BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC MỎ ĐỊA CHẤT

BÁO CÁO HỌC THUẬT

THIẾT KẾ BỘ THU CHO CÁC QUAN SÁT THỜI GIAN RỜI RẠC

TS. Nguyễn Thị Hằng

Hà Nội - 01/2023

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC MỎ ĐỊA CHẤT

BÁO CÁO HỌC THUẬT

THIẾT KẾ BỘ THU CHO CÁC QUAN SÁT THỜI GIAN RỜI RẠC

Xác nhận của bộ môn

Hà Nội - 01/2023

LỜI MỞ ĐẦU

Các hệ thống thông tin liên lạc hiện nay đang được sử dụng rộng rãi, phổ biến trong rất nhiều lĩnh vực của đời sống. Thứ nhất ta có thể kể đến vai trò của hệ thống này trong hoạt động thông tin truyền thông truyền thống. Kế tiếp, có thể nói đến sự hiệu quả của nó đã góp phần tạo ra sự bùng nổ của mạng xã hội, thương mại điện tử, giáo dục trực tuyến v.v.. Cấu trúc cơ bản của một hệ thống thông tin truyền thông là một phần kiến thức hữu dụng của các nhà khoa học, các kỹ sư làm việc trong lĩnh vực này. Vì thế nó nhận được nhiều sự quan tâm và được giảng dạy trong các chương trình học cho ngành kỹ thuật thông tin ở bậc đại học [1-4].

Một trong hai bộ phận quan trọng của hệ thống thông tin là khối thu tín hiệu. Việc hoạt động của khối thu đứng trước thách thức phải xử lý và giải mã các tín hiệu được truyền qua một khoảng các khá lớn và không thể tránh khỏi sự tác động của nhiễu. Chẳng hạn có thể kể đến khoảng cách vài chục nghìn km từ vệ tinh viễn thông tới các thiết bị được đặt ở mặt đất. Hiệu quả của việc giải mã tín hiệu số là mắc rất ít sai sót. Việc giảm thiểu sai sót như vậy được thực hiện dựa trên các phân tích kỹ càng về mặt toán học. Đây là một mảng thiết thực của việc ứng dụng toán học trong đời sống. Do đó tôi chọn đề tài : "Thiết kế bộ thu cho các quan sát thời gian rời rạc" này nhằm tìm hiểu và đưa ra rõ ràng các ứng dụng của toán học, rõ hơn là lý thuyết kiểm định trong việc giải mã các tín hiệu số của quá trình truyền thông.

Cấu trúc của báo cáo gồm 3 chương:

Chương 1: MỘT SỐ CÔNG CỤ TOÁN HỌC

Chương 2: HỆ THỐNG TRUYỀN TẢI DỮ LIỆU VÀ GIẢI MÃ

Chương 3: THIẾT KẾ BỘ GIẢI MÃ CHO KÊNH AWGN RỜI RẠC.

Hà Nội, ngày 02 tháng 01 năm 2023

Chương 1

MỘT SỐ CÔNG CỤ TOÁN HỌC

1.1. Biến ngẫu nhiên

Biến ngẫu nhiên được hiểu đơn giản là một hàm từ không gian mẫu Ω đến tập số thực (Cần thỏa mãn một vài điều kiện nhất định).

Nếu X là một biến ngẫu nhiên thì ta thường sử dụng các ký hiệu $(X = \alpha), (X > \alpha), (\alpha > X > \beta)$, v.v., để ký hiệu các biến cố liên quan đến X.

Luật phân phối xác suất của biến ngẫu nhiên X được hiểu là các thông tin về X sao cho ta có thể tính được tất cả các xác suất liên quan đến X.

Đa số biến ngẫu nhiên được quan tâm trọng đồ án này là biến ngẫu nhiên rời rạc. Với quá trình truyền tin có bộ mã rời rạc, tín hiệu được đưa ra từ máy phát là một biến ngẫu nhiên H. Tập giá trị của H thường được mô tả là $\{0, 1, 2, ..., m-1\}$. Ta dùng các ký hiệu là $P(H = i) = P_H(i)$ và gọi chúng là các xác suất tiền nghiệm.

Tín hiệu nhận được ở máy thu là một biến ngẫu nhiên Y. Y có thể là một biến rời rạc hoặc liên tục. Miền giá trị của biến Y được chia thành các phần $\{R_0, R_1, ..., R_{m-1}\}$ để xây dựng hàm giải mã. Hàm giải mã được ký hiệu là $\widehat{H}$. Ta lấy $\widehat{H}(Y \in R_i) = i$. Xác suất $P(\widehat{H} = i)$ được tính theo công thức xác suất đầy đủ bằng các thông tin về luật phân phối của H và thông tin về nhiễu trên đường truyền. Điều này sẽ được nói rõ ràng trong chương sau.

Trong nội dung của đồ án này chúng ta sẽ tính toán đến nhiễu ồn trắng. Nó còn được gọi là nhiễu Gauss hay nói cách khác nhiễu là một biến ngẫu nhiên có phân phối chuẩn. Ta nhắc lại phân phối chuẩn một chiều là phân phối có hàm mật độ là:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\dfrac{(x-\mu)^2}{2\sigma^2}} \tag{1.1}$$

Biến chuẩn có luật phân phối như trên được gọi là biến $N(\mu, \sigma^2)$

Tiếp theo ta nhắc lại biến chuẩn n chiều. Cho Σ là một ma trận xác định dương cấp n. Cho $\mu = (\mu_1, \mu_2, ..., \mu_n)^T$ là một véc tơ thực n chiều. Nếu $x = (x_1, x_2, ..., x_n)^\top \in R^n$ thì hàm mật độ của biến chuẩn n chiều, tham số μ, Σ là

$$f_X(x_1, ..., x_N) = \frac{1}{(2\pi)^{N/2}\sqrt{det\Sigma}} exp\left(-\frac{1}{2}(x-\mu)^T\Sigma^{-1}(x-\mu)\right) \tag{1.2}$$

Biến chuẩn n chiều được ký hiệu là $N(\mu, \Sigma)$

1.2. Hàm Q

Trong một số quá trình truyền tin với bộ mã rời rạc $H = \{0, 1, ..., m-1\}$, nếu không có nhiễu máy thu sẽ nhận được các tín hiệu sóng có số đo là $\{c_0, c_1, ..., c_{m-1}\}$. Tuy nhiên do có nhiễu nên tín hiệu sóng đo được ở máy thu là y thường sẽ bị sai lệch so với các số đo $\{c_0, c_1, ..., c_{m-1}\}$. Nếu nhiễu là biến ngẫu nhiên Z thì giá trị đo được ở máy thu là $c_j + Z$ (nhiễu cộng tính). Bộ giải mã sẽ đưa ra quyết định $\widehat{H}$ sai nếu nhiễu quá lớn. Trong trường hợp nhiễu có phân phối chuẩn thì xác suất để nhiễu lớn hơn một mức α nào đấy là $P(|Z| \geq \alpha)$. Do có thể quy nhiễu về biến chuẩn tắc để tính toán (coi $Z \sim N(0,1)$), ta sẽ đánh giá xác suất mắc lỗi khi giải mã bằng hàm số

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{\dfrac{-\xi^2}{2}} d\xi. \tag{1.3}$$

Đối với $Z \sim \mathcal{N}(0,1)$ thì $P_r\{Z \geq x\} = Q(x)$.

Nếu Z là phân phối chuẩn với trung bình μ và phương sai $\sigma^2 (Z \sim \mathcal{N}(\mu, \sigma^2))$, xác suất $P_r\{Z \geq x\}$ cũng có thể mô tả theo hàm Q. Trong thực tế sự kiện $Z \geq x$ tương đương với $\left\{\dfrac{Z-\mu}{\sigma} \geq \dfrac{x-\mu}{\sigma}\right\}$. Nhưng $\dfrac{(Z-\mu)}{\sigma} \sim \mathcal{N}(0,1)$. Do đó $P_r\{Z \geq x\} = Q\left(\dfrac{x-\mu}{\sigma}\right)$ và kết quả này sẽ được sử dụng thường xuyên.

Bây giờ ta mô tả một số tính chất chính của hàm Q.

(a) Nếu $Z \sim \mathcal{N}(0,1), F_Z(z) := P_r\{Z \leq z\} = 1 - Q(z)$. (Minh họa cho mối quan hệ này là các diện tích nằm bên dưới đồ thị hàm mật độ xác suất của Z.)

(b)

$$Q(0) = 1/2, Q(-\infty) = 1, Q(\infty) = 0$$

.

