



Save to a Studylist

CHƯƠNG I: NHỮNG VẤN ĐỀ CHUNG VÀ NHÌNEM CƠ BẢN

1.1. VỊ TRÍ, VAI TRÒ VÀ SƠ LƯỢC LỊCH SỬ PHÁT TRIỂN CỦA “LÝ THUYẾT THÔNG TIN”

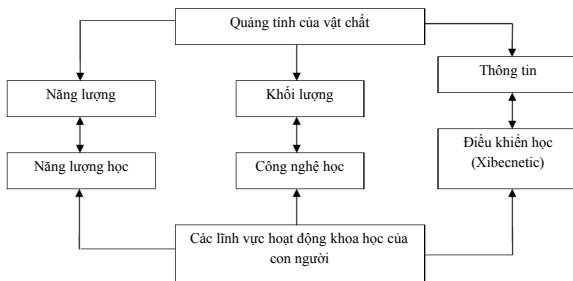
1.1.1. Vị trí, vai trò của Lý thuyết thông tin

Do sự phát triển mạnh mẽ của kỹ thuật tính toán và các hệ tự động, một ngành khoa học mới ra đời và phát triển nhanh chóng, đó là: “Lý thuyết thông tin”. Là một ngành khoa học nhưng nó không ngừng phát triển và thâm nhập vào nhiều ngành khoa học khác như: Toán; triết; hoá; Xibecnetic; lý thuyết hệ thống; lý thuyết và kỹ thuật thông tin liên lạc... và đã đạt được nhiều kết quả. Tuy vậy nó cũng còn nhiều vấn đề cần được giải quyết hoặc giải quyết hoàn chỉnh hơn.

Giáo trình “Lý thuyết thông tin” này (còn được gọi là “Cơ sở lý thuyết truyền tin”) chỉ là một bộ phận của lý thuyết thông tin chung – Nó là phần áp dụng của “Lý thuyết thông tin” vào kỹ thuật thông tin liên lạc.

Trong các quan hệ của Lý thuyết thông tin chung với các ngành khoa học khác nhau, ta phải đặc biệt kể đến mối quan hệ của nó với ngành Xibecnetic.

Mỗi quan hệ giữa các hoạt động khoa học của con người và các quang tính của vật chất được mô tả trên hình (1.1).



Hình 1.1. Quan hệ giữa hoạt động khoa học và quang tính của vật chất

- Năng lượng học: Là một ngành khoa học chuyên nghiên cứu các vấn đề liên quan tới các khái niệm thuộc về năng lượng. Mục đích của năng lượng học là làm giảm sự nặng nhọc của lao động chân tay và nâng cao hiệu suất lao động chân tay. Nhiệm vụ trung tâm của nó là tạo, truyền, thu, biến đổi, tích luỹ và xử lý năng lượng.

- Xibecnetic: Bao gồm các ngành khoa học chuyên nghiên cứu các vấn đề có liên quan đến khái niệm thông tin và tín hiệu. Mục đích của Xibecnetic là làm giảm sự nặng nhọc của trí óc và nâng cao hiệu suất lao động trí óc. Ngoài những vấn đề được xét trong Xibecnetic như đối tượng, mục đích, tối ưu hóa việc điều khiển, liên hệ ngược. Việc nghiên cứu các quá trình thông tin (như chọn, truyền, xử lý, lưu trữ và hiển thị thông tin) cũng là một vấn đề trung tâm của Xibecnetic. Chính vì vậy, lý thuyết và kỹ thuật thông tin chiếm vai trò rất quan trọng trong Xibecnetic.

- Công nghệ học: gồm các ngành khoa học tạo, biến đổi và xử lý các vật liệu mới. Công nghệ học phục vụ đặc lực cho Xibecnetic và năng lượng học. Không có công nghệ học hiện đại thì không thể có các ngành khoa học kỹ thuật hiện đại.

1.1.2. Sơ lược lịch sử phát triển

Người đặt viên gạch đầu tiên để xây dựng lý thuyết thông tin là Hartley R.V.L. Năm 1928, ông đã đưa ra số đo lượng thông tin là một khái niệm trung tâm của lý thuyết thông tin. Dựa vào khái niệm này, ta có thể so sánh định lượng các hệ truyền tin với nhau.

Năm 1933, V.A Kachenhicov chứng minh một loạt những luận điểm quan trọng của lý thuyết thông tin trong bài báo “Về khả năng thông qua của không trung và dây dẫn trong hệ thống liên lạc điện”.

Năm 1935, D.V Ageev đưa ra công trình “Lý thuyết tách tuyển tính”, trong đó ông phát biểu những nguyên tắc cơ bản về lý thuyết tách các tín hiệu.

Năm 1946, V.A Kachenhicov thông báo công trình “Lý thuyết thế chống nhiễu” đánh dấu một bước phát triển rất quan trọng của lý thuyết thông tin.

Trong hai năm 1948 – 1949, Shannon C.E công bố một loạt các công trình vĩ đại, đưa sự phát triển của lý thuyết thông tin lên một bước tiến mới chưa từng có. Trong các công trình này, nhờ việc đưa vào khái niệm lượng thông tin và tính đến cấu trúc thông kê của tin, ông đã chứng minh một loạt định lý về khả năng thông qua của kênh truyền tin khi có nhiễu và các định lý mã hoá. Những công trình này là nền tảng vững chắc của lý thuyết thông tin.

Ngày nay, lý thuyết thông tin phát triển theo hai hướng chủ yếu sau:

Lý thuyết thông tin toán học: Xây dựng những luận điểm thuận tuý toán học và những cơ sở toán học chặt chẽ của lý thuyết thông tin. Công hiến chủ yếu trong lĩnh vực này thuộc về các nhà bác học lỗi lạc như: N.Wiener, A. Feinstein, C.E Shannon, A.N. Kammôgorov, A.JA Khintrin.

Lý thuyết thông tin ứng dụng: (lý thuyết truyền tin)

Chuyên nghiên cứu các bài toán thực tế quan trọng do kỹ thuật liên lạc đặt ra có liên quan đến vấn đề chống nhiễu và nâng cao độ tin cậy của việc truyền tin. Các bác học C.E Shannon, S.O RiCe, D. Middleton, W. Peterson, A.A Khakevich, V. Kachenhicov đã có những công trình quý báu trong lĩnh vực này.

1.2. NHỮNG KHÁI NIỆM CƠ BẢN - SƠ ĐỒ HỆ TRUYỀN TIN VÀ NHIỆM VỤ CỦA NÓ

1.2.1. Các định nghĩa cơ bản

1.2.1.1. Thông tin

Định nghĩa: Thông tin là những tính chất xác định của vật chất mà con người (hoặc hệ thống kỹ thuật) nhận được từ thế giới vật chất bên ngoài hoặc từ những quá trình xảy ra trong bản thân nó.

Với định nghĩa này, mọi ngành khoa học là khám phá ra các cấu trúc thông qua việc thu thập, chế biến, xử lý thông tin. Ở đây “thông tin” là một danh từ chứ không phải là động từ để chỉ một hành vi tác động giữa hai đối tượng (người, máy) liên lạc với nhau.

Theo quan điểm triết học, thông tin là một quang tính của thế giới vật chất (tương tự như năng lượng, khối lượng). Thông tin không được tạo ra mà chỉ được sử dụng bởi hệ thu cảm. Thông tin tồn tại một cách khách quan, không phụ thuộc vào hệ thu cảm. Trong nghĩa khái quát nhất, thông tin là sự đa dạng. Sự đa dạng ở đây có thể hiểu theo nhiều nghĩa khác nhau: Tình ngẫu nhiên, trình độ tổ chức,...

1.2.1.2. Tin

Tin là dạng vật chất cụ thể để biểu diễn hoặc thể hiện thông tin. Có hai dạng: tin rời rạc và tin liên tục.

Ví dụ: Tầm ảnh, bản nhạc, bảng số liệu, bài nói,... là các tin.

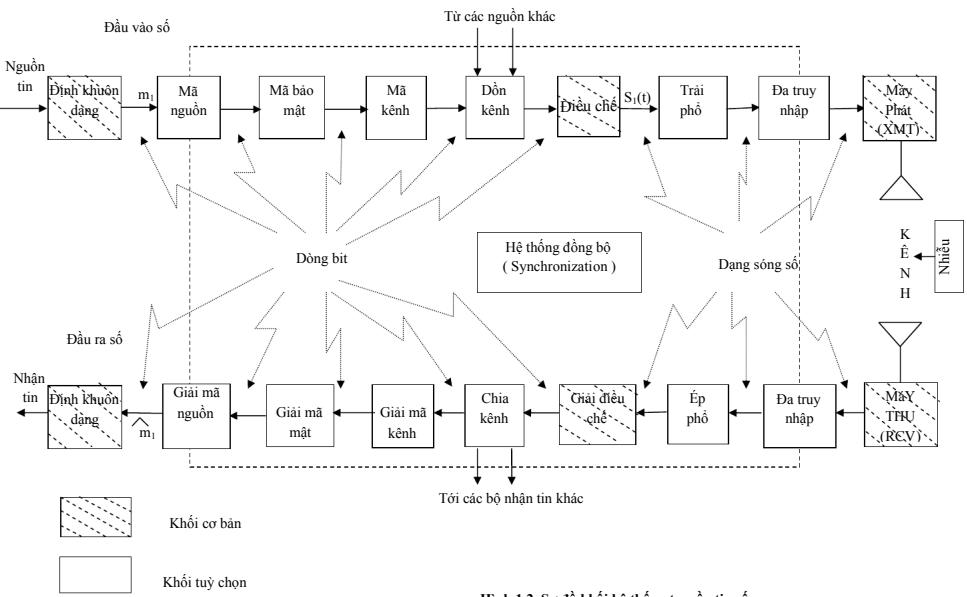
1.2.1.3. Tín hiệu

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

Chú ý: Không phải bản thân quá trình vật lý là tín hiệu, mà sự biến đổi các tham số riêng của quá trình vật lý mới là tín hiệu.

Các đặc trưng vật lý có thể là dòng điện, điện áp, ánh sáng, âm thanh, trường điện tử

1.2.2. Sơ đồ khái của hệ thống truyền tin số (Hình 1.2)



Hình 1.2. Sơ đồ khái hệ thống truyền tin số.

1.2.2.1. Nguồn tin

Nơi sản ra tin:

- Nếu tập tin là hữu hạn thì nguồn sinh ra nó được gọi là nguồn rời rạc.
- Nếu tập tin là vô hạn thì nguồn sinh ra nó được gọi là nguồn liên tục.

Nguồn tin có hai tính chất: Tính thống kê và tính hàm ý.

Với nguồn rời rạc, tính thống kê biểu hiện ở chỗ xác suất xuất hiện các tin là khác nhau.

Tính hàm ý biểu hiện ở chỗ xác suất xuất hiện của một tin nào đó sau một dãy tin khác nhau nào đó là khác nhau.

Ví dụ: $P(y|ta) \neq P(y|ba)$

1.2.2.2. Máy phát

Là thiết bị biến đổi tập tin thành tập tin hiệu tương ứng. Phép biến đổi này phải là đơn trị hai chiều (thì bên thu mới có thể “sao lại” được dung tin gửi đi). Trong trường hợp tổng quát, máy phát gồm hai khối chính.

- Thiết bị mã hoá: Làm ứng mỗi tin với một tổ hợp các ký hiệu đã chọn nhằm tăng mật độ, tăng khả năng chống nhiễu, tăng tốc độ truyền tin.

- Khối điều chế: Là thiết bị biến tập tin (đã hoặc không mã hoá) thành các tín hiệu để bức xạ vào không gian dưới dạng sóng điện từ cao tần. Về nguyên tắc, bất kỳ một máy phát nào cũng có khối này.

1.2.2.3. Đường truyền tin

Là môi trường vật lý, trong đó tín hiệu truyền đi từ máy phát sang máy thu. Trên đường truyền có những tác động làm mất năng lượng, làm mất thông tin của tín hiệu.

1.2.2.4. Máy thu

Là thiết bị lặp lại (sao lại) thông tin từ tín hiệu nhận được. Máy thu thực hiện phép biến đổi ngược lại với phép biến đổi ở máy phát: Biến tập tin hiệu thu được thành tập tin tương ứng.

Máy thu gồm hai khối:

- Giải điều chế: Biến đổi tín hiệu nhận được thành tín hiệu đã mã hoá.
- Giải mã: Biến đổi các tín hiệu đã mã hoá thành các tín hiệu tương ứng ban đầu (các tin của nguồn gửi đi).

1.2.2.5. Nhận tin

Có ba chức năng:

- Ghi giữ tin (ví dụ bộ nhớ của máy tính, băng ghi âm, ghi hình,...)
- Biểu thị tin: Làm cho các giác quan của con người hoặc các bộ cảm biến của máy thu cảm được để xử lý tin (ví dụ băng âm thanh, chữ số, hình ảnh,...)

- Xử lý tin: Biến đổi tin để đưa nó về dạng dễ sử dụng. Chức năng này có thể thực hiện bằng con người hoặc bằng máy.

1.2.2.6. Kênh truyền tin

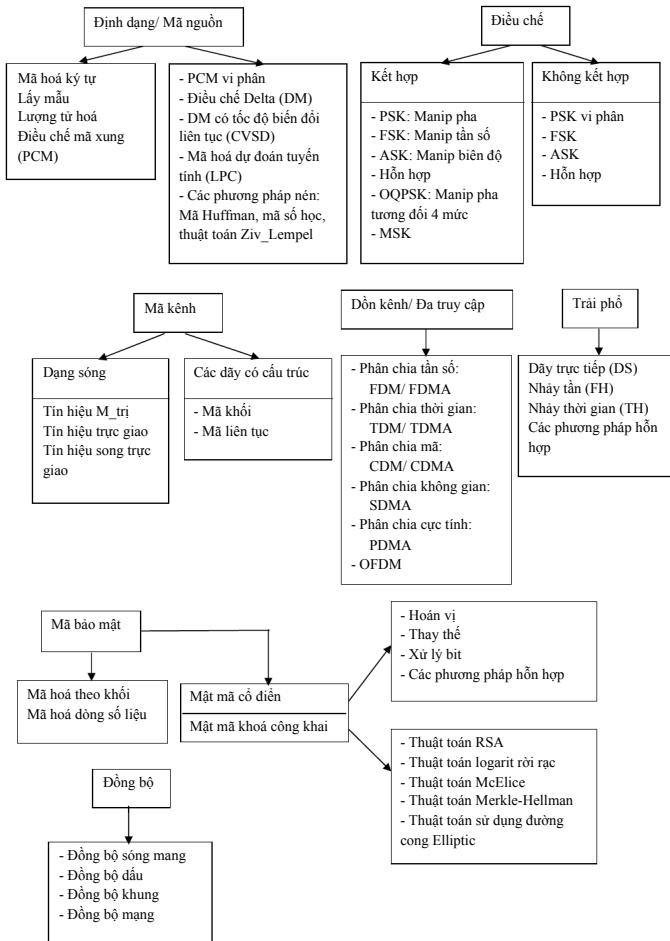
Là tập hợp các thiết bị kỹ thuật phục vụ cho việc truyền tin từ nguồn đến nơi nhận tin.

1.2.2.7. Nhiều

Là mọi yếu tố自然界 có ảnh hưởng xấu đến việc thu tin. Những yếu tố này tác động xấu đến tin truyền đi từ bên phát đến bên thu. Để cho gọn, ta gộp các yếu tố tác động đó vào một ô trên hình 1.2.

Hình 1.2 là sơ đồ khái quát nhất của một hệ truyền tin số. Nó có thể là: hệ thống vô tuyến điện thoại, vô tuyến điện báo, rada, vô tuyến truyền hình, hệ thống thông tin truyền số liệu, vô tuyến điều khiển từ xa.

1.2.2.8. Các phương pháp biến đổi thông tin số trong các khía cạnh chức năng của hệ thống



1.2.3. Những chỉ tiêu chất lượng cơ bản của một hệ truyền tin

1.2.3.1. Tính hữu hiệu

Thể hiện trên các mặt sau:

- Tốc độ truyền tin cao.
- Truyền được đồng thời nhiều tin khác nhau.
- Chi phí cho một bit thông tin thấp.

1.2.3.2. Độ tin cậy

Đảm bảo độ chính xác của việc thu nhận tin cao, xác suất thu sai (BER) thấp.

Hai chỉ tiêu trên mâu thuẫn nhau. Giải quyết mâu thuẫn trên là nhiệm vụ của lý thuyết thông tin.

1.2.3.3. An toàn

- Bí mật:
 - + Không thể khai thác thông tin trái phép.
 - + Chỉ có người nhận hợp lệ mới hiểu được thông tin.
- Xác thực: Gắn trách nhiệm của bên gửi – bên nhận với bản tin (chữ ký số).
- Toàn vẹn:
 - + Thông tin không bị bóp méo (cắt xén, xuyên tạc, sửa đổi).
 - + Thông tin được nhận phải nguyên vẹn cả về nội dung và hình thức.
- Khả dụng: Mọi tài nguyên và dịch vụ của hệ thống phải được cung cấp đầy đủ cho người dùng hợp pháp.

1.2.3.4. Đảm bảo chất lượng dịch vụ (QoS)

Đây là một chỉ tiêu rất quan trọng đặc biệt là đối với các dịch vụ thời gian thực, nhạy cảm với độ trễ (truyền tiếng nói, hình ảnh,)

CHƯƠNG II: TÍN HIỆU VÀ NHIỄU

2.1. TÍN HIỆU XÁC ĐỊNH VÀ CÁC ĐẶC TRUNG VẬT LÝ CỦA CHÚNG

Tín hiệu xác định thường được xem là một hàm xác định của biến thời gian t ($s(t)$). Hàm này có thể được mô tả bằng một biểu thức giải tích hoặc được mô tả bằng đồ thị. Một trong các đặc trưng vật lý quan trọng của tín hiệu là hàm mật độ phô biên độ phức $S(\omega)$. Với tín hiệu $s(t)$ khả tích tuyệt đối, ta có cặp biến đổi Fourier sau:

$$\dot{S}(\omega) = \int_{-\infty}^{\infty} s(t) e^{-j\omega t} dt \quad (2.1)$$

$$s(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \dot{S}(\omega) e^{j\omega t} d\omega \quad (2.2)$$

Sau đây là một số đặc trưng vật lý quen thuộc của tín hiệu:

- Thời hạn của tín hiệu (T): Thời hạn của tín hiệu là khoảng thời gian tồn tại của tín hiệu, trong khoảng này giá trị của tín hiệu không đồng nhất bằng 0.

- Bề rộng phô của tín hiệu (F): Đây là miền xác định bởi tần số khác không cao nhất của tín hiệu.

- Năng lượng của tín hiệu (E): Năng lượng của tín hiệu có thể tính theo miền thời gian hay miền tần số.

$$E = \int_{-\infty}^{\infty} s^2(t) dt = \frac{1}{2\pi} \int_{-\infty}^{\infty} |\dot{S}(\omega)|^2 d\omega \quad [J] \quad (2.3)$$

(Định lý Parseval)

- Công suất của tín hiệu (P):

$$P = \frac{E}{T} \quad [W]$$

2.2. TÍN HIỆU VÀ NHIỄU LÀ CÁC QUÁ TRÌNH NGẦU NHIÊN

2.2.1. Bản chất ngẫu nhiên của tín hiệu và nhiễu

Như đã xét ở trên, chúng ta coi tín hiệu là biểu hiện vật lý của tin (trong thông tin vô tuyến: dạng vật lý cuối cùng của tin là sóng điện tử). Quá trình vật lý mang tin diễn ra theo thời gian, do đó về mặt toán học thì khi có thể được, cách biểu diễn trực tiếp nhất cho tín hiệu là viết biểu thức của nó theo thời gian hay vẽ đồ thị thời gian của nó.

Trong lý thuyết cổ điển, dù tín hiệu tuân hoàn hoặc không tuân hoàn nhưng ta đều coi là đã biết trước và biểu diễn nó bằng một hàm tiền định của thời gian. Đó là quan niệm xác định về tín hiệu (tín hiệu tiền định). Tuy vậy, quan niệm này không phù hợp với thực tế. Thực vậy, tín hiệu tiền định không thể dùng vào việc truyền tin tức được. Với cách coi tín hiệu là biểu hiện vật lý của tín, nếu chúng ta hoàn toàn biết trước nó thì về mặt thông tin, việc nhận tín hiệu đó không có ý nghĩa gì. Nhưng nếu ta hoàn toàn không biết gì về tín hiệu truyền đi, thì ta không thể thực hiện nhận tin được. Bởi vì khi đó không có cái gì làm căn cứ để phân biệt tín hiệu với những cái không phải nó, đặc biệt là với các nhiễu. Như vậy, quan niệm hổ lý nhất là phải kể đến các đặc tính thống kê của tín hiệu, tức là phải coi tín hiệu là một quá trình ngẫu nhiên. Chúng ta sẽ gọi các tín hiệu xét theo quan điểm thống kê này là các tín hiệu ngẫu nhiên.

2.2.2. Định nghĩa và phân loại nhiễu

Trong quá trình truyền tin, tín hiệu luôn luôn bị nhiều yếu tố ngẫu nhiên tác động vào, làm mất mát một phần hoặc thậm chí có thể mất toàn bộ thông tin chứa trong nó. Những yếu tố ngẫu nhiên đó rất đa dạng, chúng có thể là những thay đổi ngẫu nhiên của các hằng số vật lý của môi trường truyền qua hoặc những loại trường điện từ cảm ứng trong công nghiệp, y học...vv... Trong vô tuyến điện, người ta gọi tất cả những yếu tố ngẫu nhiên ấy là các can nhiễu (hay nhiễu). Tóm lại, ta có thể coi nhiễu là tất cả những tín hiệu vô ích (tất nhiên là đối với hệ truyền tin ta xét) có ảnh hưởng xấu đến việc thu tin. Nguồn nhiễu có thể ở ngoài hoặc trong hệ. Nếu nhiễu xác định thì việc chống nó không có khó khăn gì về mặt nguyên tắc. Ví dụ như người ta đã có những biện pháp để chống ôn do dòng xoay chiều gây ra trong các máy khuếch đại âm tần, người ta cũng biết rõ những cách chống sự nhiễu lẫn nhau giữa các dải tần và tần số. Các loại nhiễu này không đáng ngại.

Chú ý:

Cần phân biệt nhiễu với sự méo gãy ra bởi đặc tính tần số và đặc tính thời gian của các thiết bị, kênh truyền... (méo tần số và méo phi tần số). Về mặt nguyên tắc, ta có thể khắc phục được chúng bằng cách hiệu chỉnh.

Nhiều đáng lo ngại nhất vẫn là các nhiễu ngẫu nhiên. Cho đến nay, việc chống các nhiễu ngẫu nhiên vẫn gặp những khó khăn lớn cao về mặt lý luận lẫn về mặt thực hiện kỹ thuật. Do đó, trong giáo trình này ta chỉ đề cập đến một dạng nào đó (sau này sẽ thấy ở đây thường xét nhất là nhiễu cộng, chuẩn) của nhiễu ngẫu nhiên.

Việc chia thành các loại (dạng) nhiễu khác nhau có thể làm theo các dấu hiệu sau:

1. Theo bề rộng phổ của nhiễu: có nhiễu giải rộng (phổ rộng như phổ của ánh sáng trắng gọi là tạp âm trắng), nhiễu giải hẹp (gọi là tạp âm màu).
2. Theo quy luật biến thiên thời gian của nhiễu: có nhiễu rời rạc và nhiễu liên tục.
3. Theo phương thức mà nhiễu tác động lên tín hiệu: có nhiễu cộng và nhiễu nhân.
4. Theo cách bức xạ của nhiễu: có nhiễu thụ động và nhiễu tích cực.

Nhiều thụ động là các tia phản xạ từ các mục tiêu già hoặc từ địa vật trở về dài ta xét khi các tia sóng của nó dập vào chúng. Nhiều tích cực (chủ động) do một nguồn bức xạ năng lượng (các dải hoặc các hệ thống lân cận) hoặc máy phát nhiễu của đối phương chia vào dài hoặc hệ thống đang xét.

5. Theo nguồn gốc phát sinh: có nhiều công nghiệp, nhiễu khí quyển, nhiễu vũ trụ...vv...

Trong giáo trình này khi nói về nhiễu, ta chỉ nói theo phương thức tác động của nhiễu lên tín hiệu, tức là chỉ nói đến nhiễu nhân hoặc nhiễu cộng.

Về mặt toán học, tác động của nhiễu cộng lên tín hiệu được biểu diễn bởi hệ thức sau:

$$u(t) = s(t) + n(t) \quad (2.4)$$

$s(t)$ là tín hiệu gửi đi

$u(t)$ là tín hiệu thu được

$n(t)$ là nhiễu cộng

Còn nhiễu nhân được biểu diễn bởi:

$$u(t) = \mu(t).s(t) \quad (2.5)$$

$\mu(t)$: nhiễu nhân, là một quá trình ngẫu nhiên. Hiện tượng gây nên bởi nhiễu nhân gọi là suy lạc (fading).

Tổng quát, khi tín hiệu chịu tác động đồng thời của cả nhiễu cộng và nhiễu nhân thì:

$$u(t) = \mu(t).s(t) + n(t) \quad (2.6)$$

Ở đây, ta đã coi hệ số truyền của kênh bằng đơn vị và bỏ qua thời gian giữ chậm tín hiệu của kênh truyền. Nếu kể đến thời gian giữ chậm τ của kênh truyền thi (2.6) có dạng:

$$u(t) = \mu(t).s(t-\tau) + n(t) \quad (2.7)$$

2.3. CÁC ĐẶC TRUNG THỐNG KÊ CỦA TÍN HIỆU NGẪU NHIÊN VÀ NHIỄU

2.3.1. Các đặc trưng thống kê

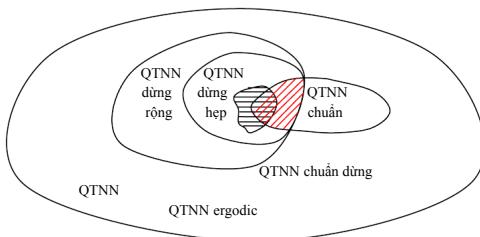
Theo quan điểm thống kê, tín hiệu và nhiễu được coi là các quá trình ngẫu nhiên. Đặc trưng cho các quá trình ngẫu nhiên chính là các quy luật thống kê (các hàm phân bố và mật độ phân bố) và các đặc trưng thống kê (kỷ vọng, phương sai, hàm tự tương quan, hàm tương quan). Các quy luật thống kê và các đặc trưng thống kê đã được nghiên cứu trong lý thuyết hàm ngẫu nhiên, vì vậy ở đây ta sẽ không nhắc lại.

Trong lớp các quá trình ngẫu nhiên, đặc biệt quan trọng là các quá trình ngẫu nhiên sau:

- Quá trình ngẫu nhiên dừng (theo nghĩa hẹp và theo nghĩa rộng) và quá trình ngẫu nhiên chuẩn dừng.

- Quá trình ngẫu nhiên ergodic

Ta minh họa chúng theo lược đồ sau:



Hình 2.1

Trong những đặc trưng thống kê của các quá trình ngẫu nhiên, hàm tự tương quan và hàm tương quan là những đặc trưng quan trọng nhất. Theo định nghĩa, hàm tự tương quan sẽ bằng:

$$\begin{aligned} R_x(t_1, t_2) &\stackrel{\Delta}{=} M\left\{[X(t_1) - m_x(t_1)][X(t_2) - m_x(t_2)]\right\} \\ &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} [x(t_1) - m_x(t_1)][x(t_2) - m_x(t_2)] W_2(x_1, x_2, t_1, t_2) dx_1 dx_2 \end{aligned} \quad (2.8)$$

$R_x(t_1, t_2)$ đặc trưng cho sự phụ thuộc thống kê giữa hai giá trị ở hai thời điểm thuộc cùng một thể hiện của quá trình ngẫu nhiên.

$W_2(x_1, x_2, t_1, t_2)$ là hàm mật độ phân bố xác suất hai chiều của hai giá trị của quá trình ngẫu nhiên ở hai thời điểm t_1 và t_2 .

Khi $t_1 = t_2$ thì (2.8) trở thành:

$$R_x(t_1, t_2) = M\left\{[X(t) - m_x(t)]^2\right\} = D_x(t) \quad (2.9)$$

Như vậy, phuong sai là trường hợp riêng của hàm tự tương quan khi hai thời điểm xét trùng nhau.

Đối với dễ tiện tính toán và so sánh, người ta dùng hàm tự tương quan chuẩn hóa được định nghĩa bởi công thức:

$$\begin{aligned} \tau_x(t_1, t_2) &\stackrel{\Delta}{=} \frac{R_x(t_1, t_2)}{\sqrt{R_x(t_1, t_1)R_x(t_2, t_2)}} = \frac{R_x(t_1, t_2)}{\sqrt{D_x(t_1)D_x(t_2)}} \\ &= \frac{R_x(t_1, t_2)}{\tau_x(t_1)\tau_x(t_2)} \end{aligned} \quad (2.10)$$

Dễ dàng thấy rằng: $|\tau_x(t_1, t_2)| \leq 1$.

2.3.2. Khoảng tương quan

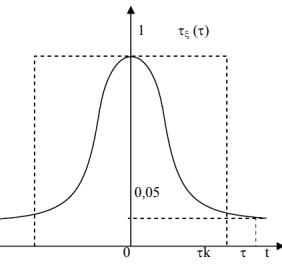
Khoảng tương quan cũng là một đặc trưng khá quan trọng. Ta thấy rằng hai giá trị của một quá trình ngẫu nhiên $\xi(t)$ chỉ tương quan với nhau khi khoảng cách τ giữa hai thời điểm xét là hữu hạn. Khi $\tau \rightarrow \infty$, thì coi như hai giá trị ấy không tương quan với nhau nữa. Tuy vậy, trong thực tế, đối với hầu hết các quá trình ngẫu nhiên chỉ cần τ đủ lớn thì sự tương quan giữa hai giá trị của quá trình đã mất. Do đó, đối với tính toán thực tế người ta định nghĩa khoảng (thời gian) tương quan như sau:

Dịnh nghĩa 1:

Khoảng tương quan τ_K là khoảng thời gian trong đó $\tau_\xi(\tau)$ không nhỏ hơn 0,05. (hình vẽ 2.2). Như vậy, $\forall \tau > \tau_K$ thì xem như hết tương quan.

Nếu cho biểu thức giải tích của $\tau_\xi(\tau)$ thì τ_K được tính như sau:

$$\tau_K = \frac{1}{2} \int_{-\infty}^{\infty} |\tau_\xi(\tau)| d\tau \quad (2.11)$$



Hình 2.2

Ý nghĩa hình học:

τ_K là nửa cạnh đáy của hình chữ nhật có chiều cao bằng đơn vị K, có diện tích bằng diện tích của miền giới hạn bởi trục hoành và đường biểu diễn $\tau_\xi(\tau)$.

Trong thực tế, ta thường gặp những quá trình ngẫu nhiên ergodic. Ví dụ: tạp âm của các máy thu vô tuyến điện,... Đổi với các quá trình ngẫu nhiên ergodic, ta có thể xác định các đặc trưng thống kê của chúng bằng thực nghiệm một cách dễ dàng.

Ta đã biết rằng, nếu $X(t)$ – ergodic và với T đủ lớn thì ta có thể viết:

$$\begin{aligned} R_X(\tau) &= M\{[X(t) - m_X][X(t-\tau) - m_X]\} \\ &\approx \frac{1}{T} \int_0^T [x(t) - m_X][x(t+\tau) - m_X] dt \end{aligned} \quad (2.12)$$

Trung bình thống kê = trung bình theo thời gian

2.4. CÁC ĐẶC TRƯNG VẬT LÝ CỦA TÍN HIỆU NGẪU NHIÊN VÀ NHIỀU. BIẾN ĐỔI WIENER – KHINCHIN

2.4.1. Những khái niệm xây dựng lý thuyết phô của quá trình ngẫu nhiên - mật độ phô công suất

Mục trước ta chỉ đưa ra một số đặc trưng thống kê của các quá trình ngẫu nhiên (tín hiệu, nhiễu) mà chưa đưa ra các đặc trưng vật lý của chúng. Về mặt lý thuyết cũng như thực tế, các đặc trưng vật lý của tín hiệu ngẫu nhiên (quá trình ngẫu nhiên) đóng một vai trò rất quan trọng ở những chương sau khi nói đến cơ sở lý thuyết chống nhiễu cũng như xét các biện pháp thực tế và các thiết bị chống nhiễu ta không thể không dùng đến những đặc trưng vật lý của tín hiệu ngẫu nhiên và nhiễu. Khi xét các loại tín hiệu xác định trong giáo trình “Lý thuyết mạch”, chúng ta đã làm quen với các đặc trưng vật lý của chúng như: năng lượng, công suất, thời hạn của tín hiệu, phô biên độ phức, mật độ phô, bề rộng phô, ... Cơ sở để hình thành các đặc trưng vật lý này là chuỗi và tích phân Fourier.

Đối với các tín hiệu ngẫu nhiên và nhiễu, ta không thể dùng trực tiếp các biến đổi Fourier để xây dựng các đặc trưng vật lý của chúng được vì những lý do sau:

- Tập các thể hiện $\{x_i(t)\}$, $i=1,2,\dots,\infty$ của quá trình ngẫu nhiên $X(t)$ cho trên khoảng T thường là một tập vô hạn (thậm chí cũng không phải là một tập đếm được).

- Nếu tín hiệu ngẫu nhiên là dừng chất thì tập vô hạn các thể hiện theo thời gian của nó thường sẽ không khả tích tuyệt đối. Tức là:

$$\lim_{T \rightarrow \infty} \int_{-T/2}^{T/2} |x(t)| dt = \infty$$

Để tránh khỏi những khó khăn trên, ta làm như sau:

Lấy hàm $x_T(t)$ trùng với một thể hiện của quá trình ngẫu nhiên trung tâm $X(t)$ (QTNN trung tâm là QTNN có kỳ vọng không) ở trong đoạn $\left[-\frac{T}{2}, \frac{T}{2}\right]$ và nó bằng không ở ngoài đoạn đó:

$$x_T(t) = \begin{cases} x(t) & |t| \leq T/2 \\ 0 & |t| > T/2 \end{cases} \quad (2.13)$$

Từ (2.13), ta thấy $x_T(t)$ thoả mãn điều kiện khả tích tuyệt đối nên có thể dùng biến đổi Fourier cho nó được. Ta đã biết rằng phô biên độ phức $\hat{S}_T(\omega)$ của $x_T(t)$ được xác định bởi tích phân thuận Fourier sau:

$$\hat{S}_T(\omega) = \int_{-T/2}^{T/2} x_T(t) e^{-j\omega t} dt \quad (2.14)$$

Theo định lý Parseval, ta có biểu thức tính năng lượng của $x_T(t)$ như sau:

$$E_T = \int_{-\infty}^{\infty} x_T^2(t) dt = \frac{1}{2\pi} \int_{-\infty}^{\infty} \left| \dot{S}_T(\omega) \right|^2 d\omega \quad (2.15)$$

Công suất của thê hiện $x_T(t)$ sẽ bằng:

$$P_T = \frac{E_T}{T} = \frac{1}{2\pi T} \int_{-\infty}^{\infty} \left| \dot{S}_T(\omega) \right|^2 d\omega = \frac{1}{2\pi} \int_{-\infty}^{\infty} \frac{\left| \dot{S}_T(\omega) \right|^2}{T} d\omega \quad (2.16)$$

Ta thấy vế trái của (2.16) là công suất của thê hiện $x_T(t)$ trong khoảng thời gian tồn tại hữu hạn T , còn vế phải là một tổng liên tục của các đại lượng $\left| \dot{S}_T(\omega) \right|^2 / T$ d ω . Rõ ràng là để đảm bảo sự bình đẳng về thứ thứ nguyên giữa hai vế của (2.16) thì lượng $\frac{\left| \dot{S}_T(\omega) \right|^2}{T} d\omega$ phải biểu thị công suất trong giải tần vô cùng bé d ω . Như vậy, $\frac{\left| \dot{S}_T(\omega) \right|^2}{T}$ sẽ biểu thị công suất của thê hiện $x_T(t)$ trong một đơn vị tần số [W/Hz] tức là mật độ phô công suất của thê hiện $x_T(t)$. Đến đây ta đặt:

$$\frac{\left| \dot{S}_T(\omega) \right|^2}{T} = G_T(\omega) \quad (2.17)$$

và gọi $G_T(\omega)$ là mật độ phô công suất của thê hiện $x_T(t)$ trong khoảng T hữu hạn. $G_T(\omega)$ đặc trưng cho sự phân bố công suất của một thê hiện $x_T(t)$ trên thang tần số. Khi cho $T \rightarrow \infty$ ta sẽ tìm được mật độ phô công suất của một thê hiện duy nhất $x_T(t)$ của quá trình ngẫu nhiên:

$$G_x(\omega) = \lim_{T \rightarrow \infty} G_T(\omega) = \lim_{T \rightarrow \infty} \frac{\left| \dot{S}_T(\omega) \right|^2}{T} \quad (2.18)$$

$G_x(\omega)$ cũng có ý nghĩa tương tự như $G_T(\omega)$.

Từ (2.18) ta thấy rằng để xác định mật độ phô công suất của cả quá trình ngẫu nhiên (tức là tập các thê hiện ngẫu nhiên) thì phải lấy trung bình thống kê đại lượng $G_x(\omega)$, tức là:

$$G(\omega) = M\{G_x(\omega)\} = M \lim_{T \rightarrow \infty} \frac{\left| \overset{\bullet}{S}_T(\omega) \right|^2}{T} \quad (2.19)$$

(2.19) là công thức xác định mật độ phô công suất của các quá trình ngẫu nhiên.

2.4.2. Cặp biến đổi Wiener – Khinchin

Để thấy được mối quan hệ giữa các đặc trưng thống kê (nói riêng là hàm tự tương quan) và các đặc trưng vật lý (nói riêng là mật độ phô công suất) ta viết lại và thực hiện biến đổi (2.19) như sau:

$$\begin{aligned} G(\omega) &= M \lim_{T \rightarrow \infty} \frac{\left| \overset{\bullet}{S}_T(\omega) \right|^2}{T} = \lim_{T \rightarrow \infty} \frac{M \left| \overset{\bullet}{S}_T(\omega) \right|^2}{T} = \\ &= \lim_{T \rightarrow \infty} \frac{1}{T} M \left\{ \overset{\bullet}{S}_T(\omega) \overset{\bullet}{S}_T(\omega)^* \right\} \xrightarrow{\text{do (2.14)}} \\ &= \lim_{T \rightarrow \infty} \frac{1}{T} M \left\{ \int_{-T/2}^{T/2} x_T(t_1) e^{-j\omega t_1} dt_1 \cdot \int_{-T/2}^{T/2} x_T(t_2) e^{-j\omega t_2} dt_2 \right\} = \\ &= \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} \int_{-T/2}^{T/2} M\{x_T(t_1) \cdot x_T(t_2)\} e^{-j\omega(t_1 - t_2)} dt_1 dt_2 \end{aligned}$$

Nhưng theo định nghĩa (2.8), ta thấy ngay $M\{x_T(t_1) \cdot x_T(t_2)\}$ là hàm tự tương quan của quá trình ngẫu nhiên trung tâm (có $m_x = 0$) nên ta có thể viết:

$$M\{x_T(t_1) \cdot x_T(t_2)\} = R_T(t_1, t_2)$$

Nếu $\tau = -t_2 + t_1$ thì đổi với những quá trình dừng, ta có:

$$M\{x_T(t_1) \cdot x_T(t_2)\} = R_T(\tau)$$

Ta có thể viết lại biểu thức cho $G(\omega)$:

$$\begin{aligned} G(\omega) &= \lim_{T \rightarrow \infty} \left\{ \frac{1}{T} \int_{-T/2-t_2}^{T/2+t_2} R_T(\tau) e^{-j\omega\tau} d\tau \int_{-T/2}^{T/2} dt_2 \right\} \\ &= \lim_{T \rightarrow \infty} \int_{-T/2-t_2}^{T/2+t_2} R_T(\tau) e^{-j\omega\tau} d\tau \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-T/2}^{T/2} dt_2 \end{aligned}$$

$$G(\omega) = \int_{-\infty}^{\infty} R(\tau) e^{-j\omega\tau} d\tau \quad (2.20)$$

Tất nhiên ở đây phải giả sử tích phân ở về phái của (2.20) tồn tại. Điều này luôn luôn đúng nếu hàm tự tương quan $R(\tau)$ khả tích tuyệt đối, tức là:

$$\int_{-\infty}^{\infty} R(\tau) d\tau < \infty$$

(2.20) là mật độ phổ công suất của quá trình ngẫu nhiên dừng. Nó biểu diễn một cách trung bình (thống kê) sự phân bố công suất của quá trình ngẫu nhiên theo tần số của các thành phần dao động điều hoà nguyên tố (tức là những thành phần dao động điều hoà vô cùng bé).

Như vậy, từ (2.20) ta có thể kết luận rằng phổ công suất $G(\omega)$ của quá trình ngẫu nhiên dừng là biến đổi thuận Fourier của hàm tự tương quan $R(\tau)$. Hiện nhiên rằng khi đã tồn tại biến đổi thuận Fourier thì cũng tồn tại biến đổi ngược Fourier sau:

$$R(\tau) = \frac{1}{2\pi} \int_{-\infty}^{\infty} G(\omega) e^{j\omega\tau} d\omega \quad (2.21)$$

Cặp công thức (2.20) và (2.21) gọi là cặp biến đổi Wiener – Khinchin, đó là sự mở rộng cặp biến đổi Fourier sang các tín hiệu ngẫu nhiên dừng (ít nhất là theo nghĩa rộng).

Rõ ràng từ định nghĩa (2.17) của mật độ phổ công suất, ta thấy hàm $G(\omega)$ là hàm chẵn của đối số ω . Do đó sau khi dùng công thức Euler ($e^{\pm j\omega\tau} = \cos\omega\tau \pm j\sin\omega\tau$) để biến đổi (2.20) và (2.21), ta được:

$$\begin{aligned} G(\omega) &= 2 \int_0^{\infty} R(\tau) \cos\omega\tau d\tau \\ R(\tau) &= \frac{1}{\pi} \int_0^{\infty} G(\omega) \cos\omega\tau d\omega \end{aligned} \quad (2.22)$$

Chú ý 1: Từ mật độ phổ công suất của tín hiệu ngẫu nhiên, không thể sao lại bất cứ một thê hiện nào (là hàm của thời gian t) của nó, vì $G(\omega)$ không chứa những thông tin (những hiểu biết) về pha của các thành phần phổ riêng lẻ. Đối với tín hiệu xác định thì từ mật độ phổ hoàn toàn có thể sao lại chính tín hiệu đó nhờ tích phân ngược Fourier. Đó là chỗ khác nhau về bản chất giữa biến đổi Fourier và biến đổi Wiener – Khinchin.

Chú ý 2: Nếu phải xét đồng thời hai quá trình ngẫu nhiên thì người ta cũng đưa ra khái niệm mật độ phổ chéo. Mật độ phổ chéo và hàm tương quan chéo của hai quá trình ngẫu nhiên có liên hệ dừng cũng thỏa mãn cặp biến đổi Wiener – Khinchin.

2.4.3. Bề rộng phổ công suất

Một đặc trưng vật lý quan trọng khác của các tín hiệu ngẫu nhiên là bề rộng phổ công suất, nó được định nghĩa bởi công thức sau:

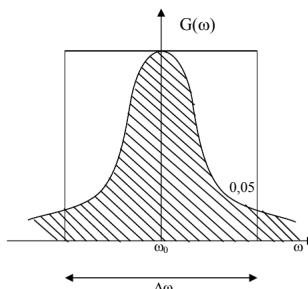
$$\Delta\omega = \frac{0}{\int_{-\infty}^{\infty} G(\omega) d\omega} \quad (2.23)$$

Trong đó:

$G(\omega)$ là mật độ phổ công suất của tín hiệu ngẫu nhiên.

$G(\omega_0)$ là giá trị cực đại của $G(\omega)$.

$\Delta\omega$ là bề rộng phổ công suất (còn gọi là bề rộng phổ) của quá trình ngẫu nhiên.



Hình 2.3

Ý nghĩa hình học:

Bề rộng phổ $\Delta\omega$ chính là đáy của hình chữ nhật có chiều cao bằng $G(\omega_0)$ và có diện tích bằng diện tích của miền giới hạn bởi trục ω và đường cong biểu diễn $G(\omega)$. (Hình 2.4).

Ý nghĩa vật lý:

Bề rộng phổ đặc trưng cho sự tập trung công suất (hoặc năng lượng) của tín hiệu ngẫu nhiên ở quanh một tần số trung tâm, ngoài ra nó cũng đặc trưng cho cả sự bằng phẳng của phổ ở quanh tần số trung tâm ω_0 .

2.4.4. Mở rộng cặp biến đổi Wiener – Khinchin cho trường hợp $R(\tau)$ không khả tích tuyệt đối

Nếu quá trình ngẫu nhiên $X(t)$ chứa các thành phần dao động điều hòa dạng:

$$X_K(t) = A_K \cos(\omega_K t - \varphi_K)$$

trong đó A_K và φ_K nói chung có thể là các đại lượng ngẫu nhiên, thì hàm tương quan trung bình:

$$R_{X_K}^*(\tau) = \frac{A_K^2}{2} \cos \omega_K \tau \text{ không thỏa mãn điều kiện khả tích tuyệt đối.}$$

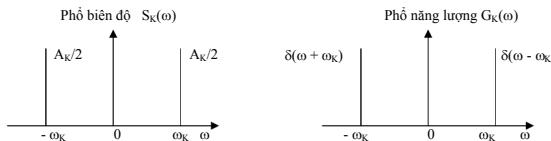
Nếu sử dụng biểu diễn sau của hàm delta:

$$\int_{-\infty}^{\infty} e^{ixy} dx = \int_{-\infty}^{\infty} \cos(xy) dx = \delta(y)$$

và biểu diễn phổ năng lượng của $X_K(t)$ dưới dạng:

$$G_K^*(\omega) = \frac{A_K^2}{4} [\delta(\omega - \omega_K) + \delta(\omega + \omega_K)]$$

thì định lý Wiener – Khinchin sẽ đúng cả đối với những quá trình ngẫu nhiên có những thành phần tần số rời rạc, kể cả thành phần một chiều ở tần số $\omega_K = 0$.



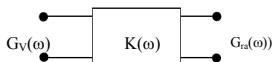
2.5. TRUYỀN CÁC TÍN HIỆU NGẪU NHIÊN QUA CÁC MẠCH VÔ TUYẾN ĐIỆN TUYẾN TÍNH

Đối với các tín hiệu xác định, trong giáo trình “Lý thuyết mạch”, ta đã xét bài toán phân tích sau: Cho một mạch tuyến tính có cấu trúc đã biết (biết hàm truyền đạt $K(\omega)$ hoặc biết phản ứng xung $g(t)$). Ta phải xét tác động đầu vào theo hướng ứng đầu ra và ngược lại. Đối với các tín hiệu ngẫu nhiên nếu số thể hiện là điểm được và hữu hạn thì ta có thể xét hướng ứng ra đối với tống tác động đầu vào như bài toán trên. Nhưng khi số thể hiện của tín hiệu ngẫu nhiên là vô hạn thì ta không thể áp dụng được những kết quả của bài toán phân tích đối với các tín hiệu xác định. Sau đây ta sẽ xét bài toán này.

2.5.1. Bài toán tối thiểu

2.5.1.1. Bài toán:

Cho một mạch tuyến tính (có tham số không đổi và biết $K(\omega)$ của nó. Biết mật độ phô công suất $G_v(\omega)$ của quá trình ngẫu nhiên tác động ở đầu vào. Ta phải tìm mật độ phô công suất $G_{ra}(\omega)$ và hàm tự tương quan $R_{ra}(\tau)$ của quá trình ngẫu nhiên ở đầu ra.



2.5.1.2. Giải bài toán:

Ở giáo trình “Lý thuyết mạch” ta đã biết hàm phô biến độ phức của tín hiệu ở đầu ra mạch vô tuyến điện tuyến tính bằng:

$$\dot{S}_{ra}(\omega) = \dot{K}(\omega) \cdot \dot{S}_v(\omega) \quad (2.24)$$

Trong đó: $\dot{K}(\omega)$ là hàm truyền của mạch đã biết.

$\dot{S}_v(\omega)$ là phô biến độ phức của tín hiệu vào

Chú ý: Đối với các quá trình ngẫu nhiên ta không biết được $\dot{S}_v(\omega)$. Không thể tính được

$\dot{S}_v(\omega)$, mặt khác ta đã biết theo (2.19):

$$\begin{aligned} G_v(\omega) &= M \lim_{T \rightarrow \infty} \left| \frac{\dot{S}_{vT}(\omega)}{T} \right|^2 = M \lim_{T \rightarrow \infty} \left\{ \frac{1}{T} \left| \frac{\dot{S}_{raT}(\omega)}{\dot{K}(\omega)} \right|^2 \right\} \\ &= \frac{1}{\left| \dot{K}(\omega) \right|^2} M \lim_{T \rightarrow \infty} \frac{\left| \dot{S}_{raT}(\omega) \right|^2}{T} = \frac{1}{\left| \dot{K}(\omega) \right|^2} \cdot G_{ra}(\omega) \\ \text{Hay: } G_{ra}(\omega) &= \left| \dot{K}(\omega) \right|^2 \cdot G_v(\omega) \end{aligned} \quad (2.25)$$

Người ta đã chứng minh được rằng hướng ứng ra của hệ thống tuyến tính có tham số không đổi là một quá trình ngẫu nhiên không dừng ngay cả khi tác động đầu vào là một quá trình ngẫu nhiên dừng.

Tuy vậy, trong trường hợp hệ thống tuyến tính thụ động có suy giảm thì ở những thời điểm $t >> t_0 = 0$ (thời điểm đặt tác động vào) thì quá trình ngẫu nhiên ở đầu ra sẽ được coi là dừng.

Khi đó hàm tự tương quan và mật độ phô công suất của quá trình ngẫu nhiên ở đầu ra sẽ liên hệ với nhau theo cấp biến đổi Wiener – Khinchin. Ta có:

$$R_{ra}(\tau) = \frac{1}{2\pi} \int_{-\infty}^{\infty} G_{ra}(\omega) e^{j\omega\tau} d\omega \quad (2.26)$$

Nhận xét:

Từ (2.25) ta thấy mật độ phô công suất của hướng ứng ra được quyết định bởi bình phương môđun hàm truyền của mạch khi đã cho phô công suất của tác động vào, nó không phụ thuộc gì vào đặc tính pha tần của mạch.

Công suất của quá trình ngẫu nhiên ở đầu ra (khi quá trình ngẫu nhiên vào là dừng):

$$R_{ra}(0) = \tau^2 = \frac{1}{2\pi} \int_{-\infty}^{\infty} G_{ra}(\omega) d\omega = P_{ra} = \frac{1}{2\pi} \int_{-\infty}^{\infty} \left| \dot{K}(\omega) \right|^2 G_v(\omega) d\omega \quad (2.27)$$

Nếu phô công suất của tác động vào không phụ thuộc tần số, tức là $G_v(\omega) = N_0$ (quá trình ngẫu nhiên có tính chất này được gọi là tạp âm trắng) thì:

$$P_{ra} = \frac{1}{2\pi} N_0 \int_{-\infty}^{\infty} \left| \dot{K}(\omega) \right|^2 d\omega \quad (2.28)$$

Vì módun hàm truyền luôn là một hàm chẵn nên:

$$P_{ra} = \frac{2}{2\pi} N_0 \int_0^{\infty} \left| \dot{K}(\omega) \right|^2 d\omega \quad (2.29)$$

Mặt khác, nếu gọi G_0 là phô công suất thực tế (phản phô công suất trải từ $0 \rightarrow \infty$) thì $G_0 = 2 N_0$ và (2.29) có thể viết lại như sau:

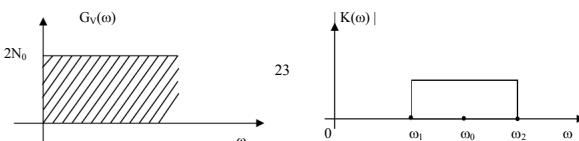
$$P_{ra} = \frac{G_0}{2\pi} \int_0^{\infty} \left| \dot{K}(\omega) \right|^2 d\omega \quad (2.30)$$

Hàm tự tương quan của quá trình ngẫu nhiên ở đầu ra trong trường hợp này sẽ bằng:

$$\begin{aligned} R_{ra}(\tau) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} G_v(\omega) \left| \dot{K}(\omega) \right|^2 e^{j\omega\tau} d\omega \\ &= \frac{1}{2\pi} N_0 \int_{-\infty}^{\infty} \left| \dot{K}(\omega) \right|^2 e^{j\omega\tau} d\omega \\ &= \frac{N_0}{2\pi} \int_{-\infty}^{\infty} \left| \dot{K}(\omega) \right|^2 e^{j\omega\tau} d\omega \\ R_{ra}(\tau) &= \frac{G_0}{2\pi} \int_0^{\infty} \left| \dot{K}(\omega) \right|^2 \cos\omega\tau d\omega \end{aligned} \quad (2.31)$$

2.5.1.3. Ví dụ 1

Một mạch vô tuyến điện tuyến tính có tham số không đổi và đặc tính truyền đạt dạng chữ nhật (hình 2.4b) chịu tác động của tạp âm trắng đứng. Tìm hàm tự tương quan của tạp âm ra.



Theo giả thiết: $G_v(\omega) = 2N_0$ và $\left| \dot{K}(\omega) \right| = \begin{cases} K_0 & \omega_1 < \omega < \omega_2 \\ 0 & \forall \omega \notin (\omega_1, \omega_2) \end{cases}$

Theo (2.31), ta có:

$$\begin{aligned} R_{ra}(\tau) &= \frac{N_0}{\pi} \int_{\omega_1}^{\omega_2} K_0^2 \cos \omega \tau d\omega = \frac{N_0 K_0^2}{\pi \tau} (\sin \omega_2 \tau - \sin \omega_1 \tau) \\ &= \frac{N_0 K_0^2}{\pi \tau} \Delta \omega \frac{\sin \frac{\Delta \omega \tau}{2}}{\Delta \omega \tau / 2} \cos \omega_0 \tau \\ R_{ra}(\tau) &= \tau_{ra}^2 \frac{\sin \frac{\Delta \omega \tau}{2}}{\Delta \omega \tau / 2} \cos \omega_0 \tau \end{aligned} \quad (2.32)$$

Đồ thị $R_{ra}(\tau)$ như hình 2.5.

(2.32) có thể viết gọn lại như sau:

$$R_{ra}(\tau) = R_{0ra}(\tau) \cos \omega_0 \tau \quad (2.32a)$$

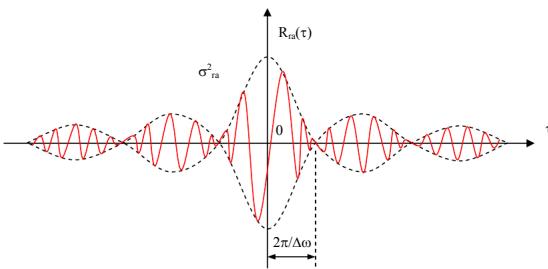
Trong đó:

$$R_{0ra}(\tau) = \sigma_{ra}^2 \frac{\sin \Delta \omega \tau / 2}{\Delta \omega \tau / 2} \quad (2.32b)$$

(2.32b) gọi là bao của hàm tần số tương quan của hướng ứng.

$$\omega_0 = \frac{\omega_1 + \omega_2}{2} \quad (2.32c)$$

gọi là tần số trung bình.



Hình 2.5.

Vậy, bao của hàm tự tương quan của tệp âm ra là một hàm của dải số τ dạng $\frac{\sin x}{x}$. Cực đại của hàm tự tương quan của tệp âm ra đạt tại $\tau = 0$ và bằng σ_{ra}^2 , tức là bằng công suất trung bình của tệp âm ra.

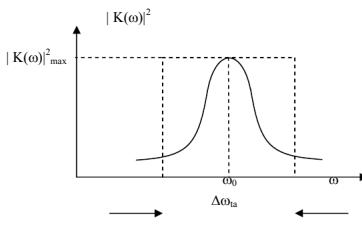
Bây giờ ta sẽ chuyển sang xét một tham số vật lý nữa để đánh giá mức độ truyền tệp âm qua mạch tuyến tính.

2.5.1.4. Giải thông tệp âm

Định nghĩa:

Giải thông tệp âm của mạch tuyến tính (hay bộ lọc tuyến tính) được xác định theo biểu thức sau:

$$\Delta\omega_{ta} = \frac{\int_0^{\infty} |K(\omega)|^2 d\omega}{\left| K(\omega) \right|_{max}^2} \quad (2.33)$$



Hình 2.6.

Ý nghĩa hình học: $\Delta\omega_{ta}$ chính là đáy của hình chữ nhật có diện tích bằng diện tích của miền giới hạn bởi đường cong $\left| \frac{\bullet}{K(\omega)} \right|^2$ và nửa trục hoành $(0, \infty)$; còn chiều cao của hình chữ nhật này là $\left| \frac{\bullet}{K(\omega_0)} \right|^2$ max.

Ý nghĩa vật lý:

$\Delta\omega_{ta}$ đặc trưng cho khả năng làm suy giảm tạp âm của các bộ lọc tuyến tính. Với cùng

$\left| \frac{\bullet}{K(\omega_0)} \right|$, bộ lọc nào có $\Delta\omega_{ta}$ càng hẹp thì công suất tạp âm đầu ra của bộ lọc ấy càng bé.

2.5.2. Bài toán tối đa

$G_R(\omega)$ và $B_R(\tau)$ chưa đặc trưng đầy đủ cho quá trình ngẫu nhiên.

Nội dung: Tìm hàm mật độ xác suất của tín hiệu ở đầu ra mạch vô tuyến điện tuyến tính.

2.5.2.1. Mở đầu

Tìm mật độ xác suất n chiều của tín hiệu ngẫu nhiên ở đầu ra mạch tuyến tính là bài toán rất khó, nó không giải được dưới dạng tổng quát. Dưới đây chỉ xét hai trường hợp đơn giản:

- Tìm mật độ xác suất một chiều của tín hiệu ra bộ lọc tuyến tính khi tác động đầu vào là tín hiệu ngẫu nhiên chuẩn (có vô hạn thể hiện). Trong trường hợp này người ta đã chứng minh được tín hiệu ra cũng là một tín hiệu ngẫu nhiên chuẩn.

- Đặt vào bộ lọc tuyến tính một tín hiệu ngẫu nhiên không chuẩn. Nếu $\frac{\Delta\omega_{ta}}{2\pi F} << 1$ (F là

bề rộng phô của tín hiệu vào) thì tín hiệu ngẫu nhiên ở đầu ra sẽ có phân bố tiệm cận chuẩn. Người ta bảo đó là sự chuẩn hóa (Gauss hóa) các quá trình ngẫu nhiên không chuẩn bằng bộ lọc giải hẹp.

2.5.2.2. Ví dụ 2

Cho tệp âm giải hẹp, chuẩn có dạng:

$$n(t) = c(t)\cos\omega_0 t + s(t)\sin\omega_0 t = A(t)\cos(\omega_0 t - \varphi) \quad (*)$$

với $c(t)$ và $s(t)$ có phân bố chuẩn cùng công suất trung bình và với $\varphi = \arctg \frac{s(t)}{c(t)}$

$$A(t) = \sqrt{c^2(t) + s^2(t)} - đường bao của nhiễu.$$

Công suất trung bình của cả hai thành phần của nhiễu bằng nhau và bằng hằng số: $\sigma_c^2 = \sigma_s^2 = \sigma^2$. Khi $n(t)$ dừng, người ta coi là hai thành phần của nhiễu không tương quan.

Tác động $n(t)$ lên bộ tách sóng tuyển tính. Hãy tìm mật độ xác suất một chiều của điện áp ra bộ tách sóng biết rằng bộ tách sóng không gây méo đường bao và không gây thêm một lượng dịch pha nào. Thực chất của bài toán là phải tìm $W_1(A)$ và $W_1(\varphi)$.

Trong giáo trình “lý thuyết xác suất”, ta đã có công thức tìm mật độ xác suất một chiều của từng đại lượng ngẫu nhiên theo mật độ xác suất đồng thời của chúng, nên ta có:

$$W_1(A) = \int_0^{2\pi} W_2(A, \varphi) d\varphi; W_1(\varphi) = \int_0^{\infty} W_2(A, \varphi) dA$$

Do đó, vấn đề ở đây là phải tìm $W_2(A, \varphi)$.

Vì bộ tách sóng không gây méo đường bao và không gây thêm một lượng dịch pha nào nên $W_2(A, \varphi)$ ở đầu ra cũng chính là $W_2(A, \varphi)$ ở đầu vào.

Tim $W_2(A, \varphi)$: Vì đầu bài chỉ cho $W_1(c)$ và $W_1(s)$ nên ta phải tìm $W_2(c, s)$, theo

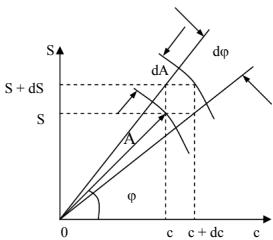
Theo giả thiết $c(t)$ và $s(t)$ không tương quan nên:

$$W_2(c, s) = W_1(c) \cdot W_1(s) \quad (2.34)$$

$$\Rightarrow W_2(c, s) = \frac{1}{\sqrt{2\pi}\delta} e^{-c^2/2\delta^2} \cdot \frac{1}{\sqrt{2\pi}\delta} e^{-s^2/2\delta^2} = \frac{1}{2\pi\delta^2} \exp\left\{-\frac{c^2+s^2}{2\delta^2}\right\}$$

$$W_2(c, s) = \frac{1}{2\pi\delta^2} \exp\left\{-\frac{1}{2\delta^2} A^2\right\} \quad (2.35)$$

Ta thấy xác suất để một điểm có tọa độ (c, s) trong hệ toạ độ Đêecac rơi vào một yếu tố diện tích $dc ds$ sẽ bằng: $P_{dc ds} = W_2(c, s) dc ds$. Để ý đến (*) ta thấy xác suất này cũng chính là xác suất để một điểm có tọa độ (A, φ) trong hệ toạ độ cực rơi vào một yếu tố diện tích $dA d\varphi$. Ta có:



Hình 2.7.

$$P_{dcds} = W_2(c, s) dc ds = W_2(A, \varphi) dA d\varphi \quad (2.36)$$

Từ đó:

$$W_2(A, \varphi) = W_2(c, s) \frac{dc ds}{dA d\varphi} \quad (**)$$

Từ H.2.7 ta thấy với $dA, d\varphi$ đều nhỏ ta có: $dc ds = Ad\varphi \cdot dA$

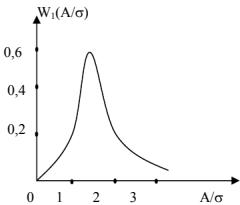
Từ (**) ta có:

$$W_2(A, \varphi) = W_2(c, s) = \frac{1}{2\pi\delta^2} \exp\left\{-\frac{A^2}{2\delta^2}\right\} \quad (2.37)$$

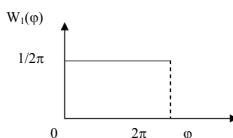
Do đó: $W_1(A) = \int_0^{2\pi} W_2(A, \varphi) d\varphi = \frac{A}{2\pi\delta^2} \exp\left\{-\frac{A^2}{2\delta^2}\right\} \int_0^{2\pi} d\varphi$

$$W_1(A) = \frac{A}{\sigma^2} \exp\left\{-\frac{A^2}{2\delta^2}\right\} \quad (2.38)$$

(2.38) gọi là phân bố Rayleigh (H.2.8).



Hình 2.8.



Hình 2.9.

Vậy nhiễu giải hẹp mà trị tức thời có phân bố chuẩn thì phân bố của đường bao là phân bố không đối xứng Rayleigh. Só dĩ như vậy vì giá trị tức thời có cả giá trị âm và giá trị dương nên phân bố mật độ xác suất sẽ đổi xứng qua trục tung (phân bố Gausse). Còn xét đường bao tức là chỉ xét biên độ (giá trị dương) nên mật độ phân bố xác suất là đường cong không đổi xứng và chỉ tồn tại ở nửa đường trực hoành.

$$W_1(\phi) = \int_0^{\infty} W_2(A, \phi) dA = \int_0^{\infty} \frac{1}{2\pi\delta^2} A \exp\left(-\frac{A^2}{2\delta^2}\right) dA \quad (2.39)$$

Vậy mật độ phân bố xác suất pha đầu của nhiễu giải hẹp, chuẩn là phân bố đều trong khoảng $(0, 2\pi)$. (H.2.9).

2.5.2.3. Ví dụ 3:

Ở đâu vào bộ tách sóng tuyển tính đặt hỗn hợp tín hiệu và nhiễu:

$$y(t) = x(t) + n(t)$$

Với: $x(t) = U_0 \cos \omega_0 t$ là tín hiệu xác định.

$n(t) = A_n(t) \cos [\omega_0 t - \phi(t)]$ là nhiễu giải hẹp, chuẩn.

Tìm mật độ phân bố xác suất đường bao và pha của điện áp đầu ra bộ tách sóng tuyển tính.

Ta có:

$$\begin{aligned} y(t) &= U_0 \cos \omega_0 t + c(t) \cos \omega_0 t + s(t) \sin \omega_0 t \\ &= [U_0 + c(t)] \cos \omega_0 t + s(t) \sin \omega_0 t = A_y(t) \cos [\omega_0 t - \phi_y(t)] \end{aligned}$$

Trong đó: $A_y(t) = \sqrt{[U_0 + c(t)]^2 + s^2(t)}$ là bao của hỗn hợp tín hiệu và nhiễu.

$$\phi_y(t) = \arctan \frac{s(t)}{U_0 + c(t)} \text{ là pha của hỗn hợp tín hiệu và nhiễu.}$$

Làm tương tự như VD2, ta có:

$$W_1(A_y) = \frac{A_y(t)}{\delta^2} \exp\left\{-\frac{A_y^2(t) + U_0^2}{\delta^2}\right\} I_0\left\{\frac{|A_y(t) + U_0|}{\delta^2}\right\} \quad (2.40)$$

(2.40) gọi là phân bố Rice (H.2.10a).

I_0 là hàm Bessel biến dạng loại 1 cấp 0.

$$I_0(z) = \frac{1}{2\pi} \int_0^{2\pi} e^{z\cos\theta} d\theta$$

$I_0(z)$ có thể viết dưới dạng chuỗi vô hạn sau:

$$I_0(z) = \sum_{n=0}^{\infty} \frac{1}{(n!)^2} \left(\frac{z}{2}\right)^{2n}$$

$$\text{Khi } z \ll 1: \quad I_0(z) = 1 + \frac{z^2}{4} + \dots \approx e^{z^2/4}$$

Nhận xét:

- Khi $a = 0 \Leftrightarrow$ không có tín hiệu, chỉ có nhiễu giải hẹp, chuẩn \Rightarrow phân bố Rice trở về phân bố Rayleigh.

- a càng lớn, phân bố Rice càng tiến tới phân bố Gausse.

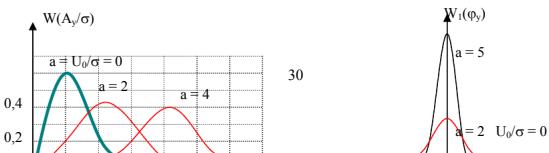
Giải thích:

$a \gg 1 \Leftrightarrow$ tín hiệu mạnh, nhiễu yếu. Tín hiệu tác dụng với thành phần không trực giao với nó của nhiễu (khi tín hiệu càng mạnh thì hỗn hợp này càng ít khác tín hiệu), còn thành phần của nhiễu trực giao với tín hiệu thì không chịu sự "chèn ép" của tín hiệu. Do đó mật độ phân bố xác suất bao của hỗn hợp sẽ mang đặc điểm của thành phần nhiễu trực giao với tín hiệu.

$$W_1(\phi_y) = \frac{1}{2\pi} \exp\left\{-\frac{U_0^2}{\delta^2}\right\} + \frac{U_0 \cos \phi_y}{2\sqrt{2\pi} \delta^2} \left[1 + \phi\left(\frac{U_0 \cos \phi_y}{\sqrt{2\delta^2}}\right) \right] \exp\left\{-\frac{U_0^2 \sin^2 \phi_y}{2\delta^2}\right\} \quad (2.41)$$

$$\text{Trong đó: } \phi(z) = \frac{2}{\sqrt{2\pi}} \int_0^z e^{-\theta^2/2} d\theta \quad \text{là tích phân xác suất.}$$

Đồ thị (2.41) biểu diễn trên hình H.2.10b.



Nhận xét:

- $a = 0 \Leftrightarrow$ chỉ có nhiễu $W_1(\varphi_y)$ chính là $W_1(\varphi)$ đã xét ở VD2.
- $a >> 1 \Rightarrow$ đường cong $W_1(\varphi_y)$ càng nhọn, hẹp.

Giải thích:

Với a càng lớn thì có thể bỏ qua ảnh hưởng xấu của nhiễu. Do đó đường bao (biên độ tín hiệu) không có gãy (không thẳng giáng) và cũng không có sai pha. Khi đó φ_y nhận giá trị “0” trong khoảng $(-\pi, \pi)$ với xác suất lớn.

2.6. BIỂU ĐIỂN PHÚC CHO THỂ HIỆN CỦA TÍN HIỆU NGĂU NHIÊN – TÍN HIỆU GIẢI HẸP

2.6.1. Cặp biến đổi Hilbert và tín hiệu giải tích

2.6.1.1. Nhắc lại cách biểu diễn một dao động điều hoà dưới dạng phức

$$\text{Cho: } x(t) = A_0 \cos(\omega_0 t + \varphi_0) = A(t) \cos\theta(t) \quad (2.42)$$

Trong đó:

ω_0 : tần số trung tâm; $\theta(t)$: pha dây dù;

φ_0 : pha đầu.

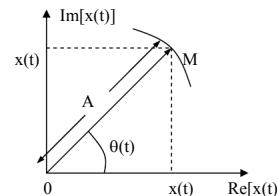
Trong “Lý thuyết mạch”, người ta rất hay dùng cách biểu diễn $x(t)$ dưới dạng phức sau:

$$\overset{\bullet}{x}(t) = x(t) + j\overset{\bullet}{x}(t) = A(t) e^{j\theta(t)} \quad (2.43)$$

Trong đó:

$$x(t) = \text{Re}[\overset{\bullet}{x}(t)];$$

$$\overset{\bullet}{x}(t) = \text{Im}[\overset{\bullet}{x}(t)] = A_0 \sin\theta(t)$$



Hình 2.11

Ta có thể biểu diễn $\dot{x}(t)$ dưới dạng một vecteur trên mặt phẳng phức.

Khi $A(t) = \text{const}$ thì quỹ tích của điểm M sẽ là một vòng tròn tâm O, bán kính OM.

$\omega(t) = d\theta(t)/dt$ là tần số của dao động (H.2.11)

2.6.1.2. Cặp biến đổi Hilbert – Tín hiệu giải tích

a. Cặp biến đổi Hilbert và tín hiệu giải tích:

Để dễ dàng biểu diễn dưới dạng phức những thể hiện phức tạp của các quá trình ngẫu nhiên, người ta dùng cặp biến đổi Hilbert. Nó cho phép ta tìm $\hat{x}(t)$ khi biết $x(t)$ và ngược lại.

Hilbert đã chứng tỏ rằng phần thực và phần ảo của hàm phức (2.43) liên hệ với nhau bởi các biến đổi tích phân đơn trị hai chiều sau:

$$\hat{x}(t) = \text{Im}[\dot{x}(t)] = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{x(\tau)}{t - \tau} d\tau = h[x(t)] \quad (2.44)$$

$$x(t) = -\frac{1}{\pi} \int_{-\infty}^{\infty} \frac{\hat{x}(\tau)}{t - \tau} d\tau = \text{Re}[\dot{x}(t)] = h^{-1}[x(t)] \quad (2.45)$$

Cặp công thức trên được gọi là cặp biến đổi Hilbert. Trong đó (2.44) gọi là biến đổi thuận Hilbert, còn (2.45) gọi là biến đổi ngược Hilbert.

Chú ý:

Cũng giống như tính chất của các tích phân, biến đổi Hilbert là một phép biến đổi tuyến tính.

(Một phép biến đổi f được gọi là tuyến tính nếu có:

$$\begin{aligned} f(x_1 + x_2) &= f(x_1) + f(x_2) \\ f(kx) &= k f(x), \quad k = \text{const} \end{aligned}$$

Các hàm $x(t)$ và $\hat{x}(t)$ được gọi là liên hiệp Hilbert đối với nhau. Tín hiệu phức $\dot{x}(t)$ có phần thực và phần ảo thỏa mãn cặp biến đổi Hilbert gọi là tín hiệu giải tích (tương ứng với tín hiệu thực $x(t)$).

b. Biến đổi Hilbert đối với tín hiệu hình sin:

Trong mục này ta sẽ chứng tỏ $\cos \omega_0 t$ và $\sin \omega_0 t$ thỏa mãn cặp biến đổi H. Thật vậy:

$$\begin{aligned}\hat{x}(t) &= \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{\cos \omega_0 \tau}{t - \tau} d\tau = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{\cos[\omega_0(t - \tau) - \omega_0 t]}{t - \tau} d\tau = \\ &= \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{\cos \omega_0(t - \tau) \cdot \cos \omega_0 t + \sin \omega_0(t - \tau) \cdot \sin \omega_0 t}{t - \tau} d\tau = \\ &= \frac{\cos \omega_0 t}{\pi} \int_{-\infty}^{\infty} \frac{\cos \omega_0(t - \tau)}{t - \tau} d\tau + \frac{\sin \omega_0 t}{\pi} \int_{-\infty}^{\infty} \frac{\sin \omega_0(t - \tau)}{t - \tau} d\tau\end{aligned}$$

Chú ý rằng: $\int_{-\infty}^{\infty} \frac{\cos az}{z} dz = 0$ và $\int_{-\infty}^{\infty} \frac{\sin az}{z} dz = \pi$

$$\Rightarrow \hat{x}(t) = \sin \omega_0 t$$

Vậy ($\sin \omega_0 t$) là liên hợp H của ($\cos \omega_0 t$)

Tương tự ($-\cos \omega_0 t$) là liên hợp phức H của ($\sin \omega_0 t$)

c. Biến đổi H đối với các hàm tổng quát hơn:

- Đối với các hàm tuần hoàn $x(t)$:

Trong “Lý thuyết mạch” ta đã biết, chuỗi Fourier của hàm tuần hoàn (thoả mãn điều kiện Dirichlet) là:

$$x(t) = \sum_{K=0}^{\infty} (a_K \cos K\omega_0 t + b_K \sin K\omega_0 t) \quad (2.46)$$

Vì biến đổi H là biến đổi tuyến tính nên biến đổi H của tổng bằng tổng các biến đổi H của các hàm thành phần, nên:

$$\hat{x}(t) = h[x(t)] = \sum_{K=0}^{\infty} (a_K \sin K\omega_0 t - b_K \cos K\omega_0 t) \quad (2.47)$$

(2.46) và (2.47) gọi là chuỗi liên hiệp H.

- $x(t)$ không tuần hoàn:

Nếu hàm không tuần hoàn $x(t)$ khả tích tuyệt đối thì khai triển Fourier của nó là:

$$x(t) = \frac{1}{2\pi} \int_0^\infty [a(\omega) \cos \omega t + b(\omega) \sin \omega t] d\omega \quad (2.48)$$

Khi đó:

$$\begin{aligned}
 \hat{x}(t) &= h[x(t)] = \frac{1}{2\pi} h \left\{ \int_0^\infty [a(\omega) \cos \omega t + b(\omega) \sin \omega t] d\omega \right\} = \\
 &= \frac{1}{2\pi} \int_0^\infty \{ H[a(\omega) \cos \omega t] + H[b(\omega) \sin \omega t] \} d\omega \\
 &= \frac{1}{2\pi} \int_0^\infty [a(\omega) \sin \omega t - b(\omega) \cos \omega t] d\omega
 \end{aligned} \tag{2.49}$$

(2.48) và (2.49) gọi là các tích phân liên hiệp H.

d. Các yếu tố của tín hiệu giải tích:

Từ (2.46) và (2.47) (hoặc từ (2.48) và (2.49)) ta xây dựng được tín hiệu giải tích ứng với tín hiệu thực $x(t)$ như sau:

$$\begin{aligned}
 \dot{\bar{x}}(t) &= x(t) + j\hat{x}(t) = A(t)e^{j\theta(t)} \\
 x(t) &= \text{Re} [\dot{\bar{x}}(t)] = A(t)\cos\theta(t) \quad (a) \\
 \hat{x}(t) &= \text{Im} [\dot{\bar{x}}(t)] = A(t)\sin\theta(t) \quad (b)
 \end{aligned}$$

- Đường bao của tín hiệu giải tích:

$$\text{Từ (a) và (b) ta thấy: } A(t) = \sqrt{x^2(t) + \hat{x}^2(t)} \tag{2.50}$$

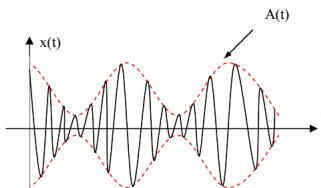
A(t) đặc trưng cho sự biến thiên (dạng biến thiên) của biên độ của tín hiệu (H.2.12).

A(t) được gọi là đường bao của tín hiệu (còn gọi là biên độ biến thiên hay biên độ tức thời của tín hiệu).

- Pha tức thời của tín hiệu giải tích:

Ký hiệu pha tức thời: $\theta(t)$
bằng:

$$\theta(t) = \arctg \frac{\hat{x}(t)}{x(t)} \tag{2.51}$$



Hình 2.12

- *Tần số góc tức thời của tín hiệu giải tích* $\hat{\omega}(t)$:

$$\omega(t) = \frac{d\theta(t)}{dt} = \left[\arctg \frac{\hat{x}(t)}{x(t)} \right]' = \left[\frac{\hat{x}'(t)/x(t)}{1 + \frac{x^2(t)}{\hat{x}^2(t)}} \right]' = \frac{x(t)\hat{x}'(t) - \hat{x}(t)x'(t)}{x^2(t) + \hat{x}^2(t)} \quad (2.52)$$

- *Tính chất của A(t):*

$$+ |A(t)| \geq |x(t)|$$

$$+ \text{Khi } \hat{x}(t) = 0 \Rightarrow A(t) = |x(t)|$$

$$+ \text{Xét: } A'(t) = \frac{x(t).x'(t) + \hat{x}(t).\hat{x}'(t)}{\sqrt{x^2(t) + \hat{x}^2(t)}}$$

$$\text{Khi } \hat{x}(t) = 0 \Rightarrow A'(t) = x'(t)$$

Vậy khi $\hat{x}(t) = 0$ thì độ nghiêng của $A(t)$ và $x(t)$ là như nhau.

- *Kết luận:*

Đối với các tín hiệu ngẫu nhiên thì các yếu tố của tín hiệu là ngẫu nhiên. Nhờ có khái niệm tín hiệu giải tích nên ta mới nghiên cứu các tính chất thống kê của các yếu tố của nó được thuận lợi, đặc biệt là trong tính toán.

2.6.2. Tín hiệu giải rộng và giải hẹp

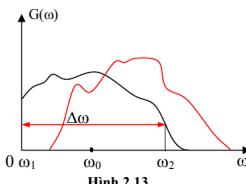
2.6.2.1. Tín hiệu giải rộng

Người ta gọi một tín hiệu là tín hiệu giải rộng nếu bì rộng phô của nó thỏa mãn bất đẳng thức sau:

$$\frac{\Delta\omega}{\omega_0} \geq 1 \quad (2.53)$$

Nhìn chung tín hiệu giải rộng là tín hiệu mà bì rộng phô của nó có thể so sánh được với ω_0 .

Trong đó $\Delta\omega = \omega_2 - \omega_1$ và $\omega_0 = \frac{\omega_2 + \omega_1}{2}$ gọi là tần số trung tâm (xem H.2.13).



Hình 2.13

Ví dụ: Các tín hiệu điều tần, điều xung, điều chế mã xung, manip tần số, manip pha,... là các tín hiệu giải rộng.

2.6.2.2. Tín hiệu giải hẹp

Nếu tín hiệu có bề rộng phô thoá mǎn:

$$\frac{\Delta\omega}{\omega_0} \leq 1 \quad (2.54)$$

Thì nó được gọi là tín hiệu giải hẹp. (H.2.14).

Ví dụ: tín hiệu giải hẹp là các tín hiệu như: tín hiệu cao tần hình sin, tín hiệu cao tần điều biến, tín hiệu đơn biến

Nhìn chung tín hiệu giải hẹp là tín hiệu mà bề rộng phô của nó khá nhô hơn so với tần số ω_0 .

2.6.2.3. Biểu diễn tín hiệu giải hẹp

Nếu một tín hiệu giải hẹp có biểu thức giải tích sau:

$$x(t) = A(t)\cos[\omega_0t - \varphi(t)] = A(t)\cos\theta(t) \quad (2.55)$$

Trong đó: ω_0t là thành phần thay đổi tuyến tính của pha chạy (pha tức thời)

$\varphi(t)$ là thành phần thay đổi chậm của pha chạy

$A(t)$ là đường bao của tín hiệu

Thì (2.55) có thể khai triển như sau:

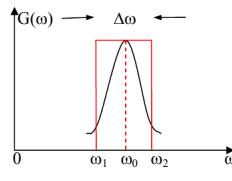
$$\begin{aligned} x(t) &= A(t)\cos\omega_0t\cos\varphi(t) + A(t)\sin\omega_0t\sin\varphi(t) \\ &= \underbrace{A(t)\cos\varphi(t)}_{c(t)}\cos\omega_0t + \underbrace{A(t)\sin\varphi(t)}_{s(t)}\sin\omega_0t \end{aligned}$$

$$= c(t)\cdot\cos\omega_0t + s(t)\cdot\sin\omega_0t \quad (2.56)$$

$c(t)\cdot\cos\omega_0t$ là tín hiệu điều biến biến đổi chậm

$s(t)\cdot\sin\omega_0t$ là tín hiệu điều biến biến đổi chậm

Vậy một tín hiệu giải hẹp hình sin bao giờ cũng có thể biểu diễn dưới dạng tổng của hai tín hiệu điều biến biến đổi chậm, với các yếu tố xác định như sau:



Hình 2.14

$$\begin{cases} A(t) = \sqrt{c^2(t) + s^2(t)} \\ \varphi(t) = \operatorname{arctg} \frac{s(t)}{c(t)} \\ \omega(t) = \frac{d\theta(t)}{dt} \end{cases} \quad (2.57)$$

Rõ ràng là các số hạng ở về phải (2.56) thỏa mãn cặp biến đổi Hilbert.

Việc biểu diễn một tín hiệu giải hẹp thành tổng của hai tín hiệu điều biên biến thiên chậm sẽ làm cho việc phân tích mạch vô tuyến điện dưới tác động của nó đơn giản đi nhiều. Ta sẽ xét lại bài toán này ở phần sau.

2.7. BIỂU DIỄN HÌNH HỌC CHO THỂ HIỆN CỦA TÍN HIỆU NGẪU NHÂN

2.7.1. Khai triển trực giao và biểu diễn vecteur của tín hiệu

2.7.1.1. Năng lượng của chuỗi Kachennhicov

Ta đã biết rất rõ khai triển trực giao Fourier cho các hàm $x(t)$ có phô vô hạn. Ở giáo trình “Lý thuyết mạch”, ta cũng biết rằng một hàm $x(t)$ có phô không chứa tần số lớn hơn F_c có thể phân tích thành chuỗi trực giao Kachennhicov sau:

$$x(t) = \sum_{K=-\infty}^{\infty} x(K\Delta t) \frac{\sin 2\pi F_c (t - K\Delta t)}{2\pi F_c (t - K\Delta t)} \quad (2.58)$$

Trong đó: $\Delta t = 1/2F_c$

Nếu ta chỉ xét tín hiệu có phô hữu hạn $x(t)$ trong khoảng thời gian T hữu hạn thì ta có biểu thức gần đúng sau để tính năng lượng của nó:

$$E = \int_{-T/2}^{T/2} x^2(t) dt \approx \int_{-T/2}^{T/2} \left[\sum_{k=1}^n x_k \frac{\sin \omega_c(t - K\Delta t)}{\omega_c(t - K\Delta t)} \right]^2 dt \quad (*)$$

Trong đó n là số các giá trị rời rạc (còn gọi là các giá trị mẫu) của thể hiện tín hiệu $x(t)$ trong khoảng quan sát T ; còn x_k là giá trị mẫu thứ K của $x(t)$ tại thời điểm rời rạc $K\Delta t$. Để cho gọn, ta đặt $\omega_c(t - K\Delta t) = \lambda$, khi đó (*) có dạng:

$$E \approx \frac{1}{\omega_c} \int_{-T/2}^{T/2} \left[\sum_{K=1}^n x_K \frac{\sin \lambda}{\lambda} \right]^2 d\lambda = \frac{1}{\omega_c} \sum_{K=1}^n x_K^2 \int_{-T/2}^{T/2} \frac{\sin^2 \lambda}{\lambda^2} d\lambda$$

$$\text{Ta có: } \int_{-T/2}^{T/2} \frac{\sin^2 \lambda}{\lambda^2} d\lambda \approx \pi \quad (\text{với } T \text{ khá lớn})$$

$$\Rightarrow E = \frac{\pi}{\omega_c} \sum_{K=1}^n x_K^2 = \frac{1}{2F_c} \sum_{K=1}^n x_K^2 \quad (2.59)$$

(2.59) cho ta tính được năng lượng của chuỗi

2.7.1.2. Biểu diễn $x(t)$ thành vectơ \vec{x} trong không gian n chiều

Khai triển Kachennhicov (2.58) là một dạng khai triển trực giao. Các hàm $\psi_K(t) = \frac{\sin \omega_c(t - K\Delta t)}{\omega_c(t - K\Delta t)}$ là các hàm trực giao.

$$\left(\int_{-\infty}^{\infty} \frac{\sin \omega_c(t - K\Delta t)}{\omega_c(t - K\Delta t)} \cdot \frac{\sin \omega_c(t - i\Delta t)}{\omega_c(t - i\Delta t)} dt \right) = \begin{cases} \pi/\omega_c & i = K \\ 0 & i \neq K \end{cases}$$

Vì vậy ta có thể coi mỗi hàm là một vecteur đơn vị trên hệ trực toạ độ trực giao. Khi T hữu hạn thì $K_{\max} = n$ cũng sẽ hữu hạn. Khi đó ta có thể coi $x(t)$ là một vectơ \vec{x} trong không gian n chiều có các thành phần (hình chiếu) trên các trục toạ độ tương ứng là $x(K\Delta t)$, ($K = \overline{1, n}$).

$$x(t) \Leftrightarrow \{x(t - \Delta t), x(t - 2\Delta t), \dots, x(t - n\Delta t)\}$$

$$x(t) \Leftrightarrow \{x_1, x_2, \dots, x_n\} \Leftrightarrow \vec{x}$$

→

Theo định nghĩa, độ dài (hay chuẩn) của vecteur \vec{x} sẽ là:

$$\left\| \vec{x} \right\| = \sqrt{\sum_{K=1}^n x_K^2} \quad \left(= \sqrt{\langle \vec{x}, \vec{x} \rangle} \right) \quad (2.60)$$

Để ý đến (2.59), ta có:

$$\left\| \vec{x} \right\| = \sqrt{2F_c E} = \sqrt{2F_c T \cdot P} = \sqrt{nP} \quad (2.61)$$

$$(n = \frac{T}{\Delta t} = 2F_c T)$$

Trong đó P là công suất của thế hiện tín hiệu trong khoảng hữu hạn T . Như vậy, với thời hạn quan sát và bề rộng phô của thế hiện cho trước thì độ dài của vecteur biểu diễn tỷ lệ với căn bậc hai công suất trung bình của nó. Nếu cho trước công suất trung bình P thì độ dài của vecteur \vec{x} sẽ tỷ lệ với \sqrt{n} (tức là tỷ lệ với căn bậc hai của đáy tín hiệu $B = F_c T = \frac{n}{2}$)

Nhận xét:

Như vậy, với cùng một công suất trung bình tín hiệu nào có đáy càng lớn (tức là tín hiệu càng phức tạp) thì độ dài của vecteur biểu diễn nó càng lớn. Khi đáy của tín hiệu càng lớn thì độ dài của vecteur tín hiệu càng lớn \rightarrow vecteur tổng của tín hiệu và nhiễu giải hợp càng ít khác vecteur tín hiệu \rightarrow ta sẽ nhận đúng được tín hiệu với xác suất cao. Để tính chồng nhiễu của tín hiệu càng cao thì yêu cầu B càng phải lớn.

Trong trường hợp $x(t)$ không rời rạc hoá: $E_x = \int_0^T x^2(t) dt$. Khi đó chuẩn của vecteur sẽ

là:

$$\left\| \vec{x} \right\| = \sqrt{\vec{x} \cdot \vec{x}} = \sqrt{2F_c E_x} \Rightarrow \left\| \vec{x} \right\| = \sqrt{2F_c \int_0^T x^2(t) dt} \quad (2.62)$$

Người ta còn gọi không gian mà chuẩn của vecteur cho bởi tích vô hướng (2.62) là không gian Hilbert và ký hiệu là L^2 . Không gian L^2 là sự mở rộng trực tiếp của không gian Euclide hữu hạn chiều lên số chiều vô hạn.

2.7.2. Mật độ xác suất của vecteur ngẫu nhiên - Khoảng cách giữa hai vecteur tín hiệu

2.7.2.1. Mật độ xác suất của vecteur ngẫu nhiên

a. Vecteur tín hiệu:

Để tiếp tục những vấn đề sau này được thuận tiện, ta đưa vào khái niệm vecteur tín hiệu.

Định nghĩa:

$$\text{Vecteur tín hiệu } \vec{x}_0 \text{ là vecteur sau: } \vec{x}_0 = \frac{\vec{x}}{\sqrt{n}} \quad (2.63)$$

Trong đó \vec{x} là vecteur biểu diễn tín hiệu $x(t)$ trong không gian n chiều.

Tính chất:

+ \vec{x}_0 có phương và chiều trùng với \vec{x}

$$+ \text{Độ lớn (modul): } \left\| \vec{x}_0 \right\| = \left\| \frac{\vec{x}}{\sqrt{n}} \right\| = \sqrt{P}$$

b. Xác suất phân bố của müt vecteur \vec{x}_0 và miền xác định của nó

Trong không gian tín hiệu, tín hiệu được biểu diễn bởi vecteur. Do đó xác suất để tồn tại tín hiệu đó ở một miền (nói riêng: tại một điểm) nào đó của không gian chính là xác suất để müt vecteur tín hiệu rơi vào miền ấy (nói riêng: điểm ấy) của không gian.

Nếu $x(t)$ là xác định thì mứt của vecteur \vec{x}_0 chỉ chiếm một diện trong không gian n chiều.

