

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÀI GIẢNG

# LÝ THUYẾT THÔNG TIN

**Biên soạn : PGS.Ts. NGUYỄN BÌNH**

Lưu hành nội bộ

**HÀ NỘI - 2006**

# LỜI NÓI ĐẦU

Giáo trình Lý thuyết thông tin là một giáo trình cơ sở dùng cho sinh viên chuyên ngành Điện tử – Viễn thông và Công nghệ thông tin của Học viện Công nghệ Bưu chính Viễn thông. Đây cũng là một tài liệu tham khảo hữu ích cho các sinh viên chuyên ngành Điện - Điện tử.

Giáo trình này nhằm chuẩn bị tốt kiến thức cơ sở cho sinh viên để học tập và nắm vững các môn kỹ thuật chuyên ngành, đảm bảo cho sinh viên có thể đánh giá các chỉ tiêu chất lượng cơ bản của một hệ thống truyền tin một cách có căn cứ khoa học.

Giáo trình gồm 6 chương, ngoài chương I có tính chất giới thiệu chung, các chương còn lại được chia thành 4 phần chính:

**Phần I:** Lý thuyết tín hiệu ngẫu nhiên và nhiễu (Chương 2)

**Phần II:** Lý thuyết thông tin và mã hóa (Chương 3 và Chương 4)

**Phần III:** Lý thuyết thu tối ưu (Chương 5)

**Phần IV:** Mật mã (Chương 6)

**Phần I: (Chương II).** Nhằm cung cấp các công cụ toán học cần thiết cho các chương sau.

**Phần II:** Gồm hai chương với các nội dung chủ yếu sau:

- **Chương III:** Cung cấp những khái niệm cơ bản của lý thuyết thông tin Shannon trong hệ truyền tin rời rạc và mở rộng cho các hệ truyền tin liên tục.

- **Chương IV:** Trình bày hai hướng kiến thiết cho hai định lý mã hóa của Shannon. Vì khuôn khổ có hạn của giáo trình, các hướng này (mã nguồn và mã kênh) chỉ được trình bày ở mức độ các hiểu biết cơ bản. Để có thể tìm hiểu sâu hơn những kết quả mới và các ứng dụng cụ thể sinh viên cần phải xem thêm trong các tài liệu tham khảo.

**Phần III: (Chương V)** Trình bày vấn đề xây dựng các hệ thống thu tối ưu đảm bảo tốc độ truyền tin và độ chính xác đạt được các giá trị giới hạn. Theo truyền thống bao trùm lên toàn bộ giáo trình là việc trình bày hai bài toán phân tích và tổng hợp. Các ví dụ trong giáo trình được chọn lọc kỹ nhằm giúp cho sinh viên hiểu được các khái niệm một cách sâu sắc hơn. Các hình vẽ, bảng biểu nhằm mô tả một cách trực quan nhất các khái niệm và hoạt động của sơ đồ khối chức năng của các thiết bị cụ thể

**Phần VI: (Chương VI)** Trình bày cơ sở lý thuyết các hệ mật bao gồm các hệ mật khóa bí mật và các hệ mật khóa công khai. Do khuôn khổ có hạn của giáo trình, một số vấn đề quan trọng còn chưa được đề cập tới (như trao đổi và phân phối khóa, xác thực, đảm bảo tính toàn vẹn ...)

Sau mỗi chương đều có các câu hỏi và bài tập nhằm giúp cho sinh viên củng cố được các kỹ năng tính toán cần thiết và hiểu sâu sắc hơn các khái niệm và các thuật toán quan trọng.

Phần phụ lục cung cấp một số kiến thức bổ xung cần thiết đối với một số khái niệm quan trọng về một số số liệu cần thiết giúp cho sinh viên làm được các bài tập được ra ở các chương.

Giáo trình được viết dựa trên cơ sở đề cương môn học Lý thuyết thông tin do Bộ Giáo dục và Đào tạo và được đúc kết sau nhiều năm giảng dạy và nghiên cứu của tác giả. Rất mong được sự đóng góp của bạn đọc.

Các đóng góp ý kiến xin gửi về

KHOA KỸ THUẬT ĐIỆN TỬ 1 - HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KM 10. ĐƯỜNG NGUYỄN TRÃI - THỊ XÃ HÀ ĐÔNG

Email: KhoaDT1@hn.vnn.vn

Hoặc [nguyenbinh1999@yahoo.com](mailto:nguyenbinh1999@yahoo.com)

Cuối cùng tôi xin chân thành cảm ơn GS. Huỳnh Hữu Tuệ đã cho tôi nhiều ý kiến quý báu trong các trao đổi học thuật có liên quan tới một số nội dung quan trọng trong giáo trình này.

NGƯỜI BIÊN SOẠN

## CHƯƠNG I: NHỮNG VẤN ĐỀ CHUNG VÀ NHỮNG KHÁI NIỆM CƠ BẢN

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

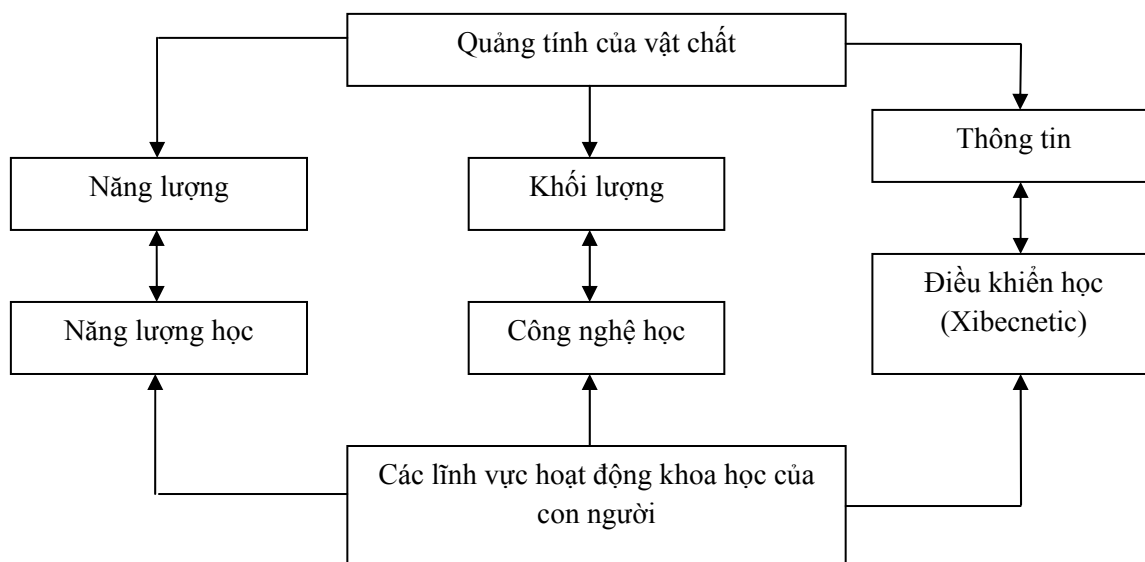
#### 1.1.1. Vị trí, vai trò của Lý thuyết thông tin

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.

Mối quan hệ giữa các hoạt động khoa học của con người và các quá trình của vật chất được mô tả trên hình (1.1).



Hình 1.1. Quan hệ giữa hoạt động khoa học và quá trình 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, thụ, biến đổi, tích lũy 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 hoá 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 đắc 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 tuyến 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 thể chống nhiễu” đánh dấu một bước phát triển rất quan trọng của lý thuyết thông tin.

Trong hai năm 1948 – 1949, Shanon 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 thống 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 thuần túy 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 Shanon, A.N. Kanmôgorov, 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 Shanon, 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 quảng 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 thụ cảm. Thông tin tồn tại một cách khách quan, không phụ thuộc vào hệ thụ 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: Tính 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, băng số liệu, bài nói,... là các tin.

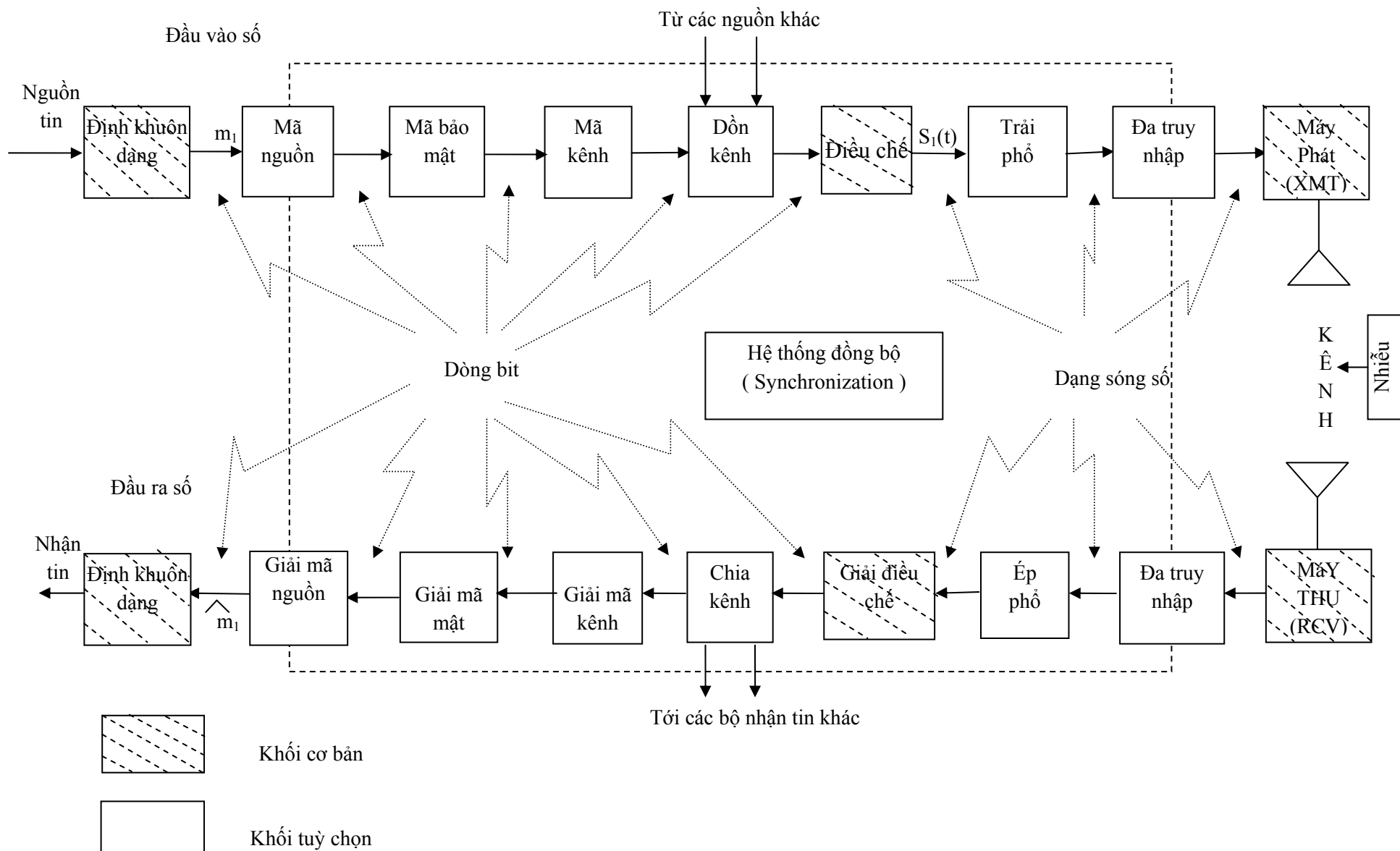
#### 1.2.1.3. Tín hiệu

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 từ

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



**Hình 1.2. Sơ đồ khối 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 tín hiệu tương ứng. Phép biến đổi này phải là đơn trị hai chiều (thì bên thu mới có thể “sao lại” được đúng 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 lập 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 tín hiệu thu được thành tập tin tương ứng.

Máy thu gồm hai khối:

- Giải điều chế: Biến đổi tín hiệu nhận được thành tin đã mã hoá.
- Giải mã: Biến đổi các tin đã mã hoá thành các tin 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**

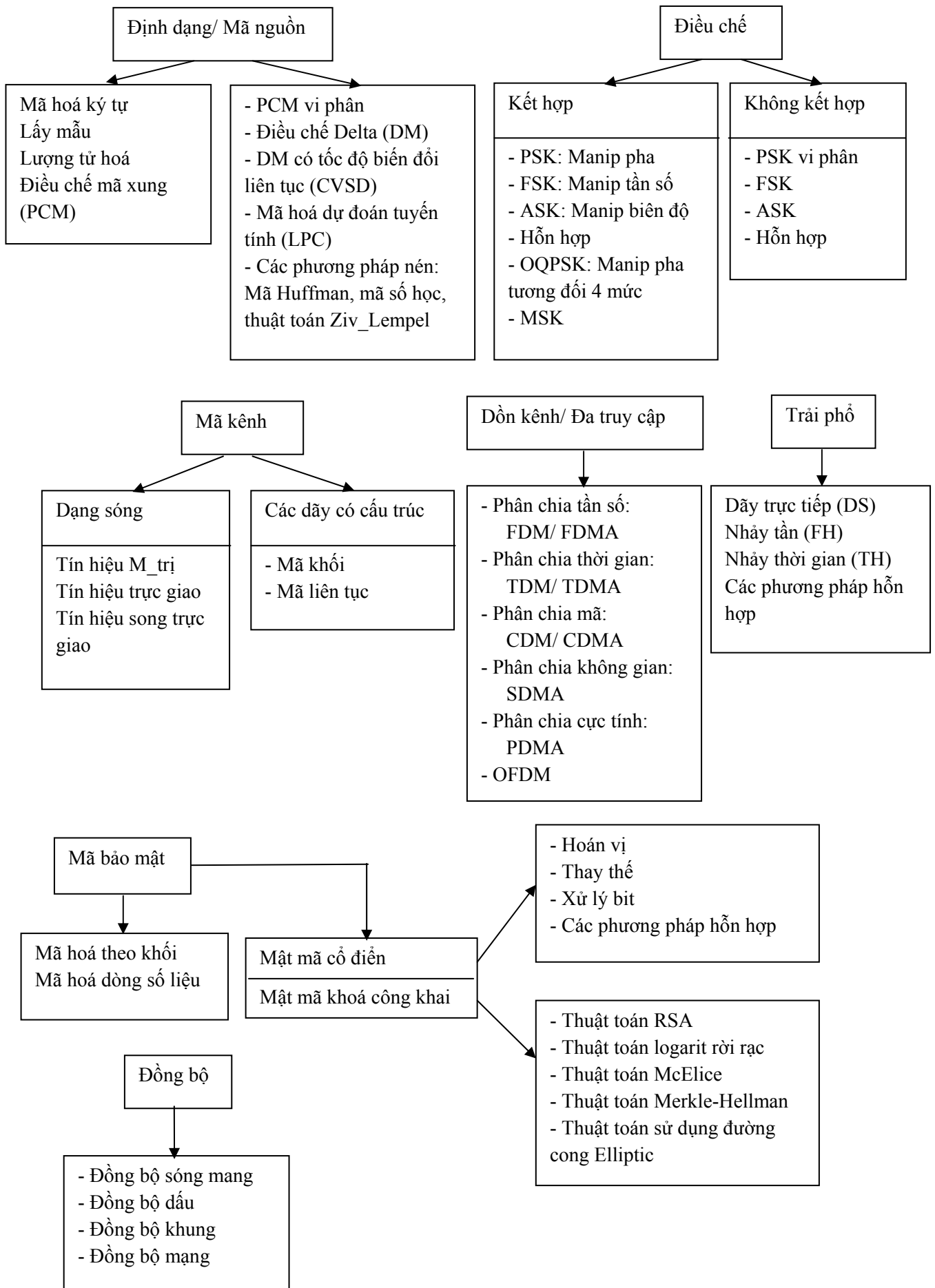
Là tập hợp các thiết bị kỹ thuật phục vụ cho việc truyền tin từ nguồn đến nơi nhận tin.

#### **1.2.2.7. Nhiễu**

Là mọi yếu tố ngẫu nhiên 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 khối tổng quát nhất của một hệ truyền tin số. Nó có thể là: hệ thống vô tuyến điện thoại, vô tuyến điện báo, radar, 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 khối 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 TRƯNG 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 phổ biên độ phức  $\dot{S}(\omega)$ . 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 phổ 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 NGẪU 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 từ). 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 tuần hoàn hoặc không tuần 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. Thật 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 tin, 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 hợp 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 nhiễu 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 ồn 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 điện đài vô tuyến điện cùng làm việc mà chúng có phổ tín hiệu trùng nhau...vv... Các loại nhiễu này không đáng ngại.

#### Chú ý:

Cần phân biệt nhiễu với sự méo gây ra bởi đặc tính tần số và đặc tính thời gian của các thiết bị, kênh truyền... (méo tuyến tính và méo phi tuyến). 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 cả 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.

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

5. Theo nguồn gốc phát sinh: có nhiễu 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  $\tau$  của kênh truyền thì (2.6) có dạng:

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

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

### 2.3.1. Các đặc trưng thống kê

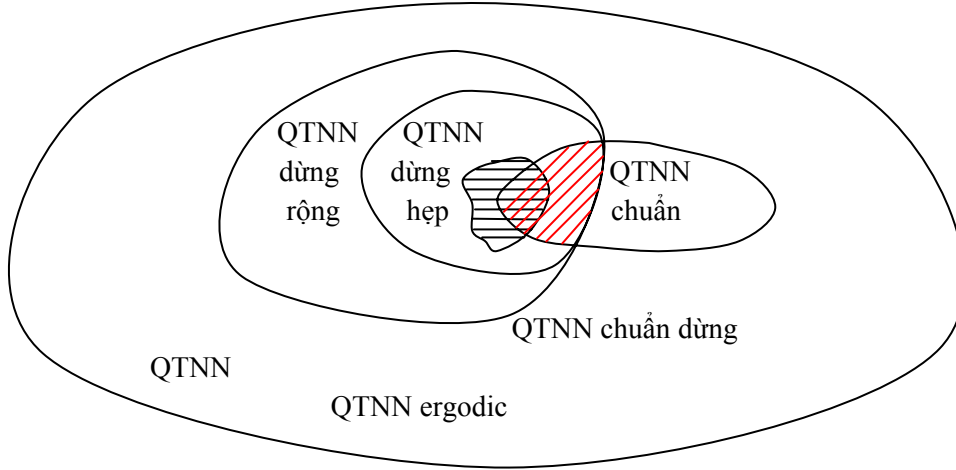
Theo quan điểm thống kê, tín hiệu và nhiễu được coi là các quá trình ngẫu nhiên. Đặc trưng cho các quá trình ngẫu nhiên chính là các quy luật thống kê (các hàm phân bố và mật độ phân bố) và các đặc trưng thống kê ( kỳ vọng, phương sai, hàm tự tương quan, hàm tương quan). Các quy luật thống kê và các 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:

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

$R_x(t_1, t_2)$  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:

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

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

Đôi khi để tiện tính toán và so sánh, người ta dùng hàm tự tương quan chuẩn hoá được định nghĩa bởi công thức:

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

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

### 2.3.2. Khoảng tương quan

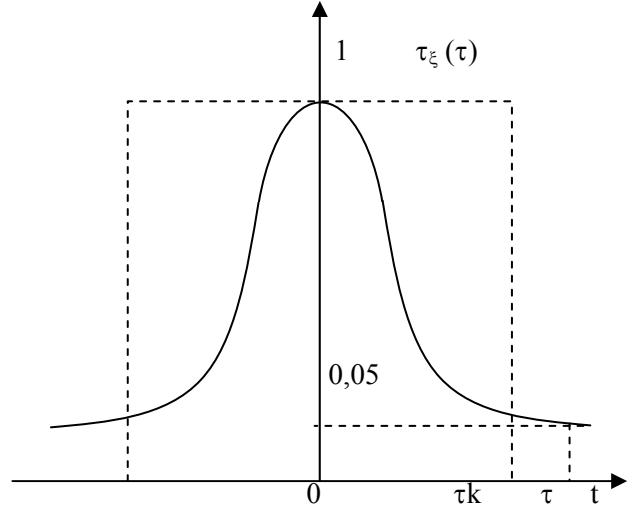
Khoảng tương quan cũng là một đặc trưng khá quan trọng. Ta thấy rằng hai giá trị của một quá trình ngẫu nhiên  $\xi(t)$  chỉ tương quan với nhau khi khoảng cách  $\tau$  giữa hai thời điểm xét là hữu hạn. Khi  $\tau \rightarrow \infty$ , thì coi như hai giá trị ấy không tương quan với nhau nữa. Tuy vậy, trong thực tế, đối với hầu hết các quá trình ngẫu nhiên chỉ cần  $\tau$  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:

#### Định nghĩa 1:

Khoảng tương quan  $\tau_K$  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  $\tau_K$  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:

$\tau_K$  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,... Đối 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:

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

Trung bình thống kê = trung bình theo thời gian



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

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

Mục trước ta mới 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, phổ biên độ phức, mật độ phổ, bề rộng phổ, ... 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 nó cũng không phải là một tập đếm được).

- Nếu tín hiệu ngẫu nhiên là dừng chặt 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  $x_T(t)$  thỏa mãn điều kiện khả tích tuyệt đối nên có thể dùng biến đổi Fourier cho nó được. Ta đã biết rằng phổ biên độ phức  $\dot{S}_T(\omega)$  của  $x_T(t)$  được xác định bởi tích phân thuận Fourier sau:

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

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 thể 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 thể 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  $\left\{ \left| \dot{S}_T(\omega) \right|^2 / T \right\} d\omega$ . Rõ ràng là để đảm

bảo sự bình đẳng về 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 dải tần vô cùng bé  $d\omega$ . Như vậy,  $\frac{\left| \dot{S}_T(\omega) \right|^2}{T}$  sẽ biểu thị công suất của thể hiện  $x_T(t)$  trong một đơn vị tần số [W/Hz] tức là mật độ phổ công suất của thể 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 phổ công suất của thể hiện  $x_T(t)$  trong khoảng  $T$  hữu hạn.  $G_T(\omega)$  đặc trưng cho sự phân bố công suất của một thể hiện  $x_T(t)$  trên thang tần số. Khi cho  $T \rightarrow \infty$  ta sẽ tìm được mật độ phổ công suất của một thể 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 phổ công suất của cả quá trình ngẫu nhiên (tức là tập các thể hiện ngẫu nhiên) thì phải lấy trung bình thống kê đại lượng  $G_x(\omega)$ , tức là:

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

(2.19) là công thức xác định mật độ phổ 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 phổ công suất) ta viết lại và thực hiện biến đổi (2.19) như sau:

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

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 đối 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  $G(\omega)$ :

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

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

Tất nhiên ở đây phải giả sử tích phân ở vế phải 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  $R(\tau)$ . Hiển 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  $\omega$ . 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 thể 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 thoả 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:

$$\Delta\omega = \frac{\int_{-\infty}^{\infty} G(\omega) d\omega}{G(\omega_0)} \quad (2.23)$$

**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.

**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  $\omega$  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  $\omega_0$ .

#### 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 hoà dạng:

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

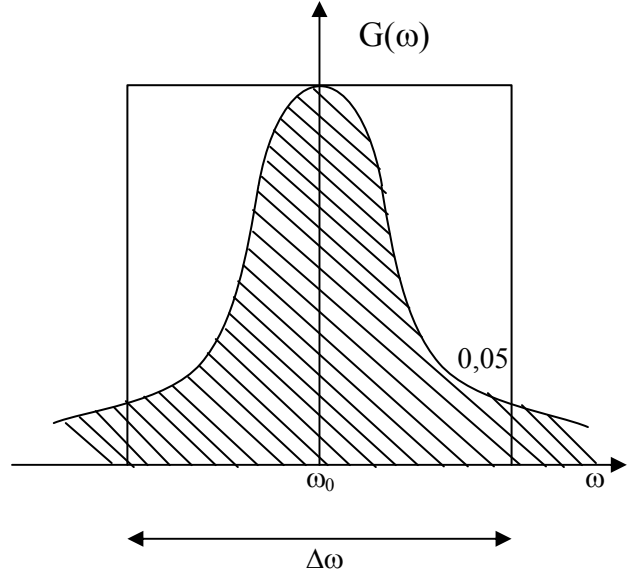
trong đó  $A_K$  và  $\varphi_K$  nói chung có thể là các đại lượng ngẫu nhiên, thì hàm tương quan trung bình:

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

Nếu sử dụng biểu diễn sau của hàm delta:

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

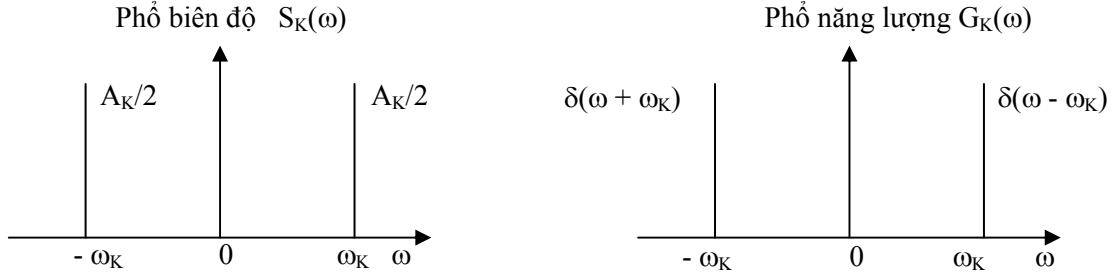
và biểu diễn phổ năng lượng của  $X_K(t)$  dưới dạng:



**Hình 2.3**

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

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  $\omega_K = 0$ .



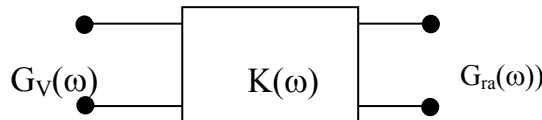
## 2.5. TRUYỀN CÁC TÍN HIỆU NGẪU NHIÊN QUA CÁC MẠCH VÔ TUYẾN ĐIỆN TUYẾN TÍNH

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  $\dot{K}(\omega)$  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 đếm được và hữu hạn thì ta có thể xét hướng ứng ra đối với từng 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  $\dot{K}(\omega)$  của nó. Biết mật độ phổ công suất  $G_v(\omega)$  của quá trình ngẫu nhiên tác động ở đầu vào. Ta phải tìm mật độ phổ 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 phổ biên 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 phổ biên 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):

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

$$\text{Hay: } G_{ra}(\omega) = |\dot{K}(\omega)|^2 \cdot G_v(\omega) \quad (2.25)$$

Người ta đã chứng minh được rằng hưởng 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  $t \gg t_0 = 0$  (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 phổ công suất của quá trình ngẫu nhiên ở đầu ra sẽ liên hệ với nhau theo cặp 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 phổ công suất của hưởng ứng ra được quyết định bởi bình phương môđun hàm truyền của mạch khi đã cho phổ 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 phổ 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 môđun 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 phổ công suất thực tế (phần phổ công suất trải từ  $0 \rightarrow \infty$ ) thì  $G_0 = 2 N_0$  và (2.29) có thể viết lại như sau:

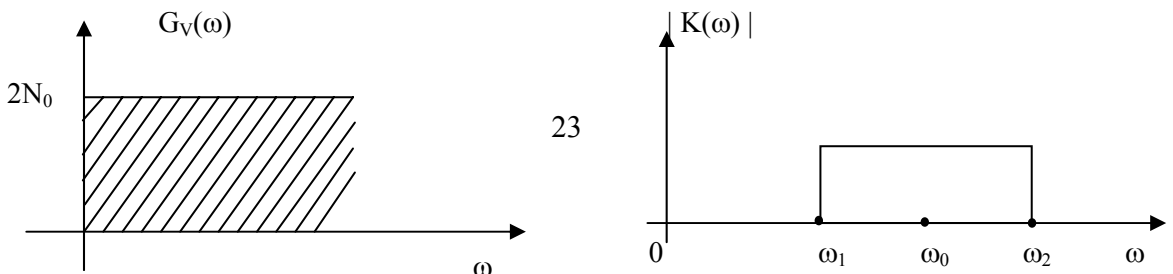
$$P_{ra} = \frac{G_0}{2\pi} \int_0^{\infty} \left| \dot{K}(\omega) \right|^2 d\omega \quad (2.30)$$

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 dừng. 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:

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

Đồ thị  $R_{ra}(\tau)$  như hình 2.5.

(2.32) có thể viết gọn lại như sau:

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

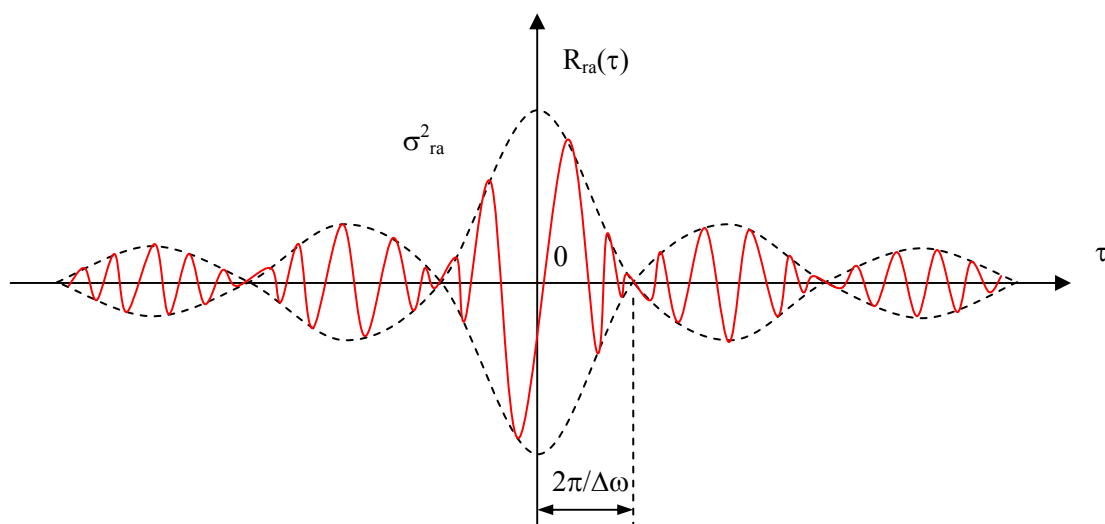
Trong đó:

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

(2.32b) gọi là bao của hàm tự tương quan của nhiễu 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 tạp âm ra là một hàm của đối số  $\tau$  dạng  $\frac{\sin x}{x}$ . Cực đại của hàm tự tương quan của tạp âm ra đạt tại  $\tau = 0$  và bằng  $\sigma_{ra}^2$ , tức là bằng công suất trung bình của tạp âm ra.

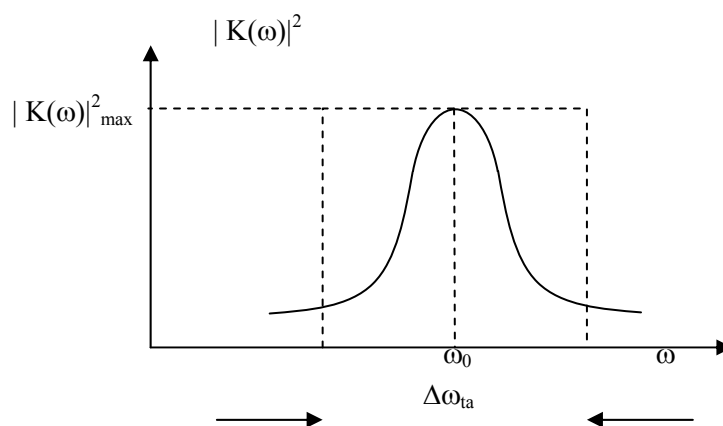
Bây giờ ta sẽ chuyển sang xét một tham số vật lý nữa để đánh giá mức độ truyền tạp âm qua mạch tuyến tính.

#### 2.5.1.4. Giải thông tạp âm

##### Định nghĩa:

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

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



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  $\left| \dot{K}(\omega) \right|^2$  và nửa trục hoành  $(0, \infty)$ ; còn chiều cao của hình chữ nhật này là  $\left| \dot{K}(\omega) \right|^2_{\max}$ .

**Ý nghĩa vật lý:**

$\Delta\omega_{ta}$  đặc trưng cho khả năng làm suy giảm tập âm của các bộ lọc tuyến tính. Với cùng  $\left| \dot{K}(\omega_0) \right|$ , bộ lọc nào có  $\Delta\omega_{ta}$  càng hẹp thì công suất tập 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  $\frac{\Delta\omega_{ta}}{2\pi F} \ll 1$  (F là bề rộng phổ 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 hoá (Gauss hoá) các quá trình ngẫu nhiên không chuẩn bằng bộ lọc giải hẹp.

#### 2.5.2.2. Ví dụ 2

Cho tập 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 tuyến 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:

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

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.

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

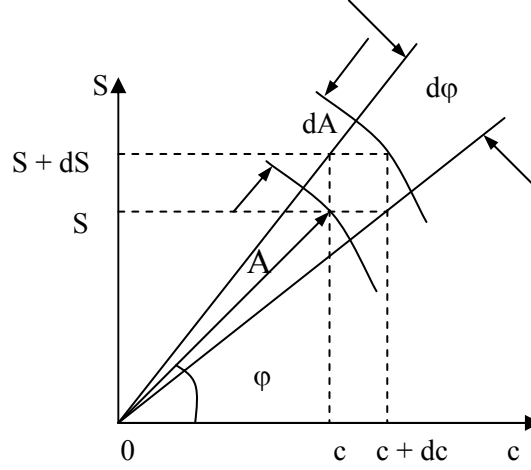
Theo giả thiết  $c(t)$  và  $s(t)$  không tương quan nên:

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

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

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

Ta thấy xác suất để một điểm có tọa độ  $(c, s)$  trong hệ tọa độ Đêcac 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  $(A, \varphi)$  trong hệ tọa độ cực rơi vào một yếu tố diện tích  $dA d\varphi$ . Ta có:



Hình 2.7.

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

Từ đó:

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

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

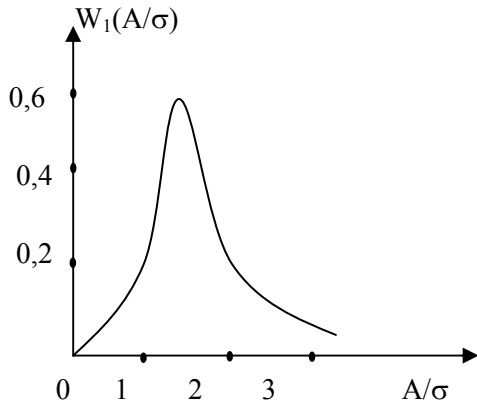
Từ (\*\*) ta có:

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

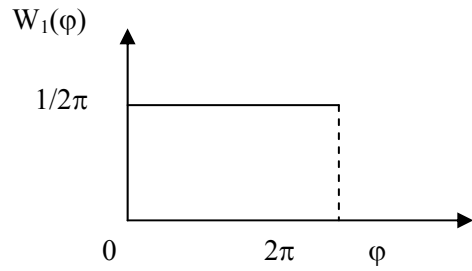
Do đó: 
$$W_1(A) = \int_0^{2\pi} W_2(A, \varphi) d\varphi = \frac{A}{2\pi\sigma^2} \exp\left\{-\frac{A^2}{2\sigma^2}\right\} \int_0^{2\pi} d\varphi$$

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

(2.38) gọi là phân bố Reyleigh (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 Reyleigh. Sở 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 đối 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 đối xứng và chỉ tồn tại ở nửa dương trục hoành.