(c) $Q(-x) + Q(x) = 1$

(d)

$$\frac{1}{\sqrt{2\pi}\alpha} e^{\frac{-\alpha^2}{2}} \left(\frac{\alpha^2}{1+\alpha^2} \right) < Q(\alpha) < \frac{1}{\sqrt{2\pi}\alpha} e^{\frac{-\alpha^2}{2}}, \alpha > 0$$

(e) Một biểu thức thay thế cho hàm Q với các cận tích phân được cố định là

$$Q(x) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} e^{-\frac{x^2}{2sin^2\theta}} d\theta.$$

Công thức này đúng với $x \geq 0$

(f)

$$Q(\alpha) \leq \frac{1}{2} e^{\frac{-\alpha^2}{2}}, \alpha \geq 0$$

Chứng minh: Kết quả của (a) và (b) khá hiển nhiên. Để chỉ ra (c) ta dùng công thức đổi biến và nhận được:

$$Q(-x) + Q(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-\frac{t^2}{2}} dt = 1$$

Để chứng minh (d) ta sử dụng công thức tích phân từng phần để thu được đẳng thức:

$$Q(\alpha) = -\frac{1}{\sqrt{2\pi}} \frac{1}{x} e^{-\frac{x^2}{2}} \Big|_{\alpha}^{+\infty} - \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{+\infty} \frac{e^{-\frac{x^2}{2}}}{x^2} dx$$

hay là:

$$\frac{1}{\sqrt{2\pi}} \frac{1}{\alpha} e^{-\frac{\alpha^2}{2}} = Q(\alpha) + \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{+\infty} \frac{e^{-\frac{x^2}{2}}}{x^2} dx$$

Bỏ đi số hạng tích phân ở vế phải ta nhận được

$$Q(\alpha) < \frac{1}{\sqrt{2\pi}\alpha} e^{\frac{-\alpha^2}{2}}.$$

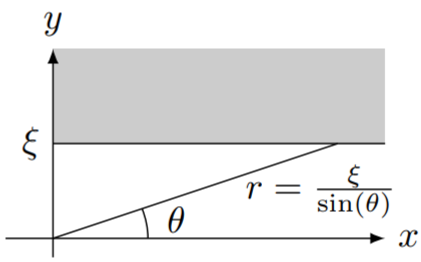
Phần còn lại của (d) được suy ra từ bất đẳng thức

$$\frac{1}{\sqrt{2\pi}} \int_{\alpha}^{+\infty} \frac{e^{-\frac{x^2}{2}}}{x^2} dx < \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{+\infty} \frac{e^{-\frac{x^2}{2}}}{\alpha^2} dx = \frac{1}{\alpha^2} Q(\alpha)$$

Để chứng minh (e), xét $Z \sim \mathcal{N}(0,1)$ và $Y \sim \mathcal{N}(0,1)$ là các biến ngẫu nhiên độc lập và xét $\xi \geq 0$. Do đó $P_r\{X \geq 0,\, Y \geq \xi\} = Q(0)Q(\xi) = \dfrac{Q(\xi)}{2}$. Sử dụng tọa độ cực để tính tích phân trên miền $x \geq 0, y \geq \xi$ (vùng được phủ mờ của hình dưới đây), ta đưa ra

$$\frac{Q(\xi)}{2} = P_r\{X \geq 0,\, Y \geq \xi\} = \int_0^{\frac{\pi}{2}} \int_{\frac{\xi}{\sin\theta}}^{\infty} \frac{e^{\frac{-r^2}{2}}}{2\pi} r dr d\theta$$

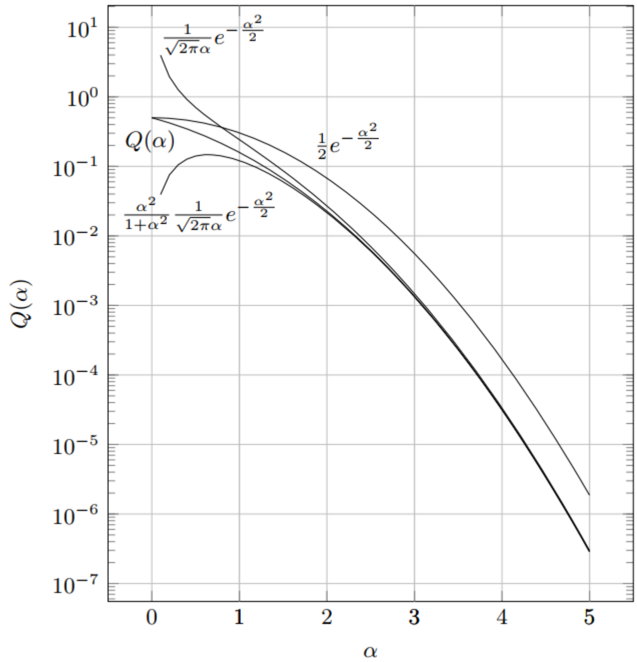
$$= \frac{1}{2\pi} \int_0^{\frac{\pi}{2}} \int_{\frac{\xi^2}{2\sin^2\theta}}^{\infty} e^{-t} dt d\theta = \frac{1}{2\pi} \int_0^{\frac{\pi}{2}} e^{-\frac{\xi^2}{2\sin^2\theta}} d\theta$$



Để chứng minh (f), ta sử dụng (e) và thực tế là $e^{-\frac{\xi^2}{2\sin^2\theta}} \leq e^{\frac{-\xi^2}{2}}$ vì $[0, \frac{\pi}{2}]$. Như vậy

$$Q(\xi) \leq \frac{1}{\pi} \int_0^{\frac{\pi}{2}} e^{\frac{-\xi^2}{2}} d\theta = \frac{1}{2} e^{\frac{-\xi^2}{2}}$$

Đồ thị của hàm Q và các giới hạn của nó được cho trong Hình 1.1



Hình 1.1: Hàm Q với các giới hạn trên và dưới .

1.3. Xích Markov

Định nghĩa 1.3.1. *Ba biến ngẫu nhiên U, V, W được hiểu là tạo thành một xích Markov theo thứ tự này và được ký hiệu là $U \longrightarrow V \longrightarrow W$, nếu phân phối của W trên giá trị đồng thời của U và V là độc lập với U, tức là $P_{W|V,U}(w|v,u) = P_{W|V}(w|v)$.*

Ta có đẳng thức:

$$P_{U,W|V}(u,w|v) = P_{U|V}(u|v).P_{W|V,U}(w|v,u).$$

Do đó nếu có xích $U \longrightarrow V \longrightarrow W$ thì

$$P_{U,W|V}(u,w|v) = P_{U|V}(u|v).P_{W|V}(w|v) \tag{1.4}$$

Đảo lại cũng đúng. Do đó ta có thể nói rằng U, V, W tạo thành một xích Markov (theo thứ tự đó) nếu và chỉ nếu U và W độc lập theo điều kiện trên V.

Nếu có xích $U \longrightarrow V \longrightarrow W$ thì sử dụng (1.4) (và đổi vai trò của W với U), ta có

$$P_{U|V,W}(u|v,w) = P_{U|V}(u|v).$$

Điều này cho thấy $W \longrightarrow V \longrightarrow U$ (cũng là một xích Markov).

Cho H, Y là các biến ngẫu nhiên và $T(Y)$ là một hàm (ngẫu nhiên hoặc xác định) của Y. Ta thấy rằng $H \longrightarrow Y \longrightarrow T(Y)$ (là xích Markov), nhưng nhìn chung $H \longrightarrow T(Y) \longrightarrow Y$ thì không đúng.

Định nghĩa 1.3.2. *Cho $T(Y)$ là một hàm của biến ngẫu nhiên Y. Nếu $H \longrightarrow T(Y) \longrightarrow Y$ thì ta nói rằng $T(Y)$ là một thống kê đầy đủ (đối với giả thiết H).*

Các phân tích về thống kê đầy đủ sẽ được vận dụng trong chương sau.

Chương 2

HỆ THỐNG TRUYỀN TẢI DỮ LIỆU VÀ GIẢI MÃ

2.1. Sơ lược về hệ thống truyền tải dữ liệu

Hệ thống truyền tải dữ liệu được được sử dụng phổ biến trong thông tin truyền thông, cụ thể là các hệ thống truyền dữ liệu bằng Bluetooth, sóng Wifi, sóng viễn thông, sóng cáp quang.

