_j) \log \frac{p(a_i/b_j)}{p(a_i)}$$

$$I(A, B) = H(A) - H(A/B) = H(B) - H(B/A)$$

- Tính chất:

$$+ \quad I(A, B) \geq 0$$

$$+ \quad I(A, B) \leq H(A)$$

Câu 9: (3 điểm) Cho kênh đối xứng nhị phân sau

$$p(a_1) = p$$

$$p(a_2) = 1 - p$$

$$p(b_1/a_2) = p(b_2/a_1) - p_s = 1 - p_d$$

Cho tốc độ truyền tin của kênh $v_k = 1/T$

Tính khả năng thông qua C' của kênh này.

Giải:

$$\text{Ta có } C' = \frac{1}{T} \max_A I(A, B) = \frac{1}{T} \max_A [H(B) - H(B/A)]$$

Trong đó:

$$\begin{aligned} H(B/A) &= - \sum_{i=1}^2 \sum_{j=1}^t p(a_i) p(b_j/a_i) \log p(b_j/a_i) \\ &= -p(a_1) [p(b_1/a_1) \log p(b_1/a_1) + p(b_2/a_1) \log p(b_2/a_1)] - \\ &\quad -p(a_2) [p(b_1/a_2) \log p(b_1/a_2) + p(b_2/a_2) \log p(b_2/a_2)] \\ &= -p[(1-p_s) \log(1-p_s) + p_s \log p_s] - (1-p)[p_s \log p_s + (1-p_s) \log(1-p_s)] \\ &= -[p_s \log p_s + (1-p_s) \log(1-p_s)] \end{aligned}$$

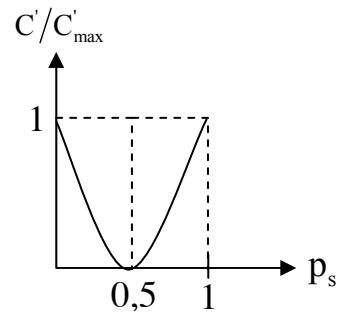
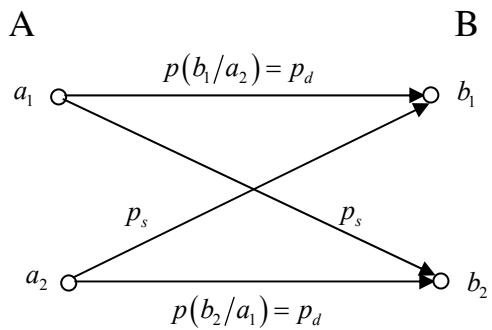
Ta thấy $H(B/A)$ không phụ thuộc vào xác suất tiên nghiệm của các tin thuộc nguồn A. Do đó:

$$C' = \frac{1}{T} \max_A H(B) - \frac{1}{T} H(B/A)$$

$$\text{Ta có } \max_A H(B) = H(B)_{\max} = \log 2 = 1 \text{ bit}$$

$$C'_{\max} = \frac{1}{T} \text{ khi } p_s = 0 \text{ (kênh không nhiễu)}$$

$$\frac{C'}{C'_{\max}} = 1 + p_s \log p_s + (1-p_s) \log(1-p_s)$$



Câu 10: (3 điểm) A chọn ngẫu nhiên một trong các số từ 0 đến 7. Tính số câu hỏi trung bình tối thiểu mà B cần đặt cho A để xác định được số mà A đã chọn. Nếu thuật toán hỏi? Giả sử A đã chọn số 3, hãy đặt các câu hỏi cần thiết?

Độ bất định của số được chọn ngẫu nhiên:

$$I(a_i) = -\log p(a_i) = -\log \frac{1}{8} = 3 \text{ bit}$$

Để tìm được số đã chọn của A, B phải đặt các câu hỏi cho A để thu được đủ một lượng thông tin cần thiết là 3 bít.

Mỗi câu hỏi của B (dạng lựa chọn) có thể xem là nguồn rác nhị phân, bởi vậy lượng thông tin nhận được sau mỗi câu trả lời tương ứng là:

$$H(B) = -p \log p - (1-p) \log(1-p)$$

Với p : xác suất nhận câu trả lời "đúng"

$1-p$: xác suất nhận câu trả lời "sai"

$$\text{Vậy số câu hỏi cần thiết } n \text{ là: } n = \frac{I(a_i)}{H(B)}$$

$$\text{Số câu hỏi trung bình tối thiểu là: } n_{\min} = \frac{I(a_i)}{H(B)_{\max}}$$

$$H(B)_{\max} \text{ khi } p = 1 - p = \frac{1}{2}$$

$$n_{\min} = \frac{3 \text{ bit}}{1 \text{ bit}} = 3 \text{ lần hỏi}$$

Giả sử A chọn số B. Các câu hỏi b có thể đặt cho A là:

- Câu 1 - Số A chọn lớn hơn 3? Trả lời: Sai
- Câu 2 - Số A chọn lớn hơn 1? Trả lời: Đúng
- Câu 3 - Số A chọn lớn hơn 2? Trả lời: Sai

Vậy số A chọn là 3

Câu 11: (4 điểm) Một thiết bị vô tuyến điện gồm 16 khối có độ tin cậy như nhau và được mắc nối tiếp. Ta sử dụng một thiết bị đo để đo tín hiệu ra của các khối. Giả sử có một khối nào đó bị hỏng. Hãy tính số lần đo trung bình tối thiểu để tìm được khối bị hỏng. Nếu thuật toán đo? Giả sử khái hỏng là khái thứ 6, tìm vị trí các điểm đo cần thiết?

Theo giả thiết độ bất định của khái hỏng là:

$$I(a_i) = -\log p(a_i) = -\log \frac{1}{16} = 4 \text{ bit}$$

Lượng thông tin nhận được sau mỗi phép đo:

$$H(B) = -p \log p - (1-p) \log(1-p)$$

Với p : xác suất có tín hiệu

$1-p$: xác suất không có tín hiệu

Để xác định được khối hỏng (khử hết độ bất định) số phép đo cần thiết n là:

$$n_{\min} = \frac{I(a_i)}{H(B)_{\max}}$$

$$H(B) \rightarrow \max \text{ khi } p = 1 - p = \frac{1}{2}$$

$$H(B)_{\max} = 1 \text{ bit}$$

$$n_{\min} = \frac{4 \text{ bit}}{1 \text{ bit}} = 4 \text{ lần đo}$$

Để n_{\min} thuật toán đo phải đảm bảo $H(B) \rightarrow \max \Rightarrow$ Mỗi lần đo phải đo ở điểm giữa của các khối cần xác định nhằm đảm bảo $p = 1 - p = \frac{1}{2}$.

Giả sử khối hỏng là khối 6. Các phép đo cần thiết là:

- Lần 1: Đo ở đâu ra khối 8: Không có tín hiệu, khối hỏng nằm trong các khối từ 1 → 8.
- Lần 2: Đo ở đâu ra khối 4: Không có tín hiệu, khối hỏng nằm trong các khối từ 5 → 8.
- Lần 3: Đo ở đâu ra khối 6: Không có tín hiệu, khối hỏng nằm trong khối 5 hoặc 6.
- Lần 4: Đo ở đâu ra khối 5: Có tín hiệu. Vậy khối hỏng là khối 6

Câu 12: (4 điểm) Trong bộ tú lơ khơ 52 quân (không kể fǎng teo), A rút ra một quân bài bất kỳ. Tính số câu hỏi trung bình tối thiểu mà B cần đặt cho A để xác định được quân bài mà A đã rút. Nếu thuật toán hỏi? Giả sử A rút ra 7 quân rô, hãy nêu các câu hỏi cần thiết?

Độ bất định về quân bài mà A đã rút:

$$I(a_i) = -\log p(a_i) = -\log \frac{1}{52} < 6 \text{ bit}$$

Giả sử B đặt cho A câu hỏi dạng lựa chọn, khi đó lượng thông tin nhận được sau mỗi câu trả lời của A là:

$$H(B) = -p \log p - (1-p) \log(1-p)$$

Với p : xác suất nhận câu trả lời là "đúng"

$1-p$: xác suất nhận câu trả lời là "sai"

Số câu hỏi cần thiết để xác định được quân bài A đã rút là: $n = \frac{I(a_i)}{H(B)}$

Ta thấy $n \rightarrow \min$ khi $H(B) \rightarrow \max$

$$H(B) = H(B)_{\max} = 1 \text{ bit} \text{ khi } p = 1 - p = \frac{1}{2}$$

Số câu hỏi trung bình tối thiểu là: $n_{\min} = \frac{\log 52}{1 \text{ bit}} < 6$ lần

Thuật toán phải đảm bảo $p = 1 - p = \frac{1}{2}$.

Giả sử A rút ra 7 rô. Các câu hỏi cần thiết có thể như sau:

- Câu 1: Quân A rút là quân đỏ? Đúng
- Câu 2: Quân A rút là quân cờ? Sai
- Câu 3: Quân A rút có giá trị ≤ 7 ? Đúng (giả sử J = 11, Q = 12, K = 13, At=1)
- Câu 4: Quân A rút có giá trị ≤ 3 ? Sai
- Câu 5: Quân A rút có giá trị ≤ 5 ? Sai
- Câu 6: Quân A rút là 6 rô? Sai

Vậy quân A rút là 7 rô

Câu 13 :(4 điểm) Trong 27 đồng xu có 1 đồng xu giả nhẹ hơn. Để tìm được đồng xu giả người ta sử dụng một cân đĩa thăng bằng. Hãy tính số lần cân trung bình tối thiểu để xác định được đồng xu giả. Nếu thuật toán cân ?

Theo giả thiết độ bất định chứa trong sự kiện đồng xu giả là :

$$I(x_i) = -\log p(x_i) = -\log 1/27 = \log 27 \text{ bit}$$

Khi sử dụng cân đĩa thăng bằng, sau mỗi lần cân các sự kiện có thể có là :

- Cân thăng bằng với xác suất p
- Cân lệch trái với xác suất q
- Cân lệch phải với xác suất 1-p-q

Lượng thông tin nhận được sau mỗi lần cân :

$$H(B) = -p \log p - q \log q - (1-p-q) \log (1-p-q)$$

Để xác định được đồng xu giả tổng lượng thông tin nhận được sau các lần cân phải không nhỏ hơn độ bất định của đồng xu giả. Như vậy số lần cân cần thiết là : $n = I(x_i)/H(B)$

Để n có giá trị nhỏ nhất thì $H(B)$ phải đạt giá trị cực đại.

Ta có $H(B) = H(B)_{\max} = \log 3$ khi $p = q = 1-p-q = 1/3$.

Khi đó $n_{\min} = I(x_i)/H(B)_{\max} = \log 27 / \log 3 = 3$ lần cân.

Thuật toán cân như sau(đảm bảo $p = q = 1-p-q$)

- Lần 1 : Chia 27 đồng xu thành 3 phần, mỗi phần có 9 đồng xu. Lấy 2 phần bất kỳ đặt lên mỗi bàn cân 1 phần . Nếu cân thăng bằng thì đồng xu giả

nằm trong 9 đồng xu chưa cân. Ngược lại, tuỳ theo cân lệch trái hay lệch phải ta cũng xác định được phần có chứa đồng xu giả.

- Lần 2 : Chia 9 đồng có chứa đồng xu giả thành 3 phần như nhau, mỗi phần có 3 đồng xu. Đặt 2 phần bất kỳ lên 2 bàn cân. Kết quả của phép cân sẽ giúp ta xác định được 3 đồng xu có chứa đồng xu giả.
- Lần 3 : Lấy 2 đồng xu bất kỳ trong 3 đồng xu có chứa đồng xu giả đặt lên 2 đĩa cân. Sau lần cân này ta sẽ xác định được đồng xu giả.

Câu 14 : (2 điểm) Tính entropie của trường sự kiện đồng thời ?

Xét 2 trường sự kiện A và B sau :

$$A = \left\{ \begin{array}{l} a_i \\ p(a_i) \end{array} \right\} i = \overline{1,0} \quad B = \left\{ \begin{array}{l} b_j \\ p(b_j) \end{array} \right\} j = \overline{1,t}$$

Khi đó, trường sự kiện đồng thời C = A.B là :

$$C = \left\{ \begin{array}{l} a_i b_j \\ p(a_i)p(b_j) \end{array} \right\} \forall i, j, i = \overline{1,0}, j = \overline{1,t}$$

Theo định nghĩa, entropie của trường sự kiện đồng thời được xác định như sau :

$$H(C) = - \sum_{i=1}^s \sum_{j=1}^t p(a_i b_j) \log p(a_i b_j)$$

Câu 15: (2 điểm) Cho kênh nhị phân đối xứng không nhớ sau (hình vẽ).

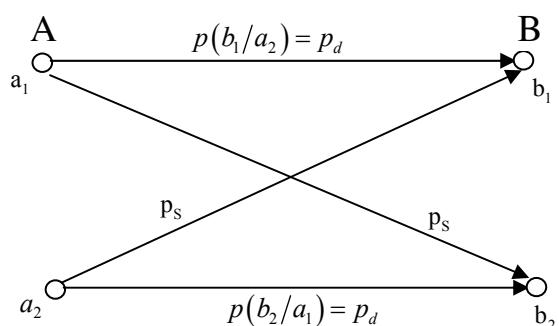
Hãy tính phân bố xác suất của các tin ở đầu ra?

Biết rằng $p(a_1) = p$; $p(a_2) = 1-p$.

Theo công thức xác suất đầy đủ ta có:

$$p(b_1) = p(a_1) \cdot p(b_1/a_1) + p(a_2) \cdot p(b_1/a_2)$$

$$\begin{aligned} p(b_2) &= p(a_1) \cdot p(b_2/a_1) + p(a_2) \cdot p(b_2/a_2) \\ &= 1 - p(b_1) \end{aligned}$$



PHẦN 2: LÝ THUYẾT MÃ HOÁ

Câu 1: (1 điểm): Định nghĩa độ dài trung bình của từ mã? Phát biểu định lý mã hóa thứ nhất của Shannon?

Xét phép mã hoá các tin rời rạc sau: $a_i \rightarrow \alpha_i^{n_i}$

$$A = \begin{pmatrix} a_i \\ p(a_i) \end{pmatrix} \rightarrow V = \begin{pmatrix} \alpha_i^{n_i} \\ p(a_i) \end{pmatrix}$$

- Định nghĩa: Độ dài trung bình của từ mã là kỳ vọng của đại lượng ngẫu nhiên n_i

$$\bar{n} = \sum_{i=1}^s p(a_i)n_i$$

- Định lý mã hoá thứ nhất của Shannon (đối với mã nhị phân)

Luôn luôn có thể xây dựng được một phép mã hoá các tin rời rạc có hiệu quả mà độ dài trung bình của từ mã có thể nhỏ tùy ý, nhưng không nhỏ hơn entropie xác định bởi các đặc tính thống kê của nguồn

$$\bar{n} \geq H_1(A)$$

Câu 2: (1 điểm) Nếu nguyên tắc lập mã tiết kiệm?