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

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 đầu vào bộ tách sóng tuyến 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.

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

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

Ta có:

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

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

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

Làm tương tự như VD2, ta có:

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

(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 Reyleigh.

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

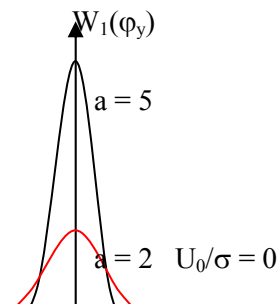
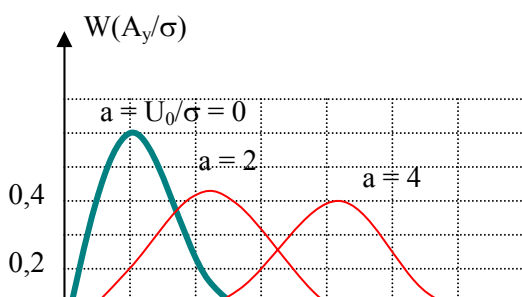
#### Giải thích:

$a \gg 1 \Leftrightarrow$  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.

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

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

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.

-  $a \gg 1 \Rightarrow$  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 gia số (không thăng giáng) và cũng không có sai pha. Khi đó  $\varphi_y$  nhận giá trị “0” trong khoảng  $(-\pi, \pi)$  với xác suất lớn.

## 2.6. BIỂU DIỄN PHỨC CHO THỂ HIỆN CỦA TÍN HIỆU NGẪU NHIÊN – TÍN HIỆU GIẢI HỢP

### 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:

$\omega_0$ : tần số trung tâm;  $\theta(t)$ : pha đầy đủ;

$\varphi_0$ : pha đầu.

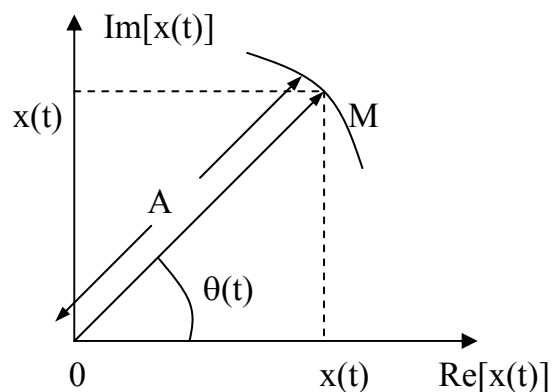
Trong “Lý thuyết mạch”, người ta rất hay dùng cách biểu diễn  $x(t)$  dưới dạng phức sau:

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

Trong đó:

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

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



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.

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

### 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 thoả 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  $\sin\omega_0 t$  thoả 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 (thỏa 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:

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

(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:

$$\dot{x}(t) = x(t) + j\hat{x}(t) = A(t)e^{j\theta(t)}$$

$$x(t) = \operatorname{Re} [\dot{x}(t)] = A(t) \cos \theta(t) \quad (a)$$

$$\hat{x}(t) = \operatorname{Im} [\dot{x}(t)] = A(t) \sin \theta(t) \quad (b)$$

**- Đường bao của tín hiệu giải tích:**

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

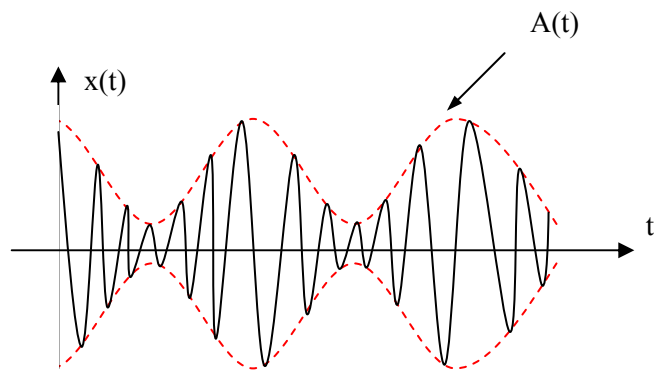
$A(t)$  đặc trưng cho sự biến thiên (dạng biến thiên) của biên độ của tín hiệu (H.2.12).

$A(t)$  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:

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



**Hình 2.12**

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

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

- 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

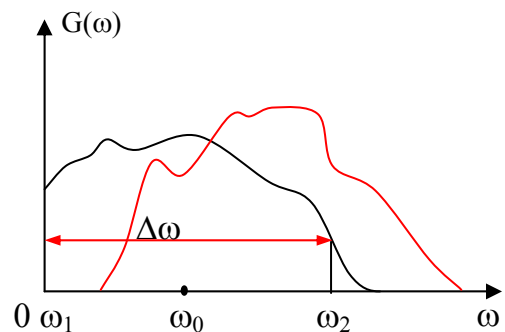
### 2.6.2.1. Tín hiệu giải rộng

Người ta gọi một tín hiệu là tín hiệu giải rộng nếu bề rộng phổ 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 bề rộng phổ của nó có thể so sánh được với  $\omega_0$ .

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

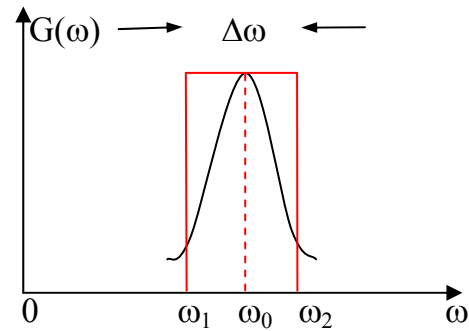
Nếu tín hiệu có bề rộng phổ thỏa mãn:

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

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 biên, tín hiệu đơn biên ....

Nhìn chung tín hiệu giải hẹp là tín hiệu mà bề rộng phổ của nó khá nhỏ hơn so với tần số  $\omega_0$ .



Hình 2.14

### 2.6.2.3. Biểu diễn tín hiệu giải hẹp

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

$$x(t) = A(t)\cos[\omega_0 t - \varphi(t)] = A(t)\cos\theta(t) \quad (2.55)$$

Trong đó:  $\omega_0 t$  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:

$$\begin{aligned} x(t) &= A(t)\cos\omega_0 t \cos\varphi(t) + A(t)\sin\omega_0 t \sin\varphi(t) \\ &= \underbrace{A(t)\cos\varphi(t)}_{c(t)} \cos\omega_0 t + \underbrace{A(t)\sin\varphi(t)}_{s(t)} \sin\omega_0 t \\ &= c(t) \cdot \cos\omega_0 t + s(t) \cdot \sin\omega_0 t \end{aligned} \quad (2.56)$$

$c(t) \cdot \cos\omega_0 t$  là tín hiệu điều biên biến đổi chậm

$s(t) \cdot \sin\omega_0 t$  là tín hiệu điều biên 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 biên biến đổi chậm, với các yếu tố xác định như sau:

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

Rõ ràng là các số hạng ở vế 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 NHIÊN

### 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 phổ vô hạn. ở giáo trình “Lý thuyết mạch”, ta cũng biết rằng một hàm  $x(t)$  có phổ 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:  $\Delta t = 1/2 F_c$

Nếu ta chỉ xét tín hiệu có phổ 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:

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

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.

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

Vì vậy ta có thể coi mỗi hàm là một vecteur đơn vị trên hệ trục tọa 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 tọa 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:

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

Đề 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 thể hiện tín hiệu trong khoảng hữu hạn  $T$ . Như vậy, với thời hạn quan sát và bề rộng phổ của thể 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 hẹp càng ít khác vecteur tín hiệu  $\rightarrow$  ta sẽ nhận đúng được tín hiệu với xác suất cao. Để tính chống 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:

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

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 mút 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 đấy của không gian chính là xác suất để mút vecteur tín hiệu rơi vào miền ấy (nói riêng: điểm ấy) của không gian.



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

Còn nếu  $x(t)$  là ngẫu nhiên có một tập các thể hiện  $\{x_i(t)\}$  thì mút 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:

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

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 các 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).

**- Tập âm trắng:**

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

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

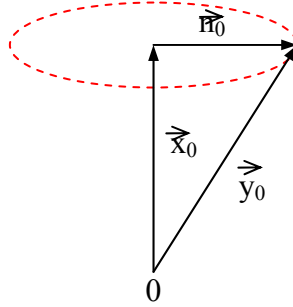
$$\begin{aligned} y(t) &= x(t) + n(t) \\ \Rightarrow \vec{y}_0 &= \vec{x}_0 + \vec{n}_0 \Rightarrow \left\| \vec{y}_0 \right\| = \sqrt{P_y} \end{aligned}$$

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

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

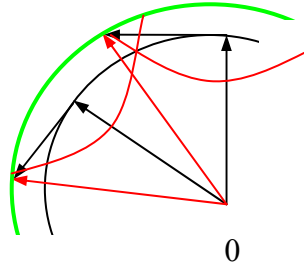
Từ (\*) ta thấy  $\vec{x}_0 \perp \vec{n}_0$  và  $\vec{y}_0$  là cạnh huyền của một tam giác vuông có hai cạnh là  $\vec{x}_0$  và  $\vec{n}_0$ .

Nếu  $x(t)$  xác định thì miền xác định của nút  $\vec{y}_0$  sẽ là đường tròn đáy của hình nón có đỉnh ở gốc tọa độ, chiều cao bằng  $\|\vec{x}_0\|$  và bán kính bằng  $\|\vec{n}_0\|$ . (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 nút  $\vec{y}_0$  sẽ là một mặt cầu có bán kính bằng  $\sqrt{P_x + P_n}$  và có tâm ở gốc tọa 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:

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

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

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

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

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

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

Trong đó  $\varphi$  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 rời rạc hoá tín hiệu thì:

$$d(u_0, v_0) = \left\| \vec{u}_0 - \vec{v}_0 \right\| = \sqrt{\frac{1}{T} \int_0^T [u(t) - v(t)]^2 dt}$$

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

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

$$R_{uv}(0) = \sqrt{D_u(t) \cdot D_v(t)} \rho_{uv}(0)$$

$$d^2(u_0, v_0) = P_u + P_v - 2\sqrt{P_u \cdot P_v} \rho_{uv}(0) \quad (2.67)$$

So sánh (2.66) và (2.67) ta thấy ngay ý nghĩa hình học của hàm tương quan chéo chuẩn hoá:  $\rho_{uv}(0)$  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  $x(t)$ .

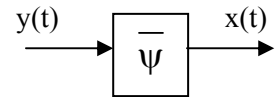
Nếu ta phát đi một thể hiện nào đó của một quá trình ngẫu nhiên  $X(t)$ :

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

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

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

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



Hình 2.16.

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

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

Khi đó máy thu có  $\overline{\Psi}$  tác dụng lên  $\vec{y}$  cho ra  $\vec{x}_j$ :  $\overline{\Psi}[\vec{y}] = \vec{x}_K$ , sẽ được gọi là máy thu tối ưu (theo nghĩa Kachennhicov trong trường hợp các tín hiệu  $x_i(t)$  là đồng 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:

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

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

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

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

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

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:

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

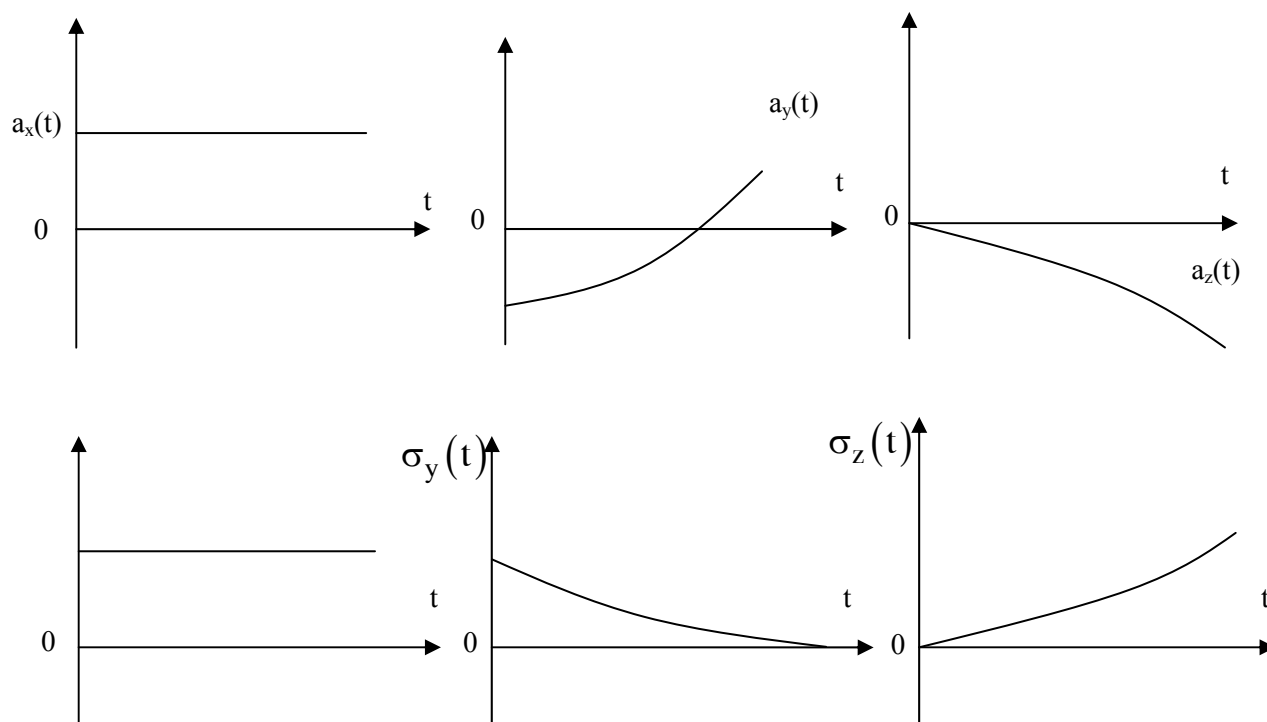
Theo định nghĩa của khoảng cách, ta có thể viết lại như sau:

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

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

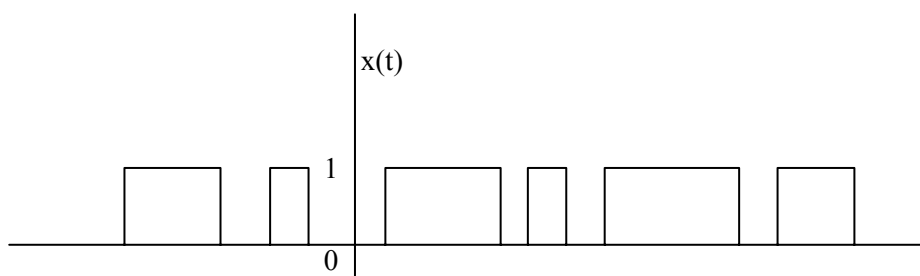
## BÀI TẬP

**2.1.** Đồ thị giá trị trung bình  $a(t)$  và giá trị trung bình bình phương  $\sigma(t)$  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  $\lambda$  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 hoá 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:

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

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

**2.4.** Tìm hàm tự tương quan và mật độ phổ 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  $\tau$  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  $S_a(t)$ :

$$S_a(t) = x(t) + j\hat{x}(t) \text{ là tín hiệu giải tích.}$$

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

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

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

Hãy tính toán và vẽ đồ thị mật độ phổ 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 dám 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 gia đình báo cho 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 gia đình. 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 gia đình. 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) thật 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, đứng 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 đấy 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 thì 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 thủ 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 thì 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 thủ 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 thủ 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, trình sát, tình báo,...) bao giờ cũng có độ bất định.

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

- Nếu tập có hai phần tử thì ta đã phải chọn. Như vậy, trong trường hợp này phép chọn có độ bất định. Nếu số phần tử của tập tăng thì 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
.	.	.
.	.	.
.	.	.
$\infty$	$\infty$	$1/\infty = 0$

$\alpha$

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

### 3.1.2.2. Kết luận

- Bảng 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 thoả 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 được:

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 thì:

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

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

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

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

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

$$\text{N như vậy, ta có: } I(x_K) = k \cdot \ln [p(x_K)] \quad (3.6)$$

Hệ số tỷ lệ  $k$  trong (3.6) có thể chọn tùy ý, nó chỉ xác định hệ đơn vị đo 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 phân 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 tùy theo cách chọn cơ sở 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 thủ tiêu nên ta có thể coi độ bất định cũng chính là thông tin. Do đó:

$$\text{Lượng thông tin} = \text{thông tin tiên nghiệm} - \text{thông tin hậu nghiệm} (*)$$

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,  $y_\ell$  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  $y_\ell$  là  $p(x_K/y_\ell)$ . Như vậy độ bất định của tin  $x_K$  khi đã rõ  $y_\ell$  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  $y_\ell$ ).

Thay (3.9) và (3.10) vào (\*), ta có:

$$\text{Lượng thông tin về } x_K = I(x_K) - I(x_K/y_\ell)$$

$$\underbrace{\text{Lượng thông tin về } x_K}_{\Downarrow \text{ Ký hiệu}} = I(x_K) - I(x_K/y_\ell)$$

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

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

(3.11) gọi là lượng thông tin về  $x_K$  khi đã rõ tin  $y_\ell$  hay còn gọi là lượng thông tin chéo về  $x_K$  do  $y_\ell$  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 tổn 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. ENTROPIE VÀ CÁC TÍNH CHẤT CỦA ENTROPIE

### 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 đề án tốt nghiệp “Khảo sát cấu trúc thống kê chữ Việt” của Đoàn Công Vinh – ĐHBK HN).

**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

Để phép đo được chính xác, trong vật lý, khi đo lường một đại lượng, ta không quan tâm đến từng trị đo được của đại lượng mà thường xét trị trung bình của chúng. Khi đó ta lấy các trị đo 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  $H_1(A)$ :

$$H_1(A) = M[I(a_i)] \quad (3.12)$$

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:

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

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

### 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:**

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

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

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

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

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

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

$$= -p(a_k) \log p(a_k) - \sum_{i=1, i \neq k}^s p(a_i) \log p(a_i) = 0$$

**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 thoả mãn (3.14)) thì entropie của nó đạt cực đại và cực đại đó bằng  $\log s$ .

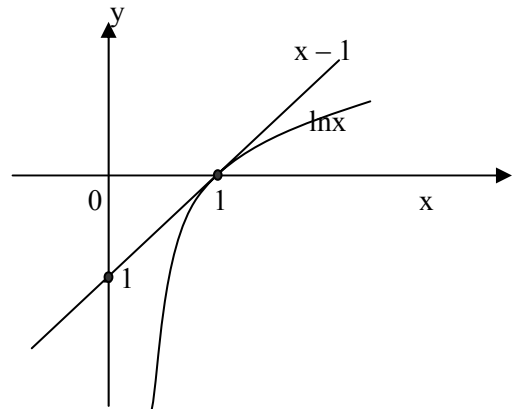
$$H_1(A_{\max}) = \log s \quad (3.17)$$

**Chứng minh:**

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

$$\text{Khi đó } p(a_i) = \frac{1}{s}, \text{ tức là nguồn gồm các dấu}$$

xung khác 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)

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

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

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

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

Entropie là một đại lượng giới nội.

Ký hiệu  $H(A)_{\max} = H_0(A)$

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

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

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

### 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.

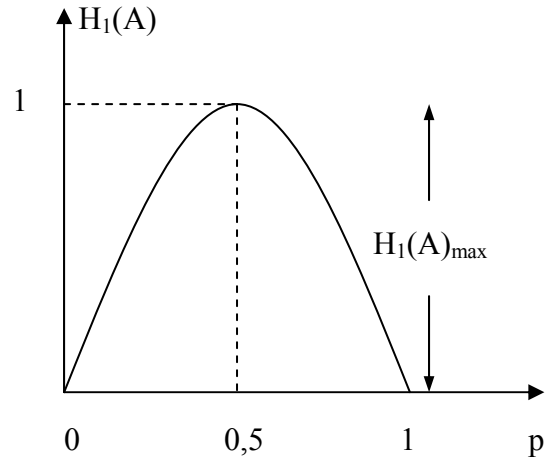
Ta thấy  $H_1(A) = f(p)$  chỉ phụ thuộc vào đặc tính thống kê của các tin.

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.



Hình 3.2.

-  $p = 0 \Rightarrow H_1(A)_{\min} = 0$ . 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 triệt.

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

### 3.2.5. Entropie của trường sự kiện đồng thời

**Định nghĩa 1:**

Có hai trường sự kiện A và B:

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

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:

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

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:

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

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

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

**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.

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

**Chứng minh:** Theo định nghĩa:

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

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

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

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

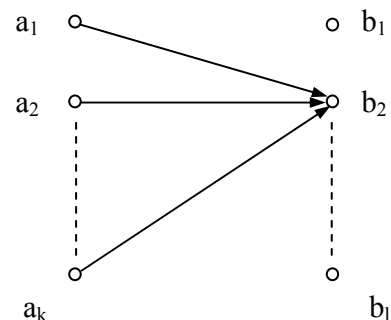
$$\Rightarrow H(A, B) = H(A) + H(B)$$

**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. ENTROPIE CÓ ĐIỀU KIỆN. LƯỢNG 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  $b_\ell$  là khác nhau. Và khi đó lượng thông tin riêng về  $a_k$  do  $b_\ell$  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  $b_\ell$  mang lại mà chỉ quan tâm đến lượng thông tin riêng trung bình về một dấu nào đó của tập  $\{a_i\}$  do  $b_\ell$  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  $b_\ell$  mang lại:

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

**Ý nghĩa:**

$H(A / b_\ell)$  là lượng thông tin tổn 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  $H(A/b_j)$ .

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

**Ý nghĩa:**

$H(A/B)$  là lượng thông tin tổn 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. Đề 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

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

$H_2(\text{Anh}) = 3,32$  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 hiểu biết nào 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 cố bất kỳ (hai nguồn tin bất kỳ) thì entropie của trường biến cố 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).

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

$$\text{Xét hiệu: } H(A/B) - H(A) = G$$

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

**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.

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

**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  $I(A, B)$ ):

$$I(A, B) = M^{\Delta} [I(a_i, b_j)] \quad (3.28)$$

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

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

$$\text{Tóm lại: } I(A, B) = H(A) - H(A/B) \quad (3.29a)$$

$$\text{Tương tự, ta có: } I(A, B) = H(B) - H(B/A) \quad (3.29b)$$

$$\text{Hay: } I(A, B) = H(A) + H(B) - H(A.B)$$

$I(A, B)$  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 tổn hao một phần. Lượng thông tin tổn hao trung bình chính là  $H(A/B)$ .

### 3.3.6.3. Tính chất 3

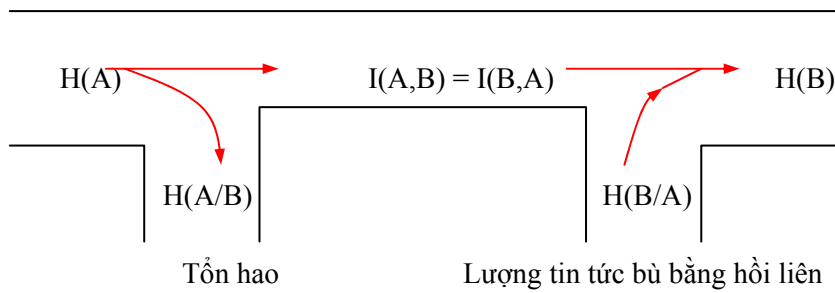
$$I(A,A) = H(A)$$

### 3.3.6.4. Tính chất 4

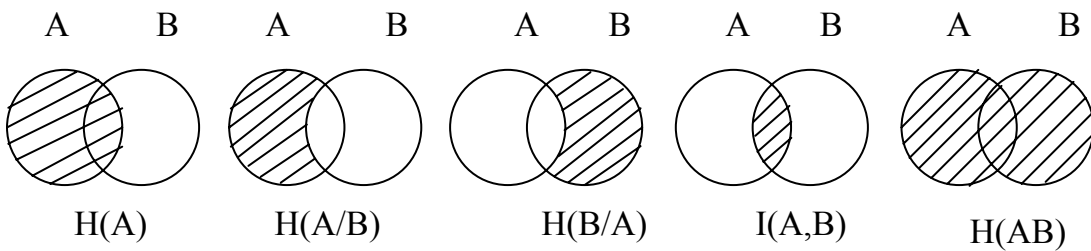
$$I(A,B) = I(B,A)$$

### 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. Lược đồ Wenn mô tả mối quan hệ giữa các đại lượng.

### 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:

$$\nu_n = \frac{\Delta}{T_n} \quad (3.32)$$

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

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

**Ví dụ:** Điện báo tay:  $\nu_n = 25 \text{ bột}$ .

Điện báo tự động:  $\nu_n = (50 \div 300) \text{ bột}$ .

Thông tin truyền số liệu:  $(500 \div n \cdot 10^4) \text{ bột}$ .

#### 3.4.2. Khả năng phát của nguồn rời rạc

**Định nghĩa:**

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

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 bột thì khả năng tối đa của máy là:

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

#### 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:**

Độ 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 đầu lối vào và trường đầu lối ra của kênh.
- Xác suất chuyển  $p(b_j/a_i)$
- Tốc độ truyền tin của kênh  $\upsilon_K$

**Định nghĩa 1:**

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

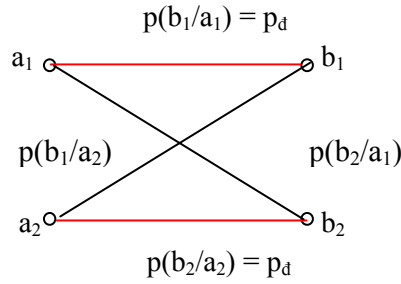
**Định nghĩa 2:**

Nếu một kênh có xác suất chuyển:

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

thì kênh đó sẽ được gọi là kênh đối xứng.

**Ví dụ:**



$\forall$  xác suất sai bằng nhau,  $\forall$  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:**

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

Trong đó:  $\nu_K = \frac{1}{T_K}$ ,  $T_K$ : thời gian trung bình để truyền một dấu qua kênh.  $\nu_K$  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 tải tin 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  $p(a_i)$ ,  $\forall a_i \in A$ ).

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

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

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:**

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

### 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

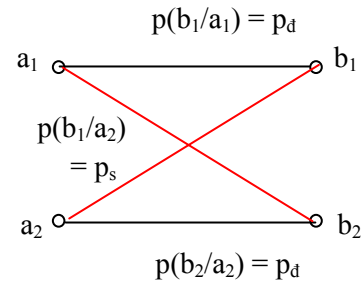
Ta có một kênh nhị phân như hình 3.4. Trong đó:

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:

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

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

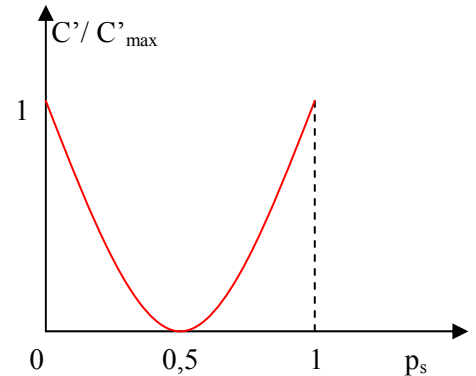
$$C' = f(p_s, T_K)$$

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

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

(3.38)

Đồ thị (3.38) biểu diễn trên hình 3.5.



Hình 3.5.

### 3.4.8. Định lý mã hoá 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 hoá và giải mã sao cho việc truyền tin có xác suất gặp lỗi bé tùy ý (nếu  $H'(A) > C'$  thì không tồn tại phép mã hoá 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 đầu  $a_1$  và  $a_2$  như hình vẽ. Các đầu  $a_1$  và  $a_2$  có cùng thời hạn T. Hãy tính khả năng thông qua  $C'$  của kênh này với điều kiện:

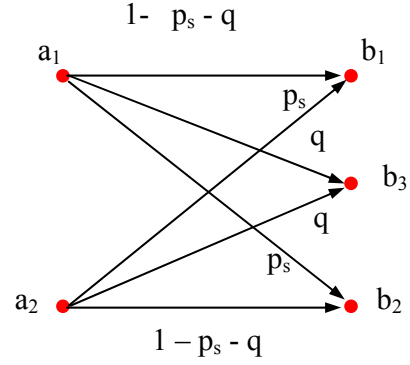
Xác suất xoá:  $p(b_3/a_i) = q$

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:

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

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:

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

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

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

Trong đó  $F = \frac{1}{T}$

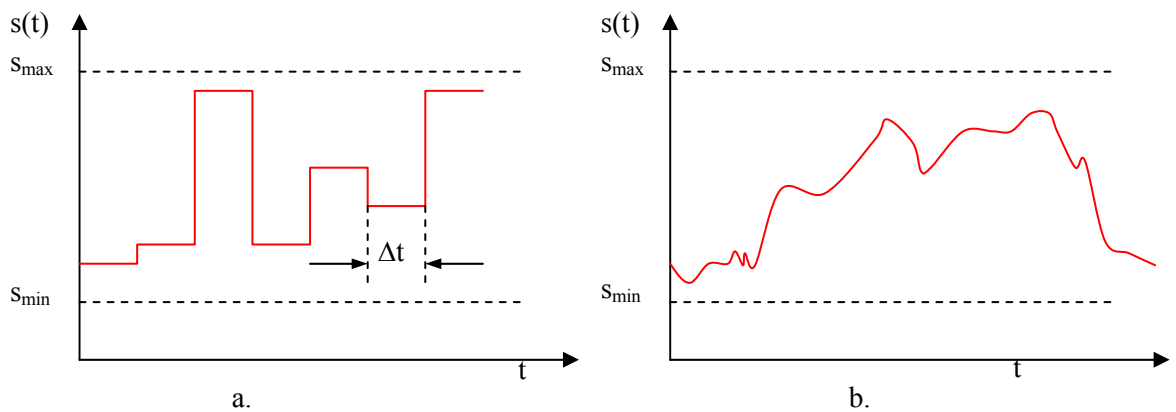
### 3.5. ENTROPIE CỦA NGUỒN LIÊN TỤC. LƯỢNG THÔNG TIN CHÉO TRUNG BÌNH TRUYỀN QUA KÊNH LIÊN TỤC KHÔNG NHỚ

#### 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.

- Tín hiệu liên tục với thời gian rời rạc (hình 3.6a).
- Tín 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 phổ trung bình
- Bề rộng phổ

#### 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 đầu lỗi vào trước hay sau bộ mã hoá: A



- Trường đầu lối ra sau bộ giải điều chế hoặc sau bộ giải mã B.

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

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

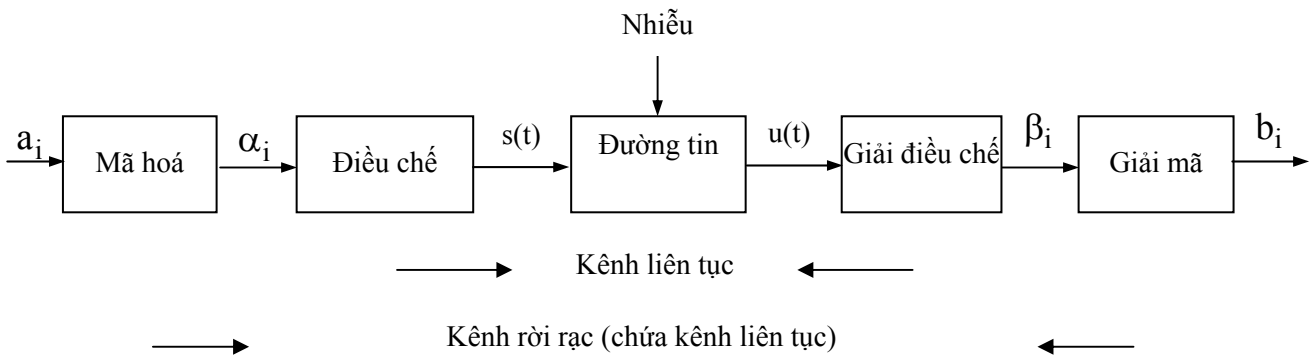
- Trường đầu lối vào (sau bộ điều chế):  $\{s(t)\}$

- Trường đầu lối 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 lối vào và tập tin lối ra liên hệ với nhau theo công thức:

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

Trong đó  $\mu = \text{const}$ ,  $(\neq t)$ ,  $n(t)$ : nhiễu cộng là tạp 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

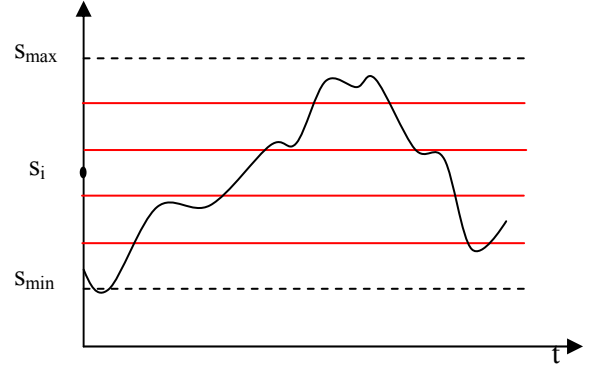
kênh trong một đơn vị thời gian). Như vậy, khả năng thông qua của kênh liên tục đúng bằng khả năng thông qua của kênh rời rạc. Tuy nhiên phép giải điều chế thường làm tổn hao thông tin, do đó khả năng thông qua của kênh rời rạc không thể lớn hơn khả năng thông qua của kênh liên tục nằm trong nó.

### 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  $\Delta S$  và được gọi là bước lượng tử (hình 3.7).



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:

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

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

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

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

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

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

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 thống kê của nguồn (tín hiệu) mà chỉ có số hạng thứ nhất phụ thuộc vào bản chất thống 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  $\nu$  lần:  $s^* = \nu \cdot s$ , khi đó:

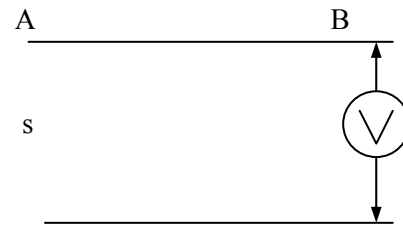
$$W_1(s^*) = W_1(s) \left| \frac{ds}{ds^*} \right| = \frac{1}{\nu} W_1(s)$$

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

$h(S)$  cũng có tính chất cộng tính.

### 3.5.5. 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 tổn hao, không gây nhiễu. ở đầu B ta đặt một máy thu là một volt kế lý tưởng (có tạp âm nội bộ bằng không, nên có thể đo với độ chính xác tùy ý,  $Z_V = \infty$ ). Tín hiệu phát nằm trong khoảng  $(0 \div 1)$  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 hoá một cách đơn giản bằng cách đối 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 đối chứng:

$$a_1 \leftrightarrow 0,01V, a_2 \leftrightarrow 0,02V, \dots, a_{100} \leftrightarrow 1V$$

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

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

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

Trong thực tế, luôn tồn tại nhiễu  $n(t)$  trên đường dây và volt kế luôn có tạp âm nội bộ. Do đó không thể chọn  $\Delta s$  nhỏ tùy 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 cũng 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 hoá các tin ở đầu thu và đầu phát. Bước lượng tử ở đầu phát là  $\Delta s$ , bước lượng tử ở đầu thu là  $\Delta u$ . 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:

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

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

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:

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

Chú ý rằng theo công thức nhân xác suất:

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

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

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:  $W_2(s, u) = W_1(u) \cdot W_1(s/u)$

$h(S/U)$  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 chứa trong mỗi dấu của  $A$ .