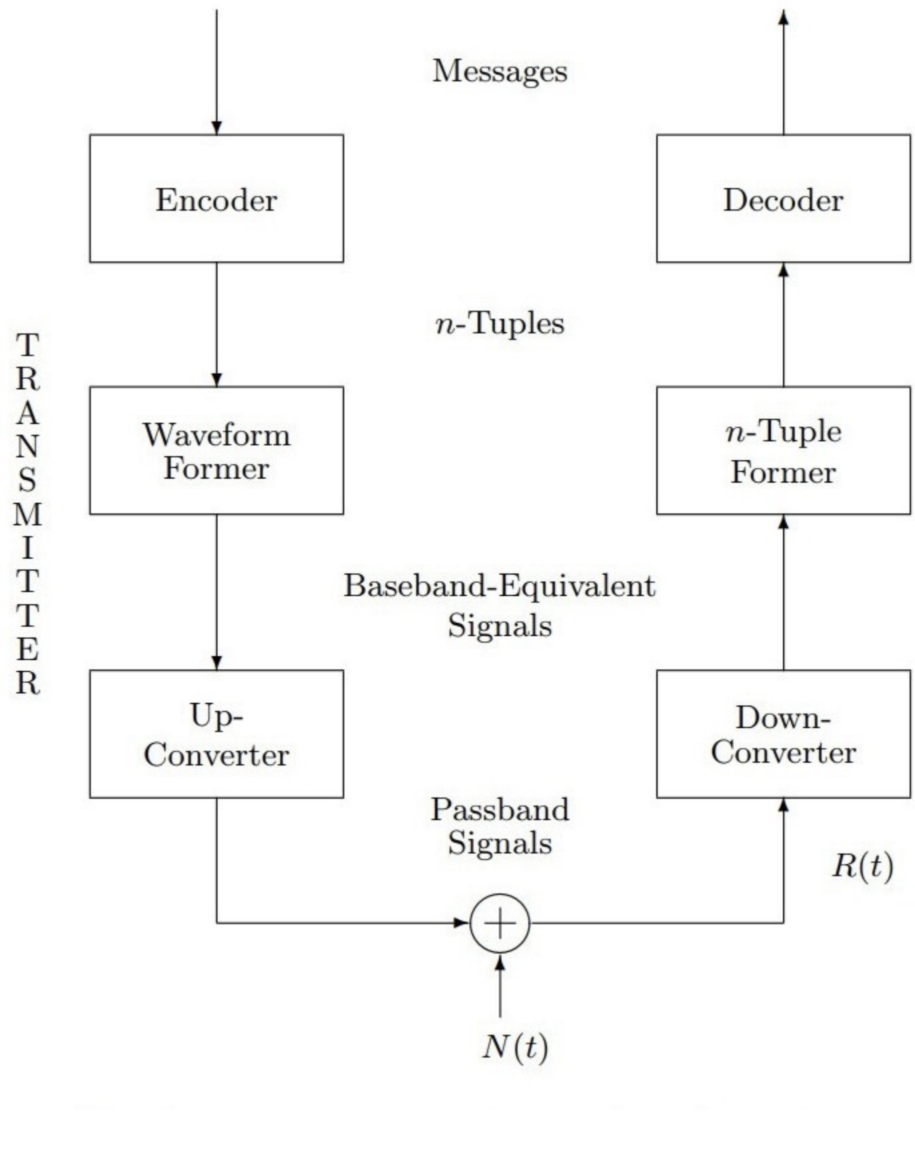
Bên dưới là sơ đồ mô tả cách vận hành của một hệ thống truyền tải dữ liệu. Có 7 bước trong sơ đồ: 3 bước đầu tiên là công việc của máy phát, 3 bước cuối là công việc của máy thu. Bước ở giữa là giai đoạn truyền tải tín hiệu. Máy phát(Transmitter) có thể hiểu là các trạm GPS, các trạm thu phát sóng viễn thông, các thiết bị điện tử như máy tính, điện thoại mà từ đó ta có nhu cầu gửi dữ liệu đi. Máy thu có thể là các trạm thu phát tín hiệu viễn thông khi nó nhận tín hiệu của cuộc gọi từ điện thoại và các thiết bị điện tử thông thường khi ta thực hiện việc nhận tín hiệu từ các thiết bị khác chuyển sang.

Trong sơ đồ có 3 bước của quá trình truyền tải được thực hiện trong máy phát (Transmitter). Bước thứ nhất là mã hóa tín hiệu (Encoder). Ví dụ các chữ cái trong 1 văn bản được chuyển thành các mã nhị phân theo bảng mã ASCII . Bước thứ 2 chuyển tín hiệu về dạng sóng bằng bộ chuyển đổi sóng (Waveform Former) để sẵn sàng đưa vào quá trình truyền tải. Bước thứ 3 là tín hiệu được đưa vào bộ phát sóng (Up-converter).

Chẳng hạn như bộ phát sóng Bluetooth, bộ phát của ăng-ten, bộ phát sóng Wifi.

Bước 4 là giai đoạn truyền tải tín hiệu giữa hai máy. Giai đoạn này diễn ra thông qua sóng viễn thông, sóng wifi, dây cáp.

3 bước còn lại thuộc về Máy thu (Receiver). Bước thứ nhất trong hoạt động của máy thu là tiếp nhận tín hiệu qua bộ thu sóng (Down-Converter). Chuyển đổi sóng về dạng n-chiều (n-Tuple Former). Bước thứ 3 là giải mã. Việc giải thích rõ hơn về giải mã là mục tiêu của báo cáo này.



Hình 2.1: Mô tả vật lý của máy phát và máy thu

2.2. Mô tả toán học của bước giải mã trong máy thu

Việc giải mã là bước cuối cùng của quá trình truyền tin. Về nguyên tắc là người vận hành hệ thống truyền tin trong đó có việc thiết lập bộ giải mã đã nắm được toàn bộ thông tin về cách mã hóa và tín hiệu sóng được truyền đi. Nếu quá trình là lý tưởng (không có nhiễu) thì bộ giải mã sẽ đưa ra được chính xác hoàn toàn thông tin được đưa vào máy phát trước khi mã hóa. Tuy nhiên các quá trình truyền tin sẽ luôn có sự tác động của nhiễu mà đáng kể nhất là những tín hiệu được truyền từ những trạm GPS ở độ cao hàng chục nghìn km trên mặt đất tới các thiết bị ở dưới mặt đất. Quá trình truyền tín hiệu sóng trong dây cáp quang vẫn có ảnh hưởng nhất định của nhiễu (chẳng hạn như ánh sáng bên ngoài).

Tình huống đơn giản nhất là bộ phận mã hóa của máy phát mã hóa thông tin thành các mã nhị phân 0,1. Ta có thể thấy trong một văn bản thông thường vị trí xuất hiện chữ cái 'a' mà có tính ngẫu nhiên. Nên dãy các mã nhị phân được sắp xếp một cách ngẫu nhiên và tín hiệu sóng được đưa ra từ máy phát cũng có tính ngẫu nhiên.

Do đó về mặt lý thuyết giá trị có thể có của một tín hiệu được đưa ra từ máy phát là có tính ngẫu nhiên. Với những hệ thống rời rạc, ta hiểu một tín hiệu được đưa ra là một biến ngẫu nhiên H mà biến này có tập giá trị là bảng chữ cái hữu hạn $\mathcal{H} = \{0, 1, ..., m-1\}$, chẳng hạn nếu nội dung thông tin được mã hóa bằng mã nhị phân thì ta hiểu một tín hiệu của máy phát là một biến ngẫu nhiên H có tập giá trị $\mathcal{H} = \{0, 1\}$.

Nếu việc truyền tải tín hiệu sóng là lý tưởng (không có nhiễu) thì máy thu sẽ nhận được các tín hiệu sóng trùng hoàn toàn với tín hiệu được gửi đi.Tuy nhiên mọi quá trình truyền tin đều có nhiễu nên tín hiệu nhận được ở máy thu không biểu hiện chính xác biến H nữa mà nó là một biến ngẫu nhiên Y (Y được biến đổi từ H dưới tác động của nhiễu). Ta gọi Y là quan sát. Việc giải mã là đưa ra phỏng đoán về giá trị của H dựa trên giá trị của quan sát Y. Trong cách nói của thống kê công việc như thế được gọi là kiểm định.

Trong thông tin, giả thuyết H là thông điệp được truyền đi và quan sát Y nhận được tại kênh đầu ra (hoặc một chuỗi các kênh đầu ra). Bộ thu đoán giá trị thực tế của H dựa trên giá trị nhận được của Y. Nếu không có gì khác, ta giả sử rằng, đối với tất cả $i \in \mathcal{H}$, người thiết kế hệ thống đã biết rõ về các giá trị $P_H(i)$ và $f_{(Y|H)}(\cdot|i)$.

Ta có thể mô tả quyết định của bộ thu bằng hàm quyết định (còn gọi là hàm giải mã) $\widehat{H}$: $\mathcal{Y} \longrightarrow \mathcal{H} = \{0, \dots, m-1\}$. Một cách để mô tả hàm quyết định là dùng đến các vùng quyết định $\mathcal{R}_i = \{y \in \mathcal{Y} : \widehat{H}(y) = i, i \in \mathcal{H}\}$. Như vậy $\mathcal{R}_i$ là tập hợp $y \in \mathcal{Y}$ mà $\{\widehat{H}(y) = i\}, i \in \mathcal{H}$.