Còn nếu $x(t)$ là ngẫu nhiên có một tập các thể hiện $\{x_i(t)\}$ thì mứt vecteur \vec{x}_0 của nó sẽ chiếm một miền nào đó trong không gian n chiều với thể tích: $V = \Delta x_1 \cdot \Delta x_2 \dots \Delta x_n$. Khi ấy, xác suất để tồn tại tín hiệu ngẫu nhiên trong miền có thể tích dV sẽ là:

$$\begin{aligned} P\{t/h \text{NN} \in dV\} &= P\{\text{mứt vecteur } t/h \text{ đó } \in dV\} = \\ &= dP = W_n(x_1, x_2, \dots, x_n) dx_1 dx_2 \dots dx_n = W_n(\vec{x}_0) dV \end{aligned} \quad (2.64)$$

Sau đây ta sẽ xét miền xác định của một số dạng tín hiệu ngẫu nhiên:

- Các thể hiện của tín hiệu phát có cùng đáy, cùng công suất:

Khi đó miền xác định của vecteur tín hiệu phát sẽ là mặt cầu có bán kính bằng chuẩn của vecteur tín hiệu phát $\left\| \vec{x}_0 \right\| = \sqrt{P}$ và có tâm ở gốc toạ độ của vecteur ấy. (Sở dĩ như vậy vì \vec{x}_0 có chuẩn không đổi nhưng phương và chiều của nó thay đổi ngẫu nhiên).

- Tụp âm trắng:

Ta đã biết rằng các thể hiện $n_i(t)$ của tụp âm trắng $n(t)$ có cùng công suất P_n . Như vậy miền xác định của tụp âm trắng là mặt cầu có bán kính bằng $\sqrt{P_n}$, có tâm là gốc của vecteur tụp âm \vec{n}_0 .

- Tổng của tín hiệu $x(t)$ và tụp âm $n(t)$:

$$\begin{aligned} y(t) &= x(t) + n(t) \\ \Rightarrow \vec{y}_0 &= \vec{x}_0 + \vec{n}_0 \Rightarrow \left\| \vec{y}_0 \right\| = \sqrt{P_y} \end{aligned}$$

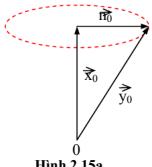
Nếu $x(t)$ và $n(t)$ không tương quan thì:

$$\begin{aligned} P_y &= P_x + P_n \quad (\text{vì } B_y(0) = B_x(0) + B_n(0)) \\ \Rightarrow \left\| \vec{y}_0 \right\| &= \sqrt{P_x + P_n} \Rightarrow \left\| \vec{y}_0 \right\|^2 = P_x + P_n \\ \Rightarrow \left\| \vec{y}_0 \right\|^2 &= \left\| \vec{x}_0 \right\|^2 + \left\| \vec{n}_0 \right\|^2 \quad (*) \end{aligned}$$

Từ (*) ta thấy $\vec{x}_0 \perp \vec{n}_0$ và \vec{y}_0 là cạnh huyền của một tam giác vuông có hai cạnh là \vec{x}_0 và \vec{n}_0 .

Nếu $x(t)$ xác định thì miền xác định của mút y_0 sẽ là đường tròn đáy của hình nón có đỉnh

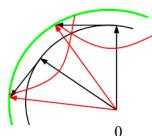
ở gốc toạ độ, chiều cao bằng $\left\| \vec{x}_0 \right\|$ và bán kính bằng $\left\| \vec{n}_0 \right\|$. (H.2.15a).



Hình 2.15a

Nếu $x(t)$ chỉ là một thể hiện nào đó của quá trình ngẫu nhiên $X(t)$ có các thể hiện cùng công

suất thì lúc đó miền xác định của mút y_0 sẽ là một mặt cầu có bán kính bằng $\sqrt{P_x + P_n}$ và có tâm ở gốc toạ độ (H.2.15b).



Hình 2.15b

2.7.2.2. Khoảng cách giữa hai vecteur tín hiệu

Để đánh giá định lượng sự khác nhau giữa hai vecteur tín hiệu, ta đưa ra khái niệm khoảng cách giữa hai vecteur tín hiệu.

Định nghĩa:

Khoảng cách giữa hai vecteur tín hiệu \vec{u}_0 và \vec{v}_0 được xác định theo biểu thức sau:

$$d(\vec{u}_0, \vec{v}_0) = \left\| \vec{u}_0 - \vec{v}_0 \right\| = \frac{1}{\sqrt{n}} \left\| \vec{u} - \vec{v} \right\|$$

$$\Rightarrow d(\vec{u}_0, \vec{v}_0) = \frac{1}{\sqrt{n}} \sqrt{\sum_{K=1}^n (u_K - v_K)^2}$$

$$\text{Hay: } d^2(\vec{u}_0, \vec{v}_0) = \frac{1}{(\sqrt{n})^2} \sum_{K=1}^n u_K^2 + \frac{1}{(\sqrt{n})^2} \sum_{K=1}^n v_K^2 - \frac{2}{n} \sum_{K=1}^n u_K \cdot v_K$$

$$\begin{aligned} \text{Ta có: } & \left\{ \begin{array}{l} \frac{1}{(\sqrt{n})^2} \sum_{K=1}^n u_K^2 = \frac{1}{n} \left\| \vec{u} \right\|^2 = \left\| \vec{u}_0 \right\|^2 = \left\| \vec{u}_0 \right\| \cdot \left\| \vec{u}_0 \right\| \cos(\vec{u}_0, \vec{u}_0) \\ \frac{1}{(\sqrt{n})^2} \sum_{K=1}^n v_K^2 = \frac{1}{n} \left\| \vec{v} \right\|^2 = \left\| \vec{v}_0 \right\|^2 = \left\| \vec{v}_0 \right\| \cdot \left\| \vec{v}_0 \right\| \cos(\vec{v}_0, \vec{v}_0) \\ \frac{1}{n} \sum_{K=1}^n u_K \cdot v_K = (\vec{u}_0, \vec{v}_0) = \left\| \vec{u}_0 \right\| \cdot \left\| \vec{v}_0 \right\| \cos(\vec{u}_0, \vec{v}_0) \end{array} \right. \end{aligned}$$

$$\begin{aligned} \Rightarrow d^2(\vec{u}_0, \vec{v}_0) &= \left\| \vec{u}_0 \right\|^2 + \left\| \vec{v}_0 \right\|^2 - 2 \left\| \vec{u}_0 \right\| \cdot \left\| \vec{v}_0 \right\| \cos(\vec{u}_0, \vec{v}_0) \\ d^2(\vec{u}_0, \vec{v}_0) &= \left\| \vec{u}_0 \right\|^2 + \left\| \vec{v}_0 \right\|^2 - 2 \left\| \vec{u}_0 \right\| \cdot \left\| \vec{v}_0 \right\| \cos\varphi \end{aligned}$$

Trong đó φ là góc hợp bởi \vec{u}_0 và \vec{v}_0 trong không gian n chiều.

$$\cos\varphi = \frac{\vec{u}_0 \cdot \vec{v}_0}{\left\| \vec{u}_0 \right\| \cdot \left\| \vec{v}_0 \right\|} \quad (2.65)$$

$$d^2(\vec{u}_0, \vec{v}_0) = P_u + P_v - 2\sqrt{P_u P_v} \cos\varphi \quad (2.66)$$

Nếu ta không rò rỉ rắc rối hóa tín hiệu thì:

$$d(\vec{u}_0, \vec{v}_0) = \left\| \vec{u}_0 - \vec{v}_0 \right\| = \sqrt{\frac{1}{T} \int_0^T [u(t) - v(t)]^2 dt}$$

$$\begin{aligned} \text{Hay } d^2(u_0, v_0) &= \frac{1}{T} \int_0^T u^2(t) dt + \frac{1}{T} \int_0^T v^2(t) dt - \frac{2}{T} \int_0^T u(t)v(t) dt \\ &= P_u + P_v - 2R_{uv}(t, t) \\ &= P_u + P_v - 2R_{uv}(0) \end{aligned}$$

Trong đó $R_{uv}(0)$ là hằng số tương quan chéo của tín hiệu $u(t)$ và $v(t)$.

$$\begin{aligned} R_{uv}(0) &= \sqrt{D_u(t) \cdot D_v(t)} \rho_{uv}(0) \\ d^2(u_0, v_0) &= P_u + P_v - 2\sqrt{P_u \cdot P_v} \rho_{uv}(0) \end{aligned} \quad (2.67)$$

So sánh (2.66) và (2.67) ta thấy ngay ý nghĩa hình học của hằng số tương quan chéo chuẩn hóa: $\rho_{uv}(0)$ đóng vai trò cosin chỉ phương của hai vecteur tín hiệu.

$$\cos\varphi = \rho_{uv}(0) \quad (2.68)$$

Kết luận:

- Với một mức nhiễu xác định, xác suất thu đúng càng cao khi các thể hiện của tín hiệu càng cách xa nhau.

- Khoảng cách giữa hai mút của hai vecteur tín hiệu càng lớn khi độ dài hai vecteur càng lớn.

2.7.3. Khái niệm về máy thu tối ưu

2.7.3.1. Máy thu tối ưu

Một cách tổng quát, ta coi một máy thu đặc trưng bởi một toán tử thu $\bar{\Psi}$ (H.2.17). Yêu cầu của toán tử thu $\bar{\Psi}$ là tác dụng vào $y(t)$ (là tín hiệu vào) phải cho ra tín hiệu đã phát $x(t)$.

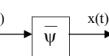
Nếu ta phát đi một thể hiện nào đó của một quá trình ngẫu nhiên $X(t)$:

$$X(t) = \{x_i(t)\} \quad (i=1, m)$$

Ta coi những thể hiện này có cùng công suất P_x , có cùng thời hạn T và có cùng bề rộng phô F_c .

Giả thiết: trong quá trình truyền từ nơi phát đến nơi thu chỉ có tạp âm trắng Gausse $n(t)$, các tín hiệu phát là đồng xác suất

Vecteur tín hiệu ta nhận được: $\vec{y}_0 = \vec{y} / \sqrt{n}$



Hình 2.16.

Nếu $\vec{y}_0 \rightarrow$ này gần với vecteur tín hiệu $\vec{x}_{j0} \rightarrow$ nhất so với các vecteur tín hiệu khác, tức là:

$$\left\| \frac{\vec{y}}{\sqrt{n}} - \frac{\vec{x}_j}{\sqrt{n}} \right\| \leq \left\| \frac{\vec{y}}{\sqrt{n}} - \frac{\vec{x}_i}{\sqrt{n}} \right\| \quad \text{Với } \forall i: i = \overline{1, m} \text{ và } i \neq j$$

Khi đó máy thu có $\vec{\psi}$ tác dụng lên \vec{y} cho ra $\vec{x}_j \rightarrow$: $\vec{\psi}[\vec{y}] = \vec{x}_j \rightarrow$, sẽ được gọi là máy thu tối ưu (theo nghĩa Kachennhivoc trong trường hợp các tín hiệu $x_i(t)$ là dòng xác suất).

2.7.3.2. Liên hệ giữa máy thu tối ưu K và máy thu theo tiêu chuẩn độ lệch trung bình bình phương nhỏ nhất

Độ lệch trung bình bình phương (tbbp) giữa tín hiệu thu được và tín hiệu phát thứ j là:

$$\overline{[y(t) - x_j(t)]^2} = \frac{1}{T} \int_0^T [y(t) - x_j(t)]^2 dt$$

Máy thu theo tiêu chuẩn độ lệch tbbp nhỏ nhất là máy thu đảm bảo:

$$\min_{\forall j} \overline{[y(t) - x_j(t)]^2} \quad j = \overline{1, m}$$

Như vậy, máy thu sẽ cho ra tín hiệu $\vec{x}_j(t) \rightarrow$ nếu:

$$\overline{[y(t) - x_j(t)]^2} \leq \overline{[y(t) - x_i(t)]^2} \quad \forall i \neq j, i = \overline{1, m}$$

$$\text{Hay } \frac{1}{T} \int_0^T [y(t) - x_j(t)]^2 dt \leq \frac{1}{T} \int_0^T [y(t) - x_i(t)]^2 dt \quad \forall i \neq j, i = \overline{1, m}$$

Nâng lên lũy thừa 1/2, ta có:

$$\sqrt{\frac{1}{T} \int_0^T [y(t) - x_j(t)]^2 dt} \leq \sqrt{\frac{1}{T} \int_0^T [y(t) - x_i(t)]^2 dt} \quad \forall i \neq j, i = \overline{1, m}$$

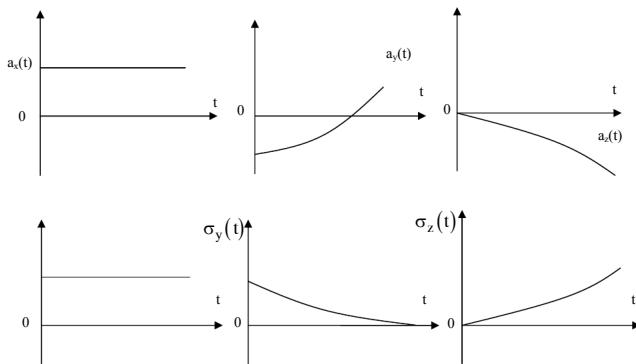
Theo định nghĩa của khoảng cách, ta có thể viết lại như sau:

$$d(\vec{y}_0, \vec{x}_{j0}) \leq d(\vec{y}_0, \vec{x}_{i0}) \quad \forall i \neq j, i = \overline{1, m}$$

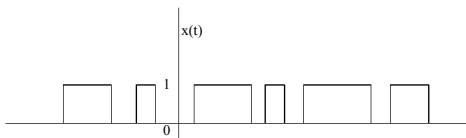
Đây chính là hệ thức đảm bảo bởi máy thu tối ưu K.

BÀI TẬP

- 2.1.** Đồ thị giá trị trung bình $a(t)$ và giá trị trung bình bình phương $\sigma^2(t)$ của các quá trình ngẫu nhiên $X(t)$, $Y(t)$ và $Z(t)$ vẽ trên hình 1 dưới đây. Hãy chỉ ra trên đồ thị miền các giá trị có thể có của các quá trình ngẫu nhiên này, biết rằng biên giới của các miền đó được xác định bởi các giá trị của $\sigma(t)$.

**Hình 1.**

- 2.2.** Trên hình 2 vẽ hàm ngẫu nhiên dừng rời rạc $X(t)$, gọi là dãy xung điện báo. Dãy xung có biên độ không đổi bằng đơn vị, có độ rộng ngẫu nhiên.

**Hình 2.**

Phân bố xác suất các giá trị (0 hoặc 1) của $X(t)$ tuân theo luật Poisson:

$$P_n(t) = \frac{(\lambda t)^n}{n!} e^{-\lambda t} \quad t > 0$$

Trong đó λ là số các bước nhảy của hàm $X(t)$ trong một đơn vị thời gian, còn $P_n(t)$ là xác suất để xảy ra n bước nhảy của hàm $X(t)$ trong thời gian t .

Hãy tìm hàm tự tương quan, hàm tương quan chuẩn hóa và thời gian tương quan của quá trình ngẫu nhiên, biết rằng $P(1) = P(0) = 0,5$.

2.3. Tìm hàm tự tương quan của quá trình ngẫu nhiên dừng sau:

$$X(t) = A \cos(2\pi f_0 t + \phi)$$

Trong đó $A = \text{const}$, $f_0 = \text{const}$, ϕ là đại lượng ngẫu nhiên có phân bố đều trong khoảng $(-\pi, \pi)$.

2.4. Tìm hàm tự tương quan và mật độ phô của tín hiệu điện báo ngẫu nhiên $X(t)$ cho bởi hình dưới đây. Biết rằng nó nhận các giá trị $+a$; - a với xác suất như nhau và bằng $1/2$. Còn xác suất để trong khoảng τ có N bước nhảy là:

$$P(N, \tau) = \frac{(\lambda \tau)^N}{N!} e^{-\lambda \tau} \quad \tau > 0$$

(theo phân bố Poisson).

2.5. Hãy chứng tỏ rằng đường bao của tín hiệu giải tích có thể biểu diễn bằng công thức sau:

$$A(t) = \sqrt{S_a(t) \cdot S_a^*(t)}$$

Trong đó: $S_a^*(t)$ là hàm liên hợp phức của $S_a(t)$:

$$S_a(t) = x(t) + jx^\wedge(t)$$

2.6. Một quá trình ngẫu nhiên dừng có hàm tự tương quan:

a. $R_{x_1}(\tau) = \sigma^2 \cdot e^{-\alpha|\tau|}$

b. $R_{x_2}(\tau) = \sigma^2 \cdot e^{-\alpha|\tau|} \cdot \cos \omega_0 \tau$

Hãy tính toán và vẽ đồ thị mật độ phô của các quá trình ngẫu nhiên trên.

CHƯƠNG 3 - CƠ SỞ LÝ THUYẾT THÔNG TIN THỐNG KÊ

3.1. THÔNG TIN - LƯỢNG THÔNG TIN – XÁC SUẤT VÀ THÔNG TIN – ĐƠN VỊ ĐO THÔNG TIN

3.1.1. Định nghĩa định tính thông tin và lượng thông tin

3.1.1.1. Thông tin

Ở chương trước, ta đã học khái niệm về thông tin. Ở đây ta sẽ xây dựng định nghĩa định tính của thông tin theo quan điểm thống kê. Để đi tới định nghĩa định tính của thông tin, ta sẽ xét ví dụ sau:

Ta nhận được một bức điện (thư) từ nhà đến. Khi chưa mở bức điện ra đọc thì ta chỉ có thể dự đoán hoặc thế này hoặc thế khác về bức điện, mà không đảm chắc nội dung của nó là gì. Nói khác đi, khi chưa mở bức điện ra đọc thì ta không thể xác định được nội dung của nó, tức là ta chưa biết giá trị bao nhiêu ta thông tin gì. Nhưng khi đã xem xong bức điện thì nội dung của nó đối với ta đã hoàn toàn rõ ràng, xác định. Lúc đó, nội dung của bức điện không còn bấp bênh nữa. Như vậy, ta nói rằng: ta đã nhận được một tin về giá dinh. Nội dung của bức điện có thể có 3 đặc điểm sau:

- Nội dung đó ta đã thừa biết. (VD: “Các em con được nghỉ hè 3 tháng”). Khi đó bức điện không cho ta một hiểu biết gì mới về tình hình giá dinh. Hay nói theo quan điểm thông tin, thì bức điện với nội dung ta đã thừa biết không mang đến cho ta một thông tin gì.

- Loại nội dung ta có thể đoán thế này hoặc thế nọ (tức là loại nội dung có độ bấp bênh nào đấy). VD: “Em An đã đỗ đại học”. Vì em An học lực trung bình nên thi vào đại học có thể đỗ, có thể không. Điện với nội dung ta không biết chắc (nội dung chứa một độ bất định nào đó) thất sự có mang đến cho ta một thông tin nhất định.

- Loại nội dung mà ta hoàn toàn không ngờ tới, chưa hề nghĩ tới. VD: “Em An trúng giải nhất trong đợt xổ số”. Bức điện như vậy, đúng về mặt thông tin mà nói, đã đưa đến cho ta một thông tin rất lớn.

Chú ý: Ở đây ta nói tới “những nội dung chưa hề nghĩ tới” phải hiểu theo ý hoàn toàn khách quan chứ không phải do sự không đầy đủ về tư duy của con người đem lại.

Từ những ví dụ trên, ta rút ra những kết luận sau về khái niệm thông tin:

- Điều gì đã xác định (khẳng định được, đoán chắc được, không bấp bênh,...) thì không có thông tin và người ta nói rằng lượng thông tin chứa trong điều ấy bằng không.

- Điều gì không xác định (bất định) thì điều đó có thông tin và lượng thông tin chứa trong nó khác không. Nếu ta càng không thể ngờ tới điều đó thì thông tin mà điều đó mang lại cho ta rất lớn.

Tóm lại, ta thấy khái niệm thông tin gắn liền với sự bất định của đối tượng ta cần xét. Có sự bất định về một đối tượng nào đó thì những thông báo về đối tượng đó sẽ cho ta thông tin. Khi không có sự bất định thì sẽ không có thông tin về đối tượng đó. Như vậy, khái niệm thông tin chỉ là một cách diễn đạt khác đi của khái niệm sự bất định.

Trước khi nhận tin (được thông báo) về một đối tượng nào đây thì vẫn còn sự bất định về đối tượng đó, tức là độ bất định về đối tượng đó khác không (có thể lớn hoặc nhỏ). Sau khi nhận tin (đã được hiểu rõ hoặc hiểu một phần) về đối tượng thi độ bất định của nó giảm đến mức thấp nhất, hoặc hoàn toàn mất. Như vậy, rõ ràng “Thông tin là độ bất định đã bị thu tiêu” hay nói một cách khác “Làm giảm độ bất định kết quả cho ta thông tin”.

3.1.1.2. Lượng thông tin

Trong lý luận ở trên, ta đã từng nói đến lượng thông tin và lượng thông tin lớn, lượng thông tin nhỏ mà không hề định nghĩa các danh từ đó. Dưới đây ta sẽ trả lời vấn đề đó.

Ở trên ta cũng đã nói: trước khi nhận tin thì độ bất định lớn nhất. Sau khi nhận tin (hiểu rõ hoặc hiểu một phần về đối tượng thi độ bất định giảm đến mức thấp nhất, có khi triệt hoàn toàn. Như vậy, có một sự chênh lệch giữa độ bất định trước khi nhận tin và độ bất định sau khi nhận tin. Sự chênh lệch đó là mức độ thu tiêu độ bất định. Độ lớn, nhỏ của thông tin mang đến ta phụ thuộc trực tiếp vào mức chênh đó. Vậy:

“Lượng thông tin là mức độ bị thu tiêu của độ bất định \Leftrightarrow Lượng thông tin = độ chênh của độ bất định trước và sau khi nhận tin = độ bất định trước khi nhận tin - độ bất định sau khi nhận tin (độ bất định tiên nghiệm - độ bất định hậu nghiệm)”.

3.1.2. Quan hệ giữa độ bất định và xác suất

3.1.2.1. Xét ví dụ sau

Ta phải chọn một phần tử trong một tập nào đó. Phép chọn như thế (hoặc “chọn” hiểu theo nghĩa rộng: thử, tìm hiểu, điều tra, trinh sát, tình báo,...) bao giờ cũng có độ bất định.

- Nếu tập chỉ có một phần tử thi ta chẳng phải chọn gì cả và như vậy không có độ bất định trong phép chọn đó.

- Nếu tập có hai phần tử thi ta đã phải chọn. Như vậy, trong trường hợp này phép chọn có độ bất định. Nếu số phần tử của tập tăng thi độ bất định sẽ tăng.

- Các bước tiếp theo sẽ cho bởi bảng sau:

Số phần tử của tập	Độ bất định của phép chọn	Xác suất chọn một phần tử trong tập
1	0	1
2	$\neq 0$	$1/2$
3	$\neq 0$	$1/3$
.	.	.
.	.	.
n	$\neq 0$	$1/n$
.	.	.
.	.	.
∞	∞	$1/\infty = 0$

Chú ý: Bảng này đưa ra với giả sử việc chọn các phần tử là đồng xác suất.

3.1.2.2. Kết luận

- Bằng này cho thấy: độ bất định gắn liền với bản chất ngẫu nhiên của phép chọn, của biến cố.
- Độ bất định (ký hiệu I) là hàm của số phần tử thuộc tập $I(x_K) = f(n)$ (a)
- Độ bất định có liên quan với xác suất chọn phần tử của tập $\Rightarrow I(x_K) = E[p(x_K)]$ (b)

Để tìm mối quan hệ giữa độ bất định I và xác suất chọn một phần tử $x_K(p(x_K))$ trong tập, ta xuất phát từ các tiêu đề sau:

Theo suy nghĩ thông thường, độ bất định I phải thỏa mãn:

$$\begin{aligned} &+ I(x_K) \geq 0 \\ &+ p(x_K) = 1 \Rightarrow I(x_K) = E[p(x_K)] = E[1] = 0 \end{aligned} \quad (3.1)$$

+ Tính cộng dồn:

Nếu x_K và x_i độc lập, thì:

$$E[p(x_K x_i)] = E[p(x_K)p(x_i)] = E[p(x_K)] + E[p(x_i)]$$

Nếu x_K và x_i phụ thuộc thi:

$$E[p(x_K x_i)] = E[p(x_K)p(x_i/x_K)] = E[p(x_K)] + E[p(x_i/x_K)]$$

Đặt $p(x_K) = p$ và $p(x_i/x_K) = q$, thì khi đó với mọi p, q ($0 < p \leq 1, 0 < q \leq 1$), ta có:

$$E[p] + E[q] = E(pq) \quad (3.2)$$

Từ (3.2) ta có thể tìm được dạng hàm $I(p)$. Lấy ví dụ 2 vế của (3.2) theo p , ta có:

$$E'(p) = q E'(pq)$$

Nhân cả 2 vế của phương trình này với p và ký hiệu $p.q = \tau$, ta có:

$$pE'(p) = \tau E'(\tau) \quad (3.3)$$

(3.3) đúng $\forall p, \tau \neq 0$. Nhưng điều này chỉ có thể có khi cả hai vế của (3.3) bằng một hằng số k nào đó:

$$pE'(p) = \tau E'(\tau) = k = \text{const}$$

Từ đó chúng ta có phương trình vi phân $pE'(p) = \text{const} = k$, lấy tích phân phương trình này, ta tìm được:

$$E(p) = k \ln p + C \quad (3.4)$$

Kết đến điều kiện ban đầu (3.1), chúng ta có:

$$E(p) = k \ln p \quad (3.5)$$

Như vậy, ta có: $I(x_K) = k \ln [p(x_K)]$ (3.6)

Hệ số tỷ lệ k trong (3.6) có thể chọn tuỳ ý, nó chỉ xác định hệ đơn vị do của $I(x_K)$. Vì $\ln[p(x_K)] \leq 0$ nên để $I(x_K) \geq 0$ thì $k < 0$.

$$\text{Nếu lấy } k = -1 \text{ thì } I(x_K) = -\ln[p(x_K)] = \ln\left[\frac{1}{p(x_K)}\right] \quad (3.7)$$

Khi đó, đơn vị đo độ bất định sẽ là đơn vị tự nhiên, ký hiệu là nat.

$$\text{Nếu lấy } k = -\frac{1}{\ln 2} \text{ thì } I(x_K) = -\frac{\ln p(x_K)}{\ln 2} = -\log_2 p(x_K) \quad (3.8)$$

Khi đó đơn vị đo độ bất định sẽ là đơn vị nhị phân, ký hiệu là bit (1 nat = 1,433 bit)

Một bit chính là độ bất định chứa trong một phần tử (biến cố của tập xác suất chọn (xuất hiện) bằng 1/2). Người ta thường sử dụng đơn vị [bit] do trong kỹ thuật tính và kỹ thuật liên lạc thường dùng các mã nhị phân.

Ngoài ra, người ta còn có thể sử dụng những đơn vị đo khác tuỳ theo cách chọn cơ số của logarit. Vì vậy trong trường hợp tổng quát, ta có thể viết:

$$I(x_K) = -\log p(x_K) \quad (3.9)$$

3.1.3. Xác định lượng thông tin

Ở mục 1, ta đã có kết luận sau:

Lượng thông tin = độ bất định tiên nghiệm - độ bất định hậu nghiệm. Vì độ bất định sẽ trở thành thông tin khi nó bị thu tiêu nên ta có thể coi độ bất định cũng chính là thông tin. Do đó:

Lượng thông tin = thông tin tiên nghiệm - thông tin hậu nghiệm (*)

Thông tin tiên nghiệm (hay còn gọi là lượng thông tin riêng) được xác định theo (3.9). Còn thông tin hậu nghiệm xác định như sau:

Gọi x_K là tin gửi đi, y_ℓ là tin thu được có chứa những dấu hiệu để hiểu biết về x_K (có chứa thông tin về x_K). Khi đó xác suất để rõ về x_K khi đã thu được y_ℓ là $p(x_K/y_\ell)$. Như vậy độ bất định của tin x_K khi đã rõ y_ℓ bằng:

$$I(x_K/y_\ell) \stackrel{(3.9)}{=} -\log p(x_K/y_\ell) \quad (3.10)$$

(3.10) được gọi là thông tin hậu nghiệm về x_K (thông tin riêng về x_K sau khi có y_ℓ).

Thay (3.9) và (3.10) vào (*), ta có:

$$\begin{aligned} \text{Lượng thông tin về } x_K &= I(x_K) - I(x_K/y_\ell) \\ \underbrace{\text{Lượng thông tin về } x_K}_{\Downarrow \text{Ký hiệu}} &= I(x_K) - I(x_K/y_\ell) \\ I(x_K, y_\ell) &= \log \frac{1}{p(x_K)} - \log \frac{1}{p(x_K/y_\ell)} \end{aligned}$$

$$\Rightarrow I(x_K, y_\ell) = \log \frac{p(x_K/y_\ell)}{p(x_K)} \quad (3.11)$$

(3.11) gọi là lượng thông tin về x_K khi đã rõ tin y_ℓ hay còn gọi là lượng thông tin chéo về x_K do y_ℓ mang lại.

Nếu việc truyền tin không bị nhiễu thì $y_\ell \equiv x_K$. Tức là nếu phát x_K thì chắc chắn nhận được chính nó. Khi đó:

$$p(x_K/y_\ell) = p(x_K/x_K) = 1$$

Từ (3.11) ta có:

$$I(x_K, y_\ell) = I(x_K, x_K) = I(x_K) = \log \frac{1}{p(x_K)} \quad (**)$$

Như vậy khi không có nhiễu, lượng thông tin nhận được đúng bằng độ bất định của sự kiện x_K , tức là đúng bằng thông tin tiên nghiệm của x_K .

Vậy lượng thông tin tồn hao trong kênh sẽ là:

$$I(x_K) - I(x_K, y_\ell) = I(x_K/y_\ell)$$

Đơn vị đo của thông tin (lượng thông tin) cũng chính là đơn vị đo độ bất định.

Nếu cơ số của logarit là 10 thì đơn vị đo thông tin được gọi là Hartley, hay đơn vị thập phân.

Nếu cơ số của logarit là $e = 2,718\dots$ thì đơn vị đo thông tin được gọi là nat, hay đơn vị đo tự nhiên.

Nếu cơ số của logarit là 2 thì đơn vị đo thông tin được gọi là bit, hay đơn vị nhị phân.

$$1 \text{ Harley} = 3,322 \text{ bit}$$

$$1 \text{ nat} = 1,443 \text{ bit}$$

3.2. ENTROPY VÀ CÁC TÍNH CHẤT CỦA ENTROPY

3.2.1. Tính chất thống kê của nguồn rời rạc và sự ra đời của khái niệm entropie

Trong mục trước, ta mới chỉ xét đến lượng thông tin về một biến cố (hay một tin) trong một tập các biến cố (hay tin) xung khắc, đồng xác suất.

Thực tế tồn tại phổ biến loại tập các biến cố (hay nguồn tin, tập tin) xung khắc, không đồng xác suất. Tức là xác suất xuất hiện các biến cố khác nhau trong tập là khác nhau. Ta gọi sự khác nhau giữa các xác suất xuất hiện biến cố của tập (hay tin của nguồn rời rạc) là tính chất thống kê của nó.

Ví dụ 1: Sự xuất hiện các con chữ trong bộ chữ Việt có xác suất khác nhau: $p(e) = 0,02843$; $p(m) = 0,02395$; $p(k) = 0,02102, \dots$ (Theo số liệu trong đồ án tốt nghiệp “Khảo sát cấu trúc thống kê chữ Việt” của Đoàn Công Vinh – ĐHBKHN).

Ví dụ 2: Xác suất xuất hiện của 26 chữ cái trong tiếng Anh: (Số liệu theo Beker và Pipe)

Ký tự	Xác suất	Ký tự	Xác suất
A	0,082	N	0,067
B	0,015	O	0,075
C	0,028	P	0,019
D	0,043	Q	0,001
E	0,127	R	0,060
F	0,022	S	0,063
G	0,020	T	0,091
H	0,061	U	0,028
I	0,070	V	0,010
J	0,002	W	0,023
K	0,008	X	0,001
L	0,040	Y	0,020
M	0,024	Z	0,001

Trong một nguồn tin như thế, ngoài thông tin riêng của mỗi tin (hay dấu) của nó, người ta còn phải quan tâm đến thông tin trung bình của mỗi tin thuộc nguồn. Người ta còn gọi thông tin trung bình do mỗi dấu của nguồn mang lại là entropie. Dưới đây ta sẽ xét kỹ định nghĩa về entropie.

3.2.2. Định nghĩa entropie của nguồn rời rạc

3.2.2.1. Đặt vấn đề

Bề pháp do được chính xác, trong vật lý, khi đo lường một đại lượng, ta không quan tâm đến từng trị do được của đại lượng mà thường xét trị trung bình của chúng. Khi đó ta lấy các trị do được cộng với nhau rồi chia cho số lượng của chúng:

$$i_{tb} = \sum_{r=1}^n i_r / n$$

Ở đây cũng có điều tương tự: ta không quan tâm đến từng thông tin riêng của mỗi dấu mà lại chú ý đến giá trị trung bình của các thông tin đó. Chỉ khác ở chỗ mỗi một thông tin riêng đến tương ứng với một xác suất xuất hiện nào đó, tức là ta có thể xem các thông tin riêng là m đại lượng ngẫu nhiên I. Do đó giá trị trung bình của các thông tin này (lượng thông tin trung bình hay entropie) chính là kỳ vọng của đại lượng ngẫu nhiên I. Ta đi tới định nghĩa sau:

3.2.2.2. Định nghĩa

Entropie của nguồn tin rời rạc là trung bình thống kê của lượng thông tin riêng của các dấu thuộc nguồn A, ký hiệu $H_1(A)$:

$$H_1(A) = \underset{\Delta}{M}[I(a_i)] \quad (3.12)$$

Trong đó a_i là các dấu của nguồn A (Ta hiểu dấu là các con chữ, hoặc các ký hiệu v.v... của nguồn). Còn nguồn A là một tập rời rạc các dấu a_i với các xác suất xuất hiện của chúng. Ta quy ước viết A như sau:

$$A = \{a_i\} = \begin{pmatrix} a_1 & a_2 & \dots & a_s \\ p(a_1) & p(a_2) & \dots & p(a_s) \end{pmatrix} \quad (3.13)$$

$$\text{Với } 0 \leq p(a_i) \leq 1 \text{ và } \sum_{i=1}^s p(a_i) = 1 \quad (3.14)$$

A được cho bởi (3.13) và (3.14) còn gọi là trường tin (hay trường biến cố). Từ (3.12) và (3.13), ta có:

$$\begin{aligned} H_1(A) &= M[I(a_i)] = \sum_{i=1}^s p(a_i) I(a_i) \\ &\Rightarrow H_1(A) = - \sum_{i=1}^s p(a_i) \log p(a_i) \end{aligned} \quad (3.15)$$

$H_1(A)$ còn gọi là entropie một chiều của nguồn rời rạc:

Ví dụ: $H_1(\text{Viết}) = 4,5167 \text{ bit}$ $H_1(\text{Nga}) = 4,35 \text{ bit}$

$H_1(\text{Anh}) = 4,19 \text{ bit}$

3.2.3. Các tính chất của entropie một chiều của nguồn rời rạc

3.2.3.1. Tính chất 1

Khi $p(a_k) = 1$ và $p(a_r) = 0$ với $\forall r \neq k$ thì:

$$H_1(A) = H_1(A_{\min}) = 0 \quad (3.16)$$

Chứng minh:

Ta đã có: $0 \leq p(a_i) \leq 1 \Rightarrow \log p(a_i) \leq 0 \Rightarrow -\log p(a_i) \geq 0$

$$\Rightarrow H_1(A) \geq 0 \Rightarrow H_1(A_{\min}) = 0$$

Bây giờ ta chỉ còn phải chứng tỏ $H_1(A_{\min}) = 0$ khi $p(a_k) = 1$ và $p(a_r) = 0 (\forall r \neq k)$.

Thật vậy, $p(a_r) = 0 \Rightarrow p(a_r) \log p(a_r) = 0 (\forall r \neq k)$

$$p(a_k) = 1 \Rightarrow p(a_k) \log p(a_k) = 0 (\forall r \neq k)$$

$$\begin{aligned} \Rightarrow H_1(A) &= -\sum_{i=1}^s p(a_i) \log p(a_i) \\ &= -p(a_k) \log p(a_k) - \sum_{i=1, i \neq k}^s p(a_i) \log p(a_i) = 0 \end{aligned}$$

Ý nghĩa:

Thực ra không cần phải chứng minh như vậy, mà lập luận như sau cũng cho ta công thức (3.16):

$$p(a_r) = 0 \Rightarrow \text{các } a_r \text{ không xuất hiện}$$

$$p(a_k) = 1 \Rightarrow \text{các } a_k \text{ chắc chắn xuất hiện}$$

\Rightarrow Không có độ bất định nào về các $a_i \Rightarrow$ lượng thông tin riêng không có \Rightarrow lượng thông tin trung bình cũng không có.

3.2.3.2. Tính chất 2

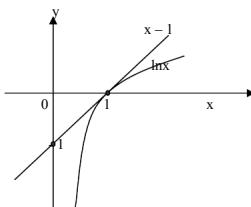
Một nguồn rời rạc gồm s dấu đồng xác suất (và thỏa mãn (3.14)) thì entropie của nó đạt cực đại và cực đại đó bằng $\log s$.

$$H_1(A_{\max}) = \log s \quad (3.17)$$

Chứng minh:

$$\text{Khi } p(a_i) = p(a_j), \forall i, \forall j (i, j \in \overline{1, s})$$

Khi đó $p(a_i) = \frac{1}{s}$, tức là nguồn gồm các dấu xung khắc và đồng khả năng.



Hình 3.1.

$$\Rightarrow H_1(A') = - \sum_{i=1}^s \frac{1}{s} \log \frac{1}{s} = \log s$$

Xét hiệu:

$$\begin{aligned} H_1(A) - \log s &= \sum_{i=1}^s p(a_i) \log \frac{1}{p(a_i)} - \log s \\ &= \sum_{i=1}^s p(a_i) \log \frac{1}{p(a_i)} - \sum_{i=1}^s p(a_i) \log s \\ &= \sum_{i=1}^s p(a_i) \left[\log \frac{1}{p(a_i)} - \log s \right] \\ &= \sum_{i=1}^s p(a_i) \log \frac{1}{p(a_i)s} = \sum_{i=1}^s p(a_i) \log x \end{aligned}$$

Ta có: $\ln x \leq x - 1 \quad \forall x$ (xem hình 3.1)

$$\Rightarrow \sum_{i=1}^s p(a_i) \log x \leq \sum_{i=1}^s p(a_i)(x-1)$$

$$\text{Mà: } \sum_{i=1}^s p(a_i) \left[\frac{1}{p(a_i)s} - 1 \right] = \sum_{i=1}^s \frac{1}{s} - \sum_{i=1}^s p(a_i) = 0$$

Vậy: $H_1(A) - \log s \leq 0 \Rightarrow H_1(A) \leq \log s$

Tóm lại, ta thấy $0 \leq H_1(A) \leq \log s$ (entropie của nguồn rời rạc)

Entropie là một đại lượng giới hạn.

Ký hiệu $H(A)_{\max} = H_0(A)$

Ví dụ: $H_0(\text{Viết}) = \log_2 36 = 5,1713 \text{ bit}$

$$H_0(\text{Nga}) = \log_2 32 = 5 \text{ bit}$$

$$H_0(\text{Anh}) = \log_2 27 = 4,75489 \text{ bit}$$

3.2.4. Entropie của nguồn rời rạc, nhị phân

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

$$\begin{cases} a_1 \Leftrightarrow "0" & \text{với xác suất } p(a_1) = p \\ a_2 \Leftrightarrow "1" & \text{với xác suất } p(a_2) = 1 - p \end{cases}$$

Ta có ngay:

$$H_1(A) = -\sum_{i=1}^2 p(a_i) \log p(a_i) = -p \log p - (1-p) = f(p) \quad (3.18)$$

Đồ thị $f(p)$ được biểu diễn trên hình 3.2.

Ta thấy $H_1(A) = f(p)$ chỉ phụ thuộc vào đặc tính thống kê của các tin.

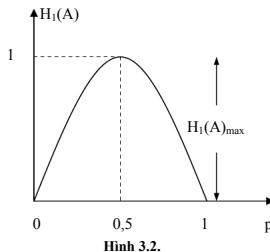
Nếu đơn vị dùng là bit thì $\max H_1(A) = 1$

Nhận xét:

- $H_1(A)$ đạt max tại $p = \frac{1}{2}$. Sở dĩ như vậy vì tập chỉ có hai phần tử, nên độ bất định của phép chọn sẽ lớn nhất khi hai dấu có xác suất xuất hiện như nhau.

- $p = 0 \Rightarrow H_1(A)_{\min} = 0$. Khi đó $1-p = 1$ là xác suất xuất hiện dấu a_2 . Vậy a_2 là một biến cố chắc chắn. Phép chọn này không có độ bất định \Rightarrow lượng thông tin trung bình là 0.

- $p = 1 \Rightarrow H_1(A)_{\min} = 0$. Giải thích tương tự.



Hình 3.2.

3.2.5. Entropie của trường sự kiện đồng thời

Định nghĩa 1:

Có hai trường sự kiện A và B:

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_s \\ p(a_1) & p(a_2) & \dots & p(a_s) \end{pmatrix} \text{ và } B = \begin{pmatrix} b_1 & b_2 & \dots & b_t \\ p(b_1) & p(b_2) & \dots & p(b_t) \end{pmatrix}$$

Các a_i và b_j là các sự kiện.

Ta xét một sự kiện tích: $c_k = a_i \cdot b_j$

$p(c_k) = p(a_i \cdot b_j)$. Ta xét trường C là giao của hai trường A và B, nếu:

$$C = A \cdot B = \begin{pmatrix} a_1 b_1 & a_1 b_2 & \dots & a_1 b_t & \dots & a_2 b_1 & \dots & a_2 b_t & \dots & a_s b_1 & \dots & a_s b_t \\ p(a_1 b_1) & p(a_1 b_2) & \dots & p(a_1 b_t) & \dots & p(a_2 b_1) & \dots & p(a_2 b_t) & \dots & p(a_s b_1) & \dots & p(a_s b_t) \end{pmatrix}$$

Trường C được gọi là trường sự kiện đồng thời (trường giao, tích) của hai trường sự kiện cơ bản A và B.

Định nghĩa 2:

Hai trường sự kiện A và B được gọi là độc lập với nhau nếu:

$$p(a_i \cdot b_j) = p(a_i) \cdot p(b_j)$$

Chú ý: Tất nhiên nếu $p(a_i)$ và $p(b_j)$ thoả mãn (3.14) thì ta cũng có:

$$0 \leq p(a_i \cdot b_j) \leq 1 ; \sum_{i=1}^s \sum_{j=1}^t p(a_i \cdot b_j) = 1 \quad (*)$$

Định lý 1:

Entropie của trường sự kiện đồng thời C = A. B sẽ bằng tổng entropie của các trường sự kiện cơ bản A và B nếu A và B độc lập.

$$H(A \cdot B) = H(A) + H(B) \quad (3.19)$$

Chứng minh: Theo định nghĩa:

$$H(A \cdot B) = - \sum_{i=1}^s \sum_{j=1}^t p(a_i \cdot b_j) \log p(a_i \cdot b_j)$$

Theo giả thiết A và B độc lập với nhau nên ta có:

$$\begin{aligned} H(A \cdot B) &= - \sum_{i=1}^s \sum_{j=1}^t p(a_i) p(b_j) \log p(a_i) - \sum_{i=1}^s \sum_{j=1}^t p(a_i) p(b_j) \log p(b_j) \\ &= - \sum_{i=1}^s p(a_i) \log p(a_i) \sum_{j=1}^t p(b_j) - \sum_{j=1}^t p(b_j) \log p(b_j) \sum_{i=1}^s p(a_i) \end{aligned}$$

$$\text{Mà: } \sum_{j=1}^t p(b_j) = 1, \sum_{i=1}^s p(a_i) = 1$$

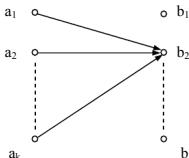
$$\Rightarrow H(A \cdot B) = H(A) + H(B)$$

Nhận xét: Tương tự, nếu các nguồn X_k , ($k = \overline{1, n}$) độc lập với nhau thì:

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

3.3. ENTROPY CÓ ĐIỀU KIỆN. LUỢNG THÔNG TIN CHÉO TRUNG BÌNH

3.3.1. Entropie có điều kiện về một trường tin này khi đã rõ một tin nhất định của



trường tin kia

3.3.1.1. Mở đầu

Trong phần trước, ta đã nói nếu truyền tin có nhiều thì tin phát đi a_k và tin thu được b_ℓ là khác nhau. Và khi đó lượng thông tin riêng về a_k do b_ℓ mang lại là:

$$I(a_k/b_\ell) = \log \frac{1}{p(a_k/b_\ell)}$$

Vấn đề: ta không quan tâm đến lượng thông tin riêng về một dấu a_k cụ thể nào của nguồn tin phát $\{a_i\}$ do b_ℓ mang lại mà chỉ quan tâm đến lượng thông tin riêng trung bình về một dấu nào đó của tập $\{a_i\}$ do b_ℓ mang lại. Ta thấy rằng $I(a_k/b_\ell)$ là một đại lượng ngẫu nhiên. Do đó tương tự như định nghĩa của entropie một chiều, ta đi tới định nghĩa sau.

3.3.1.2. Định nghĩa

Entropie có điều kiện về một trường tin này khi đã rõ một tin của trường tin kia được xác định bằng kỳ vọng của lượng thông tin riêng có điều kiện về a_k do một b_ℓ mang lại:

$$\begin{aligned} H(A/b_\ell) &\stackrel{\Delta}{=} M[I(a_i/b_\ell)] = \sum_{i=1}^s p(a_i/b_\ell) I(a_i/b_\ell) \\ &= - \sum_{i=1}^s p(a_i/b_\ell) \log p(a_i/b_\ell) \end{aligned} \quad (3.20)$$

Ý nghĩa:

$H(A/b_\ell)$ là lượng thông tin tốn hao trung bình của mỗi tin ở đầu phát khi đầu thu đã thu được b_j .

Tương tự:

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

Ý nghĩa:

$H(B/a_i)$ là lượng thông tin riêng trung bình chứa trong mỗi tin ở đầu thu khi đầu phát đã phát đi một tin a_i .

3.3.2. Entropie có điều kiện về trường tin này khi đã rõ trường tin kia

Ta thấy rằng do nhiều ngẫu nhiên nên bên thu không phải chỉ thu được một tin duy nhất mà là cả tập tin $B = \{b_j\}$ nào đó, ($j = \overline{1, t}$). Vậy $H(A/b_j)$ cũng là một đại lượng ngẫu nhiên, do

đó ta phải xét đến lượng thông tin riêng trung bình về mỗi tin ở đầu phát khi đầu thu đã thu được một dấu nào đó.

Tương tự như trên, ta cũng phải lấy trung bình thống kê của đại lượng ngẫu nhiên này.

Định nghĩa:

Entropie có điều kiện của trường sự kiện A khi đã rõ trường sự kiện B được xác định bởi kỳ vọng của đại lượng $H(A/b_j)$.

$$\begin{aligned} H(A/B) & \stackrel{\Delta}{=} M[H(A/b_j)] = \sum_{j=1}^t p(b_j)H(A/b_j) \\ & = \sum_{j=1}^t p(b_j) \left[-\sum_{i=1}^s p(a_i/b_j) \log p(a_i/b_j) \right] \\ & = -\sum_{i=1}^s \sum_{j=1}^t p(b_j)p(a_i/b_j) \log p(a_i/b_j) \end{aligned} \quad (3.21)$$

Ý nghĩa:

$H(A/B)$ là lượng thông tin tồn hao trung bình của mỗi tin ở đầu phát khi đầu thu đã thu được một dấu nào đó.

Tương tự:

$$H(B/A) = -\sum_{i=1}^s \sum_{j=1}^t p(b_j a_i) \log p(b_j/a_i) \quad (3.22)$$

Ý nghĩa:

$H(B/A)$ là lượng thông tin riêng trung bình chứa trong mỗi tin ở đầu thu khi đầu phát đã phát đi một tin nào đó.

Chú ý:

Ta xét một bộ chữ A. Để đặc trưng cho lượng thông tin riêng trung bình chứa trong mỗi con chữ khi kể đến xác suất xuất hiện các cặp chữ (VD: trong tiếng Việt: $p(a/b) \neq 0$, $p(b/a) = 0$, $p(t/a) \neq 0$, $p(a/t) \neq 0$), người ta dùng $H(A/A)$ và ký hiệu là $H_2(A)$.

Ví dụ: $H_2(\text{Việt}) = 3,2223$ bit

$$H_2(\text{Nga}) = 3,52 \text{ bit}$$

$$H_2(\text{Anh}) = 3,32 \text{ bit}$$

Việc tính H_3 , H_4 rất phức tạp.

Khakevich tính được đến H_5 . Shannon tính được đến H_8 .

3.3.3. Hai trạng thái cực đoan của kênh truyền tin

3.3.3.1. Kênh bị đứt (bị nhiễu tuyệt đối)

Trong trường hợp này, các tin thu được hoàn toàn khác các tin phát đi. Nói khác đi vì bị nhiễu tuyệt đối nên trong mọi tin $b_j \in B$ không chứa dấu hiệu gì cả về các tin đã phát đi.

Như vậy, A và B là độc lập nhau: $p(a_i / b_j) = p(a_i)$; $p(b_j / a_i) = p(b_j)$

$$\Rightarrow p(a_i | b_j) = p(a_i) p(b_j)$$

Khi đó ta có:

$$\begin{aligned} H(A/b_j) &= -\sum_{i=1}^s p(a_i) \log p(a_i) = H(A) \\ H(B/a_i) &= -\sum_{j=1}^t p(b_j) \log p(b_j) = H(B) \\ H(A/B) &= -\sum_{j=1}^t p(b_j) \sum_{i=1}^s p(a_i) \log p(a_i) = H(A) \\ H(B/A) &= -\sum_{i=1}^s p(a_i) \sum_{j=1}^t p(b_j) \log p(b_j) = H(B) \end{aligned} \quad (3.23)$$

3.3.3.2. Kênh không nhiễu

Khi đó: $t = s$. Với $\forall i = \overline{1, s}$ $a_i = b_i$

$$\Rightarrow p(a_i) = p(b_i) \text{ nên } H(A) = H(B)$$

$$p(a_k / b_k) = p(b_k / a_k) = 1$$

$$p(a_i / b_k) = p(b_i / a_k) = 0 \text{ với } \forall i \neq k$$

$$\Rightarrow \begin{cases} H(A/b_k) = 0 & H(B/a_k) = 0 \\ H(A/B) = 0 & H(B/A) = 0 \end{cases} \quad (3.24)$$

Vì khi không nhiễu, coi A và B phụ thuộc mạnh nhất, có a_i thì chắc chắn có b_i , nên độ bất định về a_i khi đã thu được b_i là không có \Rightarrow độ bất định trung bình cũng không có.

3.3.4. Các tính chất của entropie có điều kiện

3.3.4.1. Tính chất 1

Nếu A và B là hai trường biến có bất kỳ (hai nguồn tin bất kỳ) thì entropie của trường biến có đồng thời A.B bằng:

$$H(A.B) = H(A) + H(B/A) = H(B) + H(A/B) \quad (3.25)$$

Chứng minh:

$$\begin{aligned} H(A.B) &= - \sum_{i=1}^s \sum_{j=1}^t p(a_i|b_j) \log p(a_i|b_j) = \\ &= - \sum_{i=1}^s \sum_{j=1}^t p(b_j) p(a_i/b_j) \log \{p(b_j)p(a_i/b_j)\} = \\ H(A.B) &= - \sum_{i=1}^s \sum_{j=1}^t p(b_j) p(a_i/b_j) \log p(b_j) - \sum_{i=1}^s \sum_{j=1}^t p(b_j) p(a_i/b_j) \log p(a_i/b_j) = \\ &= - \underbrace{\sum_{i=1}^s p(a_i/b_j) \sum_{j=1}^t p(b_j) \log p(b_j)}_{H(B)} - \underbrace{\sum_{i=1}^s \sum_{j=1}^t p(a_i|b_j) \log p(a_i/b_j)}_{H(A/B)} \\ &= H(B) + H(A/B) \end{aligned}$$

Trong đó: $\sum_{i=1}^s p(a_i/b_j) = 1$.

3.3.4.2. Tính chất 2

Entropie có điều kiện nằm trong khoảng:

$$0 \leq H(A/B) \leq H(A) \quad (3.26)$$

Chứng minh:

+ $H(A/B) \geq 0$:

$$0 \leq p(a_i/b_j) \leq 1 \Rightarrow \log p(a_i/b_j) \leq 0$$

$$\Rightarrow -\log p(a_i/b_j) \geq 0 \Rightarrow H(A/B) \geq 0$$

Nó sẽ nhận dấu bằng khi A và B là đồng nhất (kênh không nhiễu).

+ $H(A/B) \leq H(A)$:

Xét hiệu: $H(A/B) - H(A) = G$

$$G = - \sum_{i=1}^s \sum_{j=1}^t p(b_j) p(a_i / b_j) \log p(a_i / b_j) + \sum_{i=1}^s p(a_i) \log p(a_i) \cdot 1$$

Chú ý: ta thay $1 = \sum_{j=1}^t p(b_j / a_i)$

$$\begin{aligned} \Rightarrow G &= - \sum_{i=1}^s \sum_{j=1}^t p(a_i b_j) \log p(a_i / b_j) + \sum_{i=1}^s \sum_{j=1}^t p(a_i b_j) \log p(a_i) \\ &= - \sum_{i=1}^s \sum_{j=1}^t p(a_i b_j) \log \frac{p(a_i / b_j)}{p(a_i)} \\ &= \sum_{i=1}^s \sum_{j=1}^t p(a_i b_j) \log \frac{p(a_i)}{p(a_i / b_j)} \end{aligned}$$

Áp dụng $\log x \leq x - 1$:

$$\begin{aligned} \Rightarrow G &\leq \sum_{i=1}^s \sum_{j=1}^t p(a_i b_j) \left[\frac{p(a_i)}{p(a_i / b_j)} - 1 \right] \\ G &\leq \sum_{i=1}^s \sum_{j=1}^t p(b_j) p(a_i / b_j) \left[\frac{p(a_i)}{p(a_i / b_j)} - 1 \right] \\ G &\leq \sum_{i=1}^s p(a_i) \sum_{j=1}^t p(b_j) - \sum_{i=1}^s \sum_{j=1}^t p(b_j) p(a_i / b_j) \\ G &\leq 1 \cdot 1 - 1 = 0 \end{aligned}$$

$$\Rightarrow H(A/B) \leq H(A).$$

$H(A/B) = H(A)$ khi A và B là độc lập (kênh bị đứt).

3.3.4.3. Tính chất 3

Entropie của trường sự kiện đồng thời không lớn hơn tổng entropie của các trường sự kiện cơ bản.

$$H(A \cdot B) \leq H(A) + H(B) \quad (3.27)$$

Chứng minh:

(3.27) rút ra trực tiếp từ (3.25) và (3.26).

3.3.5. Lượng thông tin chéo trung bình

Ở phần trước, chúng ta đã biết lượng thông tin chéo về một tin a_i đã phát đi do một tin b_j đã thu được mang lại là:

$$I(a_i, b_j) = \log \frac{p(a_i/b_j)}{p(a_i)}$$

Thông thường, vì bên phát phát đi một tập tin $A = \{a_i\}$ và bên thu nhận được một tập tin $B = \{b_j\}$. Do đó ta không quan tâm đến lượng thông tin chéo về một tin cụ thể a_i đã phát do một tin b_j cụ thể thu được, mà ta chỉ quan tâm đến lượng thông tin chéo trung bình về mỗi tin của tập phát A do mỗi tin của tập thu B mang lại. $I(a_i, b_j)$ là một đại lượng ngẫu nhiên, do đó ta phải lấy trung bình thống kê của nó.

Định nghĩa:

Lượng thông tin chéo trung bình (ký hiệu là $I(A, B)$):

$$I(A, B) = M \left[I(a_i, b_j) \right] \quad (3.28)$$

Xác suất để có thông tin $I(a_i, b_j)$ là $p(a_i, b_j)$, do đó ta có:

$$\begin{aligned} I(A, B) &= \sum_{i=1}^s \sum_{j=1}^t p(a_i, b_j) \log \frac{p(a_i/b_j)}{p(a_i)} \\ I(A, B) &= \sum_{i=1}^s \sum_{j=1}^t p(a_i, b_j) \log p(a_i/b_j) - \sum_{i=1}^s \sum_{j=1}^t p(a_i, b_j) \log p(a_i) \\ &= -H(A/B) + H(A) \end{aligned} \quad (3.29a)$$

Tóm lại: $I(A, B) = H(A) - H(A/B)$ (3.29a)

Tương tự, ta có: $I(A, B) = H(B) - H(B/A)$ (3.29b)

Hay: $I(A, B) = H(A) + H(B) - H(A, B)$

$I(A, B)$ còn gọi là lượng thông tin trung bình được truyền theo kênh rời rạc.

3.3.6. Tính chất của $I(A, B)$

3.3.6.1. Tính chất 1

$$I(A, B) \geq 0: \quad (3.30)$$

Theo tính chất 2 ở mục 3.3.4: $H(A/B) \leq H(A) \Rightarrow H(A) - H(A/B) \geq 0$.

$I(A, B) = 0$ khi kênh bị đứt.

3.3.6.2. Tính chất 2

$$I(A,B) \leq H(A); \quad (3.31)$$

Thật vậy: $H(A/B) \geq 0 \Rightarrow I(A,B) = H(A) - H(A/B) \leq H(A)$

$I(A,B) = H(A)$ khi kênh không có nhiễu.

Từ (3.31) ta thấy khi truyền tin trong kênh có nhiễu, thông tin sẽ bị tốn hao một phần. Lượng thông tin tốn hao trung bình chính là $H(A/B)$.

3.3.6.3. Tính chất 3

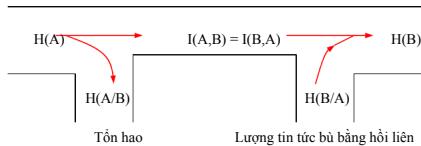
$$I(A,A) = H(A)$$

3.3.6.4. Tính chất 4

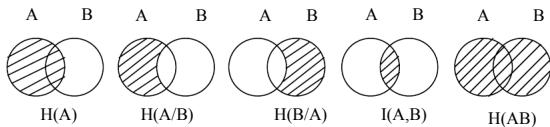
$$I(A,B) = I(B,A)$$

3.3.7. Mô hình của kênh truyền tin có nhiễu

Dựa vào (3.29a), ta có mô hình kênh truyền khi có nhiễu như sau:



Hình 3.3.



Hình 3.4. 图形描述了信道容量与互信息之间的关系。

3.4. TỐC ĐỘ PHÁT, KHẢ NĂNG PHÁT, ĐỘ THỪA, KHẢ NĂNG THÔNG QUA CỦA KÊNH RỜI RẠC

3.4.1. Tốc độ phát của nguồn rời rạc

Trong thông tin rời rạc, người ta thường phát đi các xung. Nếu gọi T_n là độ rộng trung bình của mỗi xung thì tốc độ phát của nguồn tin rời rạc được định nghĩa như sau:

$$v_n = \frac{1}{T_n} \quad (3.32)$$

(3.32) biểu thị số xung trong một đơn vị thời gian.

Thứ nguyên: $[v_n] = \text{bốt} = \text{số dấu (xung)/ sec}$

Ví dụ: Điện báo tay: $v_n = 25$ bốt.

Điện báo tự động: $v_n = (50 \div 300)$ bốt.

Thông tin truyền số liệu: $(500 \div n \cdot 10^4)$ bốt.

3.4.2. Khả năng phát của nguồn rời rạc

Định nghĩa:

$$H'(A) = v_n H(A) = \frac{H(A)}{T_n} \quad (3.33)$$

Thứ nguyên: $[H'(A)] = \text{bit/sec}$.

$$\max H'(A) = \frac{1}{T_n} H(A)$$

(3.33) biểu thị lượng thông tin trung bình do nguồn phát ra trong một đơn vị thời gian.

Ví dụ: Một máy điện báo dùng mã Bôđô đều 5 dấu, cơ số 2, tốc độ phát là 75 bốt thì khả năng tối đa của máy là:

$$H'(A)_{\max} = v_n \cdot H_1(A)_{\max} = 75 \cdot \log_2 2^5 = 375 \text{ bit/s}$$

3.4.3. Độ thừa của nguồn rời rạc

Định nghĩa:

Độ thừa của nguồn rời rạc là tỷ số:

$$D = \frac{\Delta H(A)_{\max} - H(A)}{H(A)_{\max}} = 1 - \frac{H(A)}{H(A)_{\max}} \quad (3.34)$$

$$D = 1 - \mu, \text{ trong đó: } \mu = \frac{H(A)}{H(A)_{\max}} \text{ được gọi là hệ số nén tin.}$$

Đối với nguồn tin có s dấu: $H(A)_{\max} = H_0(A) = \log s$.

Ý nghĩa:

Dộ thừa đặc trưng cho hiệu suất, khả năng chống nhiễu và độ mật của tin. Nếu D càng lớn thì hiệu suất càng thấp, độ mật càng thấp nhưng khả năng chống nhiễu càng cao.

Ví dụ:

- Đối với tiếng Việt: $H_1(\text{Việt}) = 4.5167$; $H_0(\text{Việt}) = 5.1713$

$$\Rightarrow \mu_1 = 87\% \Rightarrow D_1 = 13\%$$

$$\mu_2 = \frac{H_2(A)}{\log s} = \frac{3,2223}{5,1713} = 62\% \Rightarrow D_2 = 38\%$$

- Đối với tiếng Nga: $\mu_1 = 87\% \Rightarrow D_1 = 13\%$

$$\mu_3 = 60\% \Rightarrow D_3 = 40\%$$

- Đối với tiếng Anh: $\mu_1 = 84\% \Rightarrow D_1 = 16\%$

$$\mu_8 = 38\% \Rightarrow D_8 = 62\%$$

3.4.4. Các đặc trưng của kênh rời rạc và các loại kênh rời rạc

Một kênh rời rạc hoàn toàn được đặc trưng bởi ba tham số sau:

- Trường dấu lối vào và trường dấu lối ra của kênh.

- Xác suất chuyển $p(b_j/a_i)$

- Tốc độ truyền tin của kênh v_K

Định nghĩa 1:

Nếu một kênh có $p(b_j/a_i) \notin t$ thì được gọi là kênh đồng nhất; $p(b_j/a_i) \in t$ thì được gọi là không đồng nhất; $p(b_j/a_i) \in v$ là dấu đã phát trước nó thì được gọi là kênh có nhớ ($\forall i, j$).

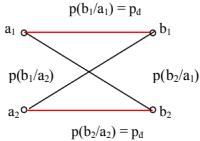
Định nghĩa 2:

Nếu một kênh có xác suất chuyển:

$$p(b_j/a_i) = \begin{cases} p_s = \text{const} & \forall i \neq j, i = \overline{1, s}, j = \overline{1, t} \\ p_d = \text{const} & \forall i = j \end{cases}$$

thì kênh đó sẽ được gọi là kênh đối xứng.

Ví dụ:



✓ xác suất sai bằng nhau, ∀ xác suất đúng bằng nhau.

Đối với kênh đối xứng nhị phân (Hình vẽ): $p_s + p_d = 1$.

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

Định nghĩa:

$$I'(A, B) \stackrel{\Delta}{=} \frac{I(A, B)}{T_K} = v_K I(A, B) \quad [\text{bit/s}] \quad (3.35)$$

Trong đó: $v_K = \frac{1}{T_K}$, T_K : thời gian trung bình để truyền một dấu qua kênh. v_K biểu thị

số dấu mà kênh đã truyền được (được truyền qua kênh) trong một đơn vị thời gian. $I'(A, B)$ là lượng thông tin đã truyền qua kênh trong một đơn vị thời gian.

Nếu kênh giãn tin: $T_K > T_n$

Nếu kênh nén tin: $T_K < T_n$

Thông thường: $T_K = T_n$

3.4.6. Khả năng thông qua của kênh rời rạc

Để đánh giá năng lực tái tạo tối đa của một kênh truyền, người ta đưa ra khái niệm khả năng thông qua.

3.4.6.1. Định nghĩa

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 có của nguồn tin A. (Cực đại này sẽ đạt được ứng với một phân bố tối ưu của các xác suất tiên nghiệm $p(a_i)$, $\forall a_i \in A$).

$$C' = \max_A^{\Delta} I'(A, B) = v_K \max_A I(A, B) \quad [\text{bit/s}] \quad (3.36)$$

$$C' = v_K C \quad \text{với } C = \max_A I(A, B)$$

C được gọi là khả năng thông qua của kênh đối với mỗi dấu.

C' là một tham số rất quan trọng của một kênh.

3.4.6.2. Tính chất

- $C' \geq 0$, $C' = 0$ khi và chỉ khi A và B độc lập (kênh bị đứt).
- $C' \leq v_K \log s$, đẳng thức chỉ xảy ra khi kênh không nhiễu. (3.37)

Chứng minh:

$$\begin{aligned} I(A, B) &\leq H(A) \\ v_K I(A, B) &\leq v_K H(A) \quad (v_K > 0) \\ \max(v_K I(A, B)) &\leq \max(v_K H(A)) \\ v_K \underbrace{\max I(A, B)}_{\leq} &\leq v_K \underbrace{\max H(A)}_{\leq} \\ C' &\leq v_K \log s \end{aligned}$$

3.4.7. Tính khả năng thông qua của kênh nhị phân đối xứng không nhớ, đồng nhất

3.4.7.1. Đặt bài toán

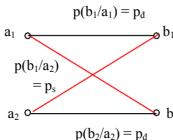
Ta có một kênh nhị phân như hình 3.4. Trong đó:

Xác suất sai: $p(b_2 / a_1) = p(b_1 / a_2) = p_s$

Xác suất đúng: $p(b_2 / a_2) = p(b_1 / a_1) = p_d$

$p(a_1) = p$; $p(a_2) = 1 - p$;

Các dấu a_1 và a_2 có cùng thời hạn T. Vấn đề: tính C' ?



3.4.7.2. Giải bài toán

Ta có:

$$C' = \frac{1}{T_K} \max_A I(A, B) = \frac{1}{T_K} \max_A [H(B) - H(B/A)]$$

Ta có ngay:

$$H(B/A) = - \sum_{i=1}^2 \sum_{j=1}^2 p(a_i) p(b_j / a_i) \log p(b_j / a_i)$$

$$\begin{aligned}
 H(B/A) &= -p(a_1)[p(b_1/a_1)\log p(b_1/a_1) + p(b_2/a_1)\log p(b_2/a_1)] \\
 &\quad - p(a_2)[p(b_1/a_2)\log p(b_1/a_2) + p(b_2/a_2)\log p(b_2/a_2)] \\
 &= -p[(1-p_s)\log(1-p_s) + p_s\log p_s] \\
 &\quad - (1-p)[p_s\log p_s + (1-p_s)\log(1-p_s)] \\
 H(B/A) &= -[p_s\log p_s + (1-p_s)\log(1-p_s)]
 \end{aligned}$$

Ta thấy $H(B/A)$ chỉ phụ thuộc vào p_s , mà không phụ thuộc vào xác suất tiên nghiệm của các dấu thuộc nguồn tin A. Do đó:

$$\begin{aligned}
 C' &= \frac{1}{T_K} \max_A [H(B) - H(B/A)] \\
 &= \frac{1}{T_K} \max_A H(B) - \frac{1}{T_K} H(B/A)
 \end{aligned}$$

Ở đây $H(B/A)$ không đổi đối với mọi trạng thái (đặc tính thống kê) của nguồn A.

Mà:

$$\max_A H(B) = H(B)_{\max} = \log_2 s = \log_2 2 = 1$$

$$\text{Vậy: } C' = \frac{1}{T_K} [1 + p_s \log p_s + (1-p_s) \log(1-p_s)]$$

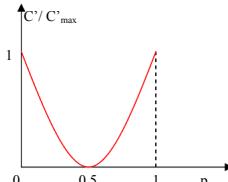
$$C' = f(p_s, T_K)$$

$$C'_{\max} = \frac{1}{T_K} \Leftrightarrow p_s = 0 \Leftrightarrow \text{Kênh không nhiễu.}$$

$$\frac{C'}{C'_{\max}} = 1 + p_s \log p_s + (1-p_s) \log(1-p_s)$$

(3.38)

Đồ thị (3.38) biểu diễn trên hình 3.5.



Hình 3.5.

3.4.8. Định lý mã hóa thứ hai của Shannon

Định lý: Nếu khả năng phát $H'(A)$ của nguồn tin rời rạc A bé hơn khả năng thông qua của kênh: ($H'(A) < C'$) thì tồn tại một phép mã hóa và giải mã sao cho việc truyền tin có xác suất gấp lối bé tuỳ ý (nếu $H'(A) > C'$ thì không tồn tại phép mã hóa và giải mã như vậy) khi độ dài từ mã đủ lớn.

Nhận xét: Đây là một định lý tồn tại vì nó không chỉ cho ta cách thiết lập một mã cụ thể nào. Lý thuyết mã kênh trong chương 4 chính là hướng dẫn cần thiết cho định lý này.

3.4.9. Khả năng thông qua của kênh nhị phân đối xứng có xoá

3.4.9.1. Đặt bài toán

Cho kênh truyền, các dấu a_1 và a_2 như hình vẽ. Các dấu a_1 và a_2 có cùng thời hạn T. Hãy tính khả năng thông qua C' của kênh này với điều kiện:

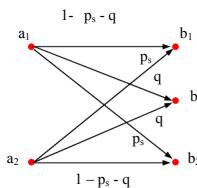
$$\text{Xác suất xoá: } p(b_3/a_1) = q$$

Xác suất thu đúng:

$$p(b_1/a_1) = p(b_2/a_2) = 1 - p_s - q$$

Xác suất thu sai:

$$p(b_2/a_1) = p(b_1/a_2) = p_s$$



3.4.9.2. Giải bài toán

Tương tự bài toán trên, ta có:

$$C' = \frac{1}{T} \max_A [H(B) - H(B/A)]$$

Trong đó:

$$\begin{aligned} H(B/A) &= -\sum_{i=1}^2 \sum_{j=1}^3 p(a_i)p(b_j/a_i) \log p(b_j/a_i) \\ &= -p[(1-p_s-q)\log(1-p_s-q) + p_s \log p_s + q \log q] \\ &\quad - (1-p)[p_s \log p_s + (1-p_s-q)\log(1-p_s-q) + q \log q] \\ &= -(1-p_s-q)\log(1-p_s-q) + p_s \log p_s + q \log q \end{aligned}$$

Ta thấy $H(B/A) \notin$ vào tính chất thống kê của nguồn A. Do đó:

$$\max_A [H(B) - H(B/A)] = \max_A H(B) - H(B/A)$$

$$H(B) = -\sum_{j=1}^3 p(b_j) \log p(b_j)$$

Trong đó:

$$\begin{aligned} p(b_3) &= p(a_1)p(b_3/a_1) + p(a_2)p(b_3/a_2) \\ &= pq + (1-p)q = q \end{aligned}$$

không phụ thuộc vào tính chất thống kê của nguồn A.

Như vậy, $H(B)$ sẽ đạt max ứng với phân bố của các xác suất $p(a_i)$ đảm bảo được:

$$p(b_1) = p(b_2) = \frac{1-q}{2}$$

$$\Rightarrow \max_A H(B) = -q \log q - (1-q) \log \frac{(1-q)}{2}$$

$$\Rightarrow C' = F \left\{ (1-q) [1 - \log(1-q)] + p_s \log p_s + (1-p_s-q) \log(1-p_s-q) \right\}$$

$$\text{Trong đó } F = \frac{1}{T}$$

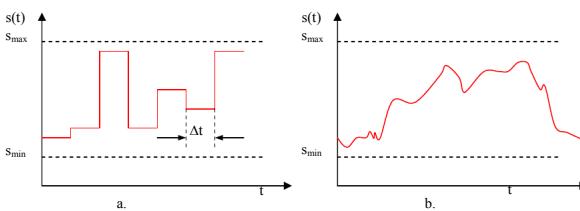
3.5. ENTROPY CỦA NGUỒN LIÊN TỤC. LUỢNG THÔNG TIN CHÉO TRUNG BÌNH TRUYỀN QUA KÊNH LIÊN TỤC KHÔNG NHỐ

3.5.1. Các dạng tín hiệu liên tục

Đối với các tín hiệu cao tần liên tục $s(t)$ thì giá trị của nó có thể nhận một cách liên tục các giá trị khác nhau trong một khoảng xác định $s_{\min} \div s_{\max}$, còn đối số thời gian t lại có thể liên tục hay rời rạc (hình 3.6).

Vì vậy, ta sẽ phân các tín hiệu liên tục ra 2 loại.

- Tin hiệu liên tục với thời gian rời rạc (hình 3.6a).
- Tin hiệu liên tục với thời gian liên tục (hình 3.6b).



Hình 3.6.

Các tham số đặc trưng của tín hiệu liên tục là:

- Công suất phô trung bình
- Bề rộng phô

3.5.2. Các đặc trưng và tham số của kênh liên tục

Ta đã biết rằng các đặc trưng của kênh rời rạc là:

- Trường dấu lồi vào trước hay sau bộ mã hóa: A

- Trường dấu lỗi ra sau bộ giải điều chế hoặc sau bộ giải mã B.

- Xác suất chuyên $p(a_i / b_j)$ hoặc $p(\alpha_i^{(n)} / \beta_i^{(n)})$

Đối với kênh liên tục, các đặc trưng của nó là:

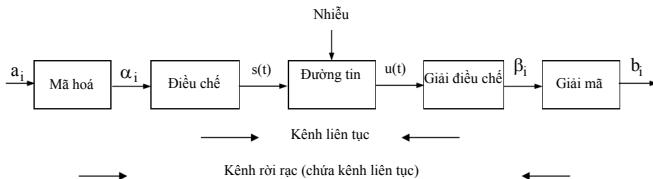
- Trường dấu lỗi vào (sau bộ điều chế): $\{s(t)\}$

- Trường dấu lỗi ra (trước bộ giải điều chế): $\{U(t)\}$

- Mật độ phân bố xác suất để xuất hiện $U_j(t)$ khi đã phát hiện $s_i(t)$:

$$W(U_j(t) / s_i(t))$$

Cũng như đối với kênh rời rạc tham số quan trọng nhất của kênh liên tục là khả năng thông qua của nó.



Định nghĩa:

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:

$$u(t) = \mu \cdot s(t) + n(t) \quad (3.39)$$

Trong đó $\mu = \text{const.}$, $(\notin t)$, $n(t)$: nhiễu công là tập âm trắng phân bố chuẩn.

3.5.3. Kênh liên tục chứa trong kênh rời rạc

Tính chất:

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

$$C_{lt}' \geq C_{r,r \text{ chứa } lt}' \quad (3.40)$$

Chứng minh:

Nếu phép giải điều chế và điều chế là hai phép thuận nghịch lẫn nhau như ta mong muốn thì khi qua bộ điều chế và giải điều chế lượng thông tin là không đổi (lượng thông tin truyền qua

kênh trong một đơn vị thời gian). Như vậy, khả năng thông qua của kênh liên tục đúng bằng khả năng thông qua của kênh rời rạc. Tuy nhiên phép giải điều chế thường làm tổn hao thông tin, do đó khả năng thông qua của kênh rời rạc không thể lớn hơn khả năng thông qua của kênh liên tục nằm trong nó.

3.5.4. Entropie của nguồn tin liên tục (của một quá trình ngẫu nhiên liên tục)

Xét một nguồn tin S ở mỗi một thời điểm có thể phát ra những tin là một đại lượng ngẫu nhiên s có thể nhận các giá trị liên tục trong khoảng $s_{\min} \div s_{\max}$ với mật độ xác suất $W_1(s)$.

Vì trong khoảng $s_{\min} \div s_{\max}$ ta có vô số những giá trị của s nên tập tin của nguồn S là một tập vô hạn và như vậy S là một nguồn tin liên tục. Để tính entropie của nguồn này ta làm như sau:

Ta thực hiện một phép lượng tử hoá hình thức bằng cách chia khoảng $s_{\min} \div s_{\max}$ ra n phần bằng nhau. Mỗi phần bằng Δs và được gọi là bước lượng tử (hình 3.7).

Ta coi rằng s sẽ nhận giá trị s_i nếu giá trị của nó nằm trong một phần thứ i nào đó. Như vậy s có thể nhận các giá trị sau: $S' = \{s_i\}, i = \overline{1, n}$. Xác suất để s nhận giá trị s_i sẽ là:

$$p(s_i) \approx W_1(s_i) \Delta s$$

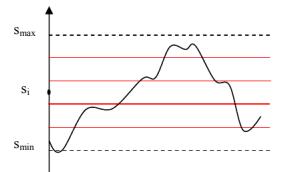
Entropie của nguồn tin đã rời rạc hoá S' sẽ bằng:

$$H(S') = \sum_{i=1}^n W_1(s_i) \Delta s \log [W_1(s_i) \Delta s]$$

Khi cho $\Delta s \rightarrow 0$, ta sẽ được entropie của nguồn tin liên tục.

$$\begin{aligned} H(S) &= \lim_{\Delta s \rightarrow 0} H(S') = \lim_{\Delta s \rightarrow 0} \left(- \sum_{i=1}^n W_1(s_i) \log [W_1(s_i)] \Delta s \right) + \\ &\quad + \lim_{\Delta s \rightarrow 0} \left(\log \frac{1}{\Delta s} \sum_{i=1}^n W_1(s_i) \Delta s \right) \end{aligned}$$

$$H(S) = \int_{-\infty}^{\infty} W_1(s) \log \frac{1}{W_1(s)} ds + \left[\lim_{\Delta s \rightarrow 0} \frac{1}{\Delta s} \underbrace{\left[\int_{-\infty}^{\infty} W_1(s) ds \right]}_{=1} \right]$$



Hình 3.7.

$$\Rightarrow H(S) = \int_{-\infty}^{\infty} W_1(s) \log \frac{1}{W_1(s)} ds + \lim_{\Delta s \rightarrow 0} \frac{1}{\Delta s} \quad (3.41)$$

Từ (3.41) ta thấy entropie một chiều của nguồn tin liên tục lớn vô hạn do $\lim_{\Delta s \rightarrow 0} \frac{1}{\Delta s} = \infty$.

Số hạng thứ hai không phụ thuộc vào bản chất thông kê của nguồn (tín hiệu) mà chỉ có số hạng thứ nhất phụ thuộc vào bản chất thông kê của nguồn, vì vậy ta có thể lấy nó đặc trưng cho những quá trình ngẫu nhiên khác nhau. Ta đặt:

$$h(S) = \int_{-\infty}^{\infty} W_1(s) \log \frac{1}{W_1(s)} ds \quad (3.42)$$

và gọi $h(S)$ là entropie vi phân (hay entropie tương đối) của nguồn S .

Chú ý:

- Khác với entropie của nguồn rời rạc, $h(S)$ có thể nhận các giá trị dương, âm (hữu hạn).

- Khác với entropie của nguồn rời rạc, $h(S)$ phụ thuộc vào thang tỷ lệ của s , tức là phụ thuộc vào việc chọn đơn vị đo. Nếu tăng s lên v lần: $s^* = vs$, khi đó:

$$W_1(s^*) = W_1(s) \left| \frac{ds}{ds^*} \right| = \frac{1}{v} W_1(s)$$

$$\Rightarrow h(s^*) = - \int_{-\infty}^{\infty} W_1(s^*) \log W_1(s^*) ds^* = h(s) + \log v$$

$h(S)$ cũng có tính chất cộng tính.

3.5. Mẫu vật lý minh họa sự lớn vô hạn của entropie của nguồn liên tục

Giả sử ta truyền tin từ A đến B bằng đường dây lý tưởng: không tốn hao, không gây nhiễu. Ở đầu B ta đặt một máy thu là một volt kế lý tưởng (có tap âm nội bộ bằng không, nên có thể đo với độ chính xác tuy ý, $Z_V = \infty$). Tin hiệu phát nằm trong khoảng (0 ± 1) Vol. Như vậy, ở đầu thu ta sẽ nhận được $u = s$.



Hình 3.8.

Nếu trường $A = \{a_i\}$, $i = \overline{1,10}$ (có 10 tin) thì ta có thể mã hóa một cách đơn giản bằng cách đổi chứng như sau:

$$a_1 \leftrightarrow 0,1V, a_2 \leftrightarrow 0,2V, \dots, a_{10} \leftrightarrow 1V$$

Giả sử các tin là đồng xác suất thì $H(A) = \log 10$.

Nếu $A = \{a_i\}$, $i = \overline{1,100}$ thì ta có thể phát đi bằng cách đổi chứng:

$$a_1 \leftrightarrow 0,01V, a_2 \leftrightarrow 0,02V, \dots, a_{100} \leftrightarrow IV$$

Nếu các tin là dòng xác suất thì $H(A) = \log 100$.

Tương tự, nếu $i = \overline{1, 10^6}$ thì chỉ cần chọn bước lượng từ $\Delta s = 10^{-6}$ thì ta có thể đảm bảo truyền được mọi tin. Nếu các tin là dòng xác suất thì $H(A) = \log 10^6$.

Vì kênh và thiết bị thu không có nhiều nén ta có thể chọn Δs bé tuy ý để truyền một số tin lớn tuỳ ý. Khi đó entropie của nguồn tin có thể lớn tuỳ ý. Nếu $\Delta s \rightarrow 0 \Rightarrow H(A) \rightarrow \infty$.

Trong thực tế, luôn tồn tại nhiều n(t) trên đường dây và volt kế luôn có tạp âm nội bộ. Do đó không thể chọn Δs nhỏ tuỳ ý được mà phải là một số hữu hạn. Vì vậy entropie của nguồn trên thực tế là hữu hạn.

3.5.6. Lượng thông tin chéo trung bình truyền theo kênh liên tục không nhớ

Xét một nguồn liên tục S và giả thiết các tin s do nguồn sinh ra là độc lập thống kê với nhau, nghĩa là xét nguồn liên tục không nhớ. Xét kênh liên tục chỉ có can nhiễu cộng n(t) có các giá trị cùng độc lập thống kê với nhau. Khi đó ở lối ra của kênh ta nhận được các tin:

$$u = \mu s + n$$

Các tin này cũng độc lập thống kê với nhau. Khi đó kênh xét cũng là kênh liên tục không nhớ. Ta sẽ tính lượng thông tin trung bình truyền theo kênh này: $I(S, U)$.

Ta cũng sẽ lượng tử hóa các tin ở đầu thu và đầu phát. Bước lượng tử ở đầu phát là Δs , bước lượng tử ở đầu thu là Δu . Khi đó ta có hai nguồn đã rời rạc sau: $S' = \{s_i\}, i = \overline{1, n}$ và $U' = \{u_j\}, j = \overline{1, m}$. Tương tự như mục 4, ta có:

$$\text{Xác suất để s nhận giá trị } s_i \text{ sẽ là: } p(s_i) = W_1(s_i) \cdot \Delta s.$$

$$\text{Tương tự, ta có: } p(u_j) = W_1(u_j) \cdot \Delta u.$$

Xác suất để đồng thời s nhận giá trị s_i và u nhận giá trị u_j gần đúng bằng:

$$p(s_i, u_j) = W_2(s_i, u_j) \cdot \Delta s \cdot \Delta u$$

Nếu coi s_i là tin truyền đi và u_j là tin nhận được tương ứng thì khi đó kênh sẽ là rời rạc không nhớ và lượng thông tin chéo trung bình truyền theo kênh rời rạc đó là:

$$I(S', U') = \sum_{i=1}^n \sum_{j=1}^m W_2(s_i, u_j) \Delta s \Delta u \cdot \log \frac{p(s_i / u_j)}{p(s_i)}$$

Chú ý rằng theo công thức nhân xác suất:

$$p(s_i/u_j) = \frac{p(s_i, u_j)}{p(u_j)} = \frac{W_2(s_i, u_j) \cdot \Delta s \cdot \Delta u}{W_1(u_j) \cdot \Delta u}$$

$$\Rightarrow I(S', U') = \sum_{i=1}^n \sum_{j=1}^m W_2(s_i, u_j) \cdot \Delta s \cdot \Delta u \cdot \log \frac{W_2(s_i, u_j) \cdot \Delta s \cdot \Delta u}{W_1(u_j) \cdot \Delta u \cdot W_1(s_i) \cdot \Delta s}$$

Khi cho $\Delta s \rightarrow 0$ và $\Delta u \rightarrow 0$ ta sẽ chuyển từ kênh rời rạc sang kênh liên tục và lượng thông tin trung bình truyền theo kênh liên tục là:

$$I(S, U) = \lim_{\substack{\Delta s \rightarrow 0 \\ \Delta u \rightarrow 0}} I(S', U') = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_2(s, u) \log \frac{W_2(s, u)}{W_1(s) \cdot W_1(u)} ds \cdot du \quad (3.43a)$$

hay

$$I(S, U) = M \left[\log \frac{W_2(s, u)}{W_1(s) \cdot W_1(u)} \right] \quad (3.43b)$$

3.6. ENTROPIE VI PHÂN CÓ ĐIỀU KIỆN. TÍNH CHẤT CỦA CÁC TÍN HIỆU GAUSSE

3.6.1. Entropie vi phân có điều kiện

Từ (3.43b), ta có:

$$I(S, U) = M \left[\log \frac{1}{W_1(s)} + \log \frac{W_2(s, u)}{W_1(u)} \right]$$

$$\Rightarrow I(S, U) = M \left[\log \frac{1}{W_1(s)} \right] + M \left[\log \frac{W_2(s, u)}{W_1(u)} \right]$$

$$= \int_{-\infty}^{\infty} W_1(s) \log \frac{1}{W_1(s)} ds + \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_2(s, u) \log \frac{W_2(s, u)}{W_1(u)} ds \cdot du \quad (3.44a)$$

Ta có thể viết dưới dạng sau:

$$I(S, U) = h(S) - h(S/U) \quad (3.44b)$$

Trong đó $h(S)$ chính là entropie vi phân của nguồn.

$$h(S) = \int_{-\infty}^{\infty} W_1(s) \log \frac{1}{W_1(s)} ds$$

$$\begin{aligned}
 h(S/U) &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_2(s,u) \log \frac{W_1(u)}{W_2(s,u)} ds du \\
 &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_2(s,u) \log \frac{1}{W_1(s/u)} ds du
 \end{aligned} \tag{3.45}$$

Chú ý:Theo công thức xác suất nhân: $W_2(s,u) = W_1(u)W_1(s/u)$

$h(S/U)$ tính theo (3.45) được gọi là entropie vi phân có điều kiện của nguồn S khi đã biết nguồn U.

Đối với nguồn rời rạc, ta có: $I(A,B) = H(A) - H(A/B)$ $H(A)$ là lượng thông tin riêng trung bình chia trong mỗi dấu của A. $H(A/B)$ là lượng thông tin tồn hao trung bình của mỗi tin do nhiễu trong kênh gây ra.Về mặt hình thức, ta thấy $h(S)$ đóng vai trò của $H(A)$, còn $h(S/U)$ đóng vai trò của $H(A/B)$.

Về mặt ý nghĩa thì không phải như vậy, bởi vì $h(S)$ và $h(S/U)$ có thể âm và phụ thuộc vào thang tỷ lệ. Tuy vậy, việc đưa ra $h(S)$ và $h(S/U)$ rất có lợi cho việc tính toán.

Từ (3.44a) và (3.44b) ta có thể suy ra các tính chất sau của $I(S,U)$:

- $I(S,U) \geq 0$, $I(S,U) = 0$ khi kênh bị đứt: $W(u/s) = W(u)$

- $I(S,U) = I(U,S) = h(U) - h(U/S)$: tính chất đối xứng.

- Nếu kênh là không nhiễu $n(t) = 0$ thì $I(S,U) = \infty$.

Hai tính chất đầu tương tự như trong trường hợp kênh rời rạc không nhớ. Tính chất sau suy ra từ tính chất lớn vô hạn của entropie của nguồn liên tục.

Chú ý: $I(S,U)$ không phụ thuộc vào thang tỷ lệ.

3.6.2. Entropie vi phân của nhiễu Gausse

Xét nhiễu Gausse $n(t)$ có $M[n] = 0$ và $D[n] = P_n$.

Hàm mật độ phân bố xác suất của nó là:

$$W(n) = \frac{1}{\sqrt{2\pi P_n}} \exp \left\{ -\frac{n^2}{2P_n} \right\}$$

Ta sẽ tính vi phân entropie vi phân của nhiễu này.

Ta có: $h(N) = \int_{-\infty}^{\infty} W(n) \log \left(\sqrt{2\pi P_n} e^{\frac{n^2}{2P_n}} \right) dn$

$$\begin{aligned} h(N) &= \int_{-\infty}^{\infty} W(n) \cdot \log \sqrt{2\pi P_n} \cdot dn + \int_{-\infty}^{\infty} W(n) \cdot \log e^{\frac{n^2}{2P_n}} \cdot dn \\ &= \log \sqrt{2\pi P_n} \underbrace{\int_{-\infty}^{\infty} W(n) dn}_{=1} + \frac{\log e}{2P_n} \underbrace{\int_{-\infty}^{\infty} n^2 \cdot W(n) dn}_{=D[n] = P_n} \\ \Rightarrow h(N) &= \log \sqrt{2\pi P_n} + \frac{1}{2} \log e \\ \Rightarrow h(N) &= \log \sqrt{2\pi P_n} e \end{aligned} \quad (3.46)$$

3.6.3. Lượng thông tin chéo trung bình truyền theo kênh Gausse

Ta có:

$$\begin{aligned} I(S, U) &= h(U) - h(U/S) \\ &= \int_{-\infty}^{\infty} W_1(u) \log \frac{1}{W_1(u)} du - h(U/S) \end{aligned}$$

Ta sẽ tính $h(U/S)$ trong trường hợp nhiễu Gausse. Kênh ta xét sẽ là kênh Gausse:

$$\begin{aligned} u(t) &= \mu s(t) + n(t) \\ h(U/S) &= - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_2(s, u) \cdot \log W_1(u/s) \cdot du \cdot ds \\ h(U/S) &= - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_1(s) \cdot W_1(u/s) \cdot \log W_1(u/s) \cdot du \cdot ds \\ &= - \int_{-\infty}^{\infty} W_1(s) \cdot ds \int_{-\infty}^{\infty} W_1(u/s) \cdot \log W_1(u/s) \cdot du \\ h(U/S) &= - \int_{-\infty}^{\infty} W_1(u/s) \cdot \log W_1(u/s) \cdot du \end{aligned} \quad (3.47)$$

Để xác định $h(U/S)$ ta phải tính được $W_1(u/s)$.

Vì yếu tố ngẫu nhiên chỉ do nhiều gây nên, do đó với bất cứ một giá trị nhất định nào của s thì xác suất để u rơi vào khoảng du cũng chính bằng xác suất để n rơi vào khoảng dn.

$$\begin{aligned}
 p\left\{u \in \frac{du}{s} \middle/ s\right\} &= p\{n \in dn\} \\
 W_1(u/s)du &= W_1(n)dn \\
 \Rightarrow W_1(u/s) &= W_1(n) \frac{dn}{du} = W_1(n) \left/ \frac{du}{dn} \right. \\
 \text{Với } \frac{du}{dn} &= \frac{d}{dn}(s+n) = \frac{ds}{dn} + \frac{dn}{dn} = 1 \quad \left(\text{Vì } \frac{ds}{dn} = 0 \text{ khi } s, n \text{ độc lập} \right) \\
 \text{Vậy } W_1(u/s) &= W_1(n) = \frac{1}{\sqrt{2\pi P_n}} \exp\left\{-\frac{n^2}{2P_n}\right\} \\
 \Rightarrow h(U/S) &= h(n) = \log \sqrt{2\pi e P_n} \\
 \Rightarrow I(U,S) &= \int_{-\infty}^{\infty} W_1(u) \log \frac{1}{W_1(u)} du - \log \sqrt{2\pi e P_n} \tag{3.48}
 \end{aligned}$$

Nếu u cũng có phân bố chuẩn thì:

$$h(U) = \log \sqrt{2\pi e P_u}$$

Do s(t) và n(t) là độc lập nên:

$$P_u = P_s + P_n = \sigma_u^2 + \sigma_n^2$$

$$\text{Vậy: } h(U) = \log \sqrt{2\pi e (P_s + P_n)}$$

Cuối cùng, ta có: $I(S,U) = h(U) - h(S/U)$

$$I(S,U) = \log \sqrt{1 + \frac{P_s}{P_n}} = \frac{1}{2} \log \left(1 + \frac{P_s}{P_n} \right) \tag{3.49}$$

Trong đó P_s là công suất trung bình của tín hiệu hữu ích (tín hiệu phát).