Từ định lý mã hoá thứ 1 của Shannon:

$$\bar{n} = \sum_{i=1}^s p(a_i)n_i \geq H_1(A) = -\sum_{i=1}^s p(a_i)\log p(a_i)$$

$$\text{ta có: } n_i \geq \log \frac{1}{p(a_i)}$$

Nguyên tắc: Các tin có xác suất xuất hiện lớn được mã hoá bằng các từ mã có độ dài nhỏ và ngược lại các tin có xác suất xuất hiện nhỏ được mã hoá bằng các từ mã có độ dài lớn.

Câu 3: (1 điểm) Trọng số của từ mã: định nghĩa và tính chất?

- Định nghĩa trọng số của từ mã: $W(\alpha_i^{n_i})$

Trọng số của 1 từ mã là số các dấu mã khác không chứa trong từ mã

- Tính chất:

$$+ \quad 0 \leq W(\alpha_i^{n_i}) \leq 1$$

$$+ \quad W(\alpha_i^n + \alpha_j^n) = d(\alpha_i^n, \alpha_j^n)$$

Câu 4: (1 điểm) Nếu các định lý quy định khả năng phát hiện sai và khả năng sửa sai của một bộ mã?

- Định lý về khả năng phát hiện sai:

Mã nhị phân có độ thừa với khoảng cách Hamming $d_0 > 1$ có khả năng phát hiện t sai thoả mãn điều kiện $t \leq d_0 - 1$.

- Định lý về khả năng sửa sai:

Mã đqueeze nhị phân có độ thừa với khoảng cách Hamming $d_0 \geq 3$ có khả năng sửa được t sai thoả mãn điều kiện: $t \leq \left\lfloor \frac{d_0 - 1}{2} \right\rfloor$. Trong đó $[x]$ ký hiệu phân nguyên của số x .

Câu 5: (2 điểm) Khoảng cách mã: định nghĩa, tính chất? Định nghĩa khoảng cách mã tối thiểu?

- Định nghĩa:

Khoảng cách giữa hai từ mã α_i^n và α_j^n là số các dấu mã khác nhau về giá trị tính theo cùng một thứ tự giữa 2 từ mã này.

$$\text{Ví dụ: } \alpha_i^7 = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0$$

$$\begin{array}{ccccccc} \alpha_j^7 & = & 1 & 0 & 1 & 0 & 0 \\ & & * & * & * & * & * \end{array}$$

$$d(\alpha_i^7, \alpha_j^7) = 5$$

- Tính chất:

$$+ \quad d(\alpha_i^n, \alpha_j^n) \geq 0$$

$$d(\alpha_i^n, \alpha_j^n) = 0 \text{ khi } \alpha_i^n \equiv \alpha_j^n$$

$$+ \quad d(\alpha_i^n, \alpha_j^n) \leq n$$

$$+ \quad \text{Tính chất tam giác: } d(\alpha_i^n, \alpha_j^n) + d(\alpha_j^n, \alpha_k^n) \geq d(\alpha_i^n, \alpha_k^n)$$

Định nghĩa khoảng cách mã tối thiểu:

$$d_0 = \min d(a_i^n, a_j^n) \text{ với mọi } i, j$$

Câu 6: (2 điểm) Cho mã xyclic $V-(n-k)$ có đa thức sinh $g(x) = 1 + x + x^3$ ($n=7, k=4$). Hãy thiết lập ma trận sinh và ma trận kiểm tra của mã này?

Cho ma trận sinh G.

$$G = \begin{pmatrix} 1 & +x & +x^3 \\ x & +x^2 & +x^4 \\ x^2 & +x^3 & +x^5 \\ x^3 & +x^4 & +x^6 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Ma trận kiểm tra H :

$$\text{Ta có: } h(x) = \frac{x^7 + 1}{g(x)} = x^4 + x^2 + x + 1$$

$$\begin{array}{r}
 \begin{array}{c} x^7 + 1 \\ \hline x^7 + x^5 + x^4 \\ x^5 + x^4 + 1 \\ x^5 + x^3 + x^2 \\ x^4 + x^3 + x^2 + 1 \\ x^4 + x^2 + x \\ \hline x^3 + x + 1 \\ x^3 + x + 1 \\ \hline 0 \end{array}
 \end{array}$$

$$h^*(X) = X^{\deg h(x)} h(X^{-1}) = x^4 + x^3 + x^2 + 1$$

$$H = \begin{pmatrix} h^*(x) \\ x \cdot h^*(x) \\ \dots \\ x^{r-1} \cdot h^*(x) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\text{Ta có } G \cdot H^T = 0$$

Câu 7: (2 điểm) hãy thiết lập từ mã hệ thống của bộ mã cyclic (7,4) có đa thức sinh $g(x) = 1 + x + x^3$ tương ứng với đa thức thông tin $a(x) = x + x^3$. (Sử dụng thuật toán 4 bước).

- Bước 1: $a(x) = x + x^3$
- Bước 2: Nâng bậc $a(x)x^{n-k} = (x^3 + x)x^{7-4} = x^6 + x^4$
- Bước 3: Chia tính dư:

$$\begin{array}{r}
 \begin{array}{c} x^6 + x^4 \\ \hline x^6 + x^4 + x^3 \\ x^3 \\ x^3 + x + 1 \\ \hline r(x) = x + 1 \end{array}
 \end{array}$$

- Bước 4: Thiết lập từ mã $f(x)$

$$f(x) = a(x)x^{n-k} + r(x)$$

$$f(x) = x^6 + x^4 + x + 1 \leftrightarrow 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1$$

$$x^6 \ . \ . \ . \ . \ . \ . \ x^6$$

Câu 8: (2 điểm) Cho phân tích $x^7 + 1$ như sau

$$x^7 + 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$$

Hãy nêu tất cả các mã xyclic có thể có trên vành $Z_2[x]/x^7 + 1$.

TT	Đa thức sinh $g(x)$	Mã (n, k)	d_0
1	$1+x$	$(7,6)$	2
2	$1+x+x^3$	$(7,4)$	3
3	$1+x^2+x^3$	$(7,4)$	3
4	$1+x+x^2+x^4$	$(7,3)$	4
5	$1+x^2+x^3+x^4$	$(7,3)$	4
6	$\sum_{i=0}^6 x^i$	$(7,1)$	7
7	1	$(7,7)$	1

Câu 9: (4 điểm) Hãy thực hiện mã hoá Shannon – Fano cho nguồn rời rạc A sau:

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{32} & \frac{1}{32} & \frac{1}{32} & \frac{1}{64} & \frac{1}{64} \end{pmatrix}$$

Đánh giá hiệu quả của phép mã hoá này?

Hãy giải mã cho dãy bít nhận được có dạng: 101100111010101...

TT	a_i	$p(a_i)$	Từ mã $\alpha_i^{n_i}$					n_i
1	a_1	$1/4$	0	0				2
2	a_2	$1/4$	0	1				2
3	a_3	$1/8$	1	0	0			3
4	a_4	$1/8$	1	0	1			3
5	a_5	$1/8$	1	1	0			3
6	a_6	$1/32$	1	1	1	0	0	5
7	a_7	$1/32$	1	1	1	0	1	5
8	a_8	$1/32$	1	1	1	1	0	5
9	a_9	$1/64$	1	1	1	1	1	6
10	a_{10}	$1/64$	1	1	1	1	1	6

- **Đánh giá hiệu quả:**

$$\bar{n} = \sum_{i=1}^{10} p(a_i) n_i = 2.2 \cdot \frac{1}{4} + 3.3 \cdot \frac{1}{8} + 3.5 \cdot \frac{1}{32} + 2.6 \cdot \frac{1}{64}$$

$$= 1 + \frac{9}{8} + \frac{15}{32} + \frac{6}{32} = 2 \cdot \frac{25}{32} \text{ dấu}$$

$$H_1(A) = \sum_{i=1}^{10} p(a_i) \log \frac{1}{p(a_i)} = 2 \cdot \frac{1}{4} \cdot \log 4 + 3 \cdot \frac{1}{8} \log 8 + 3 \cdot \frac{1}{32} \log 32 + 2 \cdot \frac{1}{64} \log 64$$

$$= 2 \cdot \frac{25}{32} \text{ bit}$$

$\bar{n} = H_1(A) \Rightarrow$ phép mã hoá là tối ưu

- **Giải mã cho dãy bít nhận sau:**

$$\begin{array}{ccccccccccccc} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \dots \\ & \downarrow & & \downarrow & & & \downarrow & & & \downarrow & & \downarrow & & \downarrow & \\ a_4 & & a_3 & & & a_8 & & a_4 & & a_2 & & & & & \end{array}$$

Câu 10: (4 điểm) *Giả sử từ mã nhận được của mã cyclic (7,3) với đa thức sinh $g(x) = 1 + x + x^2 + x^4$ có dạng sau $v(x) = x^6 + x^5 + x^4 + x^3 + x^2$. Hãy sử dụng thuật toán chia dịch vòng để tìm được từ mã đã phát, biết rằng mã (7, 3) này có $d_0 = 4$.*

- **Bước 1:** Chia $v(x)$ cho $g(x)$

$$\begin{array}{r} x^6 + x^5 + x^4 + x^3 + x^2 \\ x^6 + x^4 + x^3 + x^2 \\ \hline x^5 \\ x^5 + x^3 + x^2 + x \\ \hline r_0(x) = x^3 + x^2 + x \end{array}$$

- **Bước 2:** $W(r_0(x)) = 3 > t = \left\lceil \frac{d-1}{2} \right\rceil = \left\lceil \frac{4-1}{2} \right\rceil = 1,5$

- **Bước 3:** (lần 1) $x \cdot v(x) = x^6 + x^5 + x^4 + x^3 + 1$

$$\begin{array}{r} x^6 + x^5 + x^4 + x^3 + 1 \\ x^6 + x^4 + x^3 + x^2 \\ \hline x^5 + x^2 + 1 \\ x^5 + x^3 + x^2 + x \\ \hline r_1(x) = x^3 + x + 1 \end{array}$$

$$W(r_1(x)) = 3 > t = 1 \Rightarrow \text{Bước 3}$$

- Bước 3: (lần 2): $x^2 \cdot v(x) = x^6 + x^5 + x^4 + x + 1$

$$\begin{array}{r} x^6 + x^5 + x^4 + x + 1 \\ x^6 + x^4 + x^3 + x^2 \\ \hline x^5 + x^3 + x^2 + x + 1 \\ x^5 + x^3 + x^2 + x \\ \hline r_2(x) = 1 \end{array}$$

$$W(r_2(x)) = 1 = t$$

- Bước 4:

$$\begin{aligned} \hat{f}(x) &= \frac{x^2 v(x) + r_2(x)}{x^2} = \frac{x^6 + x^5 + x^4 + x}{x^2} \\ \hat{f}(x) &= x^6 + x^4 + x^3 + x^2 \leftrightarrow 0011101_* \end{aligned}$$

Sai ở x^5 đã được sửa

Câu 11: (3 điểm) Hãy xác định tập tất cả các từ mã của bộ mã xyclic $(7, 3)$ có đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$.

Cho mã xyclic $(7, 3)$ có $g(x) = 1 + x^2 + x^3 + x^4$ ma trận sinh:

$$G = \begin{pmatrix} 1 + x^2 + x^3 + x^4 \\ x + x^3 + x^4 + x^5 \\ x^2 + x^4 + x^5 + x^6 \end{pmatrix} = \begin{pmatrix} 1011100 \\ 0101110 \\ 0010111 \end{pmatrix}$$

Tập $2^k = 2^3 = 8$ từ mã, trong đó 7 từ mã khác không là tập các tổ hợp tuyến tính các hàng của ma trận G

$$g(x) = 1 + x^2 + x^3 + x^4 \leftrightarrow 1011100$$

$$xg(x) = x + x^3 + x^4 + x^5 \leftrightarrow 0101110$$

$$x^2 g(x) = x^2 + x^4 + x^5 + x^6 \leftrightarrow 0010111$$

$$(1+x)g(x) = 1 + x + x^2 + x^5 \leftrightarrow 1110010$$

$$(1+x^2)g(x) = 1 + x^3 + x^5 + x^6 \leftrightarrow 1001011$$

$$(x+x^2)g(x) = x + x^2 + x^3 + x^6 \leftrightarrow 0111001$$

$$(1+x+x^2)g(x) = 1 + x + x^4 + x^6 \leftrightarrow 1100101$$

Câu 12: (3 điểm) Phát biểu và chứng minh giới hạn Hamming? Định nghĩa mã hoàn thiện?

- Giới hạn Hamming.

Với mã tuyến tính (n, k) , điều kiện cần để sử được t sai là:

$$\sum_{i=0}^t C_n^i \leq 2^{n-k}$$

Chứng minh: Số các kiểu sai có trọng số i là C_n^i

$$\text{Số các kiểu sai có trọng số } \leq t \text{ là: } C_n^0 + C_n^1 + \dots + C_n^t = \sum_{i=0}^t C_n^i$$

Số các trạng thái khác nhau của các dấu kiểm tra là: $2^r = 2^{n-k}$

Để sửa được sai, mỗi trạng thái của các dấu kiểm tra chỉ được gán tối đa cho 1 kiểu sai.

Vậy để sửa được tất cả các kiểu sai có trọng số $\leq t$ ta có: $\sum_{i=0}^t C_n^i \leq 2^{n-k}$

- Định nghĩa mã hoàn thiện.

Mã hoàn thiện là mã (n, k, d) đạt được giới hạn Hamming

Ví dụ: Mã $(7, 4)$ có $d = 3$

$$\text{Ta có: } t = \left[\frac{d-1}{2} \right] = 1$$

$$C_7^0 + C_7^1 \leq 2^{7-4} = 2^3 = 8$$

$$1 + 7 = 8$$

Vậy mã $(7, 4)$ là 1 mã hoàn thiện.

Câu 13: (4 điểm) Cho phân tích của $x^{15} + 1$ như sau :

$$x^{15} + 1 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$$

Hãy nêu tất cả các mã cyclotomic có độ dài 15 trên vành $Z_2[x]/x^{15} + 1$?