Quyết định của bộ thu sẽ được ký hiệu bằng $\hat{i}$ và biến ngẫu nhiên tương ứng là $\widehat{H} \in \mathcal{H}$. Nếu có thể, ta cần đảm bảo rằng $\widehat{H} = H$, nhưng điều này nói chung là không thể. Mục tiêu là đưa ra một chiến lược sao cho xác suất đưa ra quyết định chính xác $P_c = P_r\{\widehat{H} = H\}$ được tối đa hóa. Một mục tiêu tương đương là để tối thiểu hóa xác suất mắc sai sót $P_c = P_r\{\widehat{H} = H\} = 1 - P_c$.

Kiểm định giả thuyết là trọng tâm của bài toán thông tin. Như Claude Shannon đã mô tả trong phần giới thiệu của bài báo được cho là có ảnh hưởng lớn nhất từng được viết về chủ đề này, "Bài toán cơ bản của thông tin là làm thế nào để tái hiện lại tại một thời điểm hoặc là chính xác hoặc xấp xỉ một thông điệp được chọn tại một thời điểm khác".

Ví dụ điển hình cho việc giải mã (bài toán kiểm định giả thuyết về tín hiệu nhận được của máy thu): xét bài toán truyền một bit thông tin trên một sợi quang. Bit thông tin này được mô hình hóa bởi biến ngẫu nhiên $H \in \{0, 1\}, P_H(0) = 1/2$. Nếu $H = 1$, thì máy phát bật một đi-ốt phát sáng (LED) và ánh sáng của nó được truyền qua sợi quang đến một bộ tách sóng quang ở máy thu. Bộ tách sóng quang xuất ra số lượng photon $Y \in \mathbb{N}$ mà nó phát hiện. Bài toán trên máy thu là khi có tín hiệu sóng thì phải quyết định rằng $H = 0$ (đèn LED đã tắt) hay là $H = 1$ (đèn LED đang bật). Quyết định của bộ thu chỉ có thể dựa trên thông tin đầy đủ về mô hình và giá trị quan sát thực tế $Y = y$. Điều làm cho bài toán đáng chú ý là không thể xác định H từ Y một cách chắc chắn. Ngay cả khi đèn LED tắt, máy dò vẫn có khả năng phát hiện một số photon (ví dụ: do "ánh sáng xung quanh"). Một giả thiết tốt là Y có phân phối Poisson với cường độ λ, điều này phụ thuộc vào việc đèn LED mở hay tắt. Về mặt toán học, tình huống này có mô tả như sau:

$$\text{Với} \quad H = 0, Y \sim P_{Y|H}(y|0) = \frac{\lambda_0^y}{y!} e^{-\lambda_0}$$

$$\text{Với} \quad H = 1, Y \sim P_{Y|H}(y|1) = \frac{\lambda_1^y}{y!} e^{-\lambda_1}$$

trong đó $0 \leq \lambda_0 < \lambda_1$.Thông tin trên được hiểu như sau: "Với $H = 0$, quan sát Y là phân bố Poisson với cường độ λ_0 (máy thu vẫn có thể nhận được tín hiệu sáng nhưng với cường độ yếu vì λ_0 nhỏ). Khi $H = 1$, Y là phân bố Poisson với cường độ λ_1 (máy thu vẫn có thể nhận được tín hiệu sáng nhưng với cường độ mạnh vì λ_1 lớn) ".
Từ P_H và $f_{Y|H}$, sử dụng công thức Bayes, ta nhận được

$$P_{H|Y}(i|y) = \frac{P_H(i) f_{H|Y}(y|i)}{f_H(i)}$$

trong đó $f_Y(y) = \sum_i P_H(i) f_{Y|H}(y|i)$. Trong biểu thức trên $P_{H|Y}(i|y)$ là hậu nghiệm (còn được gọi là xác suất hậu nghiệm của H khi đã cho Y). Sử dụng quan sát $Y = y$, xác suất để $H = i$ dịch chuyển từ giá trị tiền nghiệm $P_H(i)$ đến giá trị hậu nghiệm $P_{H|Y}(i|y)$.

Nếu quyết định là $\widehat{H} = i$ thì xác suất cho quyết định này chính xác chính là xác suất để $H = i$, tức là. $P_{Y|H}(i|y)$. Vì mục tiêu của ta là tối đa hóa xác suất quyết định đúng, quy tắc quyết định tối ưu là

$$\widehat{H}(y) = arg \max_{i \in \mathcal{H}} P_{H|Y}(i|y)$$

(Quy tắc quyết định MAP)
trong đó $arg \max_i g(i)$ là viết tắt của "lựa chọn một trong những đối số i mà hàm g(i) đạt được cực đại của nó". Chuyện này được gọi là quy tắc quyết định tối đa một hậu nghiệm (MAP). Trong trường hợp ghép, tức là nếu $P_{H|Y}(j|y)$ bằng $P_{H|Y}(k|y)$ bằng $max_i P_{H|Y}(i|y)$, thì không có vấn đề gì nếu chúng ta quyết định $\hat{H} = k$ hoặc $\widehat{H} = j$. Khi đó, việc đổi sang trường hợp còn lại, xác suất mà ta có quyết định đúng vẫn như vậy.

Bởi vì quy tắc MAP tối đa hóa xác suất quyết định đúng cho mỗi quan sát y, nó cũng tối đa hóa xác suất không điều kiện P_c của việc quyết định đúng. Cái được nhắc đến trước là $P_{H|Y}(\widehat{H}(y)|y)$. Nếu chúng ta thế biến ngẫu nhiên Y thay cho y, thì chúng ta sẽ nhận được một biến ngẫu nhiên. (Một hàm có giá trị thực của một biến ngẫu nhiên là một biến ngẫu nhiên). Giá trị kỳ vọng của biến ngẫu nhiên này là xác suất (không điều kiện) để quyết định đúng, tức là.

$$P_c = \mathbb{E}[P_{H|Y}(\widehat{H}(Y)|Y)] = \int_y (\widehat{H}(y)|y) f_Y(y)dy$$

Có một trường hợp đặc biệt quan trọng, đó là H có phân bố đều. Trong trường hợp này $P_{H|Y}(i|y)$, là một hàm của i, tỷ lệ với $P_{Y|H}(y|i)$. Vì vậy, đối số tối đa hóa $P_{H|Y}(i|y)$ cũng tối đa hóa $P_{Y|H}(y|i)$. Sau đó, quy tắc quyết định MAP tương đương với quyết định

$$\widehat{H}(y) = arg \max_{i \in \mathcal{H}} f_{Y|H}(y|i)$$

(Quy tắc quyết định MAP)
Được gọi là quy tắc quyết định hợp lý cực đại (ML). Cái tên này bắt nguồn từ thực tế là $f_{Y|H}(y|i)$, như một hàm của i, được gọi là hàm hợp lý.

Lưu ý rằng quy tắc quyết định ML được xác định ngay cả khi chúng ta không biết P_H. Do đó, đó là lời giải cho lựa chọn khi không biết về tiền nghiệm. (Các quy tắc quyết định MAP và ML chỉ tương đương nhau khi tiền nghiệm là đều.)

2.2.1. Kiểm định giả thuyết về mã nhị phân

Trong thực tế, các thông điệp thường được mã hóa bằng mã nhị phân. Hệ mã nhị phân là $\mathcal{H} = \{0, 1\}$ và việc giải mã của máy thu là việc kiểm định về mã nhị phân. Trong mục này ta sẽ nói về bài toán kiểm định mã nhị phân và trong mục tới ta sẽ nói về bài toán kiểm định khái quát hơn.

Vì chỉ có hai lựa chọn đối lập nhau được kiểm nghiệm, kiểm định MAP ở đây có thể viết lại dưới dạng.