Nhận xét:

Từ (3.49) ta thấy $I(S,U)$ không phụ thuộc vào hình dạng và cấu trúc của tín hiệu, mà chỉ phụ thuộc vào tỷ số P_s / P_n . Thực ra kết luận này chỉ đúng về hình thức, thực ra sau này ta sẽ thấy nếu cấu trúc và hình dạng của tín hiệu thay đổi thì P_s / P_n cũng sẽ thay đổi, do đó $I(S,U)$ cũng sẽ khác nhau đối với các tín hiệu có cấu trúc và hình dạng khác nhau.

3.6.4. Tính chất của các tín hiệu có phân bố chuẩn

Định lý:

Trong số những quá trình (tín hiệu) có cùng công suất trung bình (σ^2), tín hiệu có phân bố Gausse sẽ cho entropie vi phân lớn nhất. Tức là:

$$h(X) = - \int_{-\infty}^{\infty} W_1(x) \cdot \log W_1(x) dx \leq \log \sqrt{2\pi e \sigma^2}$$

$$\max h(X) = \log \sqrt{2\pi e \sigma^2} \text{ khi } W_1(x) = \text{mật độ chuẩn}$$

Chứng minh:

Gọi $x(t)$ là tín hiệu không Gausse.

$$\tilde{x}(t) \text{ là tín hiệu Gause: } W_1\left(\frac{\tilde{x}}{\sigma}\right) = \frac{1}{\sqrt{2\pi P_x}} \exp\left(-\frac{\tilde{x}^2}{2P_x}\right)$$

Điều cần chứng minh ở định lý trên tương đương với việc chứng minh bất đẳng thức sau:

$$h(X) - \log \sqrt{2\pi e P_x} \leq 0 \quad (*)$$

Trước hết theo giả thiết, ta có:

$$D_x = D_{\tilde{x}} = D$$

$$\Rightarrow \int_{-\infty}^{\infty} x^2 W_1(x) dx = \int_{-\infty}^{\infty} \tilde{x}^2 W_1(\tilde{x}) d\tilde{x} \quad (a)$$

Ta có:

$$\begin{aligned} h(X) &= - \int_{-\infty}^{\infty} W_1(x) \log W_1(x) dx \\ &= \log \sqrt{2\pi D} \int_{-\infty}^{\infty} W_1(x) dx + \frac{\log e}{2D} \int_{-\infty}^{\infty} x^2 W_1(x) dx \\ &\quad \left(\text{do } \int_{-\infty}^{\infty} W_1(x) dx = \int_{-\infty}^{\infty} W_1(\tilde{x}) d\tilde{x} = 1 \text{ và } \right) \quad \text{do (a)} \end{aligned}$$

$$\Rightarrow h(\tilde{X}) = - \int_{-\infty}^{\infty} \left[-\frac{1}{2} \log 2\pi D - \frac{x^2}{2D} \log e \right] W_1(x) dx \\ = - \int_{-\infty}^{\infty} W_1(x) \log W_1\left(\frac{\tilde{x}}{x}\right) dx$$

Từ (*) \Rightarrow cần chứng minh: $h(X) - h(\tilde{X}) \leq 0$

Ta có:

$$h(X) - h(\tilde{X}) = - \int_{-\infty}^{\infty} W_1(x) \log W_1(x) dx + \int_{-\infty}^{\infty} W_1(x) \log W_1\left(\frac{\tilde{x}}{x}\right) dx \\ = \int_{-\infty}^{\infty} W_1(x) \log \frac{W_1\left(\frac{\tilde{x}}{x}\right)}{W_1(x)} dx \quad (**)$$

Với $a > 1$ bao giờ ta cũng có: $\log_a x \leq x - 1$.

Nên:

$$h(X) - h(\tilde{X}) \leq \int_{-\infty}^{\infty} W_1(x) \left[\frac{W_1\left(\frac{\tilde{x}}{x}\right)}{W_1(x)} - 1 \right] dx \\ \leq \int_{-\infty}^{\infty} W_1\left(\frac{\tilde{x}}{x}\right) dx - \int_{-\infty}^{\infty} W_1(x) dx$$

vậy $h(X) - h(\tilde{X}) \leq 0 \Leftrightarrow h(X) \leq h(\tilde{X}) \forall x \neq \tilde{x}$

$$\max h(X) = h(\tilde{X}) = \log \sqrt{2\pi e D}$$

Ý nghĩa định lý:

Trong số các quá trình ngẫu nhiên có cùng phương sai thì quá trình có phân bố chuẩn thể hiện “tính ngẫu nhiên” nhiều hơn cả. Do đó ta thấy rằng trong số những tập có cùng phương sai thì tập phân bố chuẩn có tác hại lớn nhất đối với việc truyền tin. (vi entropie đặc trưng cho độ bất

định, mà entropie của tập chuẩn max nên độ bất định của nó lớn nhất). Đó là lý do vì sao trong các bài toán của vô tuyến điện thông kê người ta thường xét tập chuẩn.

Bảng phương pháp tương tự, ta có thể chứng minh được:

a. Trong số tất cả các phân bố trong một khoảng hữu hạn (a,b): $\int_a^b W_1(x)dx = 1$. ĐẠI

$$\int_a^b W_1(x)dx = 1 \text{ và } \int_0^\infty x W_1(x)dx = m. \text{ Đại lượng ngẫu nhiên phân bố theo luật mũ có entropie lớn nhất.}$$

lượng ngẫu nhiên phân bố đều có entropie lớn nhất. $H(X) = \log(b-a) = \log \sigma 2\sqrt{3} 1$

b. Trong số tất cả các đại lượng ngẫu nhiên liên tục dương có cùng kỳ vọng m:

$\int_0^\infty W_1(x)dx = 1$ và $\int_0^\infty x W_1(x)dx = m$. Đại lượng ngẫu nhiên phân bố theo luật mũ có entropie lớn nhất.

3.7. KHẢ NĂNG THÔNG QUA CỦA KÊNH GAUSSE

3.7.1. Khả năng thông qua của kênh Gausse với thời gian rời rạc

Dịnh nghĩa:

Kênh Gausse không đổi với thời gian rời rạc là kênh Gausse không đổi có tín hiệu lỗi vào s(t) là hàm liên tục của đối số rời rạc.

Ta có thể coi tín hiệu liên tục với thời gian rời rạc (hình 5.1a) là một dãy xung có biên độ là các giá trị bất kỳ trong khoảng $s_{\min} \div s_{\max}$ và chu kỳ lặp lại (đồng thời cũng là độ rộng xung) là khoảng thời gian rời rạc Δt . Đem các xung (tin) đó truyền vào kênh thì tốc độ truyền tin của kênh (cũng là tốc độ truyền tin của nguồn) với thời gian rời rạc sẽ là:

$$v_K = \frac{1}{\Delta t}$$

Tương tự như đối với kênh rời rạc, khả năng thông qua của kênh Gausse với thời gian rời rạc sẽ là:

$$C' = v_K \cdot \max I(U, S) \quad (3.50)$$

$I(U, S)$ là lượng thông tin chéo trung bình truyền trong kênh liên tục. Đối với kênh Gausse không đổi, ta có:

$$\begin{aligned} I(U, S) &= h(U) - h(N) = h(U) - \log \sqrt{2\pi e P_n} \\ &\Rightarrow \max I(U, S) = \max h(U) - \log \sqrt{2\pi e P_n} \end{aligned}$$

Theo định lý ở phần 3.6, ta thấy $h(U)$ đạt max khi U có phân bố chuẩn:

$$\max h(U) = \log \sqrt{2\pi e P_u}$$

ở một thời điểm nào đó, ta có: $u = \mu s + n$

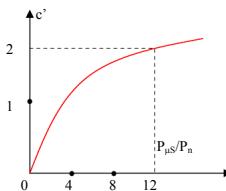
Do s và n độc lập nên: $P_u = P_{\mu s} + P_n$

Vậy:

$$C' = v_K \left[\log \sqrt{2\pi e(P_{\mu s} + P_n)} - \log \sqrt{2\pi e P_n} \right]$$

$$\Rightarrow C' = v_K \log \sqrt{\frac{P_{\mu s} + P_n}{P_n}}$$

$$\Rightarrow C' = \frac{1}{2} v_K \log \left(1 + \frac{P_{\mu s}}{P_n} \right) \quad (3.51)$$



Hình 3.9.

Trong đó $P_{\mu s}/P_n$ là tỷ số tín trên tay ở đầu ra của kênh liên tục (đầu vào bộ giải điều chế).

Ta khảo sát $C' = f(P_{\mu s}/P_n)$:

Khi $\frac{P_{\mu s}}{P_n} \rightarrow 0 \Rightarrow C' \rightarrow 0$. Tức là nếu S/N rất bé thì kênh coi như bị tắt.

Khi $\frac{P_{\mu s}}{P_n} \uparrow$ nhưng còn nhỏ (< 3) thì C' tăng theo rất nhanh.

Khi $\frac{P_{\mu s}}{P_n} \uparrow$ nhưng đã khá lớn (> 12) thì C' tăng theo rất chậm.

Do đó ta thấy không nên chạy theo việc tăng công suất của máy phát để tăng khả năng thông qua của kênh mà nên tăng tốc độ truyền tin của kênh (vì $C' \sim v_K$).

3.7.2. Khả năng thông qua của kênh Gausse với thời gian liên tục trong một giải tần hạn chế

Ta sẽ tính khả năng thông qua của kênh Gausse trong trường hợp tín hiệu vào $s(t)$ là hàm liên tục của thời gian liên tục, có phô hữu hạn F .

Ở đầu vào của bộ giải điều chế, ta có thể đặt thêm một bộ lọc tần thấp có giải thông F . (Giải tần công tác của kênh lúc này cũng chính là giải thông tần của bộ lọc này). Như vậy bộ lọc sẽ không ảnh hưởng đến mèo tín hiệu nhưng sẽ hạn chế được tạp âm trắng. Theo định lý B.A.Kachennhicop ta có thể rời rạc hoá tín hiệu theo trục t mà vẫn không làm mất thông tin nếu như $\Delta t = \frac{1}{2F}$. Như vậy ta đã thay việc truyền tín hiệu liên tục với thời gian liên tục bằng việc truyền tín hiệu liên tục với thời gian rời rạc. Khi đó tốc độ truyền của kênh (số xung truyền trong một đơn vị thời gian) sẽ là: $v_K = \frac{1}{\Delta t} = 2F$. Do đó theo (3.51), ta có:

$$C' = F \log \left(1 + \frac{P_{\mu s}}{N_0} \right) \quad (3.52)$$

Trong đó: F là bệ rộng phổ của tín hiệu

P_n là công suất trung bình của nhiễu trong giải F

Với tệp trắng ta có: $P_n = N_0 \cdot F$

N_0 là mật độ phổ công suất thực tế của nhiễu

$$\Rightarrow C' = F \log \left(1 + \frac{P_{\mu s}}{N_0 \cdot F} \right) \quad (3.52')$$

Nhận xét:

Nếu tăng C' bằng cách tăng F thì kéo theo $P_n \uparrow \Rightarrow \left(\frac{S}{N} \right) \downarrow$. Như vậy giữa C' , F và

(S/N) có sự trái giá, ta được lợi về mặt này thi phải chịu thiệt ở mặt khác.

Ta vẫn có thể thu chính xác được tín hiệu (dảm bảo $C' = \text{const}$) trong trường hợp S/N bé (công suất của máy phát nhỏ, cự ly liên lạc xa, nhiễu mạnh) bằng cách mở rộng phổ của tín hiệu. Ví dụ: trong thông tin vũ trụ, S/N rất nhỏ nên tín hiệu liên lạc phải là tín hiệu giải rộng (tín hiệu điều chế phức tạp, tín hiệu giả tệp,...)

Đó chính là ý nghĩa của (3.52), nó còn được gọi là công thức Shannon.

3.7.3. Khả năng thông qua của kênh Gausse với thời gian liên tục trong giải tần vô hạn

Trong (3.52'), nếu lấy cơ số của log là e thì C' được do bằng [nat/s]. Nếu do bằng [bit/s] thi:

$$C' = 1,443 F \ln \left(1 + \frac{P_{\mu s}}{N_0} \cdot \frac{1}{F} \right) \quad [\text{bit/s}] \quad (3.53)$$

Bây giờ ta sẽ xét sự phụ thuộc của C' vào F.

- Khi $F \rightarrow 0$ thì rõ ràng là $C' \rightarrow 0$

- Khi $F \uparrow$ thì $C' \uparrow$

Đặc biệt, ta sẽ xét giá trị của C' khi $F \rightarrow \infty$, tức là khi giải thông của kênh không hạn chế.

$$\text{Đặt } \frac{P_{\mu s}}{N_0} \cdot \frac{1}{F} = x \Rightarrow F = \frac{P_{\mu s}}{N_0} \cdot \frac{1}{x}$$

Khi $x \rightarrow 0$ thi $F \rightarrow \infty$.

$$\text{Ta ký hiệu: } C'_{\infty} = \lim_{F \rightarrow \infty} C' = \lim_{x \rightarrow 0} \left[\frac{P_{\mu s}}{N_0} \cdot \frac{1}{x} \cdot \ln(1+x) \right] \cdot 1,443$$

$$\Rightarrow C'_{\infty} = 1,443 \cdot \frac{P_{\mu s}}{N_0} \cdot \lim_{x \rightarrow 0} \left[\frac{1}{x} \ln(1+x) \right]$$

$$\text{Ta đã có: } \lim_{x \rightarrow 0} (1+x)^{1/x} = 1$$

$$\Rightarrow C'_{\infty} = 1,443 \cdot \frac{P_{\mu s}}{N_0} \quad (3.54)$$

Đồ thị $C' = f(F)$ được vẽ ở hình 3.10.

$$\text{Tại giá trị } F = \frac{P_{\mu s}}{N_0} \Rightarrow C = F = \frac{P_{\mu s}}{N_0}.$$

Từ đồ thị, ta thấy: Khả năng thông qua của kênh Gausse với thời gian liên tục là một đại lượng giới hạn: $0 \leq C' \leq C'_{\infty}$. Điều này được giải thích như sau: Trong thực tế, mọi vật đều có tần số âm nhiệt. Tần số âm nhiệt có phân bố chuẩn và có mật độ công suất $N_0 = k \cdot T^0$.

Trong đó: k là hằng số Boltzman, $k = 1,38 \cdot 10^{-23} \text{ J/d}\text{o}$.

T^0 là nhiệt độ tuyệt đối của vật.

Vì vậy khả năng thông qua của mọi kênh thực tế đều bị giới hạn.

3.7.4. Định lý mã hóa thứ hai của Shannon đối với kênh liên tục

Đối với kênh liên tục, định lý mã hóa thứ hai của Shannon được phát biểu như sau:

Định lý:

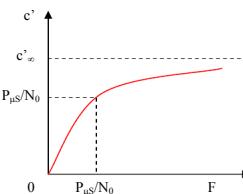
Các nguồn tin rời rạc có thể mã hóa và truyền theo kênh liên tục với xác suất sai bé tuy ý khi giải mã các tín hiệu nhận được nếu khả năng phát của nguồn nhỏ hơn khả năng thông qua của kênh. Nếu khả năng phát của nguồn lớn hơn khả năng thông qua của kênh thì không thể thực hiện được mã hóa và giải mã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

3.7.5. Ví dụ: Khả năng thông qua của một số kênh thực tế

- Kênh viễn thông chuyên tiếp:

$$C' = \left(n \cdot 10^6 \div n \cdot 10^7 \right) \text{ Hartley/s}$$

- Điện thoại, điện báo ảnh, viễn thông chuyên tiếp:



Hình 3.10.

$$C' = \left(n \cdot 10^3 \div n \cdot 10^4 \right) \text{ Hartley/s}$$

- Điện báo:

$$C' = \left(n \cdot 10 \div n \cdot 10^2 \right) \text{ Hartley/s}$$

- Con người: + Thị giác: $C'_1 = n \cdot 10^6 \text{ Hart./s}$

+ Thính giác: $C'_2 = n \cdot 10^3 \text{ Hart./s}$.

Điều này chứng tỏ "trăm nghe không bằng một thấy"

+ Xúc giác C'_3 : $C'_2 < C'_3 < C'_1$

Con người chỉ có thể nhận thức được các thông tin đưa ra với tốc độ truyền $\leq 15 \text{ Hart./s}$.

Một quyển sách 100 trang (≈ 2000 dấu/trang): $I = \left(10^3 \div 10^7 \right)$ bit.

Trí nhớ ngắn hạn của con người: $\left(10^2 \div 10^5 \right)$ bit.

Trung bình một đời người tiếp nhận $\approx 10^{10}$ bit.

BÀI TẬP

3.1. 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%. Giả sử ta gặp một nam thanh niên. Hãy tính lượng thông tin chia trong tin khi biết rằng đó là một sinh viên.

3.2. Có hai hộp đựng bút chì, mỗi hộp đựng 20 bút chì. Hộp thứ nhất có 10 bút trắng, 5 bút đen và 5 bút đỏ. Hộp thứ hai có 8 bút trắng, 8 bút đen và 4 bút đỏ. Ta 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.

3.3. Các tín hiệu x_1, x_2 với các xác suất tiên nghiệm $p(x_1) = 3/4, p(x_2) = 1/4$ được truyền theo kênh nhị phân đối xứng có nhiều như hình vẽ. Do có nhiều nên xác suất thu đúng mỗi tín hiệu giảm đi chỉ bằng $7/8$. Hãy tìm:

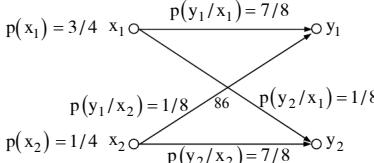
a. Lượng tin tức riêng có điều kiện $I(x_2/y_1)$

b. Lượng tin tức chéo $I(x_2, y_2)$

c.

trung

$H(X)$,



Các lượng tin tức
binh $I(X, y_2),$
 $H(X/Y), I(X, Y)$

86

3.4. Một bảng chữ cái gồm bốn con chữ x_1, x_2, x_3, x_4 . Giá trị xác suất xuất hiện riêng rẽ các chữ $p(x_i)$ và xác suất có điều kiện $p(x_j/x_i)$ cho trong các bảng dưới đây.

x_i	x_1	x_2	x_3	x_4
$p(x_i)$	0,5	0,25	0,125	0,125

$x_i \backslash x_j$	x_1	x_2	x_3	x_4	$\sum_{j=1}^4 p(x_j/x_i)$
x_1	0	0,2	0,4	0,4	1
x_2	0,2	0,2	0,3	0,3	1
x_3	0,25	0	0,25	0,5	1
x_4	0,2	0,4	0,4	0	1

Hãy tìm độ thừa của nguồn tin trong hai trường hợp:

- a. Khi các con chữ độc lập thống kê với nhau.
- b. Khi các con chữ phụ thuộc thống kê với nhau.

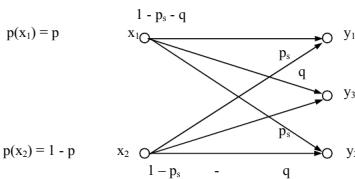
3.5. Một điện dài vô tuyến điện gồm 16 khối có giá trị như nhau về độ tin cậy và được mắc nối tiếp và một thiết bị kiểm tra – thông báo sự hỏng hóc của các khối. Hãy tính số lần thử ít nhất cần hành bằng thiết bị kiểm tra – thông báo đó để có thể phát hiện bất cứ sự hỏng hóc nào của tất cả các khối.

3.6. Một điện dài của dịch có thể làm việc trên sóng λ_1 (sự kiện A_1) hoặc ở trên sóng λ_2 (sự kiện A_2); nó cũng có thể làm việc ở chế độ liên tục (sự kiện B_1) cũng như ở chế độ xung (sự kiện B_2). Xác suất các sự kiện đồng thời có giá trị như sau:

$$p(A_1B_1) = 0,15; p(A_1B_2) = 0,7; p(A_2B_1) = 0,1; p(A_2B_2) = 0,05.$$

Hãy tính lượng tin tức về chế độ công tác của điện dài ấy nếu coi rằng độ dài bước sóng đã biết.

3.7. Xác định khả năng thông qua của kênh nhị phân đối xứng có xoá (như hình vẽ). Nếu các dấu x_i và y_j có thời hạn τ như nhau và $\tau = \frac{1}{F}$. F là tần số phát đi các dấu.



Ghi chú: Giải bằng cách tìm cực trị của hàm $H(B) = f(p)$

3.8. Ở đầu vào một máy thu nhận được tín hiệu hỗn hợp $y(t) = x(t) + n(t)$. Trong đó tín hiệu $x(t)$ và can nhiễu $n(t)$ đều là các quá trình ngẫu nhiên chuẩn, độc lập, có kỳ vọng bằng không và phương sai tần lượn bằng σ_s^2 và σ_n^2 . Hãy tính:

a. Lượng tin tức $I(x,y)$ về tín hiệu $x(t)$ chứa trong tín hiệu thu được $y(t)$.

b. Lượng tin tức chéo trung bình.

3.9. A chọn một trong các số từ $0 \div 7$. Hỏi B phải dùng trung bình bao nhiêu câu hỏi để tìm ra số A nghĩ?

3.10. Tính độ rộng giải thông của một kênh vô tuyến truyền hình truyền hình ảnh đèn trắng với 5.10^5 yếu tố, 25 ảnh trong 1s và có 8 mức sáng đồng xác suất, với tỷ số $\frac{P_s}{P_n} = \frac{\sigma_s^2}{N_0 \cdot F} = 15$.

Nếu coi rằng ảnh vô tuyến hình xem như một dạng tập âm trắng.

3.11. Tim mật độ phô tín hiệu $S(f)$ để bảo đảm tốc độ truyền tin cực đại khi cho trước công suất toàn phần của tín hiệu: $P_s = \int_{f_1}^{f_2} S(f) df$ và mật độ phô của nhiễu $N(f)$.

3.12. Hãy so sánh khả năng thông qua của hai kênh thông tin nếu kênh thứ nhất chịu một tác động của một tập âm trắng, chuẩn trong giải tần F với phương sai $\sigma^2 = 1V^2$, còn kênh thứ hai chịu tác động của một tập âm trắng, phân bố đều trong khoảng $\pm 1,5$ với giải tần $2F$. Coi rằng công suất của tín hiệu rất lớn hơn công suất của tập âm.

3.13. Trong 27 đồng xu giống nhau có 1 đồng xu giả nhẹ hơn. Giả sử ta dùng một cân đĩa thăng bằng (có hai đĩa cân) để xác định đồng xu giả. Hãy tính số lần cân trung bình tối thiểu để xác định được đồng xu giả. Nếu thuật toán cân.

3.14. Trong bộ tú lơ khơ 52 quân bài (không kể phăng teo), A rút ra một 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. Nếu thuật toán hỏi? Giả sử A đã rút ra 5 rõ, hãy nêu các câu hỏi cần thiết.

CHƯƠNG IV – CƠ SỞ LÝ THUYẾT MÃ HÓA

4.1. CÁC ĐỊNH NGHĨA VÀ KHÁI NIỆM CƠ BẢN

4.1.1. Các định nghĩa cơ bản

4.1.1.1. Mã hóa

Tập các tin rời rạc rất đa dạng và phong phú. Để hệ thống truyền tin số có thể truyền được các tin này cần phải có một quá trình biến đổi thích hợp đối với các tin rời rạc, đó chính là quá trình mã hóa.

Định nghĩa 1: Mã hóa là một ánh xạ $l - 1$ từ tập các tin rời rạc a_i lên tập các từ mã $\alpha_i^{n_i}$

$$f : a_i \rightarrow \alpha_i^{n_i}$$

Để có thể dễ dàng mã hóa và giải mã, từ các từ mã $\alpha_i^{n_i}$ thường là các phần tử của một cấu trúc đại số nào đó. Bởi vậy ta có thể định nghĩa cụ thể hơn cho phép mã hóa.

Định nghĩa 2: Mã hóa là một ánh xạ $l - 1$ từ tập các tin rời rạc a_i lên một tập con có cấu trúc của một cấu trúc đại số nào đó.

4.1.1.2. Mã

Định nghĩa 3: Mã (hay bộ mã) là sản phẩm của phép mã hóa, hay nói cách khác mã là một tập các từ mã được lập nên theo một luật đã định.

4.1.1.3. Các yếu tố của từ mã

Định nghĩa 4: Độ dài từ mã n_i là số các dấu mã cần thiết dùng để mã hóa cho tin a_i .

Nếu $n_i = \text{const}$ với mọi i thì mọi từ mã đều có cùng độ dài. Bộ mã tương ứng được gọi là bộ mã đều.

Nếu $n_i \neq n_j$ thì bộ mã tương ứng được gọi là bộ mã không đều

Định nghĩa 5: Số các dấu mã khác nhau (về giá trị) được sử dụng trong bộ mã được gọi là cơ số mã. Ta ký hiệu giá trị này là m .

Nếu $m = 2$ thì bộ mã tương ứng được gọi là mã nhị phân.

Nếu $m = 3$ thì bộ mã tương ứng được gọi là mã tam phân

.....

Nếu $m = p$ thì bộ mã tương ứng được gọi là mã p phân.

Thông thường các dấu mã được chọn là các phần tử trong một trường F nào đó.

Ví dụ 1: Từ mã α_i^7 trong bộ mã đều nhị phân có độ dài 7 có thể mô tả như sau:

$$\alpha_i^7 = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1$$

Mỗi một dấu mã trong từ mã này chỉ có thể nhận một trong hai giá trị $\{0, 1\}$, mỗi dấu mã là một phần tử của trường nhị phân $GF(2)$.

4.1.2. Các khái niệm cơ bản

4.1.2.1. Độ thừa của một bộ mã đều (D)

Cho nguồn rời rạc A gồm s tin: $A = \{a_i; \overline{I, S}\}$.

Xét phép mã hóa f sau: $f: a_i \rightarrow \alpha_i^n ; \alpha_i^n \in V$.

Cơ số mã là m, khi đó số các từ mã độ dài n có thể có là: $N = m^n$.

Định nghĩa 6: Độ thừa của một bộ mã đều được xác định theo biểu thức sau:

$$D \stackrel{\Delta}{=} \frac{H_0(V) - H_0(A)}{H_0(V)} = 1 - \frac{H_0(A)}{H_0(V)} [\%] \quad (4.1)$$

Trong đó: $H_0(A) = \log N$

$$H_0(V) = \log N = n \log m$$

Ví dụ 2: Ta có mã hóa 4 tin A, B, C, D bằng các tin từ mã của một bộ lọc giải mã đều nhị phân, có độ dài $n = 3$, khi đó độ thừa của bộ mã này là:

$$D = 1 - \frac{\log 4}{3 \log 2} = 33,33\%$$

Bộ mã này có 4 từ mã được dùng để mã hóa cho 4 tin rời rạc. Các từ mã còn lại (4 từ mã) không được dùng để mã hóa được gọi là các từ mã cảm.

Đối với các bộ từ mã đều, để đánh giá định lượng sự khác nhau giữa các từ mã trong bộ mã, ta sử dụng khái niệm khoảng cách mã sau.

4.1.2.2. Khoảng cách mã (d)

Định nghĩa 7: 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 $d(\alpha_i^n, \alpha_j^n)$

Ví dụ 3: $\alpha_i^7 = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1$

$\alpha_j^7 = 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0$

$$d(\alpha_i^7, \alpha_j^7) = 6$$

Khoảng cách mã d có đầy đủ các tính chất của khoảng cách trong một không gian metric.

$$\text{Tính chất 1: } d(\alpha_i^n, \alpha_j^n) = d(\alpha_j^n, \alpha_i^n)$$

$$\text{Tính chất 2: } 1 \geq d(\alpha_i^n, \alpha_j^n) \geq 0$$

$$\text{Tính chất 3: (Tính chất tam giác): } d(\alpha_i^n, \alpha_j^n) + d(\alpha_j^n, \alpha_k^n) \geq d(\alpha_i^n, \alpha_k^n)$$

Để đánh giá định lượng khả năng không ché sai (bao gồm khả năng phát hiện sai và khả năng sửa sai) của một bộ mã ta sử dụng khái niệm khoảng cách mã tối thiểu (hay khoảng cách Hamming) sau:

Định nghĩa 8: Khoảng cách Hamming d_0 của một bộ mã được xác định theo biểu thức sau:

$$d_0 = \min_{\forall \alpha_i^n, \alpha_j^n} d(\alpha_i^n, \alpha_j^n)$$

Ở đây α_i^n và α_j^n không đồng nhất bằng không (Ta coi α_i^n là từ mã không khi mọi dấu mã trong từ mã đều nhận giá trị không).

4.1.2.3. Trọng số của một từ mã

Định nghĩa 9: Trọng số của một từ mã $W(\alpha_i^n)$ là số các dấu mã khác không trong từ mã.

$$\text{Ví dụ: } \alpha_i^7 = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1$$

$$W(\alpha_i^7) = 4$$

Nếu ta coi mỗi từ mã α_i^n là một véc-tơ n chiều trong một không gian tuyến tính n chiều V_n , khi đó phép cộng được thực hiện giữa hai từ mã tương tự như phép cộng giữa hai véc-tơ tương ứng.

$$\text{Ví dụ 4: } \alpha_i^7 = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \Leftrightarrow (0, 1, 1, 0, 1, 0, 1)$$

$$\alpha_j^7 = 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \Leftrightarrow (1, 0, 0, 1, 1, 1, 0)$$

$$\alpha_k^7 = \alpha_i^7 + \alpha_j^7 = 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \Leftrightarrow (1, 1, 1, 1, 0, 1, 1)$$

Ở đây phép cộng trên mỗi thành phần (tọa độ) của véc-tơ được thực hiện trên trường nhị phân GF(2). Phép cộng theo modulo 2 này được mô tả như sau:

+	0	1
0	0	1
1	1	0

Sau đây là các tính chất của trọng số:

$$- 0 \leq W(\alpha_i^n) \leq 1$$

$$- d(\alpha_i^n, \alpha_j^n) = W(\alpha_i^n + \alpha_j^n)$$

4.1.3. Khả năng không chê sai của một bộ mã đều nhị phân

4.1.3.1. Khả năng phát hiện sai

Định lý 1: Một bộ mã đều nhị phân có độ thừa ($D > 0$) và có $d_0 \geq 2$ sẽ có khả năng phát hiện được t sai thỏa mãn điều kiện:

$$t \leq d_0 - 1 \quad (4.2)$$

Chứng minh:

Mọi từ mã trong bộ mã đều cách nhau một khoảng cách ít nhất là d_0 . Khi truyền tin, do có nhiều từ mã nhận được có thể bị sai ở t vị trí $t \leq d_0 - 1$. Vì vậy từ mã nhận được không thể biến thành một từ mã được dùng khác. Như vậy ta luôn có thể phát hiện được rằng từ mã đã nhận sai.

4.1.3.2. Khả năng sửa sai

Định lý 2: Một bộ mã đều nhị phân có độ thừa ($D \geq 0$) và có ($d_0 \geq 3$) sẽ có khả năng sửa được e sai thỏa mãn điều kiện:

$$e \leq \left\lfloor \frac{d_0 - 1}{2} \right\rfloor \quad (4.3)$$

Ở đây $[x]$ là ký hiệu phần nguyên của số x .

Chứng minh:

Khi truyền tin, do có nhiều, từ mã nhận được có thể bị sai ở e vị trí $\left(e \leq \left\lfloor \frac{d_0 - 1}{2} \right\rfloor \right)$. Như vậy, Khoảng cách giữa từ mã nhận được với từ mã khác tối thiểu là $e + 1$. Như vậy, ta luôn có thể xác định đúng được từ mã đã phát. Điều đó có nghĩa là ta đã sửa sai được e sai gấp phái trên được truyền.

4.1.4. Mã đều nhị phân không có độ thừa

Mã đều nhị phân không có độ thừa ($D = 0$) còn được gọi là mã đơn giản. Với mã đơn giản ta có $s = N = 2^n$. Như vậy mỗi một từ mã có thể có đều được sử dụng để mã hóa cho các tin rời rạc. Với từ mã đơn giản $d_0 = 1$. Vì vậy ta không thể phát hiện hay sửa được bất cứ một sai sót nào.

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 chỉ nhận đúng khi mọi dấu mã đều nhận đúng. Như vậy, xác suất thu đúng từ mã p_d là:

$$p_d = (1 - p_0)^n \quad (4.4)$$

Xác suất thu sai của từ mã là:

$$p_s = 1 - p_d = 1 - (1 - p_0)^n \quad (4.5.a)$$

Với $p_0 \ll 1$ ta có công thức gần đúng sau:

$$(1 - p_0)^n \approx 1 - n p_0$$

$$\text{Ta có: } p_s \approx n p_0 \quad (4.5.b)$$

Giả sử xác suất thu sai cho phép đổi với mỗi tin rời rạc là p_{sep} khi đó điều kiện sử dụng mã đơn giản trong kênh đối xứng nhị phân không nhớ là:

$$p_s \leq p_{sep}$$

$$\text{Hay } p_0 \ll \frac{p_{sep}}{n} \quad (4.6)$$

4.2. MÃ THÔNG KÊ TỐI UU

Ta xét phép mã hóa sau đối với các tin của nguồn rời rạc A:

$$f : a_i \rightarrow \alpha_i^{n_i}$$

Mỗi tin a_i được mã hóa bằng một tổ hợp mã (từ mã) $\alpha_i^{n_i}$ ($\alpha_i^{n_i}$ là một tổ hợp mã gồm n_i dấu mã).

Ta xét trường hợp mã nhị phân tức là mỗi dấu mã chỉ nhận một trong hai giá trị "0" và "1".

4.2.1. Độ dài trung bình của từ mã và mã hóa tối ưu

$$\text{Ta có } A = \left(\begin{array}{c} a_i \\ p(a_i) \end{array} \right) \xrightarrow[i=1,s]{} V = \left(\begin{array}{c} \alpha_i^{n_i} \\ p(a_i) \end{array} \right) i = \overline{1, s}$$

Định nghĩa 1: Độ dài trung bình của một tổ hợp mã được xác định theo biểu thức sau:

$$\bar{n} = M[n_i] = \sum_{i=1}^s n_i p(a_i)$$

Định nghĩa 2: Một phép mã hóa được gọi là tiết kiệm (hay tối ưu) nếu nó làm cực tiểu giá trị \bar{n} .

4.2.2. Yêu cầu của một phép mã hóa tối ưu

- $\bar{n} \rightarrow \min$.

- Có khả năng giải mã tức thì: không một dãy bít nào trong biểu diễn của một tin (ký tự) nào đó lại là phần đầu (prefix) của một dãy bít dài hơn biểu diễn cho một tin (ký tự) khác.

Ví dụ 1: Mã Morse không đảm bảo yêu cầu này vì:

Mã số cho E (.) là tiền tố của mã số cho A (._)

Mã số cho D (._) là tiền tố của mã số cho B (....)

4.2.3. Định lý mã hóa thứ nhất của Shannon (đối với mã nhị phân)

4.2.3.1. Định lý

Luôn luôn có thể xây dựng được một phép mã hóa các tin rời rạc có hiệu quả mà \bar{n} có thể nhỏ tùy ý nhưng không nhỏ hơn entropic $H(A)$ được xác định bởi đặc tính thống kê của nguồn A.

$$\bar{n} \geq H(A)$$

Chứng minh:

Nếu gọi m là cơ số của bộ mã thì lượng thông tin riêng cực đại chứa trong mỗi dấu mã là $\log m$.

Gọi n_i là độ dài của từ mã $\alpha_i^{n_i}$ ứng với tin a_i , khi đó lượng thông tin riêng cực đại chứa trong từ mã này là $n_i \log m$.

Lượng thông tin riêng trung bình của mỗi từ mã là:

$$\sum_{i=1}^s p(a_i) n_i \log m = \bar{n} \log m$$

Để phép mã hóa không làm tổn hao thông tin thì lượng thông tin riêng trung bình cực đại chứa trong mỗi từ mã phải không nhỏ hơn lượng thông tin riêng trung bình chứa trong mỗi tin thuộc nguồn. Tức là:

$$\bar{n} \log m \geq H(A)$$

$$\text{hay } \bar{n} \geq \frac{H(A)}{\log m}.$$

Với mã nhị phân ($m = 2$) ta có: $\bar{n} \geq H(A)$

4.2.3.2. Nguyên tắc lập mã tiết kiệm

$$\text{Theo định lý ta có: } \sum_{i=1}^s p(a_i) n_i \geq -\sum_{i=1}^s p(a_i) \log p(a_i)$$

Bất đẳng thức trên sẽ thỏa mãn nếu $\forall i$ ta có:

$$p(a_i) n_i \geq -p(a_i) \log p(a_i)$$

$$\text{hay } n_i \geq -\log p(a_i)$$

Nguyên tắc: Các từ mã có độ dài càng nhòe sẽ được dùng để mã hóa cho các tin có xác suất xuất hiện càng lớn và ngược lại.

4.2.4. Thuật toán Huffman

4.2.4.1. Thuật toán mã hóa

Với phép mã hóa tối ưu ta có: $\bar{n} = H(A)$

$$\text{VÀO: Nguồn rời rạc } A = \left(\begin{array}{c} a_i \\ p(a_i) \end{array} \right), i = 1, s$$

RA: Từ mã α_i^n tương ứng với tin a_i

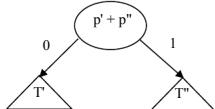
Bước 1: Khởi động một danh sách các cây nhị phân một nút chứa các trọng lượng p_1, p_2, \dots, p_n cho các tin a_1, a_2, \dots, a_n .

Bước 2: Thực hiện các bước sau $n - 1$ lần:

Tìm hai cây T' và T'' trong danh sách với các nút gốc có trọng lượng tối thiểu p' và p'' .

Thay thế hai cây này bằng cây nhị phân với nút gốc có trọng lượng $p' + p''$ và có các cây con là T' và T'' .

Đánh dấu cá mũi tên chỉ đến các cây con 0 và 1.

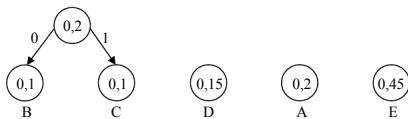


Bước 3: Mã số của tin a_i là dãy các bit được đánh dấu trên đường từ gốc của cây nhị phân cuối cùng tới nút a_i .

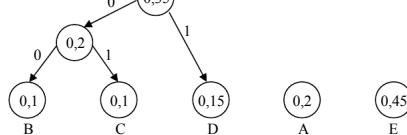
Ví dụ 1: Xét các ký tự A, B, C, D, E có các xác suất xuất hiện tương ứng là 0,2; 0,1; 0,1; 0,15; 0,45



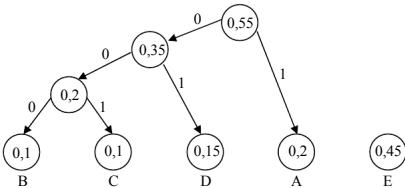
Bước 2: Lần 1:



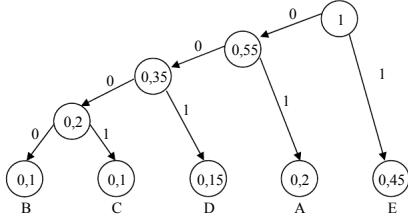
Lần 2:



Lần 3:



Lần 4:



Bước 3:

Ký tự	A	B	C	D	E
Mã tương ứng	01	0000	0001	001	1
n_i	2	4	4	3	1

Đánh giá hiệu quả:

$$\bar{n} = \sum_{i=1}^s n_i p(a_i) = 2.0.2 + 4.0.1 + 4.0.1 + 3.0.15 + 1.0.45 \\ = 2,1 \text{ dấu}$$

$$H(A) = \sum_{i=1}^s p(a_i) \log \frac{1}{p(a_i)} = 2.0.1 \log 10 + 0.15 \log \frac{100}{15} + 0.2 \log 5 + 0.45 \log \frac{100}{45} \\ = 0.2.3.3226 + 0.15.2.7375 + 0.2.2.3224 + 0.45.1.1522 \\ = 0.6645 + 0.4106 + 0.4645 + 0.5185 \\ = 2,058 \text{ bit}$$

Ta thấy $\bar{n} \geq H(A)$ **Nhận xét:** Phép mã hóa trên là gần tối ưu.

4.2.4.2. Thuật toán giải mã

VÀO: Xâubit

RA: Xâu tin (ký tự)

Bước 1: Khởi động con trỏ P chỉ đến gốc của cây Huffman.Bước 2: While (chưa đạt tới kết thúc thông báo) do:

- a. Đặt x là bit tiếp theo trong xâu bit.

b. If $x = 0$ then

Đặt $P :=$ con trỏ chỉ đến cây con trái của nó

else

$P :=$ con trỏ chỉ đến cây con phải của nó

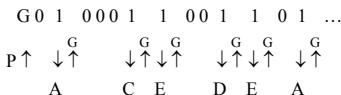
c. If (P chỉ đến nút lá) then

1. Hiển thị ký tự tương ứng với nút lá.

2. Đặt lại P để nó lại chỉ đến gốc của cây Huffman

Ví dụ 2: Thông báo nhận được: 0 1 0 0 0 1 1 0 0 1 1 0 1 ...

Quá trình giải mã:



RA: A C E D E A ...

4.3. CÁC CÁU TRÚC ĐẠI SỐ VÀ MÃ TUYÊN TÍNH

4.3.1. Một số cấu trúc đại số cơ bản

4.3.1.1. Nhóm: $\langle G, * \rangle$

Nhóm G là một tập hợp các phần tử với một phép toán trong 2 ngôi thỏa mãn các tính chất sau:

- $a, b \in G \Rightarrow a * b = c \in G$

- Tồn tại phần tử đơn vị e : $a * e = e * a = a$

- Tồn tại phần tử ngược a^{-1} : $a * a^{-1} = a^{-1} * a = e$

Nếu $a * b = b * a$ thì nhóm được gọi là nhóm giao hoán.

Ví dụ 1: Tập các số nguyên Z với phép toán cộng (+) tạo nên một nhóm giao hoán với phần tử đơn vị là 0.

Nếu số các phần tử trong nhóm $|G|$ là hữu hạn thì ta có nhóm hữu hạn $|G|$.

Nếu $H \in G$ và $\langle H, * \rangle$ tạo nên một nhóm thì H được gọi là nhóm con của G . Cấp của H là ước của cấp của G .

4.3.1.2. Nhóm cyclic

Xét nhóm hữu hạn $\langle G, * \rangle$. Nếu G có thể mô tả như sau"

$$G = \left\{ \alpha^i, \forall i \right\}$$

thì G được gọi là nhóm cyclic sinh bởi α . α được gọi là phần tử sinh (hay phần tử nguyên thủy) của nhóm.

Ví dụ 2: Xét nhóm nhân: $Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$$\text{Ta có: } 2^0 = 1 \quad 2^5 = 10$$

$$2^1 = 2 \quad 2^6 = 9$$

$$2^2 = 4 \quad 2^7 = 7$$

$$2^3 = 8 \quad 2^8 = 3$$

$$2^4 = 5 \quad 2^9 = 6$$

$$\text{Ta có thể viết } Z_{11}^* = \left\{ 2^i \bmod 11 \right\}.$$

Phần tử α được gọi là có cấp k nếu n là số nguyên dương nhỏ nhất thỏa mãn $\alpha^k \equiv 1 \pmod{n}$.

Ở ví dụ trên ta có $\text{ord}(2) = \text{ord}(8) = \text{ord}(7) = \text{ord}(9) = 10$

4.3.1.3. Vành: $\langle R, +, \cdot \rangle$

Vành R là một tập hợp các phần tử với hai phép toán trong hai ngôi (Phép cộng (+), phép nhân (\cdot)) thỏa mãn các tính chất sau:

- $\langle R, + \rangle$ là một nhóm đối với phép cộng

- $\langle R, \cdot \rangle$ là một nửa nhóm đối với phép nhân. Điều này có nghĩa là không nhất thiết mọi phần tử đều có phần tử ngược của phép nhân.

- Tính chất phân phối: $(a + b)c = ac + bc$

Vành R được gọi là vành giao hoán nếu ta có $a b = b a$

4.3.1.4. Ideal:

Ideal I là một tập con trong R có các tính chất sau:

- $a, b \in I : a + b \in I, \langle I, + \rangle$ là một nhóm đối với phép $*$.

- $c \in R : c.a \in I$

4.3.1.5. Trường $\langle F, +, \cdot \rangle$

Trường F là một tập hợp các phần tử với hai phép toán trong hai ngôi thỏa mãn:

- $\langle F, + \rangle$ là một nhóm cộng
- $\langle F^*, \cdot \rangle$ là một nhóm đối với phép nhân.

Trong đó: $F^* = F \setminus \{0\}$

Ví dụ 3: Trường nhị phân GF(2): Trường này chỉ có hai phần tử 0 và 1.

4.3.1.6. Không gian tuyến tính V_n

Các phần tử trong không gian tuyến tính được gọi là các vectơ.

$v \in V_n$ là các vectơ n chiều. Mỗi vectơ n chiều được mô tả bằng một bộ n tọa độ được sắp xếp $v \leftrightarrow (v_0, v_1, \dots, v_{n-1})$ với $v_i \in F$

Trong không gian V_n ta xác định các phép toán sau:

- Cộng vectơ: $u = (u_0, \dots, u_{n-1})$, $v = (v_0, \dots, v_{n-1})$
 $u + v = (y_0, \dots, y_{n-1})$ với $y_j = u_j + v_j \in F$
- Tích vô hướng của hai vectơ: (u, v)

$$(u, v) = \sum_{i=0}^{n-1} u_i v_i \in F$$

Hai vectơ được gọi là trực giao nếu $(u, v) = 0$

- Nhân một vectơ với một phần tử vô hướng

Xét phần tử vô hướng $\alpha \in F$

$$\alpha \cdot u = (\alpha u_1, \dots, \alpha u_{n-1})$$

4.3.2. Các dạng tuyến tính và mã tuyến tính

4.3.2.1. Dạng tuyến tính

Định nghĩa 1: Các dạng tuyến tính của k biến độc lập x_1, x_2, \dots, x_k là các biểu thức có dạng:

$$f(x_1, \dots, x_k) = \sum_{i=1}^k a_i x_i \quad (4.7)$$

Trong đó: $a_i \in F$

Nhận xét: Có sự tương ứng 1 – 1 giữa các dạng tuyến tính, các véctơ và các đa thức trong vầnh đa thức.

4.3.2.2. Mã tuyến tính

Định nghĩa 2: Mã tuyến tính độ dài n là mã mà tử mã của nó có các dấu mã là các dạng tuyến tính

Định nghĩa 3: Mã hệ thống tuyến tính (n,k) là mã tuyến tính độ dài n trong đó ta có thể chỉ ra được vị trí của k dấu thông tin trong tử mã.

Định nghĩa 4: Mã tuyến tính ngẫu nhiên là mã tuyến tính có các dấu mã được chọn ngẫu nhiên từ các dạng tuyến tính có thể có.

Nhận xét:

- Shannon đã chứng minh rằng tồn tại các mã đạt được giới hạn Shannon (thỏa mãn định lý mã hóa thứ hai) trong các mã tuyến tính ngẫu nhiên.

- Khó tìm các mã tốt trên các mã tuyến tính ngẫu nhiên. Hơn nữa việc mã hóa và giải mã cho các mã này cũng rất phức tạp. Bởi vậy các mã này chỉ có ý nghĩa về mặt lý thuyết.

Ví dụ 4: Số các dạng tuyến tính khác nhau của 4 biến độc lập là:

$$N_0 = 2^4 - 1 = 15$$

Số các mã hệ thống tuyến tính (7,4) là $N_1 = C_{11}^3 = 165$

4.3.2.3. Ma trận sinh và ma trận kiểm tra của mã tuyến tính

Để đơn giản cho việc mô tả mã tuyến tính người ta thường sử dụng ma trận sinh $G_{k,n}$. Ma trận này chứa k véctơ hàng độc lập tuyến tính tạo nên không gian mã $V_{-(n,k)}$

2^k các véctơ khác nhau là tất cả các tổ hợp tuyến tính có thể có của k véctơ hàng này.

Trong đại số tuyến tính ta biết rằng với mỗi G sẽ tồn tại ma trận $H_{r \times n}$ thỏa mãn:

$$G \cdot H^T = 0 \quad (4.8)$$

Trong đó: $r = n - k$

H^T được gọi là ma trận chuyển vị của H

H được gọi là ma trận kiểm tra của mã tuyến tính (n, k)

Ta thấy rằng H chứa r véctơ hàng trực giao với các véctơ hàng của G

Hiện nhiên là nếu a là một véctơ mã $\left(a \in V_{-(n,r)} \right)$ thì :

$$a \cdot H^T = 0 \quad (4.9)$$

Ở đây H cũng là một ma trận sinh của một mã tuyến tính $V_{(n,r)}$ và G lại chính là ma trận kiểm tra của mã này. Ta thấy rằng không gian tuyến tính C sinh bởi G là không gian không của không gian tuyến tính C^\perp sinh bởi H .

Từ (4.9) ta có thể viết ra 1 phương trình:

$$\sum_{j=1}^n a_j h_{ij} = 0 \quad , \quad i = 1, r \quad (4.10)$$

Các phương trình này còn được gọi là các tông kiểm tra. Mã C sinh bởi mã G và C^\perp sinh bởi H được gọi là các mã đối ngẫu.

Nếu $C \equiv C^\perp$ thì C được gọi là mã tự đối ngẫu. Các mã tự đối ngẫu có $r = n - k$ và bởi vậy có tốc độ $R = \frac{k}{n} = \frac{1}{2}$.

Ví dụ 5: Xét mã hệ thống tuyến tính $(7, 4)$ có các dấu mã được chọn từ các dạng tuyến tính như sau:

Từ mã a gồm các dấu mã a_i được chọn như sau:

$$\begin{aligned} a_0 &= x_0 \\ a_1 &= x_1 \\ a_2 &= x_2 \\ a_3 &= x_3 \\ a_4 &= x_0 + x_1 + x_2 \\ a_5 &= x_1 + x_2 + x_3 \\ a_6 &= x_0 + x_1 + x_3 \end{aligned}$$

Như vậy ma trận sinh G có dạng:

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

Ma trận kiểm tra của mã $(7, 4)$ này là:

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

H chính là ma trận sinh của mã $(7, 3)$ là mã đối ngẫu với mã $(7, 4)$ sinh bởi G

4.3.3. 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:

4.3.3.1. Bài toán 1

Với k và d_0 xác định, ta phải tìm được mã có độ dài với từ mã là nhỏ nhất.

Tương ứng với bài toán này ta có giới hạn Griesmer sau:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d_0}{2^i} \right\rceil \quad (4.11)$$

Ở đây $\lceil x \rceil$ chỉ số nguyên nhỏ nhất lớn hơn hoặc bằng x .

Ví dụ 6: Cho $k = 4$, $d_0 = 3$

$$n \geq 3 + 2 + 1 + 1 = 7$$

Vậy mã phải có độ dài tối thiểu là 7. Hay nói một cách khác mã $(7, 4, 3)$ là một mã tối ưu đạt được giới hạn Griesmer.

4.3.3.2. Bài toán 2

Với n và k xác định, ta phải tìm được mã có khoảng cách tiêu d_0 là lớn nhất.

Tương ứng với bài toán này ta có giới hạn Plotkin sau:

$$d_0 \leq \frac{n \cdot 2^{k-1}}{2^k - 1} \quad (4.12)$$

Ví dụ 7: Cho $k = 3$, $n = 7$

$$d_0 \leq \frac{7 \cdot 2^2}{2^3 - 1} = 4$$

Vậy khoảng cách d_0 lớn nhất là 4. Nói một cách khác mã $(7, 3, 4)$ là một mã tối ưu đạt được giới hạn Plotkin.

4.3.3.3. Bài toán 3

Với n và số sai khả sưa t xác định, ta phải tìm được 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:

$$2^{n-k} \geq \sum_{i=0}^t C_n^i \quad (4.13)$$

Ví dụ 8: 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.

4.4. VÀNH ĐA THÚC VÀ MÃ XYCLIC

4.4.1. Vành đa thức

Ta xét tập hợp các đa thức có bậc không lớn hơn $n - 1$ sau:

$$f(x) = \sum_{i=0}^{n-1} f_i x^i \quad (4.14)$$

$$\deg f(x) \leq n - 1$$

f_i là các hệ số được lấy giá trị trong một trường F nào đó.

Trên tập các đa thức này ta xác định 2 phép toán trong là phép cộng đa thức và phép nhân đa thức như sau:

4.4.1.1. Phép cộng đa thức

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

Ta có: $a(X) + b(X) = c(X)$

$$c(X) = \sum_{i=0}^{n-1} c_i x^i$$

$$c_i = a_i + b_i$$

Ở đây phép cộng các hệ số a_i và b_i được thực hiện trên trường F

Nếu ta coi mỗi đa thức có bậc nhỏ hơn hoặc bằng $n - 1$ là một vectơ trong không gian tuyến tính n chiều V_n thì phép cộng đa thức hoàn toàn tương tự như phép cộng vectơ.

Ví dụ 1: Xét $n = 7$, $F = GF(2)$

$$\begin{aligned} a(X) &= 1 + x + x^4 \Leftrightarrow a = (1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0) \\ b(X) &= x + x^2 \Leftrightarrow b = (0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0) \\ a(X) + b(X) &= 1 + x^2 + x^4 \Leftrightarrow a + b = (1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0) \end{aligned}$$

4.4.1.2. Phép nhân đa thức

Độ tích của hai đa thức có bậc $\leq n - 1$ vẫn là một đa thức có bậc $\leq n - 1$ ta phải thực hiện phép nhân 2 đa thức theo modulo $X^n + 1$ (tức là coi $X^n = 1$).

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

Ví dụ 2: $a(X) = 1 + X + X^4$, $b(X) = X + X^2$

$$\begin{aligned} a(X).b(X) &= (1 + X + X^4)(X + X^3) \bmod X^7 + 1 \\ a(X).b(X) &= (1 + X^2 + X^5 + X^3 + X^4 + X^7) \bmod X^7 + 1 \\ a(X).b(X) &= 1 + X + X^2 + X^3 + X^4 + X^5 \end{aligned}$$

Ta thấy rằng tích của hai đa thức được thực hiện trên cơ sở tích của hai đơn thức x^i và x^j .

$$x^i \cdot x^j = x^{(i+j) \bmod n} \quad (4.15)$$

Chú ý: Phép nhân các hệ số a_i và b_j là phép nhân trên trường F

4.4.1.3. Phép dịch vòng

Ta xét một trường hợp đặc biệt của phép nhân là nhân một đa thức $a(X)$ và một đơn thức x^i .

$$a(X) = \sum_{i=0}^{n-1} a_i x^i \Leftrightarrow a = (a_0, a_1, a_2, \dots, a_{n-1})$$

Xét tích sau:

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

Ta thấy biểu diễn vectơ b được dịch vòng về phía phải một cấp so với biểu diễn vectơ a .

Tương tự ta có:

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

Xét thương sau:

$$d(x) = \frac{a(X)}{x} = \frac{\sum a_i x^i}{x} \Leftrightarrow d = (a_1, a_2, \dots, a_{n-1}, a_0)$$

Ta thấy biểu diễn của véc tơ d được dịch vòng về phía trái 1 cấp so với biểu diễn của vectơ a .

Nhận xét:

$$\frac{a(X)}{x} = \frac{x^n a(X)}{x} = x^{n-1} a(X)$$

Ví dụ 3:

$$a(X) = 1 + x + x^4 \Leftrightarrow a = (1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0)$$

$$b(X) = x \cdot a(X) = x(1 + x + x^4) = x + x^2 + x^5 \Leftrightarrow b = (0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0)$$

$$d(X) = \frac{a(X)}{x} = \frac{(1 + x + x^4)}{x} = 1 + x^3 + x^6 \Leftrightarrow d = (1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1)$$

4.4.1.4. Định nghĩa vành da thực

Định nghĩa 1: Tập các da thực xác định theo (3.11) với hai phép toán cộng da thực và nhân da thực theo modulo $X^n + 1$ tạo nên vành da thực. Trong trường hợp các hệ số của các da thực nằm trong $\text{GF}(2)$ ta ký hiệu vành này là $Z_2[x]/X^n + 1$.

4.4.2. Ideal của vành da thực

Định nghĩa 2: Ideal I của vành da thực gồm tập các da thực $a(X)$ là bội của một da thực $g(X)$ thỏa mãn:

$$- g(X) | X^n + 1 \quad (g(X) \text{ là ước của } X^n + 1)$$

- $\deg g(X) = r = \min \deg a(X)$ với $\forall a(X) \in I, a(X) \neq 0$

Ta ký hiệu Ideal trong vành đa thức là $I = \langle g(X) \rangle$

Hiển nhiên là với $g(X) = \sum_{i=0}^r g_i x^i$ ta có

$$g_0 = g_r = 1, g_i \in \{0, 1\} \text{ với } i = \overline{1, r-1}$$

Để có thể tìm được tất cả các Ideal trong vành ta phải thực hiện phân tích nhị thức $X^n + 1$ thành tích của các đa thức bắt khả quy.

Định nghĩa 3: Đa thức $a(X)$ được gọi là bắt khả quy nếu nó chỉ chia hết cho 1 và cho chính nó.

Như vậy đa thức bắt khả quy là đa thức không thể phân tích thành tích các đa thức có bậc nhỏ hơn.

Định lý 4: Với $n = 2^m - 1$, đa thức $X^n + 1$ được phân tích thành tích của tất cả các đa thức bắt khả quy có bậc m và ước của m.

Ví dụ 4:

- $m = 2, n = 3$: chỉ có duy nhất một đa thức bắt khả quy bậc 2 là $x^2 + x + 1$ và một đa thức bắt khả quy bậc 1 là $(1+x)$. Như vậy:

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

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

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

- $m = 4, n = 15$: Trong số 16 đa thức bậc 4 chỉ có 3 đa thức sau là các đa thức bắt khả quy: $x^4 + x + 1, x^4 + x^3 + 1$ và $x^4 + x^3 + x^2 + x + 1$. Như vậy:

$$X^{15} + 1 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$$

Gọi số các đa thức bắt khả quy trong phân tích của $X^n + 1$ là $|I|$, khi đó số các Ideal trong vành được xác định theo biểu thức sau: $|I| = 2^l - 1$

Định nghĩa 5: Đa thức $g^*(X)$ được gọi là đa thức đối ngẫu của đa thức $g(X)$ nếu:

$$g^*(X) = X^{\deg g(X)} g(X^{-1})$$

Ví dụ 5: Cho $g(X) = (1 + X + X^3)$.

Khi đó đa thức đối ngẫu $g^*(X)$ của nó là:

$$g^*(X) = X^3 \left(1 + \frac{1}{X} + \frac{1}{X^3} \right) = X^3 + X^2 + 1$$

Nếu $g^*(X) = g(X)$ thì $g(X)$ được gọi là đa thức tự đối ngẫu.

Nhận xét:

- Nếu $a(X)$ là bất khả quy thì nó phải chứa một số lẻ các đơn thức.
- Nếu $a(X)$ là bất khả quy thì $a^*(X)$ cũng là một đa thức bất khả quy.

4.4.3. Định nghĩa mã xylic

Định nghĩa 6: Mã xylic (n, k) là Ideal $I = \langle g(X) \rangle$ của vánh đa thức $Z_2[x]/X^n + 1$.

Vì Ideal $\langle g(X) \rangle$ chứa tất cả các bội của $g(X)$ nên nếu $a(X) \in \langle g(X) \rangle$ thì $a(X):g(X)$ và hiển nhiên là $x.a(X):g(X) \Rightarrow x.a(X) \in \langle g(X) \rangle$.

Ta có thể đưa ra một định nghĩa trực quan hơn cho mã xylic.

Định nghĩa 7: Mã xylic là một bộ mã tuyến tính có tính chất sau: Nếu $a(X)$ là một từ mã thì dịch vòng của $a(X)$ cũng là một từ mã thuộc bộ mã này.

Chú ý: $g(X)$ được gọi là đa thức sinh của mã xylic

Ví dụ 7: Tập tất cả các mã xylic trên vánh $Z_2[x]/X^7 + 1$. Vánh này có tất cả 7 ideal tương ứng với 7 bộ mã xylic.

Nº	$g(X)$	Mã (n, k)	d_0
1	1	$(7, 7)$	1
2	$1 + X$	$(7, 6)$	2
3	$1 + X + X^3$	$(7, 4)$	3
3	$1 + X^2 + X^3$	$(7, 4)$	3
4	$1 + X + X^2 + X^4$	$(7, 3)$	4
4	$1 + X^2 + X^3 + X^4$	$(7, 3)$	4

7	$\sum_{i=0}^6 x^i$	(7, 1)	7
---	--------------------	--------	---

4.4.4. Ma trận sinh của mã cyclic

Vì mã cyclic (n, k) là một mã tuyến tính nên ta có thể mô tả nó thông qua ma trận sinh G nên chứa k véctơ hàng độc lập tuyến tính. Ta có thể thiết lập G như sau:

$$G = \begin{pmatrix} g(X) \\ x \cdot g(X) \\ \dots \\ x^{k-1} \cdot g(X) \end{pmatrix} \quad (4.1.6)$$

Ví dụ 8: Mã cyclic $(7, 4)$ có đa thức sinh $g(X) = 1 + X + X^3$. Ma trận sinh của mã này có thể mô tả như sau:

$$G = \begin{pmatrix} 1 + X + X^3 \\ X + X^2 + X^4 \\ X^2 + X^3 + X^5 \\ X^3 + X^4 + X^6 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

4.4.5. Ma trận kiểm tra của mã cyclic

Vì $g(X)|X^n + 1$ nên ta có thể viết $x^n + 1 = g(X)h(X)$

$$\text{Hay } h(X) = \frac{x^n + 1}{g(X)}$$

$h(X)$ được gọi là đa thức kiểm tra.

Vì $g(X) \cdot h(X) \equiv 0 \pmod{X^n + 1}$ nên các đa thức $h(X)$ và $g(X)$ được gọi là các đa thức trực giao.

$$\text{Ta có: } h(X) = \sum_{j=0}^k h_j x^j \text{ với } h_0 = h_k = 1, h_j \in \{0, 1\} \text{ với } j = \overline{2, k-1}$$

Do sự khác biệt giữa tích vô hướng của 2 véctơ và tích của hai đa thức tương ứng nên ta có thể xây dựng ma trận kiểm tra của mã cyclic sinh bởi $g(X)$ như sau:

$$H = \begin{pmatrix} h^*(X) \\ x \cdot h^*(X) \\ \vdots \\ x^{r-1} \cdot h^*(X) \end{pmatrix} \quad (4.17)$$

Ví dụ 9: Xây dựng ma trận kiểm tra cho mã xylic $(7, 4)$ có $g(X) = 1 + X + X^3$

Ta có:
$$h(X) = \frac{X^7 + 1}{X^3 + X + 1} = (1 + X)(1 + X^2 + X^3) = X^4 + X^2 + X + 1$$

$$h^*(X) = 1 + X^2 + X^3 + X^4$$

Ma trận kiểm tra:

$$H = \begin{pmatrix} 1 + X^2 + X^3 + X^4 \\ X + X^3 + X^4 + X^5 \\ X^2 + X^4 + X^5 + X^6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Ta dễ dàng kiểm tra: $G H^T = 0$

Với $a(X)$ là một từ mã ta có: $[a(X)] H^T = 0$

4.5. MÃ HÓA CHO CÁC MÃ XYCLIC

4.5.1. Mô tả từ mã của mã xylic hệ thống

Định nghĩa: Mã xylic (n, k) được gọi là một mã xylic hệ thống nếu ta có thể chỉ rõ vị trí của các dấu thông tin và các dấu kiểm tra trong từ mã.

Thông thường các dấu thông tin được sắp xếp ở k vị trí bậc cao (từ bậc r tới bậc $n - 1$). Các vị trí bậc thấp còn lại là các dấu kiểm tra (từ bậc 0 tới bậc $r - 1$)

f_0	f_1	\cdots	f_{r-1}	f_r	f_{r+1}	\cdots	f_{n-1}
r dấu kiểm tra				k dấu thông tin			
$f(X) = \sum_{i=0}^{n-1} f_i x^i = x^{n-k} \cdot a(X) + r(X)$							

Ta có: $f(X) \cdot g(X) \Rightarrow f(X) = q(X)g(X) \quad (1.18)$

$$\Rightarrow \frac{f(X)}{g(X)} = \frac{x^{n-k} \cdot a(X)}{g(X)} + \frac{r(X)}{g(X)}$$

$$\frac{f(X)}{g(X)} = q(X) + \frac{r'(X)}{g(X)} + \frac{r(X)}{g(X)} \quad (1.19)$$

Từ (1.1) và (1.2) ta thấy: $r'(X) + r(X) = 0$

4.5.2. Thuật toán mã hóa hệ thống

Từ (1.19) ta có thể mô tả thuật toán xây dựng từ mã xylic theo các bước sau:

VÀO: Tin rời rạc $a_i \in A$

RA: Từ mã $f_i(x)$ tương ứng với a_i .

Bước 1: Mô tả tin a_i trong tập tin cần mã hóa (gồm 2^k tin) bằng một đa thức $a_i(X)$ với $\deg a_i(X) \leq k - 1$.

Bước 2: Nâng bậc $a_i(X)$ bằng cách nhân nó với x^{n-k} .

Bước 3: Chia $a_i(X) \cdot x^{n-k}$ cho đa thức sinh $g(X)$ để tìm phần dư $r_i(X)$.

Bước 4: Xây dựng từ mã xylic: $f_i(x) = a_i(X) \cdot x^{n-k} + r_i(X) \quad (1.20)$

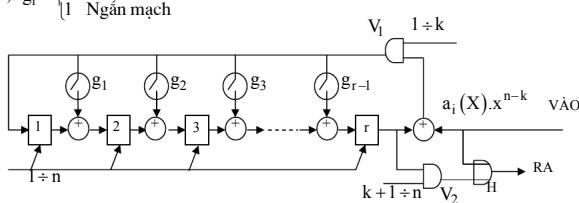
4.5.3. Thiết bị mã hóa

Phản trung tâm của thiết bị mã hóa là một thiết bị chia cho $g(X)$ để tính dư. Thực chất đây là một otomat nhớ dạng của $g(X)$.

$$\text{Giả sử: } g(X) = \sum_{i=0}^{r-1} g_i x^i \quad (1.21)$$

Khi đó thiết bị mã hóa cho mã (n, k) với đa thức sinh dạng (1.21) được mô tả như sau (Hình 4.1):

$$4.1: g_i = \begin{cases} 0 & \text{Hở mạch} \\ 1 & \text{Ngắn mạch} \end{cases}$$



Hình 4.1: Thiết bị mã hóa cho mã xylic (n, k) có đa thức sinh $g(X)$

Xung nhịp	VÀO	Trạng thái các ô nhớ				RA
		f_3	f_4	f_5	f_6	
1	1	1	0	0	0	1
2	0	0	1	0	0	0
3	0	0	0	1	0	0
4	1	1	0	0	1	1
5	0	1	1	0	0	1
6	0	1	1	1	0	1
7	0	0	1	1	1	0

4.5.5. Thuật toán thiết lập từ mã hệ thống theo phương pháp nhân

VÀO: - Mã xyclic (n, k), $g(X)$

- Tin $a_i \in A$

RA: Từ mã hệ thống của mã (n, k) xyclic

Bước 1: Mã hóa tin a_i bằng đa thức thông tin $a(X)$ với $\deg a(X) \leq k-1$,

$$a(X) = \sum_{j=0}^{k-1} a_j x^j$$

Bước 2: - Nâng bậc: $a(X) \cdot x^{n-k}$

$$a(X) \cdot x^{n-k} = \sum_{j=0}^{k-1} a_{j+r} x^{j+r} = \sum_{i=r}^{n-1} f_{i+r} x^i$$

- Tính $h(x)$.

Bước 3: for $i = 1$ to $n - k$ do

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

Bước 4: Thiết lập từ mã hệ thống.

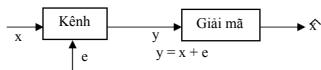
$$(f_0, f_1, \dots, f_{n-1}) \leftrightarrow f(X) = \sum_{i=r}^{n-1} f_i x^i$$

4.6. GIẢI MÃ NGƯỜNG

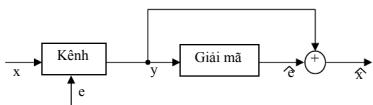
4.6.1. Hai thủ tục giải mã

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

- Phương pháp (thủ tục 1): Dẫn ra bản tin từ dãy dấu nhận được.



- Thủ tục 2: Dẫn ra véctơ sai từ dãy dấu nhận được.



4.6.2. Giải mã theo Syndrom

Giả sử $v \in V$ - mã xylic (n, k) có đa thức sinh $g(X)$.

Mã trận sinh của $V_{-}(n, k)$ có dạng:

$$G = \begin{pmatrix} g(X) \\ x \cdot g(X) \\ \dots \\ x^{k-1} \cdot g(X) \end{pmatrix}$$

Gọi $h(X) = \frac{x^n H}{g(X)}$; Ta có $\deg g(X) = r$, $\deg h(X) = k$.

Gọi $h^*(X)$ là đa thức đối ngẫu của $h(X)$. Theo định nghĩa:

$$h^*(X) = x^{\deg h(X)} \cdot h(x^{-1})$$

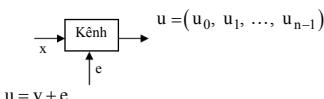
Khi đó ma trận kiểm tra của mã $V_{-}(n, k)$ có dạng:

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

Ta có $G.H^T = 0$

Với v bất kỳ, $v \in V$ ta có $v.H^T = 0$

Xét mô hình kênh truyền tin sau:



Ta có $S(u) = u.H^T = (v + e).H^T = e.H^T = S(e)$

$S(e)$ là một vectơ r chiều đặc trưng cho vectơ sai e n chiều.

Ta gọi $S(u)$ là Syndrom của vectơ nhận được 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: $S(u) = S(e) \neq 0$

Căn cứ vào trạng thái (giá trị) cụ thể của $S(e)$ mà ta có thể đưa ra một phán đoán nhất định về e .

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

4.6.3. Hệ tổng kiểm tra trực giao và có khả năng trực giao

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.

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 U_i nếu:

- Mỗi tổng kiểm tra trong hệ đều chứa U_i .
- Đầu mã U_j ($j \neq i$) chỉ nằm tối đa trong một tổng kiểm tra.

Nhận xét:

- Hệ tổng kiểm tra trực giao chứa nhiều thông tin về U_i và chứa ít thông tin về các đầu mã khác.

- Sai ở một đầu mã U_j chỉ làm ảnh hưởng tới nhiều nhất là một tổng kiểm tra trong hệ.

- Sai ở U_i sẽ làm thay đổi tất cả các giá trị của các tổng kiểm tra trong hệ.

- Ta có thể sửa được sai cho đầu U_i dựa trên thông tin về giá trị của các tổng kiểm tra bằng phương pháp bù phiếu (giải mã ngược theo da số). Khi đó khoảng cách mã Hamming đạt được theo phương pháp này sẽ thỏa mãn điều kiện:

$$d_0 = J + 1$$

Điều kiện trực giao trên là một điều kiện khá chặt chẽ, bởi vậy $J < r$ (số tổng kiểm tra độc lập tuyến tính) và không phải với bất cứ mã nào ta cũng có thể xây dựng được hệ J tổng kiểm tra trực giao thỏa mãn điều kiện $J = d_0 - 1$.

Để mở rộng hơn ta sẽ đưa ra khái niệm hệ tổng kiểm tra có khả năng trực giao.

Định nghĩa: Hệ tổng kiểm tra được gọi là có khả năng trực giao nếu nó là hệ tổng kiểm tra trực giao với một tổ hợp tuyến tính nào đó các đầu mã.

Xét tổ hợp tuyến tính các đầu mã sau: $\alpha = U_{i_1} + U_{i_2} + \dots + U_{i_m}$. Khi đó hệ tổng kiểm tra có khả năng trực giao sẽ gồm các tổng kiểm tra thỏa mãn điều kiện:

- α nằm trong tất cả các tổng kiểm tra trong hệ.
- U_j ($j \neq i_k$ với $U_{i_k} \in \alpha$) chỉ nằm trong nhiều nhất là một tổng kiểm tra trong hệ.

Nhận xét:

- Dựa trên hệ tổng kiểm tra có khả năng trực giao ta có thể giải mã được cho giá trị của α bằng phương pháp ngược.

- Để giải mã cho một đầu mã U_{i_k} cụ thể ta phải sử dụng nhiều bước (nhiều cấp ngược).

4.6.4. Giải mã ngược dựa trên hệ tổng kiểm tra trực giao

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

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

$$h^*(X) = 1 + x^2 + x^3$$

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

$$v \cdot H^T = [S_i]$$

Ta có hệ tông kiểm tra trực giao với dấu mã v_3

$$S_0 = v_0 + v_2 + v_3$$

$$S_1 = v_1 + v_4 + v_3$$

$$S_2 = v_5 + v_6 + v_3$$

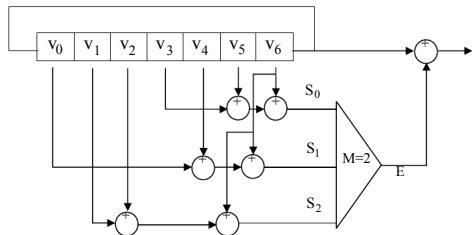
\Rightarrow Hệ tông kiểm tra với dấu mã v_6 (suy ra bằng cách dịch vòng hệ tông kiểm tra trên)

$$S_0 = v_6 + v_3 + v_5$$

$$S_1 = v_6 + v_0 + v_4$$

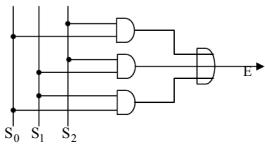
$$S_2 = v_6 + v_1 + v_2$$

Sơ đồ thiết bị giải mã theo thứ tự 2:



Sơ đồ thiết bị ngưỡng M = 2

$$E = S_0 S_1 + S_1 S_2 + S_2 S_3$$



Quá trình giải mã được thực hiện trong $2n = 14$ nhịp. 7 nhịp đầu để đưa từ mã nhận được vào các ô nhớ. Quá trình giải mã được thực hiện trong 7 nhịp sau.

Giải mã từ mã nhận được có dạng 0 0 1 1 1 1 1

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

Nhip	Trạng thái các ô nhớ							S_0	S_1	S_2	E	R_4	
	v_0	v_1	v_2	v_3	v_4	v_5	v_6						
0	0	0	1	1	1	1	1						
1	1	0	0	1	1	1	1	1	0	0	0	0	1
2	1	1	0	0	1	1	1	1	1	1	1	1	0
3	1	1	1	0	0	1	1	0	1	0	0	0	1
4	1	1	1	1	0	0	1	0	0	1	0	1	1
5	1	1	1	1	1	0	0	0	0	1	0	1	1
6	0	1	1	1	1	1	0	1	0	0	0	0	0
7	0	0	1	1	1	1	1	0	1	0	0	0	0

Từ mã đã giải mã: 0 0 1 1 1 0 1

Hay $\hat{v}(X) = x^6 + x^4 + x^3 + x^2$

Sai ở vị trí x^5 đã được sửa.

Kiểm tra lại:

$$\begin{array}{r} x^6 + x^4 + x^3 + x^2 \\ \underline{- x^6 + x^4 + x^3 + x^2} \\ 0 \end{array}$$

4.6.5. Giải mã ngưỡng dura trên hệ tổng kiểm tra có khả năng trực giao

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

$$h(X) = \frac{x^7 + 1}{g(X)} = x^4 + x^2 + x + 1$$

$$h^*(X) = 1 + x^2 + x^3 + x^4$$

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

Ta có: $vH^T = [S_i]$

Hệ tổng kiểm tra có khả năng trực giao với cặp dấu mã $v_4 + v_5$:

$$S_1 = v_5 + v_4 + v_3 + v_1$$

$$S_2 = v_5 + v_4 + v_2 + v_6$$

Dịch vòng hệ tổng kiểm tra này đi hai cấp ta có được hệ tổng kiểm tra có khả năng trực giao với cặp dấu mã: $v_6 + v_0$:

$$\dot{S}_1 = v_0 + v_6 + v_5 + v_3$$

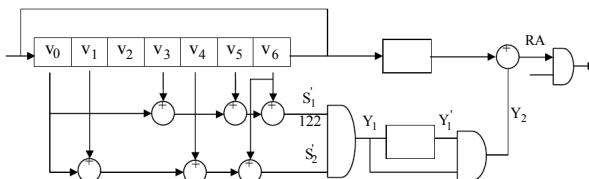
$$\dot{S}_2 = v_0 + v_6 + v_4 + v_1$$

Ở nhịp giải mã đầu tiên sau cấp ngưỡng thứ nhất ta có được giá trị đúng của $(v_0 + v_6)$.

Tới nhịp giải mã thứ hai ta có được giá trị đúng của $(v_6 + v_5)$.

Căn cứ vào các giá trị này ta có thể giải ra được giá trị đúng của v_6 sau cấp ngưỡng thứ hai.

Sơ đồ chức năng thiết bị giải mã theo thủ tục 2.



CY: Thiết bị ngưỡng ở cả hai cấp ngưỡng chỉ là một mạch VÀ có hai đầu vào.

Giả sử từ mã nhận được có dạng 0 0 1 1 1

Hay $v(X) = x^6 + x^5 + x^4 + x^3$

Quá trình giải mã được thực hiện trong $2n+1=15$ nhịp. $n=7$ nhịp đầu, từ mã nhận được đưa vào các ô nhớ. 8 nhịp sau là quá trình giải mã.

Nhịp	Trạng thái các ô nhớ							S_1'	S_2'	Y_1	Y_1'	Y_2	RA
	v_0	v_1	v_2	v_3	v_4	v_5	v_6						
1	1	0	0	0	1	1	1	1	0	0	0	0	—
2	1	1	0	0	0	1	1	1	1	1	0	0	1
3	1	1	1	0	0	0	1	1	1	1	1	1	0
4	1	1	1	1	0	0	0	0	1	0	1	0	1
5	0	1	1	1	1	0	0	0	0	0	0	0	1
6	0	0	1	1	1	1	0	1	0	0	0	0	0
7	0	0	0	1	1	1	1	0	1	0	0	0	0
8	1	0	0	0	1	1	1	1	0	0	0	0	0

Sai ở vị trí x^5 đã được sửa.

Từ mã đã giải mã: 0 0 0 1 1 0 1

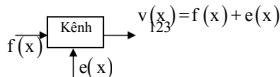
Hay $\hat{v}(x) = x^6 + x^4 + x^3$

Kiểm tra lại:

$$\begin{array}{r} \overline{x^6 + x^4 + x^3} \\ \underline{x^6 + x^4 + x^3} \\ 0 \end{array} \quad \left| \begin{array}{r} x^3 + x + 1 \\ x^3 \end{array} \right.$$

4.7. GIẢI MÃ THEO THUẬT TOÁN MEGGIT

Giả sử $f(x)$ là một từ mã của một bộ mã cyclic $V_-(n, k)$ có đa thức sinh $g(x)$. Khi đó $f(x) \vdash g(x)$.

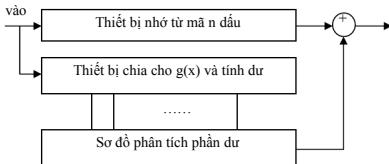


Giả sử $v(x)$ là từ mã đưa tới đầu vào bộ giải mã, khi đó:

$$\frac{v(x)}{g(x)} = \frac{f(x)}{g(x)} + \frac{e(x)}{g(x)} \quad (4.22)$$

Bằng cách phân tích phần dư của phép chia trên ta có thể tìm được đa thức sai $e(x)$.

Sơ đồ phân tích dư là một sơ đồ logic tổng hợp, đây là một thành phần chức năng quan trọng trong sơ đồ giải mã theo thuật toán Meggit sau:



Ví dụ: Xét mã cyclic $(7, 4)$ có $g(x) = x^3 + x + 1$. Giả sử dấu sai là dấu đầu tiên có bậc cao nhất của từ mã, khi đó ta có $e(x) = x^6$. Phần dư tương ứng của (4.22):

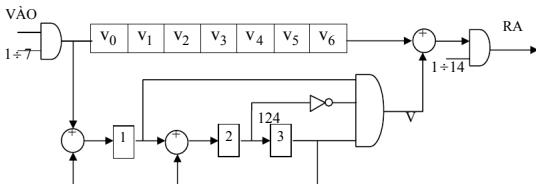
$$\begin{array}{r}
 x^6 \\
 x^4 + x^3 \\
 x^3 + x^2 + x \\
 \hline
 x^3 + x + 1
 \end{array} \quad | \quad
 \begin{array}{r}
 x^3 + x + 1 \\
 x^3 + x + 1 \\
 \hline
 x^3 + x^2 + x
 \end{array}$$

Phần dư $r(x) = x^2 + 1$

Khi nhận thấy phần dư có dạng $r(x) = x^2 + 1$ thì sơ đồ phân tích phần dư cho ra tín hiệu sửa sai (Tín hiệu 1) đưa tới bộ công mod 2 để sửa sai cho dấu mã tương ứng.

Như vậy chỉ khi phần dư có dạng 1 0 1 thì thiết bị logic tổ hợp mới tạo ra tín hiệu "1" để sửa sai.

Sơ đồ bộ giải mã có dạng:



Sau $2n = 14$ nhịp, bộ giải mã hoàn thành quá trình giải mã (7 nhịp đầu chia và tính dư dòng thời đưa từ mã vào bộ ghi dịch điện, 7 nhịp sau để giải mã).

Ví dụ từ mã nhận được có dạng:

$$v(x) = x^3 + x^2 + x \leftrightarrow 0\ 1\ 1\ 1\ 0\ 0\ 0$$

Hoạt động của bộ giải mã được mô tả theo bảng sau:

Nhịp	VÀO	Trạng thái các ô nhớ										V	RA
		v ₀	v ₁	v ₂	v ₃	v ₄	v ₅	v ₆	1	2	3		
1	0	0	0	0	0	0	0	0	0	0	0		
2	0	0	0	0	0	0	0	0	0	0	0		
3	0	0	0	0	0	0	0	0	0	0	0		
4	1	1	0	0	0	0	0	0	1	0	0		
5	1	1	1	0	0	0	0	0	1	1	0		
6	1	1	1	1	0	0	0	0	1	1	1		
7	0	0	1	1	1	0	0	0	1	0	1		
8	0	0	0	1	1	1	0	0	1	0	0	1	1
9	0	0	0	0	1	1	1	0	0	1	0	0	0
10	0	0	0	0	0	1	1	1	0	0	1	0	0
11	0	0	0	0	0	0	1	1	1	1	0	0	1
12	0	0	0	0	0	0	0	0	1	0	1	1	0
13	0	0	0	0	0	0	0	0	0	1	1	0	1
14	0	0	0	0	0	0	0	0	0	1	0	1	0

Từ mã đã sửa: $\hat{v}(x) = v(X) + e(X) = x^6 + x^3 + x^2 + x$

Dấu sai là x^6 đã được sửa

4.8. GIẢI MÃ XYCLIC THEO THUẬT TOÁN CHIA DỊCH VÒNG

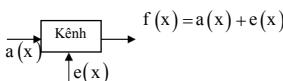
4.8.1. Nhiệm vụ của thuật toán giải mã

Ta biết rằng với mã cyclic (n, k) khi chia từ mã nhận được $f(x)$ cho đa thức sinh $g(x)$ sẽ có hai trường hợp sau xảy ra:

0 Nếu từ mã nhận đúng (không có sai trên kênh truyền: $e(x) = 0$) thì phép chia này không có dư.

- Nếu từ mã nhận sai ($e(x) \neq 0$) thì phép chia này có dư.

Cấu trúc của phần dư sẽ phản ánh cấu trúc của vectơ sai $e(x)$. Vì vậy việc phân tích cấu trúc của phần dư chính là nhiệm vụ của các thuật toán giải mã.



Ta có: $a(x) \vdots g(x)$.

$$\frac{f(x)}{g(x)} = \frac{a(x)}{g(x)} + \frac{e(x)}{g(x)} \quad (4.23)$$

Như vậy phần dư của phép chia $f(x)$ cho $g(x)$ chính là phần dư của phép chia vectơ sai $e(x)$ cho $g(x)$.

Chú ý: Phần dư của phép chia $e(x)$ cho $g(x)$ là một đa thức có bậc $\leq r - 1$. Như vậy phần dư này có 2^r trạng thái khác nhau. Trong khi đó số các kiểu sai khác nhau lại là $2^n > 2^r$.

Số các kiểu sai có trọng số $\leq t$ là:

$$C_n^0 + C_n^1 + C_n^2 + \dots + C_n^t$$

Như vậy điều kiện cần để sửa được t sai là:

$$\sum_{i=0}^t C_n^i \leq 2^{n-k} \quad (4.23)$$

Đây chính là giới hạn Hamming

4.8.2. Giải mã theo thuật toán chia dịch vòng

4.8.2.1. Nhận xét

Từ (1.1) ta thấy rằng nếu k dấu thông tin trong từ mã đầu nhận đúng thì vị trí sai các con " 1 " trong phần dư chính là vị trí tương ứng của các dấu kiểm tra bị sai. Để giải mã ta chỉ cần cộng (theo mod 2) từ mã nhận được với phần dư sau phép chia là thu được từ mã đã phát.

4.8.2.2. Thuật toán chia dịch vòng (bằng lối)

VÀO: - Từ mã nhận được $f(x)$

- Mã $V_-(n, k)$ có $g(x)$, có d_0 .

RA: - Từ mã đánh giá $\hat{f}(X)$

Bước 1: For $i := 0$ to $(n-1)$ do.

(1) Chia $f(x).x^i$ (hoặc $\frac{f(x)}{x^i}$) cho $g(x)$ để tìm phần dư $r_i(x)$.

(2) Tính $w(r_i(x))$.

- Nếu $w(r_i(x)) \leq t = \left\lceil \frac{d_0 - 1}{2} \right\rceil$ chuyển sang bước 2.

- Nếu $w(r_i(x)) > t \Rightarrow i := i + 1$. Nếu $i + 1 = n$ chuyển sang bước 3.

Bước 2: Từ mã đánh giá:

$$\hat{f}(X) = \frac{f(x).x^i + r_i(x)}{x^i}$$

$$\left(\text{Hoặc } \hat{f}(X) = x^i \left[\frac{f(x)}{x^i} + r_i(x) \right] \right)$$

Bước 3: - Thông báo không sửa được sai (Số sai vượt quá khả năng sửa sai của bộ mã)

4.8.3. Ví dụ

Giả sử từ mã nhận được của mã cyclic $(7, 3, 4)$ với đa thức sinh

$$g(x) = 1 + x + x^2 + x^4$$

$$v(x) = x + x^2 + x^3 + x^5 + x^6 \leftrightarrow 0111011$$

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

Bước 1:

(1) $i = 0$ (+) Chia $v(x)$ cho $g(x)$ để tìm phần dư $r_0(x)$.

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

$$(+)\ w(r_0(x)) = 3 > \left[\frac{4-1}{2} \right] = 1$$

(2) $i = 1$ (+) Chia $x.v(x)$ cho $g(x)$ để tìm phần dư $r_1(x)$.

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

$$(+)\ w(r_1(x)) = 1 = t$$

Bước 2: Tìm tử mã đánh giá.

$$\hat{f}(X) = \frac{x.v(x) + r_1(x)}{x} = x^5 + x^3 + x^2 + x$$

Vậy sai ở vị trí α đã được sửa

4.9. GIẢI MÃ LUỐI.

4.9.1. Trạng thái và giản đồ lưới

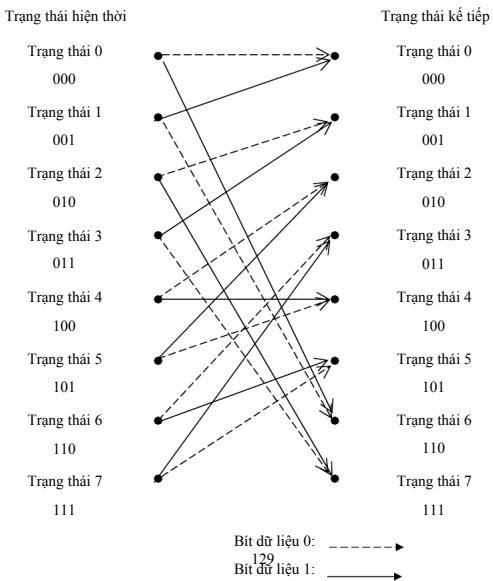
Từ bảng trạng thái của sơ đồ mã hóa ở mục 4.5.3 ta có một số nhận xét sau:

- Quá trình mã hóa luôn bắt đầu từ trạng thái toàn 0 và kết thúc cũng ở trạng thái toàn 0.
- Trong k nhịp đầu ($k = 4$) các bit ra giống như các bit vào.
- Sau nhịp thứ k, các bit kiểm tra nằm trong thanh ghi được đẩy dần ra đầu ra.

- Số các trạng thái bằng 2^{n-k} (trong ví dụ này $2^{7-4} = 8$ trạng thái) tăng theo hàm mũ khi $n - k$ tăng.

Sử dụng thanh ghi mô tả trong mục 4.5.3 ta có thể tìm được tất cả các trạng thái kế tiếp khi thanh ghi nằm ở một trạng thái xác định.

Hình sau chỉ ra tất cả các dịch chuyển trạng thái có thể ở một trạng thái bất kỳ của bộ mã hóa cho mã (7, 4, 3).



Hình 4.2: Biểu đồ chuyển trạng thái cho mã (7, 4, 3) có 8 trạng thái

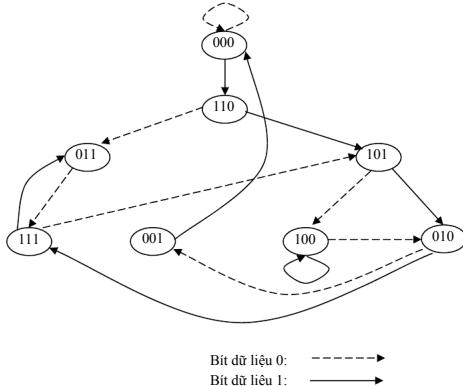
Bằng cách sử dụng biểu đồ trạng thái trên ta có thể mã hóa các bit dữ liệu 1011 mà không dùng thanh ghi dịch trong mục 4.5.2. Bit dữ liệu đầu tiên là logic 1, bởi vậy trạng thái sẽ chuyển từ 000 đến 110 (minh họa bằng đường liên kết từ trạng thái 000). Đầu ra bộ mã hóa lúc này cũng là 1 giống như đầu vào. Ở thời điểm kế tiếp trạng thái hiện tại là 110 và bit dữ liệu là logic 0, bởi vậy trạng thái sẽ chuyển từ 110 sang 011 ...