$H(A/B)$  là lượng thông tin tổn 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: 
$$h(N) = \int_{-\infty}^{\infty} W(n) \log \left( \sqrt{2\pi P_n} e^{\frac{n^2}{2P_n}} \right) dn$$

$$\begin{aligned} h(N) &= \int_{-\infty}^{\infty} W(n) \cdot \log \sqrt{2\pi P_n} \cdot dn + \int_{-\infty}^{\infty} W(n) \cdot \log e^{\frac{n^2}{2P_n}} \cdot dn \\ &= \log \sqrt{2\pi P_n} \int_{-\infty}^{\infty} \underbrace{W(n) \cdot dn}_{=1} + \frac{\log e}{2P_n} \int_{-\infty}^{\infty} \underbrace{n^2 \cdot W(n) \cdot dn}_{=D[n] = P_n} \end{aligned}$$

$$\Rightarrow h(N) = \log \sqrt{2\pi P_n} + \frac{1}{2} \log e$$

$$\Rightarrow h(N) = \log \sqrt{2\pi P_n} \cdot e \quad (3.46)$$

### 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:

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

$$\begin{aligned} h(U/S) &= - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_2(s, u) \cdot \log W_1(u/s) \cdot du \cdot ds \\ h(U/S) &= - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W_1(s) \cdot W_1(u/s) \cdot \log W_1(u/s) \cdot du \cdot ds \\ &= - \int_{-\infty}^{\infty} W_1(s) \cdot ds \int_{-\infty}^{\infty} W_1(u/s) \cdot \log W_1(u/s) \cdot du \\ h(U/S) &= - \int_{-\infty}^{\infty} W_1(u/s) \cdot \log W_1(u/s) \cdot du \quad (3.47) \end{aligned}$$

Để xác định  $h(U/S)$  ta phải tính được  $W_1(u/s)$ .

Vì yếu tố ngẫu nhiên chỉ do nhiễu 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  $dn$ .

$$p\left\{u \in \frac{du}{s}\right\} = p\{n \in dn\}$$

$$W_1(u/s)du = W_1(n)dn$$

$$\Rightarrow W_1(u/s) = W_1(n) \frac{dn}{du} = W_1(n) \frac{1}{\frac{du}{dn}}$$

$$\text{Với } \frac{du}{dn} = \frac{d}{dn}(s + n) = \frac{ds}{dn} + \frac{dn}{dn} = 1 \left( \text{Vì } \frac{ds}{dn} = 0 \text{ khi } s, n \text{ độc lập} \right)$$

$$\text{Vậy } W_1(u/s) = W_1(n) = \frac{1}{\sqrt{2\pi P_n}} \exp\left\{-\frac{n^2}{2P_n}\right\}$$

$$\Rightarrow h(U/S) = h(n) = \log \sqrt{2\pi e P_n}$$

$$\Rightarrow I(U, S) = \int_{-\infty}^{\infty} W_1(u) \cdot \log \frac{1}{W_1(u)} \cdot du - \log \sqrt{2\pi e P_n} \quad (3.48)$$

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:  $I(S, U) = h(U) - h(U/S)$

$$I(S, U) = \log \sqrt{1 + \frac{P_s}{P_n}} = \frac{1}{2} \log \left( 1 + \frac{P_s}{P_n} \right) \quad (3.49)$$

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 ( $\sigma^2$ ), tín hiệu có phân bố Gausse sẽ cho entropie vì phân lớn nhất. Tức là:

$$h(X) = - \int_{-\infty}^{\infty} W_1(x) \cdot \log W_1(x) \cdot dx \leq \log \sqrt{2\pi e \sigma^2}$$

$$\max h(X) = \log \sqrt{2\pi e \sigma^2} \text{ khi } W_1(x) - \text{mật độ chuẩn}$$

**Chứng minh:**

Gọi  $x(t)$  là tín hiệu không Gausse.

$$\tilde{x}(t) \text{ là tín hiệu Gause: } W_1\left(\tilde{x}\right) = \frac{1}{\sqrt{2\pi P_{\tilde{x}}}} \exp\left\{-\frac{\tilde{x}^2}{2P_{\tilde{x}}}\right\}$$

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:

$$D_{\tilde{x}} = D_x = D$$

$$\Rightarrow \int_{-\infty}^{\infty} \tilde{x}^2 W_1\left(\tilde{x}\right) d\tilde{x} = \int_{-\infty}^{\infty} x^2 W_1(x) dx \quad (a)$$

Ta có:

$$\begin{aligned} h\left(\tilde{X}\right) &= - \int_{-\infty}^{\infty} W_1\left(\tilde{x}\right) \log W_1\left(\tilde{x}\right) d\tilde{x} = \\ &= \log \sqrt{2\pi D} \int_{-\infty}^{\infty} W_1\left(\tilde{x}\right) d\tilde{x} + \frac{\log e}{2D} \int_{-\infty}^{\infty} x^2 W_1(x) dx \end{aligned}$$

$$\left( \text{do } \int_{-\infty}^{\infty} W_1\left(\tilde{x}\right) d\tilde{x} = \int_{-\infty}^{\infty} W_1(x) dx = 1 \text{ và do (a)} \right)$$

$$\begin{aligned}\Rightarrow h(\tilde{X}) &= - \int_{-\infty}^{\infty} \left[ -\frac{1}{2} \log 2\pi D - \frac{x^2}{2D} \log e \right] W_1(x) dx \\ &= - \int_{-\infty}^{\infty} W_1(x) \log W_1(\tilde{x}) dx\end{aligned}$$

Từ (\*)  $\Rightarrow$  cần chứng minh:  $h(X) - h(\tilde{X}) \leq 0$

Ta có:

$$\begin{aligned}h(X) - h(\tilde{X}) &= - \int_{-\infty}^{\infty} W_1(x) \log W_1(x) dx + \int_{-\infty}^{\infty} W_1(x) \log W_1(\tilde{x}) dx \\ &= \int_{-\infty}^{\infty} W_1(x) \log \frac{W_1(\tilde{x})}{W_1(x)} dx \quad (**)\end{aligned}$$

Với  $a > 1$  bao giờ ta cũng có:  $\log_a x \leq x - 1$ .

Nên:

$$\begin{aligned}h(X) - h(\tilde{X}) &\leq \int_{-\infty}^{\infty} W_1(x) \left[ \frac{W_1(\tilde{x})}{W_1(x)} - 1 \right] dx \\ &\leq \int_{-\infty}^{\infty} W_1(\tilde{x}) dx - \int_{-\infty}^{\infty} W_1(x) dx\end{aligned}$$

$$\text{Vậy } h(X) - h(\tilde{X}) \leq 0 \Leftrightarrow h(X) \leq h(\tilde{X}) \quad \forall x \neq \tilde{x}$$

$$\max h(X) = h(\tilde{X}) = \log \sqrt{2\pi e D}$$

**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. (vì 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 thống kê người ta thường xét tập chuẩn.

Bằng 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

lượng ngẫu nhiên phân bố đều có entropie lớn nhất.  $H(X) = \log(b-a) = \log \sigma 2\sqrt{3}$

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

**Định 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  $\Delta t$ . Dem 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:

$$\nu_K = 1/\Delta t$$

Tương tự như đối với kênh rời rạc, khả năng thông qua của kênh Gausse với thời gian rời rạc sẽ là:

$$C' = \nu_K \cdot \max I(U,S) \quad (3.50)$$

$I(U,S)$  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:  $u = \mu_s + n$

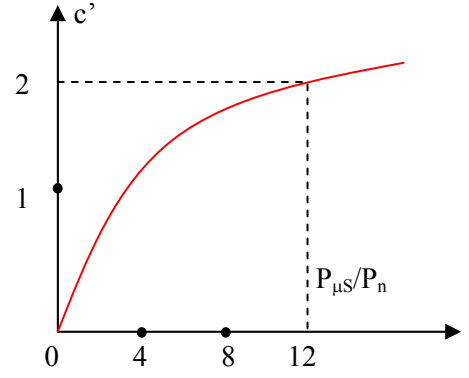
Do  $s$  và  $n$  độc lập nên:  $P_u = P_{\mu_s} + P_n$

Vậy:

$$C' = \nu_K \left[ \log \sqrt{2\pi e(P_{\mu_s} + P_n)} - \log \sqrt{2\pi e P_n} \right]$$

$$\Rightarrow C' = \nu_K \log \sqrt{\frac{P_{\mu_s} + P_n}{P_n}}$$

$$\Rightarrow C' = \frac{1}{2} \nu_K \log \left( 1 + \frac{P_{\mu_s}}{P_n} \right) \quad (3.51)$$



Hình 3.9.

Trong đó  $P_{\mu_s}/P_n$  là tỷ số tín trên tạp 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 đứt.

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  $C' \sim \nu_K$ ).

### 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 phổ 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 méo 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:  $\nu_K = \frac{1}{\Delta t} = 2F$ . Do đó theo (3.51), ta có:

$$C' = F \log \left( 1 + \frac{P_{\mu s}}{P_n} \right) \quad (3.52)$$

Trong đó: F là bề rộng phổ của tín hiệu

$P_n$  là công suất trung bình của nhiễu trong dải F

Với tạp 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 trả giá, ta được lợi về mặt này thì phải chịu thiệt ở mặt khác.

Ta vẫn có thể thu chính xác được tín hiệu (đảm 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 tạp,...)

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 dải tần vô hạn

Trong (3.52'), nếu lấy cơ số của log là e thì  $C'$  được đo bằng [nat/s]. Nếu đo bằng [bit/s] thì:

$$C' = 1,443 F \ln \left( 1 + \frac{P_{\mu s}}{N_0} \cdot \frac{1}{F} \right) \quad [\text{bit/s}] \quad (3.53)$$

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 dải 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  $x \rightarrow 0$  thì  $F \rightarrow \infty$ .

Ta ký hiệu:  $C'_\infty = \lim_{F \rightarrow \infty} C' = \lim_{x \rightarrow 0} \left[ \frac{P_{\mu s}}{N_0} \cdot \frac{1}{x} \cdot \ln(1+x) \right] \cdot 1,443$

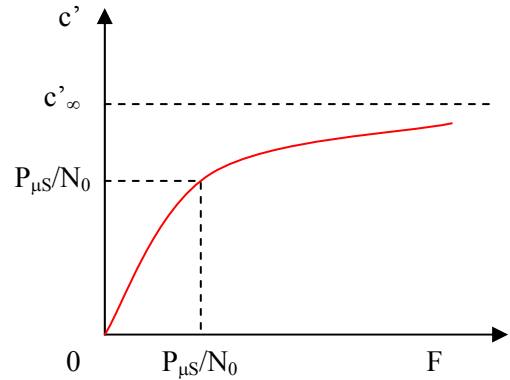
$$\Rightarrow C'_\infty = 1,443 \cdot \frac{P_{\mu s}}{N_0} \cdot \lim_{x \rightarrow 0} \left[ \frac{1}{x} \cdot \ln(1+x) \right]$$

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.

Tại giá trị  $F = \frac{P_{\mu s}}{N_0} \Rightarrow C = F = \frac{P_{\mu s}}{N_0}$ .



Hình 3.10.

Từ đồ thị, ta thấy: Khả năng thông qua của kênh Gausse với thời gian liên tục là một đại lượng giới nội:  $0 \leq C' \leq C'_\infty$ . Điều này được giải thích như sau: Trong thực tế, mọi vật đều có tạp âm nhiệt. Tạp 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,  $k = 1,38 \cdot 10^{-23}$  J/độ.

$T^0$  là nhiệt độ tuyệt đối của vật.

Vì vậy khả năng thông qua của mọi kênh thực tế đều bị giới nội.

### 3.7.4. Định lý mã hoá thứ hai của Shannon đối với kênh liên tục

Đối với kênh liên tục, định lý mã hoá thứ hai của Shannon được phát biểu như sau:

**Định lý:**

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

### 3.7.5. Ví dụ: Khả năng thông qua của một số kênh thực tế

- Kênh viễn thông chuyển tiếp:

$$C' = \left( n \cdot 10^6 \div n \cdot 10^7 \right) \text{ Hartley/s}$$

- Điện thoại, điện báo ảnh, viễn thông chuyển tiếp:

$$C' = (n \cdot 10^3 \div n \cdot 10^4) \text{ Hartley/s}$$

- Điện báo:

$$C' = (n \cdot 10 \div n \cdot 10^2) \text{ Hartley/s}$$

- 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 ( $\approx 2000$  dấu/trang):  $I = (10^3 \div 10^7) \text{ bit.}$

Trí nhớ ngắn hạn của con người:  $(10^2 \div 10^5) \text{ bit.}$

Trung bình một đời người tiếp nhận  $\approx 10^{10} \text{ bit.}$

## 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 chứa 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 hủ 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 nhiễu như hình vẽ. Do có nhiễu nên xác suất thu đúng mỗi tín hiệu giảm đi chỉ bằng  $7/8$ . Hãy tìm:

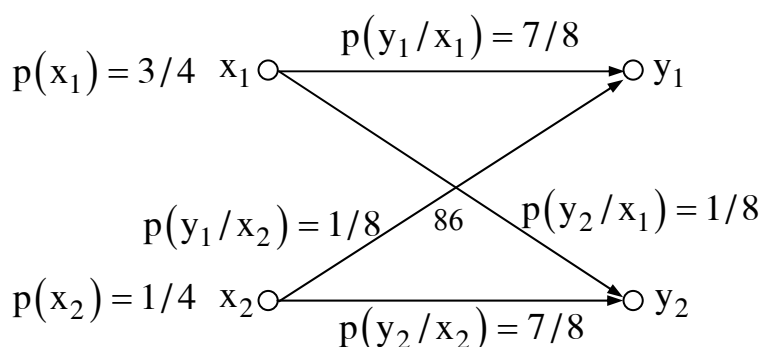
a. Lượng tin tức riêng có điều kiện  $I(x_2/y_2)$

b. Lượng tin tức chéo  $I(x_2, y_2)$

c.

trung

$H(X),$



Các lượng tin tức

trung bình  $I(X, y_2),$

$H(X/Y), I(X, Y)$

**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:

- Khi các con chữ độc lập thống kê với nhau.
- Khi các con chữ phụ thuộc thống kê với nhau.

**3.5.** Một điện đài 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 tiến 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.

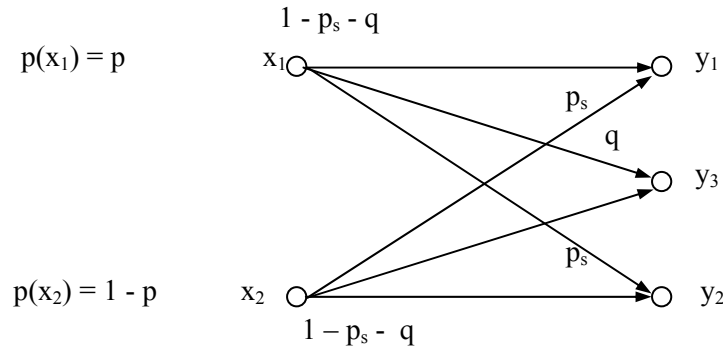
**3.6.** Một điện đài của địch có thể làm việc trên sóng  $\lambda_1$  (sự kiện  $A_1$ ) hoặc ở trên sóng  $\lambda_2$  (sự kiện  $A_2$ ); nó cũng có thể làm việc ở chế độ liên tục (sự kiện  $B_1$ ) cũng như ở chế độ xung (sự kiện  $B_2$ ). Xác suất các sự kiện đồng thời có giá trị như nhau:

$$p(A_1B_1) = 0,15; p(A_1B_2) = 0,7; p(A_2B_1) = 0,1; p(A_2B_2) = 0,05.$$



Hãy tính lượng tin tức về chế độ công tác của điện đài 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  $\tau$  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 lần lượt bằng  $\sigma_s^2$  và  $\sigma_n^2$ . Hãy tính:

- Lượng tin tức  $I(x,y)$  về tín hiệu  $x(t)$  chứa trong tín hiệu thu được  $y(t)$ .
- 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 đen trắng với  $5 \cdot 10^5$  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 truyền hình xem như một dạng tạp âm trắng.

**3.11.** Tìm mật độ phổ 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 phổ 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 tạp âm trắng, chuẩn trong giải tần  $F$  với phương sai  $\sigma^2 = 1 V^2$ , còn kênh thứ hai chịu tác động của một tạp 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 tạp 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. Nêu thuật toán cân.

**3.14.** Trong bộ tứ 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. Nêu thuật toán hỏi? Giả sử A đã rút ra 5 rô, 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 1-1 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 1-1 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  $\alpha_i^7$  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:  $A = \{a_i; \overline{1,s}\}$ .

Xét phép mã hóa  $f$  sau:  $f: a_i \rightarrow \alpha_i^n; \alpha_i^n \in V$ .

Cơ sở 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:

$$D = \frac{H_0(V) - H_0(A)}{H_0(V)} = 1 - \frac{H_0(A)}{H_0(V)} [\%] \quad (4.1)$$

Trong đó:  $H_0(A) = \log s$

$$H_0(V) = \log N = n \log m$$

**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 cấm.

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  $\alpha_i^n$  và  $\alpha_j^n$  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.

**Tính chất 1:**  $d(\alpha_i^n, \alpha_j^n) = d(\alpha_j^n, \alpha_i^n)$

**Tính chất 2:**  $1 \geq d(\alpha_i^n, \alpha_j^n) \geq 0$

**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 chống chế 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  $\alpha_i^n$  và  $\alpha_j^n$  không đồng nhất bằng không (Ta coi  $\alpha_i^n$  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.

**Ví dụ:**  $\alpha_i^7 = 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1$

$$W(\alpha_i^7) = 4$$

Nếu ta coi mỗi từ mã  $\alpha_i^n$  là một vectơ  $n$  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 vectơ tương ứng.

**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 chế 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 gặp phải 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 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 đối với mỗi tin rời rạc là  $p_{scp}$ , khi đó điều kiện sử dụng mã đơn giản trong kênh đối xứng nhị phân không nhớ là:

$$p_s \leq p_{scp}$$

$$\text{Hay } p_0 \ll \frac{p_{scp}}{n} \quad (4.6)$$

## 4.2. MÃ THỐNG KÊ TỐI ƯU

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

$$\text{Ta có } A = \left( \begin{array}{c} a_i \\ p(a_i) \end{array} \right) \xrightarrow{i=1,s} V = \left( \begin{array}{c} \alpha_i^{n_i} \\ p(a_i) \end{array} \right) \quad i = \overline{1,s}$$

**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 bit nào trong biểu diễn của một tin (ký tự) nào đó lại là phần đầu (prefix) của một dãy bit dài hơn biểu diễn cho một tin (ký tự) khác.

**Ví dụ 1:** Mã Moorse 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

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 nhỏ 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:  $\bar{n} = H(A)$

VÀO: Nguồn rời rạc  $A = \left( \begin{matrix} a_i \\ p(a_i) \end{matrix} \right), i = \overline{1, s}$

RA: Từ mã  $\alpha_i^{n_i}$  tương ứng với tin  $a_i$

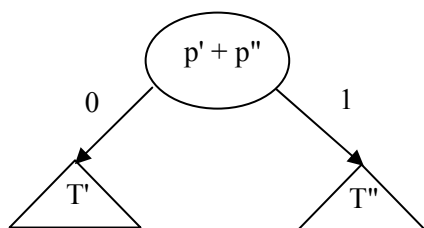
Bước 1: Khởi động một danh sách các cây nhị phân một nút chứa các trọng lượng  $p_1, p_2, \dots, p_n$  cho các tin  $a_1, a_2, \dots, a_n$ .

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 các mũi tên chỉ đến các cây con 0 và 1.

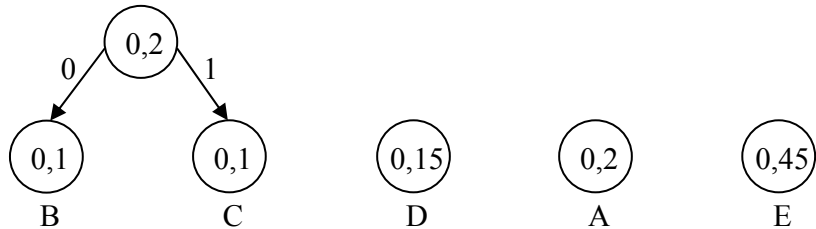


**Bước 3:** Mã số của tin  $a_i$  là dãy các bit được đánh dấu trên đường từ gốc của cây nhị phân cuối cùng tới nút  $a_i$ .

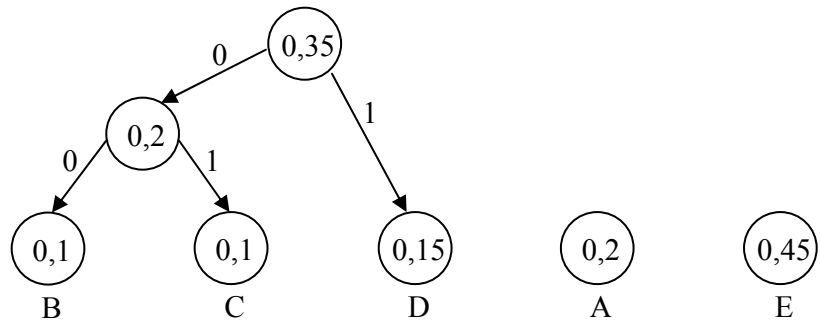
**Ví dụ 1:** Xét các ký tự A, B, C, D, E có các xác suất xuất hiện tương ứng là 0,2; 0,1; 0,1; 0,15; 0,45



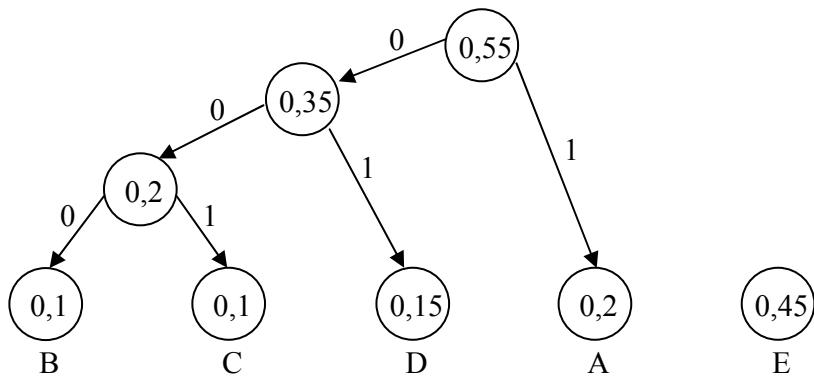
Bước 2: Lần 1:



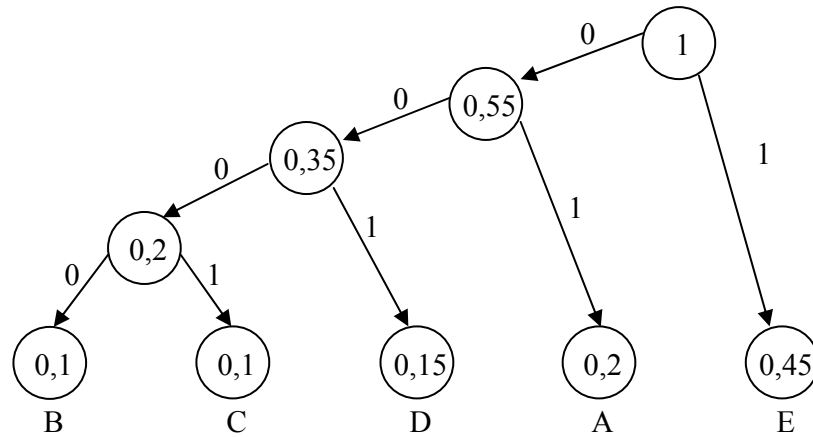
Lần 2:



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:

$$\bar{n} = \sum_{i=1}^s n_i p(a_i) = 2 \cdot 0,2 + 4 \cdot 0,1 + 4 \cdot 0,1 + 3 \cdot 0,15 + 1 \cdot 0,45 = 2,1 \text{ dấu}$$

$$\begin{aligned} H(A) &= \sum_{i=1}^s p(a_i) \log \frac{1}{p(a_i)} = 2 \cdot 0,1 \log 10 + 0,15 \log \frac{100}{15} + 0,2 \log 5 + 0,45 \log \frac{100}{45} \\ &= 0,2 \cdot 3,3226 + 0,15 \cdot 2,7375 + 0,2 \cdot 2,3224 + 0,45 \cdot 1,1522 \\ &= 0,6645 + 0,4106 + 0,4645 + 0,5185 \\ &= 2,058 \text{ bit} \end{aligned}$$

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: Xâu bit

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:

G	0	1	0	0	0	1	1	0	0	1	1	0	1	...
$P \uparrow$	$\downarrow$	$\uparrow$	$\downarrow$	$\uparrow$	$\downarrow$	$\uparrow$	$\downarrow$	$\uparrow$	$\downarrow$	$\uparrow$	$\downarrow$	$\uparrow$	$\downarrow$	$\uparrow$
	A		C	E		D	E		A					

RA: A C E D E A ...

### 4.3. CÁC CẤU TRÚC ĐẠI SỐ VÀ MÃ TUYẾN 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 cấp  $|G|$ .

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 xyclic

Xét nhóm hữu hạn  $\langle G, \bullet \rangle$ . Nếu  $G$  có thể mô tả như sau"

$$G = \{\alpha^i, \forall i\}$$

thì  $G$  được gọi là nhóm cyclic sinh bởi  $\alpha$ .  $\alpha$  được gọi là phần tử sinh (hay phần tử nguyên thủy) của nhóm.

**Ví dụ 2:** Xét nhóm nhân:  $Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$$\begin{array}{ll} \text{Ta có:} & 2^0 = 1 & 2^5 = 10 \\ & 2^1 = 2 & 2^6 = 9 \\ & 2^2 = 4 & 2^7 = 7 \\ & 2^3 = 8 & 2^8 = 3 \\ & 2^4 = 5 & 2^9 = 6 \end{array}$$

Ta có thể viết  $Z_{11}^* = \{2^i \bmod 11\}$ .

Phần tử  $\alpha$  được gọi là có cấp  $k$  nếu  $n$  là số nguyên dương nhỏ nhất thỏa mãn  $\alpha^k \equiv 1 \bmod n$ .

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:  $(a + b) \cdot c = a \cdot c + b \cdot c$

Vành  $R$  được gọi là vành giao hoán nếu ta có  $a \cdot b = b \cdot a$

#### 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 +.
- $c \in R : c \cdot a \in I$

#### 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  $v \leftrightarrow (v_0, v_1, \dots, v_{n-1})$  với  $v_i \in F$

Trong không gian  $V_n$  ta xác định các phép toán sau:

- Cộng vectơ:  $u = (u_0, \dots, u_{n-1})$ ,  $v = (v_0, \dots, v_{n-1})$

$$u + v = (y_0, \dots, y_{n-1}) \text{ với } y_j = u_j + v_j \in F$$

- 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  $\alpha \in F$

$$\alpha \cdot u = (\alpha u_0, \dots, \alpha u_{n-1})$$

### 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 véc tơ và các đa thức trong vành đa thức.

#### 4.3.2.2. Mã tuyến tính

**Định nghĩa 2:** Mã tuyến tính độ dài  $n$  là mã mà từ 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 từ 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  $k$  véc tơ hàng độc lập tuyến tính tạo nên không gian mã  $V_{-(n,k)}$

$2^k$  các véc tơ khác nhau là tất cả các tổ hợp tuyến tính có thể có của  $k$  véc tơ hàng này.

Trong đại số tuyến tính ta biết rằng với mỗi  $G$  sẽ tồn tại ma trận  $H_{r \times n}$  thỏa mãn:

$$G.H^T = 0 \quad (4.8)$$

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  $r$  véc tơ hàng trực giao với các véc tơ hàng của  $G$

Hiển nhiên là nếu  $a$  là một véc tơ mã  $\left( a \in V_{-(n,r)} \right)$  thì :

$$\mathbf{a} \cdot \mathbf{H}^T = 0 \quad (4.9)$$

Ở đây  $\mathbf{H}$  cũng là một ma trận sinh của một mã tuyến tính  $V_{-(n,r)}$  và  $\mathbf{G}$  lại chính là ma trận kiểm tra của mã này. Ta thấy rằng không gian tuyến tính  $\mathbf{C}$  sinh bởi  $\mathbf{G}$  là không gian không của không gian tuyến tính  $\mathbf{C}^\perp$  sinh bởi  $\mathbf{H}$ .

Từ (4.9) ta có thể viết ra  $r$  phương trình:

$$\sum_{j=1}^n a_j h_{ij} = 0, \quad \overline{i=1, r} \quad (4.10)$$

Các phương trình này còn được gọi là các tổng kiểm tra. Mã  $\mathbf{C}$  sinh bởi mã  $\mathbf{G}$  và  $\mathbf{C}^\perp$  sinh bởi  $\mathbf{H}$  được gọi là các mã đối ngẫu.

Nếu  $\mathbf{C} \equiv \mathbf{C}^\perp$  thì  $\mathbf{C}$  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  $\mathbf{a}$  gồm các dấu mã  $a_i$  được chọn như sau:

$$a_0 = x_0$$

$$a_1 = x_1$$

$$a_2 = x_2$$

$$a_3 = x_3$$

$$a_4 = x_0 + x_1 + x_2$$

$$a_5 = x_1 + x_2 + x_3$$

$$a_6 = x_0 + x_1 + x_3$$

Như vậy ma trận sinh  $\mathbf{G}$  có dạng:

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

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 chống 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  $n$  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 tối thiểu  $d_0$  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 sửa  $t$  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 THỨC 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

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

$$\text{Ta có: } a(X) + b(X) = c(X)$$

$$c(X) = \sum_{i=0}^{n-1} c_i x^i$$

$$c_i = a_i + b_i$$

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 véc-tơ trong không gian tuyến tính  $n$  chiều  $V_n$  thì phép cộng đa thức hoàn toàn tương tự như phép cộng véc-tơ.

**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

Đề 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:**  $a(X) = 1 + X + X^4, b(X) = X + X^2$

$$a(X).b(X) = (1 + X + X^4)(X + X^3) \bmod X^7 + 1$$

$$a(X).b(X) = (1 + X^2 + X^5 + X^3 + X^4 + X^7) \bmod X^7 + 1$$

$$a(X).b(X) = 1 + X + X^2 + X^3 + X^4 + X^5$$

Ta thấy rằng tích của hai đa thức được thực hiện trên cơ sở tích của hai đơn thức  $x^i$  và  $x^j$ .

$$x^i . x^j = x^{(i+j) \bmod n} \quad (4.15)$$

**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:

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

Ta thấy biểu diễn véc tơ  $b$  được dịch vòng về phía phải một cấp so với biểu diễn véc tơ  $a$ .

Tương tự ta có:

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

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 véc tơ  $a$ .

**Nhận xét:**

$$\frac{a(X)}{x} = \frac{x^n a(X)}{x} = x^{n-1} a(X)$$

**Ví dụ 3:**

$$\begin{aligned} a(X) &= 1 + x + x^4 \leftrightarrow a = (1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0) \\ b(X) &= x.a(X) = x(1 + x + x^4) = x + x^2 + x^5 \leftrightarrow b = (0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0) \\ d(X) &= \frac{a(X)}{x} = \frac{(1 + x + x^4)}{x} = 1 + x^3 + x^6 \leftrightarrow d = (1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1) \end{aligned}$$

#### 4.4.1.4. Định nghĩa vành đa thức

**Định nghĩa 1:** Tập các đa thức xác định theo (3.11) với hai phép toán cộng đa thức và nhân đa thức theo modulo  $X^n + 1$  tạo nên vành đa thức. Trong trường hợp các hệ số của các đa thức nằm trong  $GF(2)$  ta ký hiệu vành này là  $Z_2[X]/X^n + 1$ .

#### 4.4.2. Ideal của vành đa thức

**Định nghĩa 2:** Ideal  $I$  của vành đa thức gồm tập các đa thức  $a(X)$  là bội của một đa thức  $g(X)$  thỏa mãn:

$$- g(X) \mid X^n + 1 \quad (g(X) \text{ là ước của } X^n + 1)$$

-  $\deg g(X) = r = \min \deg a(X)$  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 bất khả quy.

**Định nghĩa 3:** Đa thức  $a(X)$  được gọi là bất khả quy nếu nó chỉ chia hết cho 1 và cho chính nó.

Như vậy đa thức bất 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 bất khả quy có bậc  $m$  và ước của  $m$ .

**Ví dụ 4:**

-  $m = 2, n = 3$ : chỉ có duy nhất một đa thức bất khả quy bậc 2 là  $x^2 + x + 1$  và một đa thức bất 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 bất khả quy, đó là  $x^3 + x + 1$  và  $x^3 + x^2 + 1$ . Như vậy:

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

-  $m = 4, n = 15$ : Trong số 16 đa thức bậc 4 chỉ có 3 đa thức sau là các đa thức bất 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 bất 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:  $|I| = 2^I - 1$

**Định nghĩa 5:** Đa thức  $g^*(X)$  được gọi là đa thức đối ngẫu của đa thức  $g(X)$  nếu:

$$g^*(X) = X^{\deg g(X)} \cdot g(X^{-1})$$

**Ví dụ 5:** Cho  $g(X) = (1 + X + X^3)$ .

Khi đó đa thức đối ngẫu  $g^*(X)$  của nó là:

$$g^*(X) = X^3 \cdot \left(1 + \frac{1}{X} + \frac{1}{X^3}\right) = X^3 + X^2 + 1$$

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 xyclic

**Định nghĩa 6:** Mã xyclic  $(n, k)$  là Ideal  $I = \langle g(X) \rangle$  của vành 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 xyclic.

**Định nghĩa 7:** Mã xyclic 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 xyclic

**Ví dụ 7:** Tập tất cả các mã xyclic trên vành  $Z_2[x]/X^7 + 1$ . Vành này có tất cả 7 ideal tương ứng với 7 bộ mã xyclic.