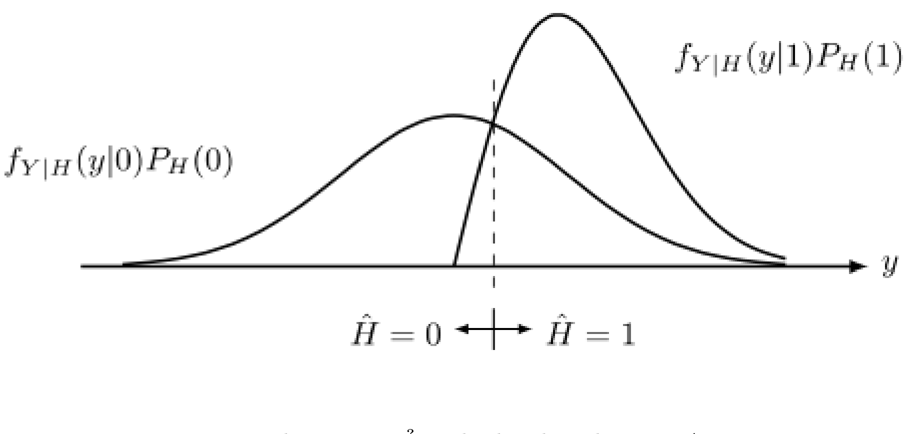
$$\frac{f_{Y|H}(y|1)P_H(1)}{f_Y(y)} \underset{\widehat{H}=0}{\overset{\widehat{H}=1}{\underset{<}{\geq}}} \frac{f_{Y|H}(y|0)P_H(0)}{f_Y(y)}$$

Ký hiệu trên có nghĩa là kiểm định MAP quyết định $\widehat{H} = 1$ khi bên trái lớn hơn hoặc bằng bên phải và quyết định $\widehat{H} = 0$ nếu trái lại. Ta nhận thấy rằng mẫu số có thể bỏ qua mà không gây ảnh hưởng đến quyết định, vì $f_Y(y)$ là một hằng số dương. Do đó, một quy tắc quyết định tương đương là.

$$
f_{Y|H}(y|1)P_H(1) \underset{\widehat{H}=0}{\overset{\widehat{H}=1}{\underset{<}{\geq}}} f_{Y|H}(y|0)P_H(0)
$$

Bài toán kiểm định này được mô tả trong Hình 2.2 khi $y \in \mathbb{R}$. Đây là một hình ảnh quan trọng giúp chúng ta hình dung những gì đang diễn ra. Chúng ta sẽ thấy rằng, nó cũng hữu ích để tính toán xác suất mắc lỗi.

Ý nghĩa của kiểm định trên là ta so sánh được các hậu nghiệm sau khi co dãn chúng bằng cách khử số dương $f_Y(y)$ ở mẫu số. Tuy nhiên, có những hình thức thay thế của kiểm định, phụ thuộc vào tình huống chi tiết, có thể thuận tiện hơn về mặt tính toán. Một kiểm định tương đương thu được bằng cách chia cả hai vế với đại lượng không âm $f_{Y|H}(y|0)P_H(1)$.



Hình 2.2: Kiểm định nhị phân MAP

Điều này dẫn đến kiểm định MAP nhị phân sau đây:

$$\Lambda(y) = \frac{f_{Y|H}(y|1)}{f_{Y|H}(y|0)} \underset{\widehat{H}=0}{\overset{\widehat{H}=1}{\underset{<}{\geq}}} \frac{P_H(0)}{P_H(1)} = \eta \tag{2.1}$$

Số đo bên trái $\Lambda(y)$ của bài toán kiểm định trên được gọi là *tỷ số hợp lý*. Trong khi vế phải là ngưỡng η. Lưu ý rằng nếu $P_H(0)$ tăng thì ngưỡng đó cũng tăng. Đổi lại, như chúng ta mong đợi, miền $\{y : \hat{H}(y) = 0\}$ trở nên lớn hơn.

Khi $P_H(0) = P_H(1) = 1/2$ ngưỡng η là đơn vị ($\eta = 1$) và kiểm định MAP trong tình huống này được gọi là kiểm định ML nhị phân:

$$f_{Y|H}(y|1) \underset{\widehat{H}=0}{\overset{\widehat{H}=1}{\underset{<}{\geq}}} f_{Y|H}(y|0)$$

Hàm giải mã ở đây là $\widehat{H}$: $\mathcal{Y} \longrightarrow \mathcal{H} = \{0, 1\}$. Hàm giải mã có thể mô tả bằng hai vùng quyết định là $\mathcal{R}_i = \{y \in \mathcal{Y} : \hat{H}(y) = i, i \in \{0, 1\}\}$.

Để tính xác suất mắc lỗi chung, ta thường tính xác suất mắc lỗi cho mỗi giả thuyết và sau đó lấy trung bình. Nếu mã gửi đi $H = 0$, quyết định không chính xác nếu $Y \in \mathcal{R}_1$ hoặc tương đương, nếu $\Lambda(y) \geq \eta$. Do đó, nếu ký hiệu $P_e(i)$ là xác suất mắc lỗi khi tín hiệu gửi đi là $H = i$, thì

$$P_e(0) = P_r(Y \in \mathcal{R}_1 | H = 0) = \int_{\mathcal{R}_1} f_{Y|H}(y|0)dy \tag{2.2}$$

hoặc, tương đương

$$P_e(0) = P_r\{\Lambda(Y) \geq \eta | H = 0\}. \tag{2.3}$$

Làm việc với vế phải của (2.2) hoặc của (2.3) là dễ dàng hơn hay là làm việc với mật độ có điều kiện của Y hoặc $\Lambda(Y)$ là dễ dàng hơn. Chúng ta sẽ quan sát các ví dụ cho cả hai trường hợp.

Các biểu thức tương tự được sử dụng cho xác suất mắc lỗi P_e (1) với tín hiệu gửi đi là $H = 1$. Sử dụng công thức xác suất đầy đủ, ta thu được xác suất mắc lỗi (vô điều kiện)

$$P_e = P_e(1)P_H(1) + P_e(0)P_H(0)$$

Công thức xác suất đầy đủ là chiến lược được dùng để tính toán xác suất, dựa vào việc chia nhỏ thành nhiều trường hợp và dùng xác suất điều kiện. Với ý tưởng này một bài toán khó được chia thành bài toán nhỏ sao cho:

(i) Ta biết cách giải các bài toán nhỏ

(ii) Khi ta có đáp án của các bài toán nhỏ, ta cũng giải giải được bài toán gốc.

2.2.2. Kiểm định giả thuyết cỡ m

Bây giờ chúng ta quay trở lại bài toán kiểm định giả thuyết cỡ m. Điều này có nghĩa là $\mathcal{H} = \{0, 1, \ldots, m-1\}$.

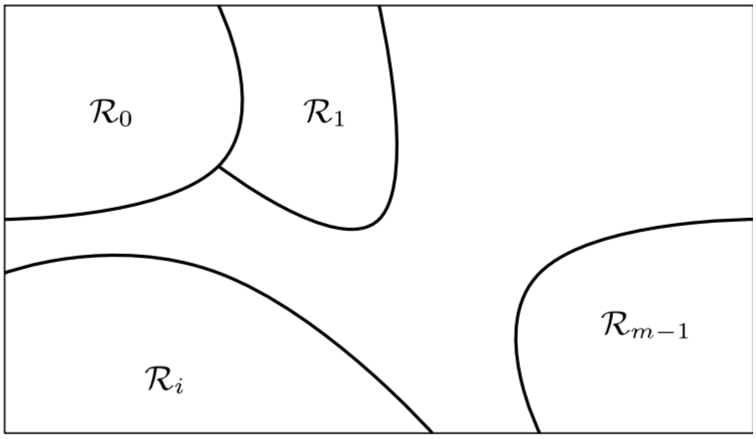
Ta nhắc lại quy tắc quyết định MAP, mà nó giảm thiểu xác suất mắc lỗi, là

$$\begin{aligned}
\widehat{H}_{MAP}(y) &= arg \max_{i \in \mathcal{H}} P_{H|Y}(i|y) \\
&= arg \max_{i \in \mathcal{H}} \frac{f_{Y|H}(y|i)P_H(i)}{f_Y(y)} \\
&= arg \max_{i \in \mathcal{H}} f_{Y|H}(y|i)P_H(i)
\end{aligned}$$

trong đó $f_{Y|H}(\cdot|i)$ là hàm mật độ xác suất của biến Y mà ta quan sát được ở máy thu khi tín hiệu được gửi đi từ máy phát là i và $P_H(i)$ là xác suất của tín hiệu thứ i. Quy tắc này cho ta kết quả giải mã $\widehat{H}$ là chỉ số i mà $P_{H|Y}(i|y)$ lớn nhất. Nếu $P_{H|Y}(i|y)$ đạt giá trị lớn nhất tại nhiều hơn một chỉ số i thì ta có thể quyết định lấy bất kỳ i nào như vậy mà không gây ảnh hưởng đến xác suất mắc lỗi. Nếu chúng ta muốn quy tắc quyết định là rõ ràng thì có thể đồng ý rằng ta chọn i lớn nhất trong các chỉ số mà $P_{H|Y}(i|y)$ max.