Như vậy qua 4 nhịp ta thấy quá trình chuyển trạng thái là:

$$000 \rightarrow 110 \rightarrow 011 \rightarrow 001 \rightarrow 110$$

Sau nhịp thứ 4, các thay đổi trạng thái sẽ tuân theo việc dịch các bit kiểm tra từ thanh ghi (ở đây là 110).

Ta cũng có thể sử dụng một cách mô tả khác cho quá trình mã hóa bằng giản đồ lưới (hình 4.4)



Hình 4.3: Gian đồ trạng thái cho mã $(7, 4, 3)$ có 8 trạng thái

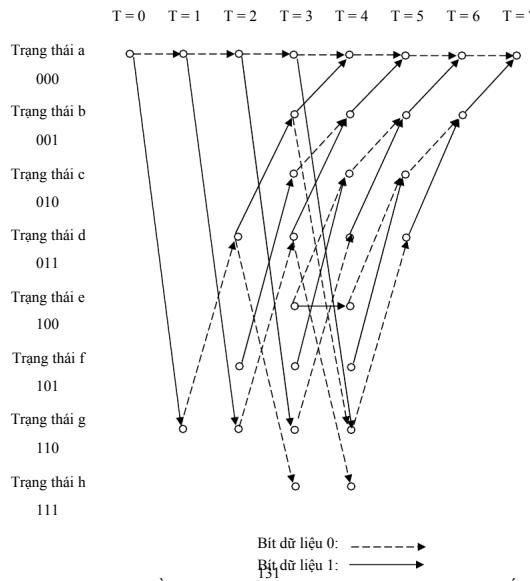
Gian đồ này được tạo nên bằng cách nối các trạng thái kế tiếp của gian đồ chuyển trạng thái ở hình 4.2 bắt đầu từ trạng thái toàn 0.

Giản đồ này minh họa toán bộ $2^k = 16$ đường dẫn có thể có cho mã $(7, 4, 3)$. Lưới có $2^{n-k} = 8$ hàng (8 trạng thái khác nhau), và có $n+1 = 8$ cột. Các nút trong cùng hàng biểu thị cùng một trạng thái trong khi đó các nút trong cùng một cột biểu thị tất cả các trạng thái có thể 000 (trạng thái a), 001 (trạng thái b), 010 (trạng thái c), ..., 111 (trạng thái h). Việc chuyển trạng thái giữa các cột kế cận được vẽ bằng các đường liên kết hoặc bằng các đường đứt nét tùy theo liệu bít ráu của bộ mã hóa là 1 hay 0.

Chi có duy nhất một trạng thái ban đầu là trạng thái toàn 0 (trạng thái a). Số các trạng thái lưới sẽ tăng theo mỗi khi bit dữ liệu mới được đưa vào bộ mã hóa.

Khi đưa bit dữ liệu đầu tiên vào bộ mã hóa ($T = 0$), có thể có hai nút khác nhau ở thời điểm tiếp nhau. Bit dữ liệu từ 2 đưa vào ($T = 1$) tạo nên số các nút có thể ở thời điểm kế tiếp là 2^2 . Số các nút có thể có sẽ tiếp tục tăng theo T cho tới khi đạt tới số nút cực đại $2^{n-k} = 8$ (Số các trạng thái lớn nhất đạt được khi $T = n - k = 3$).

Sau khi $T = k$ số các trạng thái có thể sẽ được chia đôi ở mỗi thời điểm kế tiếp hướng về trạng thái 0 là trạng thái đạt được ở $T = n$.



Hình 4.4: Giản đồ lưới cho mã $(7, 4, 3)$ có 8 trạng thái và 8 giai đoạn kế tiếp

4.9.2. Giải mã lướt.

4.9.2.1. Mở đầu.

Giải mã lướt cho mã tuyến tính do Wolf đưa ra vào 1978, tuy nhiên kỹ thuật này chỉ thích hợp cho một số mã nhất định do số các trạng thái tăng theo hàm mũ khi $n - k$ tăng.

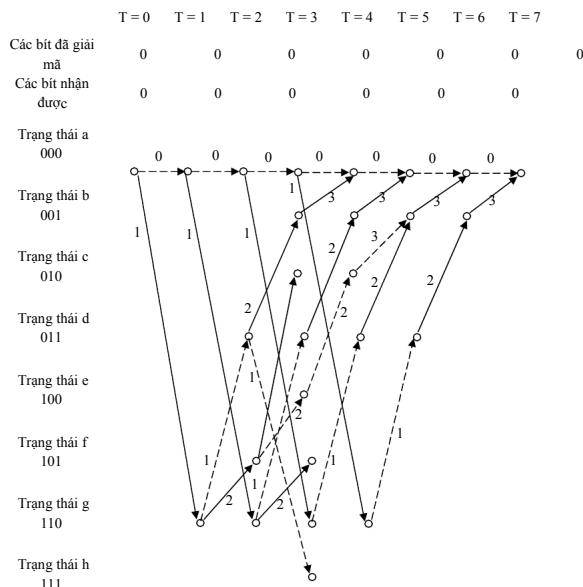
4.9.2.2. Thuật toán Viterbi

Vào 1967, Viterbi là người đầu tiên đưa ra thuật toán Viterbi (VA). Thuật toán này tìm tất cả các đường có thể trong lưới và các khoảng Hamming (hoặc các khoảng cách Euclidean) từ dây thu được ở đầu vào các bộ giải mã. Đường dẫn sẽ biểu thị khoảng cách nhỏ nhất từ dây thu được được chọn là dây phát hợp lý nhất và các dây bit thông tin kết hợp được tái tạo lại. Phương pháp này chính là phương pháp đánh giá dây hợp lý tối đa vì đường dẫn hợp lý nhất được chọn từ tập tất cả các đường dẫn trong lưới.

Hình 4.5 ghi "lịch sử" của các đường dẫn được chọn bởi bộ mã Viterbi cho mã $(7, 4, 3)$. Giả sử rằng không có sai trong kênh và bởi vậy dây vào của bộ giải mã chính là dây đã mã hóa cho dây 0000000 . Ở thời điểm đầu ($T = 1$) bit nhận được là 0 , bit này được so sánh với các bit phát có thể có là 0 và 1 tương ứng với các nhánh từ nút a và từ nút a đến g.

Độ đo của hai nhánh này là các khoảng cách Hamming của chúng (chính là sự khác nhau giữa các bit phát có thể có $(0$ hoặc 1) và bit nhận được 0). Các khoảng cách Hamming tương ứng sẽ là 0 và 1 .

Ta xác định độ đo nhánh là khoảng cách Hamming của một nhánh riêng từ các bit nhận được và độ đo đường dẫn ở thời điểm thứ T . Độ đo này bằng tổng các độ đo nhánh ở tất cả các nhánh từ $T = 0$ đến $T = T$, các độ đo đường dẫn này được ghi ở trên đỉnh của mỗi nhánh ở hình 4.5, tương ứng ở thời điểm $T = 1$ là 0 và 1 đối với các đường dẫn $a \rightarrow a$ và $a \rightarrow g$. Ở thời điểm $T = 2$ bit nhận được là 0 và các độ đo nhánh là $0, 1, 0$ và 1 tương ứng với các nhánh $a \rightarrow a$, $a \rightarrow g$, $g \rightarrow d$ và $g \rightarrow f$. Độ đo của các đường dẫn này là $0, 1, 1$, và 2 tương ứng với các đường $a \rightarrow a \rightarrow a$, $a \rightarrow a \rightarrow g$, $a \rightarrow g \rightarrow d$, $a \rightarrow g \rightarrow f$. Ở thời điểm thứ 3, bit nhận được là 0 . Có 8 nhánh có thể và các độ đo đường dẫn (xem hình 4.5) là $0, 1, 2, 1, 3, 2, 1$ và 2 tương ứng với các đường $a \rightarrow a \rightarrow a \rightarrow a$, $a \rightarrow a \rightarrow a \rightarrow g$, $a \rightarrow g \rightarrow d \rightarrow b$, $a \rightarrow g \rightarrow d \rightarrow h$, $a \rightarrow g \rightarrow f \rightarrow c$, $a \rightarrow g \rightarrow f \rightarrow e$, $a \rightarrow a \rightarrow g \rightarrow d$ và $a \rightarrow a \rightarrow g \rightarrow f$.

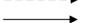


133

Bit dữ liệu 0:



Bit dữ liệu 1:



Ta ký hiệu α_1 và α_2 tương ứng là các đường $a \rightarrow a \rightarrow a \rightarrow a \rightarrow a$ và $a \rightarrow g \rightarrow d \rightarrow b \rightarrow a$, các đường này xuất phát ở nút khởi đầu a và trở về nút a ở $T = 4$. Các độ đo đường dẫn tương ứng là 0 và 3, các nhánh tiếp sau gần với $T > 4$ đi từ nút a ở $T = 4$ sẽ cộng thêm các độ đo nhánh như nhau vào các độ đo đường dẫn của cả hai đường α_1 và α_2 . Điều này có nghĩa là độ đo đường dẫn của α_2 là lớn hơn ở $T = 4$ và vẫn giữ ở mức lớn hơn với $T > 4$. Bộ giải mã Viterbi sẽ chọn đường dẫn có độ đo nhỏ nhất (chính là dây trạng thái toàn 0) và loại bỏ đường α_2 . Đường α_1 được xem là đường sống sót. Thủ tục này cũng được áp dụng ở các nút khác với $T \geq n - k = 3$. Cần lưu ý rằng các đường $a \rightarrow g \rightarrow f \rightarrow c$, $a \rightarrow a \rightarrow g \rightarrow f$, ... không thể sống sót vì các độ đo đường dẫn của chúng là lớn hơn và bởi vậy chúng bị loại bỏ khỏi bộ nhớ của bộ giải mã.

Như vậy chỉ có $2^{n-k} = 8$ đường sống sót từ $T = n - k$ đến $T = k$. Sau thời điểm $T = 3$ số các đường sống sót sẽ giảm đi một nửa sau mỗi thời điểm.

Đôi khi 2 đường nhập vào lại cùng một độ đo đường dẫn. Ở $T = 5$ các đường $a \rightarrow a \rightarrow a \rightarrow g \rightarrow d \rightarrow b$, $a \rightarrow g \rightarrow f \rightarrow e \rightarrow c \rightarrow b$ nhập lại ở nút b. Cả hai đường này đều có cùng độ đo đường dẫn là 2. Thông thường bộ giải mã Viterbi sẽ chọn ngẫu nhiên một đường sống sót và loại bỏ các đường khác. Tuy nhiên tình trạng này rất hiếm khi xảy ra trong một thuật toán Viterbi quyết định mềm (hay thuật toán Viterbi đầu ra mềm - SOVA) hay được sử dụng trong thực tế.

4.9.2.3. Giải mã Viterbi quyết định cứng.

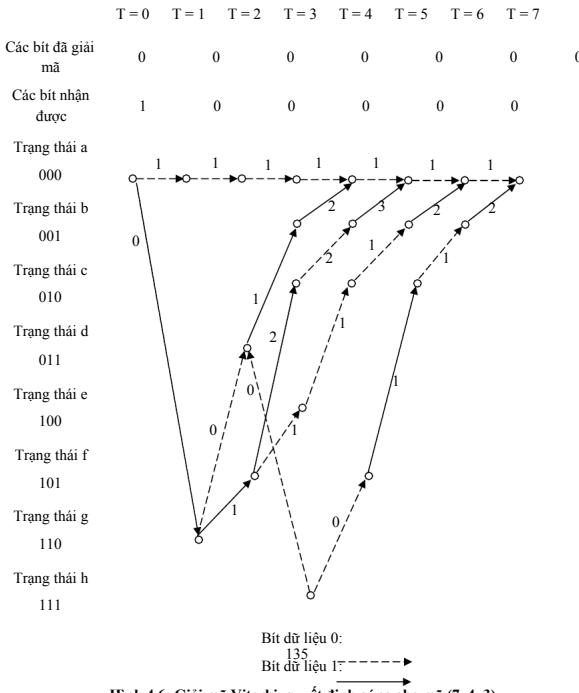
Khi giải mã quyết định cứng, bộ điều chế sẽ cho ra các quyết định cứng (1 hoặc 0) khi tạo lại dây đã phát. Trong trường hợp này các khoảng cách Hamming giữa các bit nhận được và các bit đã phát được đánh giá trong lối sẽ được dùng làm độ đo mức tin cậy.

Để minh họa cho quá trình giải mã này ta sử dụng mã (7, 4, 3) với dây bit phát là 0000000. Sai số trên kênh nằm ở bit đầu tiên và dây nhận được ở đầu ra bộ giải mã điều chế là 1000000. Bộ giải mã sẽ so sánh bit ra của bộ giải điều chế với cả hai bit có thể được giải mã (được biểu thị bằng các đường liền nét và đứt nét trên hình 4.6) là 1 và 0. Khi bit ra của bộ giải điều chế và bit được giải mã như nhau thì khoảng cách Hamming của chúng bằng 0. Ngược lại khi hai bit này khác nhau thì giá trị bằng 1 của khoảng cách Hamming sẽ được cộng thêm vào độ đo đường dẫn.

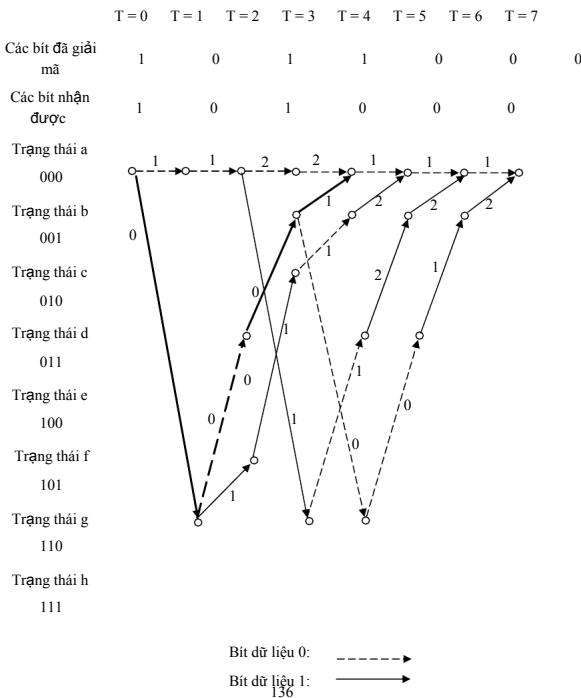
Vì ta đi ngang qua lưới nên các độ đo nhánh sẽ được cộng lại ở $T = 7$, đường dẫn có trọng số Hamming nhỏ nhất sẽ được xem là đường sống sót. Bởi vậy đây được giải mã là xâu.

Hình 4.6 minh họa việc lựa chọn đường sóng sót (được đánh giá bằng đường đứt nét đậm) của bộ giải mã Viterbi ra sao. Đường này có độ đo đường dẫn nhỏ nhất và sẽ giải mã ra được đúng dây thu được. Cần chú ý rằng độ đo đường dẫn của đường sóng sót tương đương với số sai trong dây nhận được khi bộ giải mã có khả năng sửa các sai này.

Tuy nhiên khi số sai trong kênh vượt quá khả năng sửa sai của mã thì sẽ xảy ra giải mã sai. Giả sử kênh có hai sai ở vị trí thứ 1 và vị trí thứ 3. Giải mã sai sẽ xảy ra ở 4 nhánh ban đầu (được ghi bằng đường nét trên hình 4.7) và dây được giải mã là 1011000



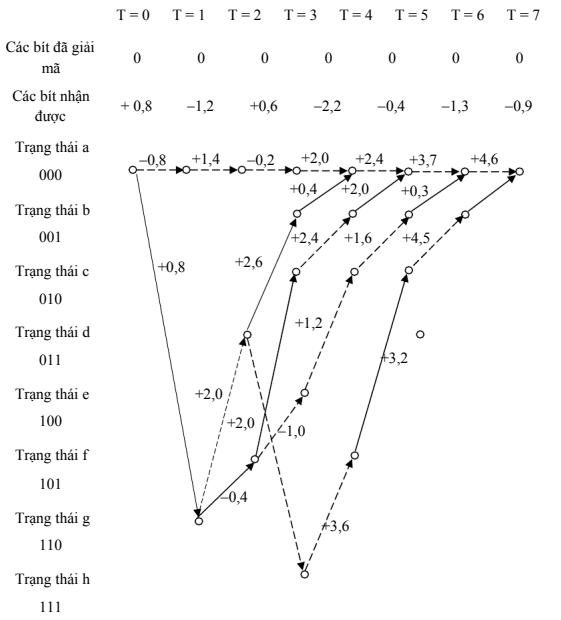
Hình 4.6: Giải mã Viterbi quyết định cứng cho mã (7, 4, 3)



Hình 4.7: Giải mã sai khi dùng giải mã Viterbi quyết định cứng

4.9.2.4. Giải mã Viterbi quyết định mềm.

Theo quan điểm giải mã Viterbi quyết định mềm, tín hiệu nhận được ở đầu ra của bộ giải mã điều chế sẽ được lấy mẫu. Sau đó các giá trị mẫu sẽ được đưa trực tiếp tới đầu vào của bộ giải mã Viterbi. Giả sử rằng ta sử dụng điều chế dịch pha nhị phân (BPSK) ở đầu phát, khi đó mức logic 0 sẽ được gửi là -1 , 0 còn mức logic 1 sẽ được gửi là $+1$. Nếu ta phát dây toán 0 thì dây phát tương ứng là $-1 - 1 - 1 - 1 - 1 - 1 - 1 - 1$. Ở máy thu, các đầu ra mềm của bộ giải mã điều chế là $+0,8, -1,2, +0,6, -2,2, -0,4, -1,3, -0,9$ (tương ứng với dây 1010000 nếu ta sử dụng giải mã quyết định cứng). Các đầu ra mềm của bộ giải mã điều chế được dùng như độ do mức độ tin cậy (xem hình 4.8).



Hình 4.8: Giải mã Viterbi quyết định mềm cho mã $(7,4,3)$

Tín hiệu ra miền đầu tiên của bộ giải điều chế là $+0,8$ ngụ ý rằng tín hiệu phát rất có thể là $+1$ và độ do mức tin cậy của quyết định này là $0,8$. Xem xét đường dẫn $a \rightarrow g$ tương ứng với logic 1, độ do nhánh của đường dẫn này là $+0,8$. Tuy nhiên đường dẫn $a \rightarrow a$ không ăn khớp với tín hiệu nhận được và độ do nhánh của đường dẫn này là $-0,8$ (tích lũy một độ ndo đường dẫn âm hay là lượng phai) do sự sai lạc của nó. Ở thời điểm thứ hai tín hiệu nhận được là $-1,2$ tạo nên các độ do đường dẫn là $+0,4, -2,0, +0,2$ và $-0,4$ tương ứng với các đường dẫn $a \rightarrow a \rightarrow a, a \rightarrow a \rightarrow g, a \rightarrow g \rightarrow d$ và $a \rightarrow g \rightarrow f$. Ta ký hiệu α_1 và α_2 là các đường $a \rightarrow a \rightarrow a \rightarrow a$ và $a \rightarrow g \rightarrow d \rightarrow b \rightarrow a$. Các độ do đường dẫn tổng cộng được tích lũy của hai đường dẫn này tương ứng là $+0,2$ và $+0,4$. Bộ giải mã Viterbi sẽ chọn đường dẫn có độ do đường dẫn lớn hơn vì mức tin cậy được tích lũy của nó lớn hơn. Bởi vậy đường α_1 sẽ được chọn (chứ không phải là đường α_2 đã được chọn trong ví dụ giải mã quyết định cứng ở trên). Điều này chứng tỏ rằng giải mã quyết định mềm có hiệu quả cao hơn giải mã quyết định cứng.

4.10. MÃ HAMMING VÀ MÃ CÓ ĐỘ DÀI CỰC ĐẠI

Mã Hamming và mã có độ dài cực đại là hai lớp mã quan trọng trong mã cyclic.

Định nghĩa: Mã cyclic Hamming là mã cyclic có đa thức sinh là đa thức nguyên thủy bậc m , mã này có các tham số như sau:

$$(n, k, d_0) = (2^m - 1, 2^m - 1 - m, 3)$$

Mã Hamming là mã tối ưu thỏa mãn giới hạn Hamming (4.13). Ngoài mã Hamming chỉ còn mã Golay (23, 12, 7) là mã hoàn thiện, mã Golay có đa thức sinh như sau:

$$g(X) = X^{11} + X^9 + X^7 + X^5 + X + 1$$

Bảng sau là danh sách các đa thức nguyên thủy có bậc m từ 2 đến 8.

Bậc	Đa thức nguyên thủy
	(0 1 2)
	(0 1 3)
	(0 1 4)
	(0 2 5), (0 2 3 4 5), (0 1 2 4 5)
	(0 1 6), (0 2 3 5 6), (0 1 2 5 6)

Bậc	Đa thức nguyên thủy
	(0 3 7), (0 1 2 3 7), (0 2 3 4 7), (0 1 2 4 5 6 7), (0 1 2 3 4 5 7), (0 2 4 6 7), (0 1 7), (0 1 3 6 7), (0 2 5 6 7),
	(0 2 3 4 8), (0 3 5 6 8), (0 1 2 5 6 7 8), (0 1 3 5 8), (0 2 5 6 8), (0 1 5 6 8), (0 1 2 3 4 6 8), (0 1 6 7 8)

Chú ý: ở bảng trên ta thấy ký hiệu viết các đa thức theo số mũ của các bậc khác không.

Ví dụ: $(02567) \leftrightarrow g(X) = X^7 + X^6 + X^5 + X^2 + 1$

Các đa thức đối ngẫu của các đa thức trong bảng cũng là các đa thức nguyên thủy, các đa thức này không được liệt kê ở đây.

Ví dụ: Đa thức đối ngẫu của $g(X) = X^4 + X + 1$ là đa thức

$$g^*(X) = X^4 + X^3 + 1.$$

Mã đối ngẫu của mã Hamming là mã có độ dài cực đại. mã này có tham số như sau:

$$(n, k, d_0) = (2^m - 1, m, 2^{m-1})$$

Đa thức sinh của mã này có dạng sau:

$$g(X) = \frac{X^{2^m-1} + 1}{h(X)}$$

Trong đó $h(X)$ là đa thức nguyên thủy bậc m .

Các mã có độ dài cực đại là các mã tối ưu thỏa mãn giới hạn Griesmer (4. 11).

Ví dụ: - Mã cyclic (7, 4) có đa thức sinh $g(X) = X^3 + X + 1$ là mã Hamming.

- Mã cyclic (7, 3) có đa thức sinh $g(X) = X^4 + X^2 + X + 1$ là mã có độ dài cực đại.

4.11. CÁC MÃ KHÓI DỰA TRÊN SỐ HỌC CỦA TRƯỜNG HỮU HẠN

4.11.1. Trường hữu hạn cơ nguyên tố GF(p)

Ta đã làm quen với trường nhị phân GF(2), trong trường này các phép toán số học được thực hiện theo modulo 2. Tương tự đối với trường GF(p) với p là số nguyên tố, các phép toán số học thích hợp (cộng và nhân) giữa hai phần tử bất kỳ của trường phải được thực hiện theo modulo p. Phần tử ngược của một phần tử bất kỳ đối với phép cộng được tính bằng kết quả của phép trừ giữa p và phần tử đó. Ví dụ trong GF(7), phần tử ngược của phép cộng của 5 là 2. Phần tử ngược của phép nhân (phần tử nghịch đảo) khó tìm hơn, tuy nhiên quan điểm sau đây sẽ giúp ta tìm được nó đồng thời cho ta một phương pháp xây dựng trường. Trong trường GF(p) người ta đã chứng

minh được rằng tồn tại ít nhất một phần tử mà các lũy thừa của nó là các phần tử khác 0 của trường. Phần tử này được gọi là phần tử nguyên thủy. Ví dụ trong trường GF(7) số 3 là phần tử nguyên thủy vì:

$$\{3^0 = 1, 3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5\}$$

Đây là một nhóm nhân xyclic cấp 6 (có thể thấy rằng nhóm nhân này có hai phần tử nguyên thủy là 3 và 5).

Với 3^6 ta thấy $3^6 = 3^5 \cdot 3 = 5 \cdot 3 \bmod 7 = 1$.

Ta có thể thực hiện phép nhân bằng cách cộng các số mũ của 3.

Ví dụ: $6 \cdot 2 = (3^3) \cdot (3^2) = 3^5 = 3$.

Bởi vậy ta có thể tìm được phần tử nghịch đảo của một phần tử 3^n bất kỳ là $3^{-n} = 3^{6-n}$. Như vậy nghịch đảo của 6 là 6 và nghịch đảo của 5 là 3.

4.11.2. Các trường mở rộng của trường nhị phân. Trường hữu hạn GF(2^m)

Ta có thể xây dựng được trường hữu hạn có số các phần tử là lũy thừa nguyên của một số nguyên tố p. Trong trường hợp này người ta cũng chứng minh được rằng luôn tồn tại một phần tử nguyên thủy trong trường và các phép toán số học sẽ được thực hiện theo modulo của một đa thức nǎo đó trên GF(p). Trong giáo trình này ta chỉ quan tâm tới trường hợp p = 2, khi đó đa thức được dùng sẽ là một trong các đa thức nhị phân nguyên thủy (chính là các đa thức sinh của mã Hamming).

Giả sử ta cần tạo một trường hữu hạn GF(q) và ký hiệu α là phần tử nguyên thủy của nó. Các lũy thừa của α (từ α^0 đến α^{q-2}) gồm q - 1 phần tử khác không của trường. Phần tử α^{q-1} sẽ bằng phần tử α^0 , còn các phần tử có số mũ cao hơn cũng lặp lại các phần tử có số mũ thấp hơn. Phương pháp nhân rút ra trực tiếp từ phép cộng modulo $(q-1)$ đối với các số mũ của α . Đối với trường GF(2^m) ta có: $\alpha^{(2^m-1)} = 1$ hay $\alpha^{(2^m-1)} + 1 = 0$.

Điều này sẽ thỏa mãn nếu có bất kỳ một nhân thức nào của đa thức này bằng không. Nhân thức mà ta chọn phải là bất khả quy và không là nhân thức của $\alpha^n + 1$ đối với bất kỳ giá trị n nào nhỏ hơn $2^m - 1$, nếu không như vậy các lũy thừa của α sẽ lặp lại trước khi chúng tạo ra tất cả các phần tử khác không của trường (điều này có nghĩa là α không phải là phần tử nguyên thủy của trường). Nhân thức thỏa mãn các tính chất trên chính là đa thức nguyên thủy có bậc m.

Ví dụ: Xét trường GF(2^3). Các nhân thức của $\alpha^7 + 1$ là

$$\alpha^7 + 1 = (\alpha + 1)(\alpha^3 + \alpha + 1)(\alpha^3 + \alpha^2 + 1)$$

Cả hai đa thức bậc 3 ở trên đều là các đa thức nguyên thủy và ta có thể chọn tùy ý. Giả sử ta tạo các lũy thừa của α theo điều kiện $\alpha^3 + \alpha + 1 = 0$. Khi đó các phần tử khác không của trường là:

$$1$$

$$\alpha$$

$$\alpha^2$$

$$\alpha^3 = \alpha + 1$$

$$\alpha^4 = \alpha^2 + \alpha$$

$$\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$$

$$\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$$

Mỗi lũy thừa của α có thể được biểu thị bằng một đa thức nhị phân có bậc nhỏ hơn hoặc bằng 2. Phép nhân các phần tử của trường được thực hiện thông qua phép cộng các số mũ của α theo modulo 7. Phép cộng được thực hiện bằng phép cộng modulo 2 các số hạng trong đa thức.

Ví dụ: $\alpha^3 + \alpha^4 = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1 = \alpha^6$

Cần chú ý rằng mỗi phần tử là phần tử đối (phản tử ngược của phép cộng) của chính nó. Điều này rút ra từ tính chất của phép cộng modulo 2. Còn một vấn đề ta chưa thỏa mãn là α có thể biểu thị bằng số như thế nào. Tuy nhiên điều này không quan trọng và ta có thể gán theo cách mà ta muốn. Ví dụ ta gán giá trị 2 cho α và 3 cho α^2 , khi đó ta đã quyết định rằng trong số học của ta $2 \cdot 2 = 3$. Điều này khác với suy nghĩ thông thường của chúng ta và bởi vậy ta phải coi việc gán các giá trị số là hoàn toàn tùy ý mặc dù có một số cách gán thuận tiện cho sử dụng.

4.11.3. Biểu diễn đa thức cho trường hữu hạn $GF(2^m)$

Ngoài cách biểu diễn số người ta có thể sử dụng biểu diễn đa thức cho các phần tử của trường hữu hạn $GF(q^m)$. Với trường $GF(2^m)$ các hệ số nhị phân của các đa thức được dùng để tạo nên biểu diễn cho các phần tử.

Ví dụ: Xét $GF(2^3)$, biểu diễn cho 8 phần tử của trường này có thể viết như sau:

$$\begin{aligned}
 0 &= 000 \\
 1 &= 001 \\
 \alpha &= 010 \\
 \alpha^2 &= 100 \\
 \alpha^3 &= \alpha + 1 = 011 \\
 \alpha^4 &= \alpha^2 + \alpha = 110 \\
 \alpha^5 &= \alpha^2 + \alpha + 1 = 111 \\
 \alpha^6 &= \alpha^2 + 1 = 101
 \end{aligned}$$

Ở đây dãy 3 bit được dùng để mô tả cho biểu diễn đa thức của các phần tử. Phép cộng được thực hiện bằng cách cộng modulo 2 theo từng bit của dãy

4.11.4. Các tính chất của đa thức và các phần tử của trường hữu hạn

4.11.4.1. Các nghiệm của đa thức

Ta biết rằng các đa thức với các hệ số thực không phải lúc nào cũng có các nhân tử thực, tuy nhiên luôn luôn có thể phân tích chúng dưới dạng các nhân thức phức. Tương tự, một đa thức bất khả quy trên trường hữu hạn luôn có thể phân tích được trong một trường mở rộng nào đó.

Ví dụ: Đa thức nhị phân $X^3 + X + 1$ có thể phân tích được trên GF(8) như sau:

$$X^3 + X + 1 = (X + \alpha)(X + \alpha^2)(X + \alpha^4)$$

Các giá trị $\alpha, \alpha^2, \alpha^4$ được gọi là các nghiệm của $X^3 + X + 1$ vì chúng biểu thị các giá trị của X làm cho đa thức bằng không.

Nếu $f(X)$ là một đa thức bất khả quy q phân thi $f(X)$ sẽ có các nghiệm trong một trường mở rộng $GF(q^m)$ nào đó, tức là $f(X)$ có thể biểu diễn bằng tích của một số hạng có dạng $(x + \beta_i)$ với β_i là phần tử của $GF(q^m)$. Hơn nữa nếu β là một nghiệm nào đó thì có thể thấy rằng các nghiệm khác có dạng $\beta^q, \beta^{q^2}, \beta^{q^3}, \dots$

Tương tự như trường hợp phân tích các đa thức với các hệ số thực ta có thể sử dụng thuật ngữ các phần tử liên hợp cho các nghiệm của một đa thức bất khả quy. Với đa thức nhị phân bất khả quy có nghiệm β thì các nghiệm liên hợp là $\beta^2, \beta^4, \beta^8, \dots$

Sự tồn tại các nghiệm liên hợp của một đa thức tương đương với các tính chất sau:
 $f(X^q) = [f(X)]^q$

Nếu β là một nghiệm của $f(X)$ thì β^d cũng là một nghiệm của $f(X)$. Đa thức $f(X)$ được gọi là đa thức tối thiểu của β . Nếu β là phần tử nguyên thủy thì $f(X)$ là một đa thức nguyên thủy. Như vậy có thể sinh ra một trường hữu hạn từ một phần tử nguyên thủy là một nghiệm của đa thức nguyên thủy.

Ví dụ: Xét trường hữu hạn GF(8) tạo bởi đa thức nguyên thủy $X^3 + X + 1$. Thé $X = \alpha, X = \alpha^2$ hoặc $X = \alpha^4$ vào đa thức này ta thấy nó bằng 0. Bởi vậy $X^3 + X + 1$ là đa thức tối thiểu của các phần tử $\alpha, \alpha^2, \alpha^4$. Tương tự thé α^3, α^6 và $\alpha^{12} (= \alpha^5)$ vào $X^3 + X + 1$ ta thấy rằng chúng là các nghiệm của đa thức này. Đa thức tối thiểu của α^0 là $(X + 1)$.

Nếu m là số nguyên nhỏ nhất để $\beta^m = 1$ thì phần tử β được gọi là có cấp m (ký hiệu $\text{ord}(\beta) = m$) và β phải là nghiệm của $X^m + 1$. Nếu β cũng là nghiệm của một đa thức bất khả quy $f(X)$ nào đó thì $f(X)$ phải là một nhân thức của $X^m + 1$.

Ví dụ: Giá trị nhỏ nhất của m để $(\alpha^3)^m = 1$ là 7. Bởi vậy đa thức $f(X) = X^3 + X^2 + 1$ là một nhân thức của $X^7 + 1$.

4.11.4.2. Các phần tử của trường hữu hạn xen như các nghiệm của một đa thức

Các nghiệm của nhị thức $X^{2^m-1} + 1$ chính là các phần tử khác không của $\text{GF}(2^m)$.

Ví dụ: Ta đã có phân tích của $X^7 + 1$ như sau:

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

Ta cũng biết rằng α là nghiệm của $(X^3 + X + 1)$ và bởi vậy α^2 và α^4 cũng là các nghiệm của nó. α^3 là nghiệm của $(X^3 + X^2 + 1)$ và bởi vậy α^6 và α^5 cũng là các nghiệm của nó. Nghiệm của $(X + 1)$ là 1.

4.11.4.3. Các nghiệm của một đa thức bất khả quy

Đa thức bất khả quy $f(X)$ bậc m sẽ có m nghiệm là $\beta, \beta^2, \beta^4, \dots, \beta^{2^{m-1}}$ và $\beta^{2^m} = \beta$ vì $\beta^{2^m-1} = 1$.

Vì các nghiệm của $X^{2^m-1} + 1$ là tất cả các phân tử khác không của $\text{GF}(2^m)$ nên một đa thức bất khả quy bậc m luôn có các nghiệm trong $\text{GF}(2^m)$. Ngược lại, các nhân thức của $X^{2^m-1} + 1$ chứa tất cả các đa thức bất khả quy bậc m. Như vậy $X^3 + X^2 + 1$ và $X^3 + X + 1$ là toàn bộ các đa thức bất khả quy bậc 3 có thể có.

Chú ý rằng $X^m + 1$ là ước của $X^n + 1$ nếu và chỉ nếu m là ước của n. Điều này cũng có nghĩa là tất cả các đa thức bất khả quy bậc m là nguyên thủy nếu $2^m - 1$ là số nguyên tố.

Ví dụ: 7 là số nguyên tố nên tất cả các đa thức bất khả quy bậc 3 đều là các đa thức nguyên thủy.

15 không là các số nguyên tố nên không phải tất cả các đa thức bất khả quy bậc 4 đều là các đa thức nguyên thủy. Có ba đa thức bất khả quy bậc 4 là $1 + X + X^4$, $1 + X^3 + X^4$ và $1 + X + X^2 + X^3 + X^4$. Chỉ có hai đa thức $1 + X + X^4$ và $1 + X^3 + X^4$ là các đa thức nguyên thủy.

4.11.4.4. Phân tích một đa thức nhị phân $f(X)$

Để phân tích một đa thức nhị phân ta phải xây dựng được trường hữu hạn mà trên nó có thể tìm được các nhân thức của đa thức này. Muốn vậy, trước tiên ta phải tìm các nhân thức bất khả quy nhị phân của đa thức $f(X)$ này (nếu có) và các bậc của chúng. Sau đó ta tìm bội chung nhỏ nhất (BCNN) c' của các bậc này. Các nhân thức của $f(X)$ sẽ được tìm trong $\text{GF}(2^{c'})$. Cần để ý rằng:

$$2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1) \left[(2^a)^{b-1} + (2^a)^{b-2} + (2^a)^{b-3} + \dots + 1 \right]$$

Bởi vậy $2^{c'} - 1$ là bội của $2^c - 1$ nếu c' là bội của c. Bằng cách chọn c' là bội của bậc c của một nhân thức bất khả quy nhị phân nào đó, khi đó các nghiệm của nó sẽ nằm trong $\text{GF}(2^c)$ và cũng nằm trong $\text{GF}(2^{c'})$.

Nếu c' là bội của các bậc của mọi đa thức bất khả quy nhị phân thì tất cả các nghiệm của chúng có thể biểu diễn được trong $\text{GF}(2^{c'})$.

Ví dụ: Đa thức $f(X) = X^5 + X^4 + 1$ được phân tích thành tích của hai đa thức bất khả quy sau:

$$X^5 + X^4 + 1 = (X^3 + X + 1)(X^2 + X + 1)$$

$$\text{Ta có } \deg(X^3 + X + 1) = 3, \deg(X^2 + X + 1) = 2$$

$$\text{BCNN}(3,2) = 6$$

Như vậy $f(X)$ có thể phân tích được thành tích của các đa thức bậc nhất trong $\text{GF}(2^6)$.

4.11.5. Xác định các mã bằng các nghiệm

Ta có thể xác định một bộ mã bằng cách cho rằng các từ mã là các đa thức nhị phân có các nghiệm xác định trong $\text{GF}(2^m)$. Chẳng hạn nếu nghiệm là α trong $\text{GF}(8)$ thì đa thức tối thiểu của nó là $X^3 + X + 1$ và tất cả các từ mã phải chia hết được cho đa thức này. Trong trường hợp này, đa thức tối thiểu đóng vai trò như đa thức sinh của mã.

Một cách tổng quát ta có thể coi đa thức sinh là BCNN của các đa thức tối thiểu của các nghiệm được xác định. Bậc của đa thức (chính là số dấu kiểm tra của mã) là số các nghiệm phân biệt sao cho tổng số các nghiệm là số dấu kiểm tra.

Nếu đa thức mã $v(X)$ có một nghiệm β thì $v(\beta) = 0$.

Cho v_n là hệ số của X^n , khi đó:

$$v_{n-1}\beta^{n-1} + \dots + v_2\beta^2 + v_1\beta + v_0\beta^0 = 0$$

Ở dạng vectơ ta có thể viết như sau:

$$v \begin{bmatrix} \beta^{n-1} \\ \vdots \\ \beta^2 \\ \beta^1 \\ \beta^0 \end{bmatrix} = 0$$

Tương tự, nếu $v(X)$ có j nghiệm từ β_1 đến β_j thì :

$$v \begin{bmatrix} \beta_1^{n-1} & \beta_2^{n-1} & \dots & \beta_j^{n-1} \\ \vdots & \vdots & & \vdots \\ \beta_1^2 & \beta_2^2 & \dots & \beta_j^2 \\ \beta_1^1 & \beta_2^1 & \dots & \beta_j^1 \\ \beta_1^0 & \beta_2^0 & \dots & \beta_j^0 \end{bmatrix} = 0$$

Ta biết rằng: $v \cdot H^T = 0$

Như vậy ma trận chuyên vị của ma trận ở trên chính là ma trận kiểm tra của mã. Các nghiệm đều là các đa thức của α (ta cũng xem như là các vectơ và chúng cũng phải được chuyên vị), bởi vậy ta có thể viết:

$$H = \begin{bmatrix} \beta_1^{n-1^T} & \dots & \beta_1^{1^T} & \beta_1^{0^T} \\ \beta_2^{n-1^T} & \dots & \beta_2^{1^T} & \beta_2^{0^T} \\ \vdots & \dots & \vdots & \vdots \\ \beta_j^{n-1^T} & \dots & \beta_j^{1^T} & \beta_j^{0^T} \end{bmatrix}$$

Ta thấy rằng chỉ cần một trong các nghiệm $\beta, \beta^2, \beta^4, \beta^8, \dots$ nằm trong ma trận kiểm tra là đủ.

4.11.6. Mã Hamming

Mã Hamming có đa thức sinh là đa thức nguyên thủy. Bởi vậy một phần tử nguyên thủy bất kỳ đều được xem là nghiệm của mã, nếu ta lấy phần tử α làm nghiệm thì:

$$H = \begin{bmatrix} \alpha^{n-1^T} & \dots & \alpha^{1^T} & \alpha^{0^T} \end{bmatrix}$$

Ta biết rằng các lũy thừa của α là tất cả các phần tử khác không của trường, điều này có nghĩa là ma trận kiểm tra H chứa mọi tổ hợp 0 và 1 có thể có.

Ví dụ: Xét mã Hamming trên $GF(8)$ có $\alpha^3 + \alpha + 1 = 0$, ma trận kiểm tra H của mã này có dạng:

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

Ma trận này chứa tất cả các vectơ cột 3 bit có thể có. Đây chính là ma trận kiểm tra của mã cyclic $(7, 4)$.

4.11.7. Mã BCH

Vào năm 1959, Bose, Ray – Chaudhuri và Hocquenghem là những người đầu tiên đưa ra lớp mã quan trọng này.

Định nghĩa: Mã BCH sửa sai là mã cyclic có 2t nghiệm liên tiếp trong $GF(q^m)$ và có độ dài là $q^m - 1$.

Sau đây là các bước để xác định một mã BCH trên $GF(q)$ có độ dài n và có khả năng sửa t sai:

1. Xác định số nguyên nhỏ nhất m sao cho $GF(q^m)$ có phần tử nguyên thủy β .

2. Chọn một số nguyên tố không âm b . Thông thường $b = 1$

3. Liệt kê ra 2t lũy thừa liên tiếp của β

$$\beta^b, \beta^{b+1}, \dots, \beta^{b+2t-1}$$

Xác định các đa thức tối thiểu trên $GF(q)$ của các phần tử này (cần chú ý rằng các phần tử liên hợp có cùng một đa thức tối thiểu)

4. Đa thức sinh $g(X)$ là BCNN của đa thức tối thiểu này. mã tạo được chính là mã cyclic (n, k) với $k = n - \deg g(X)$.

Định nghĩa: Nếu $b = 1$ thì mã BCH được gọi là mã BCH nguyên thủy. Nếu $n = q^m - 1$ thì mã BCH được gọi là mã BCH tự nhiên.

Ví dụ: Mã BCH nhị phân sửa sai đơn có độ dài $2^m - 1$ là mã có hai nghiệm liên tiếp trong $GF(2^m)$. Nếu ta chọn các nghiệm này là α và α^2 thì nghiệm thứ hai (α^2) là hiên nhiên có. Bởi vậy đây chính là mã Hamming.

Mã BCH nhị phân sửa hai sai phải có các nghiệm liên tiếp là $\alpha, \alpha^2, \alpha^3$ và α^4 . Hiên nhiên là chỉ có α và α^3 là các nghiệm độc lập (α^2 và α^4 là các phần tử liên hợp của α). Bởi vậy ta cần kiểm tra của mã này có dạng sau:

$$H = \begin{bmatrix} \alpha^{n-1^T} & \cdots & \alpha^{2^T} & \alpha^{1^T} & \alpha^{0^T} \\ \alpha^{3(n-1)^T} & \cdots & \alpha^{3,2^T} & \alpha^{3,1^T} & \alpha^{3,0^T} \end{bmatrix}$$

Các mã BCH cho phép sử dụng phương pháp giải mã đại số. Xét trường hợp $n = 15$ và có hai sai ở các vị trí i và j . Ta có syndrom sau: $s = e \cdot H^T$

Syndrom có hai thành phần s_1 và s_3 :

$$s_1 = \alpha^j + \alpha^i$$

$$s_3 = \alpha^{3j} + \alpha^{3i}$$

Thế $\alpha^j = s_1 + \alpha^i$ từ phương trình thứ nhất vào phương trình thứ hai ta có:

$$s_1^2 \alpha^i + s_1 \alpha^{2i} + s_1^3 + s_3 = 0$$

α^i chính là nghiệm của phương trình này. Vì các giá trị i và j là tùy ý nên cả hai vị trí sai có thể tìm được từ phương trình trên

Ví dụ: Mã BCH sửa 2 sai có độ dài 15 có các nghiệm α và α^3 trên GF(16) sử dụng đa thức nguyên thủy $X^4 + X + 1$. Các phần tử α^i của trường được biểu diễn bằng các đa thức có dạng sau:

$$\begin{array}{ll} \alpha^0 = 0\ 0\ 0\ 1 & \alpha^8 = 0\ 1\ 0\ 1 \\ \alpha^1 = 0\ 0\ 1\ 0 & \alpha^9 = 1\ 0\ 1\ 0 \\ \alpha^2 = 0\ 1\ 0\ 0 & \alpha^{10} = 0\ 1\ 1\ 1 \\ \alpha^3 = 1\ 0\ 0\ 0 & \alpha^{11} = 1\ 1\ 1\ 0 \\ \alpha^4 = 0\ 0\ 1\ 1 & \alpha^{12} = 1\ 1\ 1\ 1 \\ \alpha^5 = 0\ 1\ 1\ 0 & \alpha^{13} = 1\ 1\ 0\ 1 \\ \alpha^6 = 1\ 1\ 0\ 0 & \alpha^{14} = 1\ 0\ 0\ 1 \\ \alpha^7 = 1\ 0\ 1\ 1 \end{array}$$

Khi đó ma trận kiểm tra có dạng sau:

$$H = \begin{bmatrix} \alpha^{14^T} & \alpha^{13^T} & \dots & \alpha^{2^T} & \alpha^{1^T} & \alpha^{0^T} \\ \alpha^{12^T} & \alpha^{9^T} & \dots & \alpha^{6^T} & \alpha^{3^T} & \alpha^{0^T} \end{bmatrix}$$

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

Giả sử từ mã nhận được là :

$$v(X) = x^6 + x^4 + 1 \leftrightarrow 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1$$

Syndrom tương ứng là 1 1 1 0 0 1 1 0

Hay $s_1 = \alpha^{11}$, $s_3 = \alpha^5$ ($\alpha^{11} = 1\ 1\ 1\ 0$, $\alpha^5 = 0\ 1\ 1\ 0$)

Ta có phương trình sau: $\alpha^{7+i} + \alpha^{11+2i} + \alpha^3 + \alpha^5 = 0$

Với $i = 7$ ta có:

$$\alpha^{14} + \alpha^{10} + \alpha^3 + \alpha^5 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Với $i = 8$ ta có:

$$\alpha^0 + \alpha^{12} + \alpha^3 + \alpha^5 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 0$$

Như vậy sai nằm ở vị trí 7 và 8, từ mã đã phát $f(X)$ là:

$$f(X) = X^8 + X^7 + X^6 + X^4 + 1 \leftrightarrow 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1$$

Ta có thể kiểm tra lại kết quả giải mã trên theo một cách khác. Biết rằng các nghiệm α và α^3 có các đa thức tối thiểu tương ứng là $X^4 + X + 1$ và $X^4 + X^3 + X^2 + X + 1$. đa thức sinh của mã cyclic này là tích của hai đa thức tối thiểu trên $g(X) = X^8 + X^7 + X^6 + X^4 + 1$. Bởi vậy đây là mã cyclic (15, 7) và từ mã nhận được ở trên phải chia hết cho $g(X)$.

4.11.8. Các mã Reed –Solomon (RS)

Định nghĩa: Mã RS là mã BCH q phân có độ dài $q^m - 1$.

Trong $GF(q^m)$ đa thức tối thiểu của một phần tử β đơn giản chỉ là $(x - \beta)$. Bởi vậy đa thức sinh của mã RS có dạng:

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \dots (x - \alpha^{b+2t-1})$$

trong đó α là phần tử nguyên thủy của trường. Bậc của $g(x)$ bằng $2t$, như vậy với mã RS $n - k = 2t$, khoảng cách của mã RS: $d_0 = n - k + 1$

Ví dụ: Cho $n = 7$. Giả sử α là nghiệm của đa thức nguyên thủy $x^3 + x + 1$. Bởi lũy thừa liên tiếp của α là $\alpha^1, \alpha^2, \alpha^3, \alpha^4$. Như vậy đa thức sinh của mã RS sáu 2 sai là:

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$$

Cần chú ý rằng các hệ số của $g(x)$ nằm trong GF(8)

Mã RS tương ứng là mã (7, 3) có 8^3 từ mã.

Ngoài các mã tần thường là mã kiêm tra chẵn $(n, n-1)$ và mã lặp $(n, 1)$, mã RS cũng là một mã thỏa mãn giới hạn Singleton sau: $d_0 \leq n - k + 1$

4.12. CÁC MÃ CHẬP

4.12.1. Mô tả và một số khái niệm cơ bản.

Mã chập là mã tuyến tính có ma trận sinh có cấu trúc sao cho phép mã hóa có thể xem như một phép lọc (hoặc lấy tổng chập). Mã chập được sử dụng rộng rãi trong thực tế. Bởi mã hóa được xem như một tập hợp các bộ lọc số tuyến tính với dây mã là các đầu ra của bộ lọc được phép xen kẽ. Các mã chập là các mã đầu tiên được xây dựng các thuật toán giải mã quyết định phần mềm hiệu quả

Ví dụ: Mã khởi từ các khối k đầu tạo ra các khối n đầu. Với các mã chập (thường được xem là các mã dòng), bộ mã hóa hoạt động trên dòng liên tục các đầu vào không được phân thành các khối tin rời rạc. Tuy nhiên tốc độ mã $\frac{k}{n}$ được hiểu là việc đưa vào k đầu ở mỗi bước thời gian sẽ tạo ra n đầu mới. Số học có thể được thực hiện trên một trường tùy ý nhưng thông thường vẫn là trên GF(2).

Ta biểu thị các dây và các hàm truyền đạt như các chuỗi lũy thừa của biến x (đôi khi còn dùng ký hiệu D thay cho x). Dây $\{..., m_{-2}, m_{-1}, m_0, m_1, m_2, ...\}$ (với các phần tử m_i thuộc trường F) được xem như một chuỗi Laurent:

$$m(x) = \sum_{e=-\infty}^{\infty} m_e x^e$$

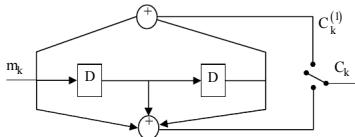
Tập tất cả các chuỗi Laurent trên F là một trường, ta ký hiệu trường này là $F[[x]]$. Như vậy $m(x) \in F[[x]]$.

Đối với dòng nhiều đầu vào ta dùng ký hiệu $m^{(1)}(x)$ biểu thị dòng đầu vào đầu tiên, $m^{(2)}(x)$ biểu thị dòng đầu vào thứ hai... Tập các dòng vào xem như một vector:

$$m(x) = [m^{(1)}(x) \ m^{(2)}(x)] \in F[[x]]^2$$

Bộ mã hóa cho mã chập thường được coi là một tập các bộ lọc số.

Ví dụ: Hình 4.2 chỉ ra một ví dụ về một bộ mã hóa

**Hình 4.2:** Bộ mã hóa cho mã chập tốc độ $R = \frac{1}{2}$

(các ô D biểu thị các ô nhớ một bit – các trigo D)

Dòng vào m_k đi qua hai bộ lọc dùng chung các phần tử nhớ tạo ra hai dòng ra:

$$C_k^{(1)} = m_k + m_{k-2} \text{ và } C_k^{(2)} = m_k + m_{k-1} + m_{k-2}$$

Hai dòng ra này được đưa ra xen kẽ để tạo ra dòng được mã C_k . Như vậy cứ mỗi bit vào lại có hai bit mã được đưa ra, kết quả là ta có một mã có tốc độ $R = \frac{1}{2}$.

Thông thường ta coi trạng thái ban đầu của các phần tử nhớ là 0, Như vậy, với dòng vào $m = \{1, 1, 0, 0, 1, 0, 1\}$ các đầu ra sẽ là:

$$C^{(1)} = \{1, 1, 1, 1, 0, 0, 0, 1\} \text{ và } C^{(2)} = \{1, 0, 0, 1, 1, 1, 0, 1\}$$

Đòng ra: $C = \{11, 10, 10, 11, 11, 01, 00, 01, 11\}$

Ở đây đầu phẩy phân cách các cặp bit ra ứng với mỗi bit vào.

Ta có thể biểu thị hàm truyền từ đầu vào $m(x)$ từ đầu ra $C^{(1)}(x)$ như sau:

$$g^{(1)}(x) = 1 + x^2. \text{ Tương tự ta có } g^{(2)}(x) = 1 + x + x^2$$

Đòng vào $m = \{1, 1, 0, 0, 1, 0, 1\}$ có thể biểu thị như sau:

$$m(x) = 1 + x + x^4 + x^6 \in GF(2)[[x]]$$

Các đầu ra sẽ là:

$$C^{(1)}(x) = m(x)g_1(x) = (1 + x + x^4 + x^6)(1 + x^2) = 1 + x + x^2 + x^3 + x^4 + x^8$$

$$C^{(2)}(x) = m(x)g_2(x) = (1 + x + x^4 + x^6)(1 + x + x^2)$$

$$= 1 + x^3 + x^4 + x^5 + x^7 + x^8$$

Với mỗi mảng bộ tốc độ $R = \frac{k}{n}$ có một hàm truyền ma trận $k \times n \in \mathbb{X}$ (còn được gọi là ma trận truyền). Với mảng tốc độ $R = \frac{1}{2}$ ở ví dụ trên ta có:

$$G_a(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$$

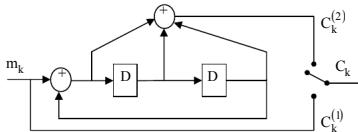
Ma trận truyền này không chỉ có dạng các đa thức, ta có thể thấy thông qua ví dụ sau:

Ví dụ: Xét ma trận truyền của mảng sau:

$$G_b(x) = \begin{bmatrix} 1 & \frac{1+x+x^2}{1+x^2} \end{bmatrix}$$

Vì có "1" ở cột đầu tiên nên đóng vào sẽ xuất hiện trực tiếp ở đầu ra đan xen, bởi vậy đây là một mảng bộ hệ thống

Bộ mã hóa cho mảng này được mô tả ở hình 3:



Hình 4.3: Bộ mã hóa hệ thống với $R = \frac{1}{2}$

Với dòng vào: $m(x) = 1 + x + x^2 + x^3 + x^4 + x^8$ các đầu ra $C_k^{(1)}$ và $C_k^{(2)}$ có dạng:

$$\begin{aligned} C_k^{(1)} &= m(x) = 1 + x + x^2 + x^3 + x^4 + x^8 \\ C_k^{(2)} &= \frac{(1+x+x^2+x^3+x^4+x^8)(1+x+x^2)}{1+x^2} \\ &= 1 + x^3 + x^4 + x^5 + x^7 + x^8 + x^{10} + \dots \end{aligned}$$

Một bộ mã hóa chỉ có các hàng đa thức trong ma trận truyền được gọi là bộ mã hóa có đáp ứng xung hữu hạn. Một bộ mã hóa có các hàm hữu tỷ trong ma trận truyền gọi là bộ mã hóa có đáp ứng xung vô hạn.

Với mảng có tốc độ k/n với $k > 1$ dãy thông báo đầu vào (ta coi như được tách ra từ một dãy thông báo thành k dãy), ta có:

$$m(x) = [m^{(1)}(x), m^{(2)}(x), \dots, m^{(k)}(x)]$$

và:

$$G(x) = \begin{bmatrix} g^{(1,1)}(x) & g^{(1,2)}(x) & \dots & g^{(1,n)}(x) \\ g^{(2,1)}(x) & g^{(2,2)}(x) & \dots & g^{(2,n)}(x) \\ \vdots & \vdots & \ddots & \\ g^{(k,1)}(x) & g^{(k,2)}(x) & \dots & g^{(k,n)}(x) \end{bmatrix}$$

Dãy ra được biểu thị như sau:

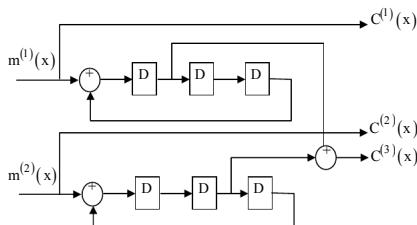
$$C(x) = [C^{(1)}(x), C^{(2)}(x), \dots, C^{(n)}(x)] = m(x)G(x)$$

Má trận truyền $G(x)$ được gọi là hệ thống nếu có thể xác định được một ma trận đơn vị trong các phần tử của $G(x)$ (chẳng hạn nếu bằng các phép hoán vị hàng và/hoặc cột của $G(x)$ có thể thu được một ma trận đơn vị).

Ví dụ: Cho mã hệ thống tốc độ $R = 2/3$ có ma trận truyền sau:

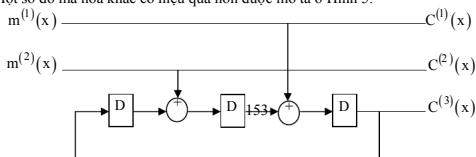
$$G(x) = \begin{bmatrix} 1 & 0 & \frac{x}{1+x^3} \\ 0 & 1 & \frac{x^2}{1+x^3} \end{bmatrix}$$

So đồ thể hiện của mã này cho trên Hình 4:



Hình 4.4: Bộ mã hóa hệ thống $R = \frac{2}{3}$

Một sơ đồ mã hóa khác có hiệu quả hơn được mô tả ở Hình 5:



Hình 4.5: Sơ đồ bộ mã hóa hệ thống $R = \frac{2}{3}$ có phần cứng đơn giản hơn

$$\text{Giả sử: } m(x) = [1 + x^2 + x^4 + x^5 + x^7 + \dots, x^2 + x^5 + x^6 + x^7 + \dots]$$

Khi đó đầu ra $C(x)$ có dạng:

$$C(x) = [1 + x^2 + x^4 + x^5 + x^7 + \dots, x^2 + x^5 + x^6 + x^7 + \dots, x + x^3 + x^5 + \dots]$$

Khi đưa ra xen kẽ dòng ra sẽ là:

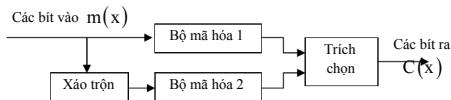
$$\{100, 001, 110, 001, 100, 111, 010, 110\}$$

Từ các ví dụ trên ta có định nghĩa sai cho mã chập

Định nghĩa: Mã chập tốc độ $R = k/n$ trên trường các chuỗi Laurent hữu tỷ $F[[x]]$ trên trường F là ánh của một ánh xạ tuyến tính đơn ánh của các chuỗi Laurent k chiều $m(x) \in F[[x]]^k$ vào các chuỗi Laurent $C(x) \in F[[x]]^n$.

4.12.2. Các mã Turbo.

Vào năm 1993, Berrou, Glavieux và Thitimajashima đã đưa ra một sơ đồ mã hóa mới cho các mã chập được gọi là mã Turbo (Hình 6). Trong sơ đồ này dòng thông tin vào được mã hóa hai lần với một bộ xáo trộn đặt giữa hai bộ mã hóa nhằm tạo ra hai dòng dữ liệu được mã hóa có thể xem là độc lập thống kê với nhau.



Hình 4.6: Bộ mã hóa Turbo

Trong sơ đồ này các bộ mã hóa thường được sử dụng là các bộ mã hóa cho mã chập có tốc độ $R = 1/2$.

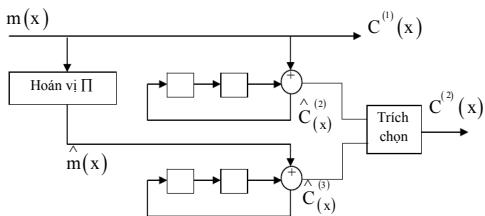
Các mã này được sử dụng rất hiệu quả trên các kênh phadinh. Người ta đã chứng tỏ rằng hiệu năng của mã Turbo sẽ tăng khi tăng kích thước của bộ xáo trộn. Tuy nhiên trong nhiều ứng dụng quan trọng (chẳng hạn khi truyền tiếng nói), kích thước bộ xáo trộn quá lớn không sử dụng được do kết quả giải mã bị giữ chậm

Ví dụ: Xét sơ đồ mã hóa Turbo có hàm truyền sau: (Hình 4.7)

$$G(x) = \frac{1}{1+x^2}$$

với bộ xáo trộn được mô tả bởi phép hoán vị Π

$$\Pi = \{8, 3, 7, 6, 9, 0, 2, 5, 1, 4\}$$



Hình 4.7:

$$\text{Giả sử dây vào là: } m(x) = [1, 1, 0, 0, 1, 0, 1, 0, 1, 1] = C^{(1)}(x)$$

Khi đó dây ra của bộ mã hóa thứ nhất là:

$$\hat{C}^{(1)}(x) = [1, 1, 1, 1, 0, 1, 1, 1, 0, 0]$$

Dãy bit được hoán vị đưa vào bộ mã hóa thứ hai là:

$$\hat{m}(x) = [1, 0, 0, 1, 1, 1, 0, 0, 1, 1]$$

Dãy ra của bộ mã hóa thứ hai là:

$$\hat{C}^{(2)}(x) = [1, 0, 1, 1, 0, 0, 0, 0, 1, 1]$$

Bộ trích chọn sẽ chọn đưa ra các bit được gạch dưới lần lượt ở các đầu $\hat{C}^{(2)}(x)$ và

$$\hat{C}^{(3)}(x)$$

Dãy bit được mã hóa ở đầu ra có giá trị $R = \frac{1}{2}$ là:

$$v(x) = [1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1]$$

Khi không dùng bộ trích chọn dãy bit ra sẽ có tốc độ $R = \frac{1}{3}$ và có dạng

$$v(x) = [1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1]$$

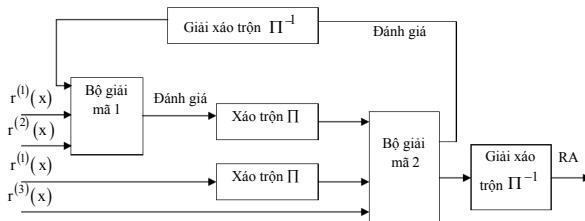
Đây ra $v(x)$ được điều chỉnh và phái qua kênh, ở đầu ra kênh tín hiệu nhận được giải điều chỉnh để tạo ra vectơ $r(x)$ bao gồm các vectơ $r^{(1)}(x)$ (tương ứng với $C^{(1)}(x)$), $r^{(2)}(x)$ (tương ứng với $\hat{C}^{(2)}(x)$) và $r^{(3)}(x)$ (tương ứng với $\hat{C}^{(3)}(x)$).

Hoạt động chung của thuật toán giải mã Turbo có thể mô tả như sau (xem hình 4.8).

Dữ liệu $(r^{(1)}(x), r^{(2)}(x))$ được đưa tới bộ giải mã 1. Trước tiên bộ giải mã này sử dụng dữ liệu thông tin tiên nghiệm trên các bit đã phát và tạo ra các bit có xác suất xuất hiện phụ thuộc vào dữ liệu quan sát được. Đầu ra đánh giá này của bộ giải mã 1 được xáo trộn theo luật hoán vị Π và được đưa tới bộ giải mã 2 và được làm thông tin tiên nghiệm. Cùng đưa tới bộ giải mã 2 là dữ liệu nhận được $(r^{(1)}(x), r^{(3)}(x))$, cần chú ý rằng $r^{(1)}(x)$ phải được đưa tới bộ

xáo trộn Π . Đầu ra đánh giá của bộ giải mã 2 được giải xáo trộn bằng luật hoán vị ngược Π^{-1} và được đưa trở lại làm thông tin tiên nghiệm cho bộ giải mã 1. Quá trình chuyển thông tin tiên nghiệm sẽ được tiếp tục cho đến khi bộ giải mã quyết định rằng quá trình đã hội tụ (hoặc cho tới khi đạt được một số lần lặp nhất định).

Phản quan trọng nhất của thuật toán giải mã này là một thuật toán giải mã quyết định mềm, thuật toán này sẽ cung cấp các đánh giá của các xác suất hiệu nghiệm cho mỗi bit vào



Hình 4.8: Sơ đồ khái niệm của bộ giải mã Turbo

BÀI TẬP

- 4.1. Hãy thiết lập các tử mã hệ thống cho mã cyclic $(7,3) = \langle 1 + x + x^2 + x^4 \rangle$ với các đa thức thông tin sau: $a_1(x) = 1 + x$

$$a_2(x) = 1 + x^2$$

4.2. Giả sử từ mã nhận được của mã cyclic $(7, 3)$ có $g(x) = 1 + x + x^2 + x^4$ có dạng

$$v(x) = x^6 + x^5 + x^4 + x^2 + x \leftrightarrow \begin{matrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ x^0 & . & . & . & . & . & x^6 \end{matrix}$$

Hãy sử dụng thuật toán chia dịch vòng để tìm được từ mã đã phát biết rằng mã $(7, 3)$ này có $d_0 = 4$.

4.3. Hãy lập bốn từ mã của mã hệ thống nhị phân $(8,4)$ biết rằng các dấu tin tức của mỗi từ mã là:

a. 1 1 0 0

b. 0 1 0 1

c. 1 0 1 0

và ma trận kiểm tra của bộ mã là: $H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

4.4. Hãy lập mã Huffman cho nguồn tin sản ra các chữ độc lập x_1, x_2, x_3, x_4 với các xác suất tương ứng $p(x_1) = 0,1; p(x_2) = 0,6; p(x_3) = 0,25; p(x_4) = 0,05$. Tính độ dài trung bình của từ mã. Tính entropie của nguồn.

4.5. Một mã đơn giản n dấu dùng trong kênh nhị phân không đổi xứng với xác suất thu sai dấu “0” là $p_0 = p(0 \rightarrow 1)$ khác xác suất thu sai dấu “1” là $p_1 = p(1 \rightarrow 0)$. Các lỗi xảy ra độc lập với nhau. Hãy tìm xác suất giải đúng mã. Xác suất này có như nhau đối với mọi từ mã không?

4.6. Cho bộ mã hệ thống nhị phân $(8,4)$, các dấu $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ là các dấu mang tin, các dấu $\alpha_5, \alpha_6, \alpha_7, \alpha_8$ là các dấu kiểm tra, được xác định như sau:

$$\begin{cases} \alpha_5 = \alpha_1 + \alpha_2 + \alpha_3 \\ \alpha_6 = \alpha_2 + \alpha_3 + \alpha_4 \\ \alpha_7 = \alpha_1 + \alpha_2 + \alpha_4 \\ \alpha_8 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \end{cases} \quad (a)$$

Chứng minh rằng khoảng cách cực tiểu của mã trong bộ mã này bằng $d_{\min} = 3$.

4.7. Xét mã $(7,4)$ có $d = 3$. Mã này sửa được một sai. Tính xác suất thu đúng một từ mã khi xác suất thu sai một dấu mã bằng p_0

4.8. Mã hệ thống $(3,1)$ có hai từ mã 000 và 111. Tính xác suất sai tương đương khi dùng mã này trong kênh đổi xứng có lỗi xảy ra với xác suất thu sai một dấu là p độc lập với nhau.

4.9. Số các tổ hợp mã của một bộ mã là $N_0 = m^n$. Trong đó số các từ mã đơn dùng là $N < N_0$ (số các từ mã còn lại gọi là các từ mã giả). Khi một từ mã dùng biến thành một từ mã giả nào đó thì ta bài việc truyền tin gấp lõi và như vậy lõi tự động được phát hiện. Hãy tính số lượng các từ mã sai có thể có mà chúng được phát hiện tự động và số tối đa các từ mã có thể sửa chữa bộ mã này. Áp dụng bảng số với $m = 2, n = 4, N = 8$.

4.10. Cho :

$$X^{15} + 1 = (X+1)(X^2 + X + 1)(X^4 + X^3 + 1)(X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1)$$

a. Hãy tìm tất cả các mã xyclic có thể có trên vánh $Z_2[x]/X^{15} + 1$

b. Hãy tìm đa thức sinh của mã BCH sửa 3 sai.

4.11. Hãy thực hiện bài tập 4.4 theo thuật toán Shannon – Fano sau:

Bước 1: Chia tập tin thành hai nhóm có tổng xác suất xấp xỉ nhau

Bước 2: Ghi "0" vào các tin của một nhóm

Ghi "1" vào các tin của nhóm còn lại

Bước 3: Với mỗi nhóm lại thực hiện các bước trên. Thuật toán dừng khi mỗi phần tử chỉ còn chứa một tin

4.12. Với mã BCH sửa 2 sai được mô tả trong ví dụ ở mục 4.10.7 hãy giải mã cho dãy sau: 1 0 0 0 1 0 1 0 0 1 0 0 0 1

4.13. Hãy giải các bài tập 3.8 và 3.14 bằng cách mã hóa nhị phân.

4.14. Cho $X^9 + 1 = (X+1)(1+X+X^2)(1+X^3+X^6)$. Hãy thiết lập tất cả các mã xyclic có thể có trên vánh $Z_2[x]/X^9 + 1$.

4.15. Hãy thực hiện mã hóa Huffman cho nguồn rời rạc sau:

$$A = \left(\begin{array}{cccccccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{32} & \frac{1}{32} & \frac{1}{32} & \frac{1}{64} & \frac{1}{64} \end{array} \right)$$

Dánh giá hiệu quả của phép mã hóa

Hãy giải mã cho dãy các bit nhận được sau: 1 0 1 1 0 0 1 1 1 0 1 0 1 ...

4.16. Hãy thiết lập tử mã hệ thống của bộ mã xyclic (7,4) có đa thức sinh $g(X) = X^3 + X^2 + 1$ tương ứng với đa thức thông tin $a(X) = X^3 + X$ theo thuật toán nhân và theo thuật toán chia.

4.17. Cho mã xyclic $(15, 11)$ có đa thức sinh $g(X) = X^4 + X + 1$. Hãy mô tả sơ đồ chức năng của thiết bị mã hóa hệ thống theo phương pháp chia đa thức cho bộ mã này. Tìm từ mã ra của thiết bị trong trường hợp đa thức thông tin đầu vào có dạng: $a(x) = x^{10} + x^9 + x^7$

CHƯƠNG V – LÝ THUYẾT THU TỐI ƯU

5.1. ĐẶT BÀI TOÁN VÀ CÁC VẤN ĐỀ CƠ BẢN

5.1.1. Thu tín hiệu khi có nhiễu là một bài toán thống kê

Ta xét trường hợp đơn giản nhất khi dạng của tín hiệu trong kênh không bị méo và chỉ bị nhiễu cộng tính. Khi đó ở đầu vào của máy thu sẽ có tổng của tín hiệu và nhiễu:

$$u(t) = \mu S_i(t - \tau) + n(t) \quad (5.1)$$

Trong đó μ - hệ số truyền của kênh (thông thường $\mu \ll 1$)

Giả thiết $\mu = \text{const.}$

τ - thời gian giữ chậm tín hiệu của kênh

$n(t)$ - nhiễu cộng, là một hàm ngẫu nhiên

Trường dấu lỗi vào $\{\alpha_i\} \quad i = \overline{1, m}$, khi đó các $S_i(t)$ là các tín hiệu phát tương ứng với các tin α_i .

Do $n(t)$ là một QTNN nên $u(t)$ cũng là một QTNN. Vậy khi nhận được $u(t)$ ta có thể đề ra m giả thiết sau:

1. $S_i(t)(\alpha_i)$ đã được gửi đi và trong quá trình truyền $S_i(t)$ được cộng thêm một nhiễu: $n(t) = u(t) - \mu S_i(t - \tau)$

2. $S_2(t)(\alpha_2)$ đã được truyền đi và trong quá trình truyền $S_2(t)$ được cộng thêm một nhiễu: $n(t) = u(t) - \mu S_2(t - \tau)$

.....

m. $S_m(t)(\alpha_m)$ đã được truyền đi và trong quá trình truyền $S_m(t)$ được cộng thêm một nhiễu: $n(t) = u(t) - \mu S_m(t - \tau)$

Nhiệm vụ của bộ thu là phải chọn một trong m giả thuyết này trong khi nó chỉ biết một số tính chất của nguồn tín hiệu và dạng của tín hiệu nhận được $u(t)$. Rõ ràng là mỗi một giả thuyết đều có một xác suất sai tương ứng vì $n(t)$ là một hàm ngẫu nhiên. Như vậy máy thu phải chọn một lời giải nào đó trong điều kiện bất định. Việc xét các quy luật chọn lời giải trong điều kiện bất định chính là nội dung của bài toán thống kê. Vì vậy thu tín hiệu khi có nhiễu là một bài toán thống kê.

5.1.2. Máy thu tối ưu

Nhiệm vụ của máy thu là phải chọn lời giải do đó máy thu còn được gọi là sô đồ giải. Yêu cầu lớn nhất của sô đồ giải là phải cho ra lời giải đúng (phát α_i ta phải tìm được β_i). Trong thực tế có rất nhiều sô đồ giải. Trong tất cả các sô đồ giải có thể có thi tại một sô đồ bảo đảm xác suất nhận lớn phải đúng là lớn nhất (xác suất giải sai là bé nhất). Sô đồ này được gọi là sô đồ giải tối ưu. Máy thu xây dựng theo sô đồ giải đó được gọi là máy thu tối ưu (hay lý tưởng)

5.1.3. Thể chổng nhiễu

Có thể dùng xác suất thu đúng để đánh giá độ chính xác của một hệ thống truyền tin một cách định lượng. Để đánh giá ảnh hưởng của nhiễu lên độ chính xác của việc thu, người ta đưa ra khái niệm tính chống nhiễu của máy thu. Nếu cùng một mức nhiễu, máy thu nào đó có xác suất thu đúng là lớn thì được coi là có tính chống nhiễu lớn. Hiển nhiên rằng tính chống nhiễu của máy thu tối ưu là lớn nhất và được gọi là thể chổng nhiễu.

5.1.4. Hai loại sai lầm khi chọn giả thuyết

a. *Sai lầm loại 1:* Gọi H_1 là giả thuyết về tin α_1 đã gửi đi. Nội dung của sai lầm này là bác bỏ H_1 mà thực tế là nó đúng. Tức là quả thật α_1 gửi đi mà ta không gửi. Sai lầm 1 là bỏ sót tin (hay mù tiêu).

b. *Sai lầm loại 2:* Thừa nhận H_1 trong khi thực tế nó sai. Tức là thực ra không có α_1 mà ta lại báo là có. Sai lầm loại này gọi là nhầm tin hoặc báo động nhầm.

Bình thường, không có điều kiện gì đặc biệt, sự tồn tại của hai loại sai lầm trên là không "ngang quyền" (không gây tác hại như nhau)

5.1.5. Tiêu chuẩn Kachennhicov.

Thông thường khái niệm tối ưu là phải hiểu theo một nghĩa nào đó, tức là tối ưu theo một tiêu chuẩn nào đó. Thông thường trong thông tin "thu tối ưu" được hiểu theo nghĩa như sau (Do Kachennhicov đề ra và gọi là tiêu chuẩn Kachennhicov).

Trong cùng một điều kiện đã cho trong số hai hay nhiều sô đồ giải, sô đồ nào đảm bảo xác suất giải đúng lớn nhất thì được gọi là tối ưu. (tiêu chuẩn này còn được gọi là tiêu chuẩn người quan sát lý tưởng).

Nhược: Không dễ dàng đến các loại sai lầm, tức là coi chúng tồn tại "ngang quyền" nhau.

Ưu: Đơn giản, dễ tính toán, dễ thực hiện.

Ngoài tiêu chuẩn Kachennhicov còn có một số những tiêu chuẩn khác như: Neyman-Pearson, Bayes, Wald Những tiêu chuẩn này khắc phục được nhược điểm trên nhưng khả phức tạp nên không dùng trong thông tin.

5.1.6. Việc xử lý tối ưu các tín hiệu

Nhiệm vụ của máy thu là cho ta các lời giải β_i . Quá trình thực hiện nhiệm vụ này được gọi là quá trình xử lý tín hiệu. Trong quá trình xử lý tín hiệu thường phải thực hiện các phép toán

tuyển tính hoặc phi tuyển tính các mạch tuyển tính hoặc phi tuyển (ví dụ: biến tần, tách sóng, lọc, hạn chế, nhân, chia, tích phân, bình phương, khuếch đại ...). Quá trình xử lý tín hiệu trong máy thu tối ưu được gọi là xử lý tối ưu tín hiệu. Xử lý để nhận lời giải có xác suất sai bé nhất.. Trước kia việc tổng hợp các máy thu (xây dựng sơ đồ giải) chỉ căn cứ vào các tiêu chuẩn chất lượng mang tính chất chắc chắn mà không mang tính chất thống kê. Ánh hưởng của nhiều lén chất lượng của máy thu chỉ được tính theo tỷ số tính /t/p. Tức là việc tổng hợp máy thu tối ưu trước đây chỉ chủ yếu dựa vào trực giác, kinh nghiệm, thí nghiệm. Ngày nay lý thuyết truyền tin đã cho phép bằng toán học tổng hợp được máy thu tối ưu ("Tối ưu" lúc này mới mang tính chất định lượng) tức là dựa vào các tiêu chuẩn tối ưu bằng công cụ thống kê toán học người ta xác định được quy tắc giải tối ưu.

5.1.7. Xác suất giải sai và quy tắc giải tối ưu

Cho α_i là tín hiệu đã gửi đi, xác suất để gửi tín hiệu này đi là $p(\alpha_i)$, $p(\alpha_i)$ được gọi là xác suất tiên nghiệm $\left(\sum_1^m p(\alpha_i) = 1 \right)$. Giả thiết rằng $S_i(t)$ có thời hạn T , $S_i(t)$ được gọi là các tín hiệu nguyên tố ứng với các dấu mã ở máy thu ta nhận được $u(t)$. Từ $u(t)$ qua sơ đồ giải ta sẽ có lời giải β_j nào đó. Nếu nhận được β_l thì ta coi rằng α_l đã được gửi đi. Như vậy α_l đã được gửi đi với một xác suất $p(\alpha_l/u)$ được gọi là xác suất hậu nghiệm. Do đó xác suất giải sai sẽ là:

$$p(sai/u, \beta_l) = 1 - p(\alpha_l/u) \quad (5.1)$$

Từ (5.1) ta sẽ tìm ra quy tắc giải tối ưu (theo tiêu chuẩn Kachennhcov)

Để tìm ra quy tắc giải tối ưu ta xét hai sơ đồ giải:

- Từ $u(t)$ cho ta β_1

- Từ $u(t)$ cho ta β_2

Nếu $p(sai/u, \beta_1) < p(sai/u, \beta_2)$ (5.2) thì ta sẽ coi sơ đồ thứ nhất tối ưu hơn sơ đồ thứ hai.

Từ (5.1) và (5.2) $\Rightarrow p(sai/u, \beta_1) > p(sai/u, \beta_2)$ (5.3)

Tức là xác suất chọn lời giải sai $p(sai/u, \beta_l)$ càng nhỏ nếu xác suất hậu nghiệm tương ứng $p(\alpha_l/u)$ càng lớn.

Ta xét m sơ đồ, khi đó ta có thể coi $(m-1)$ hệ thức sau:

$$p(\alpha_l/u) > p(\alpha_i/u) \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq l \end{cases} \quad (5.4)$$

Nếu ta có $(m-1)$ hệ thức này thì ta coi sơ đồ giải chọn β_l sẽ là tối ưu (theo nghĩa Kachenhhicov) vì nó đảm bảo xác suất phải sai là bé nhất (5.4) chính là quy tắc giải tối ưu. Sơ đồ giải thỏa mãn (5.4) chính là sơ đồ giải tối ưu.

5.1.8. Hàm hợp lý

$$\text{Dùng công thức Bayes: } p(\alpha_j/u) = \frac{p(\alpha_j)w(u/\alpha_j)}{w(u)} \quad (5.5)$$

$$\text{Thay vào (5.4) ta có: } p(\alpha_l)w(u/\alpha_l) > p(\alpha_i)w(u/\alpha_i) \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq l \end{cases} \quad (5.6)$$

$$\text{Hay } \frac{w(u/\alpha_l)}{w(u/\alpha_i)} > \frac{p(\alpha_l)}{p(\alpha_i)}$$

$$\text{Đặt } \lambda_{l/i} \triangleq \frac{w(u/\alpha_l)}{w(u/\alpha_i)} \text{ và được gọi là hàm hợp lý (tỷ số hợp lý). Nó đặc trưng cho mức độ}$$

hợp lý của giả thuyết cho rằng α_l đã được gửi đi (so với giả thuyết cho rằng α_i đã được gửi đi).

$$\text{Ta có: } \lambda_{l/i}(u) \triangleq \frac{p(\alpha_l)}{p(\alpha_i)} \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq l \end{cases} \quad (5.7)$$

(5.7) chính là quy tắc giải tối ưu viết dưới dạng hàm hợp lý.

5.1.9. Quy tắc hợp lý tối đa

Nếu mọi tín hiệu gửi đi đều đồng xác suất: $p(\alpha_l) = p(\alpha_i) = \frac{1}{m}$ với $\forall i, l = \overline{1, m}$ thì

$$(5.7) \text{ trở thành } \lambda_{l/i}(u) > 1 \quad \forall i \neq l \quad (5.8)$$

(5.8) được gọi là quy tắc hợp lý tối đa, nó hay được dùng trong thực tế vì hầu hết các hệ truyền tin đều có thể coi (với sai số chấp nhận được) nguồn đầu có các đầu đồng xác suất.

Để có thể thấy rõ ảnh hưởng của tinh thống kê của nhiễu ở (5.8) ta thường viết nó dưới dạng:

$$\begin{aligned} \lambda_{l/i}(u) &= \frac{w(u/\alpha_l)}{w(u/\alpha_i)} = \frac{w(u/\alpha_l) \cdot w(u/0)}{w(u/\alpha_i) \cdot w(u/0)} \\ &\Rightarrow \lambda_{l/i}(u) = \frac{\lambda_{l/0}(u)}{\lambda_{i/0}(u)} \Rightarrow \lambda_{l/0}(u) > \lambda_{i/0}(u) \quad \forall i \neq l \end{aligned} \quad (5.9)$$

$\lambda_{j/0}(u)$ và $\lambda_{i/0}(u)$ để tìm hon $\lambda_{l/i}(u)$. Ở đây phải hiểu rằng $W(u/0)$ chính là mật độ xác suất của nhiễu.

5.2. XỬ LÝ TỐI ƯU CÁC TÍN HIỆU CÓ THAM SỐ ĐÃ BIẾT. KHÁI NIỆM VỀ THU KẾT HỢP VÀ THU KHÔNG KẾT HỢP.

5.2.1. Đặt bài toán

Một kênh truyền tín hiệu liên tục chịu tác động của nhiễu công Gausse (chuẩn) có mật độ xác suất bằng:

$$W(n) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{n^2}{2\sigma^2}} \quad (5.10)$$

có phương sai σ^2 và kỳ vọng triết. Tín hiệu phát có mọi yếu tố triết trước (tiền định)

Hãy tìm công thức của quy tắc giải tối ưu theo quy tắc hợp lý tối đa và lập sơ đồ chức năng của sơ đồ giải tối ưu trong trường hợp này.

5.2.2. Giải bài toán

5.2.2.1. Tìm hàm hợp lý $\lambda_{j/0}(u)$

Ta có $u(t) = \mu S_j(t - \tau) + n(t)$

$\mu, \tau = \text{const}$ là các tham số của kênh đã biết

$S_j(t)$ cũng đã biết

Để tìm $\lambda_{j/0}(u)$ ta giả thiết $u(t)$ có phô hữu hạn F_c . Như vậy ta có thể rời rạc hóa $u(t)$ thành n số đoc:

u_1, u_2, \dots, u_n , $n = 2F_c T$, trong đó T là thời hạn của $u(t)$. Như vậy ta phải tìm $\lambda_{j/0}(u_1, u_2, \dots, u_n)$

$$\lambda_{j/0}(u_1, u_2, \dots, u_n) = \frac{W_n(u_1, u_2, \dots, u_n / \alpha_i)}{W_n(u_1, u_2, \dots, u_n / 0)}$$

$W_n(u_1, u_2, \dots, u_n / 0)$ chính là mật độ phân bố n chiều của nhiễu Gausse, nếu coi các số đoc của nhiễu độc lập, thông hệ với nhau thì:

$$\begin{aligned} W_n(u_1, u_2, \dots, u_n / 0) &= \prod_{k=1}^{2F_c T} W_1(u_k) = \prod_{k=1}^{2F_c T} \frac{1}{\sigma \sqrt{2\pi}} e^{-\frac{u_k^2}{2\sigma^2}} \\ &= \frac{1}{(\sigma \sqrt{2\pi})^{2F_c T}} \exp \left\{ -\sum_{k=1}^{2F_c T} \frac{u_k^2}{2\sigma^2} \right\} \end{aligned}$$

Ký hiệu $c_j(t) = \mu S_j(t - \tau)$.

Khi phát α_j ta sẽ nhận được các $u_k = c_{jk} + n_k$.

Để tính toán dễ dàng ta coi việc đã phát α_j tương đương với việc nhận được nhiễu có các giá trị nhiễu $n_k' = u_k - c_{jk}$. Tức là coi :

$$W_n(u_1, u_2, \dots, u_n / \alpha_j) = W_n(u_1', u_2', \dots, u_n' / 0)$$

Tương tự như trên ta có:

$$\begin{aligned} W_n(u_1', u_2', \dots, u_n' / 0) &= \frac{1}{(\sigma \sqrt{2\pi})^{2F_c T}} \exp \left\{ -\sum_{k=1}^{2F_c T} \frac{(u_k - c_{jk})^2}{2\sigma^2} \right\} \\ \Rightarrow \lambda_{j/0}(u_1, u_2, \dots, u_n) &= \exp \left\{ \sum_{k=1}^{2F_c T} \frac{u_k^2}{2\sigma^2} - \sum_{k=1}^{2F_c T} \frac{(u_k - c_{jk})^2}{2\sigma^2} \right\} \end{aligned}$$

Phương sai σ^2 của tệp có thể biểu thị qua mật độ phô công suất của nó và giải thông của kênh F_c

$$\sigma^2 = G_0 F_c \quad \text{Trong đó } F_c = \frac{1}{2\Delta t}$$

$$\lambda_{j/0}(u_1, u_2, \dots, u_n) = \exp \left\{ \frac{1}{G_0} \sum_{k=1}^{2F_c T} u_k^2 \Delta t - \frac{1}{G_0} \sum_{k=1}^{2F_c T} (u_k - c_{jk})^2 \Delta t \right\}$$

Khi $F_c \rightarrow \infty$ ta có:

$$\begin{aligned}
\lambda_{j,0}(u) &= \lim_{n \rightarrow \infty} \lambda_{j,0}(u_1, u_2, \dots, u_n) \\
&= \exp \left\{ \frac{1}{G_0} \left[\int_0^T u^2(t) dt - \int_0^T [u(t) - c_j(t)]^2 dt \right] \right\} \\
&= \exp \left\{ -\frac{E_j}{G_0} \left[\int_0^T C_j^2(t) dt + \frac{2}{G_0} \int_0^T u(t) c_j(t) dt \right] \right\} \\
\Rightarrow \lambda_{j,0}(u) &= \exp \left\{ -\frac{E_j}{G_0} \right\} \exp \left\{ \frac{2T}{G_0} Z_j(u) \right\} \quad (5.11)
\end{aligned}$$

Trong đó $E_j = \int_0^T c_j^2(t) dt$ là năng lượng của $c_j(t)$

$c_j(t)$ là tín hiệu nguyên tố mang tín số lõi ra của kênh

$$Z_j(u) = \frac{1}{T} \int_0^T u(t) c_j(t) dt \quad (5.12)$$

$Z_j(u)$ được gọi là tích vô hướng của $u(t)$ và $c_j(t)$

5.2.2.2. Quy tắc tối ưu viết theo các tham số của thể hiện tín hiệu.

Dùng quy tắc hợp lý tối đa $\frac{\lambda_{j,0}(u)}{\lambda_{i,0}(u)} > 1$ Với $\begin{cases} i = \overline{1, m} \\ i \neq j \end{cases}$. Lấy \log_e hai vế:

$$\begin{aligned}
&\ln \lambda_{j,0}(u) - \ln \lambda_{i,0}(u) > 0 \\
\Rightarrow \ln \lambda_{j,0}(u) &> \ln \lambda_{i,0}(u) \quad (*)
\end{aligned}$$

Thay (5.11) vào (*) ta được:

$$-\frac{E_j}{G_0} + \frac{2T}{G_0} Z_j(u) > -\frac{E_i}{G_0} + \frac{2T}{G_0} Z_i(u) \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq j \end{cases}$$

Nhân hai vế với $\frac{G_0}{2T}$ ta có:

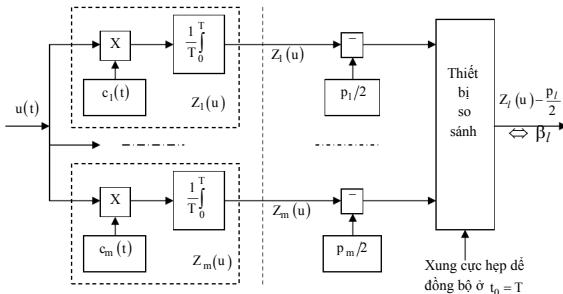
$$Z_j(u) - \frac{E_j}{2T} > Z_i(u) - \frac{E_i}{2T} \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq j \end{cases}$$

Chú ý rằng $E_j/T = P_j$ là công suất của tín hiệu $c_j(t)$ ở đầu vào sơ đồ giải.

$$Z_l(u) - \frac{P_l}{2} > Z_i(u) - \frac{P_i}{2} \quad \text{Với } i \neq l \quad (5.13)$$

Dựa vào quy tắc giải tối ưu (5.13) ta sẽ xây dựng được sơ đồ gia công tối ưu tín hiệu.

5.2.2.3. Xây dựng sơ đồ xử lý tối ưu tín hiệu



Hình 5.1: Sơ đồ gia công tối ưu tín hiệu.

Lời giải β_l lấy ra được chính là lời giải có xác suất sai bé nhất

Từ (5.12) ta đã vẽ được sơ đồ khối của việc hình thành tích vô hướng $Z_i(u)$. Sơ đồ này gồm 3 khối:

- Tạo tín hiệu $c_i(t)$ đóng vai trò như ngoại sai
- Mạch nhân đóng vai trò như biến tần
- Mạch tích phân (đóng vai trò như bộ lọc)

Người ta còn gọi sơ đồ trên là bộ lọc phối hợp chủ động (có nguồn) hay còn gọi là tương quan kẽ. Sau này chúng ta sẽ thấy được rằng để tạo tích vô hướng $Z_i(u)$ ta có thể chỉ dùng một mạch tuyến tính, đó là bộ lọc phối hợp thụ động (không nguồn)

Chú ý: Để so sánh đúng lúc, người ta phải dùng xung cực hép đồng bộ mở thiết bị so sánh vào đúng thời điểm đặc $t_0 = T$

5.2.3. Khái niệm về thu kết hợp và thu không kết hợp

5.2.3.1. Hệ có khoảng nghi chủ động.

Ở trên ta đã giải bài toán thu tối ưu các tín hiệu có các tham số đã biết (tức là xác định được một cách chính xác biên độ, tần số, pha ban đầu và $\mu, \tau = \text{const}$). Thực tế giả thiết $\mu, \tau = \text{const}$ không phù hợp vì μ, τ là các tham số của kênh phụ thuộc rất nhiều vào các yếu tố ngẫu nhiên.

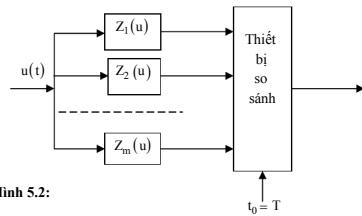
Khi μ thay đổi thì $Z_i(u)$ sẽ thay đổi tỷ lệ với μ còn p_i sẽ thay đổi tỷ lệ với μ^2 . Vì vậy để đảm bảo được quy tắc giải (5.13) ta cần có mạch tự động hiệu chỉnh để bù lại sự thay đổi của μ (ví dụ dùng mạch TĐK (APY)).