$N^o$	$g(X)$	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 xyclic

Vì mã xyclic  $(n, k)$  là một mã tuyến tính nên ta có thể mô tả nó thông qua ma trận sinh  $G$  nên chứa  $k$  vectơ hàng độc lập tuyến tính. Ta có thể thiết lập  $G$  như sau:

$$G = \begin{pmatrix} g(X) \\ x.g(X) \\ \dots \\ x^{k-1}.g(X) \end{pmatrix} \quad (4.1.6)$$

**Ví dụ 8:** Mã xyclic  $(7, 4)$  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 xyclic

Vì  $g(X) \mid X^n + 1$  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  $g(X).h(X) \equiv 0 \pmod{X^n + 1}$  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 vectơ và tích của hai đa thức tương ứng nên ta có thể xây dựng ma trận kiểm tra của mã xyclic sinh bởi  $g(X)$  như sau:

$$H = \begin{pmatrix} h^*(X) \\ x.h^*(X) \\ \vdots \\ x^{r-1}.h^*(X) \end{pmatrix} \quad (4.17)$$

**Ví dụ 9:** Xây dựng ma trận kiểm tra cho mã xyclic (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 xyclic hệ thống

**Định nghĩa:** Mã xyclic (n, k) được gọi là một mã xyclic 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)

$f_0$	$f_1$	$\dots$	$f_{r-1}$	$f_r$	$f_{r+1}$	$\dots$	$f_{n-1}$
-------	-------	---------	-----------	-------	-----------	---------	-----------

$\underbrace{\hspace{15em}}_{r \text{ dấu kiểm tra}}$ 
 $\underbrace{\hspace{15em}}_{k \text{ dấu thông tin}}$

$$f(X) = \sum_{i=0}^{n-1} f_i x^i = x^{n-k}.a(X) + r(X)$$

Ta có: 
$$f(X) : g(X) \Rightarrow f(X) = q(X).g(X) \quad (1.18)$$



$$\Rightarrow \frac{f(X)}{g(X)} = \frac{x^{n-k} \cdot a(X)}{g(X)} + \frac{r(X)}{g(X)}$$

$$\frac{f(X)}{g(X)} = q(X) + \frac{r'(X)}{g(X)} + \frac{r(X)}{g(X)} \quad (1.19)$$

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 xyclic 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 xyclic:  $f_i(x) = a_i(X) \cdot x^{n-k} + r_i(X) \quad (1.20)$

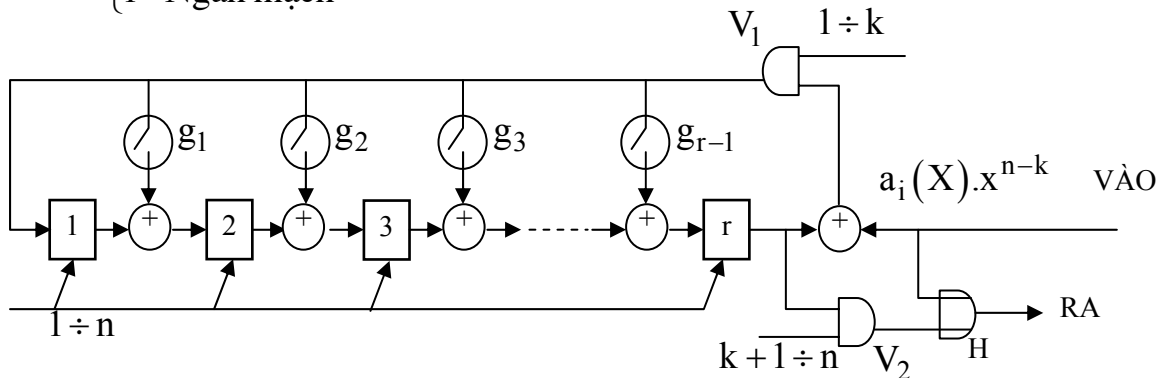
#### 4.5.3. Thiết bị mã hóa

Phần 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

$$4.1): g_i = \begin{cases} 0 & \text{Hở mạch} \\ 1 & \text{Ngắn mạch} \end{cases}$$



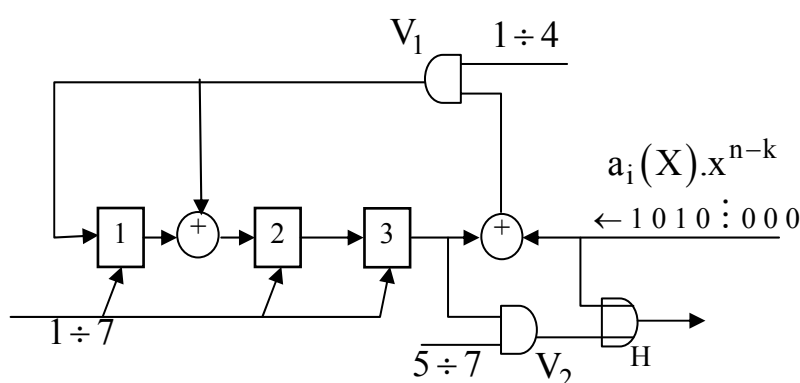
Hình 4.1: Thiết bị mã hóa cho mã xyclic  $(n, k)$  có đa thức sinh  $g(X)$

Hoạt động của thiết bị mã hóa:

- k nhịp đầu: chia và tính phần dư: Mạch và  $V_1$  mở,  $V_2$  đóng, thiết bị hoạt động như một bộ chia để tính dư. Kết thúc nhịp thứ k toàn bộ phần dư nằm trong r ô nhớ từ 1 đến r. Trong quá trình này, các dấu thông tin  $(a_i(X).x^{n-k})$  được đưa ra qua mạch hoặc H.

- r nhịp sau: đưa ra các dấu kiểm tra (phần dư) tới đầu ra. Mạch và  $V_1$  đóng, thiết bị hoạt động như một thanh ghi dịch nối tiếp. Mạch và  $V_2$  mở, các dấu kiểm tra được lần lượt đưa ra từ bậc cao tới bậc thấp. Kết thúc nhịp thứ n, toàn bộ từ mã được đưa ra đầu ra.

**Ví dụ 1:** Thiết bị mã hóa cho mã xyclic (7, 4) có  $g(X) = 1 + X + X^3$



Giả sử đa thức thông tin cần mã:  $a(X) = X^3 + X$

Quá trình hoạt động của thiết bị được mô tả trên bảng sau:

Xung nhịp	Vào	Trạng thái các ô nhớ			Ra
		1	2	3	
1	1	1	1	0	1
2	0	0	1	1	0
3	1	0	0	1	1
4	0	1	1	0	0
5	0	0	1	1	0
6	0	0	0	1	1
7	0	0	0	0	1

**Bảng 1: Quá trình hoạt động của bộ mã hóa.**

Kiểm tra lại:  $a(X).x^{n-k} = (x^3 + x).x^3 = x^6 + x^4$

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

Dư  $r(X) = x + 1$

Từ mã được thiết lập  $f(X) = x^6 + x^4 + x + 1 \leftrightarrow \begin{matrix} X^6 & & & & & & X^0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{matrix}$

#### 4.5.4. Tạo các dấu kiểm tra của mã xyclic

Giả sử  $f(X) \in V$  - mã xyclic  $(n, k)$  có đa thức sinh  $g(X)$ .

Khi đó  $f(X) \div g(X)$  hay  $f(X) = g(X) \cdot q(X) \quad (*)$

Trong đó:  $\deg f(X) \leq n - 1$

$$\deg g(X) = r = n - k$$

$$\deg q(X) \leq n - 1 - r = k - 1$$

Với  $f(X) = \sum_{i=0}^{n-1} f_i x^i$

Gọi  $h(X) = \frac{x^n + 1}{g(X)}$  ta có  $\deg h(X) = k$

Nhân hai vế của (\*) với  $h(X)$  ta có:  $f(X) \cdot h(X) = g(X) \cdot q(X) \cdot h(X)$

Vì  $g(X) \cdot h(X) = x^n + 1$  nên  $f(X) \cdot h(X) = g(X) \cdot x^n + q(X) \quad (**)$

Vì  $\deg g(X) \leq k - 1$  nên trong (\*\*) không chứa các thành phần bậc cao của  $x$  có mũ  $k, k+1, \dots, n-1$ .

Do đó các hệ số tương ứng của các thành phần này trong (\*\*) phải bằng 0. Tức là trong biểu thức:

$$f(X) \cdot h(X) = \left( \sum_{i=0}^{n-1} f_i x^i \right) \cdot \left( \sum_{j=0}^k h_j x^j \right)$$

ta phải có các số hạng có dạng:  $f_i h_j x^{i+j} = 0$  với  $i + j$  thỏa mãn:  $k \leq i + j \leq n - 1$  hay  $k - j \leq i \leq n - 1 - j$ .

Khi  $j$  chạy từ 0 đến  $k$  thì:  $n - r - j \leq i \leq n - 1 - j$ .

Như vậy ta có:

$$\sum_{j=0}^k h_j f_{n-j-i} = 0 \quad , \quad 1 \leq i \leq n - k \quad \left( \begin{smallmatrix} * \\ ** \end{smallmatrix} \right)$$

Hiển nhiên là ta luôn có:  $h_0 = h_k = 1$ .

$$\text{Từ } \left( \begin{smallmatrix} * \\ ** \end{smallmatrix} \right): f_{n-k-i} = \sum_{j=0}^{k-1} h_j f_{n-j-i} \quad , \quad 1 \leq i \leq n - k \quad \left( \begin{smallmatrix} * \\ ** \end{smallmatrix} \right)$$

$\left( \begin{smallmatrix} * \\ ** \end{smallmatrix} \right)$  là phương trình tạo các dấu kiểm tra. Ta có thể dùng nó để tạo các dấu kiểm tra trong các chương trình mã hóa và giải mã.

**Ví dụ 2:** Cho mã xyclic  $(7, 4)$  có  $g(X) = 1 + X + X^3$

$$\text{Ta có: } h(X) = \frac{x^7 + 1}{x^3 + x + 1} = x^4 + x^2 + x + 1.$$

Vậy  $h_0 = h_1 = h_2 = h_4 = 1, h_3 = 0$ .

Từ  $\left( \begin{smallmatrix} * \\ ** \end{smallmatrix} \right)$  ta thấy các dấu kiểm tra của mã này được tạo từ phương trình sau:

$$f_{3-i} = f_{7-i} + f_{6-i} + f_{5-i} \quad , \quad 1 \leq i \leq 3.$$

**Ví dụ 3:**  $a(X) = x^3 + 1$

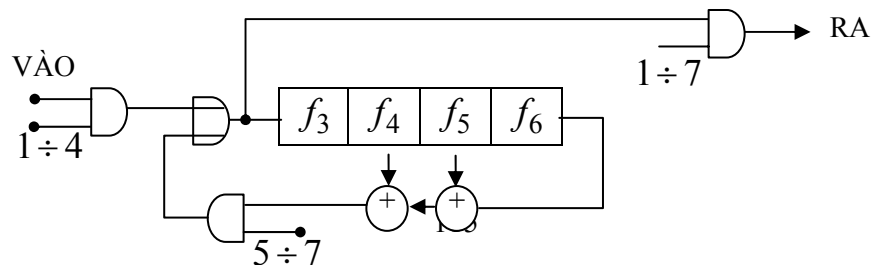
Ta có:  $f_6 = f_3 = 1, f_5 + f_4 = 0$

Khi đó:  $f_2 = f_6 + f_5 + f_4 = 1$

$$f_1 = f_5 + f_4 + f_3 = 1$$

$$f_0 = f_4 + f_3 + f_2 = 0$$

Thiết bị mã hóa xây dựng theo phương trình trên có dạng:



Xung nhip	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.

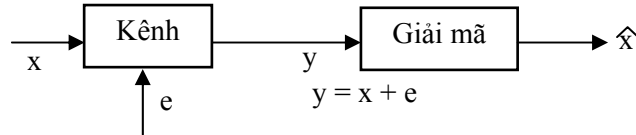
$$(f_0, f_1, \dots, f_{n-1}) \leftrightarrow f(X) = \sum_{i=0}^{n-1} f_i x^i$$

## 4.6. GIẢI MÃ NGUỒN

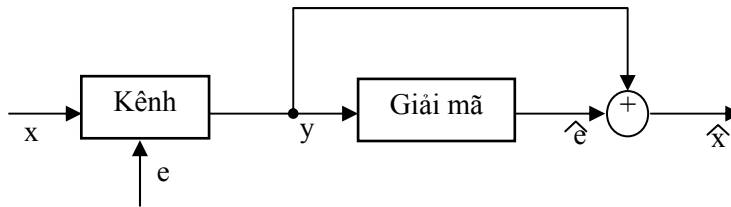
### 4.6.1. Hai thủ tục giải mã

Mọi 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 véc tơ sai từ dãy dấu nhận được.



### 4.6.2. Giải mã theo Syndrom

Giả sử  $v \in V$  - mã xyclic  $(n, k)$  có đa thức sinh  $g(X)$ .

Ma trận sinh của  $V_-(n, k)$  có dạng:

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

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:

$$h^*(X) = x^{\deg h(X)} . h(x^{-1})$$

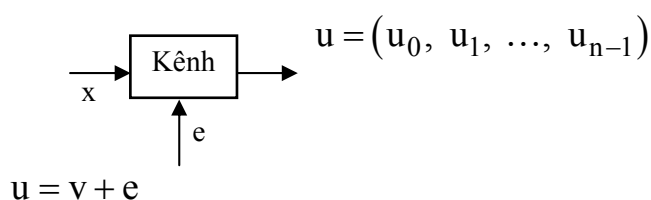
Khi đó ma trận kiểm tra của mã  $V_-(n, k)$  có dạng:

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

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  $S(u) = u.H^T = (v + r).H^T = e.H^T = S(e)$

$S(e)$  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  $u_i$ .
- Dấu 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 dấu mã khác.
- Sai ở một dấu 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 dấu  $u_i$  dựa trên thông tin về giá trị của các tổng kiểm tra bằng phương pháp bỏ phiếu (giải mã ngưỡng theo đa 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 dấu mã.

Xét tổ hợp tuyến tính các dấu 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:

- $\alpha$  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  $\alpha$  bằng phương pháp ngưỡng.
- Để giải mã cho một dấu mã  $U_{i_k}$  cụ thể ta phải sử dụng nhiều bước (nhiều cấp ngưỡng)

#### 4.6.4. Giải mã ngưỡng dựa trên hệ tổng kiểm tra trực giao

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



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

$$h^*(X) = 1 + x^2 + x^3$$

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

$$v.H^T = [S_i]$$

Ta có hệ tổng kiểm tra trực giao với dấu mã  $v_3$

$$S_0 = v_0 + v_2 + v_3$$

$$S_1 = v_1 + v_4 + v_3$$

$$S_2 = v_5 + v_6 + v_3$$

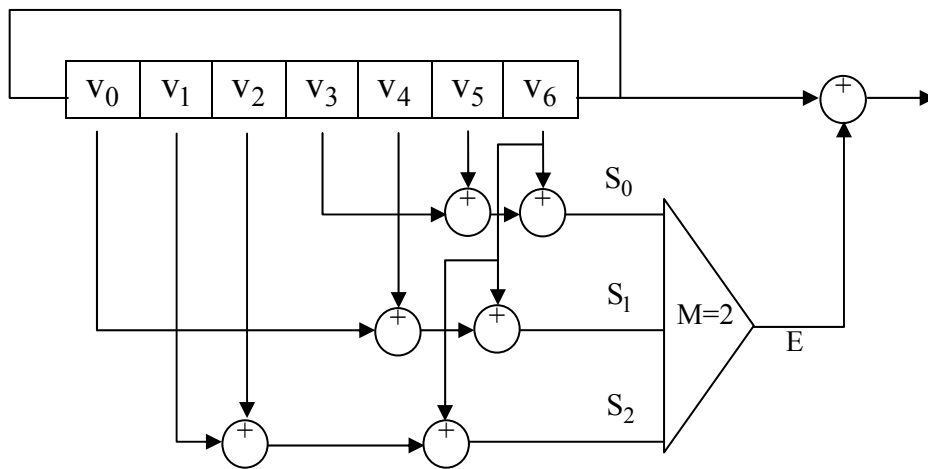
$\Rightarrow$  Hệ tổng kiểm tra với dấu mã  $v_6$  (suy ra bằng cách dịch vòng hệ tổng kiểm tra trên)

$$S_0 = v_6 + v_3 + v_5$$

$$S_1 = v_6 + v_0 + v_4$$

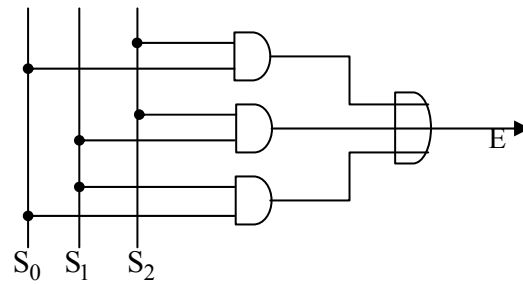
$$S_2 = v_6 + v_1 + v_2$$

Sơ đồ thiết bị giải mã theo thủ tục 2:



Sơ đồ thiết bị ngưỡng  $M = 2$

$$E = S_0S_1 + S_1S_2 + S_2S_3$$



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

$$\text{Hay } v(X) = x^6 + x^5 + x^4 + x^3 + x^2$$

Nhịp	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	1
2	1	1	0	0	1	1	1	1	1	1	1	0
3	1	1	1	0	0	1	1	0	1	0	0	1
4	1	1	1	1	0	0	1	0	0	1	0	1
5	1	1	1	1	1	0	0	0	0	1	0	1
6	0	1	1	1	1	1	0	1	0	0	0	0
7	0	0	1	1	1	1	1	0	1	0	0	0

Từ mã đã giải mã: 0 0 1 1 1 0 1

$$\text{Hay } \hat{v}(X) = x^6 + x^4 + x^3 + x^2$$

Sai ở vị trí  $x^5$  đã được sửa.

Kiểm tra lại:

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

#### 4.6.5. Giải mã ngưỡng dựa 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:  $v.H^T = [S_i]$

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:  $v_6 + v_0$ :

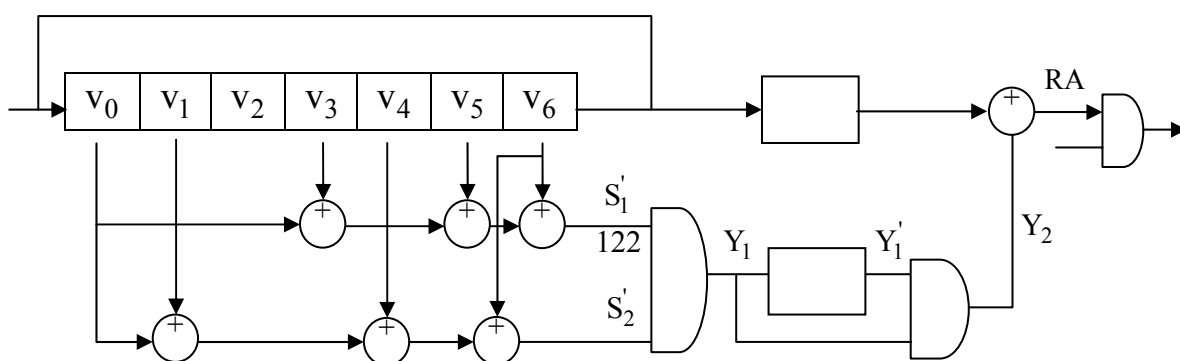
$$S'_1 = v_0 + v_6 + v_5 + v_3$$

$$S'_2 = v_0 + v_6 + v_4 + v_1$$

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 0 1 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 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

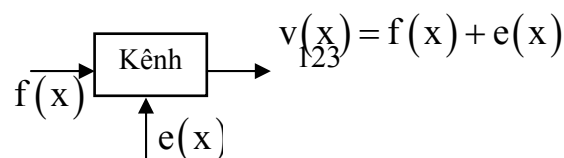
Hay  $\hat{v}(x) = x^6 + x^4 + x^3$

Kiểm tra lại:

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

#### 4.7. GIẢI MÃ THEO THUẬT TOÁN MEGGIT

Giả sử  $f(x)$  là một từ mã của một bộ mã xyclic  $V_-(n, k)$  có đa thức sinh  $g(x)$ . Khi đó  $f(x) : g(x)$ .

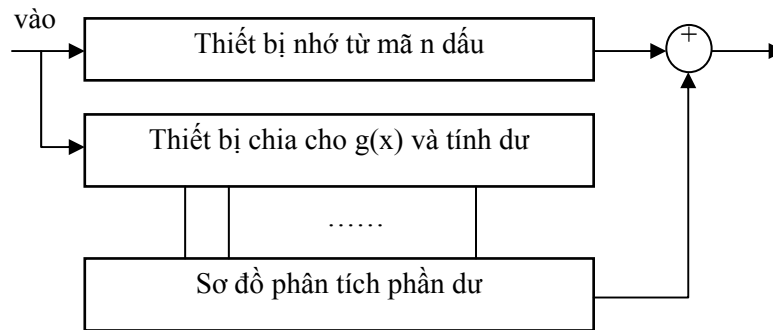


Giả sử  $v(x)$  là từ mã đưa tới đầu vào bộ giải mã, khi đó:

$$\frac{v(x)}{g(x)} = \frac{f(x)}{g(x)} + \frac{e(x)}{g(x)} \quad (4.22)$$

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 xyclic (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):

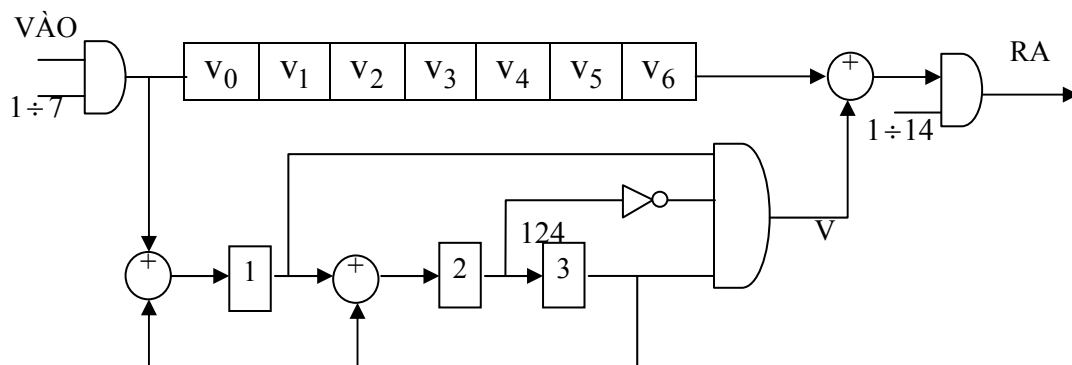
$$\begin{array}{r} x^6 \\ x^4 + x^3 \\ \hline x^3 + x^2 + x \end{array} \left| \begin{array}{l} x^3 + x + 1 \\ x^3 + x + 1 \\ \hline \end{array} \right.$$

$$\text{Phần dư } r(x) = x^2 + 1$$

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 đồng thời đưa tà mã vào bộ ghi dịch đệm, 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	1	0	1	1	0	1
13	0	0	0	0	0	0	0	0	1	1	1	0	1
14	0	0	0	0	0	0	0	0	1	0	1	0	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

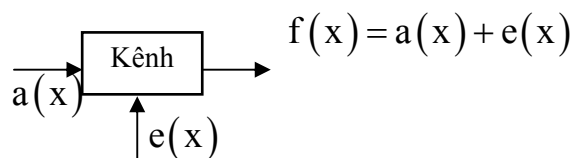
### 4.8.1. Nhiệm vụ của thuật toán giải mã

Ta biết rằng với mã xyclic  $(n, k)$  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:  $a(x) : g(x)$ .

$$\frac{f(x)}{g(x)} = \frac{a(x)}{g(x)} + \frac{e(x)}{g(x)} \quad (4.23)$$

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 (bẫy lỗi)

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  $f(x) \cdot x^i$  (hoặc  $\frac{f(x)}{x^i}$ ) cho  $g(x)$  để tìm phần dư  $r_i(x)$ .

(2) Tính  $w(r_i(x))$ .

- Nếu  $w(r_i(x)) \leq t = \left\lfloor \frac{d_0 - 1}{2} \right\rfloor$  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:

$$\hat{f}(X) = \frac{f(x) \cdot x^i + r_i(x)}{x^i}$$

$$\left( \text{Hoặc } \hat{f}(X) = x^i \left[ \frac{f(x)}{x^i} + r_i(x) \right] \right)$$

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 xyclic (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  $r_0(x)$ .

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

$$(+) \quad w(r_0(x)) = 3 > \left\lceil \frac{4-1}{2} \right\rceil = 1$$

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

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

$$(+) \quad w(r_1(x)) = 1 = t$$

Bước 2: Tìm từ mã đánh giá.

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

Vậy sai ở vị trí  $\alpha$  đã được sửa

## 4.9. GIẢI MÃ LƯỚI.

### 4.9.1. Trạng thái và giản đồ lưới

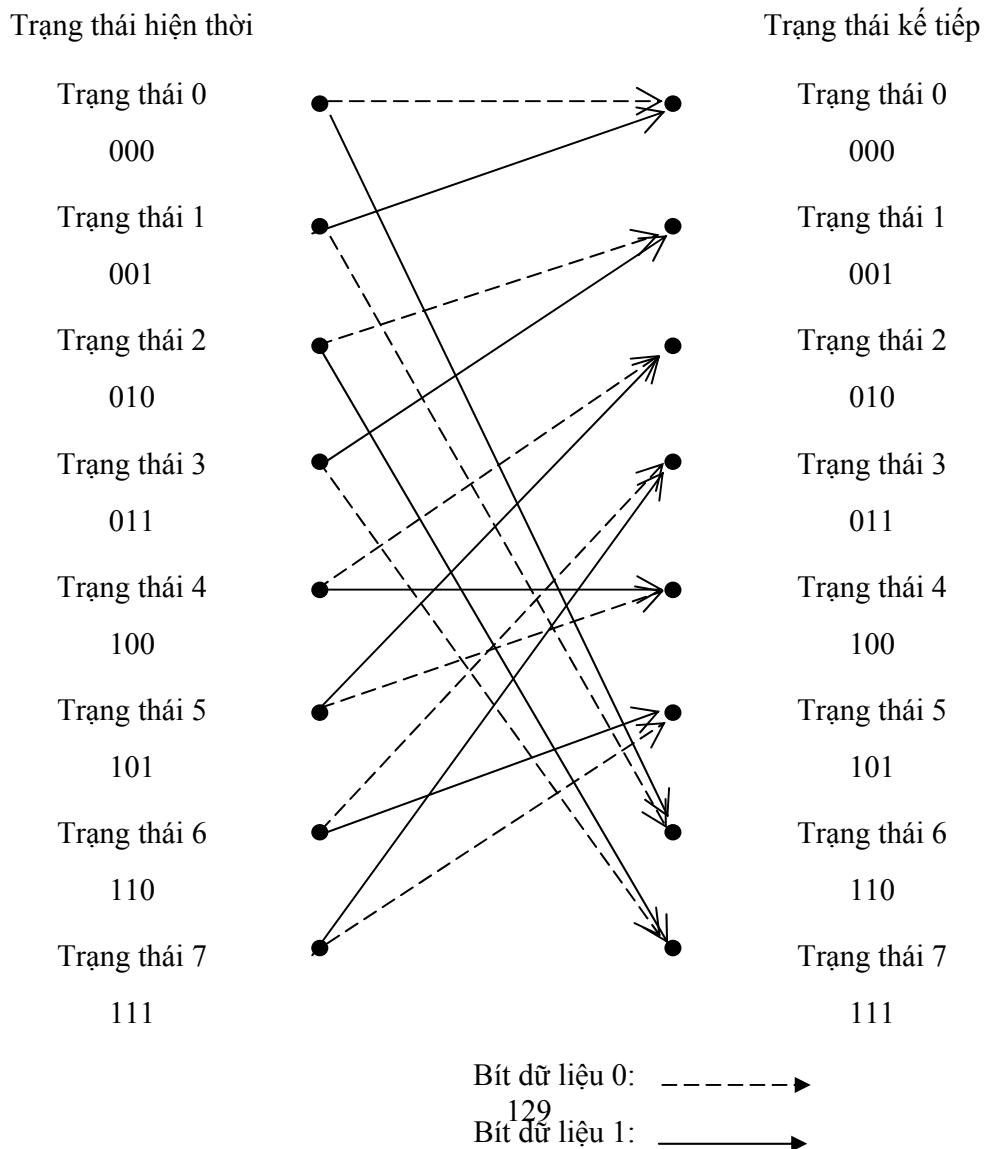
Từ bảng trạng thái của sơ đồ mã hóa ở mục 4.5.3 ta có một số nhận xét sau:

- 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

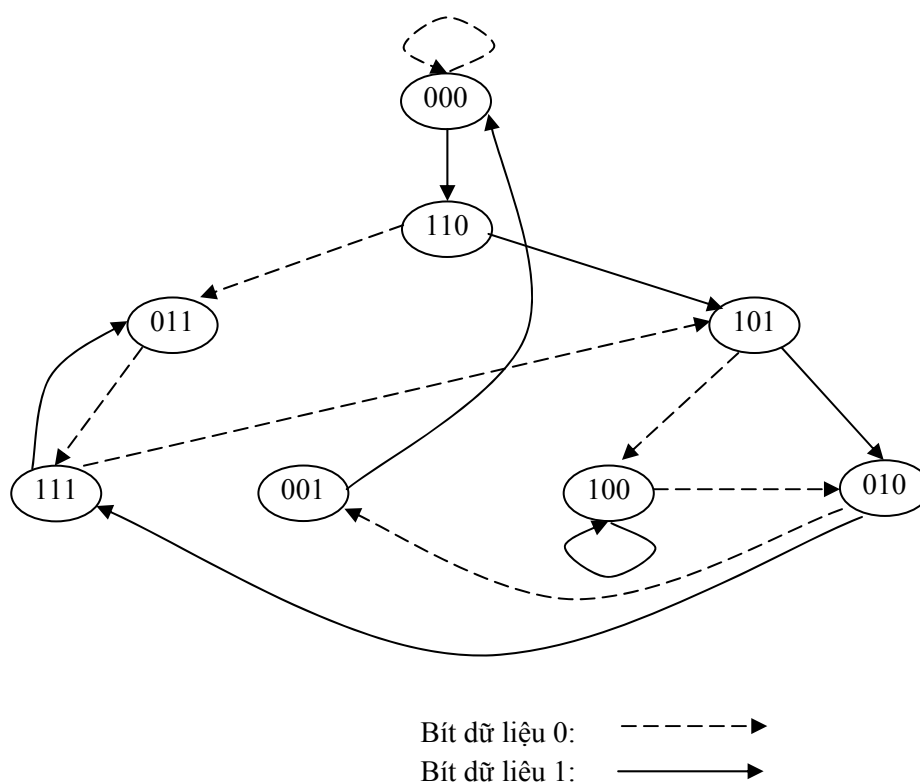
Bằng cách sử dụng biểu đồ trạng thái trên ta có thể mã hóa các bit dữ liệu 1011 mà không dùng thanh ghi dịch trong mục 4.5.2. Bit dữ liệu đầu tiên là logic 1, bởi vậy trạng thái sẽ chuyển từ 000 đến 110 (minh họa bằng đường liền nét từ trạng thái 000). Đầu ra bộ mã hóa lúc này cũng là 1 giống như đầu 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: Giản đồ trạng thái cho mã (7, 4, 3) có 8 trạng thái**

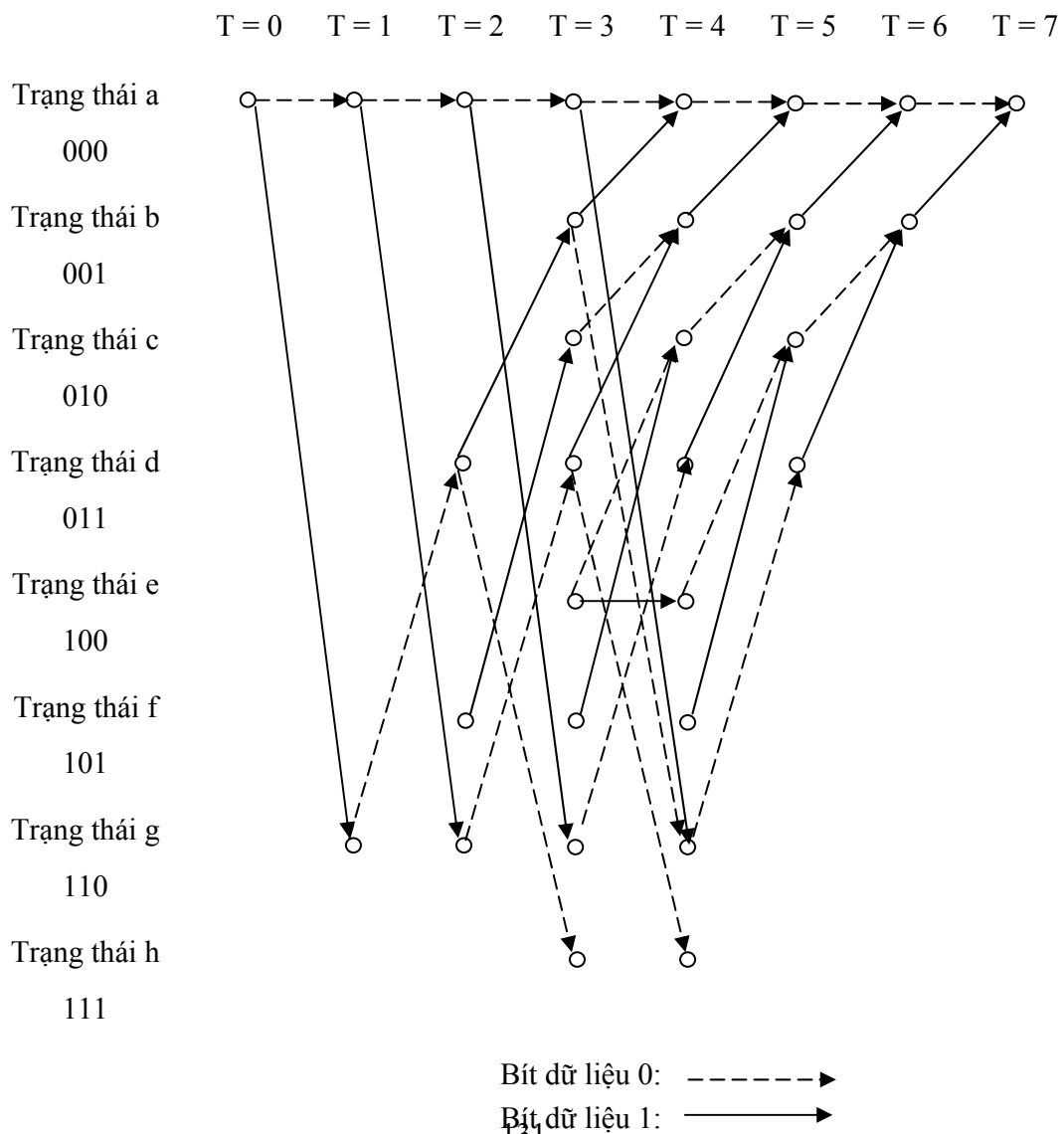
Giản đồ này được tạo nên bằng cách nối các trạng thái kế tiếp của giản đồ chuyển trạng thái ở hình 4.2 bắt đầu từ trạng thái toàn 0.

Giản đồ này minh họa toàn 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 hoặc bằng các đường liền nét hoặc bằng các đường đứt nét tùy theo liệu bít ra của bộ mã hóa là 1 hay 0.

Chỉ 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 bít dữ liệu mới được đưa vào bộ mã hóa.

Khi đưa bít dữ liệu đầu tiên vào bộ mã hóa ( $T = 0$ ), có thể có hai nút khác nhau ở thời điểm tiếp nhau. Bít dữ liệu thứ 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 lưới.

### 4.9.2.1. Mở đầu.

Giải mã lưới 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.