Khi tất cả các tín hiệu phát có cùng xác suất, thì quy tắc MAP chuyển về quy tắc ML, tức là.

$$\widehat{H}_{ML}(y) = arg \max_{i \in \mathcal{H}} f_{Y|H}(y|i)$$



Hình 2.3: Các vùng quyết định

Ta sẽ luôn giả thiết rằng $f_{Y|H}$ hoặc là có sẵn, hoặc là được tính ra từ quá trình phân tích. Trong thông tin, chúng ta thường biết trước máy phát và kênh. Trong đồ án này, máy phát là một ánh xạ từ $\mathcal{H}$ đến $\mathcal{C} \subset \mathcal{X}^n$ và kênh được mô tả bởi hàm mật độ $f_{Y|X}(y|x)$ đã biết với mỗi $x \in \mathcal{X}^n$ và mỗi $y \in \mathcal{Y}^n$. Từ hai yếu tố này, ta ngay lập tức xác định được $f_{Y|H}(y|x) = f_{Y|X}(y|c_i)$, trong đó c_i là tín hiệu được gán cho i.

Lưu ý rằng hàm quyết định (hoặc giải mã) $\widehat{H}$ gán một $i \in \mathcal{H}$ cho mỗi $y \in \mathbb{R}^n$. Như đã đề cập, hàm này có thể được mô tả bằng các miền quyết định (hoặc giải mã) $R_i, i \in \mathcal{H}$, trong đó R_i bao gồm những Y mà $\widehat{H}(y) = i$. Để thuận tiện, ta có ý tưởng là phân hoạch $\mathbb{R}^n$ thành các miền giải mã như mô tả ở Hình 2.3.

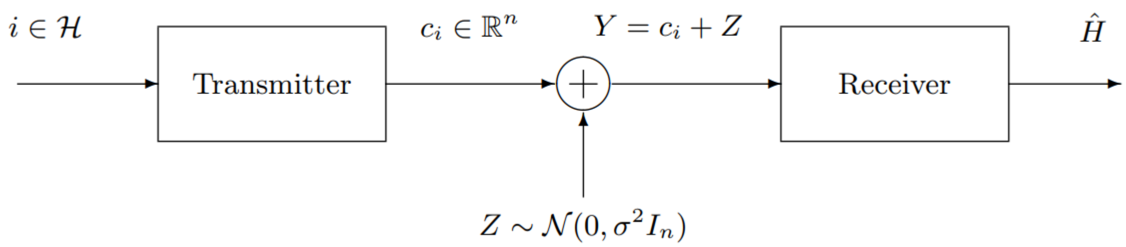
Ta sử dụng các miền giải mã để tính toán xác suất mắc lỗi P_e, hay tương đương với điều này, ta tính xác suất để quyết định là chính xác $P_c = 1 - P_e$. Trên điều kiện $H = i$ tính toán đó như sau:

$$\begin{aligned} P_e(i) &= 1 - P_c(i) \\ &= 1 - \int_{\mathcal{R}_i} f_{Y|H}(y|i)dy \end{aligned}$$

Chương 3

THIẾT KẾ BỘ GIẢI MÃ CHO KÊNH AWGN RỜI RẠC

Bài toán kiểm định giả thuyết được thảo luận trong phần này là chìa khóa trong thông tin kỹ thuật số. Nó là một trong những công việc được mô tả ở bước cuối cùng của sơ đồ truyền tin. Hình 3.1 mô tả kênh AWGN rời rạc. Giả thuyết $H \in \mathcal{H} = \{0, ..., m-1\}$ đại diện cho một thông điệp được chọn ngẫu nhiên. Máy phát ánh xạ $H = i$ đến một tín hiệu n-chiều $c_i \in \mathbb{R}^n$.



Hình 3.1: Truyền tin trên kênh có nhiễu Gauss trắng cộng tính thời gian rời rạc.

Kênh thêm một vector ngẫu nhiên Z (nhiễu) có các thành phần là biến Gauss độc lập cùng phân phối với trung bình 0 và phương sai σ^2. Nói tóm lại, $Z \sim \mathcal{N}(0, \sigma^2 I_n)$. Quan sát thu được là $Y = c_i + Z$.

Ta bắt đầu với tình huống đơn giản nhất, cụ thể là chỉ có 2 thông điệp đồng khả năng và các tín hiệu là vô hướng ($n = 1$). Sau đó, chúng ta khái quát hóa cho giá trị

n tùy ý và cuối cùng chúng ta xét đến xác suất tùy ý gán lên m thông điệp.

3.1. Kiểm định nhị phân cho các quan sát vô hướng

Cho thông điệp H thuộc tập hợp 2 thông điệp đồng khả năng $\{0, 1\}$ và giả thiết rằng máy phát ánh xạ $H = 0$ thành $c_0 \in \mathbb{R}$ và $H = 1$ thành $c_1 \in \mathbb{R}$. Thống kê đầu ra cho các giả thuyết khác nhau như sau:

$$H = 0 : Y \sim \mathcal{N}(c_0, \sigma^2)$$
$$H = 1 : Y \sim \mathcal{N}(c_1, \sigma^2)$$

Một cách tương đương để thể hiện thống kê đầu ra cho mỗi giả thuyết là

$$f_{Y|H}(y|0) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(y-c_0)^2}{2\sigma^2}\right\}$$
$$f_{Y|H}(y|1) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(y-c_1)^2}{2\sigma^2}\right\}$$

Ta tính tỷ lệ hợp lý

$$\Lambda(y) = \frac{f_{Y|H}(y|1)}{f_{Y|H}(y|0)} = \exp\left\{-\frac{(y-c_1)^2-(y-c_0)^2}{2\sigma^2}\right\} = \exp\left\{y\frac{c_1-c_0}{\sigma^2} + \frac{c_0^2-c_1^2}{2\sigma^2}\right\} \tag{3.1}$$

Ngưỡng quyết định là

$$\eta = \frac{P_H(0)}{P_H(1)}$$

Đến đây, ta đã có tất cả các thành tố để sử dụng quy tắc MAP. Thay vì so sánh $\Lambda(y)$ với ngưỡng quyết định η, ta có thể so sánh ln $\Lambda(y)$ với $ln(\eta)$. Hàm ln$\Lambda(y)$ được gọi là tỷ lệ hợp lý logarit. Do đó, quy tắc quyết định MAP có thể mô tả là

$$y\frac{c_1-c_0}{\sigma^2} + \frac{c_1^2-c_0^2}{2\sigma^2} \overset{\widehat{H}=1}{\geq} ln\eta$$

$$<$$
$$\widehat{H} = 0$$

Với tiến trình này, máy thu không còn tính hàm số mũ của quan sát nữa. Nó phải tính $\ln(\eta)$, nhưng điều này không chỉ được thực hiện cho một lần mà thực hiện cho mọi lần.

Không mất tính tổng quát, giả sử $c_1 > c_0$. Từ đó, ta có thể chia cả hai vế cho $\frac{c_1 - c_0}{\sigma^2}$ mà không làm thay đổi kết quả của so sánh trên. Ta có thể đơn giản hóa hơn nữa bằng cách chuyển các hằng số sang bên phải. Kết quả là một kiểm định đơn giản

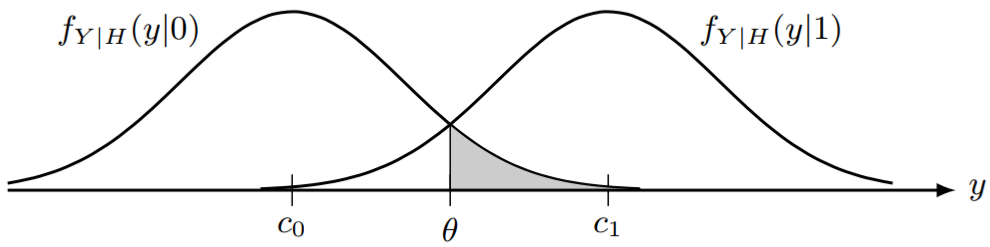
$$\widehat{H}_{MAP}(y) = \begin{cases} 1, & \text{nếu } y \geq \theta \\ 0, & \text{nếu } y < \theta \end{cases}$$

ở đây

$$\theta = \frac{\sigma^2}{c_1 - c_0} ln\eta + \frac{c_1 + c_0}{2}$$

Lưu ý rằng $P_H(0) = P_H(1)$, thì $\ln \eta = 0$ và ngưỡng quyết định θ trở thành điểm giữa $\frac{c_0 + c_1}{2}$ (Hình 3.2). Bây giờ ta xác định xác suất mắc lỗi.

$$P_e(0) = P_r(Y > \theta | H = 0) = \int_{\theta}^{\infty} f_{Y|H}(y|0)dy$$



Hình 3.2: Khi $P_H(0) = P_H(1)$, ngưỡng quyết định θ là điểm giữa giữa c_0 và c_1. Vùng phủ mờ mô tả xác suất mắc lỗi theo điều kiện $H = 0$.