Đặt

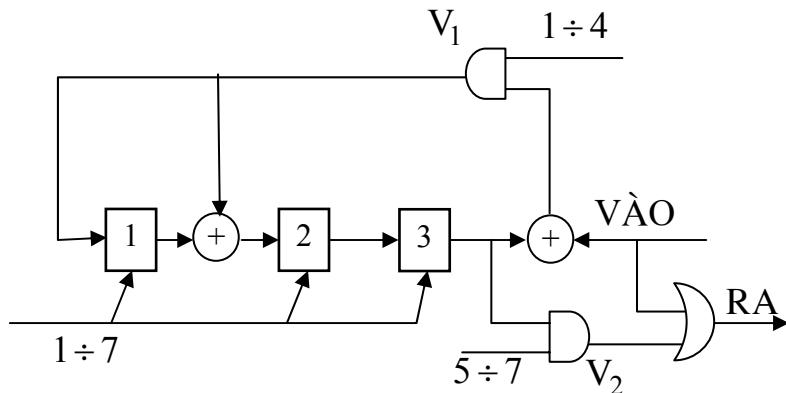
$$g_1(X) = 1 + X \quad g_2(X) = 1 + X + X^2$$

$$g_3(X) = 1 + X + X^4 \quad g_4(X) = 1 + X^3 + X^4$$

TT	Đa thức sinh	Mã (n,k)
1	$g_1(X)$	(15,14)
2	$g_2(X)$	(15,13)
3	$g_3(X)$	(15,11)
4	$g_4(X)$	(15,11)
5	$g_5(X)$	(15,11)
6	$g_1 \cdot g_2$	(15,12)
7	$g_1 \cdot g_3$	(15,10)
8	$g_1 \cdot g_4$	(15,10)
9	$g_1 \cdot g_5$	(15,10)
10	$g_2 \cdot g_3$	(15,9)
11	$g_2 \cdot (g_4)$	(15,9)
12	$g_2 \cdot g_5$	(15,9)
13	$g_3 \cdot g_4$	(15,7)
14	$g_3 \cdot g_5$	(15,7)
15	$g_4 \cdot g_5$	(15,7)
16	$g_1 \cdot g_2 \cdot g_3$	(15,8)
17	$g_1 \cdot g_2 \cdot g_4$	(15,8)
18	$g_1 \cdot g_2 \cdot g_5$	(15,8)
19	$g_2 \cdot g_3 \cdot g_4$	(15,5)
20	$g_2 \cdot g_3 \cdot g_5$	(15,5)
21	$g_1 \cdot g_3 \cdot g_4$	(15,6)
22	$g_1 \cdot g_3 \cdot g_5$	(15,6)
23	$g_1 \cdot g_4 \cdot g_5$	(15,6)
24	$g_2 \cdot g_4 \cdot g_5$	(15,5)
25	$g_3 \cdot g_4 \cdot g_5$	(15,3)
26	$g_1 \cdot g_2 \cdot g_3 \cdot g_4$	(15,4)
27	$g_1 \cdot g_2 \cdot g_3 \cdot g_5$	(15,4)
28	$g_1 \cdot g_2 \cdot g_4 \cdot g_5$	(15,4)
29	$g_2 \cdot g_3 \cdot g_4 \cdot g_5$	(15,1)
30	$g_1 \cdot g_3 \cdot g_4 \cdot g_5$	(15,2)
31	1	(15,15)

Câu 14:(3 điểm) Mô tả sơ đồ chức năng thiết bị mã hóa theo phương pháp chia cho mã cyclic hệ thống (7,4) có đa thức sinh $g(x)=1+x+x^3$. Tìm từ mã đầu ra của thiết bị này khi đa thức thông tin đầu vào $a(x)=1+x^3$.

Mã (7, 4) có $g(X)=1+X+X^3$



$$a(X)=1+X^3$$

$$a(X) \cdot x^{n-k} = X^6 + X^3$$

Xung nhịp	Vào	Trạng thái các ô nhớ			Ra
		1	2	1	
1	1	1	1	0	1
2	0	0	1	1	0
3	0	1	1	1	0
4	1	0	1	1	1
5	0	0	0	1	1
6	0	0	0	0	1
7	0	0	0	0	0

Từ mã ra $0\ 1\ 1\ 1\ 0\ 0\ 1 \leftrightarrow X + X^2 + X^3 + X^6$

Câu 15: (2 điểm) Mô tả vành đa thức với 2 phép toán cộng và nhân các đa thức theo modulo $x^n + 1$

Vành đa thức: $Z_2[x]/x^n + 1$

$$f(X) = \sum_{i=0}^{n-1} f_i x^i \quad ; \quad \deg f(X) \leq n-1 \quad ; \quad f_i \in GF(2)$$

$$\text{Phép cộng: } a(X) = \sum_{i=0}^{n-1} a_i x^i \quad ; \quad b(X) = \sum_{i=0}^{n-1} b_i x^i$$

$$c(X) = a(X) + b(X) = \sum_{i=0}^{n-1} c_i x^i \text{ trong đó } c_i = a_i + b_i \bmod 2$$

$$\text{Phép nhân: } a(X).b(X) = a(X).b(X) \bmod X^n + 1$$

Ta có $X^i \cdot X^j = X^{i+j \bmod n}$

TÓM TẮT CÔNG THỨC

- Độ đo thông tin:

$$\log \frac{1}{p(x_i)} = -\log p(x_i)$$

Đơn vị đo: bit (lb), nat (ln), hart (lg)

$$1 \text{ nat} = \log_2(e) = 1.4427 \text{ bit}$$

$$1 \text{ hart} = \log_2(10) = 3.3219 \text{ bit}$$

- Lượng tin riêng của 1 tin rời rạc:

$$I(x_i) = \log \frac{1}{p(x_i)} = -\log p(x_i) \quad (\text{đơn vị tt})$$

- Lượng tin riêng của 1 nguồn rời rạc:

$$I(X) = \sum_{i=0}^N p(x_i) \cdot \log \frac{1}{p(x_i)} = -\sum_{i=0}^N p(x_i) \cdot \log p(x_i)$$

- Entropy của 1 tin rời rạc:

$$H(x_i) = I(x_i) = -\log p(x_i)$$

- Entropy của 1 nguồn rời rạc:

$$H(X) = -\sum_{i=0}^N p(x_i) \cdot \log p(x_i)$$

- Entropy của nguồn liên tục:

$$H(X) = -\int_{-\infty}^{+\infty} w(x) \log w(x) dx; w(x) \text{ là hàm mđxs}$$

- Lượng tin riêng, entropy của tin rời rạc đồng thời:

$$I(x_i, y_j) = H(x_i, y_j) = -\log p(x_i, y_j)$$

- Lượng tin riêng, entropy của nguồn rời rạc đồng thời:

$$I(X, Y) = H(X, Y) = -\sum_{i,j} p(x_i, y_j) \cdot \log p(x_i, y_j)$$

- Entropy của nguồn liên tục đồng thời:

$$H(X, Y) = -\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log w(x, y) dx dy$$

- Entropy của tin rời rạc có điều kiện:

$$H(x_i|y_j) = \log \frac{1}{p(x_i|y_j)}$$

- Entropy của nguồn rời rạc có điều kiện:

$$H(X|Y) = -\sum_{i,j} p(x_i, y_j) \cdot \log p(x_i|y_j)$$

$$H(Y|X) = -\sum_{i,j} p(x_i, y_j) \cdot \log p(y_j|x_i)$$

- Entropy của nguồn liên tục có điều kiện:

$$H(X|Y) = -\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log w(x|y) dx dy$$

$$H(Y|X) = -\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log w(y|x) dx dy$$

- Tính chất của các entropy

+ Các entropy đều không âm.

+ Quan hệ giữa các entropy:

$$\begin{aligned} H(X, Y) &= H(X) + H(Y|X) \\ &= H(Y) + H(X|Y) \end{aligned}$$

+ Nếu X, Y độc lập thống kê:

$$H(Y|X) = H(Y); H(X|Y) = H(X)$$

$$+ 0 \leq H(X|Y) \leq H(X); 0 \leq H(Y|X) \leq H(Y)$$

+ Đổi với nguồn rời rạc có N tin: $H(X) \leq \log N$

- Lượng tin tương hỗ của 2 tin rời rạc:

$$\begin{aligned} I(x_i; y_j) &= H(x_i) - H(x_i|y_j) = \log \frac{p(x_i|y_j)}{p(x_i)} \\ &= \log \frac{p(x_i, y_j)}{p(x_i) \cdot p(y_j)} = \log \frac{p(y_j|x_i)}{p(y_j)} = H(y_j) - H(y_j|x_i) \\ I(x_i; y_j) &= I(x_i) + I(y_j) - I(x_i, y_j) \end{aligned}$$

- Lượng tin tương hỗ TB giữa 2 nguồn rời rạc:

$$\begin{aligned} I(X; Y) &= \sum_{i,j} p(x_i, y_j) \cdot \log \frac{p(x_i|y_j)}{p(x_i)} \\ &= \sum_{i,j} p(x_i, y_j) \cdot \log \frac{p(y_j|x_i)}{p(y_j)} \\ &= \sum_{i,j} p(x_i, y_j) \cdot \log \frac{p(x_i, y_j)}{p(x_i) \cdot p(y_j)} \\ &= H(X) - H(X|Y) = H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(X, Y) \end{aligned}$$

- Lượng tin tương hỗ giữa 2 nguồn liên tục:

$$\begin{aligned} I(X; Y) &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log \frac{w(x, y)}{w(x) \cdot w(y)} dx dy \\ &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log \frac{w(x|y)}{w(x)} dx dy \\ &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log \frac{w(y|x)}{w(y)} dx dy \end{aligned}$$

- Tốc độ lập tin của nguồn rời rạc:

$$R(X) = n_0 \cdot H(X) \left(\frac{\text{đv thông tin}}{\text{đv thời gian}} \right)$$

+ n_0 : số tin trung bình nguồn có thể tạo ra trong 1 đơn vị thời gian (tần số tạo tin của nguồn).

+ Nếu nguồn đồng nhất xác suất: $p(x_i) = \frac{1}{N} \quad \forall i$:

$$R = n_0 \cdot H(X)_{max} = n_0 \cdot \log N = F \cdot \log N$$

- Tốc độ lập tin của nguồn liên tục:

$$R = 2F_{max} \cdot H(X)$$

+ Đổi với nguồn có công suất định hưu hạn:

$$R = 2F_{Max} \cdot \log(x_{Max} - x_{Min})$$

+ Đổi với nguồn có công suất trung bình hưu hạn:

$$R = 2F_{Max} \cdot \log \sqrt{2\pi e P_x}$$

BÀI TẬP LÝ THUYẾT THÔNG TIN – IT4590

Bài 1. Cho nguồn tin $X = \{x_0, x_1, x_2, x_3, x_4, x_5\}$; $P_X = \left[\frac{1}{2}; \frac{1}{4}; \frac{1}{8}; \frac{1}{16}; \frac{1}{32}; \frac{1}{32}\right]$. Tính Entropy của nguồn X.

Entropy của nguồn X:

$$H(X) = - \sum_{i=0}^5 p(x_i) \log p(x_i) = - \left(\frac{1}{2} \cdot (-1) + \frac{1}{4} \cdot (-2) + \frac{1}{8} \cdot (-3) + \frac{1}{16} \cdot (-4) + \frac{1}{32} \cdot (-5) + \frac{1}{32} \cdot (-5) \right)$$
$$= 1.9375 \text{ bit/kh}$$

Bài 2. Cho 2 nguồn đồng thời X, Y với ma trận xác suất:

$$P(X, Y) = \begin{bmatrix} \frac{1}{3} & \frac{1}{6} \\ \frac{3}{6} & \frac{1}{3} \\ \frac{1}{6} & \frac{1}{3} \end{bmatrix}$$

Tính entropy đồng thời $H(X, Y)$ theo bit/tin, nat/tin, hart/tin.

GIẢI:

$$\begin{aligned} \text{Ta có: } H(X, Y) &= - \sum_{i,j} p(x_i, y_j) \cdot \log p(x_i, y_j) = \frac{1}{3} \cdot \log 3 + \frac{1}{6} \log 6 + \frac{1}{6} \log 6 + \frac{1}{3} \log 3 \\ &= 1.918 \text{ (bit/tin)} = 1.3297 \text{ (nat/tin)} = 0.5775 \text{ (hart/tin)} \end{aligned}$$

Nếu tính theo bit thì dùng $\log \text{cơ số} 2$, nat – cơ số e , hart – cơ số 10 .

Bài 3. Hệ thống truyền tin có nguồn tin vào X gồm 2 tin a, b đẳng xác suất. Hai tin này được mã hóa bằng mã nhị phân và truyền trên kênh nhị phân đổi xứng, nguồn ra Y, có xác suất truyền đúng là 0.8, xác suất truyền sai là 0.2.

- Tính các xác suất $P(X)$, $P(Y|X)$, $P(X|Y)$, $P(X, Y)$, $P(Y)$.
- Tính $H(X)$, $H(X, Y)$, $H(Y|X)$, $H(X|Y)$, $H(Y)$, $I(X; Y)$.