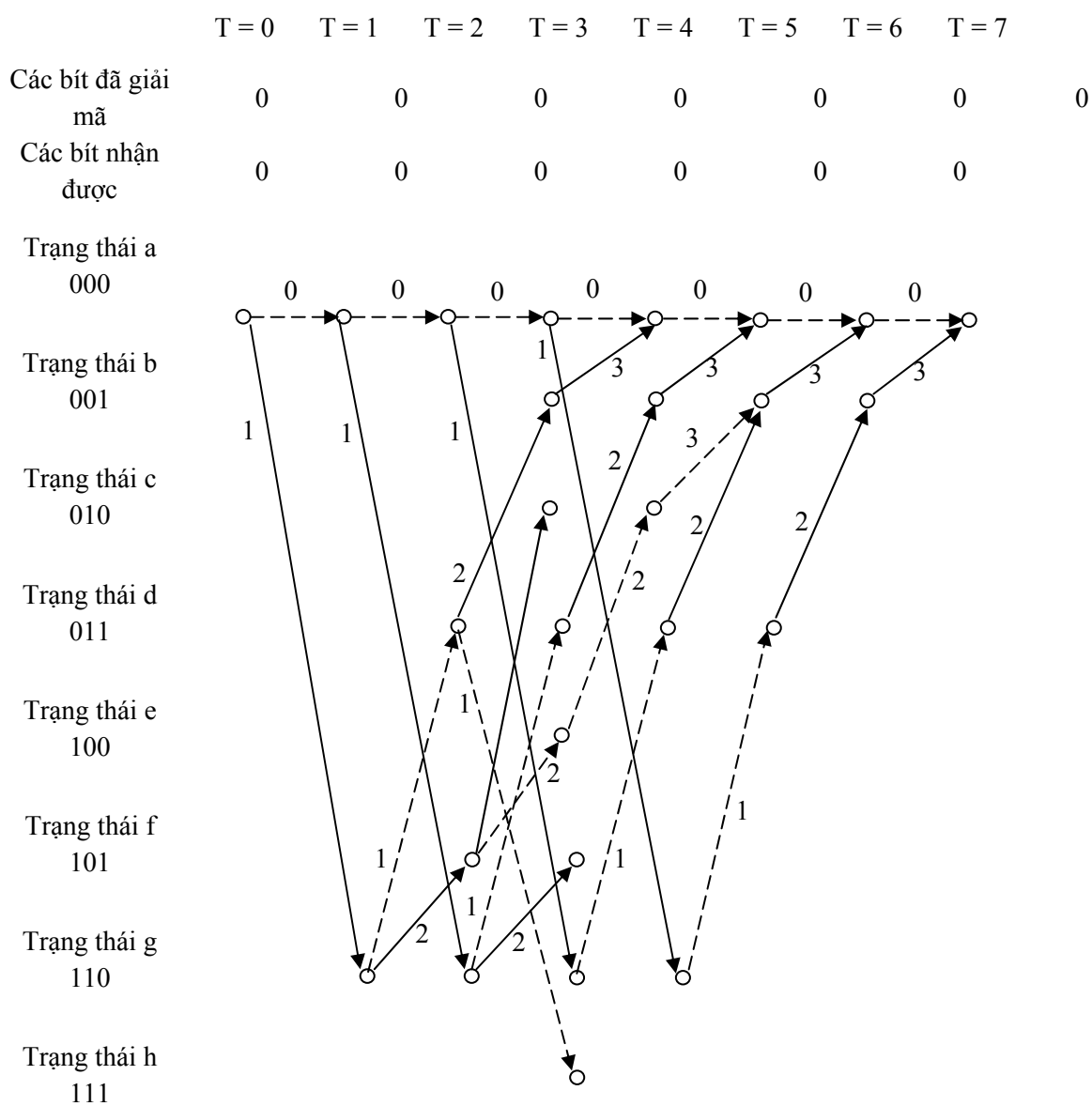
### 4.9.2.2. Thuật toán Viterbi

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 Euclide) từ dãy thu được ở đầu vào các bộ giải mã. Đường dẫn sẽ biểu thị khoảng cách nhỏ nhất từ dãy thu được được chọn là dãy phát hợp lý nhất và các dãy bit thông tin kết hợp được tái tạo lại. Phương pháp này chính là phương pháp đánh giá dãy 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 dãy vào của bộ giải mã chính là dãy đã mã hóa cho dãy 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 tới 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  $a \rightarrow a \rightarrow g \rightarrow f$ .



Ta ký hiệu  $\alpha_1$  và  $\alpha_2$  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 gắn 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  $\alpha_1$  và  $\alpha_2$ . Điều này có nghĩa là độ đo đường dẫn của  $\alpha_2$  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 dãy trạng thái toàn 0) và loại bỏ đường  $\alpha_2$ . Đường  $\alpha_1$  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.

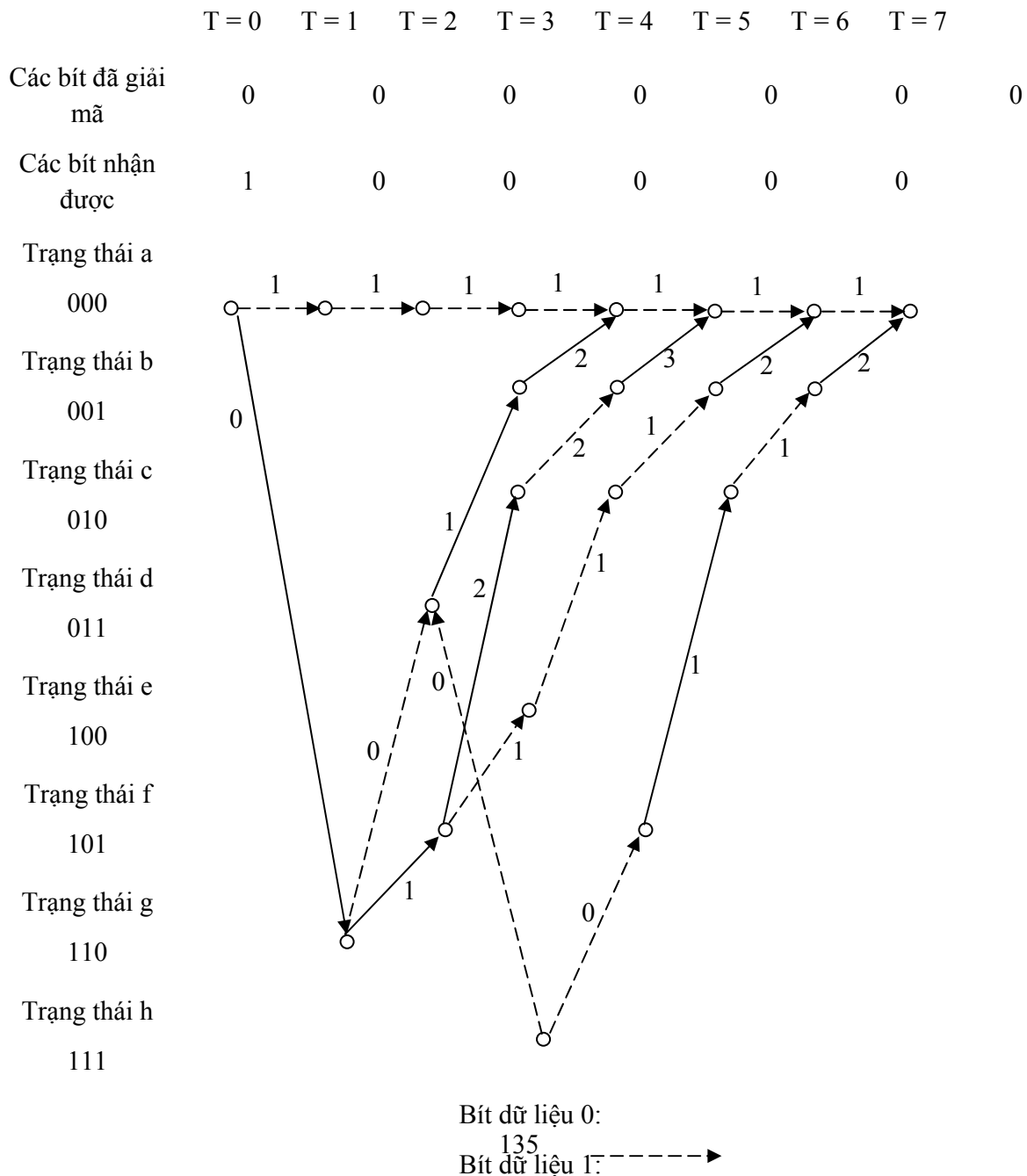
Khi giải mã quyết định cứng, bộ điều chế sẽ cho ra các quyết định cứng (1 hoặc 0) khi tạo lại dãy đã phát. Trong trường hợp này các khoảng cách Hamming giữa các bit nhận được và các bit đã phát được đánh giá trong lưới sẽ được dùng làm độ đo mức tin cậy.

Để minh họa cho quá trình giải mã này ta sử dụng mã (7, 4, 3) với dãy bit phát đi là 0000000. Sai số trên kênh nằm ở bit đầu tiên và dãy 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 dãy được giải mã là xâu.

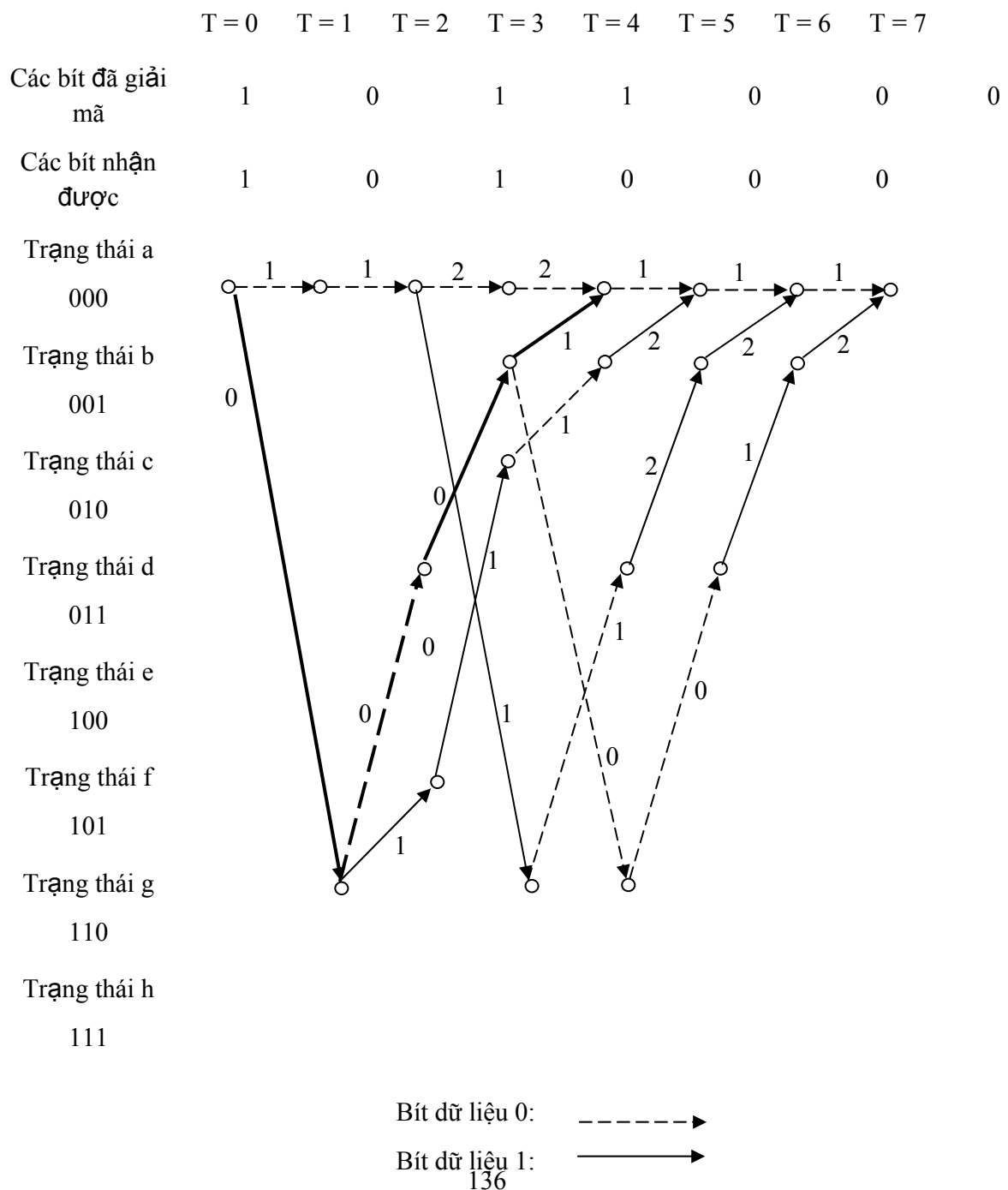
Hình 4.6 minh họa việc lựa chọn đường sống sót (được đánh giá bằng đường đứt nét đậm) của bộ giải mã Viterbi ra sao. Đường này có độ đo đường dẫn nhỏ nhất và sẽ giải mã ra được đúng dãy thu được. Cần chú ý rằng độ đo đường dẫn của đường sống sót tương đương với số sai trong dãy nhận được khi bộ giải 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 đậm nét trên hình 4.7) và dãy được giải mã là 1011000



Hình 4.6: Giải mã Viterbi quyết định cứng cho mã (7, 4, 3)

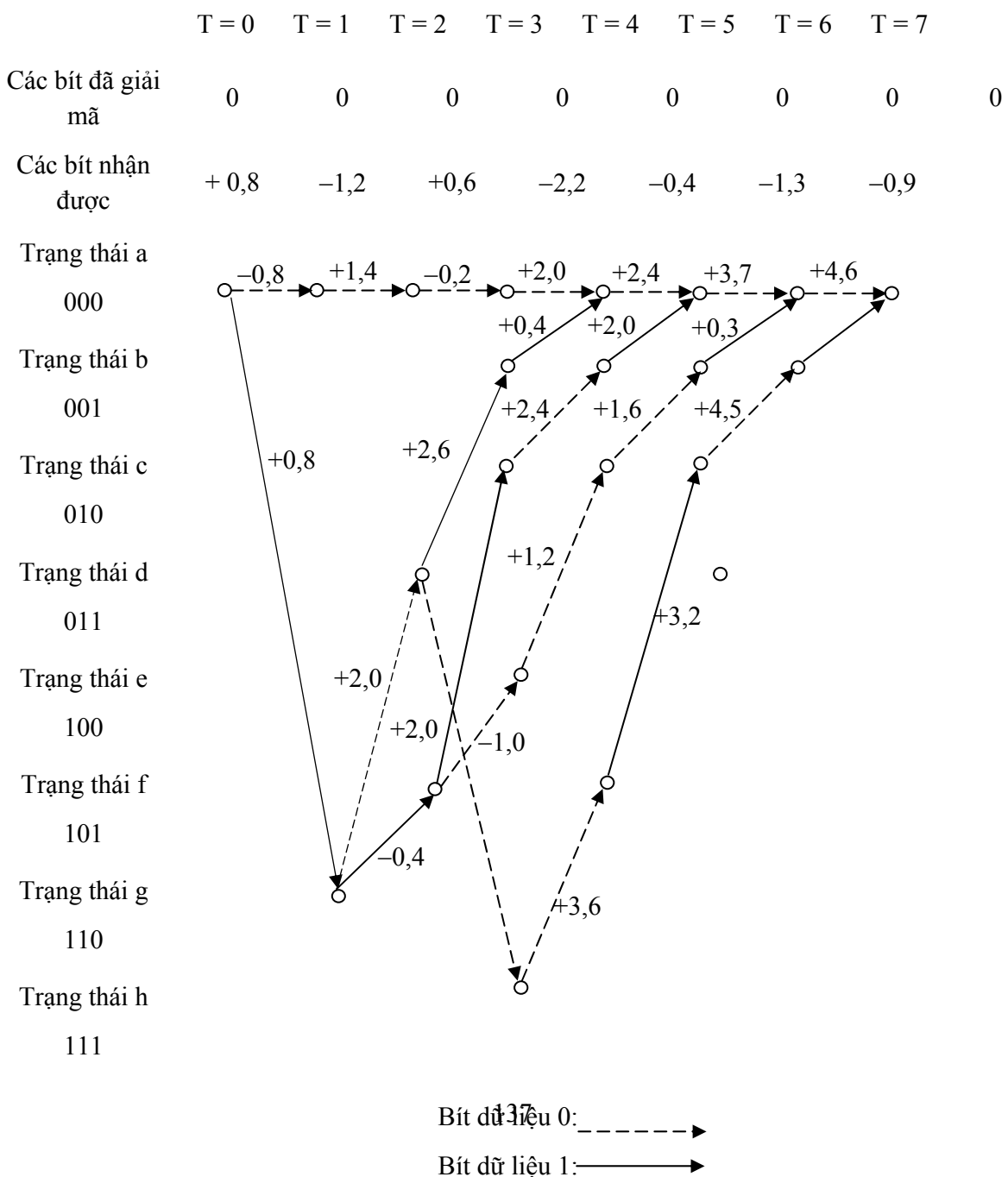




Hình 4.7: Giải mã sai khi dùng giải mã Viterbi quyết định cứng

#### 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  $+1$ , 0. Nếu ta phát dãy toàn 0 thì dãy phát tương ứng là  $-1 -1 -1 -1 -1 -1 -1$ . 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 dãy 1010000 nếu ta sử dụng giải mã quyết định cứng). Các đầu ra mềm của bộ giải mã điều chế được dùng như độ đo 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 mềm đầu tiên của bộ giải điều chế là  $+0,8$  ngụ ý rằng tín hiệu phát rất có thể là  $+1$  và độ đo mức tin cậy của quyết định này là  $0,8$ . Xem xét đường dẫn  $a \rightarrow g$  tương ứng với logic 1, độ đo 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 đo nhánh của đường dẫn này là  $-0,8$  (tích lũy một độ đo đường dẫn âm hay là lượng phạt) do sự sai lệch của nó. Ở thời điểm thứ hai tín hiệu nhận được là  $-1,2$  tạo nên các độ đo 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  $\alpha_1$  và  $\alpha_2$  là các đường  $a \rightarrow a \rightarrow a \rightarrow a \rightarrow a$  và  $a \rightarrow g \rightarrow d \rightarrow b \rightarrow a$ . Các độ đo 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 đo đường dẫn lớn hơn vì mức tin cậy được tích lũy của nó lớn hơn. Bởi vậy đường  $\alpha_1$  sẽ được chọn (chứ không phải là đường  $\alpha_2$  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 xyclic.

**Định nghĩa:** Mã xyclic Hamming là mã xyclic 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 xyclic (7, 4) có đa thức sinh  $g(X) = X^3 + X + 1$  là mã Hamming.

- Mã xyclic (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 KHỐI DỰA TRÊN SỐ HỌC CỦA TRƯỜNG HỮU HẠN

### 4.11.1. Trường hữu hạn cỡ 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 rằng  $3^6 = 3^5 \cdot 3 = 5 \cdot 3 \bmod 7 = 1$ .

Ta có thể thực hiện phép nhân bằng cách cộng các số mũ của 3.

Ví dụ:  $6 \cdot 2 = (3^3) \cdot (3^2) = 3^5 = 5$ .

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 nào 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  $\alpha$  là phần tử nguyên thủy của nó. Các lũy thừa của  $\alpha$  (từ  $\alpha^0$  đến  $\alpha^{q-2}$ ) gồm q - 1 phần tử khác không của trường. Phần tử  $\alpha^{q-1}$  sẽ bằng phần tử  $\alpha^0$ , 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 theo modulo (q - 1) đối với các số mũ của  $\alpha$ . 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  $\alpha$  sẽ lặp lại trước khi chúng tạo ra tất cả các phần tử khác không của trường (điều này có nghĩa là  $\alpha$  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  $\alpha$  theo điều kiện  $\alpha^3 + \alpha + 1 = 0$ . Khi đó các phần tử khác không của trường là:

$$\begin{aligned} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 &= \alpha + 1 \\ \alpha^4 &= \alpha^2 + \alpha \\ \alpha^5 &= \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 \\ \alpha^6 &= \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1 \end{aligned}$$

Mỗi lũy thừa của  $\alpha$  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  $\alpha$  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 (phần 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  $\alpha$  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  $\alpha$  và 3 cho  $\alpha^2$ , 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 thì  $f(X)$  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  $\beta_i$  là phần tử của  $GF(q^m)$ . Hơn nữa nếu  $\beta$  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  $\beta$  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  $\beta$  là một nghiệm của  $f(X)$  thì  $\beta^q$  cũng là một nghiệm của  $f(X)$ . Đa thức  $f(X)$  được gọi là đa thức tối tiểu của  $\beta$ . Nếu  $\beta$  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  $X^3 + X + 1$ . Thế  $X = \alpha, X = \alpha^2$  hoặc  $X = \alpha^4$  vào đa thức này ta thấy nó bằng 0. Bởi vậy  $X^3 + X + 1$  là đa thức tối tiểu của các phần tử  $\alpha, \alpha^2, \alpha^4$ . Tương tự thế  $\alpha^3, \alpha^6$  và  $\alpha^{12} (= \alpha^5)$  vào  $X^3 + X + 1$  ta thấy rằng chúng là các nghiệm của đa thức này. Đa thức tối tiểu của  $\alpha^0$  là  $(X + 1)$ .

Nếu  $m$  là số nguyên nhỏ nhất để  $\beta^m = 1$  thì phần tử  $\beta$  được gọi là có cấp  $m$  (ký hiệu  $\text{ord}(\beta) = m$ ) và  $\beta$  phải là nghiệm của  $X^m + 1$ . Nếu  $\beta$  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 xem 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  $GF(2^m)$ .

**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  $\alpha$  là nghiệm của  $(X^3 + X + 1)$  và bởi vậy  $\alpha^2$  và  $\alpha^4$  cũng là các nghiệm của nó.  $\alpha^3$  là nghiệm của  $(X^3 + X^2 + 1)$  và bởi vậy  $\alpha^6$  và  $\alpha^5$  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 phần tử khác không của  $GF(2^m)$  nên một đa thức bất khả quy bậc  $m$  luôn có các nghiệm trong  $GF(2^m)$ . 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  $GF(2^{c'})$ . Cần đề 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  $GF(2^c)$  và cũng nằm trong  $GF(2^{c'})$

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  $GF(2^{c'})$ .

**Ví dụ:** Đa thức  $f(X) = X^5 + X^4 + 1$  được phân tích thành tích của hai đa thức bất khả quy sau:

$$X^5 + X^4 + 1 = (X^3 + X + 1)(X^2 + X + 1)$$

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  $\alpha$  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  $\beta$  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  $\beta_1$  đến  $\beta_j$  thì :

$$v \begin{bmatrix} \beta_1^{n-1} & \beta_2^{n-1} & \dots & \beta_j^{n-1} \\ \vdots & \vdots & & \vdots \\ \beta_1^2 & \beta_2^2 & \dots & \beta_j^2 \\ \beta_1^1 & \beta_2^1 & & \beta_j^1 \\ \beta_1^0 & \beta_2^0 & & \beta_j^0 \end{bmatrix} = 0$$

Ta biết rằng:  $\mathbf{v} \cdot \mathbf{H}^T = 0$

Như vậy ma trận chuyển vị của ma trận ở trên chính là ma trận kiểm tra của mã. Các nghiệm đều là các đa thức của  $\alpha$  (ta cũng xem như là các vectơ và chúng cũng phải được chuyển vị), bởi vậy ta có thể viết:

$$\mathbf{H} = \begin{bmatrix} \beta_1^{n-1^T} & \dots & \beta_1^{1^T} & \beta_1^{0^T} \\ \beta_2^{n-1^T} & \dots & \beta_2^{1^T} & \beta_2^{0^T} \\ \vdots & \dots & \vdots & \vdots \\ \beta_j^{n-1^T} & \dots & \beta_j^{1^T} & \beta_j^{0^T} \end{bmatrix}$$

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  $\alpha$  làm nghiệm thì:

$$\mathbf{H} = \begin{bmatrix} \alpha^{n-1^T} & \dots & \alpha^{1^T} & \alpha^{0^T} \end{bmatrix}$$

Ta biết rằng các lũy thừa của  $\alpha$  là tất cả các phần tử khác không của trường, điều này có nghĩa là ma trận kiểm tra  $\mathbf{H}$  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  $\mathbf{H}$  của mã này có dạng:

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Ma trận này chứa tất cả các vectơ cột 3 bit có thể có. Đây chính là ma trận kiểm tra của mã xyclic (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 t sai là mã xyclic 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  $\beta$ .
2. Chọn một số nguyên tố không âm  $b$ . Thông thường  $b = 1$
3. Liệt kê ra  $2t$  lũy thừa liên tiếp của  $\beta$

$$\beta^b, \beta^{b+1}, \dots, \beta^{b+2t-1}$$

Xác định các đa thức tối tiểu trên  $GF(q)$  của các phần tử này (cần chú ý rằng các phần tử liên hợp có cùng một đa thức tối tiểu)

4. Đa thức sinh  $g(X)$  là BCNN của đa thức tối tiểu này. mã tạo được chính là mã xyclic  $(n, k)$  với  $k = n - \deg g(X)$ .

**Định nghĩa:** Nếu  $b = 1$  thì mã BCH được gọi là mã BCH nghĩa hẹp. Nếu  $n = q^m - 1$  thì mã BCH được gọi là mã BCH nguyên thủy.

**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  $\alpha$  và  $\alpha^2$  thì nghiệm thứ hai ( $\alpha^2$ ) là hiển 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  $\alpha^4$ . Hiển nhiên là chỉ có  $\alpha$  và  $\alpha^3$  là các nghiệm độc lập ( $\alpha^2$  và  $\alpha^4$  là các phần tử liên hợp của  $\alpha$ ). Bởi vậy ma trận kiểm tra của mã này có dạng sau:

$$H = \begin{bmatrix} \alpha^{n-1^T} & \dots & \alpha^{2^T} & \alpha^{1^T} & \alpha^{0^T} \\ \alpha^{3(n-1)^T} & \dots & \alpha^{3.2^T} & \alpha^{3.1^T} & \alpha^{3.0^T} \end{bmatrix}$$

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:  $s = e.H^T$

Syndrom có hai thành phần  $s_1$  và  $s_3$ :

$$\begin{aligned} s_1 &= \alpha^j + \alpha^i \\ s_3 &= \alpha^{3j} + \alpha^{3i} \end{aligned}$$

Thế  $\alpha^j = s_1 + \alpha^i$  từ phương trình thứ nhất vào phương trình thứ hai ta có:

$$s_1^2 \alpha^i + s_1 \alpha^{2i} + s_1^3 + s_3 = 0$$

$\alpha^i$  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  $\alpha$  và  $\alpha^3$  trên GF(16) sử dụng đa thức nguyên thủy  $X^4 + X + 1$ . Các phần tử  $\alpha^i$  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 :

$$v(X) = x^6 + x^4 + 1 \leftrightarrow 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1$$

Syndrom tương ứng là 1 1 1 0 0 1 1 0

$$\text{Hay } s_1 = \alpha^{11}, \quad s_3 = \alpha^5 \quad (\alpha^{11} = 1 \ 1 \ 1 \ 0, \alpha^5 = 0 \ 1 \ 1 \ 0)$$

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  $\alpha$  và  $\alpha^3$  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 xyclic 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 xyclic (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  $\beta$  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  $\alpha$  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  $\alpha$  là nghiệm của đa thức nguyên thủy  $x^3 + x + 1$ . Bởi lũy thừa liên tiếp của  $\alpha$  là  $\alpha^1, \alpha^2, \alpha^3, \alpha^4$ . Như vậy đa thức sinh của mã RS sửa 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 tầm thường là mã kiểm 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. Mở đầu và một số khái niệm cơ bản.

Mã chấp 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 chấp). Mã chấp được sử dụng rộng rãi trong thực tế. Bởi mã hóa được xem như một tập hợp các bộ lọc số tuyến tính với dãy mã là các đầu ra của bộ lọc được phép xen kẽ. Các mã chấp là các mã đầu tiên được xây dựng các thuật toán giải mã quyết định phần mềm hiệu quả

**Ví dụ:** Mã khối từ các khối  $k$  đầu tạo ra các khối  $n$  đầu. Với các mã chấp (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 dãy và các hàm truyền đạt như các chuỗi lũy thừa của biến  $x$  (đôi khi còn dùng ký hiệu  $D$  thay cho  $x$ ). Dãy  $\{\dots, m_{-2}, m_{-1}, m_0, m_1, m_2, \dots\}$  (với các phần tử  $m_i$  thuộc trường  $F$ ) được xem như một chuỗi Laurent:

$$m(x) = \sum_{e=-\infty}^{\infty} m_e x^e$$

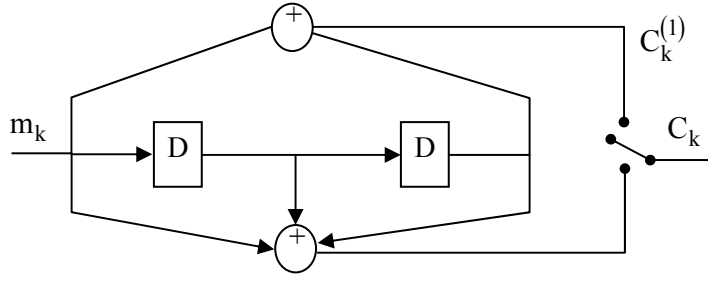
Tập tất cả các chuỗi Laurent trên  $F$  là một trường, ta ký hiệu trường này là  $F[[x]]$ . Như vậy  $m(x) \in F[[x]]$ .

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:

$$m(x) = \begin{bmatrix} m^{(1)}(x) & m^{(2)}(x) \end{bmatrix} \in F[[x]]^2$$

Bộ mã hóa cho mã chấp 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 trigơ 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:

$$C^{(1)} = \{1, 1, 1, 1, 1, 0, 0, 0, 1\} \text{ và } C^{(2)} = \{1, 0, 0, 1, 1, 1, 0, 1, 1\}$$

$$\text{Dòng ra: } C = \{11, 10, 10, 11, 11, 01, 00, 01, 11\}$$

Ở đây dấu 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:

$$g^{(1)}(x) = 1 + x^2. \text{ Tương tự ta có } g^{(2)}(x) = 1 + x + x^2$$

Dòng 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:

$$\begin{aligned} C^{(1)}(x) &= m(x)g_1(x) = (1 + x + x^4 + x^6)(1 + x^2) = 1 + x + x^2 + x^3 + x^4 + x^8 \\ C^{(2)}(x) &= m(x)g_2(x) = (1 + x + x^4 + x^6)(1 + x + x^2) \\ &= 1 + x^3 + x^4 + x^5 + x^7 + x^8 \end{aligned}$$



Với mỗi mã chập tốc độ  $R = \frac{k}{n}$  có một hàm truyền ma trận  $k \times n \in (x)$  (còn được gọi là ma trận truyền). Với mã tốc độ  $R = \frac{1}{2}$  ở ví dụ trên ta có:

$$G_a(x) = \begin{bmatrix} 1 + x^2 & 1 + x + x^2 \end{bmatrix}$$

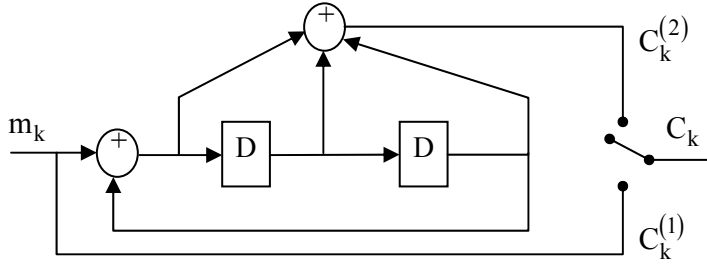
Ma trận truyền này không chỉ có dạng các đa thức, ta có thể thấy thông qua ví dụ sau:

**Ví dụ:** Xét ma trận truyền của mã chập 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 dòng vào sẽ xuất hiện trực tiếp ở đầu ra đan xen, bởi vậy đây là một mã chập hệ thống

Bộ mã hóa cho mã 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 mã 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  $k$  dòng), ta có:

$$m(x) = \begin{bmatrix} m^{(1)}(x), m^{(2)}(x), \dots, m^{(k)}(x) \end{bmatrix}$$

và:

$$G(x) = \begin{bmatrix} g^{(1,1)}(x) & g^{(1,2)}(x) & \dots & g^{(1,n)}(x) \\ g^{(2,1)}(x) & g^{(2,2)}(x) & \dots & g^{(2,n)}(x) \\ \vdots & \vdots & \dots & \vdots \\ g^{(k,1)}(x) & g^{(k,2)}(x) & \dots & g^{(k,n)}(x) \end{bmatrix}$$

Dãy ra được biểu thị như sau:

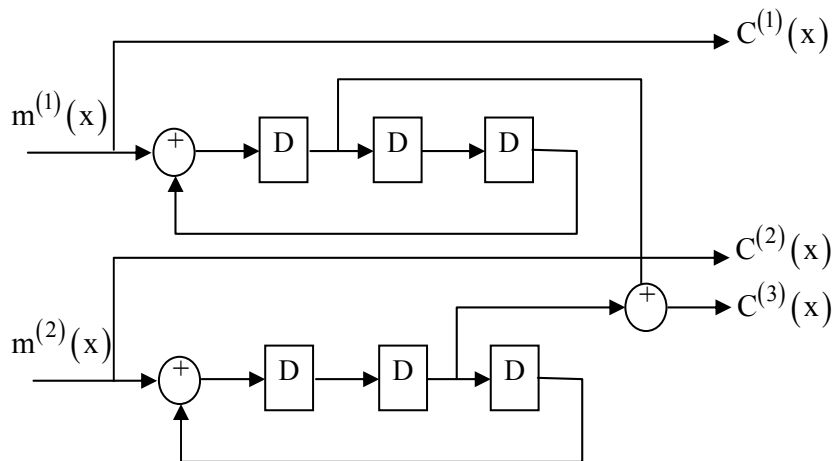
$$C(x) = [C^{(1)}(x), C^{(2)}(x), \dots, C^{(n)}(x)] = m(x)G(x)$$

Ma 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:

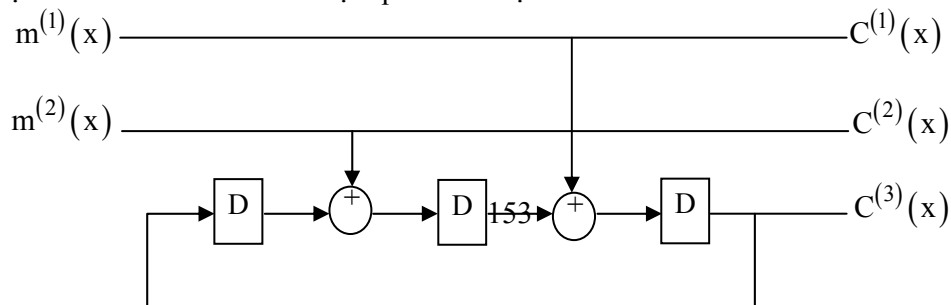
$$G(x) = \begin{bmatrix} 1 & 0 & \frac{x}{1+x^3} \\ 0 & 1 & \frac{x^2}{1+x^3} \end{bmatrix}$$

Sơ 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**

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:

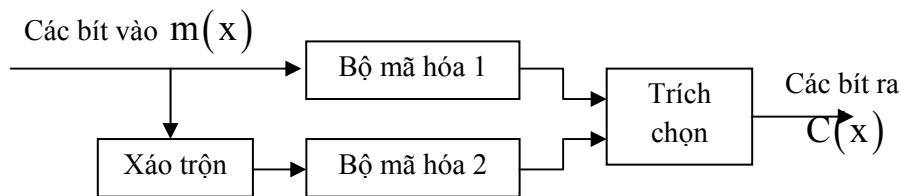
$$\{100, 001, 110, 001, 100, 111, 010, 110\}$$

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 ảnh 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  $R = 1/2$ .