Đây là xác suất mà một biến ngẫu nhiên Gaussian với trung bình c_0 và phương sai σ^2 vượt quá ngưỡng quyết định θ. Từ những nội dung về hàm Q được nhắc đến ở chương 1, ta có ngay $P_e(0) = Q\left(\frac{\theta - c_0}{\sigma}\right)$. Tương tự, $P_e(1) = Q\left(\frac{\theta - c_1}{\sigma}\right)$. Cuối cùng,

$P_e = P_H(0)Q\left(\frac{\theta - c_0}{\sigma}\right) + P_H(1)Q\left(\frac{\theta - c_1}{\sigma}\right)$

Trường hợp phổ biến nhất là khi $P_H(0) = P_H(1) = \frac{1}{2}$. Từ đó $\frac{\theta - c_0}{\sigma} = \frac{c_1 - \theta}{\sigma} = \frac{c_1 - c_0}{2\sigma} = \frac{d}{2\sigma}$. Ở đây d là khoảng cách giữa c_0 và c_1. Trong trường hợp này, $P_e = P_e(0) = P_e(1) = P_e$, ở đây

$$P_e = Q\left(\frac{d}{2\sigma}\right)$$

Kết quả này có thể thu được một cách đơn giản mà không cần tính toán phụ. Như được thể hiện trong Hình 3.2, ngưỡng quyết định là điểm giữa giữa c_0 và c_1 và $P_e = P_e(0) = Q\left(\frac{d}{2\sigma}\right)$.

3.2. Kiểm định nhị phân cho các quan sát n-chiều

Như trong tiểu mục trước, ta giả thiết rằng H lấy giá trị trong $\{0, 1\}$. Điểm thay đổi so với mục trước là các tín hiệu bây giờ là n-chiều với $n \geq 1$. Vì vậy, khi $H = 0$, máy phát gửi một véc tơ $c_0 \in \mathbb{R}^n$ nào đấy và khi $H = 1$, nó sẽ gửi $c_1 \in \mathbb{R}^n$. Nhiễu được thêm vào bởi kênh là nhiễu Gauss trắng n-chiều $Z \sim \mathcal{N}(0, \sigma^2 I_n)$ và độc lập với H.

Như đã làm trước đó, để có được quy tắc quyết định MAP, ta bắt đầu bằng cách viết ra số liệu thống kê đầu ra cho từng giả thuyết

$$H = 0 : Y = c_0 + Z \sim \mathcal{N}(c_0, \sigma^2 I_n)$$

$$H = 1 : Y = c_1 + Z \sim \mathcal{N}(c_1, \sigma^2 I_n)$$

hoặc, tương đương

$$H = 0 : Y \sim f_{Y|H}(y|0) = \frac{1}{(2\pi\sigma^2)^{n/2}} \exp\left\{-\frac{\|y - c_0\|^2}{2\sigma^2}\right\}$$

$$H = 1 : Y \sim f_{Y|H}(y|1) = \frac{1}{(2\pi\sigma^2)^{n/2}} \exp\left\{-\frac{\|y - c_1\|^2}{2\sigma^2}\right\}$$

Giống như trong trường hợp vô hướng, ta tính toán tỷ lệ hợp lý

$$\Lambda(y) = \frac{f_{Y|H}(y|1)}{f_{Y|H}(y|0)} = \exp\left\{-\frac{\|y - c_1\|^2 - \|y - c_0\|^2}{2\sigma^2}\right\}$$

Lấy logarit ở cả hai bên, chúng ta có được

$$ln\Lambda(y) = \frac{\|y - c_1\|^2 - \|y - c_0\|^2}{2\sigma^2} \tag{3.2}$$

$$= \left\langle y, \frac{c_1 - c_0}{\sigma^2} \right\rangle + \frac{\|c_0\|^2 - \|c_1\|^2}{2\sigma^2} \tag{3.3}$$

Từ (3.3), quy tắc MAP có thể viết lại là

$$\left\langle y, \frac{c_1 - c_0}{\sigma^2} \right\rangle + \frac{\|c_0\|^2 - \|c_1\|^2}{2\sigma^2} \begin{array}{c} \hat{H} = 1 \\ \geq \\ < \\ \hat{H} = 0 \end{array} ln\eta$$

Chú ý về sự tương tự với biểu thức của trường hợp vô hướng. Như đã làm với trường hợp vô hướng, ta chuyển các hằng số sang vế phải và chuẩn hóa để nhận được

$$\langle y, \psi \rangle \begin{array}{c} \hat{H} = 1 \\ \geq \\ < \\ \hat{H} = 0 \end{array} \theta$$

trong đó

$$\psi = \frac{c_1 - c_0}{d}$$

là vectơ độ dài đơn vị cùng hướng với $c_1 - c_0, d = \|c_1 - c_0\|$ là khoảng cách giữa các tín hiệu và

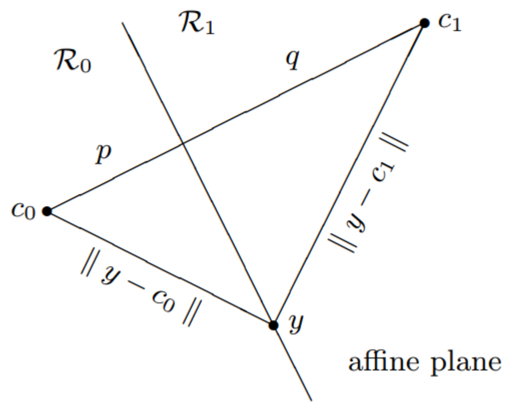
$$\theta = \frac{\sigma^2}{d} ln\eta + \frac{\|c_1\|^2 - \|c_0\|^2}{2d}$$

là ngưỡng quyết định. Như vậy, các miền quyết định $\mathcal{R}_0$ và $\mathcal{R}_1$ được phân chia bởi siêu phẳng affine

$$\left\{ y \in \mathbb{R}^n : \langle y, \psi \rangle = \theta \right\}$$

Để xác định, ta đang ghép các điểm của siêu phẳng affine phân định vào $\mathcal{R}_1$, nhưng đây là một quyết định có thể thay đổi và không ảnh hưởng đến xác suất mắc lỗi vì xác suất để Y ở trên một siêu phẳng affine bất kỳ là bằng không.

Ta nhận được một cái nhìn sâu hơn nữa về hình học bằng cách xét những y mà với nó (3.2) là không đổi. Tình huống được mô tả trong Hình 3.3, trong đó khoảng cách có dấu p là dương nếu siêu phẳng affine phân định nằm theo hướng được chỉ bởi ψ đối với c_0 và q là dương nếu siêu phẳng affine nằm theo hướng chỉ bởi $-\psi$ đối với c_1. (Trong Hình 3.3, cả p và q đều dương). Theo định lý Pythagoras áp dụng cho hai tam giác vuông với cạnh chung, cho tất cả các y trên siêu phẳng affine, $\|y - c_0\|^2 - \|y - c_1\|^2$ bằng $p^2 - q^2$.



Hình 3.3: Mặt phẳng Affine phân định $\mathcal{R}_0$ và $\mathcal{R}_1$

Lưu ý rằng p và q có liên hệ η, σ^2 và d qua đẳng thức

$$\|y - c_0\|^2 - \|y - c_1\|^2 = p^2 - q^2$$

$$\|y - c_0\|^2 - \|y - c_1\|^2 = 2\sigma^2 ln\eta$$

Do đó $p^2 - q^2 = 2\sigma^2 ln\eta$. Sử dụng điều này và $d = p + q$, chúng ta có được

$$p = \frac{d}{2} + \frac{\sigma^2 ln\eta}{d}$$

$$q = \frac{d}{2} - \frac{\sigma^2 ln\eta}{d}$$

Khi $P_H(0) = P_H(1) = \dfrac{1}{2}$, siêu phẳng affine phân định là tập hợp $y \in \mathbb{R}^n$ mà $ln\Lambda(y)$ trong (3.2) bằng 0. Đây là những điểm y có khoảng cách như nhau đến c_0 và đến c_1. Do đó, $\mathcal{R}_0$ chứa tất cả các điểm $y \in \mathbb{R}^n$ gần c_0 hơn c_1.

Một vài quan sát bổ sung được sắp xếp theo thứ tự:

- Vector ψ không bị ảnh hưởng bởi giá trị tiền nghiệm nhưng ngưỡng θ là có sự ảnh hưởng. Do đó, giá trị tiền nghiệm ảnh hưởng đến vị trí nhưng không ảnh hưởng đến hướng của siêu phẳng affine phân định. Như ta mong đợi, siêu phẳng di chuyển ra khỏi c_0 khi $P_H(0)$ tăng lên. Điều này phù hợp với trực giác của ta là miền giải mã cho một giả thuyết trở nên lớn hơn khi xác suất của giả thuyết đó tăng lên.