Khi τ thay đổi sẽ làm cho góc thời gian thay đổi gây ra sự không đồng bộ giữa $c_i(t)$ và $u(t)$. Để thực hiện được sự đồng bộ giữa $c_i(t)$ và $u(t)$ ta phải dùng hệ thống TDT (ATIY).

Để có thể tránh được sự phức tạp của thiết bị khi phải dùng thêm TĐK khi μ thay đổi người ta chọn các tín hiệu có công suất trung bình như nhau, tức là $p_i = p_j$ với $\forall i, j = \overline{1, m}$. Lúc đó quy tắc giải sẽ là:

$$Z_l(u) > Z_i(u) \quad \forall i \neq l \quad (5.14)$$

Sở dĩ giải lúc này sẽ rất đơn giản và ngay cả khi μ thay đổi ta cũng không phải dùng thêm mạch TĐK (Hình 5.2)



Hình 5.2:

Hệ thống có $p_i = p_j (\forall i, j = \overline{1, m})$ được gọi là hệ thống có khoảng nghi chủ động.

5.2.3.2. Định nghĩa thu kết hợp và thu không kết hợp

Tín hiệu tổng quát có dạng:

$$C_i(t) = C_{0i}(t) \cos(\omega t + \phi(t) + \varphi_0)$$

Khi giá công tối ưu tín hiệu ta cần biết đường bao $C_{0i}(t)$ và tần số tần thời $\omega_i(t) = \omega + \frac{d\phi(t)}{dt}$.

Nếu việc thu $C_i(t)$ cần biết φ_0 (để điều chỉnh hệ thống thu) thì được gọi là thu kết hợp.

Nếu việc thu $C_i(t)$ không cần biết φ_0 (để điều chỉnh hệ thống thu) thì được gọi là thu không kết hợp.

Thực tế khi τ thay đổi sẽ làm cho φ_0 thay đổi. τ chỉ biến thiên ít nhưng cũng đã làm cho φ_0 thay đổi rất mạnh. Khi đó ta phải chuyển sang thu không kết hợp.

5.3. PHÁT TÍN HIỆU TRONG NHIỀU NHỎ BỘ LỌC PHỐI HỢP TUYẾN TÍNH THỦ ĐỘNG.

5.3.1. Định nghĩa bộ lọc phối hợp tuyến tính thụ động

Định nghĩa: Đối với một tín hiệu xác định, một mạch tuyến tính thụ động đảm bảo tỷ số $\rho_{ra} = \left(\frac{S}{N} \right)_{ra}$ cực đại ở một thời điểm quan sát nào đây sẽ được gọi là mạch lọc phối hợp tuyến tính thụ động của tín hiệu đó.

Sau này để gọn ta chỉ gọi là bộ lọc phối hợp.

Trong đó ρ_{ra} là tỷ số giữa công suất định của tín hiệu và công suất trung bình của nhiễu ở đầu ra bộ lọc ấy.

5.3.2. Bài toán về bộ lọc phối hợp

5.3.2.1. Nội dung bài toán.

Cho ở đầu vào một mạch tuyến tính thụ động một dao động có dạng:

$$y(t) = C_i(t) + n(t)$$

$C_i(t)$ là thể hiện của tín hiệu phát đi (còn được gọi là tín hiệu tối)

$n(t)$ là nhiễu cộng, trắng, chuẩn

Hãy tổng hợp mạch đó để nó có hàm truyền sao cho ở một thời điểm quan sát $y(t)$ nào đó, ρ_{ra} của nó phải cực đại.

5.3.2.2. Giải bài toán.

Thực chất bài toán này là bài toán tổng hợp mạch (ngược với bài toán phân tích mạch) mà ta đã học ở giáo trình "Lý thuyết mạch". Nhiệm vụ của ta là phải tìm biểu thức giải tích của

hàm truyền phức $K_i(\omega)$ của mạch tuyển tính thu động sao cho ở một thời điểm quan sát (đao động nhận được) nào đó ρ_{ra} đạt max.

Gọi $S_{IV}(\omega)$ là mật độ phô (biên) phức của thế hiện tín hiệu ở đầu vào mạch tuyển tính.

Gọi $S_{ira}(\omega)$ là mật độ phô phức của thế hiện tín hiệu ở đầu ra của nó.

Khi đó theo công thức biến đổi ngược Fourier thế hiện tín hiệu ở đầu ra của mạch tuyển tính thu động này là:

$$\begin{aligned} C_{ira}(t) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} S_{ira}(\omega) e^{j\omega t} d\omega = \int_{-\infty}^{\infty} S_{ira}(2\pi f) e^{j2\pi ft} df \\ &= \int_{-\infty}^{\infty} S_{IV}(2\pi f) K_i(2\pi f) e^{j2\pi ft} df \end{aligned}$$

Trong đó: $S_{ira}(2\pi f) = S_{IV}(2\pi f) K_i(2\pi f)$

Công suất định của tín hiệu ở đầu ra của mạch:

$$P_{c_{ra}} = |C_{ira}(t_0)|^2 = \left| \int_{-\infty}^{\infty} S_{IV}(2\pi f) K_i(2\pi f) e^{j2\pi ft_0} df \right|^2$$

$C_{ira}(t_0)$ là giá trị định của tín hiệu

Theo giả thiết vi can nhiễu là tạp trắng nên mật độ phô công suất của nó sẽ là $N_0 = \text{const}$

(N_0 bằng $\frac{1}{2}$ mật độ phô công suất thực tế, vì phô thực tế chỉ có từ $0 \rightarrow \infty$). Do đó công suất trung bình của tạp ở đầu ra của mạch này sẽ là:

$$P_{n_{ra}} = \delta_n^2 = \int_{-\infty}^{\infty} N_0 |K_i(2\pi f)|^2 df = N_0 \int_{-\infty}^{\infty} |K_i(2\pi f)|^2 df$$

Ở đây ta áp dụng định lý Parseval:

$$\int_{-\infty}^{\infty} x^2(t) dt = \frac{1}{2\pi} \int_{-\infty}^{\infty} |S(\omega)|^2 d\omega$$

Ta xét tỷ số: $\rho_{ra} = \frac{P_{c_{ra}}}{P_{n_{ra}}}$

$$\rho_{ra} = \frac{\left| \int_{-\infty}^{\infty} S_{iv}(2\pi f) K_i(2\pi f) e^{j2\pi f t_0} df \right|^2}{N_0 \int_{-\infty}^{\infty} |K_i(2\pi f)|^2 df} \quad (5.15)$$

Vấn đề ở đây là phải xác định $K_i(2\pi f)$ trong (5.15) như thế nào để ρ_{ra} đạt max.

Để giải quyết vấn đề này ta có thể dùng nhiều phương pháp, ở đây ta sử dụng bất đẳng thức Byhakobekuu – Schwartz:

$$\left| \int_{-\infty}^{\infty} F(x)\varphi(x) dx \right|^2 \leq \int_{-\infty}^{\infty} |F(x)|^2 dx \int_{-\infty}^{\infty} |\varphi(x)|^2 dx \quad (5.16)$$

Đẳng thức ở (5.16) chỉ có khi: $\varphi(x) = k F^*(x)$

Trong đó: $\varphi(x), F(x)$ là các hàm phức biến thực

$F^*(x)$ là hàm liên hợp phức của $F(x)$

k là hệ số tỷ lệ

Trong (5.15) nếu cho $S_{iv}(2\pi f) e^{j2\pi f t_0}$ đóng vai trò $F(x)$, còn $K_i(2\pi f)$ đóng vai trò như $\varphi(x)$ trong (5.1).

Khi đó áp dụng (5.16) cho (5.15) ta được:

$$\begin{aligned} \rho_{ra} &\leq \frac{\int_{-\infty}^{\infty} |S_{iv}(2\pi f) e^{j2\pi f t_0}|^2 df \int_{-\infty}^{\infty} |K_i(2\pi f)|^2 df}{N_0 \int_{-\infty}^{\infty} |K_i(2\pi f)|^2 df} \\ &\Rightarrow \rho_{ra} \leq \frac{1}{N_0} \int_{-\infty}^{\infty} |S_{iv}(2\pi f) e^{j2\pi f t_0}|^2 df \\ &\Rightarrow \rho_{ra} \leq \frac{1}{N_0} \int_{-\infty}^{\infty} |S_{iv}(2\pi f)|^2 df \quad \underline{\text{Định lý Parseval}} \quad \frac{E_i}{N_0} \quad (5.18) \end{aligned}$$

$$(5.18) \text{ chứng tỏ } \rho_{ra \max} = \frac{E_i}{N_0} \quad (5.19)$$

trong đó $E_i = \int_{-\infty}^{\infty} |S_{IV}(2\pi f)|^2 df$ là năng lượng của tín hiệu tới (5.19) chứng tỏ tỷ số $\left(\frac{S}{N}\right)_{ra}$ chỉ phụ thuộc vào năng lượng của tín hiệu mà hoàn toàn không phụ thuộc vào dạng của

nó. Ta biết rằng xác suất phát hiện đúng chỉ phụ thuộc vào $\left(\frac{S}{N}\right)_{ra}$. Vì vậy theo quan điểm của bài toán phát hiện dạng của tín hiệu là không quan trọng. (Chi khi cần đo lường các tham số của tín hiệu như μ , ΔF (độ dịch tần) thì độ chính xác của phép đo và khả năng phân biệt của hệ thống sẽ phụ thuộc mạnh vào dạng tín hiệu).

Theo (5.17) ρ_{ra} chỉ đạt max khi:

$$k_i(2\pi f) = k S_{IV}^*(2\pi f) \exp\{-j2\pi f t_0\} \quad (5.20)$$

(5.20) chính là đáp số củ bài toán ta đã nêu ra ở trên. Như vậy bài toán đã giải xong. Để thấy rõ được ý nghĩa vật lý kỹ thuật ta sẽ xét kỹ (5.20) hơn nữa.

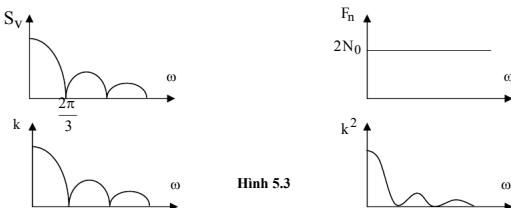
5.3.3. Đặc tính biên tần và đặc tính pha tần của bộ lọc phối hợp

5.3.3.1. Đặc tính biên tần.

Từ (5.20) ta có $|k_i(2\pi f)| = k |S_{IV}^*(2\pi f)|$ (5.21)

(5.21) là biểu thức giải tích của đặc tính biên tần của bộ lọc phối hợp, ta thấy nó có dạng giống hệt modul mật độ phô của tín hiệu. Điều đó có nghĩa là khi đã cho tín hiệu tới thì đặc tính của mạch tuyển tần cần tổng hợp sẽ do mật độ phô phức của tín hiệu quyết định.

Ngoài ra từ hình 5.3 ta còn thấy: bộ lọc phối hợp sẽ làm suy giảm các thành phần phô tín hiệu và tạp âm ứng với những phần có cường độ nhỏ của phô tín hiệu. Ở những khoảng tần số mà cường độ các thành phần phô của tín hiệu càng nhỏ thì sự suy giảm đó càng lớn.



5.3.3.2. Đặc tính pha tần.

Ta viết lại (5.20) như sau:

$$k_i(\omega) = k S_{iv}^*(\omega) e^{-j\varphi_{xi}(\omega)} e^{-j\omega t_0} = k S_{iv}^*(\omega) e^{-j\varphi(\omega)} \quad (5.22)$$

trong đó $\varphi_{xi}(\omega)$ là phô pha của tín hiệu tối.

Còn $\varphi(\omega) = [\varphi_{xi}(\omega) + \omega t_0]$ (5.23) là dịch pha gây bởi bộ lọc. Đó chính là đặc tính pha tần của bộ lọc phối hợp. Ta thấy $[\varphi_{xi}(\omega) + \omega t_0]$ là dịch pha toàn phần của tín hiệu tại thời điểm quan sát t_0 . Như vậy tại thời điểm $t = t_0$ dịch pha toàn phần của bộ lọc vừa vận khứ được dịch pha toàn phần của tín hiệu truyền tới qua bộ lọc, điều đó làm cho mọi thành phần dao động điều hòa của tín hiệu tối đồng pha với nhau. Vì vậy các thành phần dao động điều hòa được cộng lại với nhau và tín hiệu ra sẽ đạt được cực đại $t = t_0$.

Ngoài ra từ (5.20) ta thấy bộ lọc phối hợp có tính chất bất biến đối với biên độ vị thời gian và pha đầu của tín hiệu. Bởi vì các tín hiệu khác với $x_i(t)$ về biên độ và pha ban đầu ((μ_1, t_1, ψ_1)) thì mật độ phô của tín hiệu này chỉ khác nhau với mật độ phô của $x_i(t)$ một thừa số $\mu_1 \exp\{-j(\omega t_1 + \psi_1)\}$. Tính chất này của bộ lọc phối hợp rất quan trọng và đặc biệt là đối với thực tế. Thực vậy, thông thường biên độ, sự giữ chậm và pha ban đầu của tín hiệu thu ta không biết. Như vậy đang lẽ phải xây dựng một số lớn các bộ lọc mà mỗi bộ lọc chỉ làm tối ưu cho một tín hiệu có giá trị biên độ, sự giữ chậm và pha ban đầu cụ thể thì ta chỉ cần một bộ lọc phối hợp tuyến tính thu động, bộ lọc này sẽ là tối ưu cho mọi tín hiệu cùng dạng. Trong radar thông thường các tham số như biên độ và pha ban đầu nhận các giá trị ngẫu nhiên và không may thông tin có ích (có nghĩa là các tham số ký sinh). Từ kết luận trên ta thấy rằng sự tồn tại của các tham số ngẫu nhiên này không làm biến đổi cấu trúc của bộ lọc tối ưu.

5.3.4. Phản ứng xung $g_i(t)$ của mạch lọc phối hợp

Ta biết rằng phản ứng xung và hàm truyền liên hệ với nhau theo cặp biến đổi Fourier:

$$g_i(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} K_i(\omega) e^{j\omega t} d\omega$$

Thay (5.20) vào:

$$\Rightarrow g_i(t) = \frac{k}{2\pi} \int_{-\infty}^{\infty} S_{iv}^*(\omega) e^{-j\omega t_0} e^{j\omega t} d\omega$$

$$\Rightarrow g_i(t) = \frac{k}{2\pi} \int_{-\infty}^{\infty} S_{iv}^*(\omega) e^{-j\omega(t_0 - t)} d\omega$$

Ta có: $S_{iv}^*(\omega) = S_i(-\omega)$

$$\Rightarrow g_i(t) = \frac{k}{2\pi} \int_{-\infty}^{\infty} S_{iv}(-\omega) e^{j(-\omega)(t_0 - t)} d\omega$$

Đặt

$$\omega = \omega' \Rightarrow g_i(t) = \frac{k}{2\pi} \int_{-\infty}^{\infty} S_{iv}(\omega') e^{j\omega'(t_0 - t)} (-d\omega')$$

$$\Rightarrow g_i(t) = -kC_{iv}(t_0 - t)$$

Vì k là hằng số tùy ý nên ta có thể lấy:

$$g_i(t) = kC_{iv}(t_0 - t) \quad (5.23)$$

Đồ thị $g_i(t)$ vẽ trên hình 5.4.

Từ hình 5.4 ta thấy rằng để thỏa mãn điều kiện thời hiện được bộ lọc:

$$g_i(t) = 0 \text{ khi } t < 0 \text{ nên } t_0 \geq T$$

5.3.5. Hướng ứng ra của mạch lọc phối hợp

Theo tích phân Duhamen:

$$U_{ra}(t) = \int_0^t U_v(x) g(t-x) dx$$

$$C_{iv}(t)$$

$$C_{iv}(-t)$$

$$C_{iv}(t_0 - t)$$

$$C_{iv}(t_0 - t)$$

Hình 5.4

Thay (5.23) vào ta có:

$$U_{ra}(t) = k \int_0^t U_v(x) C_{iv}(t_0 - t + x) dx$$

$$t = t_0 \Rightarrow U_{ra}(t_0) = k \int_0^{t_0} U_v(x) C_{iv}(x) dx = k \int_0^{t_0} U_v(t) C_{iv}(t) dt$$

Nếu lấy $t = t_0$ và $k = \frac{1}{T}$ thì ta có:

$$U_{ra}(T) = \frac{1}{T} \int_0^T U_v(t) C_{iv}(t) dt$$

$$\Rightarrow U_{ra}(T) = Z_i(u) \quad (5.24)$$

Như vậy ta có thể dùng mạch lọc phối hợp để tạo ra tích vô hướng. Sơ đồ giải tối ưu nhờ đó sẽ đơn giản hơn rất nhiều.

5.4. LÝ LUẬN CHUNG VỀ THU KẾT HỢP CÁC TÍN HIỆU NHỊ PHÂN

5.4.1. Lập sơ đồ giải tối ưu một tuyến

5.4.1.1. Lập quy tắc giải.

Xét một nguồn tin nhị phân: $\alpha_1 \leftrightarrow "1"$ và $\alpha_2 \leftrightarrow "0"$.

Khi đó tín hiệu sẽ có hai thể hiện $S_1(t)$ và $S_2(t)$

Ta giới hạn chỉ xét nhiễu công và là tạp âm trắng, chuẩn dừng.

Tín hiệu ở đầu vào máy thu: $u(t) = C_1(t) + n(t)$, $i = 1, 2$

Ứng với quy tắc giải theo Kachennhicov ta sẽ nhận được lời giải đúng α_1 , nếu:

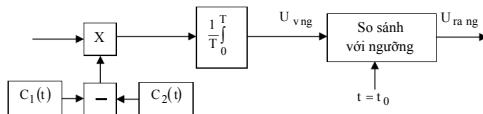
$$\frac{1}{T} \int_0^T u(t) C_1(t) dt - \frac{P_1}{2} > \frac{1}{T} \int_0^T u(t) C_2(t) dt - \frac{P_2}{2} \quad (*)$$

Để lập được sơ đồ một tuyến ta đưa (*) về dạng sau:

$$\frac{1}{T} \int_0^T u(t) [C_1(t) - C_2(t)] dt > \frac{1}{2} (P_1 - P_2) \quad (5.25)$$

$\frac{1}{2} (P_1 - P_2)$ được gọi là ngưỡng làm việc

5.4.1.2. Sơ đồ giải tối ưu một tuyến. (hình 5.5)



Hình 5.5

Nếu $U_{vng} > \frac{1}{2} (P_1 - P_2)$ thì $U_{ra ng} \neq 0$, khi đó ta xem rằng có lời giải β_1 về α_1 .

Nếu $U_{vng} < \frac{1}{2} (P_1 - P_2)$ thì $U_{ra ng} = 0$, khi đó ta xem rằng có lời giải β_2 về α_2 .

Chú ý:

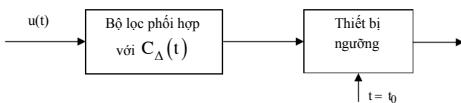
- Nếu $P_1 \neq P_2$ mà μ (hàm truyền đạt của đường truyền) thay đổi thì ta phải có thiết bị tự động điều chỉnh ngưỡng. Nếu không thì xác suất giải sai sẽ tăng lên.

- Nếu $P_1 = P_2$ thì ta không cần phải có thiết bị so sánh tự động điều chỉnh ngưỡng. Khi đó ta sẽ dùng bộ phân biệt cực. Ta quy ước rằng:

+ $U_{\text{rang}} > 0$ thì có lời giải $\beta_1 \leftrightarrow \alpha_1$

+ $U_{\text{rang}} < 0$ thì có lời giải $\beta_2 \leftrightarrow \alpha_2$

Nếu gọi $C_\Delta(t) = C_1(t) - C_2(t)$ là tín hiệu số thì khi dùng bộ lọc phối hợp với tín hiệu $C_\Delta(t)$ thiết bị sẽ đơn giản đi rất nhiều (hình 5.6.)

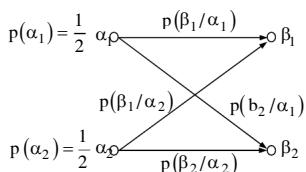


Hình 5.6.

5.4.2. Xác suất sai khi thu kết hợp tín hiệu nhị phân

5.4.2.1. Đặt bài toán

Cho kênh nhị phân, đối xứng, không nhớ có nhiễu cộng, trắng, chuẩn theo mô hình sau:



Hãy tìm công thức biểu diễn xác suất sai toàn phần (xác suất sai không điều kiện) của kênh này khi sơ đồ giải tín hiệu là tối ưu theo Kopenhicop.

5.4.2.2. Giải bài toán

Theo công thức xác suất đầy đủ:

$$p_s = p(\alpha_1) \cdot p(\beta_2 / \alpha_1) + p(\alpha_2) \cdot p(\beta_1 / \alpha_2)$$

Bđt tìm xác suất sai của hệ p_s , ta phải tìm xác suất sai của mỗi dấu $p(\beta_2 / \alpha_1)$ và $p(\beta_1 / \alpha_2)$.

Tìm $p(\beta_2 / \alpha_1)$:

- Theo quy tắc giải (5.25), $p(\beta_2 / \alpha_1)$ chính là xác suất để không thoả mãn (5.25), tức là:

$$p(\beta_2 / \alpha_1) = p\left\{ \frac{1}{T} \int_0^T U(t) [C_1(t) - C_2(t)] dt < \frac{1}{2}(P_1 - P_2) \right\} \quad (5.26)$$

Trong đó: $U(t) = C_1(t) + n(t)$ (*)

$$P_i = \frac{1}{T} \int_0^T C_i^2(t) dt \quad (**)$$

Thay (*) và (**) vào (5.26), sau một vài biến đổi đơn giản, ta có:

$$\begin{aligned} p(\beta_2 / \alpha_1) &= p\left\{ \frac{1}{T} \int_0^T C_1^2(t) dt - \frac{1}{T} \int_0^T C_1(t) C_2(t) dt + \frac{1}{T} \int_0^T n(t) [C_1(t) - C_2(t)] dt \right. \\ &\quad \left. < \frac{1}{2T} \int_0^T C_1^2(t) dt - \frac{1}{2T} \int_0^T C_2^2(t) dt \right\} \end{aligned}$$

$$\Rightarrow p(\beta_2 / \alpha_1) = p\left\{ \frac{1}{T} \int_0^T n(t) C_\Delta(t) dt < -\frac{1}{2T} \int_0^T C_\Delta^2(t) dt \right\} \quad (5.27)$$

Trong đó: $C_\Delta(t) = C_1(t) - C_2(t)$.

$P_\Delta = \frac{1}{T} \int_0^T C_\Delta^2(t) dt$ là công suất trung bình của tín hiệu hiệu số.

$\xi = \frac{1}{T} \int_0^T n(t) C_\Delta(t) dt$ là một đại lượng ngẫu nhiên, vì $n(t)$ là một quá trình ngẫu nhiên

và tích phân là một phép biến đổi tuyến tính.

$$\Rightarrow p(\beta_2 / \alpha_1) = p\left\{ \xi < -\frac{1}{2} P_\Delta \right\} \quad (5.28)$$

Theo định nghĩa xác suất:

$$p\left\{ \xi < -\frac{1}{2} P_\Delta \right\} = \int_{-\infty}^{-\frac{1}{2} P_\Delta} W(\xi) d\xi \quad (5.29)$$

Để tìm $W(\xi)$, ta thấy rằng phép biến đổi tuyến tính của một quá trình chuẩn cũng là một quá trình chuẩn. Vì $n(t)$ chuẩn nên ξ cũng chuẩn. Do đó $W(\xi) = W(n)$.

$$\Rightarrow W(\xi) = \frac{1}{\sqrt{2\pi\sigma_{\xi}^2}} \exp\left\{-\frac{[\xi - a_{\xi}]^2}{2\sigma_{\xi}^2}\right\} \quad (5.30)$$

$$\text{Trong đó: } a_{\xi} = M\left\{\frac{1}{T} \int_0^T n(t) C_{\Delta}(t) dt\right\} = \frac{1}{T} \int_0^T M\{n(t)\} C_{\Delta}(t) dt$$

Vì $M\{n(t)\} = 0$ nên $a_{\xi} = 0$.

Xác định phương sai: σ_{ξ}^2 :

$$\begin{aligned} \sigma_{\xi}^2 &= D[\xi] = D\left\{\frac{1}{T} \int_0^T n(t) C_{\Delta}(t) dt\right\} \stackrel{\Delta}{=} \frac{1}{T^2} M\left\{\left[\int_0^T n(t) C_{\Delta}(t) dt\right]^2\right\} \\ &= \frac{1}{T^2} M\left\{\int_0^T n(t) C_{\Delta}(t) dt \cdot \int_0^T n(t_1) C_{\Delta}(t_1) dt_1\right\} \\ &= \frac{1}{T^2} M\left\{\int_0^T \int_0^T C_{\Delta}(t) C_{\Delta}(t_1) n(t) n(t_1) dt dt_1\right\} \\ &= \frac{1}{T^2} \int_0^T \int_0^T C_{\Delta}(t) C_{\Delta}(t_1) M\{n(t) n(t_1)\} dt dt_1 \end{aligned} \quad (a)$$

Theo giả thiết $n(t)$ là tạp âm trắng, chuẩn, dừng, dừng biến đổi Wiener – Khinchin, ta tính được hàm tự tương quan của nó:

$$M\{n(t)n(t_1)\} \stackrel{\Delta}{=} R(t - t_1) = N_0 \delta(t - t_1) \quad (b)$$

$$\text{Với } R(t - t_1) = \int_{-\infty}^{\infty} N_0 \cdot e^{j\alpha(t - t_1)}$$

Thay (b) vào (a), ta được:

$$\sigma_{\xi}^2 = \frac{N_0}{T^2} \int_0^T \int_0^T C_{\Delta}(t) C_{\Delta}(t_1) \delta(t - t_1) dt dt_1 \quad (c)$$

Áp dụng tính chất sau của hàm δ :

$$\int_a^b f(x) \delta(x - x_0) dx = f(x_0) \quad \text{khi } a < x_0 < b$$

$$\text{ta có: } \int_a^b C_\Delta(t) \delta(t - t_1) dt = C_\Delta(t_1) \quad (d)$$

Thay (d) vào (c), ta được:

$$\begin{aligned} \sigma_\xi^2 &= \frac{N_0}{T} \int_0^T C_\Delta(t) dt \int_0^T C_\Delta(t_1) \delta(t - t_1) dt_1 = \frac{N_0}{T^2} \int_0^T C_\Delta^2(t) dt \\ &\Rightarrow \sigma_\xi^2 = \frac{N_0 P_\Delta}{T} \end{aligned} \quad (5.31)$$

Thay (5.31) vào (5.30):

$$W(\xi) = \frac{1}{\sqrt{2\pi \frac{N_0 P_\Delta}{T}}} \exp \left\{ -\frac{\xi^2}{2 \frac{N_0 P_\Delta}{T}} \right\} \quad (5.32)$$

Khi đó xác suất sai khi truyền dẫn α_1 sẽ bằng:

$$\begin{aligned} p(\beta_2 / \alpha_1) &= p\left\{ \xi < -\frac{1}{2} P_\Delta \right\} = \int_{-\infty}^{-\frac{1}{2} P_\Delta} W(\xi) d\xi = \\ &= \frac{1}{\sqrt{2\pi \frac{N_0 P_\Delta}{T}}} \int_{-\infty}^{-\frac{1}{2} P_\Delta} \exp \left\{ -\frac{\xi^2}{2 \frac{N_0 P_\Delta}{T}} \right\} d\xi = \end{aligned}$$

Đổi biến: Đặt $\eta = \frac{\xi}{\sqrt{\frac{N_0 P_\Delta}{T}}}$

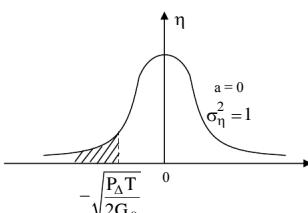
$$\Rightarrow p(\beta_2 / \alpha_1) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\sqrt{\frac{P_\Delta T}{4N_0}}} \exp \left\{ -\frac{\eta^2}{2} \right\} d\eta = \phi\left(-\sqrt{\frac{P_\Delta T}{2G_0}} \right) \quad (*)$$

Trong đó $G_0 = 2N_0$ là phô công suất thực tế.

$\phi(\cdot)$ gọi là hàm xác suất sai (còn ký hiệu là erf).

Trong giáo trình Lý thuyết xác suất, ta có: $\phi(-x) = 1 - \phi(x)$. Nên ta có:

$$P(\beta_2 / \alpha_1) = 1 - \phi\left(\sqrt{\frac{P_\Delta T}{2G_0}}\right) \quad (5.33)$$



Hình 5.7.

Tương tự:

$$P(\beta_1 / \alpha_2) = 1 - \phi\left(\sqrt{\frac{P_\Delta T}{2G_0}}\right) \quad (5.33')$$

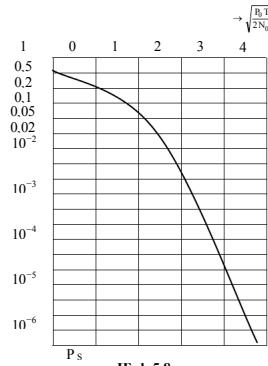
$$\Rightarrow p_s = 1 - \phi\left(\sqrt{\frac{P_\Delta T}{2G_0}}\right) \quad (5.34)$$

Đồ thị biểu diễn (5.34) vẽ trên hình 5.8. Thông thường T là xác định vì khi thiết kế hệ thống truyền tin người ta thường cho trước tốc độ truyền tin. Để giảm nhõ p_s người ta giảm nhõ G_0 bằng cách dùng các bộ khuếch đại tạp âm nhõ (khuếch đại tham số, khuếch đại lượng tử,...)

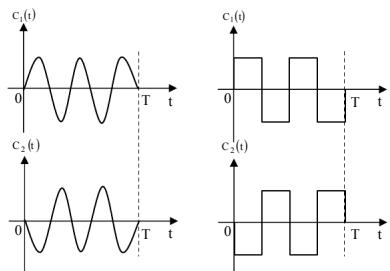
5.4.2.3. Tính xác suất sai trong một số trường hợp cụ thể

a. Các tín hiệu đối cực:

$$c_1(t) = -c_2(t)$$



Hình 5.8



$$C_{\Delta} = C_1(t) - C_2(t) \Rightarrow C_{\Delta}(t) = 2C_1(t) \Rightarrow P_{\Delta} = 4P_1 = 4P_2 = 4P_c$$

$P_c = \frac{P_1 + P_2}{2}$ là công suất trung bình của tín hiệu tối $C_i(t)$.

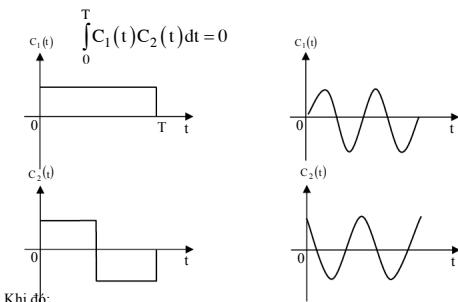
$$p_s = 1 - \phi\left(\sqrt{\frac{4P_c T}{2G_0}}\right) \Rightarrow p_s = 1 - \phi(\sqrt{2} h) \quad (5.35)$$

Trong đó $P_c T$ là năng lượng của tín hiệu.

$$h = \sqrt{\frac{P_c T}{G_0}} \quad (\text{chính là tỷ số tín/tạp})$$

b. Các tín hiệu trực giao (theo nghĩa hẹp)

Định nghĩa: Hai tín hiệu được gọi là trực giao theo nghĩa hẹp, nếu:



Khi đó:

$$\begin{aligned}
 P_{\Delta} &= \int_0^T C_{\Delta}^2(t) dt = \int_0^T C_1^2(t) dt + \int_0^T C_2^2(t) dt \\
 P_{\Delta} &= P_1 + P_2 = 2P_c \\
 \Rightarrow p_s &= 1 - \phi\left(\sqrt{\frac{2P_c T}{2G_0}}\right) \\
 p_s &= 1 - \phi(h)
 \end{aligned} \tag{5.36}$$

c. Một trong hai tín hiệu triết ($C_2(t) = 0$)

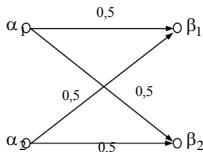
Hệ này chính là hệ truyền tín hiệu phân có khoảng nghi thu động.

$$\begin{aligned}
 C_{\Delta}(t) &= C_1(t) \Rightarrow P_{\Delta} = P_1 = 2P_c \\
 \Rightarrow p_s &= 1 - \phi(h)
 \end{aligned} \tag{5.37}$$

d. Các tín hiệu như nhau ($C_1(t) = C_2(t)$)

$$C_{\Delta}(t) = 0 \Rightarrow P_{\Delta} = 0, \phi(0) = \frac{1}{2} \Rightarrow p_s = \frac{1}{2} = p_{smax}$$

Như vậy, việc lặp lại các tin bị sai hoàn toàn: kênh liên lạc bị đứt. Mô hình kênh trong trường hợp này như sau:



Chú ý:

$$\text{Ở đây ta coi } P_c = \frac{P_1 + P_2}{2}.$$

5.5. XỬ LÝ TỐI UU CÁC TÍN HIỆU CÓ THAM SỐ NGẪU NHIÊN – THU KHÔNG KẾT HỢP

5.5.1. Các tham số của tín hiệu là các tham số ngẫu nhiên

Do chịu tác động của nhiều yếu tố ngẫu nhiên như nhiệt độ, độ ẩm, áp suất, điện áp nguồn... nên:

- Trạng thái của các khâu của mạch truyền tin luôn thay đổi.
- Các tham số vật lý của kênh luôn thay đổi (μ, τ, \dots)
- Vì vậy các tham số của tín hiệu phải là các tham số thay đổi ngẫu nhiên.

5.5.2. Xử lý tối ưu các tín hiệu có tham số ngẫu nhiên biến thiên chậm

Ta gọi một tham số ngẫu nhiên ξ là biến thiên chậm nếu trong khoảng quan sát T , các biến thiên của nó chưa kịp bộc lộ rõ ràng, tức là: $d\xi/dt \approx 0$.

Ta sẽ xét một số trường hợp cụ thể sau:

a. Nếu các tham số ngẫu nhiên biến thiên chậm có các giá trị biết trước thì ta sẽ căn cứ vào tín hiệu nguyên tố vừa nhận được để thông báo những hiểu biết về giá trị của các tham số của tín hiệu nguyên tố sẽ thu tiếp sau. Thực chất bài toán này đã xét ở trên (thu kết hợp).

b. Nếu giá trị của các tham số ngẫu nhiên biến thiên chậm không biết trước (thu không kết hợp) thì sơ đồ giải tối ưu phải có những thay đổi cơ bản. Sau đây ta sẽ xét trường hợp này.

5.5.3. Xác suất hậu nghiệm của tín hiệu có các tham số thay đổi ngẫu nhiên

Để đơn giản, ta chỉ giả sử một trong những tham số γ_i của tín hiệu $C_K(\gamma_1, \gamma_2, \dots, t)$ là ngẫu nhiên. Ở đầu thu tất cả các số còn lại đều đã biết chính xác. Giả sử tham số ngẫu nhiên này là γ_1 . Khi đó tín hiệu thứ K có tham số γ_1 không biết sẽ ký hiệu là $C_{K, \gamma_1}(t)$. Trong trường hợp tổng quát, luật phân bố của γ_1 có thể phụ thuộc vào chỉ số k . Vì vậy tính chất thống kê của tham số này được xác định bởi phân bố đồng thời sau:

$$W(C_K, \gamma_1) = p(C_K) W(\gamma_1 | C_K) \quad (5.38)$$

Trong đó: $W(\gamma_1 | C_K)$ là mật độ xác suất của tham số γ_1 khi đã biết giá trị C_K . Nếu giá trị của $\gamma_1 \notin k$ (điều này thường xảy ra trong thực tế) thì:

$$W(C_K, \gamma_1) = p(C_K) W(\gamma_1) \quad (5.39)$$

Cũng như trong trường hợp tín hiệu đã biết hoàn toàn chính xác, ta có thể tìm xác suất hậu nghiệm của $C_{K, \gamma_1}(t)$ theo công thức:

$$W(C_K, \gamma_1 | u) = b W(C_K, \gamma_1) W(u | C_K, \gamma_1) \quad (5.40) \text{ (Công thức Bayes)}$$

Trong đó $b = \text{const} (\notin k)$.

$W(u | C_K, \gamma_1)$ là mật độ xác suất của dao động nhận được nếu đã truyền tín hiệu $C_{K, \gamma_1}(t)$:

$$u(t) = C_{K,\gamma_1}(t) + n(t)$$

Ta thấy hàm $W(C_K, \gamma_1/u)$ không chỉ chứa thông tin về tín hiệu phát C_K mà còn chứa cả thông tin về γ_1 , đó là những thông tin thừa. Ta có thể bỏ những thông tin thừa này bằng cách lấy trung bình $W(C_K, \gamma_1/u)$ theo mọi giá trị có thể có của γ_1 . Khi đó ta có:

$$p(C_K/u) = \int W(C_K, \gamma_1/u) d\gamma_1 = b \cdot p(C_K) \int W(\gamma_1/C_K) W(u/C_{K,\gamma_1}) d\gamma_1 \quad (5.41)$$

Sau đó trên cơ sở phân tích xác suất hậu nghiệm $p(C_K/u)$, ta sẽ tìm được lời giải về tín hiệu đã phát:

$$p(C_K/u) > p(C_i/u) \quad \forall i \neq k \quad (5.42)$$

Nếu tín hiệu có một số tham số ngẫu nhiên $\gamma_1, \gamma_2, \dots$ thì ta cần phải tìm $W(u/C_{K,\gamma_1, \gamma_2, \dots})$ và sau đó lấy trung bình theo mọi giá trị có thể có của các tham số $\gamma_1, \gamma_2, \dots$. Chú ý rằng tính chất thống kê của các tham số $\gamma_1, \gamma_2, \dots$ được xác định bằng hàm:

$$W(C_K, \gamma_1, \gamma_2, \dots) = p(C_K) \cdot W(\gamma_1, \gamma_2, \dots / C_K)$$

Ta có:

$$p(C_K/u) = b \cdot p(C_K) \int \int \dots \int W(\gamma_1, \gamma_2, \dots / C_K) \cdot W(u/C_{K,\gamma_1, \gamma_2, \dots}) d\gamma_1 d\gamma_2 \dots \quad (5.43)$$

$p(C_K)$ là xác suất tiên nghiệm của tín hiệu phát C_K .

5.5.4. Xử lý tối ưu các tín hiệu có pha ngẫu nhiên

Để xác định cấu trúc của máy thu tối ưu, ta sẽ phân tích (5.41) có kẽ đến quy tắc giải (5.42).

Giả sử rằng các tín hiệu phát có thời hạn T và pha đầu φ thay đổi ngẫu nhiên:

$$\begin{aligned} C_{K,\varphi}(t) &= A_K(t) \cos[\theta_K(t) - \varphi] \\ &= A_K(t) \cos \theta_K(t) \cos \varphi + A_K(t) \sin \theta_K(t) \sin \varphi \\ &= C_K(t) \cos \varphi + \hat{C}_K(t) \sin \varphi \end{aligned} \quad (5.44)$$

Trong đó $C_K(t) = A_K(t) \cos \theta_K(t)$, $\hat{C}_K(t)$ là biến đổi Hilbert của $C_K(t)$.

$$\hat{C}_K(t) = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{C_K(\tau)}{t - \tau} d\tau.$$

$A_K(t)$ và $\theta_K(t)$ là bao và pha tức thời của tín hiệu $C_K(t)$. Giả sử φ là tham số ngẫu nhiên $\notin K$ và có phân bố đều:

$$W(\varphi) = \begin{cases} \frac{1}{2\pi} & \varphi \in (0, 2\pi) \\ 0 & \varphi \notin (0, 2\pi) \end{cases}$$

Giả thiết trên có nghĩa là pha φ trong khoảng $(0, T)$ được giữ không đổi và thay đổi ngẫu nhiên một cách độ lặp khi chuyển từ khoảng quan sát này sang khoảng quan sát khác.

Trước tiên ta sẽ xác định $W(u/C_{K,\varphi}) = W[n'(t) = u(t) - C_{K,\varphi}(t)]$.

Ở phần 5.2 ta đã có:

$$W_n(n'_1, \dots, n'_n / 0) = \frac{1}{(\sigma\sqrt{2\pi})^{2F_c T}} \exp \left\{ -\frac{1}{2\sigma^2} \sum_{j=1}^n (U_j - C_{K,\varphi_j})^2 \right\}$$

Trong đó: $n = 2F_c T$.

Để tìm $W(u/C_{K,\varphi})$ ta cho $F_c \rightarrow \infty$

$$\begin{aligned} W(u/C_{K,\varphi}) &= \lim_{F_c \rightarrow \infty} W_n(n'_1, \dots, n'_n / 0) = \\ &= \frac{1}{(\sigma\sqrt{2\pi})^n} \lim_{F_c \rightarrow \infty} \exp \left\{ -\frac{1}{2\sigma^2/2F_c} \sum_{j=1}^n (U_j - C_{K,j})^2 \Delta t \right\} \end{aligned}$$

Trong đó $\Delta t = \frac{1}{2F_c}; \frac{\sigma^2}{F_c} = G_0$. Khi $F_c \rightarrow \infty$ thì $\Delta t \rightarrow 0$.

$$\begin{aligned} \Rightarrow W(u/C_{K,\varphi}) &= \frac{1}{(\sigma\sqrt{2\pi})^n} \exp \left\{ -\frac{1}{G_0} \int_0^T [U(t) - C_{K,\varphi}(t)]^2 dt \right\} \\ W(u/C_{K,\varphi}) &= b_1 e^{-\frac{E_K}{G_0}} \cdot \exp \left\{ \frac{2}{G_0} \int_0^T U(t) \left[C_K(t) \cos \varphi + \hat{C}_K(t) \sin \varphi \right] dt \right\} \quad (5.45) \end{aligned}$$

$$E_K = \int_0^T C_{K,\varphi}^2(t) dt$$

Nhân tử b_1 chứa tất cả những đại lượng $\notin K$.

Biến đổi tích phân ở mũ của nhân tử hàm mũ, ta có:

$$\begin{aligned} q(k, \varphi) &= \cos \varphi \int_0^T U(t) C_K(t) dt + \sin \varphi \int_0^T U(t) \hat{C}_K(t) dt = \\ &= U_K \cos \varphi + V_K \sin \varphi \end{aligned}$$

Ký hiệu $M_K = \sqrt{U_K^2 + V_K^2}$, $\varphi_K = \arctg(V_K/U_K)$ (5.46)

Ta có thể viết: $q(k, \varphi) = M_K \cos(\varphi_K - \varphi)$ (5.47)

Theo (5.41) ta tìm được:

$$\begin{aligned} p(C_K/u) &= b_1 \cdot \frac{p(C_K)}{2\pi} e^{-E_K/G_0} \int_0^{2\pi} e^{G_0} \cos(\varphi_K - \varphi) d\varphi = \\ &= b_2 p(C_K) e^{-E_K/G_0} I_0\left(\frac{2M_K}{G_0}\right) \end{aligned}$$
(5.48)

Trong đó $I_0(x)$ là hàm Bessel biến dạng cấp 0, là một hàm đơn điệu tăng của x.

Để thuận tiện, chúng ta sẽ không so sánh các $p(C_K/u)$ mà sẽ so sánh logarit tự nhiên của chúng. Lấy ln (5.48) và áp dụng quy tắc giải, chúng ta sẽ nhận được quy tắc giải sau:

Tín hiệu $C_K(t)$ đã được phát đi, nếu:

$$\ln p(C_K) - \frac{E_K}{G_0} + \ln I_0\left(\frac{2M_K}{G_0}\right) > \ln p(C_i) - \frac{E_i}{G_0} + \ln I_0\left(\frac{2M_i}{G_0}\right) \quad \forall i \neq k$$
(5.49)

Như vậy quy tắc giải không chỉ phụ thuộc vào mức nhiễu mà còn phụ thuộc vào các tính chất của các tín hiệu. Thông thường, trong các hệ thống thực tế có khoảng nghỉ chủ động (tất cả các tín hiệu phát có năng lượng như nhau. Giả sử các tín hiệu là đồng xác suất, khi đó quy tắc giải của máy thu tối ưu có thể viết dưới dạng sau:

$$M_K > M_i \quad \forall i \neq k$$
(5.49')

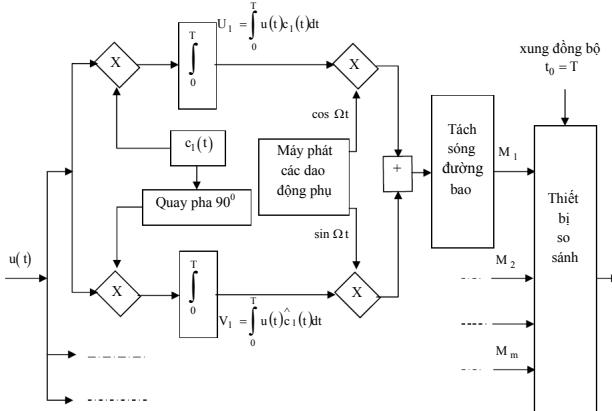
Rõ ràng là độ tin cậy của việc truyền cảng cao nếu trong điều kiện không có nhiễu M_i và M_K cảng khác nhau. Theo (5.46), giá trị M_i sẽ đạt cực tiểu bằng 0 nếu:

$$\int_0^T C_K(t) C_i(t) dt = 0; \int_0^T C_K(t) \hat{C}_i(t) dt = 0 \quad (5.50)$$

Các tín hiệu thỏa mãn (5.50) sẽ được gọi là các tín hiệu trực giao theo nghĩa chật. Các tín hiệu, các tín hiệu không giao nhau về thời gian,... là các tín hiệu trực giao theo nghĩa chật.

Như vậy, khi pha bất định, các tín hiệu trực giao theo nghĩa chật sẽ là các tín hiệu tối ưu.

Để đơn giản, ta sẽ vẽ sơ đồ giải theo (5.49').



Hình 5.9

5.5.5. So sánh thu kết hợp với thu không kết hợp

Để cụ thể, ta xét vấn đề này trong các hệ thống tin dùng tín hiệu hai phân, trực giao (chật), có nghĩa chủ động. Với giá trị đã cho của $h = \sqrt{E_c / G_0}$, xác suất sai khi thu không kết hợp sẽ được tính theo công thức sau:

$$p_s = \frac{1}{2} \exp \left\{ -\frac{h^2}{2} \right\} \quad (5.51)$$

Ta thấy:

$$p_{skh} = \frac{1}{2} \exp \left\{ -\frac{h^2}{2} \right\} > p_{skh} = 1 - \phi(h)$$

Ví dụ 1:

Khi $h = 3$: $p_{skh} \approx 1,15 \cdot 10^{-3}$; $p_{skh} \approx 5,55 \cdot 10^{-3}$. Do đó khi chuyển từ thu kết hợp sang thu không kết hợp, p_s tăng # 5 lần ($h=3$).

Thông thường khi thiết kế hệ thống truyền tin người ta ấn định trước p_s rồi tìm h để đảm bảo p_s đó.

Ví dụ 2:

Nếu $p_s = 10^{-4}$; $h_{kh} = 3,73$; $h_{kh} = 4,12$. Vì $h^2 \sim P_c$ nên khi chuyển từ thu kết hợp

sang thu không kết hợp công suất của tín hiệu phải tăng một lượng là $\left(\frac{4,12}{3,73} \right)^2 \approx 1,21$ lần.

Vậy để giữ nguyên xác suất sai $p_s = 10^{-4}$ khi thu không kết hợp, phải tăng 21% công suất so với thu kết hợp. Người ta vẫn dùng cách thu không kết hợp vì thu kết hợp đòi thiết bị phức tạp và thực hiện kỹ thuật cũng phức tạp. Do đó về mặt kinh tế, xét đến cùng thu không kết hợp vẫn tiết kiệm hơn.

5.5.6. Chú thích

Ta không xét lý tối ưu các tín hiệu có biên độ và tần số biến đổi ngẫu nhiên vì nếu dùng tín hiệu giải hẹp thì bao và tần số của nó có thể xem như đã biết trước chính xác.

Đối với các tín hiệu giải rộng thì vấn đề phải xét dày dặn hơn, khi đó ta phải xét việc xử lý tối ưu các tín hiệu có biên độ và tần số thay đổi ngẫu nhiên.

5.6. MÃ KHỐI KHÔNG GIAN, THỜI GIAN (STBC).

5.6.1. Kỹ thuật thu phân tách.

Tín hiệu nhận được ở máy thu:

$$y_1 = h_1 x + n_1$$

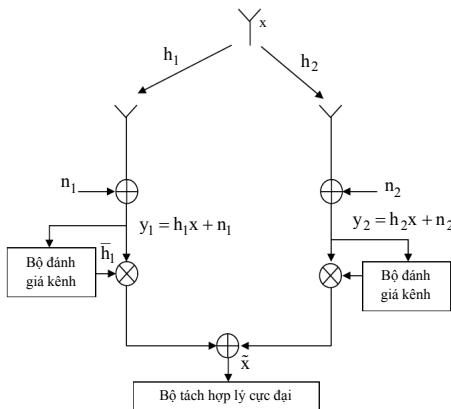
$$y_2 = h_2 x + n_2$$

$$h_1 = |h_1| e^{j\theta_1} \quad h_2 = |h_2| e^{j\theta_2}$$

Giả sử ta có thông tin đầy đủ về kênh (qua bộ đánh giá kênh). Khi đó ta có thể loại bỏ tác động của kênh tạo ra tín hiệu kết hợp ở đầu vào bộ tách hợp lý cực đại như sau:

$$\tilde{x} = \bar{h}_1 y_1 + \bar{h}_2 y_2$$

$$\begin{aligned}\tilde{x} &= \bar{h}_1 h_1 y_1 + \bar{h}_1 n_1 + \bar{h}_2 h_2 y_2 + \bar{h}_2 n_2 \\ &= (\lvert h_1 \rvert^2 + \lvert h_2 \rvert^2) x + \bar{h}_1 n_1 + \bar{h}_2 n_2\end{aligned}$$



Hình 5.10: Kỹ thuật thu phân tập dùng hai máy thu

Dựa trên khoảng cách Euclide giữa \tilde{x} và tất cả các tín hiệu phát có thể có, bộ tách hợp lý cực đại sẽ cho ra quyết định hợp lý nhất về tín hiệu đã phát. Quy tắc quyết định đơn giản ở đây là chọn tín hiệu x_i và chỉ nếu :

$$d(\tilde{x}, x_i) \leq d(\tilde{x}, x_j) \quad \forall i \neq j \quad (5.52)$$

Ở đây $d(A, B)$ là khoảng cách Euclide giữa các tín hiệu A và B

Từ (5.52) ta thấy rằng tín hiệu đã phát chính là tín hiệu có khoảng cách Euclide cực tiểu đối với tín hiệu kết hợp \tilde{x}

5.6.2. Mã khói không gian – thời gian dựa trên hai máy phát \mathbf{G}_2

Đây chính là sơ đồ STBC đơn giản nhất do Alamouti đề xuất (5.52) sử dụng hai máy phát. Ma trận phát được xác định như sau:

$$\mathbf{G}_2 = \begin{pmatrix} x_1 & x_2 \\ -\bar{x}_2 & \bar{x}_1 \end{pmatrix} \quad (5.53)$$

Việc mã hóa kết hợp và quá trình phát được nêu trong bảng sau:

Khe thời gian T	Anten	
	Tx ₁	Tx ₂
1	x ₁	x ₂
2	- \bar{x}_2	\bar{x}_1

Ở mỗi khe thời gian có hai tín hiệu thu đồng thời phát từ hai anten.

Ví dụ: Ở khe thời gian thứ nhất ($T=1$), tín hiệu x_1 được phát từ anten Tx₁, đồng thời anten Tx₂ cũng phát tín hiệu x_2 , các tín hiệu $-\bar{x}_2$ và \bar{x}_1 được đồng thời phát từ các anten Tx₁ và Tx₂ (ở đây \bar{x}_1 và \bar{x}_2 là các tín hiệu liên hợp của các tín hiệu x_1 và x_2)

5.6.2.1. STBC \mathbf{G}_2 dùng một máy thu

Giả sử ta có:

$$h_1 = h_1(T=1) = h_1(T=2)$$

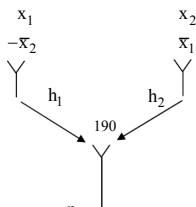
$$h_2 = h_2(T=1) = h_2(T=2)$$

Các mẫu tạp âm độc lập cộng vào ở máy thu ở mỗi khe thời gian và bởi vậy tín hiệu nhận được có thể biểu diễn như sau:

$$y_1 = h_1 x_1 + h_2 x_2 + n_1 \quad (5.54)$$

$$y_2 = -h_1 \bar{x}_2 + h_2 \bar{x}_1 + n_2 \quad (5.55)$$

y₁ sẽ nhận được trước tiên, sau đó là y₂



Tín hiệu y_1 chứa các tín hiệu được phát x_1 và x_2 , còn tín hiệu y_2 chứa các thành phần liên hợp của chúng. Để xác định các dấu đã phát ta phải tách các tín hiệu x_1 và x_2 từ các tín hiệu nhận được y_1 và y_2 . Bởi vậy cả hai tín hiệu y_1 và y_2 phải được đưa qua bộ kết hợp. Bộ kết hợp thực hiện xử lý để tách các tín hiệu x_1 và x_2 .

Đặc biệt, để tách x_1 ta kết hợp y_1 và y_2 như sau:

$$\begin{aligned}\tilde{x}_1 &= \bar{h}_1 y_1 + h_2 \bar{y}_2 \\ &= \bar{h}_1 h_1 x_1 + \bar{h}_1 h_2 x_2 + \bar{h}_1 n_1 - h_2 \bar{h}_1 x_2 + h_2 \bar{h}_2 \bar{x}_1 + h_2 \bar{n}_2 \quad (5.56) \\ &= \left(|h_1|^2 + |h_2|^2 \right) x_1 + \bar{h}_1 n_1 + h_2 \bar{n}_2\end{aligned}$$

Tương tự, đối với tín hiệu x_2 ta thực hiện như sau:

$$\begin{aligned}\tilde{x}_2 &= \bar{h}_2 y_1 + h_1 \bar{y}_2 \\ &= \bar{h}_2 h_1 x_1 + \bar{h}_2 h_2 x_2 + \bar{h}_2 n_1 + h_1 \bar{h}_1 x_2 - h_1 \bar{h}_2 x_1 - h_1 \bar{n}_2 \quad (5.57) \\ &= \left(|h_1|^2 + |h_2|^2 \right) x_2 + \bar{h}_2 n_1 - h_1 \bar{n}_2\end{aligned}$$

Từ (5.56) và (5.57) ta có thể thấy rằng ta đã tách được các tín hiệu x_1 và x_2 bằng cách phép cộng và nhân đơn giản. Từ tính trực giao có trong (5.53) ta thấy tín hiệu không mong muốn x_2 được loại bỏ khỏi (5.56) và ngược lại tín hiệu không mong muốn x_1 được loại bỏ khỏi (5.57).

5.6.2.2. STBC G_2 dùng hai máy thu

Ở máy thu thứ nhất Rx₁ ta có:

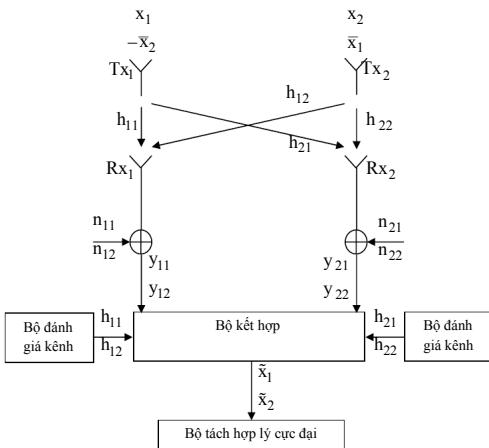
$$y_{11} = h_{11}x_1 + h_{12}x_2 + n_{11} \quad (5.58)$$

$$y_{12} = -h_{11}\bar{x}_2 + h_{12}\bar{x}_1 + n_{12} \quad (5.59)$$

Ở máy thu thứ hai Rx₂ ta có:

$$y_{21} = h_{21}x_1 + h_{22}x_2 + n_{21} \quad (5.60)$$

$$y_{22} = -h_{21}\bar{x}_2 + h_{22}\bar{x}_1 + n_{22} \quad (5.61)$$



Hình 5.12: STBC G_2 dùng hai máy thu

Tổng quát ta có thể dùng q máy thu, khi đó tín hiệu nhận được ở máy thu thứ i có dạng:

$$\begin{aligned} y_{i1} &= h_{i1}x_1 + h_{i2}x_2 + n_{i1} & i = 1, q \\ y_{i2} &= -h_{i1}\bar{x}_2 + h_{i2}\bar{x}_1 + n_{i2} \end{aligned}$$

Các tín hiệu nhận được sẽ kết hợp để tách các tín hiệu đã phát x_1 và x_2 từ các tín hiệu thu được $y_{11}, y_{12}, y_{21}, y_{22}$ như sau:

$$\tilde{x}_1 = \bar{h}_{11}y_{11} + h_{12}\bar{y}_{12} + \bar{h}_{21}y_{21} + h_{22}\bar{y}_{22} \quad (5.62)$$

$$\tilde{x}_2 = \bar{h}_{12}y_{11} - h_{11}\bar{y}_{12} + \bar{h}_{23}y_{21} - h_{21}\bar{y}_{22} \quad (5.63)$$

Tiếp tục biến đổi ta có:

$$\begin{aligned} \tilde{x}_1 &= \left(|h_{11}|^2 + |h_{12}|^2 + |h_{21}|^2 + |h_{22}|^2 \right) x_1 + \\ &\quad + \bar{h}_{11}n_{11} + h_{12}\bar{n}_{12} + \bar{h}_{21}n_{21} + h_{22}\bar{n}_{22} \end{aligned} \quad (5.64)$$

$$\begin{aligned} \tilde{x}_2 &= \left(|h_{11}|^2 + |h_{12}|^2 + |h_{21}|^2 + |h_{22}|^2 \right) x_2 + \\ &\quad + \bar{h}_{12}n_{11} - h_{11}\bar{n}_{12} + \bar{h}_{22}n_{21} - h_{21}\bar{n}_{22} \end{aligned} \quad (5.65)$$

Mở rộng cho q máy thu ta có:

$$\tilde{x}_1 = \sum_{i=1}^q \left[\left(|h_{i1}|^2 + |h_{i2}|^2 \right) x_1 + \bar{h}_{i1}n_{i1} + h_{i2}\bar{n}_{i2} \right] \quad (5.66)$$

$$\tilde{x}_2 = \sum_{i=1}^q \left[\left(|h_{i1}|^2 + |h_{i2}|^2 \right) x_2 + \bar{h}_{i2}n_{i1} - h_{i1}\bar{n}_{i2} \right] \quad (5.67)$$

Nhận xét: Trong (5.66) tín hiệu x_1 được nhân với một thành phần có liên quan đến biên độ phadinh là $|h_{11}|^2 + |h_{12}|^2$. Để thu nhận tín hiệu \tilde{x}_1 với độ tin cậy cao các biên độ của đáp ứng xung của kênh h_{ij} phải lớn. Trong (5.66) ta có thể thấy rằng có hai thành phần biên độ phadind tức là có hai đường độc lập để phát cho dấu x_1 . Bởi vậy nếu một đường bị suy giảm thì đường còn lại vẫn có thể cung cấp được x_1 với độ tin cậy cao.

BÀI TẬP

5.1. Tại lối ra của bộ khuếch đại trung gian của một máy thu các tín hiệu mang điều biến có thể hiện:

$$x(t) = \lambda \cdot S_1(t + \varphi_1) + (1 - \lambda) \cdot S_2(t + \varphi_2) + \xi(t)$$

Trong đó $\xi(t)$ là tạp âm chuẩn, dạng: $\xi(t) = X(t)\cos\omega_0t + Y(t)\sin\omega_0t$, có kỳ vọng bằng không và hàm tương quan bằng: $B_\xi(\tau) = \sigma_\xi^2 \rho(\tau) \cos\omega_0\tau$.

Còn $S_i(t, \varphi_i)$ là tín hiệu manup điều biến:

$$\begin{aligned} S_1(t, \varphi_1) &= U_m \cos(\omega_0 t + \varphi_1) \\ S_2(t, \varphi_2) &= 0 \end{aligned} \quad \left\{ \begin{array}{l} 0 \leq t \leq T \\ \end{array} \right.$$

Pha đầu φ_1 là một đại lượng ngẫu nhiên, phân bố đều trong khoảng $[-\pi, \pi]$. Tham số λ cũng là đại lượng ngẫu nhiên trong khoảng $[0, T]$, nó nhận các giá trị $\lambda = \lambda_1 = 1$ hoặc $\lambda = \lambda_0 = 0$ với các xác suất tiên nghiệm bằng:

$p(\lambda_1) = p(S_1) = p(\lambda_0) = p(S_2) = \frac{1}{2}$. Biết rằng $\lambda = \lambda_1 = 1$ khi giá trị đường bao ở đầu ra bộ tách sóng tuyến tính vượt quá ngưỡng H_0 . Trong trường hợp ngược lại thì $\lambda = \lambda_0 = 0$. Tính:

a. Ngưỡng tối ưu H_0 để đảm bảo cực tiểu hóa xác suất sai tông cộng.

b. Xác suất sai tông cộng ứng với ngưỡng H_0 đó.

5.2. Tại đầu vào bộ lọc tuyến tính tác động tín hiệu:

$$x(t) = s(t) + n(t)$$

Trong đó $n(t)$ là tạp âm trắng, chuẩn, dừng. Còn $s(t)$ là xung thị tần độc lập với $n(t)$ và có dạng:

$$s(t) = \begin{cases} A e^{A(t-T)} & t \leq T \\ 0 & t > T \end{cases}$$

Tìm hàm truyền của bộ lọc sao cho tỷ số tín trên tạp ở đầu ra của bộ lọc đạt cực đại. Tính $a = \frac{s_{ra \max}(t)}{\sigma_{ra}}$.

5.3. Xác định hàm truyền của bộ lọc FH với tín hiệu dạng:

$$S(t) = A \exp \left\{ - \left(\frac{2t}{\tau_x} \right)^2 \right\}$$

Trong đó τ_x là thời hạn của xung ở mức A/e .

5.4. Tìm sơ đồ khối của bộ lọc FH với xung thị tần chữ nhật dạng sau:

$$s(t) = \begin{cases} A & 0 \leq t \leq \tau_x \\ 0 & \forall t > \tau_x, t < 0 \end{cases}$$

Tính tỷ số tín/ tạp ở đầu ra bộ lọc này.

5.5. Chúng minh rằng máy thu tối ưu đảm bảo khoảng cách từ vecto tín hiệu nhận được tối vecto tín hiệu phát đạt cực tiểu chính là máy thu tối ưu đảm bảo xác suất sai bé nhất.

5.6. Ở đầu vào một mạch tích phân RC, tác động một tín hiệu dạng:

$$x(t) = s(t) + n(t)$$

Trong đó $n(t)$ là tạp âm trắng, chuẩn, dừng có mật độ phô:

$$S_n(f) = G_0 / 2$$

Còn $s(t)$ là xung thị tần chữ nhật dạng:

$$s(t) = \begin{cases} U_m & 0 \leq t \leq \tau_x \\ 0 & \forall t < 0, t > \tau_x \end{cases}$$

Ký hiệu $a = \frac{s_{ra\max}(t)}{\sigma_{ra}}$ là tỷ số giữa giá trị cực đại của tín hiệu trên giá trị trung bình bình phương của tạp âm ở đầu ra.

- a. Tìm sự phụ thuộc giữa a với độ rộng xung τ_x và giải thông tạp âm của mạch Δf_n .
- b. Tìm sự phụ thuộc giữa τ_x và giải năng lượng tạp âm tối ưu của mạch để trị số a đạt max.

PHỤ LỤC

BÁT ĐẲNG THỨC BUNHIACOVSKI-SCHWAZT

Định lý: Nếu $F(x)$ và $\phi(x)$ là các hàm phức thỏa mãn điều kiện:

$$\int_{-\infty}^{\infty} |F(x)|^2 dx < \infty \quad \int_{-\infty}^{\infty} |\phi(x)|^2 dx < \infty \quad (x \text{ biến thực})$$

thì ta có:

$$\left| \int_{-\infty}^{\infty} F(x)\phi(x)dx \right|^2 \leq \int_{-\infty}^{\infty} |F(x)|^2 dx \cdot \int_{-\infty}^{\infty} |\phi(x)|^2 dx$$

Chứng minh:

$$\text{Đặt } \phi(x) = \frac{\phi^*(x)}{\sqrt{\int_{-\infty}^{\infty} |\phi(x)|^2 dx}} \quad (a)$$

(Đấu * là ký hiệu liên hợp phức)

$$\text{và } \alpha = \int_{-\infty}^{\infty} \phi^*(x)F(x)dx \quad (b)$$

$$\text{Ta có: } [F(x) - \alpha\phi(x)][F^*(x) - \alpha^*\phi^*(x)] = |F(x) - \alpha\phi(x)|^2 \geq 0 \quad (c)$$

$$\text{Theo (a) ta có: } \int_{-\infty}^{\infty} |\phi(x)|^2 dx = 1$$

$$\text{Theo (b) ta có: } \int_{-\infty}^{\infty} \phi(x)F^*(x)dx = \alpha^*$$

Khi đó ta có thể viết lại (c) như sau:

$$\int_{-\infty}^{\infty} |F(x)|^2 dx + |\alpha|^2 - \alpha\alpha^* - \alpha^*\alpha \geq 0$$

$$\text{Hay } \int_{-\infty}^{\infty} |F(x)|^2 dx \geq |\alpha|^2 \quad (d)$$

Thay (a) và (b) vào (d) ta có:

$$\int_{-\infty}^{\infty} |F(x)|^2 dx \geq \frac{\left| \int_{-\infty}^{\infty} \varphi(x) F(x) dx \right|^2}{\int_{-\infty}^{\infty} |\varphi(x)|^2 dx}$$

BIÉN ĐÔI HILBERT

Định lý:

Cho tín hiệu $s(t)$ và $S(j\omega)$ là biến đổi Fourier của nó. Khi đó tín hiệu $\hat{s}(t)$ có phô:

$$\hat{s}(j\omega) = S(j\omega) e^{-j\frac{\pi}{2}\text{sign}\omega}$$

(tất cả các thành phần phô $\hat{s}(t)$ đều dịch pha đi một lượng bằng $-\frac{\pi}{2}$) có thể biểu diễn theo

$s(t)$ thông qua biến đổi tích phân sau:

$$\hat{s}(t) = -\frac{1}{\pi} \int_{-\infty}^{\infty} \frac{s(\tau)}{t-\tau} d\tau$$

Chứng minh: Ta có:

$$\hat{s}(j\omega) = S(j\omega) e^{-j\frac{\pi}{2}\text{sign}\omega} = S(j\omega) \left[\cos\left(\frac{\pi}{2}\text{sign}\omega\right) - j\sin\left(\frac{\pi}{2}\text{sign}\omega\right) \right]$$

$$\text{Trong đó: } \text{sign}\omega = \begin{cases} 1 & \text{khi } \omega > 0 \\ 0 & \omega = 0 \\ -1 & \omega < 0 \end{cases}$$

$$\cos\left(\frac{\pi}{2}\text{sign}\omega\right) = \begin{cases} 1 & \text{khi } \omega > 0 \\ 0 & \omega = 0 \\ -1 & \omega < 0 \end{cases}$$

$$\sin\left(\frac{\pi}{2}\operatorname{sign}\omega\right) = \operatorname{sign}\omega$$

Theo biến đổi ngược Fourier ta có:

$$\hat{s}(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{S}(j\omega) e^{j\omega t} d\omega = -\frac{1}{2\pi} \int_{-\infty}^{\infty} j \operatorname{sign}\omega S(j\omega) e^{j\omega t} d\omega \quad (a)$$

$$(Để ý rằng \frac{1}{2\pi} \int_{-\infty}^{\infty} S(j\omega) \cos\left(\frac{\pi}{2} \operatorname{sign}\omega\right) e^{j\omega t} d\omega = 0)$$

Mặt khác ta có:

$$\begin{aligned} & \int_{-\infty}^{\infty} \frac{e^{-j\omega\tau}}{\tau} d\tau = \underbrace{\int_{-\infty}^0 \frac{\cos\omega\tau}{\tau} d\tau}_{0} - \int_{-\infty}^{\infty} \frac{\sin\omega\tau}{\tau} d\tau \\ & \Rightarrow \int_{-\infty}^{\infty} \frac{e^{-j\omega\tau}}{\tau} d\tau = -2j \int_0^{\infty} \frac{\sin\omega\tau}{\tau} d\tau = -2j \operatorname{sign}\omega \int_{-\infty}^{\infty} \frac{\sin x}{x} dx \\ & \text{Vì } \int_{-\infty}^{\infty} \frac{\sin x}{x} dx = \frac{\pi}{2} \text{ nên ta có: } \int_{-\infty}^{\infty} \frac{e^{-j\omega\tau}}{\tau} d\tau = -j\pi \end{aligned} \quad (b)$$

Thay (b) vào (a) ta được:

$$\begin{aligned} \hat{s}(t) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} S(j\omega) e^{j\omega t} \left[\frac{1}{\pi} \int_{-\infty}^{\infty} \frac{e^{-j\omega\tau}}{\tau} d\tau \right] d\omega \\ &= \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{1}{\tau} \left[\int_{-\infty}^{\infty} S(j\omega) e^{j\omega(t-\tau)} d\omega \right] d\tau \\ &= \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{s(t-\tau)}{\tau} d\tau = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{s(\tau)}{t-\tau} d\tau \end{aligned}$$

ĐỊNH LÝ KACHENHICOV

Định lý: Nếu phô của hàm $s(t)$ không chứa các thành phần tần số lớn hơn F_m thì hàm này hoàn toàn được xác định bởi các giá trị mẫu của nó lấy ở các thời điểm cách nhau một khoảng $\Delta t \leq \frac{1}{2F_m}$

Chứng minh:

Ta sẽ chứng tỏ rằng có thể khôi phục lại được $s(t)$ từ:

$$s_\Delta(t) = s(t)\delta_\Delta(t) \quad (\text{hình C.1.c}) \quad (\text{a})$$

$$\delta_\Delta(t) = \sum_{n=-\infty}^{\infty} \delta(t - n\Delta t) \quad (\text{hình C.1.b}) \quad (\text{b})$$

$$\Delta t = \frac{1}{F_0} \leq \frac{1}{2F_m} ; \omega_0 = 2\pi F_0 ; \omega_m = 2\pi F_m$$

$\delta_\Delta(t)$ là một hàm tuần hoàn có chu kỳ Δt , vì vậy ta có thể biểu diễn nó bằng chuỗi Fourier sau:

$$\delta_\Delta(t) = \sum_{n=-\infty}^{\infty} s_n e^{jn\omega_0 t}$$

$$\text{trong đó } s_n = \frac{1}{\Delta t} \int_{-\Delta t/2}^{\Delta t/2} \delta_\Delta(t) e^{-jn\omega_0 t} dt$$

Trong khoảng $\left(-\frac{\Delta t}{2}, \frac{\Delta t}{2}\right)$ hàm $\delta_\Delta(t)$ chính là hàm $\delta(t)$

$$\text{Do đó: } s_n = \frac{1}{\Delta t} \int_{-\Delta t/2}^{\Delta t/2} \delta(t) e^{-jn\omega_0 t} dt$$

$$\text{Theo tính chất lọc của } \delta \text{ ta có } s_n = \frac{1}{\Delta t} \Rightarrow \delta_\Delta(t) = \frac{1}{\Delta t} \sum_{n=-\infty}^{\infty} e^{jn\omega_0 t}$$

Ta thấy rằng dây xung $\delta_\Delta(t)$ gồm các thành phần dao động điều hòa ở các tần số $\omega = 0, \pm\omega_0, \pm 2\omega_0, \dots$

Do đó ta có thể biểu diễn được phô của $\delta_\Delta(t)$ dưới dạng sau:

$$\overset{\cdot}{\int}_{\delta_\Delta}(\omega) = \frac{2\pi}{\Delta t} \sum_{n=-\infty}^{\infty} \delta(\omega - n\omega_0) \quad (\text{Hình C.1.e}) \quad (\text{c})$$

Theo tính chất của biến đổi Fourier phô của $s_\Delta(t)$ được tính theo tích chập sau:

$$\dot{S}_\Delta(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \dot{S}(u) \int_{-\Delta t}^{\Delta t} (\omega - u) du$$

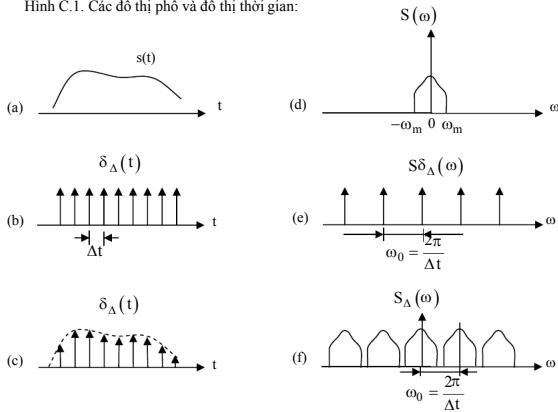
Trong đó: $\dot{S}(\omega)$ là phô của $s(t)$

$$\begin{aligned}\dot{S}_\Delta(\omega) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \dot{S}(u) \cdot \frac{2\pi}{\Delta t} \sum_{n=-\infty}^{\infty} \delta[(\omega - n\omega_0) - u] du \\ &= \frac{1}{\Delta t} \sum_{n=-\infty}^{\infty} \int_{-\infty}^{\infty} \dot{S}(u) \delta[(\omega - n\omega_0) - u] du\end{aligned}$$

Theo tính chất lọc của δ ta có:

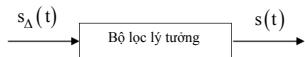
$$\dot{S}_\Delta(\omega) = \frac{1}{\Delta t} \sum_{n=-\infty}^{\infty} S(\omega - n\omega_0) \quad (\text{Hình C.1.f}) \quad (d)$$

Hình C.1. Các đồ thị phô và đồ thị thời gian:



Hình C.1

Từ (d) và hình C.1 ta thấy rằng phô của $S_\Delta(\omega)$ lặp lại một cách tuần hoàn dạng phô của $s(t)$. Dùng một bộ lọc có đặc tính tần số dạng chữ nhật lý tưởng (đường nét nét trên hình C.1.f ta có thể khôi phục lại được $s(t)$)

**LUẬT PHÂN BỐ CHUẨN**

Luật phân bố xác suất: $\phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{t^2}{2}} dt$

Mật độ phân bố xác suất: $w(x) = \phi'(x) = \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{x^2}{2}\right\}$

x	$\phi(x)$	w(x)	x	$\phi(x)$	w(x)
0,0	0,500	0,399	1,8	0,964	0,078
0,1	0,539	0,397	1,9	0,971	0,065
0,2	0,579	0,301	2,0	0,977	0,054
0,3	0,618	0,381	2,1	0,982	0,044
0,4	0,655	0,368	2,2	0,986	0,035
0,5	0,691	0,352	2,3	0,989	0,028
0,6	0,725	0,333	2,4	0,992	0,022
0,7	0,758	0,312	2,5	0,993	0,017
0,8	0,788	0,289	2,6	0,995	0,013
0,9	0,815	0,266	2,7	0,996	0,010
1,0	0,841	0,241	2,8	0,997	0,008
1,1	0,864	0,217	2,9	0,998	0,005
1,2	0,884	0,194	3,0	0,998	0,004
1,3	0,903	0,171	3,1	0,999	0,003
1,4	0,919	0,149	3,2	0,999	0,002
1,5	0,933	0,129	3,3	0,999	0,001
1,6	0,945	0,110	3,4	0,999	0,001
1,7	0,955	0,094	3,5	0,999	0,001

LOGARIT CƠ SỐ HAI CỦA CÁC SỐ NGUYÊN TỪ 1 ĐẾN 100

x_i	$\log_2 x_i$						
0,000	4,700		5,672		6,248		
1,000	4,755		5,700		6,267		
1,585	4,807		5,728		6,285		
2,000	4,858		5,755		6,304		
2,322	4,907		5,781		6,322		
2,585	4,954		5,807		6,340		
2,807	5,000		5,833		6,357		
3,000	5,044		5,858		6,375		
3,169	5,087		5,883		6,392		
3,322	5,129		5,907		6,409		
3,459	5,170		5,931		6,426		
3,585	5,209		5,954		6,443		
3,700	5,248		5,977		6,456		
3,807	5,285		6,000		6,479		
3,907	5,322		6,022		6,492		
4,000	5,357		6,044		6,508		
4,087	5,392		6,066		6,523		
4,170	5,426		6,087		6,539		
4,248	5,459		6,108		6,555		
4,322	5,492		6,129		6,570		
4,392	5,523		6,149		6,585		
4,459	5,555		6,170		6,599		
4,523	5,585		6,190		6,615		
4,585	5,615		6,209		6,629		
4,644	5,644		6,229		6,644		

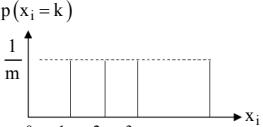
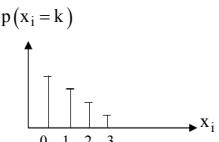
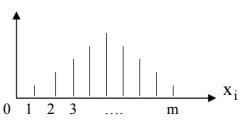
HÀM $\gamma(p) = -p \log_2 p$, HÀM $\phi(p) = -(1-p) \log_2(1-p)$, HÀM $\log_2 p$ VÀ
ENTROPIE CỦA NGUỒN NHỊ PHÂN $H(A) = \gamma(p) + \phi(p)$

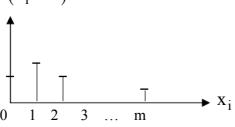
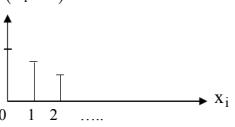
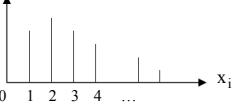
p	$-\log_2 p$	$\gamma(p)$	$H(A)$	$\phi(p)$	$-\log_2(1-p)$	$(1-p)$
6,643	0,066	0,081	0,014	0,014	0,99	
5,644	0,113	0,141	0,028	0,029	0,98	
5,059	0,152	0,194	0,042	0,044	0,97	
4,644	0,186	0,242	0,056	0,059	0,96	
4,322	0,216	0,286	0,070	0,074	0,95	
4,059	0,243	0,327	0,084	0,089	0,94	
3,936	0,268	0,366	0,097	0,105	0,93	
3,644	0,291	0,402	0,111	0,120	0,92	
3,474	0,313	0,436	0,124	0,136	0,91	
3,322	0,332	0,469	0,137	0,152	0,90	
3,184	0,350	0,499	0,150	0,168	0,89	
3,059	0,367	0,529	0,162	0,184	0,88	
2,943	0,383	0,557	0,175	0,201	0,87	
2,836	0,397	0,584	0,187	0,217	0,86	
2,737	0,411	0,610	0,199	0,234	0,85	
2,644	0,423	0,634	0,211	0,252	0,84	
2,556	0,434	0,658	0,223	0,269	0,83	
2,474	0,445	0,680	0,235	0,286	0,82	
2,396	0,455	0,701	0,246	0,304	0,81	
2,322	0,464	0,722	0,257	0,322	0,80	
2,252	0,473	0,741	0,269	0,340	0,79	
2,184	0,481	0,760	0,279	0,358	0,78	
2,120	0,488	0,778	0,290	0,377	0,77	
2,059	0,494	0,795	0,301	0,396	0,76	
2,000	0,500	0,811	0,311	0,415	0,75	

p	$-\log_2 p$	$\gamma(p)$	$H(A)$	$\phi(p)$	$-\log_2(1-p)$	$(1-p)$
---	-------------	-------------	--------	-----------	----------------	---------

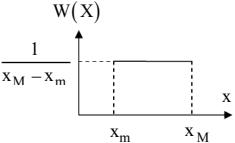
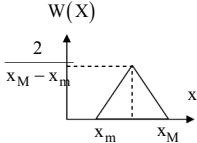
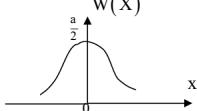
1,943	0,505	0,827	0,321	0,434	0,74
1,889	0,510	0,841	0,331	0,454	0,73
1,836	0,514	0,855	0,341	0,474	0,72
1,786	0,518	0,869	0,351	0,494	0,71
1,737	0,521	0,881	0,360	0,514	0,70
1,690	0,524	0,893	0,369	0,535	0,69
1,644	0,526	0,904	0,378	0,556	0,68
1,599	0,528	0,915	0,387	0,578	0,67
1,556	0,529	0,925	0,396	0,599	0,66
1,514	0,530	0,934	0,404	0,621	0,65
1,474	0,531	0,943	0,412	0,644	0,64
1,434	0,531	0,951	0,420	0,667	0,63
1,396	0,530	0,958	0,428	0,690	0,62
1,358	0,529	0,965	0,435	0,713	0,61
1,322	0,529	0,971	0,442	0,737	0,60
1,286	0,527	0,976	0,449	0,761	0,59
1,252	0,526	0,981	0,455	0,786	0,58
1,217	0,523	0,986	0,462	0,811	0,57
1,184	0,521	0,989	0,468	0,836	0,56
1,152	0,518	0,993	0,474	0,862	0,55
1,120	0,515	0,995	0,480	0,889	0,54
1,1089	0,512	0,997	0,485	0,916	0,53
1,059	0,508	0,999	0,491	0,943	0,52
1,029	0,504	0,999	0,495	0,971	0,51
1,000	0,500	1,000	0,500	1,000	0,50

ENTROPIE H(X) CỦA CÁC LUẬT PHÂN BỐ RỜI RẠC.

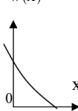
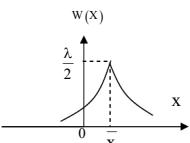
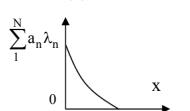
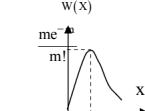
Luật phân bố	Biểu thức giải tích và đồ thị	Entropie H(X)
1. Phân bố đều	$p(x_i = k) = \begin{cases} \frac{1}{m} & 1 \leq x_i \leq m \\ 0 & m < x_i < 1 \end{cases}$ $p(x_i = k)$ 	$H(X) = \log m$
2. Phân bố bội	$p(x_i = K) = \begin{cases} p(1-p)^{k-1} & x_i > 0 \\ 0 & x_i \leq 0 \end{cases}$ $p(x_i = k)$ 	$H(X) = -\frac{p \log mp + (1-p) \log (1-p)}{p}$
3. Phân bố nhị thức Bernoulli	$p(x_i = K) = \begin{cases} C_m^k p^k (1-p)^{m-k} & 0 \leq x_i \leq m \\ 0 & 0 > x_i > m \end{cases}$ $p(x_i = k)$ 	$H(X) = -m [p \log p - (1-p) \log (1-p)] - \sum_{k=1}^{m-1} C_m^k p^k (1-p)^{m-k} \log C_m^k$

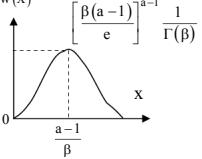
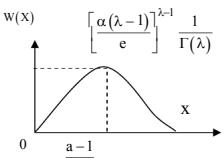
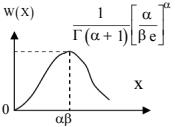
4. Phân bố siêu bội	$p(x_i = k) = \begin{cases} \frac{C_m^k C_{N-m}^{r-k}}{C_N^r} & 0 \leq x_i \leq m \\ 0 & 0 > x_i > m \end{cases}$ $p(x_i = k)$ 	$H(X) = \log C_N^r - \frac{1}{C_N^r} \cdot \sum_{k=1}^{m-1} C_m^k C_{N-m}^{r-k} \log C_m^k - \frac{1}{C_N^r} \sum_{k=l}^{m-1} C_m^k C_{N-m}^{r-k} \log C_{N-m}^{r-k}$
5. Phân bố Poisson	$p(x_i = k) = \begin{cases} \frac{\lambda^k}{K!} e^{-\lambda} & x_i > 0 \\ 0 & x_i \leq 0 \end{cases}$ $p(x_i = k)$ 	$H(X) = \lambda \log \frac{e}{\lambda} + \sum_{k=1}^{\infty} \frac{\lambda^k e^{-\lambda}}{K!} \log (K!)$
6. Phân bố Polya	$P(x_i = K) = \frac{P_0 \left(\frac{\lambda}{1 + \alpha \lambda} \right)^k}{\frac{(1 + \alpha) \dots [1 + (K-1)\alpha]}{0} \quad x_i > 0} \quad x_i \leq 0$ $p^0 = p(0) = (1 + \alpha \lambda)^{-\frac{1}{\alpha}}$ $p(x_i = k)$ 	$H(x') = -\lambda \log \lambda + \frac{1 + \alpha \lambda}{\alpha} \cdot \log(1 + \alpha \lambda) - \sum_{k=1}^{\infty} P_0 \left(\frac{\lambda}{1 + \alpha \lambda} \right)^k \cdot \frac{1(1 + \alpha) \dots [1 + (K-1)\alpha]}{K!} \cdot \log \frac{1(1 + \alpha) \dots [1 + (K-1)\alpha]}{K!}$

ENTRPIE VI PHÂN H(X) CỦA CÁC LUẬT PHÂN BỐ LIÊN TỤC.

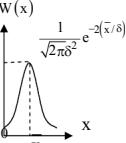
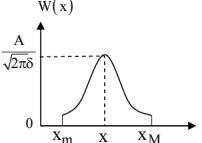
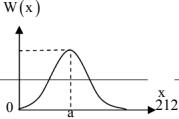
Luật phân bố	Biểu thức giải tích và đồ thị	Entropie H(X)
1. Phân bố đều	$W(X) = \begin{cases} \frac{1}{x_M - x_m} & x \in [x_m, x_M] \\ 0 & x \notin [x_m, x_M] \end{cases}$ 	$H(X) = \log m$
2. Phân bố tam giác (Simson)	$W(X) = \begin{cases} \frac{4(x - x_m)}{(x_M - x_m)^2} & x \in [x_m, \frac{x_m + x_M}{2}] \\ \frac{4(x_M - x)}{(x_M - x_m)^2} & x \in [\frac{x_m + x_M}{2}, x_M] \\ 0 & x \notin [x_m, x_M] \end{cases}$ 	$h(x) = \log \frac{(x_M - x_m)\sqrt{e}}{2}$
3. Phân bố sech ² x	$W(x) = \frac{a}{2\cosh^2 x} = \frac{a}{2} \operatorname{sech}^2 x$ 	$h(x) = \log \frac{e^2}{2a}$

4. Phân bố arcsin x	$W(x) = \begin{cases} \frac{1}{\pi} \cdot \frac{1}{\sqrt{a^2 - x^2}} & x \in (-a, a) \\ 0 & -a > x > a \end{cases}$ <p style="text-align: center;">W(x)</p>	$h(x) = \log \pi + \frac{1}{\pi} \int_0^x \frac{1}{\sqrt{a^2 - x^2}} dx$
5. Phân bố Cauchy	$W(x) = \frac{a}{\pi} \cdot \frac{1}{(x - \bar{x})^2 + a^2}$ <p style="text-align: center;">W(x)</p>	$h(x) = \log 4\pi a$
6. Phân bố Maxwell	$W(x) = \begin{cases} \frac{4}{\sqrt{\pi} (2\delta^2)^{3/2}} x^2 e^{-x^2/2\delta^2} & x > 0 \\ 0 & x < 0 \end{cases}$ <p style="text-align: center;">W(x)</p>	$h(x') = \left[\frac{1}{2} \log \frac{2\pi\delta^2}{e} + C \log e \right]$ $C \approx 0,5772$ $(C - Số Euler)$

7. Phân bố mũ một phía	$W(x) = \begin{cases} \lambda e^{-\lambda x} & x > 0 \\ 0 & x \leq 0 \end{cases}$ 	$h(x) = \log - \frac{e}{\lambda}$
8. Phân bố Laplace (phân bố mũ hai phía)	$W(x) = \frac{\lambda}{2} e^{-\lambda x-\bar{x} }$ 	$h(x) = \log \frac{2e}{\lambda}$
9. Phân bố siêu mũ	$W(x) = \begin{cases} \sum_{n=1}^N a_n \lambda_n e^{-\lambda_n n^x} & x > 0 \\ 0 & x \leq 0 \end{cases}$ 	$h(x) = - \sum_{n=1}^N a_n \lambda_n \int_0^\infty e^{-\lambda_n n^x} \cdot \log \sum_{n=1}^N a_n \lambda_n e^{-\lambda_n n^x} dx$
10. Phân bố mũ – lũy thừa	$W(x) = \begin{cases} \frac{x^m}{m!} e^{-x} & x > 0 \\ 0 & x \leq 0 \end{cases}$ 	$h(x) = \log m! + \log e - e - m \log e \left[\sum_{k=2}^m \frac{1}{k} - C \right]$ $C \approx 0,5772$ (C – Số Euler)

11. Phân bố Erlang	$W(x) = \begin{cases} \frac{\beta^a x^a - 1}{(a-1)!} e^{-\beta x} & x > 0 \\ 0 & x < 0 \end{cases}$ <p style="text-align: center;">$a = 1, 2, 3, \dots$</p> 	$h(x) = \log[(a-1)!] - \log \beta +$ $+ \left\{ a - (a-1) [\ln \Gamma(a)] \right\} \log e$ $[\ln \Gamma(a)]' = \psi(a)$ <p>$\psi(a)$ - Hàm psi của Euler</p>
12. Phân bố Pearson	$W(x) = \begin{cases} \frac{\alpha^\lambda x^{\lambda-1}}{\Gamma(\lambda)} e^{-\beta x} & x > 0 \\ 0 & x < 0 \end{cases}$ <p style="text-align: center;">$\lambda = \frac{n}{2}$ ($n = 1, 2, 3, \dots$)</p> 	$h(x) = -\log \Gamma(\lambda) - \log \alpha +$ $+ \left\{ \lambda - (\lambda - 1) [\ln \Gamma(\lambda)] \right\} \log e$ $[\ln \Gamma(\lambda)]' = \psi(\lambda)$
13. Phân bố Gamma	$W(x) = \begin{cases} \frac{1}{\beta^{\alpha+1} \Gamma(\alpha+1)} x^\alpha e^{-x/\beta} & x > 0 \\ 0 & x < 0 \end{cases}$ <p style="text-align: center;">$\alpha > -1, \beta > 0$</p> 	$h(x) = \log \Gamma(\alpha+1) - \alpha \log e.$ $- [\ln \Gamma(\alpha+1)]' + (\alpha+1) \cdot \log e + \log \beta$ $[\ln \Gamma(\alpha+1)]' = \psi(\alpha+1)$

14. Phân bố Weibull	$W(x) = \begin{cases} \alpha \beta x^{\alpha-1} e^{-\beta x^\alpha} & x > 0 \\ 0 & x \leq 0 \end{cases}$ $W(x) \quad \alpha > 0, \beta > 0$	$h(x) = \log e \left[1 + \frac{\alpha-1}{\alpha} (C + \ln \beta) \right] -$ $-\log \alpha \beta$ $C \approx 0,5772$
15. Phân bố chuẩn	$W(x) = \frac{1}{\sqrt{2\pi}\delta} \exp\left\{-\frac{(x-\bar{x})^2}{2\delta^2}\right\}$ $W(x) \quad \frac{1}{\sqrt{2\pi}\delta}$	$h(x) = \log \left[\delta \sqrt{2\pi e} \right]$
16. Phân bố chuẩn một phía	$W(x) = \begin{cases} \sqrt{\frac{2}{\pi\delta^2}} \exp\left\{-\frac{x^2}{2\delta^2}\right\} & x > 0 \\ 0 & x < 0 \end{cases}$ $W(x) \quad \delta\sqrt{n-1}$	$h(x) = \log \left[\delta \sqrt{\frac{\pi e}{2}} \right]$
17. Phân bố Rayleigh	$W(x) = \begin{cases} \frac{x}{\delta^2} \exp\left\{-\frac{x^2}{2\delta^2}\right\} & x > 0 \\ 0 & x \leq 0 \end{cases}$ $W(x)$	$h(x) = \left(\frac{C}{2} + 1 \right) \log e$ $C \approx 0,5772$

18. Phân bố modul của đại lượng ngẫu nhiên phân bố chuẩn	$W(x) = \begin{cases} \frac{1}{\sqrt{2\pi}\delta} \left[e^{-\frac{(x-\bar{x})^2}{2\delta^2}} + e^{-\frac{(x+\bar{x})^2}{2\delta^2}} \right] & x > 0 \\ 0 & x < 0 \end{cases}$ 	$h(x) = \log \left[\delta \sqrt{\frac{\pi e}{2}} \right]$
19. Phân bố chuẩn cực	$W(X) = \begin{cases} \frac{1}{\sqrt{2\pi}\delta} \left[e^{-\frac{(x-\bar{X})^2}{2\delta^2}} + e^{-\frac{(x+\bar{X})^2}{2\delta^2}} \right] & x \in [x_m, x_M] \\ 0 & x \notin [x_m, x_M] \end{cases}$ $A = \frac{1}{\sqrt{2\pi}} \left[\int_0^{(x_m-\bar{X})/\delta} e^{-t^2/2} dt - \int_0^{(x_M-\bar{X})/\delta} e^{-t^2/2} dt \right]$ 	$h(x) = \log \left[\frac{\sqrt{2\pi}\delta}{A} \right] +$ $+ \frac{1}{2} \left[1 - A \frac{x_M - \bar{X}}{\delta}, \frac{1}{\sqrt{2\pi}} e^{-\frac{(x_m - \bar{X})^2}{2\delta^2}} - A \frac{x_m - \bar{X}}{\delta} \frac{1}{\sqrt{2\pi}} e^{-\frac{(x_m - \bar{X})^2}{2\delta^2}} \right] \log e$
20. Phân bố loga chuẩn	$W(x) = \begin{cases} \frac{1}{x\delta\sqrt{2\pi}} e^{-\frac{(\ln x - a)^2}{2\delta^2}} & x > 0 \\ 0 & x < 0 \end{cases}$ 	$h(x) = \log \left[\delta e^a \sqrt{2\pi e} \right]$

21. Phân bố modul của véc-tơ nhiều chiều	$W(x) = \begin{cases} \frac{2x^{n-1} \exp\left\{-\frac{x^2}{2\delta^2}\right\}}{\left(2\delta^2\right)^{n/2} \Gamma\left(\frac{n}{2}\right)} & x > 0 \\ 0 & x < 0 \end{cases}$ <p style="text-align: center;">$n = 1, 2, 3, \dots$</p>	$h(x) = \log \frac{\delta e^{\frac{n}{2}} \Gamma\left(\frac{n}{2}\right)}{\sqrt{2}} - \frac{n-1}{2} \log \Gamma\left(\frac{n}{2}\right)$
22. Phân bố nakagami	$W(x) = \begin{cases} \frac{2m^m x^{2m-1} \exp\left\{-\frac{mx^2}{\delta^2}\right\}}{\Gamma(m)\delta^{2m}} & x > 0 \\ 0 & x < 0 \end{cases}$	$h(x) = \log \frac{\Gamma(m)\delta e^m}{2\sqrt{m}} - \frac{2m-1}{2} [\log \Gamma(m)]$
Phân bố Beta	$W(X) = \begin{cases} \frac{12}{(x_M - x_m)^4} (x - x_m)(x_M - x)^2 & x \in [x_m, x_M] \\ 0 & x \notin [x_m, x_M] \end{cases}$	$h(x) = 1,44 \ln \frac{(x_M - x_m)}{1,26}$

	x_M	
--	-------	--

CÁC ĐA THỨC TỐI TIỂU CỦA CÁC PHẦN TỬ TRONG TRƯỜNG GF(2^m)

Sau đây là danh sách các đa thức tối thiểu nhị phân cho tất cả các phần tử trong các trường mở rộng của trường nhị phân từ GF(2^2) tới GF(2^{10}).