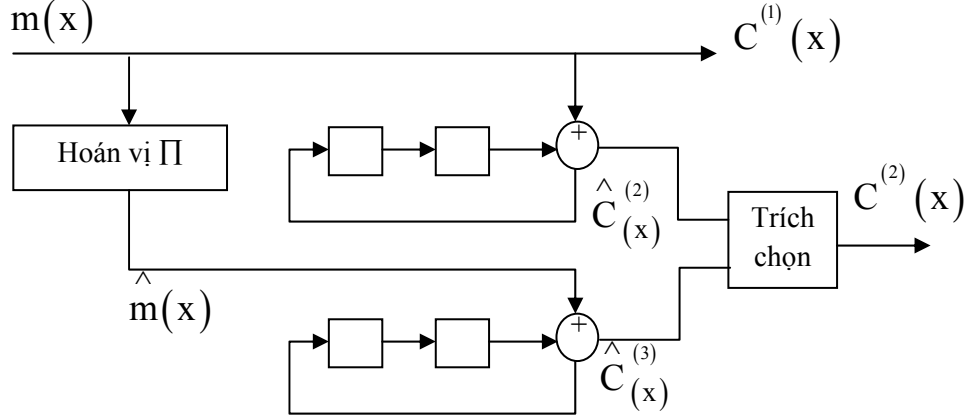
Các mã này được sử dụng rất hiệu quả trên các kênh phadih. Người ta đã chứng tỏ rằng hiệu năng của mã Turbo sẽ tăng khi tăng kích thước của bộ xáo trộn. Tuy nhiên trong nhiều ứng dụng quan trọng (chẳng hạn khi truyền tiếng nói), kích thước bộ xáo trộn quá lớn không sử dụng được do kết quả giải mã bị 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  $\Pi$

$$\Pi = \{8, 3, 7, 6, 9, 0, 2, 5, 1, 4\}$$



Hình4.7:

Giả sử dãy vào là:  $m(x) = [1, 1, 0, 0, 1, 0, 1, 0, 1, 1] = C^{(1)}(x)$

Khi đó dãy ra của bộ mã hóa thứ nhất là:

$$\hat{C}^{(2)}(x) = [1, 1, 1, 1, 0, 1, 1, 1, 0, 0]$$

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:

$$\hat{C}^{(3)}(x) = [1, 0, 1, 1, 0, 0, 0, 0, 1, 1]$$

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:

$$v(x) = [1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1]$$

Khi không dùng bộ trích chọn dãy bit ra sẽ có tốc độ  $R = \frac{1}{3}$  và có dạng

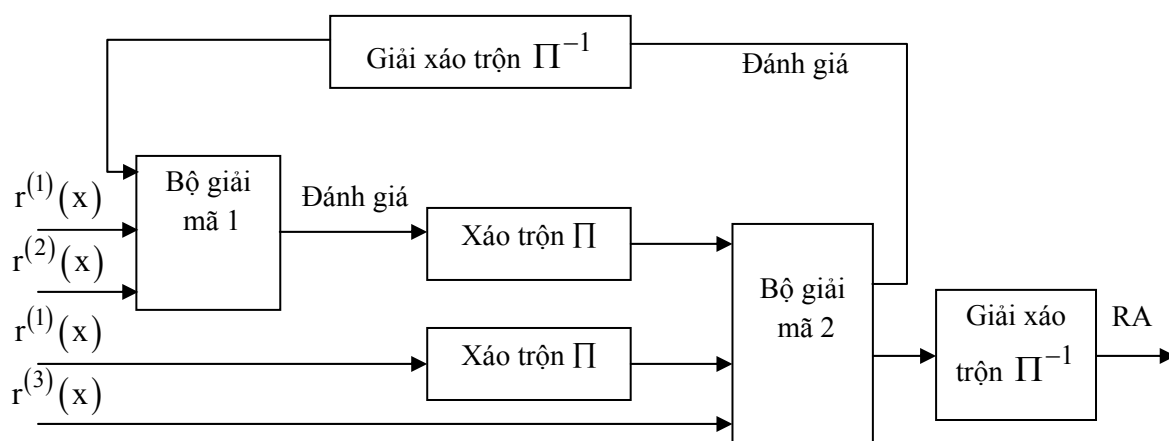
$$v(x) = [1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1]$$

Dãy ra  $v(x)$  được điều chế và phát qua kênh, ở đầu ra kênh tín hiệu nhận được giải điều chế 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 sử dụng 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  $\Pi$  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  $\Pi$ . Đầu ra đánh giá của bộ giải mã 2 được giải xáo trộn bằng luật hoán vị ngược  $\Pi^{-1}$  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)

Phần 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 khối chức năng của bộ giải mã Turbo

## BÀI TẬP

4.1. Hãy thiết lập các từ mã hệ thống cho mã xyclic  $(7, 3) = \langle 1 + x + x^2 + x^4 \rangle$  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 xyclic (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 đối 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 đối 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 đem dùng là  $N < N_0$  (số các từ mã còn lại gọi là các từ mã cấm). Khi một từ mã dùng biến thành một từ mã cấm nào đó thì ta bảo việc truyền tin gặp lỗi và như vậy lỗi 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 của bộ mã này. Áp dụng bằng 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 vành  $Z_2[x]/X^{15} + 1$

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 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 vành  $Z_2[x]/X^9 + 1$ .

**4.15.** Hãy thực hiện mã hóa Huffman cho nguồn rời rạc sau:

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{32} & \frac{1}{32} & \frac{1}{32} & \frac{1}{64} & \frac{1}{64} \end{pmatrix}$$

Đánh giá hiệu quả của phép mã 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 từ 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  $\mu$  - hệ số truyền của kênh (thông thường  $\mu \ll 1$ )

Giả thiết  $\mu = \text{const}$ .

$\tau$  - thời gian giữ chậm tín hiệu của kênh

$n(t)$  - nhiễu cộng, là một hàm ngẫu nhiên

Trường đầu lối vào  $\{\alpha_i\}$   $i = \overline{1, m}$ , khi đó các  $S_i(t)$  là các tín hiệu phát tương ứng với các tín  $\alpha_i$ .

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.  $S_1(t)(\alpha_1)$  đã được gửi đi và trong quá trình truyền  $S_1(t)$  được cộng thêm một nhiễu:

$$n(t) = u(t) - \mu S_1(t - \tau)$$

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 sơ đồ giải. Yêu cầu lớn nhất của sơ đồ giải là phải cho ra lời giải đúng (phát  $\alpha_1$  ta phải tìm được  $\beta_1$ ). Trong thực tế có rất nhiều sơ đồ giải. Trong tất cả các sơ đồ giải có thể có thì tại một sơ đồ bảo đảm xác suất nhận lớn phải đúng là lớn nhất (xác suất giải sai là bé nhất). Sơ đồ này được gọi là sơ đồ giải tối ưu. Máy thu xây dựng theo sơ đồ giải đó được gọi là máy thu tối ưu (hay lý tưởng)

### 5.1.3. Thế chống 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 thế chống 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  $\alpha_1$  đã gửi đi. Nội dung của sai lầm này là bác bỏ  $H_1$  mà thực tế là nó đúng. Tức là quả thật  $\alpha_1$  gửi đi mà ta không gửi. Sai lầm 1 là bỏ sót tin (hay mục tiêu).

b. Sai lầm loại 2: Thừa nhận  $H_1$  trong khi thực tế nó sai. Tức là thực ra không có  $\alpha_1$  mà ta lại bảo 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 sơ đồ giải, sơ 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 đảm bảo 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, Vald .... Những tiêu chuẩn này khắc phục được nhược điểm trên nhưng khá 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  $\beta_1$ . 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

tuyến tính hoặc phi tuyến nhờ các mạch tuyến tính hoặc phi tuyến (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 chức năng mà không mang tính chất thống kê. Ảnh hưởng của nhiễu lên chất lượng của máy thu chỉ được tính theo tỷ số tín hiệu / tạp. 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 đã xác định được quy tắc giải tối ưu.

### 5.1.7. Xác suất giải sai và quy tắc giải tối ưu

Cho  $\alpha_i$  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  $\left( \sum_{i=1}^m p(\alpha_i) = 1 \right)$ . 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  $\beta_j$  nào đó. Nếu nhận được  $\beta_l$  thì ta coi rằng  $\alpha_l$  đã được gửi đi. Như vậy  $\alpha_l$  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:

$$p(\text{sai} / u, \beta_l) = 1 - p(\alpha_l / u) \quad (5.1)$$

Từ (5.1) ta sẽ tìm ra quy tắc giải tối ưu (theo tiêu chuẩn Kachennhicov)

Để tìm ra quy tắc giải tối ưu ta xét hai sơ đồ giải:

- Từ  $u(t)$  cho ta  $\beta_1$

- Từ  $u(1)$  cho ta  $\beta_2$

Nếu  $p(\text{sai} / u, \beta_1) < p(\text{sai} / u, \beta_2)$  (5.2) thì ta sẽ coi sơ đồ thứ nhất tối ưu hơn sơ đồ thứ hai.

$$\text{Từ (5.1) và (5.2)} \Rightarrow p(\text{sai} / u, \beta_1) > p(\text{sai} / u, \beta_2) \quad (5.3)$$

Tức là xác suất chọn lời giải sai  $p(\text{sai} / u, \beta_l)$  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:

$$p(\alpha_l / u) > p(\alpha_i / u) \quad \text{Với} \quad \begin{cases} i = \overline{1, m} \\ i \neq l \end{cases} \quad (5.4)$$

Nếu ta có  $(m-1)$  hệ thức này thì ta coi sơ đồ giải chọn  $\beta_l$  sẽ là tối ưu (theo nghĩa Kachennhicov) 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

$$\text{Dùng công thức Bayes: } p(\alpha_j/u) = \frac{p(\alpha_j)w(u/\alpha_j)}{w(u)} \quad (5.5)$$

$$\text{Thay vào (5.4) ta có: } p(\alpha_l)w(u/\alpha_l) > p(\alpha_i)w(u/\alpha_i) \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq l \end{cases} \quad (5.6)$$

$$\text{Hay } \frac{w(u/\alpha_l)}{w(u/\alpha_i)} > \frac{p(\alpha_i)}{p(\alpha_l)}$$

$$\text{Đặt } \lambda_{l/i} \triangleq \frac{w(u/\alpha_l)}{w(u/\alpha_i)} \text{ và được gọi là hàm hợp lý (tỷ số hợp lý). Nó đặc trưng cho mức độ}$$

hợp lý của giả thuyết cho rằng  $\alpha_l$  đã được gửi đi (so với giả thuyết cho rằng  $\alpha_i$  đã được gửi đi).

$$\text{Ta có: } \lambda_{l/i}(u) \triangleq \frac{p(\alpha_i)}{p(\alpha_l)} \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq l \end{cases} \quad (5.7)$$

(5.7) chính là quy tắc giải tối ưu viết dưới dạng hàm hợp lý.

### 5.1.9. Quy tắc hợp lý tối đa

$$\text{Nếu mọi tín hiệu gửi đi đều đồng xác suất: } p(\alpha_l) = p(\alpha_i) = \frac{1}{m} \text{ với } \forall i, l = \overline{1, m} \text{ thì}$$

$$(5.7) \text{ trở thành } \lambda_{l/i}(u) > 1 \quad \text{Với } \forall i \neq l \quad (5.8)$$

(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 dấu đồng xác suất.

Để có thể thấy rõ ảnh hưởng của tính thống kê của nhiễu ở (5.8) ta thường viết nó dưới dạng:

$$\begin{aligned} \lambda_{l/i}(u) &= \frac{w(u/\alpha_l)}{w(u/\alpha_i)} = \frac{w(u/\alpha_l) : w(u/0)}{w(u/\alpha_i) : w(u/0)} \\ \Rightarrow \lambda_{l/i}(u) &= \frac{\lambda_{l/0}(u)}{\lambda_{i/0}(u)} \Rightarrow \lambda_{l/0}(u) > \lambda_{i/0}(u) \quad \forall i \neq l \end{aligned} \quad (5.9)$$

$\lambda_{j/0}(u)$  và  $\lambda_{i/0}(u)$  để tìm hơn  $\lambda_{j/i}(u)$ . 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 cộng 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  $\sigma^2$  và kỳ vọng triệt. Tín hiệu phát có mọi yếu tố triệt 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 phổ hữu hạn  $F_c$ . Như vậy ta có thể rời rạc hóa  $u(t)$  thành  $n$  số đọc:

$u_1, u_2, \dots, u_n$ ,  $n = 2F_c T$ , 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 đọc của nhiễu độc lập, thông hệ với nhau thì:

$$W_n(u_1, u_2, \dots, u_n/0) = \prod_{k=1}^{2F_c T} W_1(u_k) = \prod_{k=1}^{2F_c T} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{u_k^2}{2\sigma^2}}$$

$$= \frac{1}{(\sigma\sqrt{2\pi})^{2F_c T}} \exp \left\{ -\sum_{k=1}^{2F_c T} \frac{u_k^2}{2\sigma^2} \right\}$$

Ký hiệu  $c_j(t) = \mu S_j(t - \tau)$ .

Khi phát  $\alpha_j$  ta sẽ nhận được các  $u_k = c_{jk} + n_k$ .

Để tính toán dễ dàng ta coi việc đã phát  $\alpha_j$  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:

$$W_n(u'_1, u'_2, \dots, u'_n/0) = \frac{1}{(\sigma\sqrt{2\pi})^{2F_c T}} \exp \left\{ -\sum_{k=1}^{2F_c T} \frac{(u_k - c_{jk})^2}{2\sigma^2} \right\}$$

$$\Rightarrow \lambda_{j/0}(u_1, u_2, \dots, u_n) = \exp \left\{ \sum_{k=1}^{2F_c T} \frac{u_k^2}{2\sigma^2} - \sum_{k=1}^{2F_c T} \frac{(u_k - c_{jk})^2}{2\sigma^2} \right\}$$

Phương sai  $\sigma^2$  của tạp có thể biểu thị qua mật độ phổ 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 tin ở lối 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  $\frac{\lambda_{l/0}(u)}{\lambda_{i/0}(u)} > 1$  Với  $\begin{cases} i = \overline{1, m} \\ i \neq l \end{cases}$ . Lấy  $\log_e$  hai vế:

$$\begin{aligned}
 \ln \lambda_{l/0}(u) - \ln \lambda_{i/0}(u) &> 0 \\
 \Rightarrow \ln \lambda_{l/0}(u) &> \ln \lambda_{i/0}(u) \quad (*)
 \end{aligned}$$

Thay (5.11) vào (\*) ta được:

$$-\frac{E_l}{G_0} + \frac{2T}{G_0} Z_l(u) > -\frac{E_i}{G_0} + \frac{2T}{G_0} Z_i(u) \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq l \end{cases}$$

Nhân hai vế với  $\frac{G_0}{2T}$  ta có:

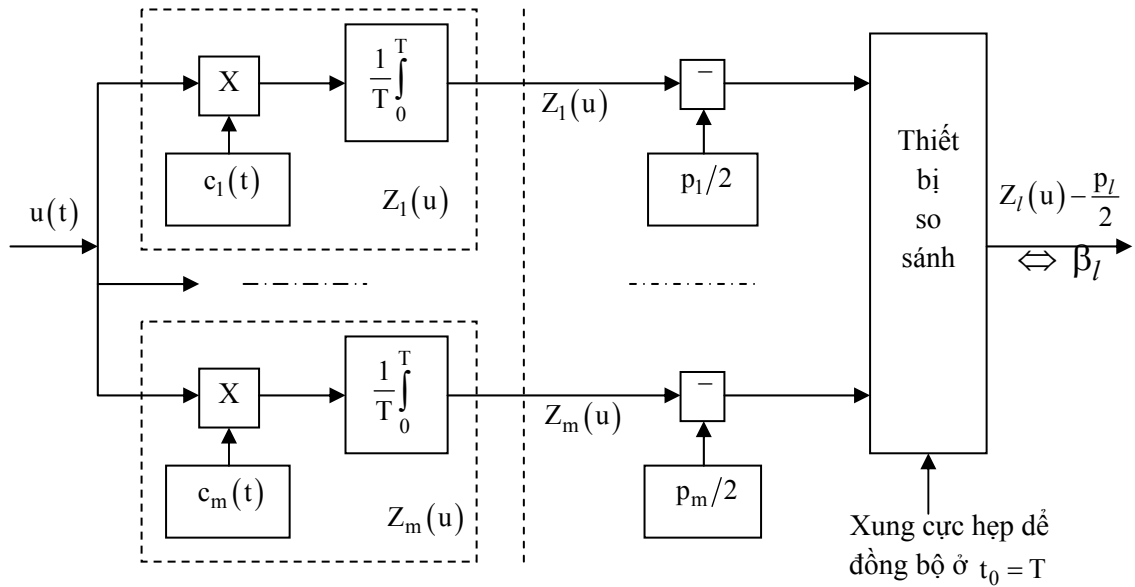
$$Z_l(u) - \frac{E_l}{2T} > Z_i(u) - \frac{E_i}{2T} \quad \text{Với } \begin{cases} i = \overline{1, m} \\ i \neq l \end{cases}$$

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  $\beta_l$  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 kè. 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 hẹp đồng bộ mở thiết bị so sánh vào đúng thời điểm đọc  $t_0 = T$



### 5.2.3. Khái niệm về thu kết hợp và thu không kết hợp

#### 5.2.3.1. Hệ có khoảng nghỉ 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  $\mu, \tau$  là các tham số của kênh phụ thuộc rất nhiều vào các yếu tố ngẫu nhiên.

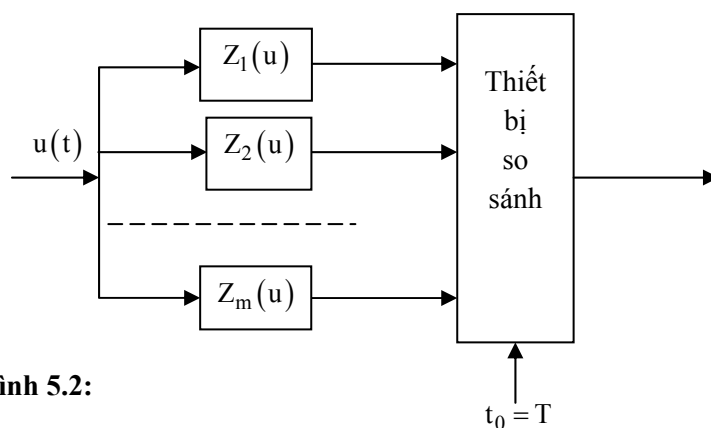
Khi  $\mu$  thay đổi thì  $Z_i(u)$  sẽ thay đổi tỷ lệ với  $\mu$  còn  $p_i$  sẽ thay đổi tỷ lệ với  $\mu^2$ . Vì vậy để đảm bảo được quy tắc giải (5.13) ta cần có mạch tự động hiệu chỉnh để bù lại sự thay đổi của  $\mu$  (ví dụ dùng mạch TĐK (APY)).

Khi  $\tau$  thay đổi sẽ làm cho gốc 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 TĐT (ATY).

Để có thể tránh được sự phức tạp của thiết bị khi phải dùng thêm TĐK khi  $\mu$  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:

$$Z_l(u) > Z_i(u) \quad \forall i \neq l \quad (5.14)$$

Sơ đồ giải lúc này sẽ rất đơn giản và ngay cả khi  $\mu$  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 nghỉ chủ động.

#### 5.2.3.2. Định nghĩa thu kết hợp và thu không kết hợp

Tín hiệu tổng quát có dạng:

$$C_i(t) = C_{0i}(t) \cos(\omega t + \phi(t) + \phi_0)$$

Khi gia công tối ưu tín hiệu ta cần biết đường bao  $C_{0i}(t)$  và tần số tức thời

$$\omega_i(t) = \omega + \frac{d\phi(t)}{dt}.$$

Nếu việc thu  $C_i(t)$  cần biết  $\phi_0$  (để điều chỉnh hệ thống thu) thì được gọi là thu kết hợp.

Nếu việc thu  $C_i(t)$  không cần biết  $\phi_0$  (để điều chỉnh hệ thống thu) thì được gọi là thu không kết hợp.

Thực tế khi  $\tau$  thay đổi sẽ làm cho  $\phi_0$  thay đổi.  $\tau$  chỉ biến thiên ít nhưng cũng đã làm cho  $\phi_0$  thay đổi rất mạnh. Khi đó ta phải chuyển sang thu không kết hợp.

### 5.3. PHÁT TÍN HIỆU TRONG NHIỀU NHỜ BỘ LỌC PHỐI HỢP TUYẾN TÍNH THỤ 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  $\rho_{ra}$  là tỷ số giữa công suất đỉnh 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 tới)

$n(t)$  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,  $\rho_{ra}$  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 tuyến tính thụ động sao cho ở một thời điểm quan sát (dao động nhận được) nào đó  $\rho_{ra}$  đạt max.

Gọi  $S_{iv}(\omega)$  là mật độ phổ (biên) phức của thể hiện tín hiệu ở đầu vào mạch tuyến tính.

Gọi  $S_{ira}(\omega)$  là mật độ phổ phức của thể hiện tín hiệu ở đầu ra của nó.

Khi đó theo công thức biến đổi ngược Fourier thể hiện tín hiệu ở đầu ra của mạch tuyến tính thụ động này là:

$$\begin{aligned} C_{ira}(t) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} S_{ira}(\omega) e^{j\omega t} d\omega = \int_{-\infty}^{\infty} S_{ira}(2\pi f) e^{j2\pi f t} df \\ &= \int_{-\infty}^{\infty} S_{iv}(2\pi f) K_i(2\pi f) e^{j2\pi f t} df \end{aligned}$$

Trong đó:  $S_{ira}(2\pi f) = S_{iv}(2\pi f) K_i(2\pi f)$

Công suất đỉnh của tín hiệu ở đầu ra của mạch:

$$p_{c_{ira}} = |C_{ira}(t_0)|^2 = \left| \int_{-\infty}^{\infty} S_{iv}(2\pi f) K_i(2\pi f) e^{j2\pi f t_0} df \right|^2$$

$C_{ira}(t_0)$  là giá trị đỉnh của tín hiệu

Theo giả thiết vì can nhiễu là tạp trắng nên mật độ phổ công suất của nó sẽ là  $N_0 = \text{const}$  ( $N_0$  bằng  $\frac{1}{2}$  mật độ phổ công suất thực tế, vì phổ thực tế chỉ có từ  $0 \div \infty$ ). 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:

$$\int_{-\infty}^{\infty} x^2(t) dt = \frac{1}{2\pi} \int_{-\infty}^{\infty} |S(\omega)| d\omega$$

Ta xét tỷ số:  $\rho_{ra} = \frac{p_{c_{ira}}}{p_{n_{ra}}}$

$$\rho_{ra} = \frac{\left| \int_{-\infty}^{\infty} S_{iv}(2\pi f) K_i(2\pi f) \exp(j2\pi f t_0) df \right|^2}{N_0 \int_{-\infty}^{\infty} |K_i(2\pi f)|^2 df} \quad (5.15)$$

Vấn đề ở đây là phải xác định  $K_i(2\pi f)$  trong (5.15) như thế nào để  $\rho_{ra}$  đạt max.

Để giải quyết vấn đề này ta có thể dùng nhiều phương pháp, ở đây ta sử dụng bất đẳng thức Byhakobckuu – Schwartz:

$$\left| \int_{-\infty}^{\infty} F(x) \varphi(x) dx \right|^2 \leq \int_{-\infty}^{\infty} |F(x)|^2 dx \int_{-\infty}^{\infty} |\varphi(x)|^2 dx \quad (5.16)$$

$$\text{Đẳng thức ở (5.16) chỉ có khi: } \varphi(x) = k F^*(x) \quad (5.17)$$

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:

$$\begin{aligned} \rho_{ra} &\leq \frac{\int_{-\infty}^{\infty} |S_{iv}(2\pi f) \exp(j2\pi f t_0)|^2 df \int_{-\infty}^{\infty} |K_i(2\pi f)|^2 df}{N_0 \int_{-\infty}^{\infty} |K_i(2\pi f)|^2 df} \\ \Rightarrow \rho_{ra} &\leq \frac{1}{N_0} \int_{-\infty}^{\infty} |S_{iv}(2\pi f) e^{j2\pi f t_0}|^2 df \\ \Rightarrow \rho_{ra} &\leq \frac{1}{N_0} \int_{-\infty}^{\infty} |S_{iv}(2\pi f)|^2 df \quad \underline{\underline{\text{Định lý Parseval}}} \quad \frac{E_i}{N_0} \quad (5.18) \end{aligned}$$

$$(5.18) \text{ chứng tỏ } \rho_{ra \max} = \frac{E_i}{N_0} \quad (5.19)$$

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. (Chỉ khi cần đo lường các tham số của tín hiệu như  $\Delta F$ ,  $\Delta F$  (độ dịch tần) thì độ chính xác của phép đo và khả năng phân biệt của hệ thống đo sẽ phụ thuộc mạnh vào dạng tín hiệu).

Theo (5.17)  $\rho_{ra}$  chỉ đạt max khi:

$$k_i(2\pi f) = kS_{iv}^*(2\pi f)\exp\{-j2\pi ft_0\} \quad (5.20)$$

(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.

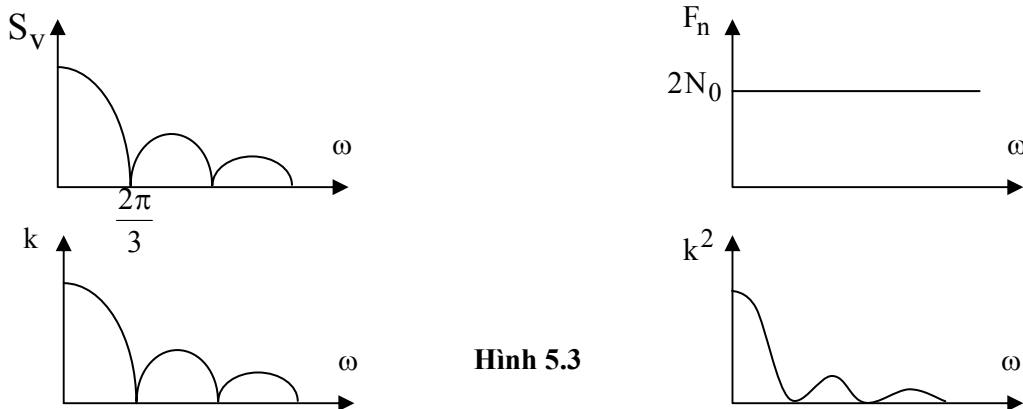
### 5.3.3. Đặc tính biên tần và đặc tính pha tần của bộ lọc phối hợp

#### 5.3.3.1. Đặc tính biên tần.

$$\text{Từ (5.20) ta có } |k_i(2\pi f)| = k|S_{iv}^*(2\pi f)| \quad (5.21)$$

(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 phổ của tín hiệu. Điều đó có nghĩa là khi đã cho tín hiệu tới thì đặc tính của mạch tuyến tính cần tổng hợp sẽ do mật độ phổ 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 phổ tín hiệu và tập âm ứng với những phần có cường độ nhỏ của phổ tín hiệu. Ở những khoảng tần số mà cường độ các thành phần phổ của tín hiệu càng nhỏ thì sự suy giảm đó càng lớn.



Hình 5.3

### 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 phổ pha của tín hiệu tới.

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 vặn khử 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 tới 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  $(\mu_1, t_1, \psi_1)$  thì mật độ phổ của tín hiệu này chỉ khác nhau với mật độ phổ 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 đáng 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 thụ 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

$$\omega' = \omega \Rightarrow g_i(t) = \frac{k}{2\pi} \int_{-\infty}^{\infty} S_{iv}(\omega') e^{j\omega'(t_0-t)} (-d\omega')$$

$$\Rightarrow g_i(t) = -k C_{iv}(t_0 - t)$$

Vì  $k$  là hằng số tùy ý nên ta có thể lấy:

$$g_i(t) = k C_{iv}(t_0 - t) \quad (5.23)$$

Đồ thị  $g_i(t)$  vẽ trên hình 5.4.

Từ hình 5.4 ta thấy rằng để thỏa mãn điều kiện thể hiện được bộ lọc:

$$g_i(t) = 0 \text{ khi } t < 0 \text{ nên } t_0 \geq T$$

### 5.3.5. Hưởng ứng ra của mạch lọc phối hợp

Theo tích phân Duhamen:

$$U_{ra}(t) = \int_0^t U_v(x) g(t-x) dx$$

Thay (5.23) vào ta có:

$$U_{ra}(t) = k \int_0^t U_v(x) C_{iv}(t_0 - t + x) dx$$

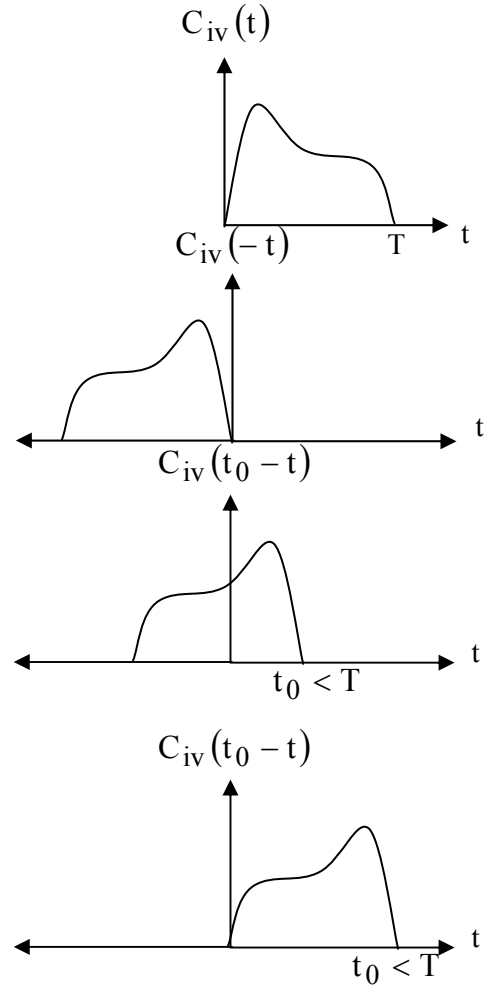
$$t = t_0 \Rightarrow U_{ra}(t_0) = k \int_0^{t_0} U_v(x) C_{iv}(x) dx = k \int_0^t U_v(t) C_{iv}(t) dt$$

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.



Hình 5.4

## 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 cộng và là tạp âm trắng, chuẩn dừng.

Tín hiệu ở đầu vào máy thu:  $u(t) = C_i(t) + n(t)$ ,  $i = 1, 2$

Ứng với quy tắc giải theo Kachennhicov ta sẽ nhận được lời giải đúng  $\alpha_1$ , nếu:

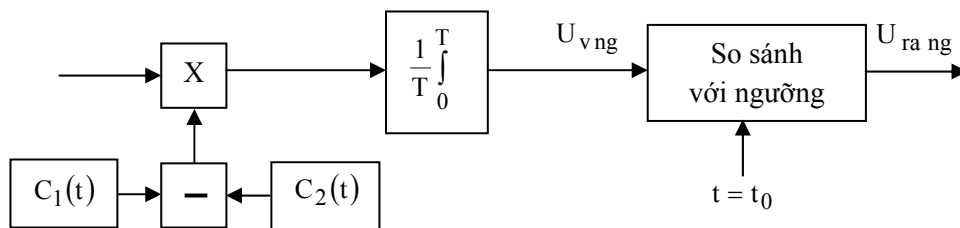
$$\frac{1}{T} \int_0^T u(t)C_1(t)dt - \frac{P_1}{2} > \frac{1}{T} \int_0^T u(t)C_2(t)dt - \frac{P_2}{2} \quad (*)$$

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  $U_{rang} \neq 0$ , khi đó ta xem rằng có lời giải  $\beta_1$  về  $\alpha_1$ .

Nếu  $U_{vng} < \frac{1}{2}(P_1 - P_2)$  thì  $U_{rang} = 0$ , khi đó ta xem rằng có lời giải  $\beta_2$  về  $\alpha_2$ .

**Chú ý:**

- Nếu  $P_1 \neq P_2$  mà  $\mu$  (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.

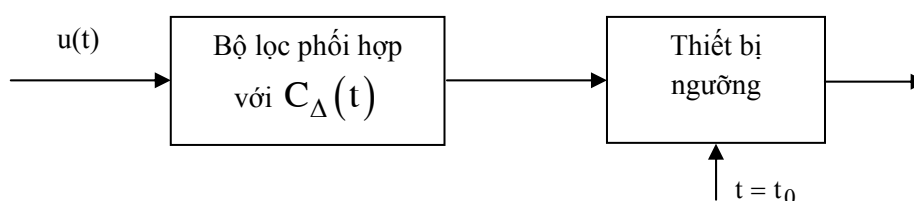


- Nếu  $P_1 = P_2$  thì ta không cần phải có thiết bị so sánh tự động điều chỉnh ngưỡng. Khi đó ta sẽ dùng bộ phân biệt cực. Ta quy ước rằng:

$$+ U_{\text{rang}} > 0 \text{ thì có lời giải } \beta_1 \leftrightarrow \alpha_1$$

$$+ U_{\text{rang}} < 0 \text{ thì có lời giải } \beta_2 \leftrightarrow \alpha_2$$

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.)

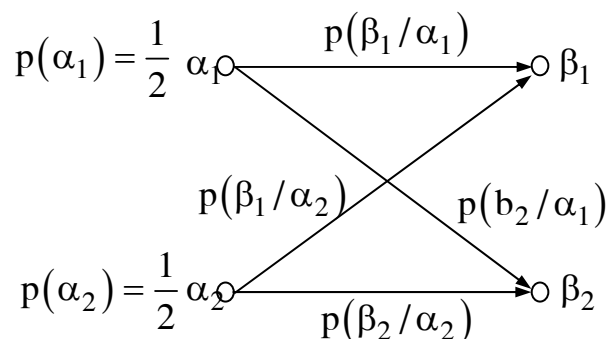


Hình 5.6.