GIẢI:

- Giả sử nguồn ra Y gồm 2 tin y_0, y_1 , từ giả thiết suy ra:

$$p(y_0|a) = p(y_1|b) = 0.8; \quad p(y_0|b) = p(y_1|a) = 0.2$$

Vì nguồn vào X gồm 2 tin a, b đẳng xác suất nên $p(a) = p(b) = \frac{1}{2} \Rightarrow P(X) = \left(\frac{1}{2}; \frac{1}{2}\right)$

Xác suất $P(Y|X)$ xác định bởi ma trận:

$$P(Y|X) = \begin{bmatrix} p(y_0|a) & p(y_0|b) \\ p(y_1|a) & p(y_1|b) \end{bmatrix} = \begin{bmatrix} 0.8 & 0.2 \\ 0.2 & 0.8 \end{bmatrix}$$

Ma trận xác suất đồng thời:

$$P(X, Y) = \begin{bmatrix} p(a, y_0) & p(a, y_1) \\ p(b, y_0) & p(b, y_1) \end{bmatrix} = \begin{bmatrix} p(y_0|a)p(a) & p(y_1|a)p(a) \\ p(y_0|b)p(b) & p(y_1|b)p(b) \end{bmatrix} = \begin{bmatrix} 0.4 & 0.1 \\ 0.1 & 0.4 \end{bmatrix}$$

Từ đây tính được $P(Y)$ (cộng tương ứng theo cột): $p(y_0) = p(y_1) = 1/2$

Ma trận $P(X|Y)$ xác định bởi:

$$P(X|Y) = \begin{bmatrix} p(x_0|y_0) & p(x_0|y_1) \\ p(x_1|y_0) & p(x_1|y_1) \end{bmatrix} = \begin{bmatrix} \frac{p(x_0, y_0)}{p(y_0)} & \frac{p(x_0, y_1)}{p(y_1)} \\ \frac{p(x_1, y_0)}{p(y_0)} & \frac{p(x_1, y_1)}{p(y_1)} \end{bmatrix} = \begin{bmatrix} 0.8 & 0.2 \\ 0.2 & 0.8 \end{bmatrix}$$

- Dùng công thức dễ dàng tính được:

Ma Katz

$$H(X) = - \sum_i p(x_i) \cdot \log p(x_i) = 1; \quad H(Y) = - \sum_j p(y_j) \cdot \log p(y_j) = 1$$

$$H(X, Y) = - \sum_{i,j} p(x_i, y_j) \cdot \log p(x_i, y_j) = 2 \left(\frac{2}{5} \cdot \log \frac{5}{2} + \frac{1}{10} \cdot \log \frac{10}{1} \right) \approx 1.7219 \frac{\text{bit}}{\text{kh}}$$

$$H(X|Y) = H(X, Y) - H(Y) = 0.7219; \quad H(Y|X) = H(X, Y) - H(X) = 0.7219$$

$$I(X; Y) = H(X) + H(Y) - H(X, Y) = 0.2781 \text{ bit/kh}$$

Bài 4. Giả sử kênh nhị phân được sử dụng để truyền nguồn tin nhị phân đằng xác suất có ma trận kênh là:

$$P(Y|X) = \begin{bmatrix} 0.75 & 0.25 \\ 0.25 & 0.75 \end{bmatrix}$$

x_0, x_1 là 2 giá trị 0 và 1 trên đầu vào kênh; y_0, y_1 là 2 giá trị 0 và 1 trên đầu ra của kênh.

- a. Tính $P(X, Y)$, $P(X|Y)$, $P(Y)$.
- b. Tính $H(X, Y)$, $H(Y|X)$, $H(X|Y)$, $H(X)$, $H(Y)$.

GIẢI:

- a. Vì nguồn tin là nguồn nhị phân đằng xác suất nên: $p(x_0) = p(x_1) = 1/2$

Ma trận xác suất đồng thời:

$$\begin{aligned} P(X, Y) &= \begin{bmatrix} p(x_0, y_0) & p(x_0, y_1) \\ p(x_1, y_0) & p(x_1, y_1) \end{bmatrix} = \begin{bmatrix} p(y_0|x_0)p(x_0) & p(y_1|x_0)p(x_0) \\ p(y_0|x_1)p(x_1) & p(y_1|x_1)p(x_1) \end{bmatrix} \\ &= \begin{bmatrix} 0.75 \cdot 0.5 & 0.25 \cdot 0.5 \\ 0.25 \cdot 0.5 & 0.75 \cdot 0.5 \end{bmatrix} = \begin{bmatrix} \frac{3}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{3}{8} \end{bmatrix} \end{aligned}$$

Từ đây suy ra: $P(Y) = \left(\frac{1}{2}; \frac{1}{2}\right)$

Ma trận xác suất có điều kiện $P(X|Y)$:

$$P(X|Y) = \begin{bmatrix} p(x_0|y_0) & p(x_0|y_1) \\ p(x_1|y_0) & p(x_1|y_1) \end{bmatrix} = \begin{bmatrix} p(x_0, y_0)/p(y_0) & p(x_0, y_1)/p(y_1) \\ p(x_1, y_0)/p(y_0) & p(x_1, y_1)/p(y_1) \end{bmatrix} = \begin{bmatrix} 3/4 & 1/4 \\ 1/4 & 3/4 \end{bmatrix}$$

- b. Entropy của nguồn rời rạc đồng thời:

$$H(X, Y) = - \sum_{i,j} p(x_i, y_j) \cdot \log p(x_i, y_j) = 2 \left(\frac{3}{8} \cdot \log \frac{8}{3} + \frac{1}{8} \cdot \log \frac{8}{1} \right) \approx 1.8113 \text{ bit/tin}$$

Entropy có điều kiện:

$$\begin{aligned} H(X|Y) &= - \sum_{i,j} p(x_i, y_j) \log p(x_i|y_j) = 0.8113 \text{ bit/tin} \\ H(Y|X) &= - \sum_{i,j} p(x_i, y_j) \log p(y_j|x_i) = 0.8113 \text{ bit/tin} \end{aligned}$$

Entropy của nguồn rời rạc:

$$H(X) = - \sum_i p(x_i) \cdot \log p(x_i) = 1; \quad H(Y) = - \sum_j p(y_j) \cdot \log p(y_j) = 1$$

Bài 5. Cho nguồn $X = \{a, b, c\}$, xác suất $P(X) = \left(\frac{1}{3}; \frac{1}{3}; \frac{1}{3}\right)$. Ma trận xác suất truyền:

$$P(Y|X) = \begin{bmatrix} 2/3 & 1/6 & 1/6 \\ 1/6 & 2/3 & 1/6 \\ 1/6 & 1/6 & 2/3 \end{bmatrix}$$

Tính $H(X)$, $H(Y)$, $H(X, Y)$, $H(X|Y)$, $I(X; Y)$.

Ma Katz

GIẢI:

Từ giả thiết: $p(a) = p(b) = p(c) = 1/3$. Ma trận xác suất đồng thời $P(X, Y)$ xác định bởi:

$$P(X, Y) = \begin{bmatrix} p(a, y_0) & p(a, y_1) & p(a, y_2) \\ p(b, y_0) & p(b, y_1) & p(b, y_2) \\ p(c, y_0) & p(c, y_1) & p(c, y_2) \end{bmatrix} = \begin{bmatrix} p(y_0|a).p(a) & p(y_1|a).p(a) & p(y_2|a).p(a) \\ p(y_0|b).p(b) & p(y_1|b).p(b) & p(y_2|b).p(b) \\ p(y_0|c).p(c) & p(y_1|c).p(c) & p(y_2|c).p(c) \end{bmatrix}$$

$$= \begin{bmatrix} \frac{2}{3} \cdot \frac{1}{3} & \frac{1}{6} \cdot \frac{1}{3} & \frac{1}{6} \cdot \frac{1}{3} \\ \frac{1}{6} \cdot \frac{1}{3} & \frac{2}{3} \cdot \frac{1}{3} & \frac{1}{6} \cdot \frac{1}{3} \\ \frac{1}{6} \cdot \frac{1}{3} & \frac{1}{6} \cdot \frac{1}{3} & \frac{2}{3} \cdot \frac{1}{3} \end{bmatrix} = \begin{bmatrix} 2/9 & 1/18 & 1/18 \\ 1/18 & 2/9 & 1/18 \\ 1/18 & 1/18 & 2/9 \end{bmatrix}$$

Suy ra: $p(y_0) = p(y_1) = p(y_2) = \frac{2}{9} + \frac{1}{18} + \frac{1}{18} = \frac{1}{3}$.

Và:

$$P(X|Y) = \begin{bmatrix} p(a|y_0) & p(a|y_1) & p(a|y_2) \\ p(b|y_0) & p(b|y_1) & p(b|y_2) \\ p(c|y_0) & p(c|y_1) & p(c|y_2) \end{bmatrix} = \begin{bmatrix} p(a, y_0)/p(y_0) & p(a, y_1)/p(y_1) & p(a, y_2)/p(y_2) \\ p(b, y_0)/p(y_0) & p(b, y_1)/p(y_1) & p(b, y_2)/p(y_2) \\ p(c, y_0)/p(y_0) & p(c, y_1)/p(y_1) & p(c, y_2)/p(y_2) \end{bmatrix}$$

$$= \begin{bmatrix} 2/3 & 1/6 & 1/6 \\ 1/6 & 2/3 & 1/6 \\ 1/6 & 1/6 & 2/3 \end{bmatrix}$$

Tùy đó có:

+ Entropy đầu vào:

$$H(X) = - \sum_{j=0,1,2} p(x_j) \cdot \log p(x_j) = 3 \cdot \frac{1}{3} \cdot \log_2 3 = 1.585 \text{ bit/tin}$$

cuu duong than cong . com

+ Entropy đầu ra:

$$H(Y) = - \sum_{j=0,1,2} p(y_j) \cdot \log p(y_j) = 3 \cdot \frac{1}{3} \cdot \log_2 3 = 1.585 \text{ bit/tin}$$

+ Entropy của 2 nguồn đồng thời:

$$H(X, Y) = - \sum_{i,j} p(x_i, y_j) \cdot \log p(x_i, y_j) = 2.8366 \text{ bit/tin}$$

+ Entropy có điều kiện:

$$H(X|Y) = - \sum_{i,j} p(x_i, y_j) \cdot \log p(x_i|y_j) = 1.2516 \text{ bit/tin}$$

+ Lượng tin tương hỗ giữa 2 nguồn:

$$I(X; Y) = \sum_{i,j} p(x_i, y_j) \cdot \log \frac{p(y_j|x_i)}{p(y_j)} = 3 \cdot \left(\frac{2}{9} \cdot \log_2 \frac{\frac{2}{3}}{\frac{1}{3}} \right) + 6 \cdot \left(\frac{1}{18} \cdot \log_2 \frac{\frac{1}{6}}{\frac{1}{3}} \right) = \frac{1}{3} \text{ bit/tin}$$

cuu duong than cong . com

- Bài 6. Cho hệ thống điều khiển nhiệt độ của lò sấy thuốc lá. Biết người ta sử dụng 20 sensors nhiệt độ. Nhiệt độ trong lò được khống chế ở $40 \pm 0.01^\circ C$. Nhiệt độ đo các thiết bị cảm biến có thể làm cho nhiệt độ lò biến thiên từ $30 - 50^\circ C$. Yêu cầu sự sai khác nhiệt độ của lò so với nhiệt độ khống chế là trong thời gian ≤ 20 phút. Giả thiết giá trị nhiệt độ ngẫu nhiên, đồng xác suất. Tính thông lượng của kênh truyền từ sensors về trung tâm xử lý.

GIẢI:

Từ bài ra ta có, khoảng giá trị nhiệt độ mà lò có thể nhận là: 29.99; 50.01. Nhiệt độ là biến ngẫu nhiên liên tục tuân theo phân phối đều trong đoạn [29,99; 50,01] (do đã giả thiết giá trị nhiệt độ ngẫu nhiên và đáng xác suất).

Để thấy rằng đây là hệ thống truyền tin có công suất định hạn chế, ta xét với 1 kênh truyền ứng với 1 sensor: với thời gian khống chế là 20 phút, ta có tần suất tạo tin: $n_0 = 20.60 = 1200 \text{ kh/s}$

Tốc độ lập tin của nguồn 1 sensor là:

$$R_0 = n_0 \cdot \log(x_{Max} - x_{Min}) = 1200 \cdot \log(50.01 - 29.99) \approx 5188.04 \text{ bit/s}$$

Tốc độ lập tin của kênh truyền có 20 sensor là: $R = 20 \cdot R_0 = 20 * 5188.04 \approx 103 \text{ kBit/s}$

$$R = 20R_0 = 20.5188.04 \approx 103 \text{ Kbit/s}$$

Thông lượng của kênh truyền cần thiết kế sao cho bằng với tốc độ lập tin của nguồn trong trường hợp lí tưởng (khi kênh không nhiễu), như vậy:

$$C = R = 103 \text{ Kbit/s}$$

- Bài 7.** Cho hệ thống truyền hình theo chuẩn CCITT, khung ảnh có kích thước 3x4 được nhìn dưới góc nhìn $\alpha = 20^0$. Góc phân biệt độ chói (phân biệt đen trắng) là $\alpha_1 = 2'$; góc phân biệt màu là $\alpha_2 = 5'$. Mắt người có khả năng lưu ảnh trong 1/25 giây. Số ảnh gửi trong 1 giây là 50 ảnh. Ảnh được chia thành pixels thỏa mãn độ phân biệt và giả sử quét thông tin của ảnh theo đường ziczac (từ trái sang phải, từ trên xuống dưới). Thông tin về độ chói của 1 pixel là 1 trong 100 mức đáng xác suất. Thông tin về màu của 1 pixel là 1 giá trị bộ ba màu cơ bản R-G-B (mỗi màu cơ bản có 256 mức).
- a. Tính tốc độ lập tin của nguồn.

- b. Để truyền ảnh này bằng kênh điện thoại thì thời gian truyền 1 ảnh là bao nhiêu?

GIẢI:

- a. D

- b. D

Bài 8. Một tín hiệu được tạo thành từ những bit nhị phân. Do nhiều nên tín hiệu truyền đi có thể bị lỗi ở một vài bit. Qua thống kê, ta thấy $1/4$ số bit 0 truyền bị lỗi, và $1/5$ số bit 1 truyền bị lỗi. Biết rằng người ra truyền đi tổng cộng 500 bit 0 và 800 bit 1. Tính xác suất nhận đúng tín hiệu.

GIẢI:

Gọi X_0, X_1 lần lượt là sự kiện gắp được bit 0, bit 1. Gọi H là sự kiện nhận đúng tín hiệu.

Ta có: \bar{H} là sự kiện tín hiệu bị lỗi; $P(H) = 1 - P(\bar{H})$.

Tùy giả thiết suy ra:

$$P(X_0) = \frac{500}{500 + 800} = \frac{5}{13}; P(X_1) = \frac{800}{500 + 800} = \frac{8}{13}$$

Có $1/4$ số bit 0 truyền bị lỗi, $1/5$ số bit 1 truyền bị lỗi nên:

$$P(\bar{H}|X_0) = \frac{1}{4}; P(\bar{H}|X_1) = \frac{1}{5}$$

Theo công thức xác suất đầy đủ:

$$P(\bar{H}) = P(X_0) \cdot P(\bar{H}|X_0) + P(X_1) \cdot P(\bar{H}|X_1) = \frac{5}{13} \cdot \frac{1}{4} + \frac{8}{13} \cdot \frac{1}{5} = \frac{57}{260} \Rightarrow P(H) = \frac{203}{260} \approx 78.08\%$$

Vậy xác suất nhận đúng tín hiệu là $\approx 78.08\%$.

Bài 9. Cho nguồn liên tục X tuân theo phân phối đều trong đoạn $[0; a]$ ($a > 0$). Xác định $H(X)$ lần lượt trong các trường hợp $a = 1; a = \frac{1}{4}; a = 4$.