Các dòng ký hiệu được hiểu như sau: Dòng 3(0, 2, 3) trong mục GF(8) tương ứng với đa thức $m(X) = 1 + X^2 + X^3$ có các nghiệm là các phần tử liên hợp $\{\alpha^3, \alpha^6, \alpha^5\}$.

GF(4)

1 (0, 1, 2)

GF(8)

1 (0, 1, 3)

3 (0, 2, 3)

GF(16)

1 (0, 1, 4)

3 (0, 1, 2, 3, 4)

5 (0, 1, 2)

7 (0, 3, 4)

GF(32)

1 (0, 2, 5)

3 (0, 2, 3, 4, 5)

5 (0, 1, 2, 4, 5)

7 (0, 1, 2, 3, 5)

11 (0, 1, 3, 4, 5)

15 (0, 3, 5)

GF(64)

1 (0, 1, 6)

3 (0, 1, 2, 4, 6)

5 (1, 2, 5, 6)

7 (0, 3, 6)

9 (0, 2, 3)

11 (0, 2, 3, 5, 6)

13 (0, 1, 3, 4, 6)

15 (0, 2, 4, 5, 6)

21 (0, 1, 2)

23 (0, 1, 4, 5, 6)

27 (0, 1, 3)

31 (0, 5, 6)

GF(128)

1 (0, 3, 7)

3 (0, 1, 2, 3, 7)

5 (0, 2, 3, 4, 7)

7 (0, 1, 2, 4, 5, 6, 7)

9 (0, 1, 2, 3, 4, 5, 7)

11 (0, 2, 4, 6, 7)

13 (0, 1, 7)

15 (0, 1, 2, 3, 5, 6, 7)

19	(0, 1, 2, 6, 7)	21	(0, 2, 5, 6, 7)
23	(0, 6, 7)	27	(0, 1, 4, 6, 7)
29	(0, 1, 3, 5, 7)	31	(0, 4, 5, 6, 7)
43	(0, 1, 2, 5, 7)	47	(0, 3, 4, 5, 7)
55	(0, 2, 3, 4, 5, 6, 7)	63	(0, 4, 7)

GF(256)

1	(0, 2, 3, 4, 8)	3	(0, 1, 2, 4, 5, 6, 8)
5	(0, 1, 4, 5, 6, 7, 8)	7	(0, 3, 5, 6, 8)
9	(0, 2, 3, 4, 5, 7, 8)	11	(0, 1, 2, 5, 6, 7, 8)
13	(0, 1, 3, 5, 8)	15	(0, 1, 2, 4, 6, 7, 8)
17	(0, 1, 4)	19	(0, 2, 5, 6, 8)
21	(0, 1, 3, 7, 8)	23	(0, 1, 5, 6, 8)
25	(0, 1, 3, 4, 8)	27	(0, 1, 2, 3, 4, 5, 8)
29	(0, 2, 3, 7, 8)	31	(0, 2, 3, 5, 8)
37	(0, 1, 2, 3, 4, 6, 8)	39	(0, 3, 4, 5, 6, 7, 8)
43	(0, 1, 6, 7, 8)	45	(0, 3, 4, 5, 8)
47	(0, 3, 5, 7, 8)	51	(0, 1, 2, 3, 4)
53	(0, 1, 2, 7, 8)	55	(0, 4, 5, 7, 8)
59	(0, 2, 3, 6, 8)	61	(0, 1, 2, 3, 6, 7, 8)
63	(0, 2, 3, 4, 6, 7, 8)	85	(0, 1, 2)
87	(0, 1, 5, 7, 8)	91	(0, 2, 4, 5, 6, 7, 8)
95	(0, 1, 2, 3, 4, 7, 8)	111	(0, 1, 3, 4, 5, 6, 8)
119	(0, 3, 4)	127	(0, 4, 5, 6, 8)

GF(512)

1	(0, 4, 9)	3	(0, 4, 3, 6, 9)
5	(0, 4, 5, 8, 9)	7	(0, 3, 4, 7, 9)
9	(0, 1, 4, 8, 9)	11	(0, 2, 3, 5, 9)
13	(0, 1, 2, 4, 5, 6, 9)	15	(0, 5, 6, 8, 9)
17	(0, 1, 3, 4, 6, 7, 9)	19	(0, 2, 7, 8, 9)
21	(0, 1, 2, 4, 9)	23	(0, 3, 5, 6, 7, 8, 9)
25	(0, 1, 5, 6, 7, 8, 9)	27	(0, 1, 2, 3, 7, 8, 9)
29	(0, 1, 3, 5, 6, 8, 9)	31	(0, 1, 3, 4, 9)

35	(0, 8, 9)	37	(0, 1, 2, 3, 5, 6, 9)
39	(0, 2, 3, 6, 7, 8, 9)	41	(0, 1, 4, 5, 6, 8, 9)
43	(0, 1, 3, 6, 7, 8, 9)	45	(0, 2, 3, 5, 6, 8, 9)
47	(0, 1, 3, 4, 6, 8, 9)	51	(0, 2, 4, 6, 7, 8, 9)
53	(0, 2, 4, 7, 9)	55	(0, 2, 3, 4, 5, 7, 9)
57	(0, 2, 4, 5, 6, 7, 9)	59	(0, 1, 2, 3, 6, 7, 9)
61	(0, 1, 2, 3, 4, 6, 9)	63	(0, 2, 5, 6, 9)
73	(0, 1, 3)	75	(0, 1, 3, 4, 5, 6, 7, 8, 9)
77	(0, 3, 6, 8, 9)	79	(0, 1, 2, 6, 7, 8, 9)
83	(0, 2, 4, 8, 9)	85	(0, 1, 2, 4, 6, 7, 9)
87	(0, 2, 5, 7, 9)	91	(0, 1, 3, 6, 8)
93	(0, 3, 4, 5, 6, 7, 9)	95	(0, 3, 4, 5, 7, 8, 9)
103	(0, 1, 2, 3, 5, 7, 9)	107	(0, 1, 5, 7, 9)
109	(0, 1, 2, 3, 4, 5, 6, 8, 9)	111	(0, 1, 2, 3, 4, 8, 9)
117	(0, 1, 2, 3, 6, 8, 9)	119	(0, 1, 9)
123	(0, 1, 2, 7, 9)	125	(0, 4, 6, 7, 9)
127	(0, 3, 5, 6, 9)	171	(0, 2, 4, 5, 7, 8, 9)
175	(0, 5, 7, 8, 9)	183	(0, 1, 3, 5, 8, 9)
187	(0, 3, 4, 6, 7, 8, 9)	191	(0, 1, 4, 5, 9)
219	(0, 2, 3)	223	(0, 1, 5, 8, 9)
239	(0, 2, 3, 5, 6, 8, 9)	255	(0, 5, 9)

GF(1024)

1	(0, 3, 10)	3	(0, 1, 2, 3, 10)
5	(0, 2, 3, 8, 10)	7	(0, 3, 4, 5, 6, 7, 8, 9, 10)
9	(0, 1, 2, 3, 5, 7, 10)	11	(0, 2, 4, 5, 10)
13	(0, 1, 2, 3, 5, 6, 10)	15	(0, 1, 3, 5, 7, 8, 10)
17	(0, 2, 3, 5, 6, 8, 10)	19	(0, 1, 3, 4, 5, 6, 7, 8, 10)
21	(0, 1, 3, 5, 6, 7, 8, 9, 10)	23	(0, 1, 3, 4, 10)
25	(0, 1, 5, 8, 10)	27	(0, 1, 3, 4, 5, 6, 7, 8, 10)
29	(0, 4, 5, 8, 10)	31	(0, 1, 5, 9, 10)
33	(0, 2, 3, 4, 5)	35	(0, 1, 4, 9, 10)
37	(0, 1, 5, 6, 8, 9, 10)	39	(0, 1, 2, 6, 10)

41	(0, 2, 5, 6, 7, 8, 10)	43	(0, 3, 4, 8, 10)
45	(0, 4, 5, 9, 10)	47	(0, 1, 2, 3, 4, 5, 6, 9, 10)
49	(0, 2, 4, 6, 8, 9, 10)	51	(0, 1, 2, 5, 6, 8, 10)
53	(0, 1, 2, 3, 7, 8, 10)	55	(0, 1, 3, 5, 8, 9, 10)
57	(0, 4, 6, 9, 10)	59	(0, 3, 4, 5, 8, 9, 10)
61	(0, 1, 4, 5, 6, 7, 8, 9, 10)	63	(0, 2, 3, 5, 7, 9, 10)
69	(0, 6, 7, 8, 10)	71	(0, 1, 4, 6, 7, 9, 10)
73	(0, 1, 2, 6, 8, 9, 10)	75	(0, 1, 2, 3, 4, 8, 10)
77	(0, 1, 3, 8, 10)	79	(0, 1, 2, 5, 6, 7, 10)
83	(0, 1, 4, 7, 8, 9, 10)	85	(0, 1, 2, 6, 7, 8, 10)
87	(0, 3, 6, 7, 10)	89	(0, 1, 2, 6, 7, 8, 10)
91	(0, 2, 4, 5, 7, 9, 10)	93	(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)
101	(0, 2, 3, 5, 10)	103	(0, 2, 3, 4, 5, 6, 8, 9, 10)
105	(0, 1, 2, 7, 8, 9, 10)	107	(0, 3, 4, 5, 6, 9, 10)
109	(0, 1, 2, 5, 10)	111	(0, 1, 4, 6, 10)
115	(0, 1, 2, 4, 5, 6, 7, 8, 10)	117	(0, 3, 4, 7, 10)
119	(0, 1, 3, 4, 6, 9, 10)	121	(0, 1, 2, 5, 7, 9, 10)
123	(0, 4, 8, 9, 10)	125	(0, 6, 7, 9, 10)
127	(0, 1, 2, 3, 4, 5, 6, 7, 10)	147	(0, 2, 3, 5, 6, 7, 10)
149	(0, 2, 4, 9, 10)	151	(0, 5, 8, 9, 10)
155	(0, 3, 5, 7, 10)	157	(0, 1, 3, 5, 6, 8, 10)
159	(0, 1, 2, 4, 5, 6, 7, 9, 10)	165	(0, 3, 5)
167	(0, 1, 4, 5, 6, 7, 10)	171	(0, 2, 3, 6, 7, 9, 10)
173	(0, 1, 2, 3, 4, 6, 7, 9, 10)	175	(0, 2, 3, 7, 8, 10)
179	(0, 3, 7, 9, 10)	181	(0, 1, 3, 4, 6, 7, 8, 9, 10)
183	(0, 1, 2, 3, 8, 9, 10)	187	(0, 2, 7, 9, 10)
189	(0, 1, 5, 6, 10)	191	(0, 4, 5, 7, 8, 9, 10)
205	(0, 1, 3, 5, 7, 10)	207	(0, 2, 4, 5, 8, 9, 10)
213	(0, 1, 3, 4, 7, 8, 10)	215	(0, 5, 7, 8, 10)
219	(0, 3, 4, 5, 7, 8, 10)	221	(0, 3, 4, 6, 8, 9, 10)
223	(0, 2, 5, 9, 10)	231	(0, 1, 3, 4, 5)
235	(0, 1, 2, 3, 6, 9, 10)	237	(0, 2, 6, 7, 8, 9, 10)

239	(0, 1, 2, 4, 6, 8, 10)	245	(0, 2, 6, 7, 10)
247	(0, 1, 6, 9, 10)	251	(0, 2, 3, 4, 5, 6, 7, 9, 10)
253	(0, 5, 6, 8, 10)	255	(0, 7, 8, 9, 10)
341	(0, 1, 2)	343	(0, 2, 3, 4, 8, 9, 10)
347	(0, 1, 6, 8, 10)	351	(0, 1, 2, 3, 4, 5, 7, 9, 10)
363	(0, 2, 5)	367	(0, 2, 3, 4, 5, 8, 10)
375	(0, 2, 3, 4, 10)	379	(0, 1, 2, 4, 5, 9, 10)
383	(0, 2, 7, 8, 10)	439	(0, 1, 2, 4, 8, 9, 10)
447	(0, 3, 5, 7, 8, 9, 10)	479	(0, 1, 2, 4, 7, 8, 10)
495	(0, 1, 2, 3, 5)	511	(0, 7, 10)

TÀI LIỆU THAM KHẢO

- [1] Nguyễn Bình, Trần Thông Quế. Cơ sở lý thuyết truyền tin.
Học viện Kỹ thuật Quân sự 1985.
- [2] Nguyễn Bình, Trần Thông Quế. 100 bài tập lý thuyết truyền tin.
Học viện Kỹ thuật Quân sự 1988.
- [3] Nguyễn Bình, Trương Nhữ Tuyên, Phạm Đạo. Bài giảng Lý thuyết thông tin
Học viện Công nghệ Bưu chính Viễn thông 2000
- [4] Nguyễn Bình. Giáo trình mật mã học
Nhà xuất bản Bưu điện 2004
- [5] McEliece R.J. The theory of Information and coding.
Cambridge University Press 1985
- [6] Wilson S.G. Digital modulation and Coding. Prentice Hall. 1996
- [7] Sweeney P. Error control coding. An Introduction. Prentice Hall. 1997.
- [8] Lin S. , Costello D.J. Error control coding: Fundamentals and Applications. Prentice Hall.
2004.
- [9] Moon T.K. Error correction coding. Mathematical Methods and Algorithms. Jhon Wiley
and Son 2005.

MỤC LỤC

LỜI NÓI DÀU	1
CHƯƠNG I: NHỮNG VẤN ĐỀ CHUNG VÀ NHỮNG KHÁI NIỆM CƠ BẢN.....	3
1.1. VỊ TRÍ, VAI TRÒ VÀ SƠ LƯỢC LỊCH SỬ PHÁT TRIỂN CỦA “LÝ THUYẾT THÔNG TIN”	3
1.1.1. Vị trí, vai trò của Lý thuyết thông tin	3
1.1.2. Sơ lược lịch sử phát triển	4
1.2. NHỮNG KHÁI NIỆM CƠ BẢN - SƠ ĐỒ HỆ TRUYỀN TIN VÀ NHIỆM VỤ CỦA NÓ.....	5
1.2.1. Các định nghĩa cơ bản.....	5
1.2.2. Sơ đồ khối của hệ thống truyền tin số (Hình 1.2).....	5
1.2.3. Những chỉ tiêu chất lượng cơ bản của một hệ truyền tin	10
CHƯƠNG II: TÍN HIỆU VÀ NHIỀU.....	11
2.1. TÍN HIỆU XÁC ĐỊNH VÀ CÁC ĐẶC TRUNG VẬT LÝ CỦA CHUNG	11
2.2. TÍN HIỆU VÀ NHIỀU LÀ CÁC QUÁ TRÌNH NGẪU NHIÊN	11
2.2.1. Bản chất ngẫu nhiên của tín hiệu và nhiễu.....	11
2.2.2. Định nghĩa và phân loại nhiễu	12
2.3. CÁC ĐẶC TRUNG THỐNG KÊ CỦA TÍN HIỆU NGẪU NHIÊN VÀ NHIỀU	13
2.3.1. Các đặc trưng thống kê	13
2.3.2. Khoảng tương quan.....	15
2.4. CÁC ĐẶC TRUNG VẬT LÝ CỦA TÍN HIỆU NGẪU NHIÊN VÀ NHIỀU. BIẾN ĐỘI WIENER – KHINCHIN	16
2.4.1. Nhũng khái niệm xây dựng lý thuyết phô của quá trình ngẫu nhiên - mật độ phô công suất	16
2.4.2. Cặp biến đổi Wiener – Khinchin	18
2.4.3. Bề rộng phô công suất.....	19
2.4.4. Mở rộng cặp biến đổi Wiener – Khinchin cho trường hợp $R(\tau)$ không khả tích tuyệt đối	20
2.5. TRUYỀN CÁC TÍN HIỆU NGẪU NHIÊN QUA CÁC MẠCH VÔ TUYẾN ĐIỆN TUYẾN TÍNH	21
2.5.1. Bài toán tối thiểu	21
2.5.2. Bài toán tối đa	26
2.6. BIỂU ĐIỂN PHỨC CHO THỂ HIỆN CỦA TÍN HIỆU NGẪU NHIÊN – TÍN HIỆU GIẢI HÉP	31
2.6.1. Cặp biến đổi Hilbert và tín hiệu giải tích	31
2.6.2. Tín hiệu giải rộng và giải hép	35

2.7. BIỂU DIỄN HÌNH HỌC CHO THỂ HIỆN CỦA TÍN HIỆU NGẦU NHIÊN	37
2.7.1. Khai triển trực giao và biểu diễn vecteur của tín hiệu.....	37
2.7.2. Mật độ xác suất của vecteur ngẫu nhiên - Khoảng cách giữa hai vecteur tín hiệu.....	39
2.7.3. Khái niệm về máy thu tối ưu	43
BÀI TẬP	45
CHƯƠNG 3 - CƠ SỞ LÝ THUYẾT THÔNG TIN THỐNG KÊ	47
3.1. THÔNG TIN - LUÔNG THÔNG TIN – XÁC SUẤT VÀ THÔNG TIN – ĐƠN VỊ ĐO THÔNG TIN	47
3.1.1. Định nghĩa định tính thông tin và lượng thông tin.....	47
3.1.2. Quan hệ giữa độ bất định và xác suất.....	48
3.1.3. Xác định lượng thông tin.....	50
3.2. ENTROPYIE VÀ CÁC TÍNH CHẤT CỦA ENTROPYIE	52
3.2.1. Tính chất thông kê của nguồn rời rạc và sự ra đời của khái niệm entropyie	52
3.2.2. Định nghĩa entropyie của nguồn rời rạc	52
3.2.3. Các tính chất của entropyie một chiều của nguồn rời rạc	53
3.2.4. Entropyie của nguồn rời rạc, nhị phân	55
3.2.5. Entropyie của trường sự kiện đồng thời.....	56
3.3. ENTROPYIE CÓ ĐIỀU KIỆN. LUÔNG THÔNG TIN CHÉO TRUNG BÌNH.....	57
3.3.1. Entropyie có điều kiện về một trường tin này khi đã rõ một tin nhất định của trường tin kia	57
3.3.2. Entropyie có điều kiện về trường tin này khi đã rõ trường tin kia	58
3.3.3. Hai trạng thái cực đoan của kênh truyền tin	60
3.3.4. Các tính chất của entropyie có điều kiện.....	61
3.3.5. Lượng thông tin chéo trung bình	63
3.3.6. Tính chất của $I(A,B)$	63
3.3.7. Mô hình của kênh truyền tin có nhiễu.....	64
3.4. TỐC ĐỘ PHÁT. KHẢ NĂNG PHÁT. ĐỘ THÙA. KHẢ NĂNG THÔNG QUA CỦA KÊNH RỒI RẠC	65
3.4.1. Tốc độ phát của nguồn rời rạc	65
3.4.2. Khả năng phát của nguồn rời rạc	65
3.4.3. Độ thừa của nguồn rời rạc	65
3.4.4. Các đặc trưng của kênh rời rạc và các loại kênh rời rạc	66
3.4.5. Lượng thông tin truyền qua kênh trong một đơn vị thời gian	67
3.4.6. Khả năng thông qua của kênh rời rạc	67
3.4.7. Tính khả năng thông qua của kênh nhị phân đối xứng không nhỏ, đồng nhất	68
3.4.8. Định lý mã hoá thứ hai của Shannon	69

3.4.9. Khả năng thông qua của kênh nhị phân đối xứng có xoá	70
3.5. ENTROPIE CỦA NGUỒN LIÊN TỤC. LƯỢNG THÔNG TIN CHÉO TRUNG BÌNH TRUYỀN QUA KÊNH LIÊN TỤC KHÔNG NHỎ.....	71
3.5.1. Các dạng tín hiệu liên tục.....	71
3.5.2. Các đặc trưng và tham số của kênh liên tục.....	71
3.5.3. Kênh liên tục chứa trong kênh rời rạc.....	72
3.5.4. Entropie của nguồn tin liên tục (của một quá trình ngẫu nhiên liên tục)	73
3.5.5. Mẫu vật lý minh họa sự lớn vô hạn của entropic của nguồn liên tục.....	74
3.5.6. Lượng thông tin chéo trung bình truyền theo kênh liên tục không nhỏ.....	75
3.6. ENTROPIE VI PHÂN CÓ ĐIỀU KIỆN. TÍNH CHẤT CỦA CÁC TÍN HIỆU GAUSSE.....	76
3.6.1. Entropie vi phân có điều kiện	76
3.6.2. Entropie vi phân của nhiễu Gausse	77
3.6.3. Lượng thông tin chéo trung bình truyền theo kênh Gausse	78
3.6.4. Tính chất của các tín hiệu có phân bố chuẩn	80
3.7. KHẢ NĂNG THÔNG QUA CỦA KÊNH GAUSSE.....	82
3.7.1. Khả năng thông qua của kênh Gausse với thời gian rời rạc.....	82
3.7.2. Khả năng thông qua của kênh Gausse với thời gian liên tục trong một giải tần hạn chế.....	83
3.7.3. Khả năng thông qua của kênh Gausse với thời gian liên tục trong giải tần vô hạn	84
3.7.4. Định lý mã hóa thứ hai của Shannon đối với kênh liên tục	85
3.7.5. Ví dụ: Khả năng thông qua của một số kênh thực tế	85
BÀI TẬP	86
CHƯƠNG IV – CƠ SỞ LÝ THUYẾT MÃ HÓA.....	90
4.1. CÁC ĐỊNH NGHĨA VÀ KHÁI NIỆM CƠ BẢN.....	90
4.1.1. Các định nghĩa cơ bản.....	90
4.1.2. Các khái niệm cơ bản.....	91
4.1.3. Khả năng không ché sai của một bộ mã đều nhị phân	93
4.1.4. Mã đều nhị phân không có độ thừa.....	94
4.2. MÃ THÔNG KÊ TỐI UU	94
4.2.1. Độ dài trung bình của từ mã và mã hóa tối ưu	95
4.2.2. Yêu cầu của một phép mã hóa tối ưu	95
4.2.3. Định lý mã hóa thứ nhất của Shannon (đối với mã nhị phân).....	95
4.2.4. Thuật toán Huffman	96
4.3. CÁC CẤU TRÚC ĐẠI SỐ VÀ MÃ TUYỀN TỈNH.....	99
4.3.1. Một số cấu trúc đại số cơ bản	99
4.3.2. Các dạng tuyển tính và mã tuyển tính	101

4.3.3. Các bài toán tối ưu của mã tuyến tính nhị phân	104
4.4. VÀNH ĐA THÚC VÀ MÃ XYCLIC	105
4.4.1. Vành đa thức	105
4.4.2. Ideal của vành đa thức	107
4.4.3. Định nghĩa mã cyclic	109
4.4.4. Ma trận sinh của mã cyclic	110
4.4.5. Ma trận kiểm tra của mã cyclic	110
4.5. MÃ HÓA CHO CÁC MÃ XYCLIC	111
4.5.1. Mô tả từ mã của mã cyclic hệ thống	111
4.5.2. Thuật toán mã hóa hệ thống	112
4.5.3. Thiết bị mã hóa	112
4.5.4. Tạo các dấu kiểm tra của mã cyclic	114
4.5.5. Thuật toán thiết lập từ mã hệ thống theo phương pháp nhân	116
4.6. GIẢI MÃ NGƯỜNG	117
4.6.1. Hai thủ tục giải mã	117
4.6.2. Giải mã theo Syndrom	117
4.6.3. Hệ tổng kiểm tra trực giao và có khả năng trực giao	118
4.6.4. Giải mã ngưỡng dựa trên hệ tổng kiểm tra trực giao	119
4.6.5. Giải mã ngưỡng dựa trên hệ tổng kiểm tra có khả năng trực giao	122
4.7. GIẢI MÃ THEO THUẬT TOÁN MEGGIT	123
4.8. GIẢI MÃ XYCLIC THEO THUẬT TOÁN CHIA DỊCH VÒNG	126
4.8.1. Nhiệm vụ của thuật toán giải mã	126
4.8.2. Giải mã theo thuật toán chia dịch vòng	127
4.8.3. Ví dụ	127
4.9. GIẢI MÃ LUỒI	128
4.9.1. Trạng thái và giản đồ lưới	128
4.9.2. Giải mã lưới	132
4.10. MÃ HAMMING VÀ MÃ CÓ ĐỘ DÀI CỨC ĐẠI	138
4.11. CÁC MÃ KHỐI DỰA TRÊN SỐ HỌC CỦA TRƯỜNG HỮU HẠN	139
4.11.1. Trường hữu hạn cơ nguyên tố GF(p)	139
4.11.2. Các trường mở rộng của trường nhị phân. Trường hữu hạn GF(2^n)	140
4.11.3. Biểu diễn đa thức cho trường hữu hạn GF(2^n)	141
4.11.4. Các tính chất của đa thức và các phần tử của trường hữu hạn	142
4.11.5. Xác định các mã bằng các nghiệm	145
4.11.6. Mã Hamming	146

4.11.7. Mã BCH	146
4.11.8. Các mã Reed –Solomon (RS)	149
4.12. CÁC MÃ CHẬP	150
4.12.1. Mở đầu và một số khái niệm cơ bản	150
4.12.2. Các mã Turbo.....	154
BÀI TẬP	156
CHƯƠNG V – LÝ THUYẾT THU TỐI ƯU	160
5.1. ĐẶT BÀI TOÁN VÀ CÁC VẤN ĐỀ CƠ BẢN	160
5.1.1. Thu tín hiệu khi có nhiễu là một bài toán thống kê	160
5.1.2. Máy thu tối ưu.....	161
5.1.3. Thé chống nhiễu.....	161
5.1.4. Hai loại sai lầm khi chọn giả thuyết.....	161
5.1.5. Tiêu chuẩn Kachennhicov.....	161
5.1.6. Việc xử lý tối ưu các tín hiệu	161
5.1.7. Xác suất giải sai và quy tắc giải tối ưu.....	162
5.1.8. Hàm hợp lý	163
5.1.9. Quy tắc hợp lý tối đa.....	163
5.2. XỬ LÝ TỐI ƯU CÁC TÍN HIỆU CÓ THAM SỐ ĐÃ BIẾT. KHÁI NIỆM VỀ THU KẾT HỢP VÀ THU KHÔNG KẾT HỢP.....	164
5.2.1. Đặt bài toán	164
5.2.2. Giải bài toán.....	164
5.2.3. Khái niệm về thu kết hợp và thu không kết hợp	168
5.3. PHÁT TÍN HIỆU TRONG NHIỀU NHỒ BỘ LỌC PHỐI HỢP TUYẾN TÍNH THU ĐỘNG..	169
5.3.1. Định nghĩa bộ lọc phối hợp tuyến tính thu động	169
5.3.2. Bài toán về bộ lọc phối hợp	169
5.3.3. Đặc tính biến tần và đặc tính pha tần của bộ lọc phối hợp	172
5.3.4. Phản ứng xung của mạch lọc phối hợp	173
5.3.5. Hướng ứng ra của mạch lọc phối hợp	174
5.4. LÝ LUẬN CHUNG VỀ THU KẾT HỢP CÁC TÍN HIỆU NHỊ PHÂN	175
5.4.1. Lập sơ đồ giải tối ưu một tuyến	175
5.4.2. Xác suất sai khi thu kết hợp tín hiệu nhị phân	176
5.5. XỬ LÝ TỐI ƯU CÁC TÍN HIỆU CÓ THAM SỐ NGẪU NHIÊN – THU KHÔNG KẾT HỢP	182
5.5.1. Các tham số của tín hiệu là các tham số ngẫu nhiên	182
5.5.2. Xử lý tối ưu các tín hiệu có tham số ngẫu nhiên biến thiên chậm	183

5.5.3. Xác suất hậu nghiệm của tín hiệu có các tham số thay đổi ngẫu nhiên.....	183
5.5.4. Xử lý tối ưu các tín hiệu có pha ngẫu nhiên.....	184
5.5.5. So sánh thu kết hợp với thu không kết hợp.....	187
5.5.6. Chú thích	188
5.6. MÃ KHỐI KHÔNG GIAN , THỜI GIAN (STBC).....	188
5.6.1. Kỹ thuật thu phân tập.....	188
5.6.2. Mã khối không gian – thời gian dựa trên hai máy phát.....	190
BÀI TẬP	193
PHỤ LỤC	196
BÁT ĐẲNG THỨC BUNHACOVSKI-SCHWAZT	196
BIỂN ĐỔI HILBERT	197
ĐỊNH LÝ KACHENNICOV	198
LUẬT PHÂN BỐ CHUẨN	201
LOGARIT CỦA CÁC SỐ NGUYỄN TỪ 1 ĐẾN 100	202
HÀM VÀ ENTROPIE CỦA NGUỒN NHÌ PHÂN.....	203
ENTROPIE $H(X)$ CỦA CÁC LUẬT PHÂN BỐ RỎI RẠC	204
ENTROPIE VI PHÂN $H(X)$ CỦA CÁC LUẬT PHÂN BỐ LIÊN TỤC	207
CÁC ĐA THỨC TỐI TIỂU CỦA CÁC PHẦN TỬ TRONG TRƯỜNG	214
TÀI LIỆU THAM KHẢO	219
MỤC LỤC.....	220

MỤC LỤC

GIỚI THIỆU TỔNG QUAN	6
1. MỤC ĐÍCH	6
2. YÊU CẦU	6
3. NỘI DUNG CÓT LÕI.....	7
4. KẾT THÚC TIỀN QUYẾT	7
5. TÀI LIỆU THAM KHAO.....	8
6. PHƯƠNG PHÁP HỌC TẬP.....	8
CHƯƠNG 1: GIỚI THIỆU	9
1. Mục tiêu.....	9
2. Đối tượng nghiên cứu.....	9
3. Mô hình lý thuyết thông tin theo quan điểm Shannon	10
4. Lượng tin biết và chưa biết	10
5. Ví dụ về lượng tin biết và chưa biết	10
6. Định lý cơ sở của kỹ thuật truyền tin	11
7. Mô tả trạng thái truyền tin có nhiễu	11
8. Minh họa kỹ thuật giảm nhiễu.....	12
9. Chi phí phải trả cho kỹ thuật giảm nhiễu	13
10. Khái niệm về dung lượng kênh truyền.....	13
11. Vấn đề sinh mã	13
12. Vấn đề giải mã.....	13
CHƯƠNG 2: ĐỘ ĐO LƯỢNG TIN	15
BÀI 2.1: ENTROPY	15
1. Mục tiêu.....	15
2. Ví dụ về entropy	15
3. Nhận xét về độ đo lượng tin	15
4. Khái niệm entropy	16
5. Entropy của một sự kiện.....	16
6. Entropy của một phân phối	16
7. Định lý dạng giải tích của Entropy	16
8. Ví dụ minh họa	17
9. Bài toán về cây tìm kiếm nhị phân-Đặt vấn đề	17
10. Bài toán về cây tìm kiếm nhị phân - Diễn giải	17
11. Bài tập	18
BÀI 2.2: CÁC TÍNH CHẤT CỦA ENTROPY	19
1. Mục tiêu:	19
2. Các tính chất cơ bản của Entropy	19
3. Minh họa tính chất 1 và 2	19
4. Minh họa tính chất 3 và 4	19
5. Định lý cực đại của entropy	20
6. Chứng minh định lý cực đại của Entropy	20
7. Bài tập	21
BÀI 2.3: ENTROPY CỦA NHIỀU BIÉN	22
1. Mục tiêu.....	22
2. Định nghĩa Entropy của nhiều biến	22
3. Ví dụ Entropy của nhiều biến	22
4. Định nghĩa Entropy có điều kiện	22

5. Ví dụ Entropy có điều kiện	23
6. Quan hệ giữa $H(X, Y)$ với $H(X)$ và $H(Y)$ khi X, Y độc lập.....	23
7. Quan hệ giữa $H(X, Y)$ với $H(X)$ và $H(Y)$ khi X, Y tương quan	24
8. Bài tập	25
BÀI 2.4: MINH HỌA CÁC ENTROPY	26
1. Mục tiêu.....	26
2. Yêu cầu của bài toán	26
3. Xác định các phân phối ngẫu nhiên của bài toán	26
4. Minh họa Entropy $H(X)$, $H(Y)$ và $H(X, Y)$	27
5. Minh họa Entropy $H(X/Y)$ và $H(Y/X)$	27
6. Minh họa quan hệ giữa các Entropy.....	27
BAI 2.5: ĐO LUÔNG TIN (MEASURE OF INFORMATION)	28
1. Mục tiêu.....	28
2. Đặt vấn đề bài toán.....	28
3. Xác định các phân phối của bài toán.....	28
4. Nhận xét dựa theo entropy	28
5. Định nghĩa lượng tin	29
6. Bài tập	29
CHƯƠNG 3: SINH MÃ TÁCH ĐƯỢC (Decypherable Coding).....	31
BÀI 3.1: KHÁI NIỆM VỀ MÃ TÁCH ĐƯỢC.....	31
1. Mục tiêu.....	31
2. Đặt vấn đề bài toán sinh mã	31
3. Khái niệm về bảng mã không tách được	32
4. Bảng mã tách được	32
5. Khái niệm bảng mã tức thời	33
6. Giải thuật kiểm tra tính tách được của bảng mã.....	33
7. Bài toán 1 - yêu cầu.....	33
8. Bài toán 1 - Áp dụng giải thuật	34
9. Bài toán 2	34
10. Bài tập	35
BÀI 3.2: QUAN HỆ GIỮA MÃ TÁCH ĐƯỢC VÀ ĐỘ DÀI MÃ.....	36
1. Mục tiêu.....	36
2. Định lý Kraftn(1949).....	36
3. Định nghĩa cây bậc D cỡ k	36
4. Vấn đề sinh mã cho cây bậc D cỡ k	37
5. Chứng minh định lý Kraft (Điều kiện cần)	37
6. Chứng minh định lý Kraft (Điều kiện đủ)	38
7. Ví dụ minh họa định lý Kraft	38
8. Bài tập	39
BÀI 3.3: TÍNH TỐI ƯU CỦA ĐỘ DÀI MÃ.....	40
1. Mục tiêu.....	40
2. Định lý Shannon (1948).....	40
3. Bảng mã tối ưu tuyệt đối	40
4. Bảng mã tối ưu tương đối.....	41
5. Điều kiện nhận biết một bảng mã tối ưu	41
6. Định lý Huffman	41
7. Phương pháp sinh mã Huffman.....	42
8. Minh họa phương pháp sinh mã Huffman	42
9. Nhận xét tính tối ưu của bảng mã Huffman	43
10. Bài tập	43

Too long to read on
your phone? Save to
read later on your
computer



CHƯƠNG 4: KÊNH TRUYỀN	
BÀI 4.1: KÊNH TRUYỀN RỎI RẠC KHÔNG NHỒNG	
1. Mục tiêu.....	46
2. Giới thiệu.....	
3. Mô hình vật lý	
4. Mô hình toán học.....	
5. Ví dụ xác định phân phối đầu nhânh.....	47
6. Lượng tin trên kênh truyền.....	47
7. Định nghĩa dung lượng kênh truyền.....	48
BÀI 4.2: CÁC DẠNG KÊNH TRUYỀN	49
1. Mục tiêu.....	49
2. Hiểu định lý về dung lượng kênh truyền,Kênh truyền không mất tin.....	49
3. Kênh truyền xác định	49
4. Kênh truyền không nhiễu	50
5. Kênh truyền không sử dụng được.....	50
6. Kênh truyền đối xứng.....	50
7. Xây dựng công thức tính dung lượng kênh truyền đối xứng	51
8. Định lý về dung lượng kênh truyền.....	52
9. Bài tập	52
BÀI 4.3: LUẬC ĐỘ GIẢI MÃ	53
1. Mục tiêu.....	53
2. Đặt vấn đề bài toán giải mã	53
3. Ví dụ bài toán giải mã	53
4. Các khái niệm cơ bản của kỹ thuật truyền tin	54
5. Ví dụ minh họa các khái niệm cơ bản	54
6. Các dạng sai số cơ bản	55
7. Phương pháp xây dựng lược đồ giải mã tối ưu	55
8. Minh họa xây dựng lược đồ giải mã tối ưu	56
9. Minh họa cách tính các sai số.....	57
10. Bài tập 1	58
11. Bài Tập 2	58
CHƯƠNG 5: SỬA LỖI.....	59
BÀI 5.1: NGUYÊN LÝ KHOẢNG CÁCH NHỎ NHẤT HAMMING	59
1. Mục tiêu:	59
2. Khoảng cách Hamming.....	59
3. Kênh truyền đối xứng nhị phân và lược đồ giải mã tối ưu	59
4. Ví dụ kênh truyền đối xứng nhị phân.....	60
5. Quan hệ giữa xác suất giải mã và khoảng cách Hamming	60
6. Nguyên lý Hamming	60
7. Bài tập	61
BÀI 5.2: BỐ ĐỀ VỀ TỰ SỬA LỖI VÀ CẬN HAMMING	62
1. Mục tiêu.....	62
2. Bố đề về tự sửa lỗi.....	62
3. Chứng minh và minh họa bố đề	62
4. Cận Hamming	63
5. Phân các dạng lỗi.....	64
6. Bài tập	64
BÀI 5.3: MÃ KIỂM TRA CHẨN LẺ	64
1. Mục tiêu:	64
2. Bộ mã kiểm tra chẵn lẻ	65

3. Phương pháp kiểm tra chẵn lẻ	65
4. Phương pháp sinh mã kiểm tra chẵn lẻ	66
5. Ví dụ sinh mã kiểm tra chẵn lẻ	66
6. Định lý quan hệ giữa độ dài mã n, số bit kiểm tra m và số lỗi tự sửa e	67
7. Ví dụ tìm m nhỏ nhất từ n và e	68
8. Ví dụ tìm e lớn nhất từ m và n	68
9. Bài tập	68
BÀI 5.4: NHÓM CỘNG TÍNH VÀ BỘ TỬ MÃ CHẴN LẺ	69
1. Mục tiêu	69
2. Khái niệm nhóm cộng tính	69
3. Tính chất của bộ mã chẵn lẻ	69
4. Ví dụ minh họa	70
5. Phương pháp sinh mã kiểm tra chẵn lẻ nhanh	71
6. Ví dụ sinh mã kiểm tra chẵn lẻ nhanh	71
7. Bài tập	72
BÀI 5.5: LUỢC ĐỒ SỬA LỐI TỐI ƯU	73
1. Mục tiêu	73
2. Đặt vấn đề	73
3. Định nghĩa Hiệp hợp	73
4. Lược đồ sửa lỗi theo các hiệp hợp	74
5. Lược đồ sửa lỗi thông qua bộ lỗi	74
6. Ví dụ minh họa lược đồ sửa lỗi 1 bit	74
7. Ví dụ minh họa lược đồ sửa lỗi 2 bit	75
8. Ví dụ minh họa lược đồ sửa lỗi 3 bit	76
9. Xác suất truyền đúng	76
10. Bài tập	76
BÀI 5.6: MÃ HAMMING	76
1. Mục tiêu	76
2. Mã Hamming	77
3. Tính chất	77
4. Ví dụ minh họa	77
5. Bài tập	78
BÀI 5.7: THANH GHI LÙI TÙNG BUỚC	79
1. Mục tiêu	79
2. Đặt vấn đề	79
3. Biểu diễn vật lý của thanh ghi	79
4. Biểu diễn toán học của thanh ghi	80
5. Ví dụ thanh ghi lui từng bước	80
6. Chu kỳ của thanh ghi	81
7. Ví dụ tìm chu kỳ của thanh ghi	81
8. Bài tập	82
BÀI 5.8: MÃ XOAY VÒNG	82
1. Mục tiêu	82
2. Mã trật kiểm tra chẵn lẻ mã xoay vòng	83
3. Định nghĩa mã xoay vòng	83
4. Phương pháp sinh nhanh bộ mã xoay vòng	83
5. Ví dụ sinh nhanh bộ mã xoay vòng	84
6. Bài tập	85
BÀI 5.9: ĐÁ THỨC ĐẶC TRUNG CỦA THANH GHI	86
1. Mục tiêu	86

2. Định nghĩa đa thức đặc trưng của thanh ghi	86
3. Quan hệ giữa chu kỳ n, đa thức đặc trưng và đa thức ($x^n + 1$).....	86
4. Thủ tục sinh thanh ghi lùi từng bước	87
5. Ví dụ minh họa	87
6. Bài tập	87
Bài 5.10: PHƯƠNG PHÁP SINH MÃ XOAY VÒNG	88
1. Mục tiêu.....	88
2. Đặt vấn đề.....	88
3. Phương pháp sinh bằng mã xoay vòng.....	88
4. Ví dụ minh họa 1	89
5. Ví dụ minh họa 2	89
6. Ví dụ minh họa 3	90
7. Bảng liệt kê một số đa thức đặc trưng	90
8. Bài tập	90
BÀI TẬP TỔNG HỢP	91
1. Mục tiêu.....	91
2. Bài 1	91
3. Bài 2	91
4. Bài 3	92
5. Bài 4	93
TÀI LIỆU THAM KHẢO	95

GIỚI THIỆU TỔNG QUAN

GIÁO TRÌNH LÝ THUYẾT THÔNG TIN

MỤC ĐÍCH

- ❖ Giáo trình này sẽ cung cấp cho người đọc những khái niệm cơ bản của lý thuyết thông tin như: Độ đo lượng tin (Measure of Information), Sinh mã tách được (Decypherable Coding), Kênh truyền tin rời rạc không nhớ (Discrete Memoryless Channel) và Sửa lỗi trên kênh truyền (Error Correcting Codings).
- **Liên quan đến Độ đo lượng tin**, giáo trình sẽ trình bày các khái niệm cơ bản về thông tin, entropy, một số công thức, tính chất, các định lý quan trọng của entropy và cách tính lượng tin.
- **Về Sinh mã tách được**, giáo trình sẽ giới thiệu đến người học các vấn đề về yêu cầu của bài toán sinh mã, giải mã duy nhất, cũng như mã tức thời và giải thuật kiểm tra mã tách được. Các định lý quan trọng được đề cập trong nội dung này là: Định lý Kraft (1949), Định lý Shannon (1948) và Định lý sinh mã Huffman.
- **Về kênh truyền tin rời rạc không nhớ**, giáo trình sẽ giới thiệu mô hình kênh truyền theo 2 khía cạnh vật lý và toán học. Các khái niệm về dung lượng kênh truyền, phân lớp kênh truyền, định lý về dung lượng kênh truyền, cũng như các khái niệm trong kỹ thuật truyền tin và phương pháp xây dựng lược đồ giải mã tối ưu cũng được trình bày trong môn học này.
- **Vấn đề Sửa lỗi (hay xử lý mã sai) trên kênh truyền** là một vấn đề rất quan trọng và được quan tâm nhiều trong môn học này. Các nội dung được giới thiệu đến các bạn sẽ là Nguyên lý Khoảng cách Hamming, các định lý về Cân Hamming, phương pháp kiểm tra chẵn lẻ, các lược đồ sửa lỗi, Bảng mã Hamming và Bảng mã xoay vòng.
- ❖ Hơn nữa, hầu hết các vấn đề nêu trên đều được đưa vào nội dung giảng dạy ở các bậc Đại học của một số ngành trong đó có ngành Công nghệ thông tin. Do đó, để có một tài liệu phục vụ công tác giảng dạy của giáo viên cũng như việc học tập và nghiên cứu của sinh viên, chúng tôi mạnh dạn biên soạn giáo trình này nhằm giúp cho sinh viên có một tài liệu tự học và nghiên cứu một cách hiệu quả.

YÊU CẦU

- ❖ Sau khi học xong môn này, sinh viên phải có được những khả năng sau:
 - Hiểu các khái niệm về thông tin, Entropy, Entropy của một phân phối, Entropy của nhiều phân phối, Entropy có điều kiện, Độ đo lượng tin. Vận dụng giải quyết các bài toán về xác định lượng tin.
 - Biết khái niệm về mã tách được, mã không tách được, bảng mã tối ưu. Hiểu Định lý Kraft (1949), Định lý Shannon (1948), Định lý sinh mã Huffman và phương pháp sinh mã Huffman. Vận dụng để sinh bảng mã tách được tối ưu, nhận biết được bảng mã như thế nào là bảng mã tối ưu và có thể vận dụng để viết các chương trình sinh mã, giải mã (hay viết chương trình nén và giải nén). Từ đây, các sinh viên có thể tự nghiên cứu các loại bảng mã khác để vận dụng cho việc mã hóa và bảo mật thông tin một cách hiệu quả.

- Biết các khái niệm về kênh truyền tin rời rạc không nhớ, dung lượng kênh truyền và phân lớp kênh truyền. Hiểu định lý về dung lượng kênh truyền, phương pháp xây dựng lược đồ giải mã tối ưu và cách tính xác suất truyền sai trên kênh truyền.
 - Biết các khái niệm về khoảng cách Hamming, nguyên lý khoảng cách Hamming, các định lý về Cận Hamming, phương pháp kiểm tra chẵn lẻ, các lược đồ sửa lỗi, Bảng mã Hamming và Bảng mã xoay vòng.
 - Vận dụng các kiến thức học được để thiết kế một hệ thống truyền nhận dữ liệu với quy trình cơ bản: mã hóa, giải mã và bảo mật thông tin.
- ❖ Lý thuyết thông tin cũng là một trong các môn học khó của ngành Công nghệ thông tin vì nó đòi hỏi người học phải có kiến thức cơ bản về toán và xác suất thống kê. Do đó, đòi hỏi người học phải tự bổ sung các kiến thức cơ bản về toán và xác suất thống kê cho mình (nếu thiếu), tham gia lớp học đầy đủ và làm các bài tập theo yêu cầu của môn học thì mới tiếp thu kiến thức môn học một cách hiệu quả.

NỘI DUNG CỐT LÕI

Giáo trình gồm 5 chương được trình bày trong 45 tiết giảng cho sinh viên chuyên ngành Công nghệ thông tin, trong đó có khoảng 30 tiết lý thuyết và 15 tiết bài tập mà giáo viên sẽ hướng dẫn cho sinh viên trên lớp.

Chương 1: Giới thiệu. *Chương này trình bày các nội dung có tính tổng quan về môn học bao gồm: các đối tượng nghiên cứu, mô hình lý thuyết thông tin theo quan điểm của nhà toán học Shannon, khái niệm về lượng tin biết và chưa biết, định lý cơ bản của kỹ thuật truyền tin.*

Chương 2: Độ đo lượng tin. *Chương này trình bày các vấn đề cơ bản về entropy, các tính chất của entropy, entropy của nhiều biến, entropy có điều kiện, các định lý về quan hệ giữa các entropy và lượng tin của một sự kiện.*

Chương 3: Sinh mã tách được. *Nội dung chính của chương này bao gồm các khái niệm về mã tách được, quan hệ giữa mã tách được và độ dài mã, tính tối ưu của độ dài mã.*

Chương 4: Kênh truyền. *Các nội dung được trình bày trong chương này bao gồm khái niệm về kênh truyền tin rời rạc không nhớ, các mô hình truyền tin ở khía cạnh vật lý và toán học, dung lượng trên kênh truyền, phân lớp các kênh truyền. Phương pháp xây dựng lược đồ giải mã tối ưu và cách tính xác suất truyền sai cũng được giới thiệu trong chương này.*

Chương 5: Sửa lỗi. *Chương này trình bày các nội dung cốt lõi sau: khái niệm về khoảng cách Hamming, nguyên lý khoảng cách nhỏ nhất Hamming, bối cảnh về tự sửa lỗi và định lý Cận Hamming. Chương này cũng giới thiệu về bộ mã kiểm tra chẵn lẻ, phương pháp kiểm tra chẵn lẻ, lược đồ sửa lỗi tối ưu, mã Hamming và mã xoay vòng.*

KẾT THÚC TIÊN QUYẾT

Để học tốt môn học này, đòi hỏi sinh viên phải nắm vững các môn học có liên quan như: xác suất thống kê, đại số boole (phép toán Modulo 2 và đa thức nhị phân). Các môn học có liên quan và có thể tham khảo thêm như kỹ thuật số, hệ điều hành, mạng máy tính.

TÀI LIỆU THAM KHẢO

1. David J.C. Mackey, *Information Theory, Inference, and Learning Algorithms*, CamBridge University Express-2003.
2. G.J.ChaiTin, *Algorithmic Information Theory*, CamBridge University Express-1992.
3. Sanford Goldman, *Information Theory*.
4. <http://www.inference.phy.cam.ac.uk/mackay/info-theory/course.html>.
5. http://en.wikipedia.org/wiki/Information_theory.
6. <http://www-2.cs.cmu.edu/~dst/Tutorials/Info-Theory/>.
7. <http://cscs.umich.edu/~crshalizi/notebooks/information-theory.html>.
8. <http://www.lecb.ncifcrf.gov/~toms/paper/primer/primer.pdf>.
9. <http://www.cs.ucl.ac.uk/staff/S.Bhatti/D51-notes/node27.html>.
10. <http://guest.engelschall.com/~sb/hamming/>.
11. http://www2.rad.com/networks/1994/err_con/hamming.htm

PHƯƠNG PHÁP HỌC TẬP

Để phục vụ cho mục tiêu nâng cao khả năng tự học tập và tự nghiên cứu của sinh viên, giáo trình này được biên soạn cùng với các giáo trình khác thuộc chuyên ngành Công nghệ thông tin của Khoa Công nghệ thông tin và Truyền thông – Đại Học Cần Thơ theo dự án **ASVIET002CNTT** “**Tăng cường hiệu quả đào tạo và năng lực đào tạo của sinh viên khoa Công nghệ Thông tin – Đại học Cần Thơ**”. Chúng tôi đã cố gắng trình bày giáo trình này một cách có hệ thống các nội dung theo bố cục các chương ứng với các khối kiến thức nêu trên, mỗi chương được trình bày theo bố cục của các bài học và mỗi bài học giới thiệu đến người học một vấn đề nào đó trong số các vấn đề của một khối kiến thức tương ứng với một chương. Khi học xong các bài học của một chương, người học sẽ có một khái niệm cần thiết tương ứng cho môn học. Nội dung của các bài học đều được đưa vào các ví dụ để người học dễ hiểu, tùy theo từng vấn đề mà người học cần phải học và nghiên cứu trong thời lượng từ 1 đến 2 tiết tự học cho một bài học trong một chương. Như vậy, để học tốt môn học này, trước hết sinh viên cần phải:

- Học đầy đủ các môn học tiên quyết, bổ sung những kiến thức cơ bản về toán và xác suất thống kê (nếu thiếu).
- Học và nghiên cứu kỹ từng chương theo trình tự các chương được trình bày trong giáo trình này. Trong từng chương, học các bài theo thứ tự được trình bày, sau mỗi bài phải làm bài tập đầy đủ (nếu có).
- Tham gia lớp đầy đủ, thảo luận các vấn đề tồn tại chưa hiểu trong quá trình tự học.
- Sau mỗi chương học, phải nắm vững các khái niệm, các định nghĩa, các công thức tính toán và vận dụng giải các bài toán có tính chất tổng hợp được giới thiệu ở cuối chương.
- Vận dụng kiến thức có được sau khi học xong các chương để giải một số bài tập tổng hợp ở cuối giáo trình, từ đó giúp cho người học hiểu sâu hơn về môn học và có thể giải quyết các vấn đề tương tự trong thực tế.

Việc cho ra đời một giáo trình với những mục đích như trên là không đơn giản khi khả năng và kinh nghiệm của người soạn còn có hạn, nhiều khái niệm, thuật ngữ dùng trong giáo trình chưa được định nghĩa một cách chính thống. Vì vậy giáo trình này chắc không tránh khỏi những khiếm khuyết, rất mong nhận được sự góp ý của các đồng nghiệp và người đọc.

CHƯƠNG 1: GIỚI THIỆU

1: Mục tiêu

Sau khi hoàn tất bài học này bạn có thể biết:

- Đối tượng nghiên cứu,
- Mô hình lý thuyết thông tin theo quan điểm Shannon,
- Các khái niệm về Lượng tin biết và lượng tin chưa biết,
- Định lý cơ sở của kỹ thuật truyền tin,
- Khái niệm chung về dung lượng kênh truyền,
- Vấn đề sinh mã và giải mã.

Đối tượng nghiên cứu

Lý thuyết thông tin được xây dựng trên hai hướng khác nhau bởi hai nhà toán học Shannon (1948) và Wiener (1949). Lý thuyết thông tin nghiên cứu quá trình xử lý tín hiệu như sau:

Đầu vào (input): nhận tín hiệu từ một lĩnh vực cụ thể, tức là tín hiệu xuất hiện theo các ký hiệu (symbol) từ một tập hợp cho trước và theo phân phối xác suất đã biết.

Tín hiệu được truyền đi trên kênh truyền (channel) và có thể bị nhiễu cũng theo một phân phối xác suất nào đó. Kênh truyền có thể được hiểu dưới hai nghĩa:

Dưới nghĩa vật lý: kênh truyền là một hệ thống truyền tín hiệu (dây dẫn, mạch, sóng, ...) và gây nhiễu tùy thao chất lượng của hệ thống.

Dưới nghĩa toán học: kênh truyền là các phân phối xác suất xác định trên lớp các tín hiệu đang xét ở đầu nhận tín hiệu (output).

Ở đầu ra (output): dựng lại tín hiệu chân thật nhất có thể có so với tín hiệu ở đầu vào.

Shannon xây dựng mô hình lý thuyết thông tin trên cơ sở giải quyết bài toán: sinh mã độ dài tối ưu khi nhận tín hiệu đầu vào. Tín tối ưu được xét trên 3 yếu tố sau:

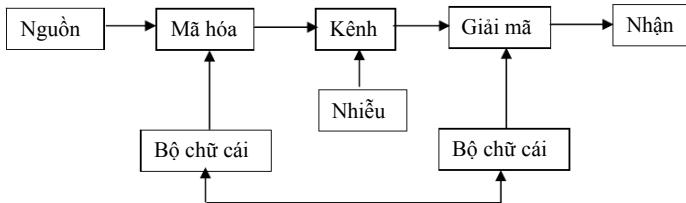
Phân phối xác suất của sự xuất hiện của các tín hiệu.

Tính duy nhất của mã và cho phép tự điều chỉnh mã sai nếu có với độ chính xác cao nhất. Giải mã đồng thời tự động điều chỉnh mã hoặc xác định đoạn mã truyền sai.

Trong khí đó, Wiener lại nghiên cứu phương pháp xử lý tín hiệu ở đầu ra: ước lượng tối ưu chuỗi tín hiệu so với chính nó khi nhận ở đầu vào không qua quá trình sinh mã. Như vậy phương pháp Wiener được áp dụng trong những trường hợp con người không kiểm soát được quá trình truyền tín hiệu. Môn “xử lý tín hiệu” đã đề cập đến vấn đề này.

Mô hình lý thuyết thông tin theo quan điểm Shannon

Lý thuyết thông tin được xét ở đây theo quan điểm của Shannon. Đối tượng nghiên cứu là một hệ thống liên lạc truyền tin (communication system) như sơ đồ dưới đây:



Điễn giải:

- Nguồn (source) thông tin còn gọi là thông báo cần được truyền ở đầu vào (Input).
- Mã hóa (encode) là bộ sinh mã. Ứng với một thông báo, bộ sinh mã sẽ gán cho một đối tượng (object) phù hợp với kỹ thuật truyền tin. Đối tượng có thể là:
 - Dãy số nghị phân (Digital) dạng: 01010101, cũng giống như mã máy tính.
 - Sóng liên tục (Analog) cũng giống như truyền radio.
- Kênh (channel) là phương tiện truyền mã của thông tin.
- Nhiễu (noise) được sinh ra do kênh truyền tin. Tùy vào chất lượng của kênh truyền mà nhiễu nhiều hay ít.
- Giải mã (decode) ở đầu ra (output) đưa dãy mã trở về dạng thông báo ban đầu với xác suất cao nhất. Sau đó thông báo sẽ được chuyển cho người nhận. Trong sơ đồ trên, chúng ta quan tâm đến 2 khối mã hóa và giải mã trong toàn bộ môn học.

Lượng tin biết và chưa biết

Một biến ngẫu nhiên (BNN) X luôn mang một lượng tin nào đó. Nếu X chưa xảy ra (hay ta chưa biết cụ thể thông tin về X) thì lượng tin của nó là chưa biết, trong trường hợp này X có một lượng tin chưa biết. Ngược lại nếu X đã xảy ra (hay ta biết cụ thể thông tin về X) thì lượng tin về biến ngẫu nhiên X coi như đã biết hoàn toàn, trong trường hợp này X có một lượng tin đã biết.

Nếu biết thông tin của một BNN X thông qua BNN Y đã xảy ra thì ta có thể nói: chúng ta chỉ biết một phần lượng thông tin của X đó trên cơ sở biết Y.

Ví dụ về lượng tin biết và chưa biết

Ta xét ví dụ về một người tổ chức trò chơi may rủi khán giả với việc tung một đồng tiền “có đầu hình – không có đầu hình”. Nếu người chơi chọn mặt không có đầu hình thì thắng khi kết quả tung đồng tiền là không có đầu hình, ngược lại thì thua. Tuy nhiên người tổ chức chơi có thể “ăn gian” bằng cách sử dụng 2 đồng tiền “Thật- Giả” khác nhau sau:

- + Đồng tiền loại 1 (hay đồng tiền thật): đồng chất có 1 mặt có đầu hình.
- + Đồng tiền loại 2 (hay đồng tiền giả): đồng chất, mỗi mặt đều có 1 đầu hình.

Mặc dù người tổ chức chơi có thể “ăn gian” nhưng quá trình trao đổi 2 đồng tiền cho nhau là ngẫu nhiên, vậy liệu người tổ chức chơi có thể “ăn gian” hoàn toàn được không? Hay lượng tin biết và chưa biết của sự kiện lấy một đồng tiền từ 2 đồng tiền nói trên được hiểu như thế nào?

Ta thử xét một trường hợp sau: nếu người chơi lấy ngẫu nhiên 1 đồng tiền và sau đó thực hiện việc tung đồng tiền lấy được 2 lần. Qua 2 lần tung đồng tiền, ta đếm được số đầu hình xuất hiện. Dựa vào số đầu hình xuất hiện, ta có thể phán đoán được người tổ chức chơi đã lấy được đồng tiền nào.

Chẳng hạn: Nếu số đầu hình đếm được sau 2 lần tung là 1 thì đồng tiền đã lấy được là đồng tiền thật. Ngược lại nếu số đầu hình đếm được là 2 thì đồng tiền đã lấy được có thể là thật hay cũng có thể là giả. Như vậy, ta đã nhận được một phần thông tin về loại đồng tiền qua số đầu hình đếm được sau 2 lần tung. Ta có thể tính được lượng tin đó bằng bao nhiêu? (*Việc tính lượng tin này sẽ được thảo luận sau*). Dưới đây là một số bảng phân phối của bài toán trên:

Gọi BNN X về loại đồng tiền ($X=1$ nếu lấy được đồng tiền loại 1 và $X=2$ nếu lấy được đồng tiền loại 2 được lấy).

Khi đó phân phối của X có dạng:

X	1	2
P	0.5	0.5

Đặt BNN Y là BNN về số đầu hình đếm được sau 2 lần tung. Khi đó ta có thể xác định được phân phối của Y với điều kiện xảy ra của X trong 2 trường hợp sau.

Phân phối của Y khi biết $X=1$ có dạng:

Y/X=1	0	1	2
P	0.25	0.5	0.25

Phân phối của Y khi biết $X=2$ có dạng:

Y/X=2	0	1	2
P	0	0	1

Định lý cơ sở của kỹ thuật truyền tin

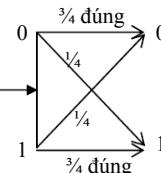
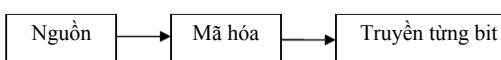
Trong “A New Basic of Information Theory (1954)”, Feinstein đã đưa ra định lý sau: “Trên một kênh truyền có nhiều, người ta luôn có thể thực hiện một phương pháp truyền sao cho đạt được sai số nhỏ hơn sai số cho phép (nhỏ bất kỳ) cho trước đối với kênh truyền.”

Chúng ta sẽ không chứng minh định lý, thay vào đó, chúng ta sẽ tham khảo đến các minh họa giảm nhiễu trong các nội dung tiếp theo của bài học.

Mô tả trạng thái truyền tin có nhiễu

Giả sử, một thông báo được truyền đi trên một kênh truyền nhị phân rời rạc. Thông báo cần truyền được mã hóa thành dãy số nhị phân $(0,1)$ và có độ dài được tính theo đơn vị bit. Giả sử 1 bit truyền trên kênh nhiễu với xác suất $1/4$ (hay tính trung bình cứ truyền 4 bit thì có thể nhiễu 1 bit).

Ta có sơ đồ trạng thái truyền tin sau:



Minh họa kỹ thuật giảm nhiễu

Trong kỹ thuật truyền tin, người ta có thể làm giảm sai lầm khi nhận tin bằng cách truyền lặp lại 1 bit với số lần lặp.

Ví dụ: truyền lặp lại 3 cho 1 bit cần truyền (xác suất nhiễu 1 bit bằng $1/4$). Khi nhận 3 bit liền nhau ở cuối kênh được xem như là 1 bit. Giá trị của bit này được hiểu là 0 (hay 1) nếu bit 0 (bit 1) có số lần xuất hiện nhiều hơn trong dãy 3 bit nhận được liền nhau (hay giải mã theo nguyên tắc đa số). Ta cần chứng minh với phương pháp truyền này thì xác suất truyền sai thật sự $< 1/4$ (xác suất nhiễu cho trước của kênh truyền).

Sơ đồ truyền tin:

Bit truyền	Tuyễn lặp 3 lần	Nhận 3 bit	Giải mã
0	000	000	0
	000	001	0
	000	010	0
	000	100	0
	000	101	1
	000	011	1
	000	110	1
	000	111	1
	111	000	0
	111	001	0
1	111	010	0
	111	100	0
	111	011	1
	111	110	1
	111	111	1
	111	111	1

Thật vậy:

Giả sử X_i xác định giá trị đúng hay sai của bit thứ i nhận được ở cuối kênh truyền với $X_i=1$ nếu bit thứ i nhận được là sai và $X_i=0$ nếu bit thứ i nhận được là đúng. Theo giả thiết ban đầu của kênh truyền thì phân phối xác suất của X_i có dạng Bernoulli $b(1/4)$:

X_i	1	0
P	$3/4$	$1/4$

Gọi $Y = \{X_1 + X_2 + X_3\}$ là tổng số bit nhận sai sau 3 lần truyền lặp cho 1 bit. Trong trường hợp này Y tuân theo phân phối Nhị thức $B(p,n)$, với $p=1/4$ (xác suất truyền sai một bit) và $q=3/4$ (xác suất truyền đúng 1 bit):

$Y \sim B(i,n)$ hay

$$p(Y=i) = C_n^i \cdot p^i q^{n-i}$$

Trong đó: $C_n^i = \frac{n!}{i!(n-i)!}$

Vậy truyền sai khi $Y \in \{2, 3\}$ có xác xuất là:

$$P_{\text{sai}} = P(Y \geq 2) = P(Y=2) + P(Y=3) = B(2,3) + B(2,3)$$

$$\text{Hay } Psai = (C_2^2 \left(\frac{1}{4}\right)^2 \cdot \left(\frac{3}{4}\right)^1) + (C_3^3 \left(\frac{1}{4}\right)^3 \cdot \left(\frac{3}{4}\right)^0) = \frac{10}{64} < \frac{1}{4} \text{ (dpcm).}$$

Chi phí phải trả cho kỹ thuật giảm nhiễu

Theo cách thức lặp lại như trên, ta có thể giảm sai lầm bao nhiêu cũng được (lặp càng nhiều thì sai càng ít), nhưng thời gian truyền cũng tăng lên và chi phí truyền cũng sẽ tăng theo.

Hay ta có thể hiểu như sau:

Lặp càng nhiều lần 1 bit \Rightarrow thời gian truyền càng nhiều \Rightarrow chi phí càng tăng.

Khái niệm về dung lượng kênh truyền

Ví dụ trên cho chúng ta thấy cần phải xác định một thông số cho truyền tin để đảm bảo sai số chấp nhận được và đồng thời tốc độ truyền cũng không quá chậm.

Khái niệm “dung lượng” kênh truyền là khái niệm rất cơ bản của lý thuyết truyền tin và là một đại lượng vật lý đồng thời cũng là đại lượng toán học (có đơn vị là bit). Nó cho phép xác định tốc độ truyền tối đa của mỗi kênh truyền. Do đó, dựa vào dung lượng kênh truyền, người ta có thể chỉ ra tốc độ truyền tin đồng thời với một phương pháp truyền có sai số cho phép.

Vấn đề sinh mã

Từ kỹ thuật truyền tin trên cho ta thấy quá trình sinh mã và giải mã được mô tả như sau: một đơn vị thông tin nhận được ở đầu vào sẽ được gán cho một ký hiệu trong bộ ký hiệu sinh mã. Một ký hiệu mã được gán n lần lặp lại (dựa vào dung lượng của kênh truyền, ta có thể xác định được n). Thiết bị sinh mã (Coding device/ Encoder) sẽ thực hiện quá trình sinh mã.

Như vậy, một đơn vị thông tin từ nguồn phát tin sẽ được thiết bị sinh mã gán cho một dãy n ký hiệu mã. Dãy ký hiệu mã của 1 đơn vị thông tin được gọi là một từ mã (Code word). Trong trường hợp tổng quát, người ta có thể gán một khối ký tự mã cho một khối thông tin nào đó và được gọi là một từ mã.

Vấn đề giải mã

Ở cuối kênh truyền, một thiết bị giải mã (Decoding device/ Decoder) sẽ thực hiện quá trình ngược lại như sau: kiểm tra dãy ký hiệu mã để quyết định giải mã về một từ mã và đưa nó về dạng khối tin ban đầu.

Ví dụ:

Khối tin ban đầu : 01010101

Khối ký hiệu mã ở đầu truyền (lặp 3 lần): 000111000111000111000111.

Khối ký hiệu mã ở đầu nhận : 001110100111011001000111

Khối tin nhận được cuối cùng : 01011001 (sai 2 bit so với khối tin ban đầu)

Do đó làm sao để đưa khối tin nhận được về khối tin ban đầu 01010101, đây chính là công việc của bộ giải mã (Decoder).

Một vấn đề quan trọng cần lưu ý là phải đồng bộ giữa tốc độ nạp thông tin (phát tín hiệu) với tốc độ truyền tin. Nếu tốc độ nạp thông tin bằng hoặc lớn hơn so với tốc độ truyền tin của kênh, thì cần phải giảm tốc độ nạp thông tin sao cho nhỏ hơn tốc độ truyền tin.

CHƯƠNG 2: ĐỘ ĐO LƯỢNG TIN

Mục tiêu: trình bày các khái niệm về độ đo lượng tin chưa biết và đã biết về một biến ngẫu nhiên X. Tính toán các lượng tin này thông qua định nghĩa và các tính chất của Entropy từ một hay nhiều biến ngẫu nhiên.

BÀI 2.1: ENTROPY

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu được các khái niệm Entropy,
- Biết Entropy của một sự kiện và Entropy của một phân phối,
- Hiểu Định lý dạng giải tích của Entropy,
- Biết Bài toán về cây tìm kiếm nhị phân và
- Làm kiến thức cơ sở để hiểu và học tốt các bài học tiếp theo.

Ví dụ về entropy

Trước hết, ta cần tìm hiểu một ví dụ về khái niệm độ do của một lượng tin dựa vào các sự kiện hay các phân phối xác suất ngẫu nhiên như sau:

Xét 2 BNN X và Y có phân phối sau:

$X=\{1, 2, 3, 4, 5\}$ có phân phối đều hay $p(X=i) = 1/5$.
 $Y=\{1, 2\}$ cũng có phân phối đều hay $p(Y=i) = 1/2$.

Bản thân X và Y đều mang một lượng tin và thông tin về X và Y chưa biết do chúng là ngẫu nhiên. Do đó, X hay Y đều có một lượng tin không chắc chắn và lượng tin chắc chắn, tổng của 2 lượng tin này là không đổi và thực tế nó bằng bao nhiêu thì ta chưa thể biết. Lượng tin không chắc chắn của X (hay Y) được gọi là Entropy.

Tuy nhiên, nếu X và Y có tương quan nhau thì X cũng có một phần lượng tin không chắc chắn thông qua lượng tin đã biết của Y (hay thông tin về Y đã được biết). Trong trường hợp này, một phần lượng tin không chắc chắn của thông qua lượng tin đã biết của Y được gọi là Entropy có điều kiện.

Nhận xét về độ đo lượng tin

Rõ ràng, ta cần phải xây dựng một đại lượng toán học rất cụ thể để có thể đo được lượng tin chưa biết từ một biến ngẫu nhiên. Một cách trực quan, lượng tin đó phải thể hiện được các vấn đề sau:

Một sự kiện có xác suất càng nhỏ thì sự kiện đó ít xảy ra, cũng có nghĩa là tính không chắc chắn càng lớn. Nếu đo lượng tin của nó thì nó cho một lượng tin không biết càng lớn.

Một tập hợp các sự kiện ngẫu nhiên (hay Biến ngẫu nhiên) càng nhiều sự kiện có phân phối càng đều thì tính không chắc chắn càng lớn. Nếu đo lượng tin của nó thì sẽ được lượng tin không biết càng lớn. Hay lượng tin chắc chắn càng nhỏ.

Một phân phối xác suất càng lênh nhìu (có xác xuất rất nhỏ và rất lớn) thì tính không chắc chắn càng ít và do đó sẽ có một lượng tin chưa biết càng nhỏ so với phân phối xác suất đều hay lượng tin chắc chắn của nó càng cao.

Khái niệm entropy

Trong tiếng việt ta chưa có từ tương đương với từ Entropy, tuy nhiên chúng ta có thể tạm hiểu hiểu thoáng qua trước khi đi vào định nghĩa chắc chắn về mặt toán học của Entropy như sau:

Entropy là một đại lượng toán học dùng để đo lượng tin không chắc (hay lượng ngẫu nhiên) của một sự kiện hay của phân phối ngẫu nhiên cho trước. Hay một số tài liệu tiếng anh gọi là Uncertainty Measure.

Entropy của một sự kiện

Giả sử có một sự kiện A có xác suất xuất hiện là p. Khi đó, ta nói A có một lượng không chắc chắn được đo bởi hàm số $h(p)$ với $p \subseteq [0,1]$. Hàm $h(p)$ được gọi là Entropy nếu nó thoả 2 tiêu đề toán học sau:

Tiêu đề 01: $h(p)$ là hàm liên tục không âm và đơn điệu giảm.

Tiêu đề 02: nếu A và B là hai sự kiện độc lập nhau, có xác suất xuất hiện lần lượt là p_A và p_B . Khi đó, $p(A,B) = p_A \cdot p_B$ nhưng $h(A,B) = h(p_A) + h(p_B)$.

Entropy của một phân phối

Xét biến ngẫu nhiên X có phân phối:

X	x_1	x_2	x_3	...	x_M
P	p_1	p_2	p_3	...	p_M

Nếu gọi A_i là sự kiện $X=x_i$, ($i=1,2,3,\dots$) thì Entropy của A_i là: $h(A_i)=h(p_i)$

Gọi $Y=h(X)$ là hàm ngẫu nhiên của X và nhận các giá trị là dãy các Entropy của các sự kiện $X=x_i$, tức là $Y=h(X)=\{h(p_1), h(p_2), \dots, h(p_n)\}$.

Vậy, Entropy của X chính là kỳ vọng toán học của $Y=h(X)$ có dạng:

$H(X)=H(p_1, p_2, p_3, \dots, p_n) = p_1h(p_1)+p_2h(p_2)+\dots+p_nh(p_n)$.

Tổng quát:

$$H(X) = \sum_{i=1}^n p_i h(p_i)$$

Định lý dạng giải tích của Entropy

Định lý: Hàm $H(X) = H(p_1, p_2, \dots, p_M) = C \sum_{i=1}^M p_i \log(p_i)$

$C = \text{const} > 0$

Cơ số logarithm là bất kỳ.

Bố đắc: $h(p)=C \log(p)$.

Trường hợp $C=1$ và cơ số logarithm = 2 thì đơn vị tính là bit.

Khi đó: $h(p)=-\log_2(p)$ (dvt: bit) và

$$H(X) = H(p_1, p_2, \dots, p_M) = -\sum_{i=1}^M p_i \log_2(p_i)$$

Qui ước trong cách viết: $\log(p_i) = \log_2(p_i)$

Ví dụ minh họa

Nếu sự kiện A có xác suất xuất hiện là 1/2 thì $H(A) = -\log(1/2) = 1$ (bit)
Xét BNN X có phân phối sau:

X	x ₁	x ₂	x ₃
P	1/2	1/4	1/4

$$H(X) = H(1/2, 1/4, 1/4) = -(1/2\log(1/2)+1/4\log(1/4)+1/4\log(1/4)) = 3/2 \text{ (bit)}$$

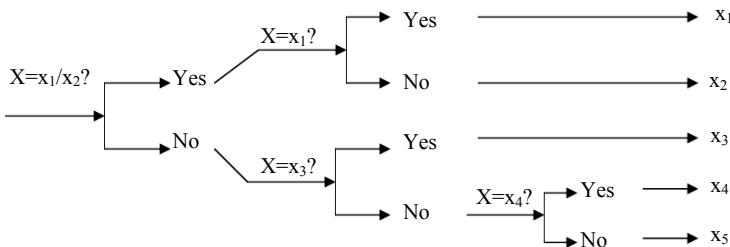
Bài toán về cây tìm kiếm nhị phân - Đặt vấn đề

Giả sử, tìm 1 trong 5 người có tên biết trước sẽ xuất hiện theo phân phối sau:

X	x ₁	x ₂	x ₃	x ₄	x ₅
P	0,2	0,3	0,2	0,15	0,15

Trong đó: x₁, … x₅ lần lượt là tên của 5 người mà ta cần nhận ra với cách xác định tên bằng câu hỏi đúng sai (yes/no).

Sơ đồ dưới đây minh họa cách xác định tên của một người:



Bài toán về cây tìm kiếm nhị phân - Diễn giải

Theo sơ đồ trên:

Để tìm x₁, x₂, x₃ với xác suất tương ứng là 0,2, 0,3, 0,2 ta chỉ cần 2 câu hỏi.

Để tìm x₄, x₅ với xác suất tương ứng 0,15, 0,15 thì ta cần 3 câu hỏi.

Vậy:

Số câu hỏi trung bình là: $2 \times (0,2+0,3+0,2) + 3 \times (0,15+0,15) = 2.3$

Mặt khác: Entropy của X: $H(X) = H(0,2, 0,3, 0,2, 0,15, 0,15) = 2.27$.

Ta luôn có số câu hỏi trung bình luôn $\geq H(X)$ (theo định lý Shannon sẽ trình bày sau). Vì số câu hỏi trung bình trong trường hợp này xác suất H(X) nên đây là số câu hỏi trung bình tối ưu để tìm ra tên chính xác của một người. Do đó, sơ đồ tìm kiếm trên là sơ đồ tối ưu.

Sinh viên tự cho thêm 1 hay 2 sơ đồ tìm kiếm khác và tự diễn giải tương tự - xem như bài tập.

Bài tập

Tính $H(X)$ với phân phối sau:

X	x_1	x_2	x_3
P	1/3	1/3	1/3

Tính $H(Y)$ với phân phối sau:

Y	x_1	x_2	x_3	x_4
P	1/6	2/6	1/6	2/6

BÀI 2.2: CÁC TÍNH CHẤT CỦA ENTROPY

Mục tiêu:

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu các tính chất cơ bản của Entropy,
- Hiểu định lý cực đại của Entropy,
- Vận dụng giải một số bài toán về Entropy,
- Làm cơ sở để vận dụng giải quyết các bài toán tính dung lượng kênh truyền.

Các tính chất cơ bản của Entropy

Xét biến ngẫu nhiên $X = \{x_1, x_2, \dots, x_M\}$. Entropy của biến ngẫu nhiên X có các tính chất:

1. Hàm số $f(M) = H(\frac{1}{M}, \dots, \frac{1}{M})$ đơn điệu tăng.
2. Hàm số $f(ML) = f(M)+f(L)$.
3. $H(p_1, p_2, \dots, p_M) = H(p_1 + p_2 + \dots + p_r, p_{r+1} + p_{r+2} + \dots + p_M)$

$$+ (p_1 + p_2 + \dots + p_r)H(\frac{p_1}{\sum_{i=1}^r p_i}, \dots, \frac{p_r}{\sum_{i=1}^r p_i})$$

$$+ (p_{r+1} + p_{r+2} + \dots + p_M)H(\frac{p_{r+1}}{\sum_{i=r+1}^M p_i}, \dots, \frac{p_M}{\sum_{i=r+1}^M p_i})$$
4. $H(p, 1-p)$ là hàm liên tục theo P.

Minh họa tính chất 1 và 2

Minh họa tính chất 1:

Trong trường hợp biến ngẫu nhiên X có phân phối đều Entropy của X như sau :

$$H(X) = H\left(\frac{1}{M}, \frac{1}{M}, \dots, \frac{1}{M}\right) = -\frac{1}{M} \log \frac{1}{M} - \frac{1}{M} \log \frac{1}{M}, \dots, -\frac{1}{M} \log \frac{1}{M} = -M \frac{1}{M} \log \frac{1}{M}$$

$$\Rightarrow H(X) = -\log \frac{1}{M} = \log M \text{ là hàm đơn điệu tăng}$$

Minh họa tính chất 2:

Trong trường hợp 2 biến ngẫu nhiên X, Y độc lập có phân phối đều với BNN X có M sự kiện và BNN Y có L sự kiện.

Gọi $f(M)$, $f(L)$ lần lượt là Entropy của X, của Y. Theo tính chất 2 của Entropy ta có $f(ML) = f(M) + f(L)$

Minh họa tính chất 3 và 4

Minh họa tính chất 3:

Xét con xúc sắc có 6 mặt với xác suất xuất hiện các mặt được cho trong bảng sau:

X	x_1	x_2	x_3	x_4	x_5	x_6
P	10%	20%	25%	25%	15%	5%

Ta có thể gom các sự kiện x_1, x_2, x_3 lại thành một sự kiện mới là x_{123} có xác suất xuất hiện là 55%, gom sự kiện x_5 và x_6 lại thành sự kiện x_{56} có xác suất 20%.

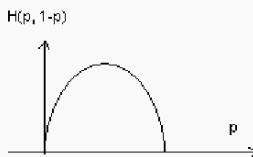
Ta được một nhiên ngẫu nhiên mới X^* có phân phối sau:

X^*	x_{123}	x_4	x_{56}
P	55%	25%	20%

Đến đây các bạn có thể áp dụng công thức để tính, so sánh các Entropy và nhận xét tính chất 3. Phần này xem như bài tập cho sinh viên.

Minh họa tính chất 4:

Để hiểu tính chất thứ 4, ta xét dạng đồ thị của hàm số $H(p, 1-p)$:



Rõ ràng $H(p, 1-p)$ là một hàm liên tục theo p .

Định lý cực đại của entropy

Định lý: $H(p_1, p_2, \dots, p_M) \leq \log(M)$

Trong đó: đẳng thức xảy ra khi và chỉ khi $p_1 = \dots = p_M = 1/M$
Bổ đề: cho 2 bộ $\{p_1, p_2, \dots, p_M\}$ và $\{q_1, q_2, \dots, q_M\}$ là các bộ số dương bất kỳ và

$$\sum_{i=1}^M p_i = \sum_{i=1}^M q_i$$

Khi đó, ta có $H(p_1, p_2, \dots, p_M) = -\sum_{i=1}^M p_i \log_2 p_i \leq -\sum_{i=1}^M p_i \log_2 q_i$ (*)

Đẳng thức xảy ra khi $p_i = q_i$ với $\forall i = 1, \dots, M$.

Chứng minh định lý cực đại của Entropy

Chứng minh bổ đề:

Theo toán học ta luôn có thể chứng minh được $\ln(x) \leq x-1$ với $x > 0$ và đẳng thức đúng khi $x=1$.

Đặt $x = q_i/p_i$ Suy ra $\ln(q_i/p_i) \leq q_i/p_i - 1$ (và đẳng thức đúng khi $q_i=p_i$ với mọi i).

$$\begin{aligned} &\Leftrightarrow \sum_{i=1}^M p_i \ln \frac{q_i}{p_i} \leq \sum_{i=1}^M (q_i - p_i) = 1 - 1 = 0 \\ &\Leftrightarrow -\sum_{i=1}^M p_i \ln p_i \leq -\sum_{i=1}^M p_i \ln q_i \quad (\text{đẳng thức xảy ra khi } q_i=p_i). \end{aligned} \quad (1)$$

Theo toán học ta có $\ln x = \log_2 x / \log_2 e$ (2)

Từ (1) và (2), ta có $-\sum_{i=1}^M p_i \log p_i \leq -\sum_{i=1}^M p_i \log q_i$ (đẳng thức xảy ra khi $q_i=p_i$.)

Chứng minh định lý:

$$\text{Đặt } q_i = \frac{1}{M}, \quad \forall i$$

Từ bổ đề, ta có:

$$-\sum_{i=1}^M p_i \log_2 p_i \leq -\sum_{i=1}^M p_i \log_2 \frac{1}{M} = \log_2 M \sum_{i=1}^M p_i = \log_2 M$$

và đẳng thức chỉ xảy ra khi $p_i = \frac{1}{M}$, $\forall i$ (đpcm).

Bài tập

Bài 1: Cho 2 biến ngẫu nhiên X, Y độc lập nhau có phân phối sau:

X	x ₁	x ₂
P	1/2	1/2

Y	y ₁	y ₂	y ₃	y ₄
P	1/4	1/4	1/4	1/4

Tính H(X), H(Y).

Bài 2: Kiểm tra lại kết quả của bài 1 bằng tính chất 2.

Bài 3: Cho biến ngẫu nhiên X có phân phối sau:

X	x ₁	x ₂	x ₃	x ₄	x ₅	x ₆
P	10%	20%	25%	25%	15%	5%

Ta có thể gom các sự kiện x₁, x₂, x₃ lại thành một sự kiện mới là x₁₂₃ có xác suất xuất hiện là 55%, gom sự kiện x₅ và x₆ lại thành sự kiện x₅₆ có xác suất 20%.

Ta được một biến ngẫu nhiên mới X* có phân phối sau:

X*	x ₁₂₃	x ₄	x ₅₆
P	55%	25%	20%

- Tính entropy của X, X* và kiểm tra lại tính chất 3.
- Kiểm tra lại định lý cực đại từ dữ liệu cho trên.

BÀI 2.3: ENTROPY CỦA NHIỀU BIẾN

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu biết các định nghĩa Entropy của nhiều biến và Entropy có điều kiện,
- Hiểu mối quan hệ giữa $H(X, Y)$ với $H(X)$ và $H(Y)$ khi X, Y độc lập,
- Hiểu mối quan hệ giữa $H(X, Y)$ với $H(X)$ và $H(Y)$ khi X, Y tương quan,
- Vận dụng mối quan hệ giữa các Entropy để tính các Entropy một cách hiệu quả,
- Vận dụng Entropy có điều kiện để làm cơ sở tính lượng tin trong bài học kế tiếp

Định nghĩa Entropy của nhiều biến

Giả sử: X và Y là 2 biến ngẫu nhiên cho trước với $p_{ij} = p(X=x_i, Y=y_j)$ ($\forall i=1, \dots, M$ và $j=1, \dots, L$).

Khi đó, Entropy $H(X, Y)$ có dạng:

$$H(X, Y) = -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log_2 p(x_i, y_j)$$

Hay

$$H(X, Y) = -\sum_{i=1}^M \sum_{j=1}^L p_{ij} \log_2 p_{ij}$$

Một cách tổng quát:

$$H(x_1, \dots, x_n) = -\sum_{x_1, \dots, x_n} p(x_1, \dots, x_n) \log_2 p(x_1, \dots, x_n)$$

Ví dụ Entropy của nhiều biến

Cho 2 BNN X và Y độc lập nhau và có các phân phối:

X=1	0	1	
	0.5	0.5	

Y	0	1	2	
	0.25	0.5	0.25	

Tính $H(X, Y)$.

- Lập phân phối của $P(X, Y)$

X, Y	X=0, Y=0	X=0, Y=1	X=0, Y=2	X=1, Y=0	X=1, Y=1	X=1, Y=2
P(X, Y)	0.125	0.25	0.125	0.125	0.25	0.125

- $H(X, Y) = H(0.125, 0.25, 0.125, 0.125, 0.25, 0.125) = 2.5$ (Bit)

Định nghĩa Entropy có điều kiện

Entropy của Y với điều kiện $X=x_i$ ($i=1, \dots, M$) được định nghĩa là:

$$H(Y/X = x_i) = -\sum_{j=1}^L p(y_j/x_i) \log_2 p(y_j/x_i)$$

Entropy của Y với điều kiện X xảy ra được định nghĩa là:

$$H(Y/X) = \sum_{i=1}^M p(x_i) H(Y/X=x_i)$$

Ví dụ Entropy có điều kiện

Xét biến ngẫu nhiên X và biến ngẫu nhiên Y có tương quan nhau. Các phân phối như sau:

X	1 . 2
P	0.5 0.5

Phân phối của Y có điều kiện X:

Y/X=1	0 1 2
P	0.25 0.5 0.25
Y/X=2	0 1 2
P	0 0 1

Entropy của $Y/X=1$ và $Y/X=2$ như sau :

$$H(Y/X=1)=H(0.25, 0.5, 0.25) = -0.25 \log 0.25 - 0.5 \log 0.5 - 0.25 \log 0.25$$

$$= 0.5 + 0.5 + 0.5 = 1.5 \text{ (Bit)}$$

$$H(Y/X=2) = H(0; 0; 1) = 0 \text{ (Bit)}$$

Entropy của Y khi X xảy ra:

$$H(Y/X) = P(X=1) H(Y/X=1) + P(X=2) H(Y/X=2) = (0.5 \times 1.5) + ((0.5 \times 0) = 0.75 \text{ (Bit).})$$

Quan hệ giữa $H(X, Y)$ với $H(X)$ và $H(Y)$ khi X, Y độc lập

Định lý 1: $H(X, Y) \leq H(X) + H(Y)$ và đẳng thức xảy ra khi X, Y độc lập

Chứng minh:

Ta có:

$$P(x_i) = \sum_{j=1}^L p(x_i, y_j)$$

$$P(y_i) = \sum_{i=1}^M p(x_i, y_j)$$

$$H(X) = -\sum_{i=1}^M p(x_i) \log_2 p(x_i) = -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log_2 p(x_i)$$

$$H(Y) = -\sum_{j=1}^L p(y_j) \log_2 p(y_j) = -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log_2 p(y_j)$$

$$\Rightarrow H(X) + H(Y) = -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) [\log_2 p(x_i) + \log_2 p(y_j)]$$

$$\Rightarrow H(X) + H(Y) = -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) [\log_2 p(x_i) p(y_j)] \quad (1)$$

Đặt $q_{ij} = p(x_i)p(y_j)$

$$\Rightarrow -\sum_{i=1}^M \sum_{j=i}^L p_{ij} \log_2 q_{ij} \geq -\sum_{i=1}^M \sum_{j=1}^L p_{ij} \log_2 p_{ij} \quad (2)$$

Đẳng thức xảy ra khi $p(x_i, y_j) = p_{ij} = q_{ij} = p(x_i)p(y_j)$ hay X, Y độc lập nhau.