## 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 Koppennhicop.

### 5.4.2.2. Giải bài toán

Theo công thức xác suất đầy đủ:

$$p_s = p(\alpha_1) \cdot p(\beta_2 / \alpha_1) + p(\alpha_2) \cdot p(\beta_1 / \alpha_2)$$

Để 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 thỏa mãn (5.25), tức là:

$$p(\beta_2 / \alpha_1) = p \left\{ \frac{1}{T} \int_0^T U(t) [C_1(t) - C_2(t)] dt < \frac{1}{2} (P_1 - P_2) \right\} \quad (5.26)$$

$$\text{Trong đó: } U(t) = C_1(t) + n(t) \quad (*)$$

$$P_i = \frac{1}{T} \int_0^T C_i^2(t) dt \quad (**)$$

Thay (\*) và (\*\*) vào (5.26), sau một vài biến đổi đơn giản, ta có:

$$\begin{aligned} p(\beta_2 / \alpha_1) &= p \left\{ \frac{1}{T} \int_0^T C_1^2(t) dt - \frac{1}{T} \int_0^T C_1(t) \cdot C_2(t) dt + \frac{1}{T} \int_0^T n(t) [C_1(t) - C_2(t)] dt \right. \\ &\quad \left. < \frac{1}{2T} \int_0^T C_1^2(t) dt - \frac{1}{2T} \int_0^T C_2^2(t) dt \right\} \\ \Rightarrow p(\beta_2 / \alpha_1) &= p \left\{ \frac{1}{T} \int_0^T n(t) \cdot C_\Delta(t) dt < -\frac{1}{2T} \int_0^T C_\Delta^2(t) dt \right\} \end{aligned} \quad (5.27)$$

$$\text{Trong đó: } C_\Delta(t) = C_1(t) - C_2(t).$$

$$P_\Delta = \frac{1}{T} \int_0^T C_\Delta^2(t) dt \text{ là công suất trung bình của tín hiệu hiệu số.}$$

$$\xi = \frac{1}{T} \int_0^T n(t) \cdot C_\Delta(t) dt \text{ là một đại lượng ngẫu nhiên, vì } n(t) \text{ là một quá trình ngẫu nhiên}$$

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  $\xi$  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:  $\sigma_\xi^2$ :

$$\begin{aligned} \sigma_\xi^2 &= D[\xi] = D \left\{ \frac{1}{T} \int_0^T n(t) C_\Delta(t) dt \right\} \stackrel{\Delta}{=} \frac{1}{T^2} M \left\{ \left[ \int_0^T n(t) C_\Delta(t) dt \right]^2 \right\} \\ &= \frac{1}{T^2} M \left\{ \int_0^T n(t) C_\Delta(t) dt \cdot \int_0^T n(t_1) C_\Delta(t_1) dt_1 \right\} \\ &= \frac{1}{T^2} M \left\{ \int_0^T \int_0^T C_\Delta(t) C_\Delta(t_1) n(t_1) n(t) dt dt_1 \right\} \\ &= \frac{1}{T^2} \int_0^T \int_0^T C_\Delta(t) C_\Delta(t_1) M\{n(t) n(t_1)\} dt dt_1 \end{aligned} \quad (a)$$

Theo giả thiết  $n(t)$  là tạp âm trắng, chuẩn, dừng, dùng biến đổi Wiener – Khinchin, ta tính được hàm tự tương quan của nó:

$$M\{n(t) n(t_1)\} \stackrel{\Delta}{=} R(t - t_1) = N_0 \delta(t - t_1) \quad (b)$$

$$\text{Với } R(t - t_1) = \int_{-\infty}^{\infty} N_0 \cdot e^{j\omega(t - t_1)}$$

Thế (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  $\delta$ :

$$\int_a^b f(x) \delta(x - x_0) dx = f(x_0) \quad \text{khi } a < x_0 < b$$

ta có: 
$$\int_a^b C_{\Delta}(t_1) \delta(t - t_1) dt_1 = C_{\Delta}(t) \quad (d)$$

Thay (d) vào (c), ta được:

$$\begin{aligned} \sigma_{\xi}^2 &= \frac{N_0}{T^2} \int_0^T C_{\Delta}(t) dt \int_0^T C_{\Delta}(t_1) \delta(t - t_1) dt_1 = \frac{N_0}{T^2} \int_0^T C_{\Delta}^2(t) dt \\ \Rightarrow \sigma_{\xi}^2 &= \frac{N_0 P_{\Delta}}{T} \end{aligned} \quad (5.31)$$

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  $\alpha_1$  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  $\eta = \frac{\xi}{\sqrt{\frac{N_0 P_{\Delta}}{T}}}$

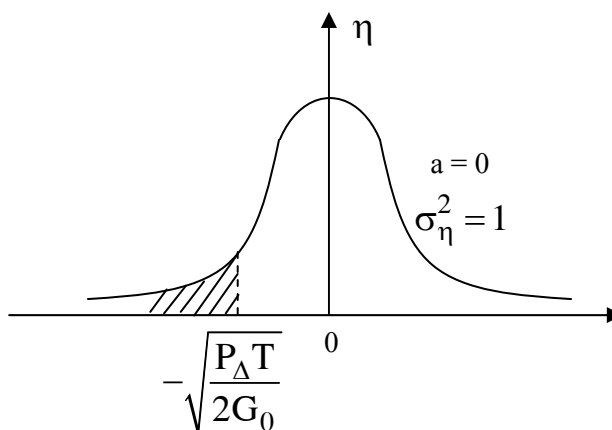
$$\Rightarrow p(\beta_2 / \alpha_1) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\sqrt{\frac{P_{\Delta} T}{4N_0}}} \exp \left\{ -\frac{\eta^2}{2} \right\} d\eta = \Phi \left( -\sqrt{\frac{P_{\Delta} T}{2G_0}} \right) \quad (*)$$

Trong đó  $G_0 = 2N_0$  là phổ 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:

$$p(\beta_1 / \alpha_2) = 1 - \phi\left(\sqrt{\frac{P_\Delta T}{2G_0}}\right) \quad (5.33')$$

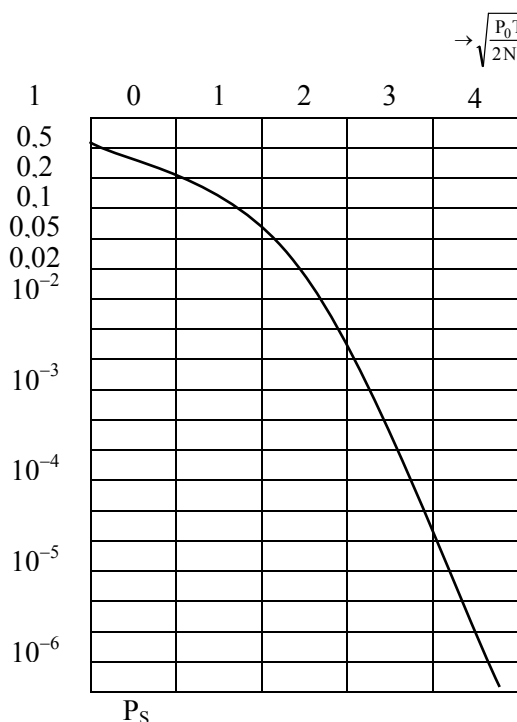
$$\Rightarrow p_s = 1 - \phi\left(\sqrt{\frac{P_\Delta T}{2G_0}}\right) \quad (5.34)$$

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 nhỏ  $p_s$  người ta giảm nhỏ  $G_0$  bằng cách dùng các bộ khuếch đại tạp âm nhỏ (khuếch đại tham số, khuếch đại lượng tử,...)

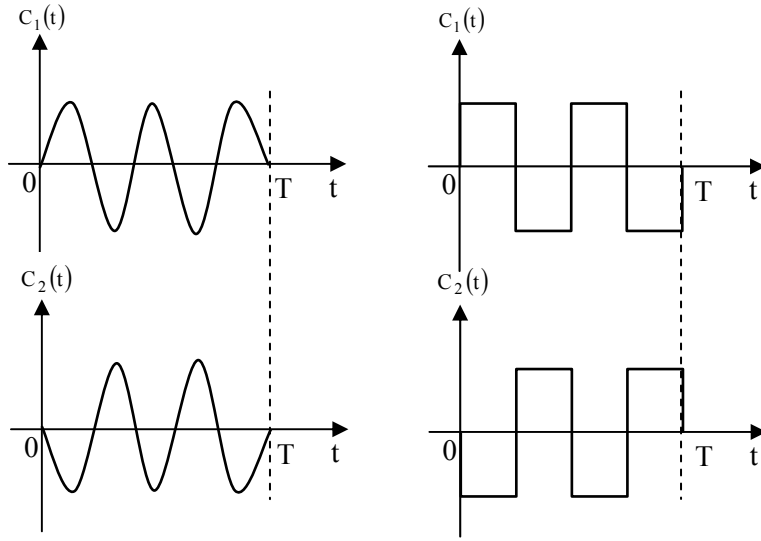
#### 5.4.2.3. Tính xác suất sai trong một số trường hợp cụ thể

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 tới  $C_i(t)$ .

$$p_s = 1 - \phi\left(\sqrt{\frac{4P_c T}{2G_0}}\right) \Rightarrow p_s = 1 - \phi(\sqrt{2} h) \quad (5.35)$$

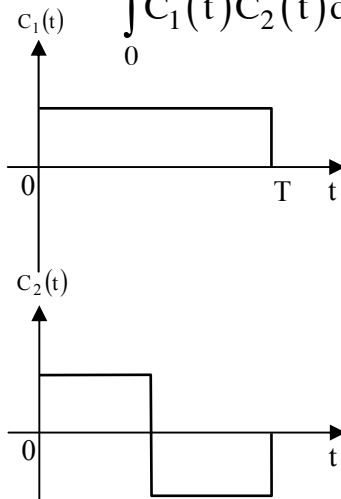
Trong đó  $P_c T$  là năng lượng của tín hiệu.

$$h = \sqrt{\frac{P_c T}{G_0}} \quad (\text{chính là tỷ số tín/tạp})$$

### b. Các tín hiệu trực giao (theo nghĩa hẹp)

**Định nghĩa:** Hai tín hiệu được gọi là trực giao theo nghĩa hẹp, nếu:

$$\int_0^T C_1(t) C_2(t) dt = 0$$



Khi đó:

$$P_{\Delta} = \int_0^T C_{\Delta}^2(t) dt = \int_0^T C_1^2(t) dt + \int_0^T C_2^2(t) dt$$

$$P_{\Delta} = P_1 + P_2 = 2P_c$$

$$\Rightarrow p_s = 1 - \phi\left(\sqrt{\frac{2P_c T}{2G_0}}\right)$$

$$p_s = 1 - \phi(h) \quad (5.36)$$

**c. Một trong hai tín hiệu triệt ( $C_2(t) = 0$ )**

Hệ này chính là hệ truyền tín hiệu phân có khoảng nghỉ thụ động.

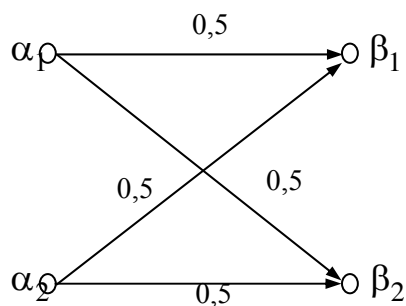
$$C_{\Delta}(t) = C_1(t) \Rightarrow P_{\Delta} = P_1 = 2P_c$$

$$\Rightarrow p_s = 1 - \phi(h) \quad (5.37)$$

**d. Các tín hiệu như nhau ( $C_1(t) = C_2(t)$ )**

$$C_{\Delta}(t) = 0 \Rightarrow P_{\Delta} = 0, \phi(0) = \frac{1}{2} \Rightarrow p_s = \frac{1}{2} = p_{s\max}$$

Như vậy, việc lặp lại các tín hiệu 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 ƯU 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 ( $\mu, \tau, \dots$ )
- 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  $\xi$  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  $\gamma_i$  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  $\gamma_1$ . Khi đó tín hiệu thứ  $K$  có tham số  $\gamma_1$  không biết sẽ ký hiệu là  $C_{K, \gamma_1}(t)$ . Trong trường hợp tổng quát, luật phân bố của  $\gamma_1$  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  $\gamma_1$  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  $\gamma_1$ , 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  $\gamma_1$ . Khi đó ta có:

$$p(C_K / u) = \int W(C_K, \gamma_1 / u) d\gamma_1 = b.p(C_K) \int W(\gamma_1 / C_K) W(u / C_K, \gamma_1) d\gamma_1 \quad (5.41)$$

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:

$$p(C_K / u) = b'.p(C_K) \int \dots \int W(\gamma_1, \gamma_2, \dots / C_K) \cdot W(u / C_K, \gamma_1, \gamma_2, \dots) d\gamma_1 d\gamma_2 \dots \quad (5.43)$$

$p(C_K)$  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 các định cấu trúc của máy thu tối ưu, ta sẽ phân tích (5.41) có kể đến quy tắc giải (5.42).

Giả sử rằng các tín hiệu phát có thời hạn  $T$  và pha đầu  $\varphi$  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  $\varphi$  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  $\varphi$  trong khoảng  $(0, T)$  được giữ không đổi và thay đổi ngẫu nhiên một cách độ lập khi chuyển từ khoảng quan sát này sang khoảng quan sát khác.

$$\text{Trước tiên ta sẽ xác định } W(u/C_{K,\varphi}) = W[n'(t) = u(t) - C_{K,\varphi}(t)].$$

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  $F_c \rightarrow \infty$

$$\begin{aligned} W(u/C_{K,\varphi}) &= \lim_{F_c \rightarrow \infty} W_n(n'_1, \dots, n'_n / 0) = \\ &= \frac{1}{(\sigma\sqrt{2\pi})^n} \lim_{F_c \rightarrow \infty} \exp \left\{ -\frac{1}{2\sigma^2/2F_c} \sum_{j=1}^n (U_j - C_{Kj})^2 \Delta t \right\} \end{aligned}$$

Trong đó  $\Delta t = \frac{1}{2F_c}$ ;  $\frac{\sigma^2}{F_c} = G_0$ . Khi  $F_c \rightarrow \infty$  thì  $\Delta t \rightarrow 0$ .

$$\Rightarrow W(u/C_{K,\varphi}) = \frac{1}{(\sigma\sqrt{2\pi})^n} \exp \left\{ -\frac{1}{G_0} \int_0^T [U(t) - C_{K,\varphi}(t)]^2 dt \right\}$$

$$W(u/C_{K,\varphi}) = b_1 \cdot e^{-\frac{E_K}{G_0}} \cdot \exp \left\{ \frac{2}{G_0} \int_0^T U(t) \left[ C_K(t) \cos \varphi + \hat{C}_K(t) \sin \varphi \right] dt \right\} \quad (5.45)$$

$$E_K = \int_0^T C_{K,\varphi}^2(t) dt$$

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:

$$\begin{aligned} q(k, \varphi) &= \cos \varphi \int_0^T U(t) C_K(t) dt + \sin \varphi \int_0^T U(t) \hat{C}_K(t) dt = \\ &= U_K \cos \varphi + V_K \sin \varphi \end{aligned}$$

$$\text{Ký hiệu } M_K = \sqrt{U_K^2 + V_K^2}, \quad \varphi_K = \arctg(V_K / U_K) \quad (5.46)$$

$$\text{Ta có thể viết: } q(k, \varphi) = M_K \cos(\varphi_K - \varphi) \quad (5.47)$$

Theo (5.41) ta tìm được:

$$\begin{aligned} p(C_K / u) &= b_1 \cdot \frac{p(C_K)}{2\pi} \cdot e^{-E_K / G_0} \int_0^{2\pi} e^{\frac{2}{G_0} M_K \cos(\varphi_K - \varphi)} d\varphi = \\ &= b_2 \cdot p(C_K) e^{-E_K / G_0} I_0\left(\frac{2M_K}{G_0}\right) \end{aligned} \quad (5.48)$$

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:

$$\ln p(C_K) - \frac{E_K}{G_0} + \ln I_0\left(\frac{2M_K}{G_0}\right) > \ln p(C_i) - \frac{E_i}{G_0} + \ln I_0\left(\frac{2M_i}{G_0}\right) \quad \forall i \neq k \quad (5.49)$$

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:

$$M_K > M_i \quad \forall i \neq k \quad (5.49')$$

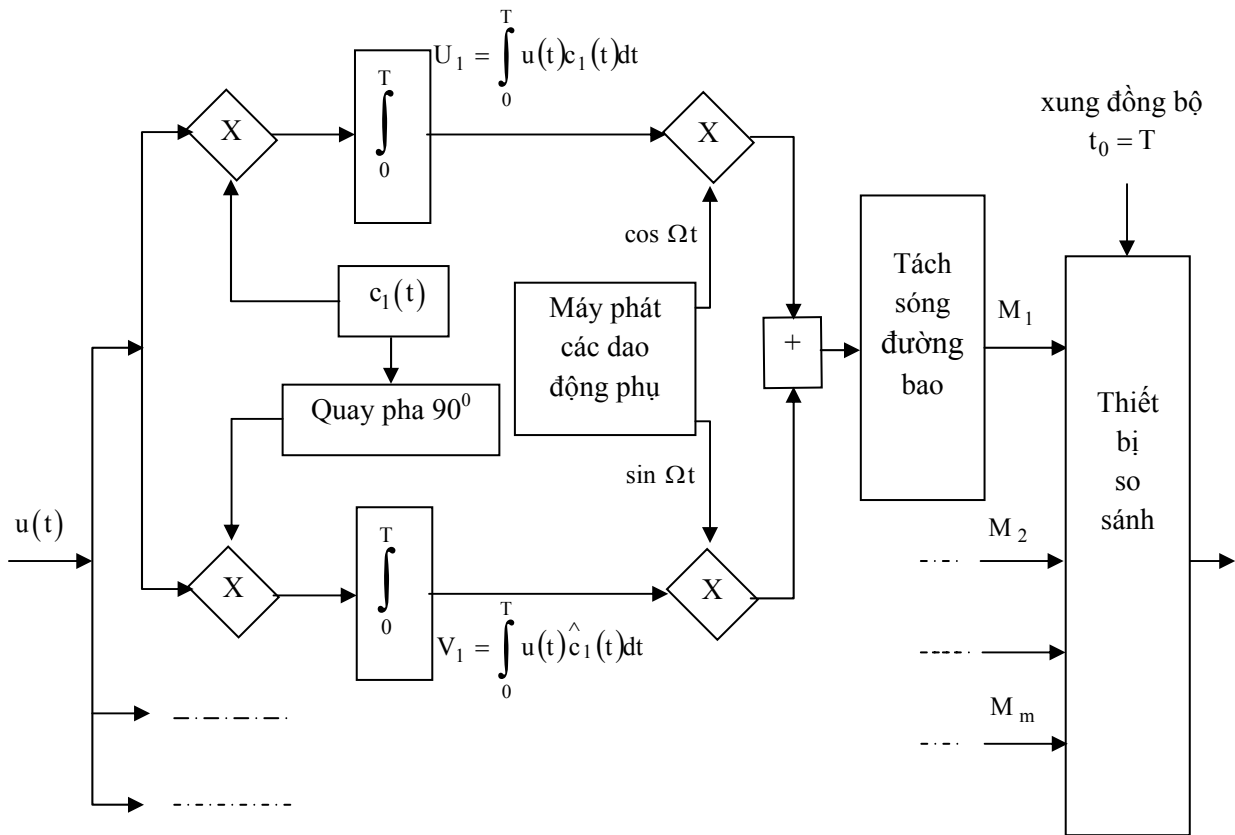
Rõ ràng là độ tin cậy của việc truyền càng cao nếu trong điều kiện không có nhiễu  $M_i$  và  $M_K$  càng khác nhau. Theo (5.46), giá trị  $M_i$  sẽ đạt cực tiểu bằng 0 nếu:

$$\int_0^T C_K(t) C_i(t) dt = 0; \int_0^T C_K(t) \hat{C}_i(t) dt = 0 \quad (5.50)$$

Các tín hiệu thoả mãn (5.50) sẽ được gọi là các tín hiệu trực giao theo nghĩa chặt. Các tín hiệu, các tín hiệu không giao nhau về thời gian,... là các tín hiệu trực giao theo nghĩa chặt.

Như vậy, khi pha bất định, các tín hiệu trực giao theo nghĩa chặt 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 thông tin dùng tín hiệu hai phân, trực giao (chặt), có nghi 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:

$$p_{s_{kh}} = \frac{1}{2} \exp \left\{ -\frac{h^2}{2} \right\} > p_{s_{kh}} = 1 - \Phi(h)$$

**Ví dụ 1:**

Khi  $h = 3$ :  $p_{s_{kh}} \approx 1,15 \cdot 10^{-3}$ ;  $p_{s_{kh}} \approx 5,55 \cdot 10^{-3}$ . 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  $p_s = 10^{-4}$ :  $h_{kh}=3,73$ ;  $h_{k_{kh}}=4,12$ . 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 xử 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 đầy đủ 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 KHÓI KHÔNG GIAN , THỜI GIAN (STBC).

### 5.6.1. Kỹ thuật thu phân tập.

Tín hiệu nhận được ở máy thu:

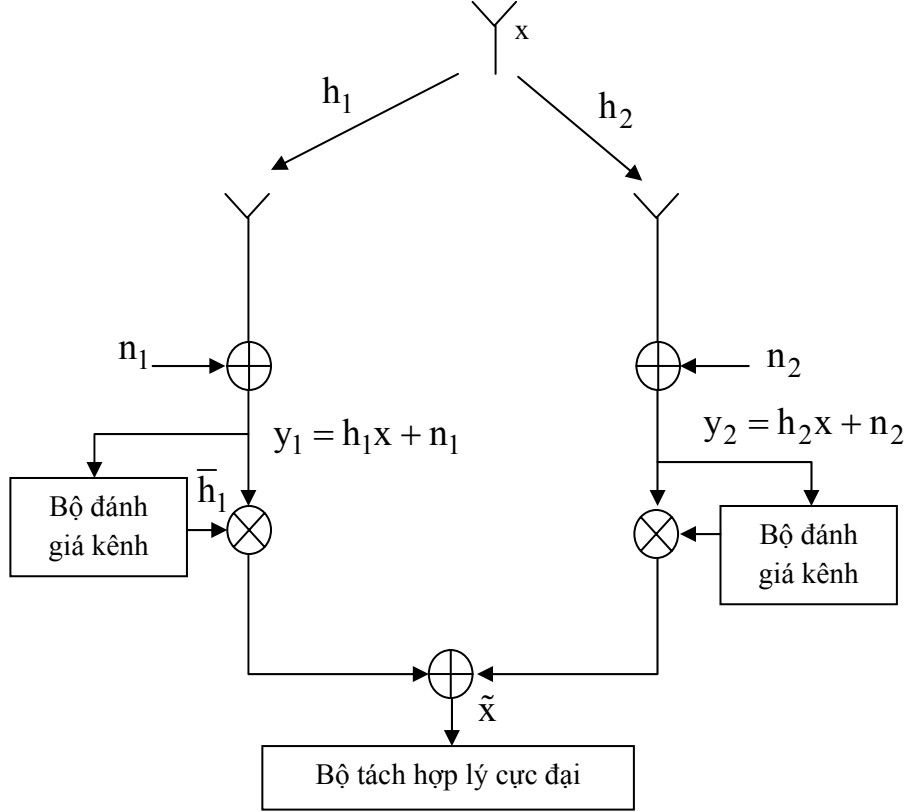
$$y_1 = h_1 x + n_1$$

$$y_2 = h_2 x + n_2$$

$$h_1 = |h_1| e^{j\theta_1} \quad h_2 = |h_2| e^{j\theta_2}$$

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:

$$\begin{aligned}\tilde{x} &= \bar{h}_1 y_1 + \bar{h}_2 y_2 \\ \tilde{x} &= \bar{h}_1 h_1 y_1 + \bar{h}_1 n_1 + \bar{h}_2 h_2 y_2 + \bar{h}_2 n_2 \\ &= (|h_1|^2 + |h_2|^2) x + \bar{h}_1 n_1 + \bar{h}_2 n_2\end{aligned}$$



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  $x_1$  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 khối không gian – thời gian dựa trên hai máy phát $G_2$

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:

$$G_2 = \begin{pmatrix} x_1 & x_2 \\ -\bar{x}_2 & \bar{x}_1 \end{pmatrix} \quad (5.53)$$

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  $Tx_1$ , đồng thời anten  $Tx_2$  cũng phát tín hiệu  $x_2$ , các tín hiệu  $-\bar{x}_2$  và  $\bar{x}_1$  được đồng thời phát từ các anten  $Tx_1$  và  $Tx_2$  (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 $G_2$ dùng một máy thu

Giả sử ta có:

$$h_1 = h_1(T=1) = h_1(T=2)$$

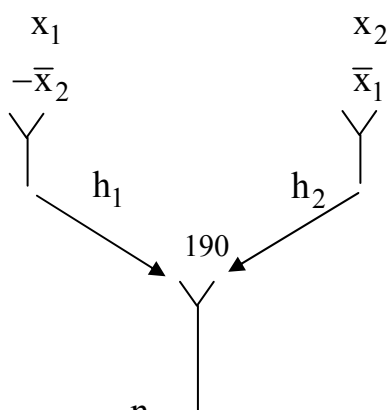
$$h_2 = h_2(T=1) = h_2(T=2)$$

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:

$$y_1 = h_1 x_1 + h_2 x_2 + n_1 \quad (5.54)$$

$$y_2 = -h_1 \bar{x}_2 + h_2 \bar{x}_1 + n_2 \quad (5.55)$$

$y_1$  sẽ nhận được trước tiên, sau đó là  $y_2$



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:

$$\begin{aligned}\tilde{x}_1 &= \bar{h}_1 y_1 + h_2 \bar{y}_2 \\ &= \bar{h}_1 h_1 x_1 + \bar{h}_1 h_2 x_2 + \bar{h}_1 n_1 - h_2 \bar{h}_1 x_2 + h_2 \bar{h}_2 \bar{x}_1 + h_2 \bar{n}_2 \\ &= \left( |h_1|^2 + |h_2|^2 \right) x_1 + \bar{h}_1 n_1 + h_2 \bar{n}_2\end{aligned}\quad (5.56)$$

Tương tự, đối với tín hiệu  $x_2$  ta thực hiện như sau:

$$\begin{aligned}\tilde{x}_2 &= \bar{h}_2 y_1 + h_1 \bar{y}_2 \\ &= \bar{h}_2 h_1 x_1 + \bar{h}_2 h_2 x_2 + \bar{h}_2 n_1 + h_1 \bar{h}_1 x_2 - h_1 \bar{h}_2 x_1 - h_1 \bar{n}_2 \\ &= \left( |h_1|^2 + |h_2|^2 \right) x_2 + \bar{h}_2 n_1 - h_1 \bar{n}_2\end{aligned}\quad (5.57)$$

Từ (5.56) và (5.57) ta có thể thấy rằng ta đã tách được các tín hiệu  $x_1$  và  $x_2$  bằng các 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  $Rx_1$  ta có:

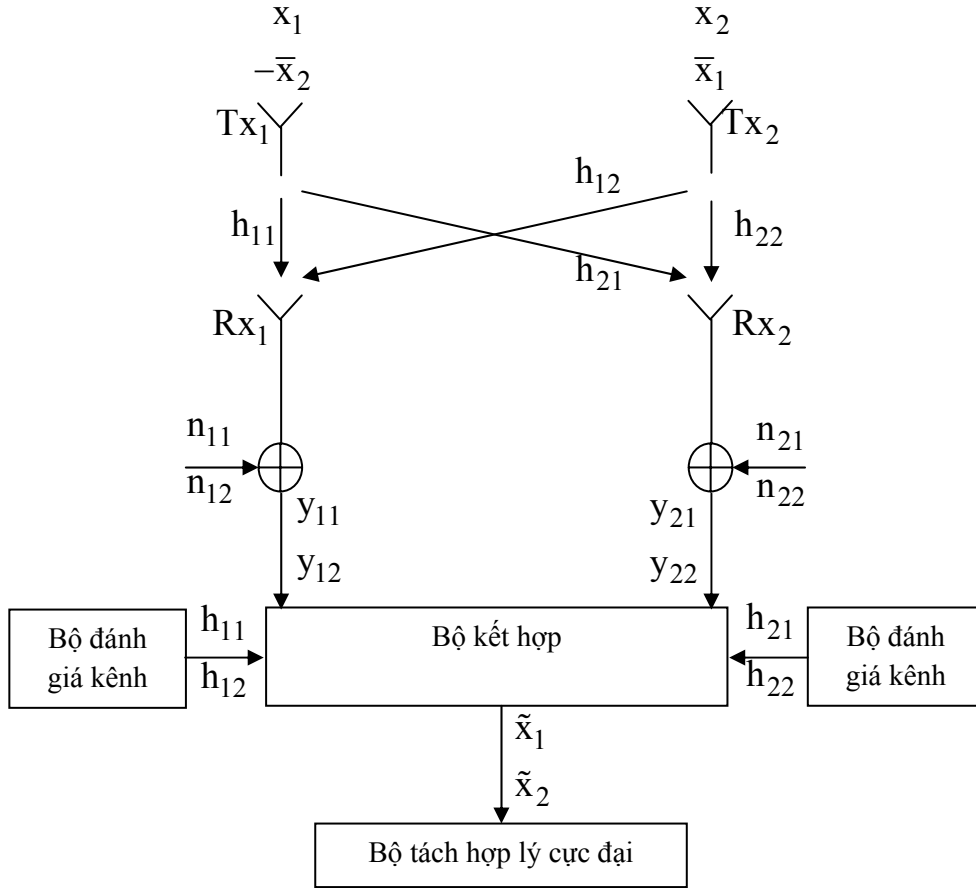
$$y_{11} = h_{11}x_1 + h_{12}x_2 + n_{11} \quad (5.58)$$

$$y_{12} = -h_{11}\bar{x}_2 + h_{12}\bar{x}_1 + n_{12} \quad (5.59)$$

Ở máy thu thứ hai  $Rx_2$  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:

$$\begin{aligned} y_{i1} &= h_{i1}x_1 + h_{i2}x_2 + n_{i1} \\ y_{i2} &= -h_{i1}\bar{x}_2 + h_{i2}\bar{x}_1 + n_{i2} \end{aligned} \quad i = \overline{1, q}$$

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:

$$\begin{aligned} \tilde{x}_1 = & \left( |h_{11}|^2 + |h_{12}|^2 + |h_{21}|^2 + |h_{22}|^2 \right) x_1 + \\ & + \bar{h}_{11}n_{11} + h_{12}\bar{n}_{12} + \bar{h}_{21}n_{21} + h_{22}\bar{n}_{22} \end{aligned} \quad (5.64)$$

$$\begin{aligned} \tilde{x}_2 = & \left( |h_{11}|^2 + |h_{12}|^2 + |h_{21}|^2 + |h_{22}|^2 \right) x_2 + \\ & + \bar{h}_{12}n_{11} - h_{11}\bar{n}_{12} + \bar{h}_{22}n_{21} - h_{21}\bar{n}_{22} \end{aligned} \quad (5.65)$$

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 pha định là  $|h_{i1}|^2 + |h_{i2}|^2$ . 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 pha định tức là có hai đường độc lập để phát cho đầu  $x_1$ . 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 biên 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:  $\xi(t) = X(t)\cos\omega_0 t + Y(t)\sin\omega_0 t$ , 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 maníp điều biên:

$$\left. \begin{aligned} S_1(t, \varphi_1) &= U_m \cos(\omega_0 t + \varphi_1) \\ S_2(t, \varphi_2) &= 0 \end{aligned} \right\} 0 \leq t \leq T$$

Pha đầu  $\varphi_1$  là một đại lượng ngẫu nhiên, phân bố đều trong khoảng  $[-\pi, \pi]$ . Tham số  $\lambda$  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:

- Ngưỡng tối ưu  $H_0$  để đảm bảo cực tiểu hoá xác suất sai tổng cộng.
- Xác suất sai tổng 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 độ lập với  $n(t)$  và có dạng:

$$s(t) = \begin{cases} A \cdot e^{A(t-T)} & t \leq T \\ 0 & t > T \end{cases}$$

Tìm hàm truyền của bộ lọc sao cho tỷ số tín trên tạp ở đầu ra của bộ lọc đạt cực đại. Tính  $a = \frac{s_{\text{ra max}}(t)}{\sigma_{\text{ra}}}$ .

**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  $\tau_x$  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.** Chứng minh rằng máy thu tối ưu đảm bảo khoảng cách từ vector tín hiệu nhận được tới vector 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 phổ:

$$S_n(f) = G_0/2$$

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  $\tau_x$  và giải thông tạp âm của mạch  $\Delta f_n$ .

b. Tìm sự phụ thuộc giữa  $\tau_x$  và giải năng lượng tạp âm tối ưu của mạch để trị số  $a$  đạt max.