GIẢI:

Vì X tuân theo phân phối đều trong $[0; a]$ nên ta có hàm mật độ xác suất của biến ngẫu nhiên X :

$$w(x) = \begin{cases} \frac{1}{a}, & x \in [0; a] \\ 0, & \text{otherwise} \end{cases}$$

Do đó, entropy của nguồn liên tục X là:

$$H(X) = - \int_0^a w(x) \cdot \log w(x) dx = \int_0^a \frac{1}{a} \cdot \log a dx = \frac{1}{a} \cdot \log a \cdot \int_0^a dx = \frac{1}{a} \cdot \log(a) \cdot a = \log a$$

+ Với $a = 1$: $H(X) = \log_2 1 = 0$

+ Với $a = \frac{1}{4}$: $H(X) = \log_2 0.25 = -2$ (không tồn tại do entropy luôn không âm)

+ Với $a = 4$: $H(X) = \log_2 4 = 2$ (bit/tín).

Bài 10. Cho nguồn liên tục X có hàm mật độ xác suất xác định bởi:

$$w(x) = \begin{cases} \frac{e^{-x}}{\lambda}, & x > 0 \\ 0, & x \leq 0 \end{cases}$$

Xác định $H(X)$.

GIẢI:

Entropy của nguồn liên tục X xác định bởi:

$$H(X) = \int_{-\infty}^{+\infty} w(x) \cdot \log \frac{1}{w(x)} dx = \int_0^{+\infty} \frac{e^{-x}}{\lambda} \cdot \log \frac{\lambda}{e^{-x}} dx = \frac{1}{\lambda} \int_0^{+\infty} e^{-x} \cdot (\log \lambda - \log e^{-x}) dx = \dots$$

Bài 11. Cho kênh truyền tin gồm 4 đầu vào, 3 đầu ra có ma trận kênh là:

$$P(B, A) = \begin{bmatrix} 0.1 & 0.05 & 0.05 & 0.11 \\ 0.08 & 0.03 & 0.12 & 0.04 \\ 0.13 & 0.09 & 0.14 & 0.06 \end{bmatrix}$$

Ma Katz

- a. Xác định $H(A)$, $H(B)$, $H(A|B)$, $H(B|A)$, $I(A; B)$.
- b. Nguồn A có tốc độ ký hiệu là 100 kh/s. Xác định tốc độ lập tin của nguồn A, độ dư tương đối của nguồn A và thông lượng kênh truyền tin.

GIẢI:

- a. Từ ma trận kênh suy ra:

$$\begin{aligned} P(a_1) &= 0.1 + 0.08 + 0.13 = 0.31; P(a_2) = 0.05 + 0.03 + 0.09 = 0.17; \\ P(a_3) &= 0.05 + 0.12 + 0.14 = 0.31; P(a_4) = 0.11 + 0.04 + 0.06 = 0.21 \\ P(b_1) &= 0.1 + 0.05 + 0.05 + 0.11 = 0.31; P(b_2) = 0.08 + 0.03 + 0.12 + 0.04 = 0.27; \\ P(b_3) &= 0.13 + 0.09 + 0.14 + 0.06 = 0.42 \end{aligned}$$

Do đó:

$$\begin{aligned} H(A) &= -\sum_i P(a_i) \cdot \log P(a_i) \approx 1.955 \text{ bit/kh} \\ H(B) &= -\sum_j P(b_j) \cdot \log P(b_j) \approx 1.559 \text{ bit/kh} \end{aligned}$$

Entropy của 2 nguồn A, B đồng thời:

$$H(A, B) = -\sum_{i,j} P(a_i, b_j) \cdot \log P(a_i, b_j) \approx 3.447 \text{ bit/kh}$$

Suy ra:

$$\begin{aligned} H(A|B) &= H(A, B) - H(B) \approx 3.447 - 1.559 \approx 1.888 \text{ bit/kh} \\ H(B|A) &= H(A, B) - H(A) \approx 3.447 - 1.955 \approx 1.492 \text{ bit/kh} \end{aligned}$$

Lượng tin tương hỗ:

$$I(A; B) = H(A) + H(B) - H(A, B) = 1.955 + 1.559 - 3.447 = 0.067 \text{ bit/kh}$$

- b. Tốc độ lập tin của nguồn A:

$$R = n_0 \cdot H(A) = 100 \cdot 1.955 = 195,5 \frac{\text{bit}}{\text{s}}$$

Độ dư tương đối:

$$d = 1 - \frac{H(A)}{H(A)_{Max}} = 1 - \frac{1.955}{\log_2 4} = 2.25\%$$

($H(A)$ cực đại khi nguồn đãng xác suất, mà nguồn A gồm 4 tin nên có $H(A)_{max}$ như trên)

Thông lượng kênh:

$$C = n_0 \cdot I(A; B) = 100 \cdot 0.067 = 6.7 \text{ bit/s}$$

Bài 12. Xét một máy đánh chữ gồm 26 phím (từ A đến Z). Giả sử trong 1 giây có thể gõ được 20 phím.

- a. Trong trường hợp lí tưởng, máy đánh chữ hoạt động chính xác, khi đó thông lượng của kênh truyền bằng bao nhiêu ?
- b. Giả sử máy đánh chữ có thể bị lỗi như sau: ấn một phím không chỉ có thể in ra ký tự tương ứng mà còn cả ký tự kế tiếp với xác suất như nhau. Ví dụ ấn A thì có thể in ra A hoặc B, ấn Z thì có thể sinh ra Z hoặc A. Tính thông lượng kênh truyền.

GIẢI:

- a. Thông lượng của kênh truyền trong trường hợp lí tưởng:

$$C = n_0 \cdot H(A)_{Max} = 20 \cdot \log_2 26 \approx 94 \text{ bit/s}$$

- b. Khi gõ một phím, có hai ký tự có thể được in ra với khả năng như nhau, do đó $H(A|B) = \log_2 2$, thông lượng của kênh có nhiều:

$$C = n_0 \cdot I(A; B) = 20 \cdot (H(A) - H(A|B)) = 20 \cdot (\log_2 26 - \log_2 2) \approx 74 \text{ bit/s}$$

Ma Katz

Bài 13. Cho kênh nhị phân đối xứng có xác suất truyền lỗi là $p = 10^{-3}$.

- Tính lượng tin tương hỗ.
- Nếu chuỗi bit được truyền đi có chiều dài 1KB thì có bao nhiêu bit lỗi?

GIẢI:

- Gọi nguồn vào là X, nguồn ra là Y, do đây là kênh nhị phân đối xứng nên ta có:

$$X = \{x_0, x_1\}; Y = \{y_0, y_1\}; P(X) = \left(\frac{1}{2}; \frac{1}{2}\right)$$

Ma trận kênh:

$$P(Y|X) = \begin{bmatrix} p(y_0|x_0) & p(y_0|x_1) \\ p(y_1|x_0) & p(y_1|x_1) \end{bmatrix} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

Entropy có điều kiện:

$$H(Y|X) = 2(1-p).\log\frac{1}{1-p} + 2p.\log\frac{1}{p}$$

Ma trận xác suất đồng thời:

$$P(X, Y) = \begin{bmatrix} p(x_0, y_0) & p(x_0, y_1) \\ p(x_1, y_0) & p(x_1, y_1) \end{bmatrix} = \begin{bmatrix} (1-p)\cdot\frac{1}{2} & p\cdot\frac{1}{2} \\ p\cdot\frac{1}{2} & (1-p)\cdot\frac{1}{2} \end{bmatrix}$$

Suy ra:

$$P(y_0) = \sum_i p(x_i, y_j) = (1-p)\cdot\frac{1}{2} + p\cdot\frac{1}{2} = \frac{1}{2}; P(y_1) = \dots = \frac{1}{2}$$

Entropy nguồn ra Y: $H(Y) = -\sum_j p(y_j).\log p(y_j) = 1$

Lượng tin tương hỗ:

$$I(X; Y) = H(Y) - H(Y|X) = 1 - 2(1-p).\log\frac{1}{1-p} - 2p.\log\frac{1}{p} \approx 0,98859 \text{ bit/kh}$$

- Ta có:

$$1KB = 1024B = 8192 \text{ bit}$$

Xác suất truyền lỗi là $p = 10^{-3}$ nên số bit lỗi là:

$$8192 \cdot 10^{-3} = 9 \text{ bit} \text{ (lấy phần nguyên trên)}$$

Bài 14. Xét một bản tin bao gồm họ và tên của bạn, nơi sinh của bạn (gồm 3 thông tin: phường/xã, quận/huyện, tỉnh/TP), bao gồm các chữ cái không dấu, không phân biệt chữ hoa chữ thường, không có khoảng trắng. Nguồn X gồm các tin là các chữ cái khác nhau trong bản tin, xác suất của tin trong nguồn là tần suất xuất hiện của từng chữ cái trong bản tin.

- Viết bản tin ứng với thông tin của bạn.
- Xác định mô hình của nguồn X ứng với bản tin trên.
- Tính entropy của nguồn X.

GIẢI:

- Bản tin như sau:

LAMMINHANHQUYNHMAIHAIBATRUNGHANOI

Ma Katz

b. Số kí tự trong bản tin: $N = 33$

Nguồn X = {A, B, G, H, L, M, N, O, Q, R, T, U, Y}

Xác suất xuất hiện của từng tin trong nguồn:

$$P(A) = \frac{6}{33}; P(B) = \frac{1}{33}; P(G) = \frac{1}{33}; P(H) = \frac{5}{33}; P(L) = \frac{1}{33}; P(M) = \frac{3}{33}; P(N) = \frac{5}{33}; P(O) = \frac{1}{33}; \\ P(Q) = \frac{1}{33}; P(R) = \frac{1}{33}; P(T) = \frac{1}{33}; P(U) = \frac{2}{33}; P(Y) = \frac{1}{33}.$$

Suy ra:

$$P(X) = \left(\frac{6}{33}; \frac{1}{33}; \frac{1}{33}; \frac{5}{33}; \frac{1}{33}; \frac{3}{33}; \frac{5}{33}; \frac{1}{33}; \frac{1}{33}; \frac{1}{33}; \frac{2}{33}; \frac{1}{33} \right)$$

c. Entropy của nguồn X:

$$H(X) = \sum_{i=1}^{14} P(x_i) \cdot \log \frac{1}{P(x_i)} \\ = \frac{6}{33} \log_2 \frac{33}{6} + 8 \left(\frac{1}{33} \cdot \log_2 33 \right) + 2 \left(\frac{5}{33} \cdot \log_2 \frac{33}{5} \right) + \frac{3}{33} \log_2 11 + \frac{2}{33} \log_2 \frac{33}{2} \\ = 2.7402 \text{ bit/tin}$$

Bài 15. Nguồn X gồm 2 tin có xác suất lần lượt là p và $1 - p$, với $p = 1/q$, q là giá trị ứng với chữ cái đầu tiên trong họ của bạn, được cho trong bảng sau:

A=1; B=2; C=3; D=4; E=5; F=6; G=7; H=8; I=9; K=10; L=11; M=12; N=13; O=14; P=15;

Q=16; R=17; S=18; T=19; U=20; V=21; X=22; Y=23; Z=24

Ví dụ, nếu bạn họ Nguyễn, chữ cái đầu là N, khi đó $q = 13$; $p = 1/13$.

Ma trận kênh được cho bởi xác suất:

$$P(Y|X) = \begin{bmatrix} 2/3 & 1/3 \\ 1/3 & 2/3 \end{bmatrix}$$

Tính $H(X)$, $H(X,Y)$, $I(X;Y)$.

GIẢI:

Họ Lâm $\Rightarrow p = \frac{1}{11} \Rightarrow P(X) = \left(\frac{1}{11}; \frac{10}{11} \right)$

Ma trận xác suất đồng thời:

$$P(X,Y) = \begin{bmatrix} p(x_0, y_0) & p(x_0, y_1) \\ p(x_1, y_0) & p(x_1, y_1) \end{bmatrix} = \begin{bmatrix} p(y_0|x_0)p(x_0) & p(y_1|x_0)p(x_0) \\ p(y_0|x_1)p(x_1) & p(y_1|x_1)p(x_1) \end{bmatrix} = \begin{bmatrix} \frac{2}{3} \cdot \frac{1}{11} & \frac{1}{3} \cdot \frac{1}{11} \\ \frac{1}{3} \cdot \frac{10}{11} & \frac{2}{3} \cdot \frac{10}{11} \end{bmatrix} = \begin{bmatrix} \frac{2}{33} & \frac{1}{33} \\ \frac{10}{33} & \frac{20}{33} \end{bmatrix}$$

Từ đây suy ra: $P(y_0) = \frac{2}{33} + \frac{10}{33} = \frac{12}{33}$; $P(y_1) = \frac{1}{33} + \frac{20}{33} = \frac{21}{33}$; $P(Y) = \left(\frac{12}{33}; \frac{21}{33} \right)$

Entropy của nguồn X:

$$H(X) = - \sum_i p(x_i) \cdot \log p(x_i) = \frac{1}{11} \cdot \log_2 11 + \frac{10}{11} \cdot \log_2 \frac{11}{10} = 0.4395 \text{ bit/tin}$$

Entropy của nguồn rời rạc đồng thời:

$$H(X, Y) = - \sum_{i,j} p(x_i, y_j) \cdot \log p(x_i, y_j) = \frac{2}{33} \cdot \log_2 \frac{33}{2} + \frac{1}{33} \cdot \log_2 33 + \frac{10}{33} \cdot \log_2 \frac{33}{10} + \frac{20}{33} \cdot \log_2 \frac{33}{20} \\ = 1.3578 \frac{\text{bit}}{\text{tin}}$$

Entropy của nguồn ra Y:

$$H(Y) = - \sum_i p(y_i) \cdot \log p(y_i) = \frac{12}{33} \cdot \log_2 \frac{33}{12} + \frac{21}{33} \cdot \log_2 \frac{33}{21} = 0.9457 \frac{\text{bit}}{\text{tin}}$$

Ma Katz

Lượng tin tương hỗ:

$$I(X; Y) = H(X) + H(Y) - H(X, Y) = 0.0274 \frac{\text{bit}}{\text{tin}}$$

Bài 16. Cho bộ mã

a – 0000

b – 1002

c – 2100

d – 222

e – 2101

f – 1111

g – 0210

h – 0220

i – 2020

k – 120

l – 221

m – 212

a. Vẽ cây mã

b. Dựa vào cây mã để xác định các đặc tính và tham số cơ bản của bộ mã

GIẢI:

a. Cây mã tự vẽ:

b. Từ cây mã rút ra các đặc tính của bộ mã như sau:

+ Tính đều: bộ mã không đều do các từ mã có độ dài khác nhau (có từ mã độ dài 3, có từ mã độ dài 4).