(Theo bô đề định lý cực đại)

Mặt khác:

$$H(X, Y) = -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log_2 p(x_i, y_j) = -\sum_{i=1}^M \sum_{j=1}^L p_{ij} \log_2 p_{ij} \quad (3)$$

Từ (1), (2) và (3), ta có $H(X, Y) \leq H(X) + H(Y)$ và đẳng thức xảy ra khi X, Y độc lập (đpcm)

Hệ quả:

$$H(X_1, \dots, X_n) \leq H(X_1) + \dots + H(X_n)$$

$$H(X_1, \dots, X_n; Y_1, \dots, Y_n) \leq H(X_1, \dots, X_n) + H(Y_1, \dots, Y_n)$$

Quan hệ giữa $H(X, Y)$ với $H(X)$ và $H(Y)$ khi X, Y tương quan

Định lý 2: $H(X, Y) = H(X) + H(Y/X) = H(Y) + H(X/Y)$.

Định lý 3: $H(Y/X) \leq H(Y)$ và Dấu đẳng thức xảy ra khi và chỉ khi X và Y độc lập nhau.

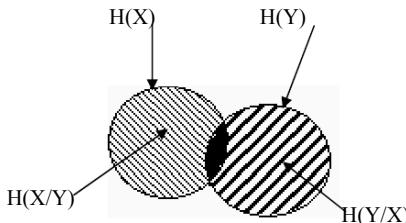
Chứng minh định lý 2:

$$\begin{aligned} H(X, Y) &= -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log_2 p(x_i, y_j) \\ &= -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log_2 [p(x_i) \cdot p(y_j/x_i)] \\ &= -\sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log_2 p(x_i) - \sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log_2 p(y_j/x_i) \\ &= H(X) + H(Y/X) \end{aligned}$$

Tương tự ta có: $H(X, Y) = H(Y) + H(X/Y)$

Chứng minh định lý 3:

Từ định lý 1 và định lý về quan hệ giữa các Entropy, ta có:
 $H(X,Y) = H(X) + H(Y/X) \leq H(X) + H(Y) \Rightarrow H(Y/X) \leq H(Y)$.



Sinh viên tự chứng minh

Bài tập

Xét BNN X và BNN Y có tương quan nhau. Các phân phối như sau:

X	1	2	
P	0.5	0.5	

Phân phối của Y có điều kiện X:

Y/X=1	0	1	2	
P	0.25	0.5	0.25	
Y/X=2	0	1	2	
P	0	0	1	

1. Tính các Entropy sau: $H(X)$, $H(Y)$.
2. Tính các Entropy có điều kiện sau: $H(X/Y)$, $H(Y/X)$.
3. Tính các Entropy sau: $H(X,Y)$.
4. Từ kết quả câu 1,2 và 3 hãy minh họa các định lý 1, 2 và 3 cho bài học.

BÀI 2.4: MINH HỌA CÁC ENTROPY

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết được Yêu cầu của bài toán,
- Biết cách xác định các phân phối ngẫu nhiên của bài toán,
- Vận dụng các bài học trước để tính các Entropy $H(X)$, $H(Y)$ và $H(X,Y)$,
- Vận dụng các bài học trước để tính các Entropy có điều kiện $H(X/Y)$ và $H(Y/X)$,
- Nhận xét và so sánh quan hệ giữa các Entropy
- Ngoài ra còn giúp bạn ôn tập và hiểu rõ hơn các công thức tính Entropy.

Yêu cầu của bài toán

Ta xét ví dụ về một người tổ chức trò chơi may rủi khách quan với việc tung một đồng tiền “có đầu hình – không có đầu hình”. Nếu người chơi chọn mặt không có đầu hình thì thắng khi kết quả tung đồng tiền là không có đầu hình, ngược lại thì thua. Tuy nhiên người tổ chức chơi có thể “ăn gian” bằng cách sử dụng 2 đồng tiền “Thật- Giả” khác nhau sau:

- + Đồng tiền loại 1 (hay đồng tiền thật): đồng chất có 1 mặt có đầu hình.
- + Đồng tiền loại 2 (hay đồng tiền giả): đồng chất, mỗi mặt đều có 1 đầu hình.

Mặc dù người tổ chức chơi có thể “ăn gian” nhưng quá trình trao đổi 2 đồng tiền cho nhau là ngẫu nhiên, vậy liệu người tổ chức chơi có thể “ăn gian” hoàn toàn được không? Hay lượng tin biết và chưa biết của sự kiện lấy một đồng tiền từ 2 đồng tiền nói trên được hiểu như thế nào?

Ta thử xét một trường hợp sau: nếu người tổ chức chơi lấy ngẫu nhiên 1 đồng tiền và sau đó thực hiện việc tung đồng tiền lấy được 2 lần. Qua 2 lần tung đồng tiền, ta đếm được số đầu hình xuất hiện. Dựa vào số đầu hình xuất hiện, ta có thể phán đoán được người tổ chức chơi đã lấy được đồng tiền nào.

Chẳng hạn: Nếu số đầu hình đếm được sau 2 lần tung là 1 thì đồng tiền đã lấy được là đồng tiền thật, ngược lại nếu số đầu hình đếm được là 2 thì đồng tiền đã lấy được có thể là thật hay cũng có thể là giả. Như vậy, ta đã nhận được một phần thông tin về loại đồng tiền qua số đầu hình đếm được sau 2 lần tung. Ta có thể tính được lượng tin đó bằng bao nhiêu? (*Việc tính lượng tin này sẽ được thảo luận sau*).

Xác định các phân phối ngẫu nhiên của bài toán

Đặt X là biến ngẫu nhiên về loại đồng tiền.

Phân phối của X:

X	1	2
P	0.5	0.5

Đặt biến ngẫu nhiên Y là số đầu hình đếm được sau 2 lần tung:

Phân phối của Y khi nhận được đồng tiền có 1 mặt có đầu hình ($Y/X=1$)

Y/X=1	0	1	2
P	0.25	0.5	0.25

Phân phối của Y khi nhận được đồng tiền có 2 mặt đều có đầu hình ($Y/X=2$)

$Y/X=2$	0	1	2
P	0	0	1

Tìm phân phối của Y:

$$P(Y=0) = p(X=1)p(Y=0/X=1) + p(X=2)p(Y=0/X=2) = 0,5 \times 0,25 + 0,5 \times 0 = 0,125$$

$$P(Y=1) = p(X=1)p(Y=1/X=1) + p(X=2)p(Y=1/X=2) = 0,5 \times 0,5 + 0,5 \times 0 = 0,250$$

$$P(Y=2) = p(X=1)p(Y=2/X=1) + p(X=2)p(Y=2/X=2) = 0,5 \times 0,25 + 0,5 \times 1 = 0,625$$

Y	0	1	2
P	0.125	0.25	0.625

Minh họa Entropy $H(X)$, $H(Y)$ và $H(X,Y)$

Entropy của X:

$$H(X) = H(0.5, 0.5)$$

$$= -(0.5)\log(0.5) - (0.5)\log(0.5) = 1 \text{ (bit)}$$

Entropy của Y:

$$H(X) = H(0.125, 0.25, 0.625)$$

$$= -(0.125)\log(0.125) + (0.25)\log(0.25) + (0.625)\log(0.625) = 1.2988 \text{ (bit)}$$

Entropy của X và Y: $H(X,Y)$

Xem như bài tập dành cho các bạn sinh viên

Entropy của Y/X là trung bình của các entropy $Y/X=x_i$.

Vậy, Entropy của Y có điều kiện X: $H(Y/X) = \sum_{i=1}^M p(x_i).H(Y/X=x_i)$

Tương tự: $H(Y/Z/X)$, $H(Z/X,Y)$

Minh họa Entropy $H(X/Y)$ và $H(Y/X)$

Tính Entropy của Y khi biết X: $H(Y/X)$

$$H(Y/X=1) = H(0.25, 0.5, 0.25)$$

$$= -(0.25)\log 0.25 + 0.5\log 0.5 + 0.25\log 0.25 = 1.5 \text{ (bit)}$$

$$H(Y/X=2) = H(0, 0, 1) = 0$$

$$H(Y/X) = p(X=1)H(Y/X=1) + p(X=2)H(Y/X=2) = 0.5 \times 1.5 + 0.5 \times 0 = 0.75 \text{ (bit)}$$

Tính Entropy của X khi biết Y: $H(X/Y)$

Xem như bài tập dành cho các bạn sinh viên (Gợi ý: bạn nên lập các phân phối cho các trường hợp $(X/Y=0)$, $(X/Y=1)$ và $(X/Y=2)$).

Minh họa quan hệ giữa các Entropy

Xem như bài tập dành cho các bạn sinh viên.

Gợi ý: sau khi bạn tính $H(X,Y)$ và $H(X/Y)$, bạn dựa vào các định lý 1,2 và 3 cùng với các kết quả đã tính được để so sánh và minh họa.

BAI 2.5: ĐO LƯỢNG TIN (MESURE OF INFORMATION)

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết bài toán tính lượng tin,
- Hiểu định nghĩa lượng tin,
- Biết cách tính lượng tin,
- Có thể vận dụng để tính lượng tin cho các bài toán tương tự.

Đặt vấn đề bài toán

Ta xét ví dụ về một người tổ chức trò chơi may rủi khán quan với việc tung một đồng tiền “có đầu hình – không có đầu hình”. Nếu người chơi chọn mặt không có đầu hình thì thắng khi kết quả tung đồng tiền là không có đầu hình, ngược lại thi thua. Tuy nhiên người tổ chức chơi có thẻ “ăn gian” bằng cách sử dụng 2 đồng tiền “Thật- Giả” khác nhau sau:

- + Đồng tiền loại 1 (hay đồng tiền thật): đồng chất có 1 mặt có đầu hình.
- + Đồng tiền loại 2 (hay đồng tiền giả): đồng chất, mỗi mặt đều có 1 đầu hình.

Mặc dù người tổ chơi có thẻ “ăn gian” nhưng quá trình trao đổi 2 đồng tiền cho nhau là ngẫu nhiên, vậy liệu người tổ chức chơi có thẻ “ăn gian” hoàn toàn được không? Ta thử xét một trường hợp sau: nếu người chơi lấy ngẫu nhiên 1 đồng tiền và sau đó thực hiện việc tung đồng tiền lấy được 2 lần. Qua 2 lần tung đồng tiền, ta đếm được số đầu hình xuất hiện. Dựa vào số đầu hình xuất hiện, hãy tính lượng tin về loại đồng tiền lấy được là bao nhiêu?

Xác định các phân phối của bài toán

Đặt biến ngẫu nhiên X là loại đồng tiền, khi đó phân phối của X có dạng :

X	1	2
P	0.5	0.5

Đặt biến ngẫu nhiên Y là số đầu hình đếm được sau 2 lần tung. Khi đó ta có thể xác định được phân phối của Y trong 2 trường hợp sau.

Trường hợp 1: Phân phối của Y khi biết đồng tiền là thật (X=1) có dạng:

Y/X=1	0	1	2
P	0.25	0.5	0.25

Trường hợp 2: Phân phối của Y khi biết đồng tiền là giả (X=2) có dạng:

Y/X=2	0	1	2
P	0	0	1

Ta có thể tính dễ dàng phân phối của Y như sau:

Y	0	1	2
P	0.125	0.25	0.625

Nhận xét dựa theo entropy

Từ các bảng phân phối trên, ta có:

Entropy của Y:

$$H(Y) = H(0.125, 0.25, 0.625) = 1.3 \text{ (bit)}$$

Entropy của Y khi biết X

$$H(Y/X=1) = H(0.25, 0.5, 0.25) = 1.5 \text{ (bit)}$$

$$H(Y/X=2) = H(0, 0, 1) = 0$$

$$H(Y/X) = p(X=1)H(Y/X=1) + p(X=2)H(Y/X=2) = 0.75 \text{ (bit)}$$

Vậy, $H(Y) > H(Y/X)$

Định nghĩa lượng tin

Từ nhận xét về quan hệ giữa các entropy ở trên, ta có thể định nghĩa lượng tin như sau:

Định nghĩa: Lượng tin (hay thông lượng) của X khi Y xảy ra là lượng chênh lệch giữa lượng không chắc chắn của X và lượng không chắc chắn của X khi Y xảy ra có quan hệ với X.

Ta có thể hiểu khái niệm này như sau: X và Y là 2 biến ngẫu nhiên nên chúng có 2 lượng tin không chắc chắn. Nếu X và Y độc lập, thì X xảy ra không ảnh hưởng tới Y nên ta vẫn không biết gì thêm về X và X giữ nguyên lượng không chắc chắn của nó. Trong trường hợp này lượng tin về X khi Y xảy ra là bằng 0. Nếu Y có tương quan với X thì khi Y xảy ra ta biết hoàn toàn về Y và một phần thông tin về X. Phần thông tin đó chính là lượng tin đã biết về X nhưng vẫn chưa biết hết về X. Bài toán ở đây là tính lượng tin đã biết về X khi Y xảy ra.

Ký hiệu: $I(X/Y) = H(X) - H(X/Y)$ là lượng tin đã biết về X khi Y đã xảy ra.

Chú ý: ta luôn có $I(X/Y) = I(Y/X)$

Ví dụ: xét lại ví dụ trên, ta có lượng tin về X khi biết Y là

$$I(X/Y) = I(Y/X) = H(Y) - H(Y/X) = 1.3 - 0.75 = 0.55 \text{ (bit)}.$$

Bài tập

1. Thực hiện một phép thử con xúc sắc đồng chất đồng thời với một đồng tiền cũng đồng chất. Trong đó, con xúc sắc có các mặt điểm từ 1 đến 6, đồng tiền một mặt có đầu hình và mặt kia không có đầu hình. Trước tiên thử con xúc sắc, nếu số điểm ≤ 4 thì tung đồng tiền một lần, ngược lại thì tung đồng tiền hai lần. Tính lượng tin về số điểm con xúc sắc khi biết thông tin về số đầu hình đếm được.

2. Người ta thực hiện một khảo sát trên các sinh viên đại học về mối quan hệ giữa khả năng học tập với sở hữu phương tiện di lại và tình thần ái hữu. Kết quả cho thấy:

Trong tổng số sinh viên có $3/4$ sinh viên hoàn thành chương trình học và $1/4$ không hoàn thành. Trong số sinh viên hoàn thành chương trình học, 10% có xe con. Ngược lại, trong số sinh viên không hoàn thành chương trình học có tới 50% có xe con.

Tất cả sinh viên có xe con đều tham gia hội ái hữu sinh viên. Trong số sinh viên không có xe con (kể cả hoàn thành hay không hoàn thành khóa học) thì 40% sinh viên tham gia hội ái hữu sinh viên.

- a. Tìm thông tin về trạng thái học tập của sinh viên khi biết điều kiện về phương tiện di lại của họ.
- b. Tìm thông tin về tình trạng học tập của sinh viên khi biết tình thần ái hữu của họ.

3. Những người dân của một làng được chia làm 2 nhóm A và B. Một nửa nhóm A chuyên nói thật, 3/10 nói dối và 2/10 từ trối trả lời. Trong nhóm B: 3/10 nói thật, 1/2 nói dối và 2/10 từ trối trả lời. Giả sử p là xác suất chọn 1 người thuộc nhóm A và $I(p) = I(Y/X)$ là lượng tin về người nói thật sau khi đã chọn nhóm, tính $I(p)$, tìm p^* sao $I(p^*) = \text{Max}(I(p))$ và tính $I(p^*)$.

CHƯƠNG 3: SINH MÃ TÁCH ĐƯỢC

(Decypherable Coding)

Mục tiêu:

Phân này đề cập đến bài toán mã hóa (coding) các giá trị của một biến X. Khi mã các giá trị của X người ta phải sử dụng bảng ký tự mã (Coding Character Table) hay bảng chữ cái (Code Alphabet). Như vậy, một giá trị x của X sẽ được mã thành một từ mã (Code Word) w dưới dạng một dãy các ký tự mã với độ dài là n ký tự. Trong truyền tin, một dãy các giá trị của X được phát sinh và được mã thành một dãy liên tục các từ mã hay một dãy các ký tự mã lấy từ bảng ký tự mã. Vấn đề cần giải quyết là:

1. Khi nhận một dãy ký tự mã liên tục đó thì ta có thể giải mã thành một dãy các giá trị duy nhất của X hay không ? Nói cách khác, dãy ký tự mã này có tách được thành các từ mã một cách duy nhất hay không ?
2. Chỉ ra phương pháp xây dựng mã tách được tối ưu.

BÀI 3.1: KHÁI NIỆM VỀ MÃ TÁCH ĐƯỢC

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết yêu cầu của bài toán sinh mã,
- Hiểu khái niệm về bảng mã tách được và bảng mã không tách được,
- Hiểu khái niệm về bảng mã tức thời,
- Hiểu giải thuật kiểm tra tính tách được của một bảng mã,
- Vận dụng giải thuật kiểm tra tính tách được của một bảng mã để kiểm tra xem một bảng mã có phải là bảng mã tách được hay không.

Đặt vấn đề bài toán sinh mã

Giả sử nguồn tin X xuất hiện và được ghi lại thông qua một thiết bị đặc biệt. Chẳng hạn như ảnh được ghi lại bằng máy ảnh, âm thanh được ghi lại bằng máy ghi âm, ... Qua kênh truyền, những thông tin này cần phải được mã hóa cho phù hợp. Để có thể mã hóa người ta cần một bảng chữ cái gồm các chữ cái quy định trước (chẳng hạn bảng chữ cái la tinh, bảng mã nhị phân, ...). Mỗi giá trị của X sau đó được mã dưới dạng một dãy hữu hạn các chữ cái và ta gọi dãy hữu hạn các chữ cái gán cho một giá trị của x là một từ mã.

Ta xét BNN $X = \{x_1, x_2, \dots, x_n\}$ có phân phối $\{p_1, p_2, \dots, p_n\}$ được quan sát liên tục và độc lập. Dãy các giá trị nhận được gọi là thông báo (Message) có dạng $x_1|x_2|...|x_n$. Tập hợp $A = \{a_1, a_2, \dots, a_n\}$ là tập hợp ký tự mã (Code Characters) hay là bảng chữ cái (Code Alphabet) dùng để sinh mã. Một giá trị $x_i \in X$ được gán bởi một dãy hữu hạn các ký tự mã được gọi là từ mã (Code word). Tập hợp gồm tất cả các từ mã gán cho tất cả các giá trị của X được gọi là bộ mã hay bảng mã (Code). Các từ mã phải khác nhau từng đôi một.

Bộ mã được gọi là tách được nếu như từ một dãy các ký tự mã nhận được liên tục (được mã hóa từ bộ mã này), ta luôn luôn giải mã được với kết quả duy nhất là dãy các giá trị gốc của X.

Shannon (1948) lần đầu tiên đã đưa ra định lý cơ sở về sinh mã tách được. Mc Millan (1956) đã chứng minh định lý về điều kiện cần và đủ của bảng mã tách được. Nhưng vẫn đề sinh mã tách được chỉ được xét một cách chuẩn mực bởi Feinstein (1958), Abramson (1963) và Fano (1961). Sardinas(1960) và Patterson (1963) đã đưa ra định lý về giải thuật kiểm tra tính tách được của một bảng mã. Abramson (1963) đã đưa ra khái niệm bảng mã tức thời.

Trong phạm vi bài giảng này, bài toán sinh mã tối ưu được đặt ra ở đây là tìm ra một phương pháp sinh mã sao cho độ dài trung bình của các từ mã trong bộ mã là nhỏ nhất. Nghĩa là, nếu giá trị x_i được gán bởi từ mã có độ dài n_i thì bài toán sinh mã phải thỏa:

$$\sum_{i=1}^n p_i n_i \rightarrow \text{Min}$$

Huffman (1950) đã đưa ra qui trình xây dựng một bảng mã tối ưu thỏa yêu cầu này.

Khái niệm về bảng mã không tách được

Bảng mã không tách được là bảng mã mà khi mã hóa thông báo **Msg** ta sẽ nhận được một dãy các từ mã **ws**, và khi giải mã dãy các từ mã **ws** thì ta có thể nhận được nhiều thông báo **Msg** khác nhau.

Ví dụ: Xét biến ngẫu nhiên $X=\{x_1, x_2, x_3, x_4\}$ có bảng mã $W=\{w_1=0, w_2=1, w_3=01, w_4=10\}$.

Giả sử thông báo nguồn có nội dung: $x_1x_2x_3x_4x_3x_2x_1$. Khi đó dãy mã tương ứng viết từ W có dạng: 0101100110.

Nếu giải mã tuần tự từ trái qua phải ta nhận kết quả: $x_1x_2x_1x_2x_2x_1x_1x_2x_2x_1$. Nhưng nếu bằng phương pháp khác ta có thể nhận được kết quả: $x_3x_3x_4x_3x_4$ và nhiều thông báo khác nữa.

Nhận xét: Bảng mã giải mã không tách được là bảng mã mà trong đó tồn tại ít nhất một từ mã này là mã khóa của một hay nhiều từ mã khác trong bộ mã (ví dụ từ mã $w_1=0$ hay $w_2=1$ là mã khóa của w_3).

Bảng mã tách được

Bảng mã tách được là bảng mã mà khi mã hóa thông báo **Msg** ta sẽ nhận được dãy các từ mã **ws**, và khi giải mã dãy các từ mã **ws** thì ta chỉ nhận được một thông báo duy nhất là **Msg** ban đầu.

Ví dụ: Xét biến ngẫu nhiên $X=\{x_1, x_2\}$ có bảng mã tương ứng $W=\{w_1=0, w_2=01\}$.

Phương pháp giải mã được sử dụng như sau: chỉ giải mã khi nào đã nhận được đoạn mã với độ dài bằng độ dài của từ mã dài nhất.

Giả sử dãy mã nhận được (cần giải mã) là: 0010000101001.

Sử dụng phương pháp giải mã trên ta nhận được duy nhất dãy thông báo gốc:

$x_1x_2x_1x_1x_1x_2x_2x_1x_2$.

Có thể chi tiết hóa các bước giải mã dãy từ mã trên như sau:

Nhận được đoạn 00 \rightarrow Giải ra x_1 , còn lại 0.

Nhận tiếp 1 \rightarrow 01 \rightarrow Giải ra x_2 .

Nhận tiếp 00 \rightarrow Giải ra x_1 , còn lại 0.

- Nhận tiếp 0 -> 00 -> Giải ra x_1 , còn lại 0.
 Nhận tiếp 0 -> 00 -> Giải ra x_1 , còn lại 0.
 Nhận tiếp 1 -> 01 -> Giải ra x_2 .
 Nhận tiếp 01 -> Giải ra x_2 .
 Nhận tiếp 00 -> Giải ra x_1 , còn lại 0.
 Nhận tiếp 1 -> 01 -> Giải ra x_2 .

Kết quả dãy thông báo là: $x_1x_2x_1x_1x_1x_2x_2x_1x_2$.

Kết luận: Bảng mã tách được là bảng mã mà trong đó không tồn tại từ mã này là mã khóa từ mã khác, tuy nhiên vẫn có thể tồn tại từ mã này là tiền tố (phản đầu) của từ mã kia.

Khái niệm bảng mã tức thời

Bảng mã tức thời là bảng mã mà khi mã hóa thông báo **Msg** ta sẽ nhận được dãy các từ mã **ws**, và khi giải mã dãy các từ mã **ws** thì ta chỉ nhận được một thông báo duy nhất là **Msg** ban đầu. **Abramson đã chứng minh được kết quả sau: Bảng mã tức thời là bảng mã không tồn tại từ mã này là tiền tố của từ mã khác.**

Ví dụ 1: Bảng mã $W=\{w_1=10; w_2=101; w_3=100\}$ không phải bảng mã tức thời vì w_1 là tiền tố của w_2 và w_3 .

Ví dụ 2: Bảng mã $W=\{w_1=0, w_2=100, w_3=101, w_4=11\}$ là bảng mã tức thời vì không tồn tại từ mã này là tiền tố của từ mã khác.

Giải thuật kiểm tra tính tách được của bảng mã

Thủ tục sau đây do Sardinas (1960), Patterson (1963) và Abramson (1963) đưa ra nhằm kiểm tra xem một bảng mã nào đó có phải là bảng mã tách được (bảng mã cho phép giải mã duy nhất) hay không.

Input: Bảng mã W

Output: Kết luận bảng mã tách được hay không tách được.

Giải thuật:

Bước khởi tạo: Gán tập hợp $S_0=W$.

Bước 1: xác định tập hợp S_1 từ S_0 :

- Khởi tạo $S_1=\{\}$
- Với $\forall w_i, w_j \in S_0$, ta xét: nếu $w_i=w_jA$ (w_j là tiền tố của w_i) hoặc $w_j=w_iA$ (w_i là tiền tố của w_j) thì thêm A (phản hậu tố) vào S_1 .

Bước k: xác định tập hợp S_k ($k \geq 2$) từ tập hợp S_0 và S_{k-1} :

- Khởi tạo: $S_k=\{\}$
- Với $\forall w_i \in S_0$ và $\forall v_j \in S_{k-1}$, ta xét: nếu $w_i=v_jA$ (v_j là tiền tố của w_i) hoặc $v_j=w_iA$ (w_i là tiền tố của v_j) thì thêm A (phản hậu tố) vào S_k .

Điều kiện để dừng vòng lặp:

Nếu $S_k=\{\}$ thì dừng và kết luận bảng mã tách được ($k \geq 1$).

Nếu tồn tại từ mã w_i trong S_k hay $S_k \cap S_0 \neq \emptyset$ thì dừng và kết luận bảng mã không tách được.

Nếu $S_k=S_{k-1}$ thì dừng và kết luận bảng mã tách được ($k \geq 1$).

Bài toán 1 - yêu cầu

Bài toán: Kiểm tra xem bảng mã $W=\{a, c, ad, abb, bad, deb, bbcd\}$ có phải là bảng mã tách được hay không?

Áp dụng Giải thuật kiểm tra tính tách được của một bảng mã:

Bước khởi tạo: $S_0=\{a, c, ad, abb, bad, deb, bbcd\}$

Bước 1: Tính S_1

Khởi tạo $S_1=\{\}$

Vì a là tiền tố của ad nên đưa phần hậu tố “ d ” vào $S_1 \Rightarrow S_1=\{d\}$.

Vì a là tiền tố của abb nên đưa phần hậu tố “ bb ” vào $S_1 \Rightarrow S_1=\{d, bb\}$.

Kiểm tra điều kiện dừng: không thỏa -> qua bước 2.

Bước 2: Tính S_2 từ S_0 và S_1 .

Khởi tạo $S_2=\{\}$.

Vì $d \in S_1$ là tiền tố của $deb \in S_0$ nên đưa phần hậu tố “ eb ” vào S_2

$\Rightarrow S_2=\{eb\}$

Vì $bb \in S_1$ là tiền tố của $bbcd \in S_0$ nên đưa phần hậu tố “ cde ” vào S_2

$\Rightarrow S_2=\{eb, cde\}$

Kiểm tra điều kiện dừng: không thỏa -> qua bước 3.

Bài toán 1 - Áp dụng giải thuật

Bước 3: Tính S_3 từ S_0 và S_2 .

Khởi tạo $S_3=\{\}$.

Vì $c \in S_0$ là tiền tố của $cde \in S_2$ nên đưa phần hậu tố “ de ” vào S_3

$\Rightarrow S_3=\{de\}$

Kiểm tra điều kiện dừng: không thỏa -> qua bước 4.

Bước 4: Tính S_4 từ S_0 và S_3 .

Khởi tạo $S_4=\{\}$.

Vì $de \in S_3$ là tiền tố của $deb \in S_0$ nên đưa phần hậu tố “ b ” vào S_4

$\Rightarrow S_4=\{b\}$

Kiểm tra điều kiện dừng: không thỏa -> qua bước 5.

Bước 5: Tính S_5 từ S_0 và S_4 .

+ khởi tạo $S_5=\{\}$.

+ Vì $b \in S_4$ là tiền tố của $bad \in S_0$ nên đưa phần hậu tố “ ad ” vào $S_5 \Rightarrow S_5=\{ad\}$

+ Vì $b \in S_4$ là tiền tố của $bbcd \in S_0$ nên đưa “ $bcde$ ” vào S_5

$\Rightarrow S_5=\{ad, bcde\}$

Kiểm tra điều kiện dừng: Vì S_5 có chứa từ mã ad nên dừng lại và kết luận đây là bảng mã không tách được.

Bài toán 2

Bài toán: Kiểm tra xem bảng mã $W=\{010, 0001, 0110, 1100, 00011, 00110, 11110, 101011\}$ có phải là bảng mã tách được không?

Áp dụng Giải thuật kiểm tra tính tách được của một bảng mã:

Bước khởi tạo và bước 1

- Tập hợp $S_0=\{010, 0001, 0110, 1100, 00011, 00110, 11110, 101011\}$

- Tập hợp $S_1=\{1\}$

Dành cho sinh viên tự làm các bước tiếp theo.

Kết quả gợi ý:

Tập hợp $S_2=\{100, 1110, 01011\}$

Tập hợp $S_3=\{11\}$

Tập hợp $S_4=\{00, 110\}$

Tập hợp $S_5=\{01, 0, 011, 110\}$

Tập hợp $S_6=\{0, 10, 001, 110, 0011, 0110\}$

Tập hợp S_6 chứa từ mã 0110 nên bảng mã này không phải là bảng mã tách được.

Bài tập

1. Hãy cho biết bảng mã sau có phải là bảng mã tách được hay không?
 $W=\{w_1=00, w_2=01, w_3=0010, w_4=0111, w_5=0110\}$
2. Hãy lấy ví dụ một bảng mã tách được, và chứng minh nó là bảng mã tách được.

BÀI 3.2: QUAN HỆ GIỮA MÃ TÁCH ĐƯỢC VÀ ĐỘ DÀI MÃ

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể hiểu:

- Định lý Kraft (1949),
- Định nghĩa cây bậc D cỡ K,
- Vấn đề sinh mã cho cây bậc D cỡ K,
- Vận dụng định lý Kraft để kiểm tra sự tồn tại bảng mã tách được và sinh bảng mã tách được.

Định lý Kraft(1949).

Giả sử $X = \{x_1, x_2, \dots, x_M\}$ là biến ngẫu nhiên chứa các giá trị cần truyền có phân phối là $P = \{p_1, p_2, \dots, p_M\}$.

$A = \{a_1, a_2, \dots, a_D\}$ là bộ ký tự sinh mã có D chữ cái (D được gọi là cơ số sinh mã).

Giá trị x_i được mã hóa thành từ mã w_i có độ dài là n_i .

Đặt $N = \{n_1, n_2, \dots, n_M\}$ là tập hợp độ dài các từ mã.

Định lý (Kraft- 1949):

Điều kiện cần và đủ để tồn tại bảng mã tíc thời với độ dài $N = \{n_1, n_2, \dots, n_M\}$ là

$$\sum_{i=1}^M D^{-n_i} \leq 1$$

Ví dụ 1: Bộ mã $W = \{w_1, w_2, w_3\}$ với $M=3$; $n_1=1$; $n_2=2$; $n_3=3$; $D=2$

$$\sum_{i=1}^M D^{-n_i} = \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} = \frac{7}{8} < 1$$

=> Tồn tại bảng mã tíc thời.

Ví dụ 2: Bộ mã W={w₁, w₂, w₃} với M=3; n₁=n₂=1; n₃=2; D=2

$$\sum_{i=1}^M D^{-n_i} = \frac{1}{2^1} + \frac{1}{2^1} + \frac{1}{2^2} = \frac{5}{4} > 1$$

=> Không tồn tại bảng mã tíc thời.

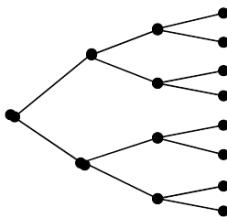
Đề nghị: sinh viên tìm hiểu nội dung tiếp theo và trở lại giải thích 2 ví dụ trên.

Định nghĩa cây bậc D cỡ k.

Định nghĩa: Cây bậc D cỡ k là cây có hệ thống nút, cạnh thỏa điều kiện:

- Từ 1 nút có số cạnh đi ra không vượt quá D hay một nút có không quá D nút con.
- Nút cuối cùng (Nút lá) cách nút gốc không vượt quá k cạnh.

Ví dụ: cây bậc D=2 và cõ k=3

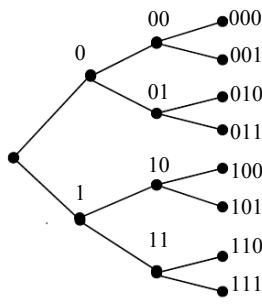


Vấn đề sinh mã cho cây bậc D cõ k

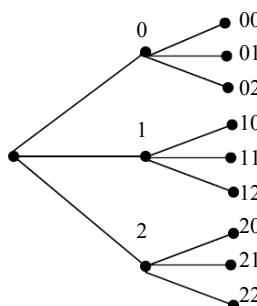
Sinh mã cho các nút của cây bậc D cõ K (trừ nút gốc):

Để đơn giản hóa: mỗi nút (trừ nút gốc) được ký hiệu bởi dây ký hiệu của nút cha làm tiền tố + một ký tự bổ sung lấy từ tập hợp $\{0, 1, 2, \dots, D-1\}$ thay cho bảng chữ cái $A=\{a_1, a_2, \dots, a_D\}$.

Ví dụ 1: Cây bậc D=2 cõ k=3



Ví dụ 2: Cây bậc D=3 cõ k=2.



Tính chất:

- + Các nút (trừ nút gốc) của cây đều được mã hóa từ bảng chữ cái $\{0, 1, 2, \dots, D-1\}$
- + Mỗi nút (đã mã hóa) có mã của nút kè trước là tiền tố.
- + Tổng số các nút lá bằng $D^k =$ tổng số các mã tucus thời có thể có.

Chứng minh định lý Kraft (Điều kiện cân)

Giả sử, cho trước bảng mã tucus thời $W=\{w_1, w_2, \dots, w_M\}$ với $N=\{n_1 \leq n_2 \leq \dots \leq n_M\}$. Ta cần c/m:

$$\sum_{i=1}^M D^{-n_i} \leq 1$$

Xây dựng cây bậc D cõ n_M và sinh mã cho các nút trừ nút gốc với các ký tự mã lấy từ bảng chữ cái $A = \{0, 1, 2, \dots, D-1\}$. Mã tại mỗi nút (trừ nút gốc) đều có khả năng được chọn là từ mã.

Như vậy, ta tiến hành chọn các từ mã cho bảng mã tucus thời với qui tắc là: một nút nào đó được chọn để gán một từ mã thì tất cả các nút kè sau nút gán từ mã phải được xóa. Cụ thể như sau:

Chọn một nút có mã với độ dài mã là n_1 gán cho nó một từ mã w_1 .

\Rightarrow Tổng số nút lá được xóa tương ứng là $D^{n_M - n_1}$

Chọn một nút có mã với độ dài mã là n_2 gán cho nó một từ mã w_2 .

\Rightarrow Tổng số nút lá được xóa tương ứng là $D^{n_M - n_2}$

.....

Chọn một nút có mã với độ dài mã là n_n gán cho nó một từ mã w_n .

\Rightarrow số nút lá được gán từ mã là $D^{n_M - n_M}$

Vậy số nút lá bị xóa hoặc được gán từ mã là:

$$\Rightarrow D^{n_M - n_1} + D^{n_M - n_1} + \dots + D^{n_M - n_M} = \sum_{i=1}^M D^{n_M - n_i} \leq D^{n_M} = \text{tổng số nút lá.}$$

$$\Rightarrow \sum_{i=1}^M D^{-n_i} \leq 1 \text{ (đpcm)}$$

Chứng minh định lý Kraft (Điều kiện đủ)

Giả sử: $\sum_{i=1}^M D^{-n_i} \leq 1$, để cần chứng minh tồn tại bảng mã tức thời với $N=\{n_1, n_2, \dots, n_M\}$, ta chỉ cần chỉ ra thủ tục xây dựng bảng mã tức thời như sau:

Thủ tục tạo mã tức thời:

Xét $N=\{n_1, n_2, \dots, n_M\}$ và cơ sở sinh mã là D :

Bước 1: Ta xếp thứ tự $n_1 \leq n_2 \leq \dots \leq n_M$, xây dựng cây bậc D cỡ $k=n_M$ và sinh mã cho các nút.

Bước 2: Chọn nút bất kỳ trên cây có độ dài n_1 gán cho từ mã w_1 và xóa tất cả các nút kề sau nó.

Bước 3: Lặp lại các bước 2 đối với việc chọn các từ mã còn lại w_2, \dots, w_M ứng với n_2, \dots, n_M .

\Rightarrow Bảng mã $W=\{w_1, w_2, \dots, w_M\}$ là bảng mã tức thời.

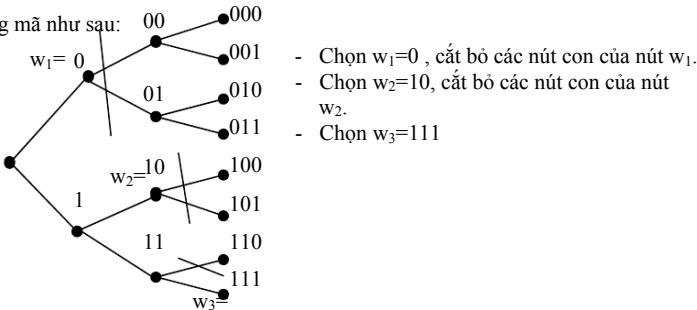
Ví dụ minh họa định lý Kraft

Ví dụ 1: Xét bảng mã thỏa $M=3$, $D=2$, $n_1=1$, $n_2=2$, $n_3=3$. Vậy ta kiểm tra xem có tạo được bảng mã tức thời hay không?

$$\text{Ta có } \sum_{i=1}^3 2^{-n_i} = 2^{-1} + 2^{-2} + 2^{-3} = \frac{7}{8} < 1$$

$\Rightarrow W=\{w_1, w_2, w_3\}$ là bảng mã tức thời

Ta Xây dựng bảng mã như sau:



Chú ý: ngoài bảng mã tíc thời chọn được ở trên, ta còn có thể sinh được nhiều bảng mã tíc thời khác. Để nghị sinh viên đưa ra bảng mã tíc thời khác.

Bài tập

1. Tìm 1 bảng mã tách được thỏa tính chất $D = 2$, $k = 4$?
2. Tìm tất cả các bảng mã tách được thỏa tính chất $D=2$, $k=3$?
3. Hãy chỉ ra bảng mã sau đây là bảng mã không tách được:
 $W=\{w_1=00, w_2=1, w_3=100, w_4=110, w_5=111\}$
4. Hãy tìm một bảng mã nhị phân tách được có ít nhất 5 từ mã thỏa điều kiện

$$\sum_{i=1}^M D^{-n_i} = 1$$

BÀI 3.3: TÍNH TỐI ƯU CỦA ĐỘ DÀI MÃ

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu định lý Shannon (1948),
- Biết được các tiêu chuẩn đánh giá bảng mã tối ưu tuyệt đối và bảng mã tối ưu tương đối,
- Điều kiện nhận biết một bảng mã tối ưu,
- Hiểu Định lý Huffman,
- Biết Phương pháp sinh mã Huffman,
- Vận dụng phương pháp sinh mã Huffman để sinh mã Huffman cho một thông báo,
- Vận dụng phương pháp sinh mã Huffman để viết chương trình nén.

Định lý Shannon (1948)

Phát biểu định lý:

$$\text{Đặt } \bar{n} = \sum_{i=1}^M p_i n_i \text{ là độ dài trung bình của bảng mã.}$$

$$\text{Khi đó } \bar{n} \geq \frac{H(X)}{\log_2 D}$$

$$\text{Đáu đắng thức xảy ra khi và chỉ khi } p_i = D^{-n_i} \text{ hay } \sum_{i=1}^M D^{-n_i} = 1$$

Điển giải: Đối với mã tách được độ dài trung bình của mã sẽ có cận dưới là $\frac{H(X)}{\log_2 D}$. Nếu mã không tách được độ dài trung bình của nó có thể nhỏ hơn cận dưới. Nếu mã tách được không tối ưu thì độ dài của nó sẽ lớn hơn nhiều so với cận dưới, còn nếu mã tách được tối ưu thì độ dài trung bình của nó gần với cận dưới.

Bài toán đặt ra sẽ là tìm phương pháp xây dựng bảng mã tách được tối ưu.

Chú ý:

$$H_D(X) = -\sum p_i \log_D p_i$$

$$H_D(X) = \frac{H(X)}{\log_2 D} = \frac{-\sum p_i \log_2 p_i}{\log_2 D}$$

là entropy của X với cơ số D.

Bảng mã tối ưu tuyệt đối

Định lý: Bảng mã được gọi là tối ưu tuyệt đối khi $\bar{n} = \frac{H(X)}{\log_2 D}$ hay $p_i = D^{-n_i}$

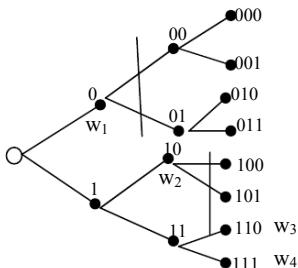
Ví dụ: xét biến ngẫu nhiên $X = \{x_1, x_2, x_3, x_4\}$

Có phân phối: $P = \{1/2, 1/4, 1/8, 1/8\}$

Có bảng mã $W = \{w_1=0, w_2=10, w_3=110, w_4=111\}$

Tính được độ dài trung bình từ mã: $\bar{n} = \frac{1}{2}*1 + \frac{1}{4}*2 + \frac{1}{8}*3 + \frac{1}{8}*3 = \frac{12}{8} = 1.75$

Tính Entropy của X: $H(X) = H(0.5, 0.25, 0.125, 0.125) = 0.5 + 0.5 + 0.375 + 0.375 = 1.75$
 $\log_2 D = 1$.



$W = \{w_1, w_2, w_3, w_4\}$ là bảng mã tối ưu
tuyệt đối vì thỏa điều kiện:

$$\bar{n} = \frac{H(X)}{\log_2 D}$$

Bảng mã tối ưu tương đối

Định lý: Bảng mã được gọi là tối ưu tương đối khi: $\frac{H(X)}{\log_2 D} \leq \bar{n} < \frac{H(X)}{\log_2 D} + 1$

Điều kiện nhận biết một bảng mã tối ưu

Định lý (với $D=2$):

- Xác suất p_i càng lớn thì độ dài n_i của từ mã w_i càng nhỏ.
- Giả sử $p_1 \geq p_2 \geq \dots \geq p_M$. Nếu $p_i \geq p_{i+1} \geq p_{i+r}$ thì $n_i \leq n_{i+1} \leq n_{i+r}$ thì 2 từ mã tương ứng với 2 giá trị có xác suất nhỏ nhất có độ dài mã bằng nhau $n_{M-1} = n_M$.
- Trong các từ mã có độ dài bằng nhau và cùng bằng n_M (đài nhất) thì tồn tại ít nhất 2 từ mã w_{M-1} và w_M có $M-1$ ký tự đầu giống nhau và ký tự thứ M khác nhau.

Ví dụ: xét bảng mã $W = \{w_1=0, w_2=100, w_3=101, w_4=1101, w_5=1110\}$

Bảng mã trên không phải là bảng mã tối ưu vì 2 từ mã w_4, w_5 có độ dài lớn nhất =4 ký tự nhưng 3 ký tự đầu khác nhau.

Ghi chú: $D > 2$ được xét tương tự.

Định lý Huffman

Định lý: Giả sử X có phân phối xác suất với thứ tự giảm dần sau:

X	x_1	x_2	...	x_M
P	$p_1 \geq$	$p_2 \geq$...	$\geq p_M$

Giả sử bảng mã của X là $W = \{w_1, w_2, \dots, w_{M-1}, w_M\}$.

Đặt $x_{M-1,M} = \{x_{M-1}, x_M\}$ có xác suất là $p_{M-1,M} = p_{M-1} + p_M$.
và $X^* = \{x_1, x_2, \dots, x_{M-1,M}\}$ có phân phối sau:

X^*	x_1	x_2	...	x_{M-2}	$x_{M-1,M}$
P	p_1	p_2	...	p_{M-2}	$p_{M-1,M}$

Giả sử $W^* = \{w_1, w_2, \dots, w_{M-2}, x_{M-1,M}^*\}$ là bảng mã tối ưu của X^* . Khi đó:

- $w_{M-1} = w_{M-1,M}^* + "0"$.
- $w_M = w_{M-1,M}^* + "1"$.

Phương pháp sinh mã Huffman

Giả sử X có phân phối xác suất với thứ tự giảm dần sau:

X	x ₁	x ₂	...	x _M
P	p ₁ ≥	p ₂ ≥	...	≥ p _M

Thủ tục lùi (D=2):

Khởi tạo: Đặt M₀=M

Bước 1:

- Đặt $x_{M_0-1, M_0} = \{x_{M_0-1}, x_{M_0}\}$ có xác suất $p_{M_0-1, M_0} = p_{M_0-1} + p_{M_0}$
- Sắp xếp lại theo thứ tự giảm dần của xác suất ta nhận được dãy phân phối mới có M₀-1 phần tử như sau: $p_1, p_2, \dots, p_{M_0-2}, p_{M_0-1, M_0}$

Bước 2: Lặp lại bước 1 với sự lưu vết

$$w_{M_0-1} = w_{M_0-1, M_0} + "0"$$

$$w_{M_0} = w_{M_0-1, M_0} + "1"$$

Giảm M₀: M₀=M₀-1, vòng lặp kết thúc khi M₀=2

(**Chú ý:** trong trường hợp tổng quát, vòng lặp kết thúc khi M₀ ≤ D.)

Thủ tục tiến:

Đi ngược lại so với thủ tục lùi đồng thời xác định từ mã ở mỗi bước từ sự lưu vết ở thủ tục lùi.

Minh họa phương pháp sinh mã Huffman

Ví dụ 1: sinh bảng mã nhị phân Huffman cho X có phân phối sau:

X	x ₁	x ₂	x ₃	x ₄	x ₅	x ₆
P	0.3	0.25	0.2	0.1	0.1	0.05

Thủ tục lùi:

Bước 1 Bước 2 Bước 3 Bước 4 Bước 5

X	P	X	P	X	P	X	P	X	P
x ₁	0.3	x ₁	0.3	x ₁	0.3	x ₂₃	0.45	x ₁₅₆₄	0.55
x ₂	0.25	x ₂	0.25	x ₅₆₄	0.25	x ₁	0.3	x ₂₃	0
x ₃	0.2	x ₃	0.2	x ₂	0.25	x ₅₆₄	0.25	x ₁	0.45
x ₄	0.1	x ₅₆	0.15	x ₃	0.2	x ₁	0	x ₂₃	1
x ₅	0.1	0	x ₄	1	0	x ₅₆₄	1	0	
x ₆	0.05	1							

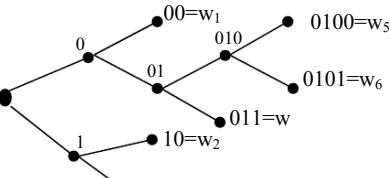
Thủ tục tiên:

Bước 1 Bước 2 Bước 3 Bước 4 Bước 5

X	W	X	W	X	W	X	W	X	W
x ₁₅₆₄	0	x ₂₃	1	x ₁	00	x ₁	00	x ₁	00 = w ₁
x ₂₃	1	x ₅₆₄	01	x ₅₆₄	01	x ₂	10	x ₂	10 = w ₂
		x ₁	00	x ₂	10	x ₃	11	x ₃	11 = w ₃
		x ₅₆₄	01	x ₃	11	x ₅₆	010	x ₄	011 = w ₄
				x ₃	11	x ₄	011	x ₅	0100 = w ₅
						x ₆			0101 = w ₆

Nhận xét tính tối ưu của bảng mã Huffman

Vẽ cây Huffman của bảng mã trên:



Độ dài trung bình của từ mã:

$$\bar{n} = (0.3 \times 2) + (0.25 \times 2) + (0.2 \times 2) + (0.1 \times 3) + (0.1 \times 4) + (0.05 \times 4) = 2.4$$

Entropy của X: $H(X) = H(0.3, 0.25; 0.2, 0.1, 0.1, 0.05)$
 $= 2.4$

Nhận xét: Do $D = 2$ và $\log_2 D = 1$, Ta có $\bar{n} = H(X)$ nên bảng mã trên tối ưu tuyệt đối.**Bài tập**

1. Cho biến ngẫu nhiên X có phân phối sau:

X	x ₁	x ₂	x ₃	x ₄
P	0.4	0.3	0.2	0.1

2. Cho biến ngẫu nhiên Y có phân phối sau:

Y	y ₁	y ₂	y ₃	y ₄	y ₅	y ₆	y ₇	y ₈	y ₉
P	0.3	0.2	0.2	0.1	0.05	0.05	0.04	0.03	0.03

3. Cho đoạn văn bản “thoi the thi thoi thi the thoii thi the”. Tìm bảng mã nhị phân Huffman dùng để mã hóa đoạn văn bản trên.
4. Thay từng ký tự trong đoạn văn bản trên thành một từ mã, cắt từng đoạn 8 bits đổi thành số thập phân. Cho biết dãy số thập phân kết quả.

CHƯƠNG 4: KÊNH TRUYỀN

Mục tiêu:

Trình bày mô hình truyền tin rời rạc từng ký tự mã độc lập lẫn nhau (phù hợp với đặc điểm của kênh). Mô hình này còn gọi là kênh truyền rời rạc không nhớ (Memoryless Discret Channel). Từ mô hình này người ta có thể xây dựng cách tính dung lượng kênh truyền và phương pháp phân loại đầu nhận để có thể giải mã tốt nhất.

BÀI 4.1: KÊNH TRUYỀN RỒI RẠC KHÔNG NHỚ

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết mô hình kênh truyền tin rời rạc không nhớ ở 2 khía cạnh vật lý và toán học.
- Khái niệm về lượng tin trên kênh truyền
- Định nghĩa dung lượng kênh truyền

Giới thiệu

Trước hết, ta có thể hiểu khái niệm kênh truyền rời rạc và không nhớ ở bài học này như sau: khái niệm truyền rời rạc ở đây là truyền tuần tự các ký tự độc lập nhau (hay truyền từng ký tự một), còn khái niệm không nhớ ở đây là chỉ xét mối quan hệ giữa ký tự truyền và ký tự nhận được tương ứng, không xét đến mối quan hệ giữa ký tự nhận được với ký tự nhận được trước đó.

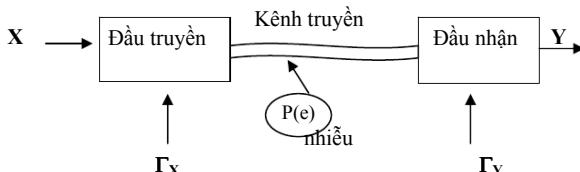
Khái niệm về một kênh truyền rời rạc dựa vào phân bố xác suất của tín hiệu ra phụ thuộc vào tín hiệu vào và trạng thái của kênh truyền đã được chuẩn hóa bởi Feinstein (1958) và Wolfowitz (1961). Dung lượng kênh (Channel Capacity) được xác định chính xác nhờ Muroya (1953) và Fano (1961). Giải thuật và chương trình tính dung lượng kênh đã được viết bởi Eisenberg (1963).

Định lý cơ bản về truyền tin đã chỉ ra rằng “với dung lượng kênh cho trước luôn có thể tìm ra một phương pháp truyền tin với lượng tin nhỏ hơn dung lượng kênh và đạt sai số nhỏ hơn sai số cho phép bất kỳ”. Định lý cơ bản về truyền tin đã được Feinstein (1954, 1958) khảo sát. Các nhà khoa học Blackwell, Breinan (1958, 1959) và Thomasian (1961) đã lần lượt chỉnh lý để đạt chuẩn tốt hơn. Trong các nội dung tiếp theo của bài học, các bạn sẽ tìm hiểu về mô hình kênh truyền tin rời rạc không nhớ ở khía cạnh vật lý và toán học. Đặc biệt ở mô hình toán học sẽ chỉ ra cách xác định phân phối ở đầu ra dựa vào phân phối ở đầu vào.

Mô hình vật lý

Một thông báo được cấu tạo từ các ký hiệu của một bảng chữ cái ở đầu truyền (input) và được truyền trên kênh. Thông báo được nhận ở cuối kênh (hay đầu nhận-output) và được giải mã theo bảng chữ cái ở đầu truyền. Mặt khác, từng ký tự ở đầu nhận có thể quan hệ với các ký tự ở đầu nhận trước đó, các ký tự ở đầu truyền và trạng thái của kênh truyền. Để đơn giản, ở đây chúng ta chỉ xét mô hình vật lý như sau:

Xét từng ký tự ở đầu nhận chỉ phụ thuộc vào ký tự ở đầu truyền tương ứng với nó, nếu kênh truyền có nhiều thì một ký tự ở đầu truyền có thể được diễn giải (nhiều) ra nhiều ký tự khác nhau ở đầu nhận và do đó tạo ra một phân phối xác suất có điều kiện cho ký tự ở đầu nhận. *Mô hình truyền tin rời rạc không nhớ là mô hình truyền tin chỉ xét mối quan hệ giữa ký tự truyền và ký tự nhận được tương ứng, không xét mối quan hệ giữa ký tự nhận được và ký tự nhận được trước đó.* Mô hình:



Các qui ước:

- X : là biến ngẫu nhiên có giá trị cần truyền ở đầu truyền.
- Y : là biến ngẫu nhiên chứa giá trị có thể nhận được ở đầu nhận.
- Γ_X : là bảng chữ cái sinh mã ở đầu truyền.
- Γ_Y : là bảng chữ cái giải mã ở đầu nhận.
- X, Y, Γ_X, Γ_Y : đều hữu hạn và rời rạc.
- Truyền rời rạc từng ký tự và nhận cũng rời rạc từng ký tự.
- Ký tự nhận sau không phụ thuộc vào ký tự nhận trước.

Mô hình toán học

Ta gọi:

- $\Gamma_X = \{x_1, x_2, \dots, x_M\}$ là bộ ký tự sinh mã ở đầu truyền (input).
- $\Gamma_Y = \{y_1, y_2, \dots, y_L\}$ là bộ ký tự giải mã ở đầu nhận (output).
- Biến ngẫu nhiên X lấy giá trị (đã mã hóa) trên Γ_X và có phân phối $p(X=x_i)=p(x_i)$ với $i=1, \dots, M$.
- Biến ngẫu nhiên Y lấy giá trị (giải mã) trên Γ_Y và có phân phối xác suất có điều kiện: $P(Y=y_j|X=x_i)=p(y_j|x_i)=p_{ij}$ với $j=1, \dots, L$.

Gọi $A = [p_{ij}]$ là ma trận truyền tin hay mô hình truyền tin của kênh truyền rời rạc không nhớ.

Với $i=1, M$, $j=1, L$ và $p_{ij} = p(Y=y_j|X=x_i) = p(y_j|x_i)$ là xác suất nhận được giá trị y_j khi đã truyền giá trị x_i .

Tính phân phối đầu nhận:

$$\begin{aligned} \text{Ta có: } p(Y=y_j) &= p(y_j) = \sum_{i=1}^M p(x_i) \cdot p(y_j / x_i) \\ &\Rightarrow p(y_j) = \sum_{i=1}^M p(x_i) \cdot p(y_j / x_i) \\ &= \sum_{i=1}^M p(x_i) \cdot p_{ij} \end{aligned}$$

$$\text{Vậy } p(y_j) = P'_X \cdot A_j \quad (1)$$

$$\text{Một cách tổng quát: } P'_Y = P'_X \cdot A \quad (2)$$

Trong đó:

- A_j là cột thứ j của A
- $P'_X = [p(x_1), p(x_2), \dots, p(x_M)]$.
- $P'_Y = [p(y_1), p(y_2), \dots, p(y_M)]$.

Ví dụ xác định phân phối đầu nhận

Cho ma trận truyền tin như sau:

$$A = \begin{matrix} x_1 & \begin{bmatrix} 0.5 & 0.2 & 0.3 \end{bmatrix} \\ x_2 & \begin{bmatrix} 0.3 & 0.5 & 0.2 \end{bmatrix} \\ x_3 & \begin{bmatrix} 0.2 & 0.3 & 0.5 \end{bmatrix} \end{matrix}$$

$$y_1 \quad y_2 \quad y_3$$

Xác suất truyền: $p(x_1)=0.5$ và $p(x_2)=p(x_3)=0.25$.

Ta tìm phân phối của Y :

Ta có: $P_X = (0.5, 0.25, 0.25)$

Áp dụng công thức (1) ở trên ta được:

$$p(y_1) = P_{x_1} \cdot A_1 = 0.375$$

$$p(y_2) = P_{x_2} \cdot A_2 = 0.3$$

$$p(y_3) = P_{x_3} \cdot A_3 = 0.325$$

$$\Rightarrow P'_Y = (0.375, 0.3, 0.325)$$

Lượng tin trên kênh truyền

Ví dụ: cho ma trận truyền tin như sau:

$$A = \begin{matrix} x_1 & \begin{bmatrix} 0.5 & 0.2 & 0.3 \end{bmatrix} \\ x_2 & \begin{bmatrix} 0.3 & 0.5 & 0.2 \end{bmatrix} \\ x_3 & \begin{bmatrix} 0.2 & 0.3 & 0.5 \end{bmatrix} \end{matrix}$$

$$y_1 \quad y_2 \quad y_3$$

Xác suất truyền: $p(x_1)=0.5$ và $p(x_2)=p(x_3)=0.25$.

$X = \{x_1, x_2, x_3\}$ được xem như tập các ký tự truyền và $Y = \{y_1, y_2, y_3\}$ là tập các ký tự nhận.

Tính lượng tin trên kênh truyền:

Ta tìm phân phối của Y :

Ta có: $P_X = (0.5, 0.25, 0.25)$

Áp dụng công thức (1) ở trên ta được:

$$p(y_1) = P_{x_1} \cdot A_1 = 0.375$$

$$p(y_2) = P_{x_2} \cdot A_2 = 0.3$$

$$p(y_3) = P_{x_3} \cdot A_3 = 0.325$$

$$\Rightarrow P'_Y = (0.375, 0.3, 0.325)$$

Tính các Entropy:

$$H(Y) = H(0.375, 0.3, 0.325) = 1.58 \text{ (bit)}$$

$$H(Y/X=x_1) = H(0.5, 0.2, 0.3) = 1.49 \text{ (bit)}$$

$$H(Y/X=x_2) = H(0.3, 0.5, 0.2) = 1.49 \text{ (bit)}$$

$$H(Y/X=x_3) = H(0.2, 0.3, 0.5) = 1.49 \text{ (bit)}$$

$$H(Y/X) = p(x_1) \cdot H(Y/X=x_1) + p(x_2) \cdot H(Y/X=x_2) + p(x_3) \cdot H(Y/X=x_3) = 1.49 \text{ (bit)}$$

Lượng thông tin truyền trên kênh: $I(X/Y) = I(Y/X) = H(Y) - H(Y/X) = 0.09 \text{ (bit)}$

Định nghĩa dung lượng kênh truyền

Dựa vào ma trận truyền tin A, ta có thể dễ dàng tính lượng tin trên kênh truyền.

$$I(X/Y) = H(X) - H(Y/X)$$

$$= H(Y) - H(X/Y)$$

$$= I(Y/X)$$

Ta có $I(X/Y) = H(Y) - H(Y/X)$, trong đó:

$$H(Y) = H(P_X \cdot A) \text{ phụ thuộc vào } P_X.$$

$$H(Y/X) \text{ phụ thuộc vào } P_X$$

Vậy: $I(Y/X)$ phụ thuộc hoàn toàn vào P_X và do đó $I(Y/X)$ có thể đạt Max với P_X xác định nào đó.

Ta định nghĩa: $C = \max_{\forall p(X)} I(X / Y)$ là dung lượng của kênh truyền (ĐVT: bit).

BAI 4.2: CÁC DẠNG KÊNH TRUYỀN

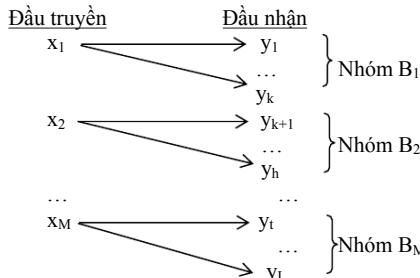
Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết kênh truyền không mất tin,
- Biết kênh truyền xác định,
- Biết kênh truyền không nhiễu,
- Biết kênh truyền không sử dụng được,
- Hiểu kênh truyền đối xứng,

Hiểu định lý về dung lượng kênh truyền, Kênh truyền không mất tin

Mô hình: từ tập hợp các giá trị có thể nhận được ở đầu nhận $Y=\{y_1, y_2, \dots, y_L\}$ được phân thành M nhóm B_i tương ứng với các giá trị x_i ở đầu truyền và xác suất để nhận x_i với điều kiện đã nhận y_j là $p(X=x_i | Y=y_j \in B_i)=1$ (với $M < L$).

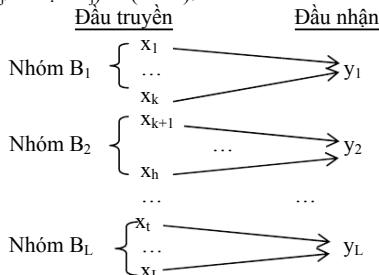


Đặc trưng của kênh truyền không mất tin là $H(X|Y)=0$. Có nghĩa là lượng tin chưa biết về X khi nhận Y là bằng 0 hay ta có thể hiểu khi nhận được Y thì ta hoàn toàn có thể biết về X .

Dung lượng: $C=\log_2 M$ (Sinh viên tự chứng minh, xem như bài tập)

Kênh truyền xác định

Mô hình: từ tập hợp các giá trị có thể truyền ở đầu truyền được phân thành L nhóm B_j tương ứng với các giá trị có thể nhận được y_j ở đầu nhận và xác suất để nhận y_j với điều kiện đã truyền x_i là $p(Y=y_j | X=x_i \in B_j)=1$ ($M>L$).

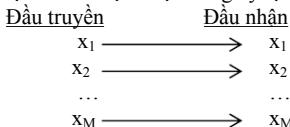


Đặc trưng của kênh truyền xác định là $H(Y|X)=0$. Có nghĩa là lượng tin chưa biết về Y khi truyền X bằng 0 hay khi truyền X thì ta biết sẽ nhận được Y .

Dung lượng: $C = \log_2 L$ (Sinh viên tự chứng minh, xem như bài tập)

Kênh truyền không nhiễu

Mô hình: là sự kết hợp của kênh truyền xác định và kênh truyền không mất thông tin, truyền ký tự nào sẽ nhận được đúng ký tự đó.



Đặc trưng: $H(X/Y)=H(Y/X)=0$.

Dung lượng: $C = \log_2 L = \log_2 M$ (Sinh viên tự chứng minh, xem như bài tập)

Ví dụ: ma trận truyền tin của kênh truyền không nhiễu với $M=L=3$:

$$A = \begin{bmatrix} x_1 & 1 & 0 & 0 \\ x_2 & 0 & 1 & 0 \\ x_3 & 0 & 0 & 1 \end{bmatrix}$$

$$y_1 \ y_2 \ y_3$$

Kênh truyền không sử dụng được.

Mô hình: là kênh truyền mà khi truyền giá trị nào thì mất giá trị đó hoặc xác suất nhiễu thông tin trên kênh truyền lớn hơn xác suất nhận được.

Đặc trưng: $H(X/Y)=H(Y/X)=\max$

Dung lượng: $C=0$ (Sinh viên tự chứng minh, xem như bài tập)

Ví dụ: kênh truyền có ma trận truyền tin như sau:

$$A = \begin{pmatrix} \varepsilon & 1-\varepsilon \\ \varepsilon & 1-\varepsilon \end{pmatrix}$$

Kênh truyền đối xứng

Mô hình: là kênh truyền mà ma trận truyền tin có đặc điểm sau:

- + Mỗi dòng của ma trận A là một hoán vị của phân phối $P=\{p'_1, p'_2, \dots, p'_L\}$
- + Mỗi cột của ma trận A là một hoán vị của $Q=\{q'_1, q'_2, \dots, q'_M\}$

Ví dụ: cho kênh truyền đối xứng có ma trận truyền tin như sau:

$$A = \begin{bmatrix} x_1 & 1/2 & 1/3 & 1/6 \\ x_2 & 1/3 & 1/6 & 1/2 \\ x_3 & 1/6 & 1/2 & 1/3 \end{bmatrix}$$

$$y_1 \quad y_2 \quad y_3$$

Xây dựng công thức tính dung lượng kênh truyền đối xứng

Do $H(Y/X)$ không phụ thuộc vào phân phối của $X \Rightarrow \text{Max}$ của $I(X/Y)$ được quy về mã của $H(Y)$.
Hay

$$C = \text{Max } I(X/Y) = \text{Max}(H(Y) - H(Y/X))$$

Ta có thể tính dễ dàng:

$$H(Y/X) = -\sum_{j=1}^L p_j' \log p_j' = \text{const}$$

Do đó:

$$C = \text{Max } I(X/Y) = \text{Max } H(Y) + \sum_{j=1}^L p_j' \log p_j'$$

Do $H(Y) \leq \log L \Rightarrow$ ta cần chứng tỏ “=” xảy ra khi $p_1 = p_2 = \dots = p_L = 1/L$

Xét trường hợp $P(X=x_i) = 1/M$, với mọi $i \Rightarrow$ chứng minh $P(Y=y_j) = 1/L$ với mọi j

Thật vậy :

$$\begin{aligned} P(Y=y_j) &= \sum_{i=1}^M P(Y=y_j, X=x_i) \\ &= \sum_{i=1}^M P(X=x_i)P(Y=y_j | X=x_i) = \frac{1}{M} \sum_{i=1}^M P_{ij} = \frac{1}{M} q_i \end{aligned}$$

Từ A ta nhận thấy:

$$A = \begin{pmatrix} p_{11} & \dots & p_{1L} \\ \dots & \dots & \dots \\ p_{M1} & \dots & p_{ML} \end{pmatrix} \Rightarrow \sum_A = \text{tổng các phần tử của A.}$$

$$\text{Do } \sum_A = \sum_A^{+hang} = \sum_A^{+cot} \Rightarrow M = L \sum_{i=1}^M q_i \Rightarrow \sum_{i=1}^M q_i = \frac{M}{L}$$

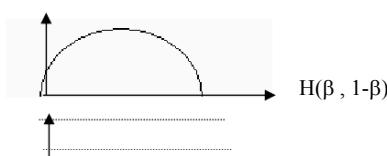
$$\begin{aligned} \Rightarrow P(Y=y_j) &= \frac{1}{M} \frac{M}{L} = \frac{1}{L} \Rightarrow H(Y) = -\sum p_j' P(Y=y_j) \log P(Y=y_j) = \log L = \text{Max} \\ \Rightarrow H(Y) &\text{ đạt max là } \log L \text{ khi } P(Y=y_j) = 1/L \text{ hoặc } P(X=x_i) = 1/M \end{aligned}$$

Vậy: $C = \log L - H(p'_1, p'_2, \dots, p'_L)$ hay $C = \log L + \sum_{j=1}^L p_j \log p_j$

Chú ý: trường hợp kênh 1 bit với nhiễu β

$$\text{Ma trận truyền tin } A = \begin{pmatrix} 1-\beta & \beta \\ \beta & 1-\beta \end{pmatrix}$$

$$\text{Dung lượng } C = 1 + (1-\beta) \log(1-\beta) + \beta \log \beta = 1 - H(\beta, 1-\beta)$$





$$1 - H(\beta, 1-\beta)$$

Định lý về dung lượng kênh truyền

Giả sử ma trận A có dạng vuông và có ma trận nghịch đảo là A^{-1}

Ký hiệu $A = [p_{ij}]$ với $i=1,2,\dots,M$ và $j=1,2,\dots,M$

$A^{-1} = [q_{ij}]$ với $i=1,2,\dots,M$ và $j=1,2,\dots,M$

Đặt tham số $d_k = \sum_{j=1}^M q_{jk} \exp_2 \left[- \sum_{i=1}^M q_{ji} H(Y/X=x_i) \right], \forall k = 1, M$

Nếu $d_k > 0$ thì dung lượng kênh truyền có dạng:

$$C = \log \left\{ \sum_{j=1}^M \exp_2 \left[- \sum_{i=1}^M q_{ji} H(Y/X=x_i) \right] \right\}$$

Giá trị cực đại đạt khi tín hiệu vào $X=X^*$ thỏa phân phối $P(X^*=x_k)=2^{-C}d_k$

Hay $C=\max I(X/Y)=I(X^*/Y)$

Chú ý:

- Điều kiện $d_k > 0$ cho phép hàm $I(X/Y)$ là hàm lồi \Rightarrow Tồn tại Max tuyêt đối tại phân phối của X^* với $p(X^*=x_k)=2^{-C} d_k = p_k$ (với mọi k).

- Nếu điều kiện ma trận vuông hoặc ma trận nghịch đảo không thỏa thì giá trị cực đại max sẽ nằm trên đường biên của miền xác định $\{p_k > 0 \text{ và } \sum p_k = 1\}$

Bài tập

- Cho một kênh truyền có ma trận truyền tin như sau:

$$\begin{matrix} x_1 \\ x_2 \\ x_3 \end{matrix} \begin{bmatrix} 1/2 & 1/3 & 1/6 \\ 1/3 & 1/6 & 1/2 \\ 1/6 & 1/2 & 1/3 \end{bmatrix}$$

$$y_1 \quad y_2 \quad y_3$$

Tính dung lượng kênh truyền.

- Chứng minh các công thức tính dung lượng kênh truyền trên.

BÀI 4.3: LUẬT QUỐC ĐỒ GIẢI MÃ

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết đặt vấn đề bài toán giải mã,
- Hiểu các khái niệm cơ bản của kỹ thuật truyền tin,
- Biết và hiểu các dạng sai sót cơ bản của kỹ thuật truyền tin,
- Hiểu phương pháp xây dựng lược đồ giải mã tối ưu,
- Vận dụng xây dựng lược đồ giải mã tối ưu và tính các dạng xác suất truyền sai.

Đặt vấn đề bài toán giải mã

Phân tích yêu cầu giải mã:

Khi truyền giá trị x_i , ta sẽ nhận được y_j .

Đối với kênh truyền không nhiễu thì y_j chính là x_i . Đối với kênh truyền có nhiễu thì y_j có thể khác x_i . Do đó ta cần tìm cách giải mã y_j về giá trị x_i khi kênh truyền có nhiễu.

Phép phân hoạch các giá trị ở đầu nhận:

Phép phân hoạch tập các giá trị ở đầu nhận $y_j \in Y$ là phép phân chia tập Y thành các tập con B_i sao cho:

$$1. \begin{cases} B_i \cap B_j = \emptyset \\ \bigcup_{i=1}^M B_i = Y \end{cases} \quad (\forall i \neq j)$$

2. Khi nhận $y_j \in B_i$ thì giải mã về x_i .

Ví dụ bài toán giải mã

Cho tập các từ mã truyền X và tập các dãy n bit nhận được Y như sau:

$$X = \{0000, 0101, 1110, 1011\}$$

$$Y = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, \\ 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$$

Giả sử ta có thể phân hoạch tập Y thành các tập con B_i như sau:

$$B_1 = \{0000, 1000, 0001, 0010\}$$

$$B_2 = \{0101, 1101, 0100, 0111\}$$

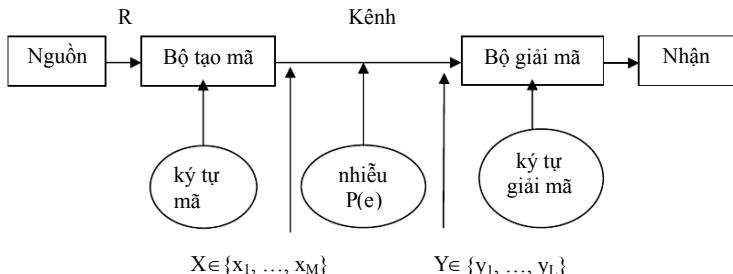
$$B_3 = \{1110, 0110, 1111, 1100\}$$

$$B_4 = \{1011, 0011, 1010, 1001\}$$

Giả sử nhận $y_j = 0011$ thì giải mã về $x_4 = 1011$ vì $y_j \in B_4$.

Các khái niệm cơ bản của kỹ thuật truyền tin

Xét sơ đồ truyền tin như sau:



Điễn giải:

- Nguồn phát tín hiệu (hay thông báo) với vận tốc R (tín hiệu/giây).
- Tín hiệu được mã hóa từ bộ ký tự mã.
- Tín hiệu mã hóa được truyền trên kênh với vận tốc C (ký tự/giây), C đồng thời là dung lượng của kênh truyền.
- Tín hiệu truyền trên kênh có thể bị nhiễu với xác suất P(e).
- Trước khi nhận, tín hiệu mã hóa được giải mã theo một phương thức tối ưu và độ chính xác cao nhất có thể có.

Bài toán đặt ra ở đây: tìm giải pháp tạo mã sao cho sai số đầu nhận có xác suất nhỏ hơn ε bất kỳ ($\epsilon < P(e)$) đồng thời với đồng bộ hóa: vận tốc phát thông báo ở nguồn R và vận tốc truyền tải ≤ C (C là dung lượng kênh).

Các khái niệm cơ bản:

Tử mã: là dãy n ký tự truyền hay dãy n ký tự nhận đúng.

Bộ mã (S,n): là tập hợp gồm S từ mã với độ dài mỗi từ mã đều bằng n và được ký hiệu là $x^{(1)}, \dots, x^{(n)}$.

Lực đòn giải mã: là một hàm gán cho một dãy n ký tự nhận được y_j một từ mã của bộ mã W = {w₁, w₂, ..., w_s}. Ký hiệu: $g(y_j) = w_i$

Lực đòn giải mã tối ưu: là lực đòn giải mã sao cho tổng xác suất truyền sai là nhỏ nhất hay tổng xác suất truyền đúng là lớn nhất.

Nghĩa là: khi nhận y_j thì ta giải mã về w_i^* sao cho:

$$P(w_i^*/y_j) = \operatorname{Max} \{P(w_k/y_j)\}$$

$$\forall w_k \in W$$

Ví dụ minh họa các khái niệm cơ bản

Giả sử kênh truyền từng bit với C=1, nguồn phát thông báo với tốc độ R=2/5 bit/giây (R<C). Để thuận lợi cho mã hóa và giảm nhiễu, ta xét từng khoảng thời gian n = 5 giây. Như vậy trong khoảng thời gian n = 5 giây, ta có:

- Tập hợp các tín hiệu khác nhau là $2^{nR} = 4$. Giả sử 4 tín hiệu là m₁, m₂, m₃, m₄.
- Số bit được phát ra là nR=2 bit và một tín hiệu dạng m_i được kết cấu bởi một dãy các bit.

- Quá trình mã hóa các tín hiệu m_1, m_2, m_3, m_4 cần chú ý là: mỗi m_i cần được mã hóa với số bit tối đa là $nC=5$ bit. Vậy, ta có thể mã hóa các tín hiệu m_i theo 2 cách sau:

Cách 1:

$$\begin{aligned}m_1 &= 00000 \\m_2 &= 01101 \\m_3 &= 11010 \\m_4 &= 10111\end{aligned}$$

Cách 2:

$$\begin{aligned}m_1 &= 00 \\m_2 &= 01 \\m_3 &= 10 \\m_4 &= 11\end{aligned}$$

Nếu sử dụng cách 1 với độ dài 5 bit, trong đó 5 bit có thể hiểu là có 2 bit thông tin cần truyền và 3 bit con lại là 3 bit được bổ sung để phát hiện nhiễu theo một phương pháp nào đó sẽ được đề cập ở các nội dung tiếp theo sau. Với cách mã hóa này, ta có nhiều khả năng phát hiện và sửa sai do nhiễu.

Nếu sử dụng cách 2 thì trường hợp có 1 bit truyền sai sẽ dẫn đến trùng lặp sang một trong các tín hiệu khác. Ví dụ truyền $m_1=00$ và nhận 2 bit là 01 (do nhiễu), trong trường hợp này 01 chính là m_2 , đây là một tín hiệu đúng nên ta không thể phát hiện có nhiễu hay không nhiễu.

Như vậy, trong khoảng thời gian truyền và dung lượng kênh cho phép, ta cần mã hóa mỗi tín hiệu càng dài càng tốt nhưng không được vượt quá độ dài mã cho phép. Trường hợp với thời gian $n=5$ và $c=1$ bit thì $nC=5$ là số bit tối đa có thể truyền nên ta chỉ mã hóa tín hiệu với độ dài mã tối đa là 5 bit.

Các dạng sai số cơ bản

Xác suất truyền sai từ mã x_i : $p(e/x_i) = \sum p(Y=y_j \notin B_i/X=x_i)$

Xác suất truyền sai trung bình: $p(e) = \sum_{i=1}^M p(X=x_i)p(e/x_i)$

Xác suất truyền sai lớn nhất: $p_m(e) = \max_{i=1,M} p(e/x_i)$

Phương pháp xây dựng lược đồ giải mã tối ưu

Theo công thức Bayes:

Ta có: $P(w_k/y_j) = [p(w_k).p(y_j/w_k)] / p(y_j)$ với ($\forall w_k \in W$)

Từ định nghĩa lược đồ giải mã tối ưu:

\Rightarrow tìm w_k sao cho $P(w_k/y_j) \rightarrow \text{Max} \Leftrightarrow p(w_k).p(y_j/w_k) \rightarrow \text{Max}$.

Như vậy, ta có thể xây dựng lược đồ giải mã tối ưu theo các bước sau:

Bước 0: Khởi tạo các $B_i = \emptyset$ ($\forall i$)

Bước lập: xét với mọi $y_j \in Y$

+ Tính:

$$p(w_1).p(y_j/w_1)$$

$$p(w_2).p(y_j/w_2)$$

...

$$p(w_M).p(y_j/w_M)$$

- + So sánh các giá trị tính trên và chọn giá trị w^*_i sao cho $p(w^*_i) \cdot p(y_i/w^*_i) = \text{Max} \{p(w_k) \cdot p(y_j/w_k)\}$ ($\forall w_k \in W$)
- + $B_i = B_i + \{y_i\}$ và $g(y_i) = w^*_i$.

Minh họa xây dựng lược đồ giải mã tối ưu

Bài toán:

Cho ma trận truyền tin A và xác suất ở đầu truyền như sau:

$$\begin{array}{c|ccc} x_1 & 1/2 & 1/3 & 1/6 \\ x_2 & 1/3 & 1/6 & 1/2 \\ x_3 & 1/6 & 1/2 & 1/3 \end{array}$$

$$y_1 \quad y_2 \quad y_3$$

Với $p(x_1)=1/2$; $p(x_2)=p(x_3)=1/4$. Hãy xây dựng lược đồ giải mã tối ưu.

Áp dụng phương pháp xây dựng lược đồ giải mã tối ưu:

Bước 0: $B_1=\{\}$; $B_2=\{\}$; $B_3=\{\}$;

Bước 1: Nhận giá trị y_1 , ta tính:

$$\begin{aligned} &+ p(x_1) \cdot p(y_1/x_1) = 1/2 \cdot 1/2 = 1/4 \quad (\text{Max}) \\ &+ p(x_2) \cdot p(y_1/x_2) = 1/4 \cdot 1/3 = 1/12 \\ &+ p(x_3) \cdot p(y_1/x_3) = 1/4 \cdot 1/6 = 1/24 \end{aligned}$$

Do $p(x_1) \cdot p(y_1/x_1)$ lớn nhất nên liệt kê y_1 vào tập hợp B_1 tương ứng với x_1 .

$$\Rightarrow B_1=\{y_1\}.$$

Bước 2: Nhận giá trị y_2 , ta tính:

$$\begin{aligned} &+ p(x_1) \cdot p(y_2/x_1) = 1/2 \cdot 1/3 = 1/6 \quad (\text{Max}) \\ &+ p(x_2) \cdot p(y_2/x_2) = 1/4 \cdot 1/6 = 1/24 \\ &+ p(x_3) \cdot p(y_2/x_3) = 1/4 \cdot 1/2 = 1/8 \end{aligned}$$

Do $p(x_1) \cdot p(y_2/x_1)$ lớn nhất nên liệt kê y_2 vào tập hợp B_1 tương ứng với x_1 .

$$\Rightarrow B_1=\{y_1, y_2\}.$$

Bước 3: Nhận giá trị y_3 , ta tính:

$$\begin{aligned} &+ p(x_1) \cdot p(y_3/x_1) = 1/2 \cdot 1/6 = 1/12 \\ &+ p(x_2) \cdot p(y_3/x_2) = 1/4 \cdot 1/2 = 1/8 \quad (\text{Max}) \\ &+ p(x_3) \cdot p(y_3/x_3) = 1/4 \cdot 1/3 = 1/12 \end{aligned}$$

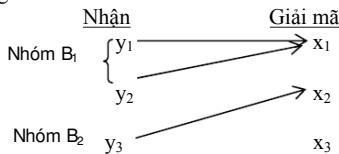
Do $p(x_1) \cdot p(y_3/x_1)$ lớn nhất nên liệt kê y_3 vào tập hợp B_2 tương ứng với x_2 .

$$\Rightarrow B_2=\{y_3\}.$$

Kết quả:

Phân hoạch: $B_1 = \{y_1, y_2\}$, $B_2 = \{y_3\}$ và $B_3 = \{\}$.

Lược đồ giải mã tối ưu:



Minh họa cách tính các sai số

Xét lại ví dụ minh họa xây dựng lược đồ giải mã tối ưu trên, ta có:

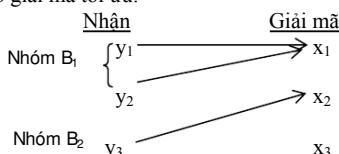
- Ma trận truyền tin A:

$$\begin{matrix} x_1 & \left[\begin{matrix} 1/2 & 1/3 & 1/6 \end{matrix} \right] \\ x_2 & \left[\begin{matrix} 1/3 & 1/6 & 1/2 \end{matrix} \right] \\ x_3 & \left[\begin{matrix} 1/6 & 1/2 & 1/3 \end{matrix} \right] \end{matrix}$$

$$\begin{matrix} y_1 & y_2 & y_3 \end{matrix}$$

- Xác suất ở đầu truyền: $p(x_1) = 1/2$; $p(x_2) = p(x_3) = 1/4$.

- Lược đồ giải mã tối ưu:



- Phân hoạch: $B_1 = \{y_1, y_2\}$, $B_2 = \{y_3\}$ và $B_3 = \{\}$.

Tính các xác suất truyền sai:

Xác suất truyền sai một từ mã:

$$\begin{aligned} \text{Xác suất truyền sai từ mã } x_1: p(e/x_1) &= \sum p(Y=y_j \notin B_1/X=x_1) \\ &= p(y_3/x_1) = 1/6 \end{aligned}$$

$$\begin{aligned} \text{Xác suất truyền sai từ mã } x_2: p(e/x_2) &= \sum p(Y=y_j \notin B_2/X=x_2) \\ &= p(y_1/x_2) + p(y_2/x_2) = 1/3 + 1/6 = 1/2 \end{aligned}$$

$$\begin{aligned} \text{Xác suất truyền sai từ mã } x_3: p(e/x_3) &= \sum p(Y=y_j \notin B_3/X=x_3) \\ &= p(y_1/x_3) + p(y_2/x_3) + p(y_3/x_3) = 1/6 + 1/3 + 1/2 = 1 \end{aligned}$$

$$\text{Xác suất truyền sai trung bình: } p(e) = \sum_{i=1}^M p(X=x_i) p(e/x_i)$$

$$\Rightarrow p(e) = p(x_1).p(e/x_1) + p(x_2).p(e/x_2) + p(x_3).p(e/x_3) = 1/2.1/6 + 1/4.1/2 + 1/4.1 = 11/24$$

$$\text{Xác suất truyền sai lớn nhất: } p_m(e) = \max_{i=1,M} p(e/x_i)$$

$$\Rightarrow pm(e) = \max \{ p(e/x_1), p(e/x_2), p(e/x_3) \} = p(e/x_3) = 1$$

Bài tập 1

1. Cho ma trận truyền tin sau:

$$\begin{matrix} x_1 & \left[\begin{matrix} 1/2 & 1/3 & 1/6 \end{matrix} \right] \\ x_2 & \left[\begin{matrix} 1/3 & 1/6 & 1/2 \end{matrix} \right] \\ x_3 & \left[\begin{matrix} 1/6 & 1/2 & 1/3 \end{matrix} \right] \end{matrix}$$

$y_1 \quad y_2 \quad y_3$

Biết xác suất ở đầu truyền: $p(x_1)=5/10$, $p(x_2)=3/10$, $p(x_3)=2/10$.

- Tính dung lượng kênh truyền.
- Xây dựng lược đồ giải mã tối ưu.
- Tính các sai số $p(e)$ và $p_m(e)$.

2. Cho ma trận truyền tin sau:

$$\begin{matrix} x_1 & \left[\begin{matrix} 7/12 & 3/12 & 2/12 \end{matrix} \right] \\ x_2 & \left[\begin{matrix} 2/12 & 7/12 & 3/12 \end{matrix} \right] \\ x_3 & \left[\begin{matrix} 3/12 & 2/12 & 7/12 \end{matrix} \right] \end{matrix}$$

$y_1 \quad y_2 \quad y_3$

Biết xác suất ở đầu truyền: $p(x_1)=1/3$, $p(x_2)=1/3$, $p(x_3)=1/3$.

- Tính dung lượng kênh truyền.
- Xây dựng lược đồ giải mã tối ưu
- Tính các sai số $p(e)$ và $p_m(e)$.

Bài Tập 2

1. Cho ma trận truyền tin sau:

$$\begin{matrix} x_1 & \left(\begin{matrix} 1/2 & 1/3 & 1/6 \end{matrix} \right) \\ x_2 & \left(\begin{matrix} 1/6 & 1/2 & 1/3 \end{matrix} \right) \\ x_3 & \left(\begin{matrix} 1/3 & 1/6 & 1/2 \end{matrix} \right) \end{matrix}$$

$y_1 \quad y_2 \quad y_3$

Biết $p(x_1)=1/2$, $p(x_2)=1/4$, $p(x_3)=1/4$.

- Tính dung lượng kênh truyền.
- Xây dựng lược đồ giải mã tối ưu.
- Tính các sai số $p(e)$ và $p_m(e)$.

2. Cho ma trận truyền tin sau:

$$\begin{matrix} x_1 & \left(\begin{matrix} 7/10 & 2/10 & 1/10 \end{matrix} \right) \\ x_2 & \left(\begin{matrix} 1/10 & 7/10 & 2/10 \end{matrix} \right) \\ x_3 & \left(\begin{matrix} 2/10 & 1/10 & 7/10 \end{matrix} \right) \end{matrix}$$

$y_1 \quad y_2 \quad y_3$

Biết xác suất truyền $p(x_1)=0.4$, $p(x_2)=0.4$, $p(x_3)=0.2$.

- Tính dung lượng kênh truyền.
- Xây dựng lược đồ giải mã tối ưu.
- Tính các sai số $p(e)$ và $p_m(e)$.

CHƯƠNG 5: SỬA LỖI

Mục tiêu: Xây dựng nguyên tắc sửa lỗi dựa vào khoảng cách Hamming. Trên nguyên tắc này, phương pháp sửa lỗi “kiểm tra chẵn lẻ (parity check)” được xây dựng và tạo ra quy trình sửa lỗi tối ưu và phù hợp với công nghệ truyền tin hiện nay.

BÀI 5.1: NGUYÊN LÝ KHOẢNG CÁCH NHỎ NHẤT HAMMING

Mục tiêu:

Sau khi hoàn tất bài học này bạn có thể hiểu:

- Định nghĩa khoảng cách Hamming
- Kênh truyền đối xứng nhị phân và lược đồ giải mã tối ưu
- Quan hệ giữa xác suất giải mã và khoảng cách Hamming
- Nguyên lý khoảng cách nhỏ nhất của Hamming.

Khoảng cách Hamming

Định nghĩa: cho v_1 và v_2 là 2 dãy nhị phân dài n bit, ta gọi khoảng cách Hamming giữa 2 dãy v_1 , v_2 là số bit tương ứng khác nhau. Ký hiệu: $d(v_1, v_2)$.

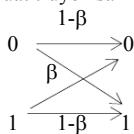
Ví dụ:

$$\begin{aligned}v_1 &= 10101010 \\v_2 &= 10101111\end{aligned}$$

Ta nhận thấy rằng bit thứ 6 và bit thứ 8 giữa v_1 và v_2 là khác nhau nên số bit tương ứng khác nhau giữa v_1 và v_2 là 2. Do đó, ta nói khoảng cách Hamming giữa v_1 và v_2 là 2 hay $d(v_1, v_2) = 2$

Kênh truyền đối xứng nhị phân và lược đồ giải mã tối ưu

Xét kênh truyền đối xứng nhị phân. Giả sử ta truyền các dãy từ mã nhị phân có độ dài n bits với xác suất truyền sai 1 bit là β .



Gọi $W = \{w_1, w_2, \dots, w_s\}$ là tập s từ mã truyền, độ dài mỗi từ mã đều bằng n bit.

$V = \{v_1, v_2, \dots, v_{2^n}\}$ là tập các dãy n bit nhận được ở cuối kênh với W có phân phối đều, xác suất để nhận v_j khi truyền w_i là $p(v_j/w_i) = p_{ij}$.

Theo lược đồ giải mã tối ưu ta có: khi nhận v_j thì giải mã về w_i^* sao cho:

$$P(w_i^*/v_j) = \text{Max} \{P(w_k/v_j)\}$$

$$(\forall w_i \in W)$$

Ta có: $P(w_k/v_j) = [p(w_k).p(y_j/w_k)] / p(y_j)$ với $(\forall w_k \in W)$

$$\Rightarrow P(w_k/v_j) \rightarrow \text{Max} \Leftrightarrow p(w_k).p(y_j/w_k) \rightarrow \text{Max}.$$

Do W có phân phối đều nên $P(w_k/y_j) \rightarrow \text{Max} \Leftrightarrow p(y_j/w_k) \rightarrow \text{Max}$

Vậy: để tìm w_i^* sao cho $P(w_i^*/y_j) = \text{Max}\{P(w_k/y_j)\}$ ta chỉ cần tìm w_i^* sao cho

$$P(y_j/w_i^*) = \text{Max}\{P(y_j/w_k)\} \quad (\text{chi dựa vào ma trận truyền tin A})$$

Ví dụ kênh truyền đối xứng nhị phân

Xét ma trận truyền tin A và xác suất ở đầu truyền như sau:

$$A = \begin{bmatrix} w_1 & \begin{bmatrix} 1/2 & 1/3 & 1/6 \\ 1/3 & 1/6 & 1/2 \\ 1/6 & 1/2 & 1/3 \end{bmatrix} \\ w_2 & \\ w_3 & \end{bmatrix} \quad \text{và } p(w_1) = p(w_2) = p(w_3) = 1/3.$$

$$\begin{array}{ccc} v_1 & v_2 & v_3 \end{array}$$

dựa vào lược đồ giải mã tối ưu ta có:

- Nhận v_1 giải mã về w_1
- Nhận v_2 giải mã về w_3
- Nhận v_3 giải mã về w_2 .

Quan hệ giữa xác suất giải mã và khoảng cách Hamming

Giả sử nhận được v:

Xét 2 từ mã w_1 và w_2 cần chọn để giải mã cho v.

+ Gọi $d_1=d(v, w_1)$, $d_2=d(v, w_2)$.