## PHỤ LỤC

### BẤT ĐẲNG THỨC BUNHIACOVSKI-SCHWAZT

**Định lý:** Nếu  $F(x)$  và  $\varphi(x)$  là các hàm phức thỏa mãn điều kiện:

$$\int_{-\infty}^{\infty} |F(x)|^2 dx < \infty \quad \int_{-\infty}^{\infty} |\varphi(x)|^2 dx < \infty \quad (x \text{ biến thực})$$

thì ta có:

$$\left| \int_{-\infty}^{\infty} F(x)\varphi(x)dx \right|^2 \leq \int_{-\infty}^{\infty} |F(x)|^2 dx \cdot \int_{-\infty}^{\infty} |\varphi(x)|^2 dx$$

**Chứng minh:**

$$\text{Đặt } \phi(x) = \frac{\varphi^*(x)}{\sqrt{\int_{-\infty}^{\infty} |\varphi(x)|^2 dx}} \quad (a)$$

(Dấu \* là ký hiệu liên hợp phức)

$$\text{và } \alpha = \int_{-\infty}^{\infty} \varphi^*(x)F(x)dx \quad (b)$$

$$\text{Ta có: } [F(x) - \alpha\phi(x)][F^*(x) - \alpha^*\phi^*(x)] = |F(x) - \alpha\phi(x)|^2 \geq 0 \quad (c)$$

$$\text{Theo (a) ta có: } \int_{-\infty}^{\infty} |\phi(x)|^2 dx = 1$$

$$\text{Theo (b) ta có: } \int_{-\infty}^{\infty} \phi(x)F^*(x)dx = \alpha^*$$

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:

$$\int_{-\infty}^{\infty} |F(x)|^2 dx \geq \frac{\left| \int_{-\infty}^{\infty} \phi(x) F(x) dx \right|^2}{\int_{-\infty}^{\infty} |\phi(x)|^2 dx}$$

## BIẾN ĐỔI 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 phổ:

$$\hat{S}(j\omega) = S(j\omega) e^{-j\frac{\pi}{2} \text{sign } \omega}$$

(tất cả các thành phần phổ  $\hat{s}(t)$  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:

$$\hat{S}(j\omega) = S(j\omega) e^{-j\frac{\pi}{2} \text{sign } \omega} = S(j\omega) \left[ \cos\left(\frac{\pi}{2} \text{sign } \omega\right) - j \sin\left(\frac{\pi}{2} \text{sign } \omega\right) \right]$$

$$\text{Trong đó: } \text{sign } \omega = \begin{cases} 1 & \text{khi } \omega > 0 \\ 0 & \omega = 0 \\ -1 & \omega < 0 \end{cases}$$

$$\cos\left(\frac{\pi}{2} \text{sign } \omega\right) = \begin{cases} 1 & \text{khi } \omega > 0 \\ 0 & \omega = 0 \\ -1 & \omega < 0 \end{cases}$$

$$\sin\left(\frac{\pi}{2}\text{sign}\omega\right) = \text{sign}\omega$$

Theo biến đổi ngược Fourier ta có:

$$\hat{s}(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{S}(j\omega) e^{j\omega t} d\omega = -\frac{1}{2\pi} \int_{-\infty}^{\infty} j \text{sign}\omega S(j\omega) e^{j\omega t} d\omega \quad (a)$$

$$(\text{Để ý rằng } \frac{1}{2\pi} \int_{-\infty}^{\infty} S(j\omega) \cos\left(\frac{\pi}{2}\text{sign}\omega\right) e^{j\omega t} d\omega = 0)$$

Mặt khác ta có:

$$\begin{aligned} \int_{-\infty}^{\infty} \frac{e^{-j\omega\tau}}{\tau} d\tau &= \underbrace{\int_{-\infty}^{\infty} \frac{\cos\omega\tau}{\tau} d\tau}_0 - \int_{-\infty}^{\infty} \frac{\sin\omega\tau}{\tau} d\tau \\ \Rightarrow \int_{-\infty}^{\infty} \frac{e^{-j\omega\tau}}{\tau} d\tau &= -2j \int_0^{\infty} \frac{\sin\omega\tau}{\tau} d\tau = -2j \text{sign}\omega \int_{-\infty}^{\infty} \frac{\sin x}{x} dx \end{aligned}$$

$$\text{Vì } \int_{-\infty}^{\infty} \frac{\sin x}{x} dx = \frac{\pi}{2} \text{ nên ta có: } \int_{-\infty}^{\infty} \frac{e^{-j\omega\tau}}{\tau} d\tau = -j\pi \quad (b)$$

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 KACHENNHICOV

**Định lý:** Nếu phổ 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:

$$s_{\Delta}(t) = s(t) \cdot \delta_{\Delta}(t) \quad (\text{hình C.1.c}) \quad (a)$$

$$\delta_{\Delta}(t) = \sum_{n=-\infty}^{\infty} \delta(t - n\Delta t) \quad (\text{hình C.1.b}) \quad (b)$$

$$\Delta t = \frac{1}{F_0} \leq \frac{1}{2F_m} \quad ; \quad \omega_0 = 2\pi F_0 \quad ; \quad \omega_m = 2\pi F_m$$

$\delta_{\Delta}(t)$  là một hàm tuần hoàn có chu kỳ  $\Delta t$ , 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 dãy 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 phổ của  $\delta_{\Delta}(t)$  dưới dạng sau:

$$\dot{\int}_{\delta_{\Delta}}(\omega) = \frac{2\pi}{\Delta t} \sum_{n=-\infty}^{\infty} \delta(\omega - n\omega_0) \quad (\text{Hình C.1.e}) \quad (c)$$

Theo tính chất của biến đổi Fourier phổ của  $s_{\Delta}(t)$  được tính theo tích chập sau:



$$\dot{S}_{\Delta}(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \dot{S}(u) \int_{\delta_{\Delta}} (\omega - u) du$$

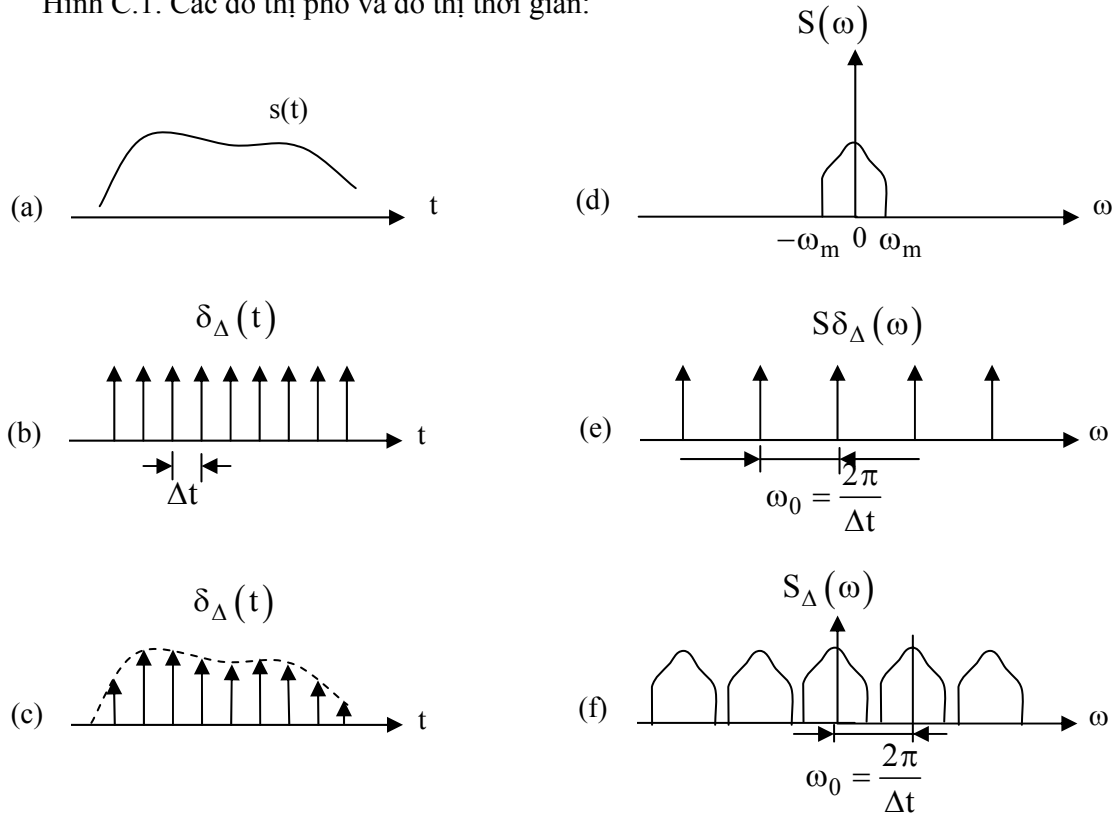
Trong đó:  $\dot{S}(\omega)$  là phổ của  $s(t)$

$$\begin{aligned} \dot{S}_{\Delta}(\omega) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \dot{S}(u) \cdot \frac{2\pi}{\Delta t} \sum_{n=-\infty}^{\infty} \delta[(\omega - n\omega_0) - u] du \\ &= \frac{1}{\Delta t} \sum_{n=-\infty}^{\infty} \int_{-\infty}^{\infty} \dot{S}(u) \cdot \delta[(\omega - n\omega_0) - u] du \end{aligned}$$

Theo tính chất lọc của  $\delta$  ta có:

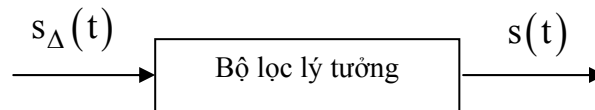
$$\dot{S}_{\Delta}(\omega) = \frac{1}{\Delta t} \sum_{n=-\infty}^{\infty} \dot{S}(\omega - n\omega_0) \quad (\text{Hình C.1.f}) \quad (d)$$

Hình C.1. Các đồ thị phổ và đồ thị thời gian:



Hình C.1

Từ (d) và hình C.1 ta thấy rằng phổ của  $S_{\Delta}(t)$  lặp lại một cách tuần hoàn dạng phổ của  $s(t)$ . Dùng một bộ lọc có đặc tính tần số dạng chữ nhật lý tưởng (đường đứt 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:  $w(x) = \phi'(x) = \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{t^2}{2}\right\}$

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**

$x_i$	$\log_2 x_i$	$x_i$	$\log_2 x_i$	$x_i$	$\log_2 x_i$	$x_i$	$\log_2 x_i$
	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

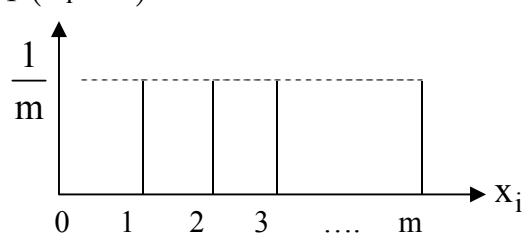
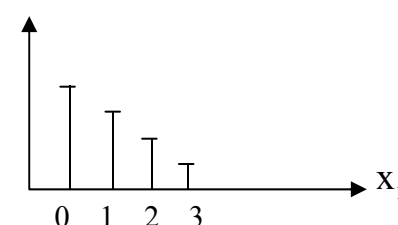
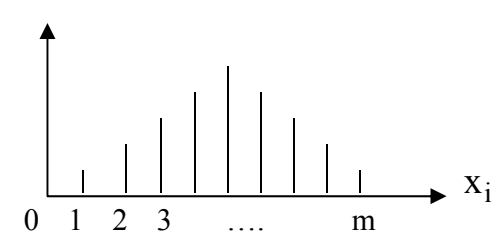
**HÀM  $\gamma(p) = -p \log_2 P$ , HÀM  $\phi(p) = -(1-p) \log_2 (1-p)$ , HÀM  $\log_2 p$  VÀ ENTROPIE CỦA NGUỒN NHỊ PHÂN  $H(A) = \gamma(p) + \phi(p)$**

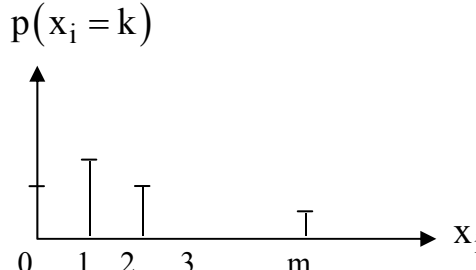
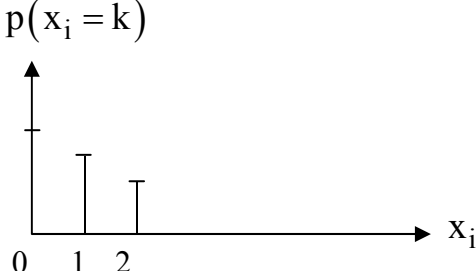
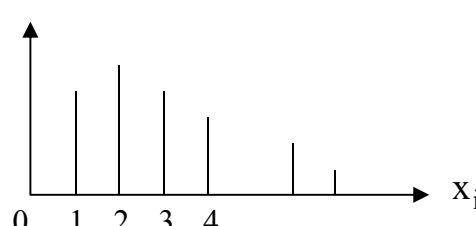
p	$-\log_2 p$	$\gamma(p)$	$H(A)$	$\phi(p)$	$-\log_2 (1-p)$	$(1-p)$
	6,643	0,066	0,081	0,014	0,014	0,99
	5,644	0,113	0,141	0,028	0,029	0,98
	5,059	0,152	0,194	0,042	0,044	0,97
	4,644	0,186	0,242	0,056	0,059	0,96
	4,322	0,216	0,286	0,070	0,074	0,95
	4,059	0,243	0,327	0,084	0,089	0,94
	3,936	0,268	0,366	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	$-\log_2 p$	$\gamma(p)$	$H(A)$	$\phi(p)$	$-\log_2 (1-p)$	$(1-p)$
---	-------------	-------------	--------	-----------	-----------------	---------

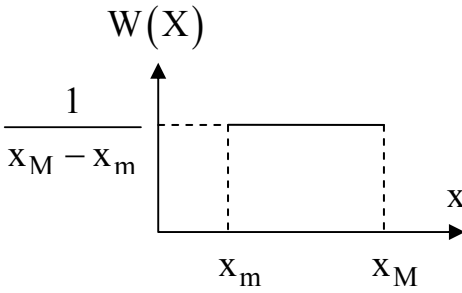
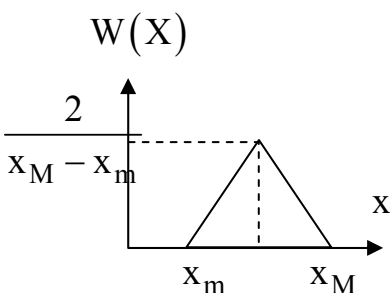
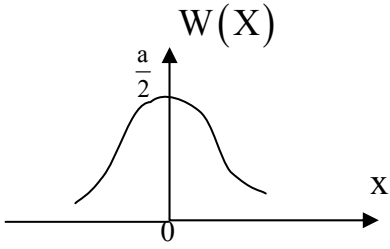
1,943	0,505	0,827	0,321	0,434	0,74
1,889	0,510	0,841	0,331	0,454	0,73
1,836	0,514	0,855	0,341	0,474	0,72
1,786	0,518	0,869	0,351	0,494	0,71
1,737	0,521	0,881	0,360	0,514	0,70
1,690	0,524	0,893	0,369	0,535	0,69
1,644	0,526	0,904	0,378	0,556	0,68
1,599	0,528	0,915	0,387	0,578	0,67
1,556	0,529	0,925	0,396	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	$p(x_i = K) = \begin{cases} C_m^k p^k (1-p)^{m-k} & 0 \leq x_i \leq m \\ 0 & 0 > x_i > m \end{cases}$ $p(x_i = k)$ 	$H(X) = -m[p \log p - (1-p) \log (1-p)] -$ $- \sum_{k=1}^{m-1} C_m^k p^k (1-p)^{m-k} \log C_m^k$

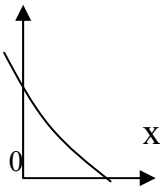
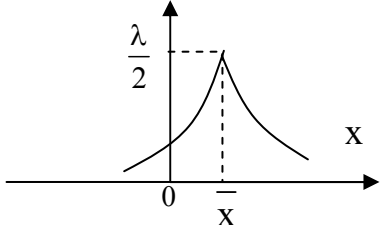
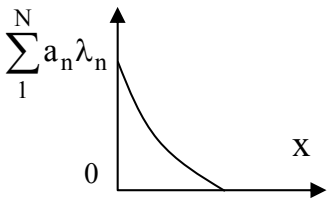
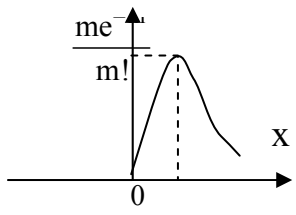
<p>4. Phân bố siêu bội</p>	$p(x_i = K) = \begin{cases} \frac{C_m^k C_{N-m}^{r-k}}{C_N^r} & 0 \leq x_i \leq m \\ 0 & 0 > x_i > m \end{cases}$ 	$H(X) = \log C_N^r - \frac{1}{C_N^r} \cdot \sum_{k=1}^{m-1} C_m^k C_{N-m}^{r-k} \log C_m^k - \frac{1}{C_N^r} \sum_{k=1}^{m-1} C_m^k C_{N-m}^{r-k} \log C_{N-m}^{r-k}$
<p>5. Phân bố Poisson</p>	$p(x_i = k) = \begin{cases} \frac{\lambda^k}{K!} e^{-\lambda} & x_i > 0 \\ 0 & x_i \leq 0 \end{cases}$ 	$H(X) = \lambda \log \frac{e}{\lambda} + \sum_{k=1}^{\infty} \frac{\lambda^k e^{-\lambda}}{K!} \log(K!)$
<p>6. Phân bố Polya</p>	$P(x_i = K) = \begin{cases} P_0 \left( \frac{\lambda}{1 + \alpha \lambda} \right)^k \cdot \frac{(1 + \alpha) \dots [1 + (k-1)\alpha]}{K!} & x_i > 0 \\ 0 & x_i \leq 0 \end{cases}$ $P^0 = p(0) = (1 + \alpha \lambda)^{-\frac{1}{\alpha}}$ 	$H(x') = -\lambda \log \lambda + \frac{1 + \alpha \lambda}{\alpha} \cdot \log(1 + \alpha \lambda) - \sum_{k=1}^{\infty} P_0 \cdot \left( \frac{\lambda}{1 + \alpha \lambda} \right)^k \cdot \frac{1(1 + \alpha) \dots [1 + (K-1)\alpha]}{K!} \cdot \log \frac{1(1 + \alpha) \dots [1 + (K-1)\alpha]}{K!}$

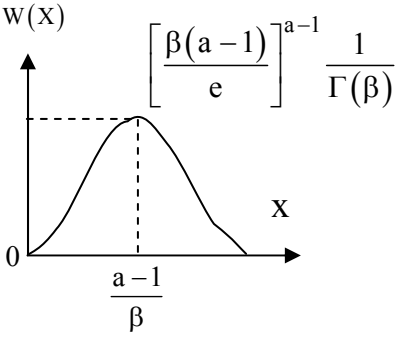
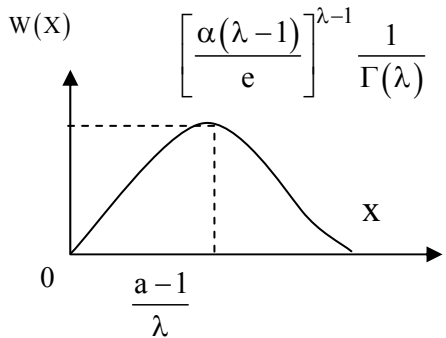
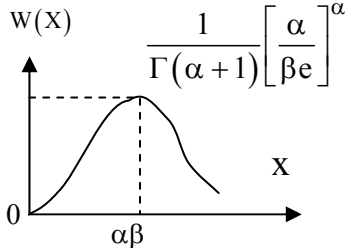
**ENTRIPIE VI PHÂN  $H(X)$  CỦA CÁC LUẬT PHÂN BỐ LIÊN TỤC.**

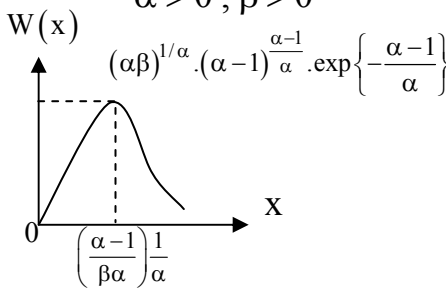
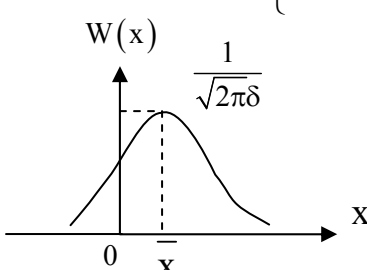
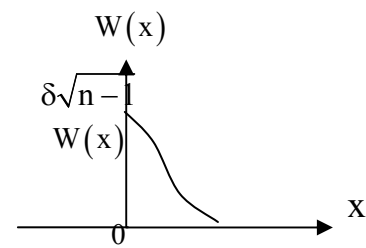
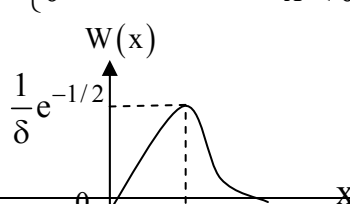
Luật phân bố	Biểu thức giải tích và đồ thị	Entropie $H(X)$
1. Phân bố đều	$W(X) = \begin{cases} \frac{1}{x_M - x_m} & x \in [x_m, x_M] \\ 0 & x \notin [x_m, x_M] \end{cases}$ 	$H(X) = \log m$
2. Phân bố tam giác (Simson)	$W(X) = \begin{cases} \frac{4(x - x_m)}{(x_M - x_m)^2} & x \in \left[x_m, \frac{x_m + x_M}{2}\right] \\ \frac{4(x_M - x)}{(x_M - x_m)^2} & x \in \left[\frac{x_m + x_M}{2}, x_M\right] \\ 0 & x \notin [x_m, x_M] \end{cases}$ 	$h(x) = \log \frac{(x_M - x_m)\sqrt{e}}{2}$
3. Phân bố $\text{sech}^2 x$	$W(x) = \frac{a}{2\text{ch}^2 x} = \frac{a}{2} \text{sech}^2 x$ 	$h(x) = \log \frac{e^2}{2a}$

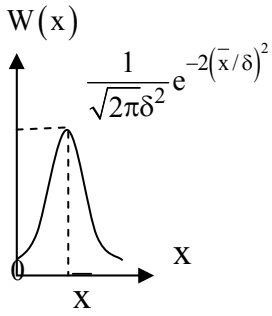
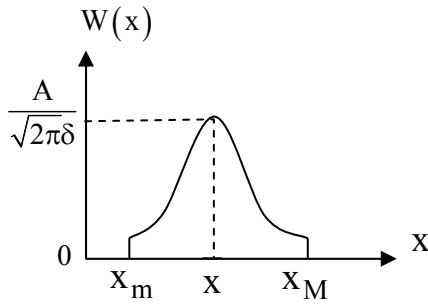
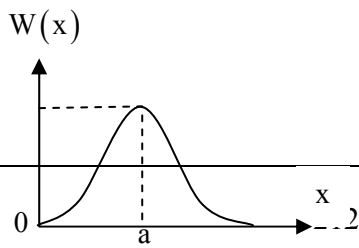


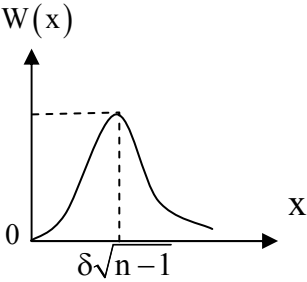
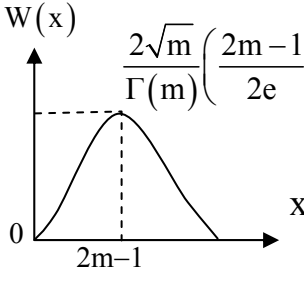
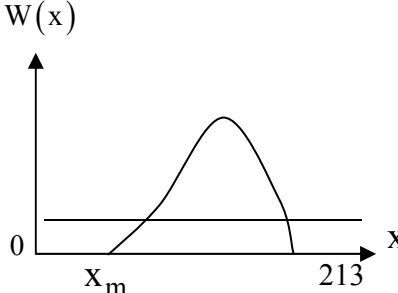
<p>4. Phân bố arcsin x</p>	$W(x) = \begin{cases} \frac{1}{\pi} \cdot \frac{1}{\sqrt{a^2 - x^2}} & x \in (-a, a) \\ 0 & -a > x > a \end{cases}$	$h(x) = \log \pi + \frac{1}{\pi} + \frac{1}{\pi} \int_0^1 \frac{\log(a^2 - x^2)}{\sqrt{a^2 - x^2}} dx$
<p>5. Phân bố Cauchy</p>	$W(x) = \frac{a}{\pi} \cdot \frac{1}{(x - \bar{x})^2 + a^2}$	$h(x) = \log 4\pi a$
<p>6. Phân bố Maxweel</p>	$W(x) = \begin{cases} \frac{4}{\sqrt{\pi}(2\delta^2)^{3/2}} x^2 \cdot e^{-x^2/2\delta^2} & x > 0 \\ 0 & x < 0 \end{cases}$	$h(x') = \left[ \frac{1}{2} \log \frac{2\pi\delta^2}{e} + C \log e \right]$ <p><math>C \approx 0,5772</math></p> <p>(C – Số Euler)</p>

<p>7. Phân bố mũ một phía</p>	$W(x) = \begin{cases} \lambda e^{-\lambda x} & x > 0 \\ 0 & x < 0 \end{cases}$ <p style="text-align: center;"><math>w(x)</math></p> 	$h(x) = \log -\frac{e}{\lambda}$
<p>8. Phân bố Laplace (phân bố mũ hai phía)</p>	$W(x) = \frac{\lambda}{2} e^{-\lambda  x - \bar{x} }$ <p style="text-align: center;"><math>w(x)</math></p> 	$h(x) = \log \frac{2e}{\lambda}$
<p>9. Phân bố siêu mũ</p>	$W(x) = \begin{cases} \sum_{n=1}^N a_n \lambda_n e^{-\lambda_n x} & x > 0 \\ 0 & x < 0 \end{cases}$ <p style="text-align: center;"><math>w(x)</math></p> 	$h(x) = -\sum_{n=1}^N a_n \lambda_n \int_0^{\infty} e^{-\lambda_n x} \cdot \log \sum_{n=1}^N a_n \lambda_n e^{-\lambda_n x} dx$
<p>10. Phân bố mũ – lũy thừa</p>	$W(x) = \begin{cases} \frac{x^m}{m!} e^{-x} & x > 0 \\ 0 & x < 0 \end{cases}$ <p style="text-align: center;"><math>w(x)</math></p> 	$h(x) = \log m! + \log e - e - m \log e \left[ \sum_{k=2}^m \frac{1}{k} - C \right]$ <p style="text-align: center;"><math>C \approx 0,5772</math> (C – Số Euler)</p>

<p>11. Phân bố Erlang</p>	$W(x) = \begin{cases} \frac{\beta^a x^{a-1}}{(a-1)!} e^{-\beta x} & x > 0 \\ 0 & x < 0 \end{cases}$ $a = 1, 2, 3, \dots$ 	$h(x) = \log[(a-1)!] - \log \beta + \left\{ a - (a-1) [\ln \Gamma(a)]' \right\} \log e$ $[\ln \Gamma(a)]' = \psi(a)$ <p><math>\psi(a)</math> - Hàm psi của Euler</p>
<p>12. Phân bố Pearsom</p>	$W(x) = \begin{cases} \frac{\alpha^\lambda x^{\lambda-1}}{\Gamma(\lambda)} e^{-\beta x} & x > 0 \\ 0 & x < 0 \end{cases}$ $\lambda = \frac{n}{2} \quad (n = 1, 2, 3, \dots)$ 	$h(x) = -\log \Gamma(\lambda) - \log \alpha + \left\{ \lambda - (\lambda-1) [\ln \Gamma(\lambda)]' \right\} \log e$ $[\ln \Gamma(\lambda)]' = \psi(\lambda)$
<p>13. Phân bố Gamma</p>	$W(x) = \begin{cases} \frac{1}{\beta^{\alpha+1} \Gamma(\alpha+1)} x^\alpha e^{-x/\beta} & x > 0 \\ 0 & x < 0 \end{cases}$ $\alpha > -1, \beta > 0$ 	$h(x) = \log \Gamma(\alpha+1) - \alpha \log e$ $[\ln \Gamma(\alpha+1)]' + (\alpha+1) \log e + \log \beta$ $[\ln \Gamma(\alpha+1)]' = \psi(\alpha+1)$

<p>14. Phân bố Weibull</p>	$W(x) = \begin{cases} \alpha \beta x^{\alpha-1} e^{-\beta x^\alpha} & x > 0 \\ 0 & x < 0 \end{cases}$ <p><math>\alpha &gt; 0, \beta &gt; 0</math></p> 	$h(x) = \log e \left[ 1 + \frac{\alpha-1}{\alpha} (C + \ln \beta) \right] - \log \alpha \beta$ <p><math>C \approx 0,5772</math></p>
<p>15. Phân bố chuẩn</p>	$W(x) = \frac{1}{\sqrt{2\pi}\delta} \cdot \exp \left\{ -\frac{(x - \bar{x})^2}{2\delta^2} \right\}$ 	$h(x) = \log \left[ \delta \sqrt{2\pi e} \right]$
<p>16. Phân bố chuẩn một phía</p>	$W(x) = \begin{cases} \sqrt{\frac{2}{\pi}} \frac{1}{\delta} \exp \left\{ -\frac{x^2}{2\delta^2} \right\} & x > 0 \\ 0 & x < 0 \end{cases}$ 	$h(x) = \log \left[ \delta \sqrt{\frac{\pi e}{2}} \right]$
<p>17. Phân bố Rayleigh</p>	$W(x) = \begin{cases} \frac{x}{\delta^2} \exp \left\{ -\frac{x^2}{2\delta^2} \right\} & x > 0 \\ 0 & x < 0 \end{cases}$ 	$h(x) = \left( \frac{C}{2} + 1 \right) \log e$ <p><math>C \approx 0,5772</math></p>

<p>18. Phân bố modul của đại lượng ngẫu nhiên phân bố chuẩn</p>	$W(x) = \begin{cases} \frac{1}{\sqrt{2\pi}\delta} \left[ e^{-\frac{(x-\bar{x})^2}{2\delta^2}} + e^{-\frac{(x+\bar{x})^2}{2\delta^2}} \right] & x > 0 \\ 0 & x < 0 \end{cases}$ 	$h(x) = \log \left[ \delta \sqrt{\frac{\pi e}{2}} \right]$
<p>19. Phân bố chuẩn cực</p>	$W(x) = \begin{cases} \frac{1}{\sqrt{2\pi}\delta} \left[ e^{-\frac{(x-\bar{x})^2}{2\delta^2}} + e^{-\frac{(x+\bar{x})^2}{2\delta^2}} \right] & x \in [x_m, x_M] \\ 0 & x \notin [x_m, x_M] \end{cases}$ $A = \frac{1}{\frac{1}{\sqrt{2\pi}} \left[ \int_0^{(x_M-\bar{x})} e^{-t^2/2} dt - \int_0^{(x_m-\bar{x})\delta} e^{-t^2/2} dt \right]}$ 	$h(x) = \log \left[ \frac{\sqrt{2\pi}\delta}{A} \right] + \frac{1}{2} \left[ 1 - A \frac{x_M - \bar{X}}{\delta} \cdot \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{(x_M - \bar{X})^2}{2\delta^2}} - \right. \\ \left. - A \frac{x_m - \bar{X}}{\delta} \cdot \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{(x_m - \bar{X})^2}{2\delta^2}} \right] \log e$
<p>20. Phân bố loga chuẩn</p>	$W(x) = \begin{cases} \frac{1}{x\delta\sqrt{2\pi}} \frac{(\ln x - a)^2}{2\delta^2} & x > 0 \\ 0 & x < 0 \end{cases}$ 	$h(x) = \log \left[ \delta e^a \sqrt{2\pi e} \right]$

<p>21. Phân bố modul của véctor nhiều chiều</p>	$W(x) = \begin{cases} \frac{2x^{n-1} \exp\left\{-\frac{x^2}{2\delta^2}\right\}}{(2\delta^2)^{n/2} \Gamma\left(\frac{n}{2}\right)} & x > 0 \\ 0 & x < 0 \end{cases}$ $n = 1, 2, 3, \dots$ 	$h(x) = \log \frac{\delta e^{\frac{n}{2}} \Gamma\left(\frac{n}{2}\right)}{\sqrt{2}} - \frac{n-1}{2} \log \Gamma\left(\frac{n}{2}\right)$
<p>22. Phân bố nakagami</p>	$W(x) = \begin{cases} \frac{2m^m x^{2m-1} \exp\left\{-\frac{mx^2}{\delta^2}\right\}}{\Gamma(m) \delta^{2m}} & x > 0 \\ 0 & x < 0 \end{cases}$ 	$h(x) = \log \frac{\Gamma(m) \delta e^m}{2\sqrt{m}} - \frac{2m-1}{2} [\log \Gamma(m)]$
<p>Phân bố Beta</p>	$W(X) = \begin{cases} \frac{12}{(x_M - x_m)^4} (x - x_m)(x_M - x)^2 & x \in [x_m, x_M] \\ 0 & x \notin [x_m, x_M] \end{cases}$ 	$h(x) \approx 1,44 \ln \frac{(x_M - x_m)}{1,26}$

	$x_M$	
--	-------	--

## CÁC ĐA THỨC TỐI TIỂU CỦA CÁC PHẦN TỬ TRONG TRƯỜNG $GF(2^m)$ .

Sau đây là danh sách các đa thức tối tiểu 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: Fuldamentals and Applications. Prentice Hall.  
2004.
- [9] Moon T.K. Error correction coding. Mathematical Methods and Algorithms. Jhon Wiley  
and Son 2005.

## MỤC LỤC

<b>LỜI NÓI ĐẦU .....</b>	<b>1</b>
<b>CHƯƠNG I: NHỮNG VẤN ĐỀ CHUNG VÀ NHỮNG KHÁI NIỆM CƠ BẢN.....</b>	<b>3</b>
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
<b>CHƯƠNG II: TÍN HIỆU VÀ NHIỄU .....</b>	<b>11</b>
2.1. TÍN HIỆU XÁC ĐỊNH VÀ CÁC ĐẶC TRƯNG VẬT LÝ CỦA CHÚNG .....	11
2.2. TÍN HIỆU VÀ NHIỄU 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 TRƯNG THỐNG KÊ CỦA TÍN HIỆU NGẪU NHIÊN VÀ NHIỄU .....	13
2.3.1. Các đặc trưng thống kê .....	13
2.3.2. Khoảng tương quan.....	15
2.4. CÁC ĐẶC TRƯNG VẬT LÝ CỦA TÍN HIỆU NGẪU NHIÊN VÀ NHIỄU. BIẾN ĐỔI WIENER – KHINCHIN .....	16
2.4.1. Những khái niệm xây dựng lý thuyết phổ của quá trình ngẫu nhiên - mật độ phổ công suất.....	16
2.4.2. Cặp biến đổi Wiener – Khinchin .....	18
2.4.3. Bề rộng phổ 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 DIỄN PHỨC CHO THỂ HIỆN CỦA TÍN HIỆU NGẪU NHIÊN – TÍN HIỆU GIẢI HẸP .....	31
2.6.1. Cặp biến đổi Hilbert và tín hiệu giải tích .....	31
2.6.2. Tín hiệu giải rộng và giải hẹp .....	35

2.7. BIỂU DIỄN HÌNH HỌC CHO THỂ HIỆN CỦA TÍN HIỆU NGẪU 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
<b>CHƯƠNG 3 - CƠ SỞ LÝ THUYẾT THÔNG TIN THỐNG KÊ .....</b>	<b>47</b>
3.1. THÔNG TIN - LƯỢNG 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. ENTROPIE VÀ CÁC TÍNH CHẤT CỦA ENTROPIE .....	52
3.2.1. Tính chất thống kê của nguồn rời rạc và sự ra đời của khái niệm entropie.....	52
3.2.2. Định nghĩa entropie của nguồn rời rạc .....	52
3.2.3. Các tính chất của entropie một chiều của nguồn rời rạc .....	53
3.2.4. Entropie của nguồn rời rạc, nhị phân .....	55
3.2.5. Entropie của trường sự kiện đồng thời .....	56
3.3. ENTROPIE CÓ ĐIỀU KIỆN. LƯỢNG THÔNG TIN CHÉO TRUNG BÌNH.....	57
3.3.1. Entropie có điều kiện về một trường tin này khi đã rõ một tin nhất định của trường tin kia .....	57
3.3.2. Entropie 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 entropie 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 THỪA. KHẢ NĂNG THÔNG QUA CỦA KÊNH RỜI 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 nhớ, 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 NHỚ .....	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 hoạ sự lớn vô hạn của entropie của nguồn liên tục.....	74
3.5.6. Lượng thông tin chéo trung bình truyền theo kênh liên tục không nhớ.....	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 hoá 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
<b>CHƯƠNG IV – CƠ SỞ LÝ THUYẾT MÃ HÓA.....</b>	<b>90</b>
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 chế sai của một bộ mã đều nhị phân .....	93
4.1.4. Mã đều nhị phân không có độ thừa.....	94
4.2. MÃ THỐNG KÊ TỐI ƯU .....	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 TUYẾN TÍNH.....	99
4.3.1. Một số cấu trúc đại số cơ bản.....	99
4.3.2. Các dạng tuyến tính và mã tuyến tính .....	101

4.3.3. Các bài toán tối ưu của mã tuyến tính nhị phân .....	104
4.4. VÀNH ĐA THỨC 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 xyclic .....	109
4.4.4. Ma trận sinh của mã xyclic.....	110
4.4.5. Ma trận kiểm tra của mã xyclic .....	110
4.5. MÃ HÓA CHO CÁC MÃ XYCLIC.....	111
4.5.1. Mô tả từ mã của mã xyclic 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 xyclic .....	114
4.5.5. Thuật toán thiết lập từ mã hệ thống theo phương pháp nhân .....	116
4.6. GIẢI MÃ NGƯỠNG .....	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 LƯỚI.....	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 CỰC 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 $GF(2^m)$ .....	140
4.11.3. Biểu diễn đa thức cho trường hữu hạn $GF(2^m)$ .....	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
<b>CHƯƠNG V – LÝ THUYẾT THU TỐI ƯU .....</b>	<b>160</b>
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. Thế 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 NHIỄU NHỜ BỘ LỌC PHỐI HỢP TUYẾN TÍNH THỤ ĐỘNG..	169
5.3.1. Định nghĩa bộ lọc phối hợp tuyến tính thụ động .....	169
5.3.2. Bài toán về bộ lọc phối hợp .....	169
5.3.3. Đặc tính biên 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. Hưởng 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
<b>PHỤ LỤC.....</b>	<b>196</b>
BẤT ĐẲNG THỨC BUNHIACOVSKI-SCHWAZT.....	196
BIẾN ĐỔI HILBERT.....	197
ĐỊNH LÝ KACHENNHICOV.....	198
LUẬT PHÂN BỐ CHUẨN.....	201
LOGARIT CƠ SỐ HAI CỦA CÁC SỐ NGUYÊN TỪ 1 ĐẾN 100.....	202
HÀM VÀ ENTROPIE CỦA NGUỒN NHỊ PHÂN.....	203
ENTROPIE $H(X)$ CỦA CÁC LUẬT PHÂN BỐ RỜI RẠC.....	204
ENTRIPIE VI PHÂN $H(X)$ CỦA CÁC LUẬT PHÂN BỐ LIÊN TỤC.....	207
CÁC ĐA THỨC TỐI TIỂU CỦA CÁC PHẦN TỬ TRONG TRƯỜNG.....	214
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>219</b>
<b>MỤC LỤC.....</b>	<b>220</b>

**BÀI GIẢNG**

**LÝ THUYẾT THÔNG TIN**

**Mã số : 492LTT340**

**Chịu trách nhiệm bản thảo**

**TRUNG TÂM ĐÀO TẠO BƯU CHÍNH VIỄN THÔNG 1**