+ Tính đầy: bộ mã chưa đầy do các nhánh của cây mã chưa tỏa ra hết.

+ Tính prefix: bộ mã có tính prefix do các nút biểu diễn từ mã đều là nút lá.

+ Tính phân tách được: do bộ mã có tính prefix nên cột 1 của bảng thử mã chẵn chẵn rõ ràng, nên bộ mã là phân tách được.

Các tham số của bộ mã:

+ Cơ số: từ các nút tỏa ra không quá 3 nhanh, nên bộ mã có cơ số 3.

+ Số từ mã: N = 12

Bài 17. Sử dụng bảng thử tính phân tách để kiểm tra xem bộ mã: 11, 201, 110, 021, 011, 1010 có phân tách được hay không? Hãy vẽ cây mã của bộ mã này.

GIẢI:

Bảng thử tính phân tách:

Từ mã	Cột 1	Cột 2
11	0 (11 là phần đầu 110)	21 (0 là phần đầu 021)
201		11 (0 là phần đầu 011) 11 trùng với từ mã
110		
021		
011		
1010		

Vậy bộ mã này không phân tách được.

Bài 18. Cho bản tin 001011011101001010110001. Mã hóa bản tin bằng thuật toán Lempel-Ziv.

GIẢI:

B1: Tách từ thông tin theo thứ tự từ điển:

Ma Katz

0-01-011-0111-010-0101-0110-00-1

B2: Lập từ điển mã hóa

STT	Từ	Từ cũ (STT từ cũ)	Kí tự lấy thêm
0	---	---	---
1	0	rỗng (0)	0
2	01	0 (1)	1
3	011	01 (2)	1
4	0111	011 (3)	1
5	010	01 (2)	0
6	0101	010 (5)	1
7	0110	011 (3)	0
8	00	0 (1)	0
9	1	rỗng (0)	1

B3: Mã hóa: từ mã gồm 2 phần là mã nhị phân cho số thứ tự của phần từ cũ + phần kí tự lấy thêm

Độ dài từ mã: $n = n_1 + n_2$; $n_1 = \lceil \log_2 N \rceil$ với N là số từ trong từ điển, n_2 là số kí tự lấy thêm (1)

Có: $N = 9 \Rightarrow n_1 = 4, n_2 = 1 \Rightarrow n = 5$

STT từ cũ ở dạng nhị phân	Kí tự lấy thêm	Từ mã
0000	0	00000
0001	1	00011
0010	1	00101
0011	1	00111
0010	0	00100
0101	1	01011
0011	0	00110
0001	0	00010
0000	1	00001

Bài 19. X

Bài 20. Hk

Bài 21.

cuu duong than cong . com

Ma Katz

KHOA KỸ THUẬT ĐIỆN TỬ 1**NGÂN HÀNG CÂU HỎI THI TỰ LUẬN****Tên học phần: Lý thuyết thông tin****Mã học phần: ELE 1319****Ngành đào tạo: ĐT-VT, Đ-ĐT, CNTT, ATTT****Trình độ đào tạo: Đại học****1. Ngân hàng câu hỏi thi****• Câu hỏi loại 1 điểm****Câu hỏi 1.1**

- Viết biểu thức tính lượng tin chứa trong tin x với xác suất $p(x)$.
- Cho $p(x)=1/16$. Tính lượng tin riêng chứa trong sự kiện x.

Câu hỏi 1.2

Cho nguồn rời rạc $\alpha = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 1/16 & 1/8 & 1/16 & 1/4 & 1/4 & 1/4 \end{pmatrix}$. Tính entropy của nguồn α .

Câu hỏi 1.3

Cho mã khối tuyến tính (5,2) có các từ mã được tạo ra theo quy luật sau:
 $m_1 m_2 \rightarrow c_1 c_2 c_3 c_4 c_5$ với:

$$c_1 = m_1; c_2 = m_2; c_3 = m_2; c_4 = m_1; c_5 = m_1 + m_2.$$

Tìm ma trận sinh G và ma trận kiểm tra H cho mã này.

Câu hỏi 1.4

Hãy viết các công thức mô tả mối quan hệ giữa các đại lượng $H(X)$, $H(Y)$, $H(X/Y)$, $H(Y/X)$, $H(X,Y)$ và $I(X;Y)$.

Câu hỏi 1.5

Cho mã Hamming (7,3). Mã này được sử dụng để phát hiện sai và có thể sửa được 1 lỗi đơn trong một từ mã 7 bit. Hỏi mã này sử dụng bao nhiêu bit để kiểm soát lỗi và bao nhiêu bit để truyền dữ liệu?

Câu hỏi 1.6

Chứng minh rằng nếu $g(x)$ là đa thức sinh của một mã cyclic (n,k) bất kỳ thì hệ số tự do $g_0 = 1$.

Câu hỏi 1.7

Nêu định nghĩa và tính chất của entropy của nguồn rời rạc A sau:

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_s \\ p(a_1) & p(a_2) & \dots & p(a_s) \end{pmatrix}$$

Câu hỏi 1.8

Nêu định nghĩa và tính chất của khoảng cách giữa 2 từ mã α_i^n và α_j^n của một bộ mã đều nhị phân $d(\alpha_i^n, \alpha_j^n)$.

Câu hỏi 1.9

Trọng số của một từ mã $\omega(\alpha_i^n)$: Định nghĩa và tính chất.

Câu hỏi 1.10

Phát biểu 2 định lý về khả năng phát hiện sai và khả năng sửa sai của một bộ mã đều nhị phân có độ thừa ($D>0$).

Câu hỏi 1.11

Tính entropy của nguồn rời rạc nhị phân sau:

$$A = \begin{pmatrix} a_1 & a_2 \\ p & 1-p \end{pmatrix}$$

Câu hỏi 1.12

Nêu định nghĩa và tính chất của Entropy có điều kiện $H(A/B)$.

Câu hỏi 1.13

Nêu định nghĩa và tính chất của lượng thông tin chéo.

Câu hỏi 1.14

Nêu định nghĩa và tính chất của khả năng thông qua của nguồn rời rạc.

Câu hỏi 1.15

Phát biểu định lý mã hóa thứ nhất của Shannon.

Câu hỏi 1.16

Nêu 2 yêu cầu của phép mã hóa tối ưu.

Câu hỏi 1.17

Định nghĩa mã cyclic

Câu hỏi 1.18

Trong phần mã hóa nguồn – Nén dữ liệu, chúng ta nói rằng các bộ mã sử dụng cho nén dữ liệu thường là các bộ mã không đều. Hãy giải thích một cách rõ ràng nhất có thể về kết luận trên.

Câu hỏi 1.19

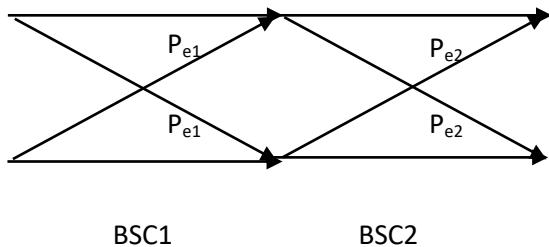
Cho biết mã hóa kênh được sử dụng trong hệ thống truyền tin với mục đích gì? Mã hóa kênh được xây dựng dựa trên nguyên tắc gì? Hãy ví dụ một số loại mã hóa kênh mà em biết.

Câu hỏi 1.20

Cho mã tuyến tính (7,4,3). Hãy tính xác suất thu sai 1 từ mã khi truyền tin qua kênh đối xứng nhị phân có xác suất thu sai 1 dấu mã là p_0 .

Câu hỏi 1.21

Cho hai kênh BSC được mắc nối tiếp như hình :



Xác suất lỗi bit khi truyền trên kênh BSC1 và BSC2 tương ứng là p_{e1} và p_{e2} . Tính xác suất lỗi bit khi truyền qua hai kênh này.

Câu hỏi 1.22

Tính entropy vi phân của biến ngẫu nhiên X có hàm phân bố xác suất:

$$p(x) = \begin{cases} a^{-1} & (0 \leq x \leq a) \\ 0 & (x \neq) \end{cases} \quad \text{với hai trường hợp:}$$

- a. $a=1$
- b. $a=4$

Câu hỏi 1.23

Cho một nguồn rời rạc không nhớ (DMS) như sau.

$$\mathbf{X} = \begin{pmatrix} x_1 & x_2 & x_3 \\ \frac{1}{2} & p & q \end{pmatrix}$$

- a. Tính lượng thông tin trung bình thông kê $H(X)$ của nguồn.
- b. Tìm giá trị cực đại của $H(X)$, chỉ rõ điều kiện để có cực đại này.

Câu hỏi 1.24

Cho kênh nhị phân đối xứng BSC với xác suất lỗi bit $p_e = 0,01$.

- a. Tính xác suất nhận được m bit sai trong n bit truyền đi ($m < n$).
- b. Tính xác suất nhận được chuỗi 15 bit trong đó có ít hơn 3 bit sai

- Câu hỏi loại 2 điểm

Câu hỏi 2.1

Cho nguồn rời rạc $\alpha = \begin{pmatrix} a & b & c & d & e & f & g \\ 0,01 & 0,24 & 0,05 & 0,2 & 0,47 & 0,01 & 0,02 \end{pmatrix}$.

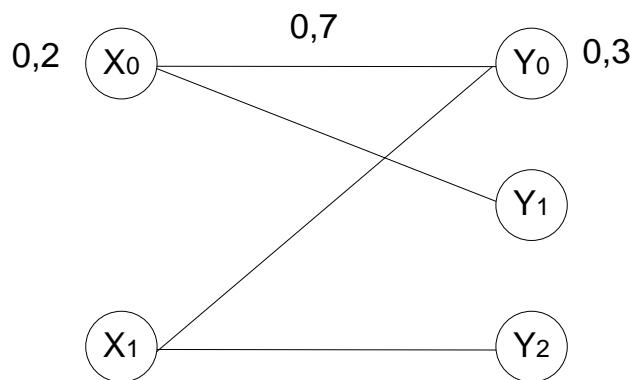
- Tính entropy của nguồn α
- Không cần tính, em hãy cho biết tin nào trong nguồn này chứa nhiều thông tin nhất và giải thích tại sao.

Câu hỏi 2.2

Tính Entropy vi phân của các quá trình ngẫu nhiên liên tục X có phân bố hàm số mũ $f(x) = \lambda e^{-\lambda x}$ ($x \geq 0$) với hằng số $\lambda > 0$.

Câu hỏi 2.3

Cho mô hình kênh rời rạc sau:



Điền các xác suất còn thiếu vào mô hình này.

Câu hỏi 2.4

Giả sử rằng X là một biến ngẫu nhiên có entropy $H(X)=8$ bit. Giả sử rằng $Y(X)$ là một hàm toán học thỏa mãn quan hệ ánh xạ 1-1.

- Hỏi entropy của Y bằng bao nhiêu?
- Entropy có điều kiện $H(Y/X)$ và $H(X/Y)$ bằng bao nhiêu?
- Entropy kết hợp của X và Y , $H(X,Y)$ bằng bao nhiêu?
- Gia sử rằng hàm xác định $Y(X)$ là không thể biến đổi ngược; nghĩa là các giá trị khác nhau của X có thể tương ứng với cùng một giá trị của $Y(X)$. Trong trường hợp đó, $H(Y)$ và $H(X/Y)$ sẽ thay đổi ra sao?

Câu hỏi 2.5

Một nguồn nhị phân độc lập với phân bố xác suất nguồn là 0,25 và 0,75 được truyền trên kênh nhị phân đối xứng với xác suất chuyển sai $p = 0,01$. Tính các đại lượng $H(X/Y)$ và $I(X;Y)$.

Câu hỏi 2.6

Trong một bộ tú lơ khơ 52 quân bài (không kể phăng teo), A rút ra 1 môt quân bài bất kỳ. Tính số câu hỏi trung bình tối thiểu mà B cần đặt ra cho A để xác định được quân bài mà A đã rút (câu hỏi có dạng trả lời có – không hoặc đúng – sai). Nêu thuật toán hỏi. Giả sử A đã rút ra 5 cờ, hãy nêu các câu hỏi cần thiết của B, các trả lời tương ứng của A và phán đoán tương ứng của B.

Câu hỏi 2.7

Có 2 hộp đựng bút chì, mỗi hộp đựng 20 bút chì. Hộp thứ nhất có 10 bút chì trắng, 5 bút chì đen và 5 bút chì đỏ. Hộp thứ 2 có 8 bút chì trắng, 8 bút chì đen, 4 bút chì đỏ. Thực hiện các 2 phép thử lấy hú hoạ một bút chì từ mỗi hộp. Hỏi rằng phép thử nào trong hai phép thử nói trên có độ bất định lớn hơn.

Câu hỏi 2.8

Một thiết bị điện tử gồm 16 khối có giá trị như nhau về độ tin cậy và được mắc nối tiếp. Giả sử có một khối hỏng. Hãy sử dụng một thiết bị đo tín hiệu ra để xác định khối hỏng. Tính số lần đo trung bình tối thiểu cần thực hiện bằng thiết bị đo này để có thể xác định được khối hỏng. Nêu thuật toán đo? Giả sử khối hỏng là khối thứ 12 hãy chỉ ra các lần đo cần thiết và kết quả đo tương ứng, các phán đoán đưa ra sau mỗi lần đo?

Câu hỏi 2.9

- Hãy cho biết nhược điểm của mã Huffman khi sử dụng cho mục đích nén dữ liệu?
- Cho hai bộ mã khác nhau dùng để mã hóa cho các ký tự a, b, c, d. Trong bảng, p_i là xác suất xuất hiện của mỗi ký tự. Hỏi chiều dài trung bình để mã hóa cho một ký tự trong mỗi bộ mã là bao nhiêu?

a_i	$c_1(a_i)$	$c_2(a_i)$	p_i
a	1000	0	$\frac{1}{2}$
b	0100	10	$\frac{1}{4}$
c	0010	110	$\frac{1}{8}$
d	0001	111	$\frac{1}{8}$

Câu hỏi 2.10

Có 8 chai nước mắm được đánh số từ 1 đến 8 trong đó có 1 chai làm từ cá ở gần nhà máy Formosa nên có chứa kim loại nặng. Kết quả phân tích một mẫu nước mắm chỉ cho biết chính xác mẫu đó có chứa kim loại nặng hay không. Giả thiết các chai nước mắm có xác suất chứa kim loại nặng như nhau. Hãy cho biết số lần phân tích mẫu nước mắm tối thiểu cần thực hiện? Hãy nêu thuật toán tổng quát để tạo mẫu nước mắm để phân tích? Giả sử chai số 7 chứa kim loại nặng, hãy chỉ ra cách tạo mẫu nước mắm trong các lần phân tích, kết quả tương ứng với mỗi lần phân tích và phán đoán đưa ra sau mỗi lần phân tích?