+ Ta có: $p(v/w_1)=\beta^{d_1}(1-\beta)^{n-d_1}$ (xác suất để nhận v khi truyền w_1).

$P(v/w_2)=\beta^{d_2}(1-\beta)^{n-d_2}$ (xác suất để nhận v khi truyền w_2).

$$\text{So sánh xác suất: } \frac{p(v/w_1)}{p(v/w_2)} = \frac{\beta^{d_1}(1-\beta)^{n-d_1}}{\beta^{d_2}(1-\beta)^{n-d_2}} = \left(\frac{1-\beta}{\beta} \right)^{d_2-d_1}$$

Nếu $0 < \beta < \frac{1}{2}$ thì $\frac{1-\beta}{\beta} > 1$

Do đó: $P(v/w_1) > P(v/w_2) \Leftrightarrow d_1 < d_2$

Nhận xét: xác suất giải mã càng lớn thì **khoảng cách Hamming** càng nhỏ.

Nguyên lý Hamming

Định lý: trên kênh truyền đối xứng nhị phân với s từ mã ở đầu truyền có độ dài n bit, lược đồ giải mã tối ưu có thể thay thế bằng lược đồ giải mã theo khoảng cách Hamming với nguyên lý: nếu nhận được v, ta sẽ giải ra w_i^*

sao cho $d(v, w_i^*) = \text{Min } d(v, w_k)$ (với $\forall w_k \in W$).

Ví dụ: xét bộ mã $W=\{w_1=00000, w_2=10011, w_3=11100, w_4=01111\}$

Giả sử nhận được dãy v=01011.

ta có: $d(v, w_1)=3$; $d(v, w_2)=2$; $d(v, w_3)=4$; $d(v, w_4)=1$.

vậy v được giải về w_4 vì khoảng cách Hamming giữa v và w_4 là nhỏ nhất.

Bài tập

1. Cho bộ mã $W=\{w_1=000000, w_2=101010, w_3=111000, w_4=111111\}$ và nhận được dãy $v=010111$, khi đó giải mã về từ mã nào? diễn giải?
2. Cho bộ mã $W=\{w1=000000, w2=010101, w3=000111, w4=111111\}$ và Nhận được dãy $v=010111$, khi đó giải mã về từ mã nào? diễn giải?

BÀI 5.2: BỎ ĐỀ VỀ TỰ SỬA LỖI VÀ CẬN HAMMING

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết được Bỏ đề về tự sửa lỗi,
- Hiểu Định lý về cận Hamming,
- Biết phân loại được các dạng lỗi,
- Làm cơ sở lý thuyết cho các phương pháp sửa lỗi được trình bày trong các bài học tiếp theo.

Bỏ đề về tự sửa lỗi

Đặt vấn đề: một từ mã w dài n bit khi được truyền tuần tự từng bit có thể sai e bit. Vấn đề đặt ra là khoảng cách (Hamming) giữa các từ mã và sai số e quan hệ với nhau như thế nào để có thể phân biệt tốt nhất đồng thời tất cả các từ mã? Bỏ đề sau xác định quan hệ này.

Bỏ đề:

Xét bộ mã $W = \{w_1, w_2, \dots, w_s\}$, gồm có s từ mã nhị phân dài n bit và 1 số nguyên dương e .

1. Nếu $d(w_i, w_j) \geq 2e+1$ (với $\forall i \neq j$)

Khi đó: tất cả các dãy nhận được v có số bit lỗi $\leq e$ thì v có thể tự điều chỉnh (hay tự sửa lỗi).

2. Nếu $d(w_i, w_j) \geq 2e$ (với $\forall i \neq j$)

Khi đó: tất cả các dãy nhận được v có số bit lỗi $< e$ thì v có thể tự điều chỉnh. Tất cả các dãy nhận được có số bit lỗi $= e$ thì ta chỉ phát hiện là v có lỗi và không thể tự điều chỉnh được.

3. Ngược lại;

Nếu v có số chữ số bit lỗi $\leq e$ và có thể tự điều chỉnh thì $d(w_i, w_j) \geq 2e+1$ (với $\forall i \neq j$).

Nếu v có số chữ số bit lỗi $\leq e-1$ tự điều chỉnh được và tất cả các tín hiệu với số chữ số bit lỗi $\leq e$ được phát hiện thì khoảng cách giữa các từ mã luôn thỏa: $d(w_i, w_j) \geq 2e$ (với $\forall i \neq j$).

Chứng minh và minh họa bỏ đề

a. Giả sử: $d(w, w') \geq 2e+1$ với $\forall i \neq j$. Nếu w và w' có cùng khoảng cách đối với dãy v thì $d(v, w) = d(v, w') \geq e+1$. Vậy, nếu $d(v, w^*) \leq e$ thì v có thể được giải mã ra w^* .

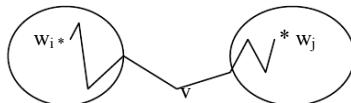
b. Nếu $d(w_i, w_j) \geq 2e$ với $\forall i \neq j$, có khả năng có v, w và w' với số chữ số lỗi là: $d(v, w) = d(v, w') = e$ ($d(v, w) + d(v, w') \geq d(w, w') \geq 2e$). Có thể phát hiện ra các từ mã gần v , nhưng do tồn tại cùng lúc nhiều từ mã gần nhất với v dẫn đến không giải mã được, ngược lại hoàn toàn tương tự.

Minh họa:

a. $d(w_i, w_j) = 2e + 1 = 7$, $e = 3$

Nếu $v \in B_i$ thì v được giải mã về w_i

Nếu $v \in B_j$ thì v được giải mã về w_j



b. $d(w_i, w_j) = 2e = 8$ ($e = 4$, $e - 1 = 3$)

nếu $v \notin B_i$, $v \notin B_j \Rightarrow$ các điểm cách tâm khoảng cách 3 thì luôn được giải mã, còn các điểm cách tâm 4 thì chỉ phát hiện lỗi chứ không thể giải mã được.

c. Mã 3 chiều (x, y, z) bắt đầu từ gốc 000. Cứ một tín hiệu thay đổi thì mã bị đẩy di theo 1 cạnh, chẳng hạn:

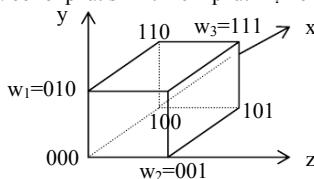
000 cách 010, 001 bởi 1 cạnh,

011 cách 010, 111 và 001 bởi 1 cạnh.

Như vậy, nếu ta chọn $w_1=010$, $w_2=001$, $w_3=111$ thì khoảng cách giữa chúng là 2

$$d(w_1, w_2)=d(w_1, w_3)=d(w_2, w_3)=2$$

vậy nếu có lỗi phát sinh thì chỉ phát hiện chứ không sửa được.



Cận Hamming.

Đặt vấn đề: trong tổng số 2^n dãy nhị phân dài n bit có thể chọn ra bao nhiêu dãy để tạo thành một bộ mã có thể tự điều chỉnh được e bit lỗi. Định lý cận Hamming cho chúng ta xác định số từ mã có độ dài n bit với giả thiết: có khả năng tự sửa được e bit lỗi (điều kiện cần tự sửa lỗi).

Định lý: Nếu bộ mã W có s từ mã có độ dài n bit có thể tự sửa được e bit lỗi thì

$$s \leq \frac{2^n}{\sum_{i=1}^e C_n^i}$$

Ghi chú: $C_n^i = n!/(i!(n-i)!)$

Chứng minh:

Xét từ mã nhị phân w_i có độ dài n bit và có khả năng tự sửa được e bit lỗi.

$$\text{Số dãy } v_j \text{ sai khác với } w_i \text{ từ } 0 \text{ đến } e \text{ bit là: } C_n^0 + C_n^1 + C_n^2 + \dots + C_n^e = \sum_{i=0}^e C_n^i$$

Tương ứng với s từ mã, tổng số dãy v_j có thể tự sửa lỗi là: $s \cdot \sum_{i=0}^e C_n^i \leq 2^n$
(2^n là tổng số dãy nhị phân dài n bits).

$$\Rightarrow s \leq \frac{2^n}{\sum_{i=1}^e C_n^i}$$

Phân các dạng lỗi

Giả sử ta truyền từ mã n bit $w_i \in W$ ($1 \leq i \leq s$) và nhận được dãy n bit v_j ($1 \leq j \leq 2^n$).

Các loại lỗi có thể phát hiện sau:

Lỗi có thể tự điều chỉnh:

Trong trường hợp này tồn tại duy nhất từ mã w^*_i sao cho $d(v_j, w^*_i) = \text{Min } d(v_j, w_k)$ với $\forall w_k \in W$.
=> v_j được giải mã về w^*_i

Lỗi chỉ phát hiện không điều chỉnh được:

Trong trường hợp này tồn tại từ mã w^*_i và w^{**}_i sao cho
 $d(v_j, w^*_i) = d(v_j, w^{**}_i) = \text{Min } d(v_j, w_k)$ với $\forall w_k \in W$
=> v_j không thể giải mã chính xác.

Lỗi không phát hiện được.

Trong trường hợp ta giải mã ra w^*_i nhưng khác với w_i đã truyền.

Bài tập

1. Cho $n=7$ và $e=2$, hãy áp dụng định lý cận Hamming cho biết số từ mã tối đa của bộ mã W .
2. Cho $n=7$ và $e=2$, hãy áp dụng định lý cận Hamming cho biết số từ mã tối đa của bộ mã W .
3. Hãy cho một ví dụ cụ thể minh họa các trường hợp phân loại lỗi.

BÀI 5.3: MÃ KIỂM TRA CHĂN LẺ**Mục tiêu:**

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu bộ mã kiểm tra chẵn lẻ,
- Hiểu phương pháp kiểm tra chẵn lẻ,

- Biết tính chất cơ bản của phương pháp kiểm tra chẵn lẻ,
- Hiểu và vận dụng tốt phương pháp sinh mã kiểm tra chẵn lẻ,
- Hiểu và vận dụng tốt Định lý quan hệ giữa độ dài mã n, số bit kiểm tra m và số lỗi tự sửa e,
- Vận dụng cho các bài học tiếp theo.

Bộ mã kiểm tra chẵn lẻ

Bộ mã kiểm tra chẵn lẻ là bộ mã gồm s từ mã, trong đó mỗi từ mã có dạng sau:

$$w' = \underbrace{r_1 r_2 r_3 \dots r_m}_{m \text{ bit kiểm tra}} \underbrace{r_{m+1} r_{m+2} \dots r_{m+k}}_{k \text{ bit thông tin}} \quad (\text{với } n = m+k).$$

Ghi chú: trong một số trường hợp sinh mã theo phương pháp kiểm tra chẵn lẻ, thứ tự các bit kiểm tra và các bit thông tin có thể xen kẽ nhau (theo một thứ tự nào đó, chẳng hạn như mã Hamming,...) hay cũng có thể theo một thứ tự khác (theo quy ước khác). Ở đây, ta chọn thứ tự các bit kiểm tra chẵn lẻ và các bit thông tin như trên để dễ tính toán nhưng vẫn mất tính tổng quát hóa.

Trong đó: w' viết theo dòng là chuyển vị của w (w được viết theo cột)

- + r_i : là bit thứ i của từ mã ($1 \leq i \leq n$).
- + n : độ dài của từ mã hay số bit của từ mã chẵn lẻ.
- + m : số bit kiểm tra.
- + $k = n-m$: số bit thông tin $\Rightarrow s=2^k$ (vì với k bit thông tin thì ta chỉ có thể biểu diễn tối đa 2^k trạng thái thông tin k bit).
- + Đoạn kiểm tra: gồm m bit dùng để kiểm tra mã sai.
- + Đoạn thông tin: gồm k bit thông tin.

Mỗi đoạn mã thông tin có duy nhất một đoạn mã kiểm tra và được xác định bởi hệ phương trình tuyến tính nhị phân sau:

$$\left\{ \begin{array}{l} a_{11}r_1 + a_{12}r_2 + \dots + a_{1n}r_n = 0 \\ a_{21}r_1 + a_{22}r_2 + \dots + a_{2n}r_n = 0 \\ \dots \quad \dots \quad \dots \quad \dots \\ a_{n1}r_1 + a_{n2}r_2 + \dots + a_{nn}r_n = 0 \end{array} \right.$$

Gọi $A=\|a_{ij}\|=A_{m \times n}$, $a_{ij} \in \{0,1\}$, $i=\overline{1,m}$, $j=\overline{1,n}$. Ma trận A được gọi là ma trận kiểm tra chẵn lẻ có hạng là m (hay $\text{Rank}(A)=m$).

Các phép toán trong Modulo 2 (+,-):

$$\begin{aligned} 0 + 1 &= 1 + 0 = 1; & 0 - 1 &= 1 - 0 = 1; \\ 1 + 1 &= 1 - 1 = 0; \end{aligned}$$

Phương pháp kiểm tra chẵn lẻ

Giải $w'=r_1 r_2 \dots r_n$ là từ mã truyền (hay dãy n bit truyền) và $v'=r_1 r_2 \dots r_n$ là dãy n bit nhận được.

Qui ước: v', w' (lần lượt là chuyển vị của v và w) được viết theo dòng. Còn v, w được viết theo cột.

Nếu $A.v = 0$ thì $v = w$, ta gọi v là chẵn (trường hợp nhận đúng)

Nếu $A.v \neq 0$ thì $v \neq w$, ta gọi v là lẻ (trường hợp nhận sai).

Ta gọi $z = v-w$ là bộ lỗi giữa v và w . Nghĩa là tại các vị trí $z = \{0\}$ thì bit nhận được tương ứng là bit đúng và tại các vị trí $z = \{1\}$ thì bit nhận được tương ứng là bit sai (hay bit lỗi).

Ta gọi $C = A.v$ là bộ sửa lỗi (hay bộ điều chỉnh lỗi).

Ta có $C = A.z = A.(v-w) = A.v - A.w = A.v \Rightarrow C = A.v = A.z$

Tính chất của bộ sửa lỗi: dây n bit nhận được v và bộ lỗi tương ứng có cùng bộ điều chỉnh.

Phương pháp sinh mã kiểm tra chẵn lẻ

Giả sử: cho trước ma trận kiểm tra chẵn lẻ A với $\text{Rank}(A) = m$.

Tim bộ mã chẵn lẻ $W = \{w_1, w_2, w_3, \dots, w_s\}$

Bước 0: Xác định các giá trị n, m, k, s

Độ dài của từ mã $n =$ số cột của ma trận A .

Số bit kiểm tra $m =$ số dòng của ma trận A .

Số bit thông tin: $k = n - m$.

Số từ mã $s = 2^k$ của bộ mã.

Bước i: Tìm các từ mã thứ i ($1 \leq i \leq s$):

Gọi k_{p_i} là triền khai nhị phân k bit của số i

Từ mã cần tìm là: $w'_i = r_1 r_2 \dots r_m k_{p_i}$

Giải hệ phương trình $A.w_i = 0$ để tìm m bit kiểm tra ứng với k bit thông tin (k_{p_i}) đã biết
 \Rightarrow từ mã w_i

Ví dụ sinh mã kiểm tra chẵn lẻ

Xây dựng bộ mã kiểm tra chẵn lẻ được sinh từ ma trận kiểm tra A như sau:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \quad \text{Rank}(A) = 3$$

Bước 0:

$n = 6$ (= số dòng của ma trận A)

$m = 3$ (= số cột của ma trận A)

Số bit thông tin $k = n - m = 3 \Rightarrow$ Số từ mã $s = 2^k = 8$ từ mã.

Bước i: Tìm từ mã thứ i ($1 \leq i \leq s$):

- $w'_1=r_1r_2r_3000$ (000 là triển khai nhị phân k=3 bits của số i=0)
- $w'_1=r_1r_2r_3001$ (001 là triển khai nhị phân k=3 bits của số i=1)
- $w'_2=r_1r_2r_3010$ (010 là triển khai nhị phân k=3 bits của số i=2)
- $w'_3=r_1r_2r_3011$ (011 là triển khai nhị phân k=3 bits của số i=3)
- $w'_4=r_1r_2r_3100$ (100 là triển khai nhị phân k=3 bits của số i=4)
- $w'_5=r_1r_2r_3101$ (101 là triển khai nhị phân k=3 bits của số i=5)
- $w'_6=r_1r_2r_3110$ (110 là triển khai nhị phân k=3 bits của số i=6)
- $w'_7=r_1r_2r_3111$ (111 là triển khai nhị phân k=3 bits của số i=7)

Giải hệ phương trình $A.w_i=0$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \Rightarrow \begin{cases} r_1 = 0 \\ r_2 + r_3 = 1 \Rightarrow \begin{cases} r_1 = 0 \\ r_2 = 0 \end{cases} \Rightarrow w'_1=001001 \\ r_1 + r_3 = 1 \end{cases}$$

Giải hệ phương trình $A.w_2=0$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \Rightarrow \begin{cases} r_1 = 1 \\ r_2 + r_3 = 0 \Rightarrow \begin{cases} r_1 = 1 \\ r_2 = 1 \end{cases} \Rightarrow w'_2=111010 \\ r_1 + r_3 = 0 \end{cases}$$

Giải tương tự cho các trường hợp còn lại ta có:

$$\begin{aligned} w'_0 &= 000000, w'_3 = 110011, w'_4 = 110100, \\ w'_5 &= 111101, w'_6 = 001110, w'_7 = 000111. \end{aligned}$$

$$\Rightarrow W = \{000000, 001001, 111010, 110011, 110100, 111101, 001110, 000111\}$$

Định lý quan hệ giữa độ dài mă n, số bit kiểm tra m và số lỗi tự sửa e

Điều kiện cần (Cận Hamming):

Điều kiện cần để bộ mă chẵn lẻ có độ dài n bit có thể tự sửa được e bit lỗi với k bit thông tin và m bit kiểm tra là:

$$2^m \geq \sum_{i=0}^e C_n^i$$

Điều kiện đủ (ĐK Vasharmov-Gilbert-Sacks):

Điều kiện đủ để bộ mă kiểm tra chẵn lẻ có độ dài n bit với m bit kiểm tra chẵn lẻ có thể tự sửa được e bit lỗi là:

$$2^m > \sum_{i=0}^{2e-1} C_{n-1}^i$$

Ghi chú: $C_n^i = n!/(i!(n-i)!)$

Ví dụ tìm m nhỏ nhất từ n và e

Giả sử biết trước $n=7$ và $e=1$. Tìm số bit kiểm tra tối thiểu cần thiết của bộ mã chẵn lẻ.

Theo định lý điều kiện cần (Cận Hamming):

$$\text{Ta có: } 2^m \geq \sum_{i=0}^e C_n^i$$

$$\Leftrightarrow 2^m \geq \sum_{i=0}^{e-1} C_7^i \quad (*)$$

$$m = 1 \Rightarrow (*) \text{ sai.}$$

$$m = 2 \Rightarrow (*) \text{ sai.}$$

$$m \geq 3 \Rightarrow (*) \text{ đúng.}$$

Vậy số bit kiểm tra tối thiểu cần thiết là $m = 3$.

Ví dụ tìm e lớn nhất từ m và n

Giả sử cho trước $m=3$, $k=2$. Tìm số bit lỗi lớn nhất có thể tự sửa e ?

Theo định lý điều kiện đủ (DK Vassharmov-Gilbert-Sacks):

$$2^m \geq \sum_{i=0}^{2e-1} C_{n-1}^i \Leftrightarrow 2^3 \geq \sum_{i=0}^{2e-1} C_{5-1}^i \quad (*)$$

$$e = 1 \Rightarrow (*) \text{ đúng.}$$

$$e > 1 \Rightarrow (*) \text{ sai.}$$

Vậy số bit lỗi lớn nhất có thể tự sửa là $e = 1$.

Bài tập

1. Xây dựng bộ mã kiểm tra chẵn lẻ được sinh từ ma trận kiểm tra A như sau:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

2. Tìm bộ mã kiểm tra chẵn lẻ được sinh từ ma trận kiểm tra A như sau:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

➤ **Gợi ý giải bài tập 1 & 2:** dựa vào phương pháp sinh mã kiểm tra chẵn lẻ và tham khảo ví dụ sinh mã kiểm tra chẵn lẻ.

3. Xét bộ mã kiểm tra chẵn lẻ độ dài 15 bit có thể tự sửa được 1 bit lỗi trên đường truyền, hãy cho biết số bit kiểm tra chẵn lẻ tối thiểu?

4. Xét bộ mã kiểm tra chẵn lẻ độ dài 8 bit với 4 bit kiểm tra chẵn lẻ. Hãy cho biết số lỗi tự sửa tối đa của bộ mã?

➤ **Gợi ý giải bài tập 3 & 4:** dựa vào định lý Điều kiện cần (Cận Hamming) và Điều kiện đủ (DK Varshamov-Gilbert-Sacks).

BÀI 5.4: NHÓM CỘNG TÍNH VÀ BỘ TỪ MÃ CHĂN LẺ

Mục tiêu.

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu Khái niệm nhóm cộng tính,
- Biết các tính chất của bộ mã chẵn lẻ,
- Vận dụng sinh ma trận kiểm tra chẵn lẻ từ bộ mã kiểm tra chẵn lẻ.
- Vận dụng tốt phương pháp sinh bộ mã kiểm tra chẵn lẻ từ các từ mã độc lập duy nhất của bộ mã.

Khái niệm nhóm cộng tính.

Đặt vấn đề:

Như chúng ta đã biết, phương pháp sinh mã kiểm tra chẵn lẻ giúp ta sinh bộ mã kiểm tra chẵn lẻ với số từ mã tương ứng là $s=2^k$. Với phương pháp này, ta phải xác định từng từ mã một (bằng cách giải hệ phương trình duy nhất nhị phân). Giả sử: $k=5$ ta phải xác định $s=2^5=32$ từ mã hay $k=10$ ta phải xác định $s=2^{10}=1024$ từ mã,... Điều này sẽ mất nhiều thời gian nếu k càng lớn. Vấn đề đặt ra ở đây là tìm ra một phương pháp sinh bộ mã kiểm tra chẵn lẻ nhanh hơn về mặt thời gian. Phương pháp sinh mã kiểm tra chẵn lẻ dựa theo lý thuyết nhóm sẽ giải quyết vấn đề này.

Khái niệm nhóm cộng tính:

Nhóm G được gọi là một nhóm cộng tính nếu G có các tính chất:

- $\forall a, b \in G \Rightarrow a+b \in G$ (tính chất cộng).
- $\forall a, b, c \in G \Rightarrow a + (b + c) = (a + b) + c$ (tính chất kết hợp).
- $\exists \emptyset \in G$ sao cho $\emptyset + a = a + \emptyset = a, \forall a \in G$ (\emptyset là Identity Element của G).
- $\forall a \in G \exists -a \in G : a + (-a) = \emptyset$

Nhóm G là nhóm hoán vị (nhóm Aben) nếu $\forall a, b \in G \Rightarrow a + b = b + a$.

Ví dụ:

- Tập hợp các số nguyên với phép + thông thường là nhóm Aben.
- Tập hợp các số nhị phân có độ dài n bit cùng với phép + trong Modulo 2 tạo thành nhóm Aben.

Tính chất của bộ mã chẵn lẻ

Tính tương đương của bộ mã nhóm cộng tính và bộ từ mã kiểm tra chẵn lẻ được thể hiện qua 2 định lý sau:

Định lý 1: tập hợp các từ mã trong bộ mã kiểm tra chẵn lẻ là một nhóm cộng tính.
(Đề nghị sinh viên chứng minh định lý này dựa vào các tính chất của nhóm cộng tính)

Định lý 2: Nếu tập hợp W là tập các dãy nhị phân với độ dài các dãy cùng bằng n và W là một nhóm Aben với phép cộng Modulo 2 thì W có thể xem như một bộ mã kiểm tra chẵn lẻ được sinh ra từ ma trận A có dạng như sau:

$$A = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1k} \\ b_{21} & b_{22} & \dots & b_{2k} \\ I_m & & & \\ \dots & \dots & \dots & \dots \\ b_{m1} & b_{m2} & \dots & b_{mk} \end{bmatrix}$$

Trong đó:

- Ma trận A có m dòng và n cột.
- I_m là ma trận đơn vị cấp m.
- k: là số dãy nhị phân (hay từ mã) độc lập tuyến tính lớn nhất.
- n: là độ dài của từ mã và $m = n - k$.
- b_{ij} : được xác định bằng cách dựa vào hệ phương trình tuyến tính (*) và k từ mã độc lập tuyến tính như sau:

$$w'_i = \underbrace{r_1 r_2 r_3 \dots r_m}_{r_m+1 r_{m+2} \dots r_n} (\forall i = \overline{1, k})$$

Đoạn kiểm tra Đoạn thông tin

$$(*) \begin{cases} r_i = b_{11} r_{m+1} + \dots + b_{kk} r_{m+k} \\ r_m = b_{m1} r_{m+1} + \dots + b_{mk} r_{m+k} \end{cases}$$

Thết k từ mã độc lập tuyến tính vào hệ pt (*) để tìm các $b_{ij} \Rightarrow$ ma trận A.

Ví dụ minh họa

Xét tập hợp M gồm có 8 dãy nhị phân dài 6 bits như sau:

$$\begin{array}{cccccc} & r_1 & r_2 & r_3 & r_4 & r_5 & r_6 \\ \hline w'_0 & 0 & 0 & 0 & 0 & 0 & 0 \\ w'_1 & 1 & 0 & 1 & 0 & 0 & 1 \\ w'_2 & 1 & 1 & 0 & 0 & 1 & 0 \\ w'_3 & 0 & 1 & 0 & 1 & 0 & 1 \\ w'_4 & 0 & 1 & 1 & 0 & 1 & 1 (w'_1 + w'_2) \\ w'_5 & 1 & 1 & 1 & 1 & 0 & 0 (w'_1 + w'_3) \\ w'_6 & 1 & 0 & 0 & 1 & 1 & 1 (w'_2 + w'_3) \\ w'_7 & 0 & 0 & 1 & 1 & 1 & 0 (w'_1 + w'_2 + w'_3) \end{array}$$

Ta thấy $\{w_1, w_2, w_3\}$ là tập hợp lớn nhất các từ mã độc lập tuyến tính từ tập hợp M:

$$\begin{aligned} w'_1 &= 1 \ 0 \ 1 \ 0 \ 0 \ 1 \\ w'_2 &= 1 \ 1 \ 0 \ 0 \ 1 \ 0 \\ w'_3 &= 0 \ 1 \ 0 \ 1 \ 0 \ 1 \end{aligned}$$

$$\Rightarrow n=6 \text{ và } k=3. \Rightarrow m = n - k = 3.$$

Như vậy: ma trận kiểm tra chẵn lẻ có dạng như sau:

$$A = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ I_3 & b_{21} & b_{22} & b_{23} \\ & b_{31} & b_{32} & b_{33} \end{bmatrix}$$

Các b_{ij} ($\forall i, i = \overline{1,3}$) được xác định từ hệ phương trình tuyến tính nhị phân sau:

$$\begin{aligned} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} &= b_{11} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + b_{12} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + b_{13} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \\ \Rightarrow \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} &= b_{21} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + b_{22} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + b_{23} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} &= b_{31} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + b_{32} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + b_{33} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \\ \Rightarrow \begin{cases} b_{11} = 1 & b_{12} = 1 & b_{13} = 1 \\ b_{21} = 1 & b_{22} = 1 & b_{23} = 0 \\ b_{31} = 1 & b_{32} = 0 & b_{33} = 1 \end{cases} \\ \Rightarrow A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \end{aligned}$$

Vậy ta có thể sử dụng nhóm M như là một bộ mã kiểm tra chẵn lẻ.

Phương pháp sinh mã kiểm tra chẵn lẻ nhanh

Bước khởi tạo: xác định các giá trị n, m, k, s .

Bước 1: sinh k từ mã độc lập tuyến tính (dltt).

Bước 2: cộng tổ hợp các từ mã:

+ Cộng các tổ hợp của 2 từ mã từ k mã dltt \Rightarrow có C_k^2 từ mã.

+ Cộng các tổ hợp của k từ mã từ k từ mã dltt \Rightarrow có C_k^k từ mã.

Bước 3: Cộng $s-1$ từ mã đã tìm được để tìm từ mã cuối cùng $\Rightarrow C_k^0 = 1$ từ mã.

Tổng số từ mã $s = \sum_{i=0}^k C_k^i = 2^k$ từ mã.

Ví dụ sinh mã kiểm tra chẵn lẻ nhanh

Tìm bộ mã nhóm khi biết trước ma trận kiểm tra $A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

Bước khởi tạo: $n = 6, m = 3, k = 3, s = 2^k = 8$.

Bước 1: Sinh $k = 3$ từ độc lập truyền tính: $w'_1=001001$, $w'_2=111010$, $w'_3=110100$

Bước 2: Cộng tổ hợp các từ mã.

+ Cộng các tổ hợp 2 từ mã đltt:

$$w'_4=w'_1+w'_2=110011$$

$$w'_5=w'_1+w'_3=111101$$

$$w'_6=w'_2+w'_3=001110$$

+ Cộng các tổ hợp 3 từ mã đltt:

$$w'_7=w'_1+w'_2+w'_3=001111$$

Bước 3: xác định từ mã cuối cùng:

$$w'_0=w'_1+w'_2+w'_3+w'_4+w'_5+w'_6+w'_7=000000$$

Bài tập

1. Sử dụng phương pháp sinh mã nhanh cho bộ mã từ ma trận kiểm tra A như sau:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

2. Sử dụng phương pháp sinh mã nhanh cho bộ mã từ ma trận kiểm tra A trong các trường hợp sau:

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

BÀI 5.5: LUẬT ĐỒ SỬA LỖI TỐI ƯU

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết được vấn đề của bài toán,
- Hiểu Định nghĩa Hiệp hợp,
- Vận dụng để xây dựng lược đồ sửa lỗi theo các hiệp hợp,
- Vận dụng để xây dựng lược đồ sửa lỗi thông qua bộ sửa lỗi,
- Vận dụng tính Xác suất truyền đúng cho lược đồ sửa lỗi,
- Kiến thức đạt được sẽ là cơ sở để các bạn có thể ứng dụng cho việc thiết kế một hệ thống mã hóa, giải mã và bảo mật thông tin.

Đặt vấn đề

Trong một hệ thống liên lạc truyền tin, bên cạnh các yêu cầu thiết bị (như nguồn phát, bộ mã hóa, kênh truyền, bộ giải mã,...) đảm bảo tốt cho việc truyền và nhận dữ liệu thì còn có các khía cạnh khác như phương pháp mã hóa và giải mã sao cho tối ưu là phần rất quan trọng trong hệ thống. Vấn đề luôn được đặt ra ở đây là làm thế nào để chỉ ra một phương pháp giải mã tối ưu, có nghĩa là hệ thống phải có khả năng phát hiện và sửa lỗi một cách chính xác nhất có thể có khi nhiều xảy ra. Đây chính là vấn đề chính được thảo luận trong suốt bài học này.

Định nghĩa Hiệp hợp

Gọi $W = \{w_1, w_2, \dots, w_s\}$ là bộ mã kiểm tra chẵn lẻ,
 $V = \{v_1, v_2, \dots, v_r\}$ là tập hợp các dãy n bit có thể nhận được ở cuối kênh.

Ta gọi một hiệp hợp của W trong V là tập hợp có dạng $z + W$ (z là bộ lỗi)

Ví dụ: Cho ma trận kiểm tra chẵn lẻ sau:

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Từ A, ta có thể xây dựng được bộ mã tương ứng sau: $W = \{w'_0 = 0000, w'_1 = 0101, w'_2 = 1110, w'_3 = 1011\}$.

Ta có thể thấy rằng, các bộ lỗi một bit khác nhau có thể có là $z = \{1000, 0100, 0010, 0001\}$. Do đó các hiệp hợp ứng với các bộ lỗi 1 bit sẽ là:

	w ₀	w ₁	w ₂	w ₃
	0000	0101	1110	1011

Hiệp hợp 1	1000	1101	0110	0011	(với $z_1 = 1000$)
Hiệp hợp 2	0100	0001	1010	1111	(với $z_2 = 0100$)
Hiệp hợp 3	0010	0111	1100	1001	(với $z_3 = 0010$)
Hiệp hợp 4	0001	0100	1111	1010	(với $z_4 = 0001$)

Trong đó: hiệp hợp $i = w_i + z_i$, các bạn có thể xét thêm các bộ lỗi sai 2 bit, 3 bit, ... để được các hiệp hợp ứng với các bộ lỗi sai 2 bit, 3bit,....

Lược đồ sửa lỗi theo các hiệp hợp

Bước 1: Lập bảng các hiệp hợp ứng với các bộ lỗi cần thiết

- Dòng đầu tiên viết các từ mã $w_i \in W$.
- Các dòng tiếp theo ứng với cột $w_0 = 00\dots00$ viết các bộ lỗi z (các bộ lỗi 1 bit, 2 bit,...).
- Các dòng ở cột thứ i được xác định bởi $z + w_i$

Bước 2: Quá trình giải mã

Giải mã: khi nhận v , ta xác định cột thứ i chứa v và giải mã về w_i tương ứng.

Ví dụ: xây dựng lược đồ sửa lỗi theo các hiệp hợp cho bộ mã được sinh từ ma trận kiểm tra chẵn lẻ sau:

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Từ A, ta có thể xây dựng được bộ mã tương ứng sau: $W = \{w'_0 = 0000, w'_1 = 0101, w'_2 = 1110, w'_3 = 1011\}$.

Bước 1: Lập bảng các hiệp hợp ứng với các bộ lỗi cần thiết:

Ta xây dựng các hiệp hợp ứng với các bộ lỗi sai 1 bit. Vậy $z = \{1000, 0100, 0010, 0001\}$.

	w_0	w_1	w_2	w_3
	0000	0101	1110	1011

Hiệp hợp 1 1000 1101 0110 0011 (với $z_1 = 1000$)

Hiệp hợp 2 0100 0001 1010 1111 (với $z_2 = 0100$)

Hiệp hợp 3 0010 0111 1100 1001 (với $z_3 = 0010$)

Hiệp hợp 4 0001 0100 1111 1010 (với $z_4 = 0001$)

(Bảng các hiệp hợp)

Bước 2: Quá trình giải mã:

Giả sử nhận $v = 0111$. Tra tim v trên bảng các Hiệp hợp ta có v ở cột 1. Do đó, v được giải mã về $w_1 = 0101$.

Giả sử nhận $v = 1010$. Tra tim v trên bảng các Hiệp hợp ta có v ở cột 2 hay cột 3. Do đó, v được giải mã về w_2 hay w_3 , trong trường hợp này giải mã không chính xác. Đề nghị các bạn lưu ý và cho ý kiến của bạn về các trường hợp giải mã không chính xác này.

Lược đồ sửa lỗi thông qua bộ lỗi

Để xây dựng lược đồ sửa lỗi thông qua bộ sửa lỗi, ta dựa vào tính chất của bộ sửa lỗi. Như vậy ta có thể thấy lược đồ giải mã gồm 2 bước sau:

Bước 1: Lập bảng sửa lỗi: Bộ lỗi (Z) – Bộ sửa lỗi ($C = A^*Z$).

Bước 2: Quá trình sửa lỗi

- Khi nhận được dãy n bit $v \in V$, ta xác định bộ điều lỗi C cho v với $C = A.v$.
- Tra bảng sửa lỗi để tìm bộ lỗi z_0 ứng với C.
- Giải mã $w = v + z_0$.

Ví dụ minh họa lược đồ sửa lỗi 1 bit

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

Xét bộ mã được sinh từ ma trận $A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$

Bộ mã tương ứng được xác định là: $w_1=000000$, $w_2=101101$, $w_3=111010$, $w_4=010111$

(Đề nghị các bạn tham khảo phương pháp sinh mã chẵn lẻ và xây dựng lại bộ mã từ ma trận kiểm tra chẵn lẻ A).

Lược đồ sửa lỗi:

Bước 1: Lập bảng sửa lỗi: Bộ lỗi- Bộ điều chỉnh ($e = 1$)

	Bộ lỗi (z')	Bộ điều chỉnh ($C' = A.z$)	
Bộ 0 lỗi	000000	0000	
Bộ lỗi 1 bit	100000	1000	1 Bộ
	010000	0100	
	001000	0010	
	000100	0001	
	000010	1110	
	000001	1011	

Bước 2: Quá trình sửa lỗi

- Giả sử nhận $v=001101$, tính $C = A.v = 1000$
- Tra bảng sửa lỗi để tìm bộ lỗi z_0 ứng với C , ta có $z_0 = 100000$
- Giải mã $w = v + z_0 = 001101 + 100000 = 101101 = w_2$

Ví dụ minh họa lược đồ sửa lỗi 2 bit

Lược đồ sửa lỗi:

Bước 1: Lập bảng sửa lỗi: Bộ lỗi- Bộ điều chỉnh ($e = 2$)

	Bộ lỗi (z')	Bộ điều chỉnh ($C' = A.z$)	
Bộ lỗi 2 bit	110000	1100	7 Bộ
	101000	1010	
	100100	1001	
	100010	0110	
	100001	0011	
	011000	0110	
	010100	0101	

(Tất cả các bộ 2 lỗi còn lại có trùng bộ điều chỉnh với các bộ ở trên)

Bước 2: Quy trình sửa lỗi

- Giả sử nhận $v=100111$, tính $C = A.v = 1100$
- Tra bảng sửa lỗi để tìm bộ lỗi z_0 ứng với C , ta có $z_0 = 110000$
- Giải mã $w = v + z_0 = 100111 + 110000 = 010111 = w_4$

Ví dụ minh họa lược đồ sửa lỗi 3 bit

Lược đồ sửa lỗi:

Bước 1: Lập bảng sửa lỗi: Bộ lỗi- Bộ điều chỉnh ($e = 3$)

Bộ lỗi 3 bit	z'		$C = A.z$
	110100	110101	
	110001	0111	
			2 Bộ

(Tất cả các bộ 3 lỗi còn lại có trùng bộ điều chỉnh với các bộ ở trên)

Bước 2: Quy trình sửa lỗi

Giả sử nhận $v=011001$, tính $C = A.v = 110100$

Tra bảng sửa lỗi để tìm bộ lỗi z_0 ứng với C , ta có $z_0 = 110100$

Giải mã $w=v + z_0 = 011001 + 110100 = 101101 = w_2$

Chú ý:

Tổng số bộ điều chỉnh $= 2^m$. Trong một số trường hợp, bộ mã chẵn lẻ chỉ cho phép phát hiện lỗi trên đường truyền và không thể giải mã chính xác do tổng số bộ điều chỉnh $= 2^m$ và số bộ lỗi có thể lớn hơn nhiều (so với tổng số bộ điều chỉnh).

Xác suất truyền đúng

Gọi N_i là số bộ lỗi ứng với i lỗi có thể tự sửa, khi đó xác suất truyền đúng và tự điều chỉnh sẽ là:

$$P(e') = \sum_{i=0}^n N_i \cdot \beta \cdot (1 - \beta)^{n-i}$$

Với n là độ dài từ mã

Ví dụ: xét trường hợp các ví dụ trên với $n=6$ và tự sửa $e = 3$ bit lỗi. Áp dụng công thức trên ta có:

$$P(e') = \sum_{i=0}^3 N_i \cdot \beta \cdot (1 - \beta)^{n-i} = (1 - \beta)^6 + 6\beta(1 - \beta)^5 + 7\beta^2(1 - \beta)^4 + 2\beta^3(1 - \beta)^3$$

Bài tập

1. Cho ma trận kiểm tra chẵn lẻ sau:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- Xây dựng bộ mã kiểm tra chẵn lẻ.
- Minh họa quy trình sửa lỗi 1 bit.

2. Từ kết quả của bài tập 1, hãy minh họa lược đồ sửa lỗi thông qua bộ điều chỉnh trong các trường hợp lỗi 1 bit, 2 bit. Tính xác suất truyền đúng cho các trường hợp có thể tự sửa được.

BÀI 5.6: MÃ HAMMING

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Hiệu Mã Hamming,
- Hiệu tính chất của mã Hamming.

Mã Hammin

Mã Hamming là một dạng mã nhóm (mã kiểm tra chẵn lẻ) được xác định từ ma trận kiểm tra chẵn lẻ A có dạng sau:

- Cột thứ j của ma trận A là biểu diễn nhị phân m bit (m là số bit kiểm tra chẵn lẻ) của số j theo qui ước biểu diễn nhị phân của số j được viết theo thứ tự từ dưới lên trên (viết theo cột), tương đương với viết từ trái sang phải (viết theo dòng).
- Các bit ở vị trí 2^i ($i = 0, 1, 2, \dots$) được chọn làm bit kiểm tra.

Ví dụ 1: biểu diễn nhị phân của số $j = 3$ có $m = 3$ bit như sau:

Viết theo dòng: 011 (viết từ trái sang phải)

Viết theo cột: $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ (viết từ dưới lên)

Ví dụ 2: ma trận kiểm tra chẵn lẻ với $n=6$, $m=3$ có thể viết như sau:

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Từ mã Hamming có dạng: $w=r_1r_2r_3r_4r_5r_6$. Trong đó, $r_1r_2r_4$ là các bit kiểm tra và $r_3r_5r_6$ là các bit thông tin (vì các bit ở vị trí 2^i (với $i = 0, 1, 2, \dots$) được chọn làm bits kiểm tra).

Tính chât

Nếu cho trước số bit (m) và số bit lỗi tự sửa (e) thì số bit tối đa của bộ mã Hamming (n) có thể được ước lượng từ bất đẳng thức sau:

$$2^m \geq \sum_{i=0}^e C_n^i$$

Ví dụ minh họa

Tim bộ mã Hamming với $n = 6$ và $m = 3$

Ta có thể viết ngay ma trận kiểm tra chẵn lẻ cho bộ mã Hamming

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Từ A $\Rightarrow k = n - m = 3$.

Các bit ở các vị trí 1, 2, 4 được chọn làm các bit kiểm tra.

\Rightarrow số từ mã của bộ mã Hamming là $s = 2^k = 8$

Tim k từ mã độc lập tuyến tính có dạng:

$$w'_1 = r_1r_2r_401$$

$$w'_2 = r_1r_2r_410$$

$$w'_3 = r_1r_21r_400$$

Giải các hệ phương trình: $A.w_1=0$, $A.w_2=0$, $A.w_3=0$

Các từ mã còn lại được xác định theo phương pháp sinh mã nhanh.

Ghi chú: Kết quả chi tiết xây dựng bảng mã Hamming dành cho sinh viên tự làm.

Bài tập

1. Viết ma trận kiểm tra chẵn lẻ cho bộ mã Hamming với $n = 15$.
2. Từ kết quả bài tập 1, hãy tìm các từ mã Hamming độc lập tuyến tính tương ứng.
3. Xét bộ mã Hamming với số bit kiểm tra cho trước là m , khi đó:
 - Độ dài mã tối thiểu là bao nhiêu?
 - Độ dài mã tối đa là bao nhiêu?

BÀI 5.7: THANH GHI LÙI TỪNG BƯỚC

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể biết:

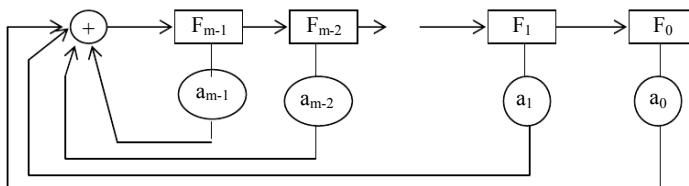
- Đặt vấn đề về thanh ghi lùi từng bước,
- Cách biểu diễn vật lý của thanh ghi,
- Cách biểu diễn toán học của thanh ghi,
- Tìm chu kỳ của thanh ghi.

Đặt vấn đề

Như chúng ta đã biết, phương pháp sinh bộ mã kiểm tra chẵn lẻ dựa trên lý thuyết nhóm cho phép chúng ta sinh mã nhanh bằng cách chỉ sinh ra k từ mã độc lập tuyến tính trong tổng số $s=2^k$ từ mã, từ k từ mã này ta có thể xác định các từ mã còn lại (bằng cách cộng tổ hợp các từ mã). Vấn đề đặt ra ở đây là làm sao để tìm ra một phương pháp sinh mã khác sao cho số từ mã sinh ban đầu nhỏ hơn k (k là số từ mã độc lập tuyến tính của bộ mã kiểm tra chẵn lẻ) và từ đây ta có thể xác định nhanh các từ mã còn. Cụ thể dựa trên mô hình của thanh ghi lùi từng bước có thể giải quyết được vấn đề này.

Biểu diễn vật lý của thanh ghi

Để gọi một cách ngắn gọn, ta qui ước gọi thanh ghi thay vì gọi thanh ghi lùi từng bước. Biểu diễn vật lý của thanh ghi có thể thấy như hình vẽ dưới đây:



- $F_{m-1}, F_{m-2}, \dots, F_1, F_0$: các bit lưu trữ dữ liệu nhị phân.
- $a_{m-1}, a_{m-2}, \dots, a_1, a_0$: các công tắc (switch) dùng để đóng ($=1$) hay mở ($=0$).
- $(+)$: là bộ làm tính cộng trong phép toán modulo 2 sau mỗi xung đồng hồ với dữ liệu do các bit của thanh ghi gửi về.

Quá trình dịch chuyển lùi từng bước: sau mỗi xung đồng hồ thì dữ liệu trong bit F_i sẽ được chuyển về lưu trữ ở bit F_{i-1} ($F_1 \rightarrow F_0$; $F_2 \rightarrow F_1$; ...; $F_{m-2} \rightarrow F_{m-3}$; $F_{m-1} \rightarrow F_m$). Tất cả các giá trị trên các F_i (trước khi có xung điện) sẽ được chuyển về bộ cộng (tùy theo các công tắc đóng hay mở), tổng của các giá trị này sẽ được đưa vào lưu trữ ở bit F_{m-1} .

Ta sẽ nghiên cứu thanh ghi này cụ thể hơn trong các nội dung tiếp theo nhằm tìm ra một phương pháp sinh mã mà ta có thể gọi là mã xoay vòng. Đây cũng là một dạng mã kiểm tra chẵn lẻ.

Biểu diễn toán học của thanh ghi

Mục tiêu của việc biểu diễn toán học là để tìm ra các mô hình tính toán phục vụ cho việc nghiên cứu sinh mã xoay vòng chẵn lẻ từ thanh ghi.

Gọi $x = (x_0, x_1, \dots, x_{m-2}, x_{m-1})$ là giá trị các bit của thanh ghi tại thời điểm trước khi có nhịp xung đồng hồ.

$x' = (x'_0, x'_1, \dots, x'_{m-2}, x'_{m-1})$ là giá trị các bit của thanh ghi sau khi có nhịp xung đồng hồ.

Khi đó ta có:

$$x'_0 = x_1$$

$$x'_1 = x_2$$

$$x'_2 = x_3$$

.....

$$x'_{m-2} = x_{m-1}$$

$$x'_{m-1} = a_0 x_0 + a_1 x_1 + \dots + a_{m-1} x_{m-1}.$$

Hay viết theo dạng ma trận ta có $x' = T.x$

Trong đó:

$$T = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ a_0 & a_1 & a_2 & a_3 & \dots & a_{m-2} & a_{m-1} \end{bmatrix}$$

- T : Ma trận vuông cấp m .
- Dòng cuối của ma trận: là các hệ số: a_0, a_1, \dots, a_{m-1} .
- Gốc trên bên phải: là ma trận đơn vị cấp $m-1$.

T được gọi là ma trận đặc trưng của thanh ghi lùi từng bước.

Quá trình dịch chuyển lùi từng bước của thanh ghi:

Gọi $x^{(0)} = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{m-1} \end{pmatrix}$ là véc tơ chỉ giá trị của thanh ghi tại thời điểm đang xét.

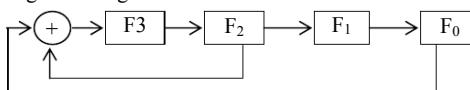
Giá trị của thanh ghi sau 1 xung đồng hồ là $x^{(1)} = T.x^{(0)}$

Giá trị của thanh ghi sau 2 xung đồng hồ là $x^{(2)} = T.x^{(1)} = T^2.x^{(0)}$

Giá trị của thanh ghi sau 3 xung đồng hồ là $x^{(3)} = T.x^{(2)} = T^3.x^{(0)}$

Ví dụ thanh ghi lui từng bước

Cho thanh ghi lui từng bước sau:



Từ thanh ghi, ta có: $m=4$, $a_0=1$, $a_1=0$, $a_2=1$, $a_3=0$.

Ma trận đặc trưng của thanh ghi: $T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

Chu kỳ của thanh ghi

Như đã trình bày ở trên về quá trình dịch chuyển lùi từng bước của thanh ghi:

Nếu ta gọi $x^{(0)} = \begin{pmatrix} x_0 \\ x_2 \\ x_3 \\ \vdots \\ x_{m-1} \end{pmatrix}$ là vec tơ chỉ giá trị của thanh ghi tại thời điểm khởi tạo thì các giá trị của thanh ghi ở các thời điểm tiếp theo như sau:

Giá trị của thanh ghi sau 1 xung đồng hồ là $x^{(1)} = T \cdot x^{(0)}$

Giá trị của thanh ghi sau 2 xung đồng hồ là $x^{(2)} = T \cdot x^{(1)} = T^2 \cdot x^{(0)}$

Giá trị của thanh ghi sau 3 xung đồng hồ là $x^{(3)} = T \cdot x^{(2)} = T^3 \cdot x^{(0)}$

Giá trị của thanh ghi sau n xung đồng hồ là $x^{(n)} = T^n \cdot x^{(0)}$ (bởi vì số trạng thái thông tin khác nhau có thể có là 2^m)

Vậy chu kỳ của thanh ghi là số xung nhịp đồng hồ để thanh ghi lặp lại trạng thái ban đầu. Nghĩa là nếu $x^{(0)} \neq 0$ và $\exists n > 0$ sao cho $x^{(n)} = x^{(0)}$ thì ta nói n là chu kỳ của thanh ghi.

Lưu ý:

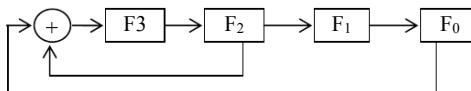
Cách viết biểu diễn nhị phân cho giá trị của $x^{(i)}$ theo thứ tự từ trên xuống (theo cột), tương ứng với viết từ trái sang phải (theo dòng). Ví dụ: biểu diễn nhị phân của $x^{(i)} = 3$ có $m = 3$ bit như sau:

Viết theo dòng: $x^{(i)} = 011$ (viết từ trái sang phải)

Viết theo cột: $x^{(i)} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ (viết từ trên xuống)

Ví dụ tìm chu kỳ của thanh ghi

Cho thanh ghi lui từng bước như hình sau:



Từ thanh ghi ta có: $m=4$, $a_0=1$, $a_1=0$, $a_2=1$, $a_3=0$.

Ma trận đặc trưng của thanh ghi: $T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

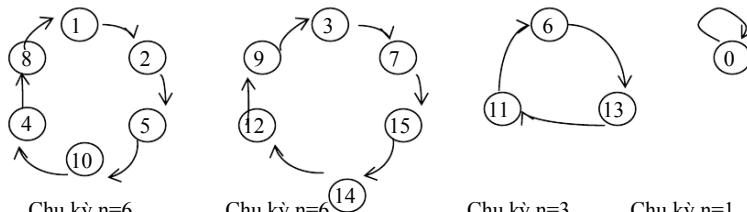
Đặc giá trị khởi tạo của thanh ghi $x^{(0)} = 1$ = $\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Tìm chu kỳ:

$$\begin{aligned} X^{(1)} = T \cdot x^{(0)} &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \Rightarrow x^{(2)} = T \cdot x^{(1)} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \Rightarrow x^{(3)} = T \cdot x^{(2)} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \\ \Rightarrow x^{(4)} = T \cdot x^{(3)} &= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \Rightarrow x^{(5)} = T \cdot x^{(4)} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow x^{(6)} = T \cdot x^{(5)} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = x^{(0)} \end{aligned}$$

Tương tự:

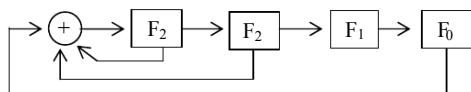
- + Khi chọn $x^{(0)} = 3$ thì ta cũng có chu kỳ $n = 6$.
- + Khi chọn $x^{(0)} = 6$ thì ta có chu kỳ $n = 3$.
- + Khi chọn $x^{(0)} = 0$ thì ta có chu kỳ $n = 1$.



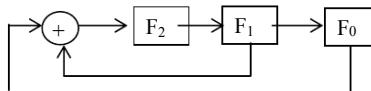
Thanh ghi trên có 4 chu kỳ.

Bài tập

1. Tìm các chu kỳ của thanh ghi lui từng bước như hình sau:



2. Tìm các chu kỳ của thanh ghi lui từng bước như hình sau:



BÀI 5.8: MÃ XOAY VÒNG

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Biết cách xác định ma trận kiểm tra chẵn lẻ cho mã xoay vòng (hay còn gọi là mã vòng),
- Hiểu định nghĩa mã xoay vòng,
- Vận dụng xây dựng bộ mã xoay vòng,
- Vận dụng phương pháp sinh nhanh bộ mã xoay vòng để sinh bộ mã kiểm tra chẵn lẻ.

Ma trận kiểm tra chẵn lẻ mã xoay vòng

Định nghĩa: ma trận kiểm tra chẵn lẻ được thiết kế từ thanh ghi lùi từng bước là ma trận có dạng sau:

$$A = [x^{(0)} | T x^{(0)} | T^2 x^{(0)} | \dots | T^{n-1} x^{(0)}]$$

Trong đó:

- T là ma trận đặc trưng của thanh ghi.
- $x^{(0)} \neq 0$: là giá trị khởi tạo của thanh ghi.
- n : là chiều dài của từ mã và cũng là chu kỳ của thanh ghi.
- m : là số bit kiểm tra hay số bit của thanh ghi.

Ví dụ: xét lại ví dụ tìm chu kỳ thanh ghi, nếu chọn giá trị khởi tạo của thanh ghi là $x^{(0)} = 1$ thì ta có ma trận kiểm tra với chu kỳ $n=6$ như sau:

$$A = [x^{(0)} \ x^{(1)} \ x^{(2)} \ x^{(3)} \ x^{(4)} \ x^{(5)}] = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Định nghĩa mã xoay vòng

Mã xoay vòng là mã kiểm tra chẵn lẻ được sinh ra từ ma trận kiểm tra chẵn lẻ ứng với chu kỳ n của thanh ghi lùi từng bước có dạng như:

$$A = [x^{(0)} | Tx^{(0)} | T^2 x^{(0)} | \dots | T^{n-1} x^{(0)}]$$

Ví dụ: xét lại ma trận kiểm tra chẵn lẻ ở trên

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \quad (\text{chu kỳ } n = 6)$$

Ta có $n = 6$, $m = 3$, $k = 2 \Rightarrow s = 2^k = 2^2 = 4$ từ mã.

Áp dụng Phương pháp sinh mã nhanh bộ mã kiểm tra chẵn lẻ ta có bộ mã kiểm tra chẵn lẻ gồm 4 từ mã sau: $w_0 = 000000$, $w_1 = 101010$, $w_2 = 010101$, $w_4 = 111111$, đây chính là một trong các bộ mã xoay vòng sinh từ thanh ghi lùi từng bước nêu trên (**Các bước sinh mã nhanh để nghị các bạn tự làm**)

Phương pháp sinh nhanh bộ mã xoay vòng

Cách sinh nhanh k từ mã độc lập tuyến tính của bộ mã vòng từ $a_0, a_1, a_2, \dots, a_{m-1}$:

Bước 1: sinh mã xoay vòng đầu tiên

Sinh mã xoay vòng đầu tiên có dạng $w_1 = a_0 a_1 a_2 \dots a_{m-1} \underbrace{1000 \dots 00}_{k-1 \text{ bit } 0}$

Bước 2: sinh $k-1$ từ mã độc lập tuyến tính còn lại

$w_2 = 0a_0a_1a_2\dots a_{m-1} \underbrace{1000\dots 0}_{k-2 \text{ bit } 0}$ (dịch w_1 sang phải 1 bit).

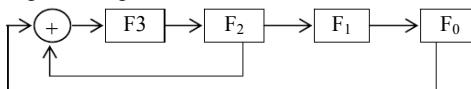
.....
 $w_k = \underbrace{000\dots 0}_{k-1 \text{ bit } 0}a_0a_1a_2\dots a_{m-1}1$ (dịch từ w_{k-1} sang phải 1 bit).

Bước 3: xác định các từ mã còn lại của bộ mã

Các từ mã còn lại gồm ($2^k - k$ từ mã) được xác định bằng cách cộng tổ hợp của 2, 3, ..., k từ mã từ k từ mã độc lập tuyếntính ở trên.

Ví dụ sinh nhanh bộ mã xoay vòng

Cho thanh ghi lui từng bước như hình sau:



Từ thanh ghi, ta có: m=4, n=6, a₀=1, a₁=0, a₂=1, a₃=0.

Bước 1: Sinh mã xoay vòng đầu tiên

$$w_1 = 101010$$

Bước 2: Sinh k - 1 từ mã độc lập tuyếntính còn lại

$$w_2 = 010101$$

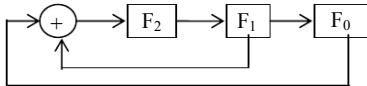
Bước 3: Xác định các từ mã còn lại của bộ mã

$$w_3 = 111111 (w_1 + w_2), w_0 = 000000 (w_1 + w_2 + w_3)$$

Bộ mã vòng vừa sinh là W={000000, 101010, 010101, 111111}

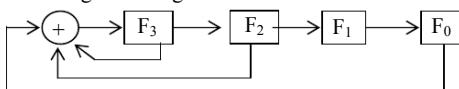
Bài tập

1. Cho thanh ghi lùi từng bước sau:



- Tìm ma trận kiểm tra chẵn lẻ có số cột $n > 4$
- Từ kết quả câu a, xác định bộ mã xoay vòng tương ứng.
- Tìm bộ mã xoay vòng theo phương pháp sinh nhanh bộ mã xoay vòng

2. Cho thanh ghi lùi từng bước sau:



- Tìm ma trận kiểm tra chẵn lẻ có số cột $n > 4$
- Từ kết quả câu a, xác định bộ mã xoay vòng tương ứng.
- Tìm bộ mã xoay vòng theo phương pháp sinh nhanh bộ mã xoay vòng.

BÀI 5.9: ĐA THỨC ĐẶC TRUNG CỦA THANH GHI

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu định nghĩa đa thức đặc trưng của thanh ghi,
- Hiểu Quan hệ giữa chu kỳ n, đa thức đặc trưng và đa thức $(x^n + 1)$,
- Vận dụng sinh thanh ghi lui từng bước,
- Làm cơ sở để vận dụng sinh bộ mã vòng.

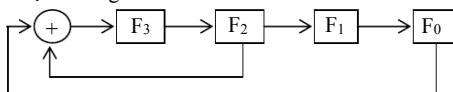
Định nghĩa đa thức đặc trưng của thanh ghi

Định nghĩa: đa thức đặc trưng của thanh ghi có ma trận đặc trưng là T là đa thức có dạng

$$g_m(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} + x^m.$$

với $a_0, a_1, a_2, \dots, a_{m-1}$ là các công tác của thanh ghi và m là số bit của thanh ghi

Ví dụ: xét lại thanh ghi như hình sau:



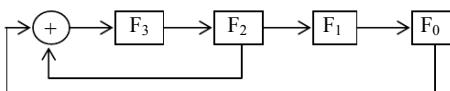
$$a_0 = 1, a_1 = 0, a_2 = 1, a_3 = 0$$

Đa thức đặc trưng của thanh ghi có dạng: $g_m(x) = 1 + x^2 + x^4$.

Quan hệ giữa chu kỳ n, đa thức đặc trưng và đa thức $(x^n + 1)$

Đa thức đặc trưng của thanh ghi $g_m(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} + x^m$ luôn chia hết đa thức $(x^n + 1)$.

Ví dụ: xét lại thanh ghi lui từng bước như hình sau:



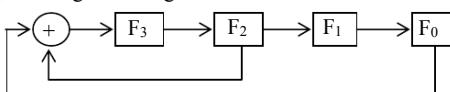
Từ thanh ghi ta có thể xác định các kết quả sau:

- $a_0 = 1, a_1 = 0, a_2 = 1, a_3 = 0$
- Đa thức đặc trưng của thanh ghi có dạng: $g_4(x) = 1 + x^2 + x^4$.
- Thanh ghi này có chu kỳ n = 6.

Thực hiện phép chia đa thức $(x^6 + 1) : (1 + x^2 + x^4) = (x^2 + 1) \Rightarrow$ chia hết.

Ghi chú: phép toán trên đa thức nhị phân vẫn là phép toán Modulo 2.

Ví dụ: xét lại thanh ghi lui từng bước như hình sau:



$$a_0 = 1, a_1 = 0, a_2 = 1, a_3 = 0$$

đa thức đặc trưng của thanh ghi có dạng: $g_4(x) = 1 + x^2 + x^4$.

thanh ghi này có chu kỳ n = 6 và $(x^6 + 1) : 1 + x^2 + x^4 = x^2 + 1$.

Thủ tục sinh thanh ghi lùi từng bước

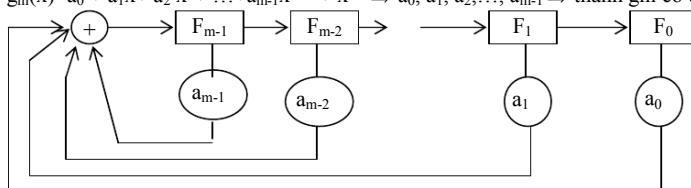
Để sinh thanh ghi lùi từng bước với số bit là m và có chu kỳ n, ta có thể thực hiện theo các bước sau:

Bước 1: xác định đa thức đặc trưng của thanh ghi

- Tìm 2 đa thức $g_m(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} + x^m$ và $h_k(x) = h_0 + h_1x + h_2x^2 + \dots + h_{k-1}x^{k-1} + x^k$ sao cho $(x^n + 1) = g_m(x) * h_k(x)$.
- Nếu $\exists (x^n + 1) = g_m(x) * h_k(x)$ thì ta chọn $g_m(x)$ làm đa thức đặc trưng cho thanh ghi (vì số bit kiểm tra của bộ mã là m) và thực hiện bước 2.
- Ngược lại: không tồn tại thanh ghi theo yêu cầu.

Bước 2: vẽ thanh ghi

Từ $g_m(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} + x^m \Rightarrow a_0, a_1, a_2, \dots, a_{m-1} \Rightarrow$ thanh ghi có dạng:



Ví dụ minh họa

Thiết kế thanh ghi có $m=3$ bit và chu kỳ $n=7$, ta thực hiện theo 2 bước sau:

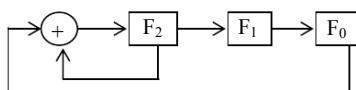
Bước 1: Xác định đa thức đặc trưng của thanh ghi

Ta có $(x^7 + 1) : (1 + x^2 + x^3) = (1 + x^2 + x^3 + x^4)$

Do $m=3$ nên chọn $g_3(x) = (1 + x^2 + x^3)$ làm đa thức đặc trưng của thanh ghi.

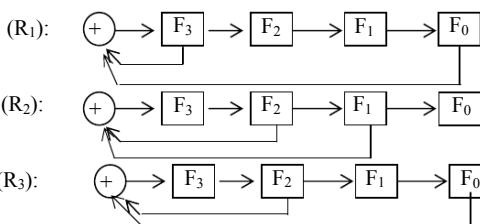
Bước 2: Vẽ thanh ghi

Từ $g_3(x) = (1 + x^2 + x^3)$ ta có, $a_0=1, a_1=0, a_2=1$



Bài tập

- Trong các thanh ghi sau đây, thanh ghi nào sinh ra bộ mã vòng có độ dài $n=15$ bit?



- Nêu các bước cần thiết để thiết kế bộ mã xoay vòng độ dài 15 bit với số bit kiểm tra là 4. Vẽ sơ đồ thanh ghi dạng tổng quát.

Bài 5.10: PHƯƠNG PHÁP SINH MÃ XOAY VÒNG

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu các phương pháp sinh mã vòng,
- Biết bảng liệt kê một số đa thức đặc trưng,
- Vận dụng để sinh mã vòng theo nhiều cách khác nhau.

Đặt vấn đề

Để sinh bộ mã kiểm tra chẵn lẻ, ta có thể dựa theo nhiều phương pháp khác nhau như: sinh mã dựa theo lý thuyết nhóm, mã Hamming,... Vấn đề đặt ra ở đây là làm sao để sinh bộ mã xoay vòng với độ dài n bit và m bit kiểm tra chẵn lẻ. Phương pháp sinh mã xoay vòng dựa trên lý thuyết về đa thức đặc trưng nhị phân của thanh ghi giúp ta có cái nhìn tổng quát về vấn đề sinh bộ mã xoay vòng theo nhiều cách khác nhau.

Phương pháp sinh bằng mã xoay vòng

Để sinh mã xoay vòng độ dài n bit với m bit kiểm tra và k bit thông tin, ta có thể thực hiện theo các bước sau:

Bước 1: tìm 2 đa thức $g_m(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} + x^m$
và $h_k(x) = h_0 + h_1x + h_2x^2 + \dots + h_{k-1}x^{k-1} + x^k$ sao cho $(x^n + 1) = g_m(x) * h_k(x)$.

Nếu $\exists (x^n + 1) = g_m(x) * h_k(x)$ thì chuyển sang bước 2

Ngược lại không thể sinh bộ mã vòng theo yêu cầu.

Bước 2: ta có thể sinh bộ mã xoay vòng theo các cách như dưới đây:

Cách 1: Chọn đa thức $g_m(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} + x^m$

$\Rightarrow a_0, a_1, a_2, \dots, a_{m-1}$

\Rightarrow thanh ghi \Rightarrow ma trận đặc trưng T

\Rightarrow chu kỳ n \Rightarrow ma trận kiểm tra chẵn lẻ A.

\Rightarrow Bộ mã xoay vòng.

Cách 2: chọn đa thức $g_m(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} + x^m$

$\Rightarrow a_0, a_1, a_2, \dots, a_{m-1}$

\Rightarrow Sinh nhanh k từ mã độc lập tuyến tính với từ mã sinh độc lập tuyến tính đầu tiên có dạng: $w_1 = a_0a_1a_2\dots a_{m-1}1000\dots 00 \Rightarrow$ Bộ mã xoay vòng.

$\underbrace{\quad\quad\quad}_{k-1 \text{ bit } 0}$

Cách 3: chọn $h_k(x) = h_0 + h_1x + h_2x^2 + \dots + h_{k-1}x^{k-1} + x^k$ làm đa thức sinh ma trận kiểm tra chẵn lẻ cho bộ mã vòng có dạng:

$$\left(\begin{array}{ccccccccccccc} 0 & 0 & - & - & - & 0 & 0 & 1 & h_{k-1} & - & - & - & h_1 & h_0 \\ 0 & - & - & - & 0 & 0 & 1 & h_{k-1} & - & - & - & - & h_1 & h_0 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 0 & 1 & k_{k-1} & - & - & - & - & h_1 & h_0 & 0 & 0 & - & - & 0 \\ 1 & h_{k-1} & - & - & - & h_1 & h_0 & 0 & 0 & - & - & - & 0 & 0 \end{array} \right) \begin{array}{c} \uparrow \\ m \\ \downarrow \\ \xleftarrow{(m-1) \text{ bits}} \end{array}$$

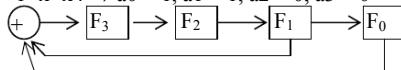
\Rightarrow Sinh bộ mã xoay vòng theo Phương pháp sinh nhanh bộ mã xoay vòng.

Nhận xét: kết quả theo 3 cách sinh bộ mã xoay vòng nói trên la như nhau (cho cùng bộ mã).

Ví dụ minh họa 1

Thiết kế thanh ghi và sinh ma trận kiểm tra chẵn lẻ.

Chọn đa thức $g_m(x) = 1+x+x^4 \Rightarrow a_0 = 1, a_1 = 1, a_2 = 0, a_3 = 0$



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

Ma trận đặc trưng của thanh ghi: $T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

Tìm chu kỳ của thanh ghi:

$$\text{Chọn giá trị khởi tạo } x^{(0)} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\begin{aligned} x^{(1)} = T \cdot x^{(0)} &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}; x^{(2)} = T x^{(1)} &= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}; x^{(3)} = T x^{(2)} &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}; x^{(4)} = T x^{(3)} &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}; x^{(5)} = T x^{(4)} &= \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \\ x^{(6)} = T x^{(5)} &= \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}; x^{(7)} = T x^{(6)} &= \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}; x^{(8)} = T x^{(7)} &= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}; x^{(9)} = T x^{(8)} &= \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}; x^{(10)} = T x^{(9)} &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \\ x^{(11)} = T x^{(10)} &= \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}; x^{(12)} = T x^{(11)} &= \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}; x^{(13)} = T x^{(12)} &= \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}; x^{(14)} = T x^{(13)} &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}; x^{(15)} = T x^{(14)} &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = x^{(0)} \end{aligned}$$

Ma trận kiểm tra chẵn lẻ :

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

\Rightarrow Bộ mã xoay vòng với $n=14$, $m=4$, $k=11$.

Ví dụ minh họa 2

Chọn đa thức $g_m(x) = 1+x+x^4 \Rightarrow a_0 = 1, a_1 = 1, a_2 = 0, a_3 = 0$.

Bước 1: Sinh mã xoay vòng đầu tiên

$$w_1 = 11001000000000$$

Bước 2: Sinh k - 1 từ mã độc lập tuyến tính còn lại

$$w_2 = 01100100000000$$

$$w_3 = 00110010000000$$

$$w_4 = 00011001000000$$

$$w_5 = 00001100100000$$

$$w_6 = 00000110010000$$

$$w_7 = 000000110010000$$

$$w_8 = 000000011001000$$

$$w_9 = 000000001100100$$

$$w_{10} = 000000000110010$$

$$w_{11} = 000000000011001$$

Bước 3: Xác định các từ mã còn lại của bộ mã

(215 - 11) từ mã còn lại được xác định bằng cách cộng tổ hợp 2, 3, 4,.., k = 11 từ mã từ k=11 từ mã độc lập tuyến tính.

Ví dụ minh họa 3

Chọn $h_k(x) = 1 + x + x^2 + x^3 + x^5 + x^7 + x^8 + x^{11}$ làm đa thức sinh ma trận kiểm tra chẵn lẻ cho bộ mã vòng $\Rightarrow h_0 = 1, h_1 = 1, h_2 = 1, h_3 = 1, h_4 = 0, h_5 = 1, h_6 = 0, h_7 = 1, h_8 = 1, h_9 = 0, h_{10} = 0$.

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \text{Bộ mã xoay vòng}$$

Bảng liệt kê một số đa thức đặc trưng

M	Đa thức	M	Đa thức
3	$1+x+x^3$	14	$1+x+x^6+x^{10}+x^{14}$
4	$1+x+x^4$	15	$1+x+x^{15}$
5	$1+x^2+x^5$	16	$1+x+x^3+x^{12}+x^{16}$
6	$1+x+x^6$	17	$1+x^2+x^7$
7	$1+x^3+x^7$	18	$1+x^7+x^{18}$
8	$1+x^2+x^3+x^4+x^8$	19	$1+x+x^2+x^5+x^{19}$
9	$1+x^4+x^9$	20	$1+x^3+x^{20}$
10	$1+x^3+x^{10}$	21	$1+x^2+x^{21}$
11	$1+x^2+x^{11}$	22	$1+x+x^{22}$
12	$1+x+x^4+x^6+x^{12}$	23	$1+x^3+x^{23}$
13	$1+x+x^3+x^4+x^{13}$	24	$1+x+x^2+x^7+x^{24}$

Bài tập

- Tìm bộ mã vòng có độ dài 7 bit.
- Tìm thanh ghi sinh bộ mã vòng có độ dài 15 bit.
- Tìm thanh ghi sinh bộ mã vòng có độ dài 31 bit.

BÀI TẬP TỔNG HỢP

Mục tiêu

Sau khi hoàn tất bài học này bạn có thể:

- Hiểu rõ hơn về nội dung môn học.
- Vận dụng nội dung môn học để giải quyết một số bài tập tổng hợp.

Bài 1

Xét một mô hình chẩn đoán bệnh từ các triệu chứng: A, B và C; để chẩn đoán 1 trong 4 bệnh: 1, 2, 3 và 4 với ma trận chẩn đoán (hay ma trận truyền tin).

		Bệnh	1	2	3	4
		Triệu chứng				
A		0,6	0,3	0	0,1	
	B	0,2	0,6	0,2	0	
C		0	0	0,3	0,7	

Yêu cầu:

Câu 1: Vẽ sơ đồ mô tả mô hình chẩn đoán bệnh trên và diễn giải các ý nghĩa của sơ đồ.

Câu 2: Nếu phân phối của Triệu chứng có dạng:

Triệu chứng	A	B	C
P	0,5	0,3	0,2

Tính các lượng sau :

- Lượng ngẫu nhiên (Entropy) của Triệu chứng .
- Lượng ngẫu nhiên của Bệnh.
- Lượng ngẫu nhiên của Bệnh khi biết Triệu chứng.
- Lượng chẩn đoán đúng.(Lượng thông tin biết về Bệnh thông qua Triệu chứng) và tỷ lệ chẩn đoán đúng là bao nhiêu phần trăm.

Câu 3: Bây giờ người ta sử dụng 2 bit để mã thông tin về Triệu chứng (có 1 triệu chứng dự trữ) và 5 bit để mã các triệu chứng khi chẩn đoán bệnh trực tuyến. Mô tả các đoạn của dãy 5 bit trong phương pháp kiểm tra chẵn lẻ.

Câu 4: Nếu sử dụng ma trận kiểm tra chẵn lẻ dạng:

1	1	1	0	1
0	1	0	1	1
1	0	0	1	1

Tính các từ mã.

Xây dựng Bộ sửa lỗi 1 bit dùng cho tự động sửa lỗi tối ưu trong quá trình chẩn đoán trực tuyến. Cho một ví dụ.

Bài 2

Xét một kênh truyền tin đặc biệt dạng : Truyền X → Nhận Y.

Truyền một giá trị của X có thể nhận được nhiều giá trị khác nhau của Y với các xác suất khác nhau. Bảng xác suất truyền X và nhận các Y khác nhau được cho dưới đây:

X \ Y	y ₁	y ₂	y ₃	y ₄	y ₅	y ₆
x ₀	0,6	0,1	0,1	0,05	0,05	0,1
x ₁	0,1	0,05	0,6	0,1	0,1	0,05
x ₂	0,05	0,1	0,1	0,05	0,6	0,1
x ₃	0,1	0,05	0,05	0,1	0,1	0,6

Yêu cầu:

Câu 1: Vẽ sơ đồ mô tả kênh truyền tin trên và diễn giải các ý nghĩa của sơ đồ.

Câu 2: Nếu phân phối của X có dạng :

X	x ₀	x ₁	x ₃	x ₄
P	0.5	0.25	0.15	0.1

tính thông lượng về X truyền trên kênh.

Câu 3: Phân phối của X cần có dạng như thế nào để thông lượng truyền trên kênh là lớn nhất.

Tính dung lượng kênh truyền.

Câu 4: Bây giờ người ta sử dụng 2 bit để mã thông tin về X và 4 bit để mã các giá trị truyền trên kênh. Mô tả các đoạn của dãy 4 bit trong phương pháp kiểm tra chẵn lẻ.

Câu 5: Nếu sử dụng ma trận kiểm tra chẵn lẻ dạng:

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Tính các từ mã.

Xây dựng Bộ sửa lỗi dùng cho tự động sửa lỗi tối ưu trong quá trình truyền tin. Cho một ví dụ.

Bài 3

Người ta cần đánh giá kênh truyền tin và chuẩn bị thực hiện truyền một loại tín hiệu đặc biệt: X = {x₀, x₁, x₂, x₃}

Công việc đầu tiên là phải khảo sát kênh truyền. Kết quả khảo sát cho thấy:

Kênh có thể truyền nhận được 8 giá trị khác nhau, để có khả năng phát hiện lỗi hoặc điều chỉnh lỗi. Ma trận truyền tin có dạng:

X \ Y	y ₁	y ₂	y ₃	y ₄	y ₅	y ₆	y ₇	y ₈
x ₀	0,6	0,1	0,05	0,05	0,05	0,05	0,05	0,05
x ₁	0,05	0,05	0,6	0,1	0,05	0,05	0,05	0,05
x ₂	0,05	0,05	0,05	0,05	0,6	0,1	0,05	0,05
x ₃	0,05	0,05	0,05	0,05	0,05	0,05	0,6	0,1

Yêu cầu:

Câu 1: Vẽ sơ đồ mô tả kênh truyền tin trên và diễn giải các ý nghĩa của sơ đồ. Nếu phân phối của X có dạng :

X	x ₀	x ₁	x ₃	x ₄
P	0.5	0.25	0.15	0.1

tính thông lượng về X truyền trên kênh.

Câu 2: Phân lớp các giá trị của Y về các lớp B_0, B_1, B_2 , và B_3 dùng để giải mã tối ưu Y tốt nhất về các giá trị tương ứng của X.

Câu 3: Bây giờ người ta sử dụng 2 bit để mã thông tin về X và 4 bit để mã các giá trị truyền trên kênh. Mô tả các đoạn của dãy 4 bit trong phương pháp kiểm tra chẵn lẻ.

Câu 4: Nếu sử dụng ma trận kiểm tra chẵn lẻ dạng:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Tính các từ mã.

Xây dựng Bộ sửa lỗi dùng cho tự động sửa lỗi tối ưu trong quá trình truyền tin. Cho một ví dụ.

Bài 4

Xét một mô hình chẩn đoán bệnh từ các triệu chứng: A, B và C; để chẩn đoán 1 trong 4 bệnh: 1, 2, 3 và 4 với ma trận chẩn đoán (hay ma trận truyền tin)

		Bệnh	1	2	3	4
		Triệu chứng				
A	Triệu chứng	0,5	0,3	0	0,2	
	B	0,1	0,2	0,7	0	
C		0	0,1	0,3	0,6	

Yêu cầu:

Câu 1: Giả sử người ta biết thêm 3 triệu chứng gây bệnh khác đó là : D, E và F và muốn ghi lại các triệu chứng này thông qua bảng ký hiệu $A = \{+, -\}$.

Hãy kiểm tra tính tách đưc của bảng mã sau :

Triệu chứng : X	A	B	C	D	E	F
Mã : W	+	-+	++-	--+-	+++-	--

Câu 2: Nếu các triệu chứng ở câu 1 có phân phối :

Triệu chứng : X	A	B	C	D	E	F
P	0.5	0.2	0.2	0.05	0.03	0.2

Giả sử có một người bệnh với 1 trong 5 triệu chứng trên đến khám bệnh và bác sĩ sẽ hỏi bệnh với nguyên tắc, sao cho người bệnh chỉ trả lời bằng 2 câu : Đúng hoặc Sai.

- Tìm phương pháp hỏi bệnh với số câu hỏi trung bình ít nhất.
- Tính số câu hỏi trung bình.
- Tính lượng ngẫu nhiên của Triệu chứng.
- Nhận xét gì về số câu hỏi trung bình và lượng ngẫu nhiên của triệu chứng.

Câu 3: Bây giờ sử dụng mô hình 3 triệu chứng {A, B, C} và 4 bệnh. Vẽ sơ đồ mô hình chẩn đoán bệnh và diễn giải các ý nghĩa của sơ đồ.

Câu 4: Từ kết quả câu 3, người ta sử dụng 2 bit để mã thông tin về Triệu chứng (có 1 triệu chứng dự trữ) và 5 bit để mã các triệu chứng khi chẩn đoán bệnh trực tuyến. *Mô tả các đoạn* của dãy 5 bit trong phương pháp kiểm tra chẵn lẻ.

Câu 5: Nếu sử dụng ma trận kiểm tra chẵn lẻ dạng:

$$A = \begin{array}{|c|c|c|c|c|} \hline 1 & 1 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 0 & 1 & 1 \\ \hline \end{array}$$

Tính các từ mã.

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 nat = log₂(e) = 1.4427 bit

1 hart = log₁₀(10) = 3.3219 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:

$$H(X) = - \int_{-\infty}^{+\infty} w(x) \log w(x) dx; \quad w(x) \text{ là hàm mdfs}$$

- 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:

$$H(X, Y) = - \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log w(x, y) dxdy$$

- 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:

$$H(X|Y) = - \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log w(x|y) dxdy$$

$$H(Y|X) = - \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log w(y|x) dxdy$$

- 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:

$$H(Y|X) = H(Y); \quad H(X|Y) = H(X)$$

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

+ Đổi với nguồn rời rạc có N tin: $H(X) \leq \log N$

- Lượng tin tương hỗ của 2 tin rời rạc:

$$I(x_i; y_j) = H(x_i) - H(x_i|y_j) = \log \frac{p(x_i|y_j)}{p(x_i)}$$

$$= \log \frac{p(x_i, y_j)}{p(x_i) \cdot p(y_j)} = \log \frac{p(y_j|x_i)}{p(y_j)} = H(y_j) - H(y_j|x_i)$$

$$I(x_i; y_j) = I(x_i) + I(y_j) - I(x_i, y_j)$$

- Lượng tin tương hỗ giữa 2 nguồn rời rạc:

$$I(X; Y) = \sum_{i,j} p(x_i, y_j) \cdot \log \frac{p(x_i|y_j)}{p(x_i)}$$

$$= \sum_{i,j} p(x_i, y_j) \cdot \log \frac{p(y_j|x_i)}{p(y_j)}$$

$$= \sum_{i,j} p(x_i, y_j) \cdot \log \frac{p(x_i, y_j)}{p(x_i) \cdot p(y_j)}$$

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

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

- Lượng tin tương hỗ giữa 2 nguồn liên tục:

$$I(X; Y) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log \frac{w(x, y)}{w(x) \cdot w(y)} dxdy$$

$$= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log \frac{w(x|y)}{w(x)} dxdy$$

$$= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} w(x, y) \cdot \log \frac{w(y|x)}{w(y)} dxdy$$

- 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 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:

$$R = 2F_{max} \cdot H(X)$$

+ Đối với nguồn có công suất định hưu hạn:

$$R = 2F_{Max} \cdot \log(x_{Max} - x_{Min})$$

+ Đối với nguồn có công suất trung bình hạn chế:

$$R = 2F_{Max} \cdot \log \sqrt{2\pi e P_x}$$

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:

$$P(X, Y) = \begin{bmatrix} \frac{1}{3} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{3} \end{bmatrix}$$

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 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:

$$P(X|Y) = \begin{bmatrix} p(x_0|y_0) & p(x_0|y_1) \\ p(x_1|y_0) & p(x_1|y_1) \end{bmatrix} = \begin{bmatrix} \frac{p(x_0, y_0)}{p(y_0)} & \frac{p(x_0, y_1)}{p(y_0)} \\ \frac{p(x_1, y_0)}{p(y_0)} & \frac{p(x_1, y_1)}{p(y_0)} \end{bmatrix} = \begin{bmatrix} 0.8 & 0.2 \\ 0.2 & 0.8 \end{bmatrix}$$

- Dùng công thức dễ dàng tính được:

Ma Katz

$$H(X) = - \sum_i p(x_i) \cdot \log p(x_i) = 1; H(Y) = - \sum_j p(y_j) \cdot \log p(y_j) = 1$$

$$H(X, Y) = - \sum_{i,j} p(x_i, y_j) \cdot \log p(x_i, y_j) = 2 \left(\frac{2}{5} \cdot \log \frac{5}{2} + \frac{1}{10} \cdot \log \frac{10}{1} \right) \approx 1.7219 \text{ bit/kh}$$

$$H(X|Y) = H(X, Y) - H(Y) = 0.7219; H(Y|X) = H(X, Y) - H(X) = 0.7219$$

$$I(X; Y) = H(X) + H(Y) - H(X, Y) = 0.2781 \text{ bit/kh}$$

Bài 4. Giá sử kênh nhị phân được sử dụng để truyền nguồn tin nhị phân đẳng 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 đẳng xác suất nên: $p(x_0) = p(x_1) = 1/2$

Ma trận xác suất đồng thời:

$$P(X, Y) = \begin{bmatrix} p(x_0, y_0) & p(x_0, y_1) \\ p(x_1, y_0) & p(x_1, y_1) \end{bmatrix} = \begin{bmatrix} p(y_0|x_0)p(x_0) & p(y_1|x_0)p(x_0) \\ p(y_0|x_1)p(x_1) & p(y_1|x_1)p(x_1) \end{bmatrix}$$

$$= \begin{bmatrix} 0.75 \cdot 0.5 & 0.25 \cdot 0.5 \\ 0.25 \cdot 0.5 & 0.75 \cdot 0.5 \end{bmatrix} = \begin{bmatrix} \frac{3}{8} & \frac{1}{8} \\ \frac{1}{8} & \frac{3}{8} \end{bmatrix}$$

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:

$$H(X|Y) = - \sum_{i,j} p(x_i, y_j) \log p(x_i|y_j) = 0,8113 \text{ bit/tin}$$

$$H(Y|X) = - \sum_{i,j} p(x_i, y_j) \log p(y_j|x_i) = 0,8113 \text{ bit/tin}$$

Entropy của nguồn rời rạc:

$$H(X) = - \sum_i p(x_i) \cdot \log p(x_i) = 1; H(Y) = - \sum_j p(y_j) \cdot \log p(y_j) = 1$$

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

Too long to read on
your phone? Save
to read later on
your computer



 Save to a Studylist

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:

$$P(X|Y) = \begin{bmatrix} p(a|y_0) & p(a|y_1) & p(a|y_2) \\ p(b|y_0) & p(b|y_1) & p(b|y_2) \\ p(c|y_0) & p(c|y_1) & p(c|y_2) \end{bmatrix} = \begin{bmatrix} p(a, y_0)/p(y_0) & p(a, y_1)/p(y_1) & p(a, y_2)/p(y_2) \\ p(b, y_0)/p(y_0) & p(b, y_1)/p(y_1) & p(b, y_2)/p(y_2) \\ p(c, y_0)/p(y_0) & p(c, y_1)/p(y_1) & p(c, y_2)/p(y_2) \end{bmatrix}$$

$$= \begin{bmatrix} 2/3 & 1/6 & 1/6 \\ 1/6 & 2/3 & 1/6 \\ 1/6 & 1/6 & 2/3 \end{bmatrix}$$

Từ đó có:

+ Entropy đầu vào:

$$H(X) = - \sum_{j=0,1,2} p(x_j). \log p(x_j) = 3 \cdot \frac{1}{3} \cdot \log_2 3 = 1.585 \text{ bit/tin}$$

cuu duong than cong . com

+ Entropy đầu ra:

$$H(Y) = - \sum_{j=0,1,2} p(y_j). \log p(y_j) = 3 \cdot \frac{1}{3} \cdot \log_2 3 = 1.585 \text{ bit/tin}$$

+ Entropy của 2 nguồn đồng thời:

$$H(X, Y) = - \sum_{i,j} p(x_i, y_j). \log p(x_i, y_j) = 2.8366 \text{ bit/tin}$$

+ Entropy có điều kiện:

$$H(X|Y) = - \sum_{i,j} p(x_i, y_j). \log p(x_i|y_j) = 1.2516 \text{ bit/tin}$$

+ Lượng tin tương hỗ giữa 2 nguồn:

$$I(X; Y) = \sum_{i,j} p(x_i, y_j). \log \frac{p(y_j|x_i)}{p(y_j)} = 3 \cdot \left(\frac{2}{9} \cdot \log_2 \frac{\frac{2}{3}}{\frac{1}{3}} \right) + 6 \cdot \left(\frac{1}{18} \cdot \log_2 \frac{\frac{1}{6}}{\frac{1}{3}} \right) = \frac{1}{3} \text{ bit/tin}$$

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 $40 \pm 0.01^{\circ}\text{C}$. Nhiệt độ đo các thiết bị cấp nhiệt có thể làm cho nhiệt độ lò biến thiên từ $30 - 50^{\circ}\text{C}$. Yêu cầu sự sai khác nhiệt độ của lò so với nhiệt độ khống chế là trong thời gian ≤ 20 phút. Giá 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).

Dễ 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: $R = 20 \cdot R_0 = 20 * 5186.5 \approx 100 \text{ kBit/s}$

$$R = 20R_0 = 20.5188.04 \approx 103 \text{ Kbit/s}$$

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 $\alpha = 20^\circ$. 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

cuu duong than cong . com

Ma Katz

- 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 gặp 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; $P(H) = 1 - P(\bar{H})$.

Từ 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:

$$P(\bar{H}) = P(X_0).P(\bar{H}|X_0) + P(X_1).P(\bar{H}|X_1) = \frac{5}{13} \cdot \frac{1}{4} + \frac{8}{13} \cdot \frac{1}{5} = \frac{57}{260} \Rightarrow P(H) = \frac{203}{260} \approx 78.08\%$$

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/tin).

- 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:

$$P(B, A) = \begin{bmatrix} 0.1 & 0.05 & 0.05 & 0.11 \\ 0.08 & 0.03 & 0.12 & 0.04 \\ 0.13 & 0.09 & 0.14 & 0.06 \end{bmatrix}$$

- 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 $H(A|B) = \log 2$, thông lượng của kênh có nhiều:

$$C = n_0 \cdot I(A; B) = 20 \cdot (H(A) - H(A|B)) = 20 \cdot (\log_2 26 - \log_2 2) \approx 74 \text{ bit/s}$$

Bài 13. Cho kênh nhị phân đối xứng có xác suất truyền lỗi là $p = 10^{-3}$.

a. Tính lượng tin tương hỗ.

b. Nếu chuỗi bit được truyền đi có chiều dài 1KB thì có bao nhiêu bit lỗi?

GIẢI:

a. 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:

$$P(y_0) = \sum_i p(x_i, y_0) = (1-p)\cdot\frac{1}{2} + p\cdot\frac{1}{2} = \frac{1}{2}; P(y_1) = \dots = \frac{1}{2}$$

Entropy nguồn ra Y: $H(Y) = -\sum_j p(y_j).\log p(y_j) = 1$

Lượng tin tương hỗ:

$$I(X; Y) = H(Y) - H(Y|X) = 1 - 2(1-p).\log \frac{1}{1-p} - 2p.\log \frac{1}{p} \approx 0,98859 \text{ bit/kh}$$

b. 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:

a. Bản tin như sau:

LAMMINHANHQUYNHMAIHAIABTRUNGHNHOI

Ma Katz

b. Số ký 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:

$$\begin{aligned} H(X) &= \sum_{i=1}^{14} P(x_i) \cdot \log \frac{1}{P(x_i)} \\ &= \frac{6}{33} \log_2 \frac{33}{6} + 8 \left(\frac{1}{33} \cdot \log_2 33 \right) + 2 \left(\frac{5}{33} \cdot \log_2 \frac{33}{5} \right) + \frac{3}{33} \log_2 11 + \frac{2}{33} \log_2 \frac{33}{2} \\ &= 2.7402 \text{ bit/tin} \end{aligned}$$

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:

$$\begin{aligned} H(X,Y) &= - \sum_{i,j} p(x_i, y_j) \cdot \log p(x_i, y_j) = \frac{2}{33} \cdot \log_2 \frac{33}{2} + \frac{1}{33} \cdot \log_2 33 + \frac{10}{33} \cdot \log_2 \frac{33}{10} + \frac{20}{33} \cdot \log_2 \frac{33}{20} \\ &= 1.3578 \frac{\text{bit}}{\text{tin}} \end{aligned}$$

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 rỗng, 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)
110		11 trùng với từ mã
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