Câu hỏi 2.11

Một nguồn rời rạc gồm N tin tức $X = (x_1, x_2, \dots, x_{N-2}, x_{N-1}, x_N)$, với $N \geq 3$ và xác suất xuất hiện các tin tức tương ứng là $(2^{-1}, 2^{-2}, \dots, 2^{-(N-2)}, 2^{-(N-1)}, 2^{-(N-1)})$.

- Hãy xây dựng một mã Huffman nhị phân cho nguồn rời rạc trên.
- Hãy đánh giá hiệu quả của mã Huffman nhị phân vừa xây dựng được.

Câu hỏi 2.12

Cho một nguồn rời rạc với xác suất xuất hiện các sự kiện như sau ($1/3, 1/3, 1/4, 1/12$).

- Hãy xây dựng hai mã Huffman nhị phân có độ dài các từ mã tương ứng là (1, 2, 3, 3) và (2, 2, 2, 2).
- Hãy so sánh hiệu quả của hai mã Huffman nhị phân vừa xây dựng được.

Câu hỏi 2.13

Một thành phố nọ có 1% dân số là sinh viên. Trong số sinh viên có 50% là nam thanh niên. Số nam thanh niên trong thành phố là 32% dân số. Giả sử ta gặp một nam thanh niên. Hãy tính lượng thông tin chứa trong tin khi biết rằng đó là một nam sinh viên.

Câu hỏi 2.14

Một bình đựng gồm hai viên bi đen và ba viên bi trắng. Thực hiện lấy hai lần liên tiếp một cách ngẫu nhiên ra mỗi lần một viên bi, bi được lấy ra thì không bỏ lại vào bình. Quan sát thứ tự màu các viên bi lấy được. Gọi A là thông điệp (tin) cho chúng ta biết đã lấy được viên bi thứ hai là viên bi đen. Hãy tính lượng tin mang lại của thông điệp A.

Câu hỏi 2.15

Trong 27 đồng xu giống nhau có một đồng xu giả nhẹ hơn. Giả sử ta dùng một cân đĩa thăng bằng (có 2 đĩa cân) để xác định đồng xu giả. Hãy tính số lần cân trung bình tối thiểu để có thể xác định được đồng xu giả. Nêu thuật toán cân.

Câu hỏi 2.16

Cho mã khói tuyến tính (6,3) với ma trận sinh:

$$G_{3 \times 6} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

- Tìm ma trận kiểm tra H cho bộ mã.
- Tìm khoảng cách Hamming của bộ mã.

Câu hỏi 2.17

Cho mã cyclic (7,4) với đa thức sinh $g(x) = x^3 + x^2 + 1$.

- Hỏi mã này có khả năng phát hiện và sửa bao nhiêu sai?
- Tìm từ mã hệ thống đầu ra với đầu vào m=1111

Câu hỏi 2.18

Tính độ rộng giải thông của 1 kênh vô tuyến truyền hình truyền hình ảnh đen trắng với 5.10^5 điểm ảnh (pixel)/ảnh ; 25 ảnh/s và có 8 mức sáng đồng xác suất, với tỉ số tín/tạp $\frac{S}{N} = \frac{\sigma^2 s}{G_0 F} = 15$. Coi rằng ảnh vô tuyến truyền hình xem như 1 dạng tệp âm trắng.

Câu hỏi 2.19

Tín hiệu thoại có băng tần W=3,4kHz.

- Tính khả năng thông qua của kênh với điều kiện SNR=30dB
- Tính SNR tối thiểu cần thiết để kênh có thể truyền tín hiệu thoại số có tốc độ 4800bps.

Câu hỏi 2.20

Cho một mã khối tuyến tính có ma trận sinh G dưới đây:

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

- Tìm ma trận kiểm tra H.
- Hỏi mã này có khoảng cách Hamming bằng bao nhiêu?

Câu hỏi 2.21

Tìm mã cyclic (8,5) trên vành đa thức $Z_2[x]/x^8 + 1$. Tìm khoảng cách Hamming của mã đó.

Câu hỏi 2.22

Mã nào dưới đây là mã cyclic? Mã nào dưới đây tương đương với một mã cyclic?

- $C_1 = 0000; 1110; 1011; 0111; 1101$
- $C_2 = 111; 100; 010; 001$
- C_3 với ma trận sinh G_1 :

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

- C_4 với ma trận sinh G_2 :

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

Câu hỏi 2.23

Cho mã cyclic (7,4) có đa thức sinh $g(x) = 1 + x + x^3$. Hãy xây dựng ma trận sinh G và ma trận kiểm tra H ở dạng hệ thống của mã này.

Câu hỏi 2.24

Cho mã cyclic (15,8) có $g(x) = x^7 + x^6 + x^4 + 1$. Hãy xây dựng ma trận sinh G và ma trận kiểm tra H ở dạng hệ thống?

Câu hỏi 2.25

Xét mã khối nhị phân tuyến tính dạng hệ thống (5,2) có ma trận sinh có dạng :

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

- Liệt kê tất cả các từ mã của bộ mã.
- Bộ mã này có khả năng phát hiện và sửa bao nhiêu sai?

Câu hỏi 2.26

Hãy phân tích nhị thức $x^7 + 1$ thành tích của các đa thức bất khả qui và mô tả tất cả các mã cyclic có độ dài $n = 7$ trên vành đa thức $\mathbb{Z}_2[x]/x^7 + 1$

Câu hỏi 2.27

Hãy phân tích nhị thức $x^{15} + 1$ thành tích của các đa thức bất khả qui và tính số lượng các mã cyclic có độ dài $n = 15$ trên vành đa thức $\mathbb{Z}_2[x]/x^{15} + 1$.

Câu hỏi 2.28

Cho mã cyclic (7,4,3) có $g(x) = 1 + x + x^3$. Giả sử từ mã nhận được của bộ mã trên có dạng: $v(x) = x^6 + x^5 + x^4 + x^3 \leftrightarrow 0001111$. Hãy sử dụng thuật toán chia dịch vòng (bảy lõi) để tìm lại từ mã đã phát?

Câu hỏi 2.29

Cho $g(x) = x^8 + x^6 + x^4 + x^2 + 1$ là đa thức trên trường nhị phân.

- Tìm mã cyclic có tỉ lệ mã $r_i = k/n$ nhỏ nhất với đa thức sinh là $g(x)$.
- Tìm khoảng cách Hamming của bộ mã ở câu a.

Câu hỏi 2.30

Xét đa thức $g(x) = x + 1$ trên trường nhị phân.

- Chứng minh rằng đa thức này có thể tạo ra một mã cyclic với n bất kỳ. Tìm k tương ứng.
- Chọn một giá trị n bất kỳ. Tìm dạng hệ thống của G và H của mã được tạo nên bởi g(x).

- Câu hỏi loại 3 điểm

Câu hỏi 3.1

- Cho mã khối tuyến tính (n,k) có khoảng cách tối thiểu Hamming $d_0 = 8$. Hỏi mã này có khả năng phát hiện bao nhiêu sai và sửa bao nhiêu sai?

b. Một mã khói tuyến tính ($n,2$) có khoảng cách tối thiểu Hamming $d_0 = 5$. Xác định chiều dài n tối thiểu.

c. Cho biết có tồn tại một mã khói tuyến tính với các tham số $n = 15, k = 7, d_{min} = 5$ hay không?

Câu hỏi 3.2

Bộ mã nào dưới đây có thể hoặc không thể là mã Huffman của bất kỳ một nguồn rời rạc nào? Nếu không thể thì giải thích tại sao? Nếu có thể thì hãy cho ví dụ một nguồn tin tương ứng với bộ mã đó. Chú ý, mỗi câu đã liệt kê toàn bộ các từ mã (cách nhau bởi dấu phẩy) trong một bộ mã

- a. 0, 10, 111, 101
- b. 00, 010, 011, 10, 110
- c. 1, 000, 001, 010, 011

Câu hỏi 3.3

Cho mã khói tuyến tính (7,3) với ma trận sinh:

$$G_{3 \times 7} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

- a. Tìm ma trận kiểm tra H cho bộ mã.
- b. Tìm khoảng cách Hamming của bộ mã.
- c. Cho bản tin đầu vào $m=110$, tìm từ mã tương ứng.

Câu hỏi 3.4

Cho mã cyclic (7,3) với đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$.

- a. Xây dựng sơ đồ mã hóa theo phương pháp nhân.
- b. Tìm từ mã đầu ra với bản tin đầu vào $m=111$.
- c. Kiểm tra lại kết quả ở câu b) bằng thuật toán mã hóa theo phương pháp nhân.

Câu hỏi 3.5

- a. Tính entropy của một nguồn rời rạc không nhớ gồm 5 ký tự {A,B,C,D,E} với các xác suất tương ứng $\{1/2, 1/4, 1/8, 1/16, 1/16\}$.
- b. Xác định lượng thông tin chứa trong chuỗi phát đi DATED.
- c. Xây dựng cây mã hóa Huffman cho nguồn 5 ký tự này.

Câu hỏi 3.6

Xét một mã cyclic nhị phân tuyến tính hệ thống (9,3) có đa thức sinh $g(x) = 1 + x^3 + x^6$.

- a. Xây dựng mạch lập mã hệ thống cho mã theo thuật toán chia.

- b. Mô tả hoạt động của mạch, tìm từ mã đầu ra tương ứng với khối tin vào $a = 101$.
c. Kiểm tra kết quả câu b) bằng thuật toán tương ứng.

Câu hỏi 3.7

Xét một bộ mã khói nhị phân tuyến tính hệ thống $(8,4)$. Từ mã của bộ mã có dạng $c = a_1a_2a_3a_4a_5a_6a_7a_8$ trong đó các dấu mang tin là $a_1 \div a_4$, các dấu kiểm tra là $a_5 \div a_8$.

Biết các dấu kiểm tra được xác lập theo các mối quan hệ:

$$\begin{cases} a_5 = a_1 + a_2 + a_3 \\ a_6 = a_2 + a_3 + a_4 \\ a_7 = a_1 + a_2 + a_4 \\ a_8 = a_1 + a_2 + a_3 + a_4 \end{cases}$$

- a. Xây dựng ma trận sinh, ma trận kiểm tra cho mã này
b. Chứng minh rằng khoảng cách mã cực tiểu (khoảng cách mã tối thiểu, khoảng cách mã Hamming tối thiểu) của mã $d_{\min} = 3$.

Câu hỏi 3.8

Cho mã cyclic $(7,4)$ có đa thức sinh $g(x) = 1 + x + x^3$. Hãy mô tả sơ đồ chức năng của thiết bị mã hoá hệ thống cho bộ mã này theo phương pháp chia. Giả sử đa thức thông tin $a(x) = 1 + x^2 + x^3$. Hãy tìm từ mã ở đầu ra của thiết bị và kiểm tra lại bằng thuật toán 4 bước tạo từ mã hệ thống.

Câu hỏi 3.9

Cho mã cyclic $(7,3)$ có đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$. Hãy mô tả sơ đồ chức năng của thiết bị mã hoá hệ thống cho bộ mã này theo phương pháp nhân. Giả sử đa thức thông tin $a(x) = 1 + x^2$. Hãy tìm từ mã ở đầu ra của thiết bị và kiểm tra lại bằng thuật toán tạo từ mã hệ thống theo phương pháp nhân.

Câu hỏi 3.10

- a. Xây dựng một mã cyclic $(6,2)$ trên trường $Z_2[x]/x^6 + 1$.
b. Tìm ma trận G dạng hệ thống của mã này và tìm tất cả các từ mã của bộ mã.
c. Mã này có thể sửa bao nhiêu lỗi ?

Câu hỏi 3.11

Hãy thực hiện mã hoá Huffman cho nguồn rác A sau:

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ \frac{1}{2} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{32} & \frac{1}{32} & \frac{1}{32} & \frac{1}{64} & \frac{1}{128} & \frac{1}{128} \end{pmatrix}$$

Đánh giá hiệu quả của phép mã hoá

Hãy thực hiện giải mã cho dãy bit nhận được có dạng:

1 0 1 1 0 0 1 1 1 0 1 0 1....

Câu hỏi 3.12

Hãy thực hiện mã hóa Huffman cho nguồn rời rạc sau :

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 \\ 0,25 & 0,20 & 0,15 & 0,12 & 0,10 & 0,05 & 0,08 & 0,05 \end{pmatrix}$$

Đánh giá hiệu quả của phép mã hóa

Hãy thực hiện giải mã cho dãy bit nhận được có dạng : 11001110101000111...

Câu hỏi 3.13

Cho sơ đồ một kênh rời rạc không nhớ (DMC) trong đó nguồn phát X gồm hai tin x_1 và x_2 ; nguồn Y gồm hai tin y_1 và y_2 . Biết $p(x_1)=1/2$, $p(y_1/x_1)=1$, $p(y_1/x_2)=\alpha$, $p(y_2/x_1)=0$, $p(y_2/x_2)=1-\alpha$.

a. Hãy tính $H(X)$, $H(Y)$, $H(X,Y)$.

b. Tìm điều kiện của α để $H(Y)$ đạt giá trị cực đại. Khi đó, giá trị của $I(X,Y)$ bằng bao nhiêu (dẫn giải một cách chi tiết nhất có thể để có được kết quả đó).

Câu hỏi 3.14

Xét một kênh rời rạc nhị phân đối xứng không nhớ có ma trận kênh cho như sau:

$\begin{pmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{pmatrix}$. Biết đầu vào kênh là một nguồn rời rạc nhị phân không nhớ

$X = \{0,1\}$ với $p(0)=1/2$, đầu ra kênh là một nguồn rời rạc nhị phân không nhớ $Y = \{0,1\}$.

a. Hãy tính $H(X)$, $H(Y)$, $H(X,Y)$ và $I(X,Y)$.

b. Xác định các giá trị của ε để dung lượng của kênh đạt cực đại, và cực tiểu.

Câu hỏi 3.15

Cho kênh nhiễu Gaussian trắng cộng có đầu ra $Y = X + N$ ở đó X là đầu vào kênh và N là nhiễu với hàm phân bố xác suất Gauss $f(n) = \frac{1}{\sqrt{2\pi\sigma_n^2}} \cdot e^{-n^2/2\sigma_n^2}$. Giả sử X cũng có phân bố Gauss giống như N với $E(X) = 0$; $E(X^2) = \sigma_x^2$.

a. Tính entropy vi phân của nhiễu N

b. Tính lượng thông tin chéo $I(X,Y)$

Câu hỏi 3.16

Cho các nguồn rời rạc với bảng phân bố xác suất hợp $p(x_k, y_l)$ như bảng dưới đây.

Hãy tính $H(X)$, $H(Y)$, $H(X, Y)$, $H(X/Y)$, $H(Y/X)$, $I(X, Y)$.

	x_1	x_2	x_3	x_4
y_1	1/8	1/16	1/32	1/32
y_2	1/16	1/8	1/32	1/32
y_3	1/16	1/16	1/16	1/16
y_4	1/4	0	0	0

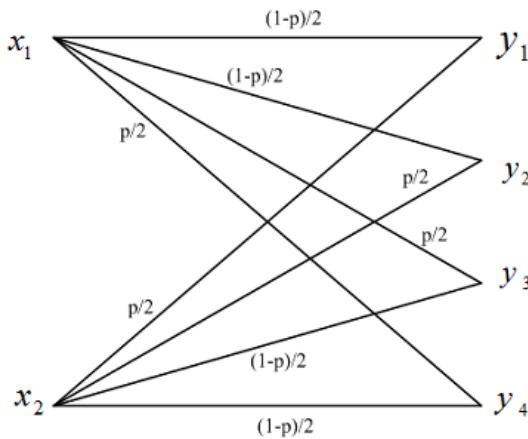
Câu hỏi 3.17

Các tín hiệu x_1 và x_2 có xác suất xuất hiện tiên nghiệm tương ứng là $p(x_1) = 3/4$ và $p(x_2) = 1/4$ được truyền theo kênh nhị phân rời rạc đối xứng không nhớ có nhiễu có xác suất chuyển sai $p_e = 1/8$. Tính:

- a. Lượng tin tức riêng có điều kiện $I(x_2 / y_2)$
- b. Lượng tin tức chéo $I(x_2; y_2)$
- c. Các đại lượng $H(X / y_1)$, $H(X)$, $H(X, Y)$, $H(X / Y)$, $I(X; Y)$

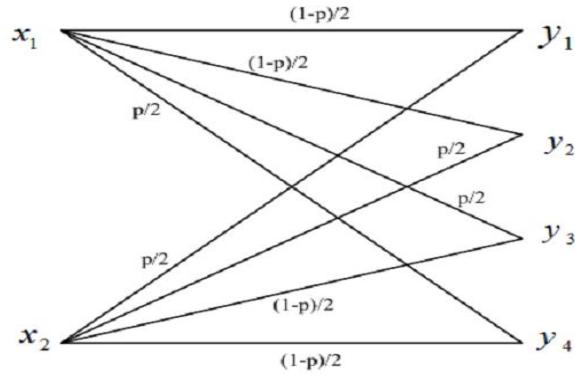
Câu hỏi 3.18

Cho sơ đồ kênh như hình vẽ. Biết $p(x_1) = 2/3$, hãy tính các đại lượng $H(X)$, $H(Y)$, $H(X, Y)$, $H(X/Y)$, $H(Y/X)$, $I(X, Y)$.



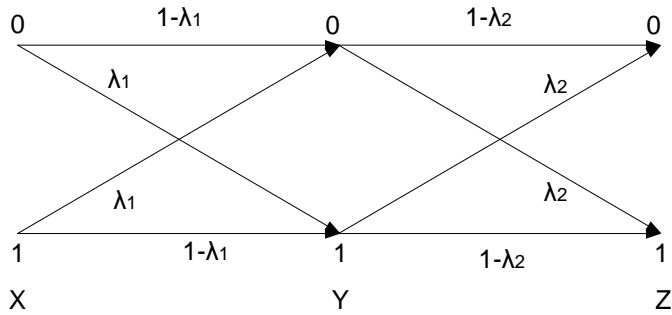
Câu hỏi 3.19

Cho sơ đồ kênh rời rạc không nhớ như hình vẽ, tính dung lượng của kênh :



Câu hỏi 3.20

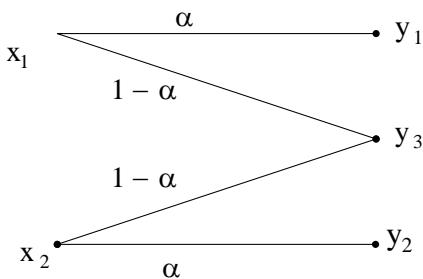
Tính khả năng thông qua C_1 của kênh $X \rightarrow Y$ và khả năng thông qua C_2 của kênh $Y \rightarrow Z$, khả năng thông qua C_3 của kênh $X \rightarrow Z$.



Câu hỏi 3.21

Cho sơ đồ kênh rời rạc không nhớ (DMC) như hình vẽ. Biết thời hạn các ký hiệu phát x_1 và x_2 đều là T_p .

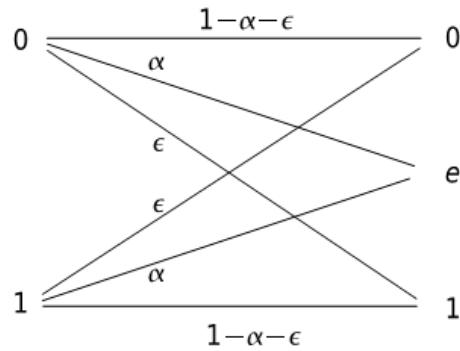
- Hãy tính dung lượng của kênh.
- Khảo sát sơ bộ (phác họa biến thiên) dung lượng kênh theo giá trị của α .
- Giải thích rõ ý nghĩa của các cực đại, cực tiểu (nếu có).



Câu hỏi 3.22

Cho sơ đồ kênh rời rạc không nhớ (DMC) như hình vẽ. Biết thời hạn các ký hiệu phát 0 và 1 đều là T_p .

- Hãy tính dung lượng của kênh.
- Trong trường hợp kênh nhị phân đối xứng ($\alpha = 0$) dung lượng kênh bằng bao nhiêu?



- **Câu hỏi loại 4 điểm**

Câu hỏi 4.1

Cho mã cyclic (7,3) có đa thức sinh $g(x) = 1 + x + x^2 + x^4$.

- Vẽ sơ đồ mã hóa cho bộ mã theo phương pháp nhân.
- Hỏi mã này có khả năng sửa được bao nhiêu sai?
- Gia sử phía phát phát đi từ mã 0011101. Do có lỗi nên phía thu nhận được từ mã bị sai ở vị trí x^5 . Hãy sử dụng thuật toán chia dịch vòng để tìm lại từ mã đã phát.

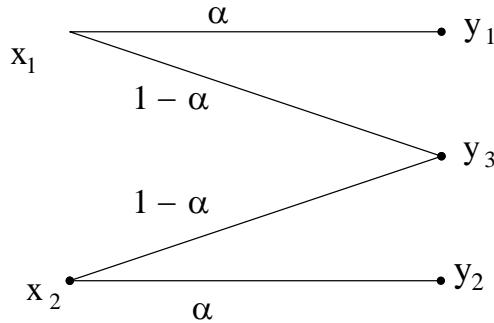
Câu hỏi 4.2

Cho mã cyclic (7,3) với đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$.

- Vẽ sơ đồ mã hóa theo phương pháp chia.
- Khoảng cách Hamming của bộ mã bằng bao nhiêu?
- Vẽ sơ đồ giải mã cho mã này theo phương pháp tổng kiểm tra trực giao.
- Gia sử phía thu nhận được từ mã $c = x^2 + x^4 + x^6 = 0010101$. Thực hiện giải mã để tìm ra từ mã đã phát.

Câu hỏi 4.3

Cho sơ đồ kênh rời rạc như hình vẽ dưới đây trong đó nguồn tín hiệu phát gồm $X = (x_1, x_2)$. Biết xác suất phát các tín hiệu $p(x_1) = p(x_2) = 0,5$.



- a. Hãy tính $H(X)$.
- b. Hãy tính $p(X = x_n, Y = y_m)$, với $n=1,2$ và $m=1,2,3$ để từ đó tính $H(X, Y)$ dưới dạng hàm số của α .
- c. Hãy tính $p(Y = y_m)$, với $m=1,2,3$ để từ đó tính $H(Y)$ dưới dạng hàm số của α .
- d. Hãy tính $I(X, Y)$ dưới dạng hàm số của α ? Hãy xác định giá trị của α khi $I(X, Y)$ đạt giá trị cực đại và khi $I(X, Y)$ đạt giá trị cực tiểu? Hãy cho biết ý nghĩa trực quan của các kênh ứng với các giá trị cực trị của $I(X, Y)$?

Câu hỏi 4.4

Gọi C là một mã cyclic nhị phân có độ dài từ mã là 15 bit và được tạo ra bởi đa thức sinh $g(x) = x^5 + x^3 + x + 1$

- a. Hãy chứng tỏ rằng $g(x)$ là một đa thức sinh hợp lệ của một mã cyclic có độ dài từ mã là 15 bit. Tìm đa thức kiểm tra của mã C.
- b. Tính số bit thông tin của mã C và số từ mã trong mã C.
- c. Tạo ma trận sinh và ma trận kiểm tra cho mã C.
- d. Vẽ sơ đồ hệ thống thiết bị thực hiện mã C theo phương pháp chia có dư. Hãy lập bảng phân tích hoạt động của hệ thống thiết bị để tính từ mã ứng với đa thức bản tin $x^9 + x^4 + x^2 + 1$.

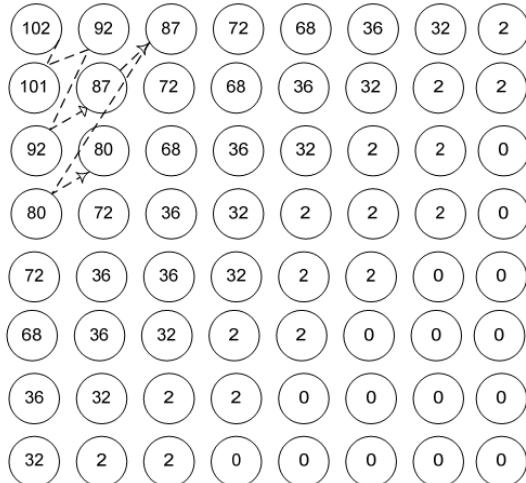
Câu hỏi 4.5

Một văn bản được viết từ các ký tự từ $x_1 \div x_{14}$, biết tần suất xuất hiện của các ký tự trong văn bản lần lượt là: 1200; 2400; 9600; 2400; 9600; 2400; 1200; 9600; 9600; 38400; 9600; 9600; 9600; 38400 (lần).

- a. Hãy thực hiện mã hóa Huffman cho văn bản.
- b. Đánh giá hiệu quả của phép mã hóa xây dựng trong câu a.
- c. Kiểm tra bất đẳng thức kép về độ dài trung bình từ mã. Có nhận xét gì?
- d. Hãy tính tỷ số nén thu được khi sử dụng bộ mã xây dựng ở phần a so với khi sử dụng mã ASCII với độ rộng 1 Byte.

Câu hỏi 4.6

Giá trị mức xám của một khối (block) ảnh 8×8 như trong ma trận sau.



Người ta cần thực hiện nén ảnh này. Một cách đơn giản nhất là áp dụng cách mã hóa các mức xám theo phương pháp mã hóa Huffman

- Hãy xây dựng bộ mã biểu diễn các giá trị mức xám của ảnh theo phương pháp mã hóa Huffman
- Đánh giá tính hiệu quả của bộ mã thu được.
- Giả sử ảnh được quét zig-zag theo đường đứt nét, với dãy bít nhận được như sau 0100110100111010101 ... hãy khôi phục lại các giá trị mức xám của gốc ảnh ứng với dãy bít đã cho.
- So với việc mã hóa trực tiếp các giá trị mức xám bằng mã ASCII (độ rộng 1Byte), phương pháp mã hóa Huffman tiết kiệm được bao nhiêu phần trăm dung lượng.

Câu hỏi 4.7

Cho mã cyclic (15,7) và đa thức $g(x) = x^8 + x^7 + x^6 + x^4 + 1$

- Chứng minh rằng $g(x)$ có thể là đa thức sinh của mã cyclic (15,7).
- Vẽ sơ đồ tạo mã theo phương pháp chia và giải thích ngắn gọn nguyên lý hoạt động của mạch.
- Xác định từ mã dạng hệ thống tương ứng với bản tin $m(x) = x^3 + x$ (theo thuật toán)
- Đa thức $d(x) = x^{14} + x^{12} + x^8 + x + 1$ có phải là một từ mã của bộ mã không? Vì sao?

Câu hỏi 4.8

Cho mã cyclic (15,8) và đa thức $g(x) = x^7 + x^6 + x^4 + 1$

- Chứng minh rằng $g(x)$ có thể là đa thức sinh của mã cyclic (15,8)
- Vẽ sơ đồ tạo mã theo phương pháp chia và giải thích ngắn gọn nguyên lý hoạt động của mạch.

c. Xác định từ mã dạng hệ thống tương ứng với bản tin $m(x) = x^2 + x$ (theo thuật toán).

d. Đa thức $d(x) = x^{10} + x^9 + x^8 + x + 1$ có phải là một từ mã của bộ mã không? Vì sao?

Câu hỏi 4.9

Cho $x^{15} + 1 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$.

a. Tìm mã cyclic (15,3) trên vành $\mathbb{Z}_2[x]/x^{15} + 1$.

b. Liệt kê 4 từ mã bất kỳ của bộ mã (15,3) trên vành này.

c. Vẽ sơ đồ tạo mã cyclic (15,3) bằng phương pháp chia.

d. Sử dụng thuật toán tìm từ mã đầu ra biết bản tin đầu vào $m = 1+x$

2. Đề xuất các phương án tổ hợp câu hỏi thi thành các đề thi:

Phương án 1:

- 1 câu 1 điểm
- 1 câu 2 điểm
- 1 câu 3 điểm
- 1 câu 4 điểm

Phương án 2:

- 2 câu 2 điểm (1 câu từ 2.1 đến 2.15 ; 1 câu từ 2.16 đến 2.30)
- 2 câu 3 điểm (1 câu từ 3.1 đến 3.12 ; 1 câu từ 3.13 đến 3.22)

3. Hướng dẫn cần thiết khác:

.....
...

Ngân hàng câu hỏi thi này đã được thông qua bộ môn và nhóm cán bộ giảng dạy học phần.

Hà Nội, ngày . . . tháng năm 2016

Q.Trưởng khoa

Trưởng bộ môn

Giảng viên chủ trì biên soạn

TS. Nguyễn Ngọc Minh

TS. Trương Trung Kiên

Nguyễn Thị Hương Thảo

Nguyễn Quốc Dinh