- Hiệu ứng nêu trên của giá trị tiền nghiệm được khuếch đại khi σ^2 tăng lên. Điều này cũng phù hợp với trực giác của chúng ta rằng bộ giải mã phụ thuộc ít hơn vào quan sát và nhiều hơn vào giá trị tiền nghiệm khi quan sát trở nên nhiễu hơn.

- Chú ý đến sự tương tự của (3.2) và (3.3) với (3.1). Điều này cho thấy mối quan hệ chặt chẽ giữa các trường hợp vô hướng và véc tơ. Ta có thể có thấy được rõ hơn bằng cách thay một hệ tọa độ mới với gốc ở điểm $\frac{c_0+c_1}{2}$ và tọa độ đầu tiên theo hướng $\psi = \frac{c_0+c_1}{d}$, trong đó một lần nữa $d = \|c_1 - c_0\|$. Trong hệ tọa độ mới này, $H = 0$ được ánh xạ vào vector $\tilde{c}_0 = \left(\frac{-d}{2}, 0, .., 0\right)^\intercal$ và $H = 1$ được ánh xạ thành $\tilde{c}_1 = \left(\frac{d}{2}, 0, .., 0\right)^\intercal$. Nếu $\tilde{y} = (\tilde{y}_1, ..., \tilde{y}_n)^\intercal$ là đầu ra kênh trong hệ tọa độ mới này $\langle \tilde{y}, \psi \rangle = \tilde{y}_1$. Điều này cho thấy rằng đối với một quyết định nhị phân, trường hợp vector về cơ bản là trường hợp vô hướng được nhúng trong một không gian n-chiều.

Đối với trường hợp vô hướng, ta tính xác suất mắc lỗi bằng xác suất có điều kiện trên $H = 0$ và $H = 1$ và sau đó loại bỏ xác suất điều kiện bằng công thức xác suất đầy đủ: $P_e = P_e(0)P_H(0) + P_e(1)P_H(1)$.

Khi $H = 0$, $Y = c_0 + Z$ và bộ giải mã MAP đưa ra quyết định sai khi $\langle Z, \psi \rangle \geq p$, tức là hình chiếu của Z lên vectơ đơn vị định hướng ψ có chiều dài (có dấu) bằng hoặc lớn hơn p. Tình huống mắc lỗi như vậy được mô tả rõ ràng theo Hình 2.7, nhưng nó cũng có thể đưa ra được bằng cách chèn $Y = c_0 + Z$ vào $\langle Y, \psi \rangle \geq \theta$. Vì $\langle Z, \psi \rangle$ là một biến ngẫu nhiên Gaussian có trung bình là 0 và phương sai là σ^2, ta thu được

$$P_e(0) = Q\left(\frac{p}{\sigma}\right) = Q\left(\frac{d}{2\sigma} + \frac{\sigma ln\eta}{d}\right)$$

Tương tự như vậy, ta tìm thấy

$$P_e(1) = Q\left(\frac{q}{\sigma}\right) = Q\left(\frac{d}{2\sigma} - \frac{\sigma ln\eta}{d}\right)$$

Trường hợp $P_H(0) = P_H(1) = 0,5$ là trường hợp phổ biến nhất. Bởi vì $p = q = \frac{d}{2}$, việc xác định xác suất lỗi cho trường hợp đặc biệt này rất đơn giản:

$$P_e = P_e(1) = P_e(0) = P_r\left\{\langle Z, \psi\rangle \geq \frac{d}{2}\right\} = Q\left(\frac{d}{2}\right)$$

3.3. Kiểm định bậc m cho quan sát *n*-chiều

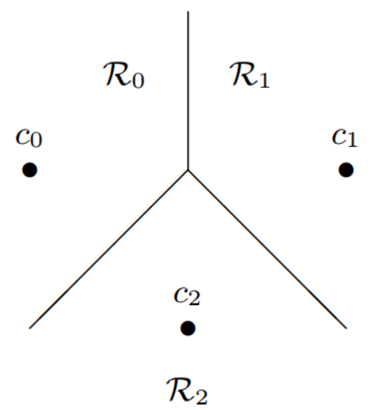
Trường hợp $H = i, i \in \mathcal{H} = \{0, 1, \ldots m-1\}$, đầu vào kênh là $c_i \in \mathbb{R}^n$. Đầu tiên ta giả thiết đơn giản là $P_H(i) = \frac{1}{m}$, đây là một giả thiết phổ biến trong hệ thống truyền tin. Sau này chúng ta sẽ thấy rằng khái quát hóa của nó cũng không quá phức tạp.

Khi $Y = y \in R^n$, quy tắc kiểm định ML(Maximum Likelihood decision rule) là:

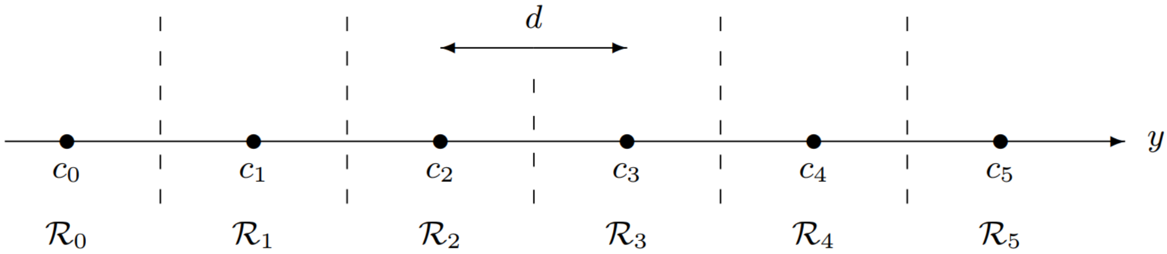
$$\hat{H}_{ML}(y) = arg \max_{i \in \mathcal{H}} f_{Y|H}(y|i)$$

$$= arg \max_{i \in \mathcal{H}} \frac{1}{(2\pi\sigma^2)^{n/2}} \exp\left\{-\frac{\|y - c_0\|^2}{2\sigma^2}\right\}$$
$$= arg \min_{i} \|y - c_i\|$$

Do đó, quy tắc quyết định ML cho kênh AWGN trở thành quy tắc quyết định theo khoảng cách tối thiểu (minh họa trong Hình 3.4). Bỏ qua các ranh giới, $\mathcal{R}_i$ tương ứng với miền Voronoi của c_i, được định nghĩa là tập hợp các điểm trong $\mathbb{R}^n$ gần với c_i nhất so với bất kỳ c_j nào khác.



Hình 3.4: Ví dụ về miền Voronoi trong $\mathbb{R}^2$.



Hình 3.5: Chòm sao PAM cỡ 6 ở $\mathbb{R}$.

Ví dụ 3.3.1. (PAM cỡ m) Hình 3.5 mô tả bộ tín hiệu $\{c_0, c_1, ..., c_5\} \subset \mathbb{R}$ của bộ điều biến biên độ xung(PAM) cỡ 6. Giả sử rằng kênh là AWGN, bộ giải mã ML có chứa 6 miền giải mã. Các điểm tín hiệu là các phần tử của $\mathbb{R}$ và bộ giải mã ML chọn theo quy tắc khoảng cách tối thiểu. Khi giả thuyết là $H = 0$, bộ giải mã cho kết quả sai nếu quan sát $y \in \mathbb{R}$ rơi ra ngoài vùng giải mã $\mathcal{R}_0$. Đây là trường hợp nếu nhiễu $Z \in \mathbb{R}$ lớn hơn $d/2$, trong đó $d = c_i - c_{i-1}, i = 1, ..., 5$. Vậy

$$P_e(0) = P_r\left\{Z > \frac{d}{2}\right\} = Q\left(\frac{d}{2\sigma}\right)$$

Do tính đối xứng, $P_e(5) = P_e(0)$. Đối với $i \in \{1, 2, 3, 4\}$, xác suất mắc lỗi khi $H = i$ là xác suất của biến cố $\left\{Z \geq \frac{d}{2}\right\} \cup \left\{Z < -\frac{d}{2}\right\}$. Biến cố này là hợp của các biến cố xung khắc. Xác suất của nó là tổng của xác suất của các biến cố riêng lẻ. Do đó

$$P_e(i) = P_r\left\{\{Z \geq \frac{d}{2}\} \cup \{Z < -\frac{d}{2}\}\right\} = 2P_r\left\{Z \geq \frac{d}{2}\right\} = 2Q\left(\frac{d}{2\sigma}\right), i \in \{1, 2, 3, 4\}$$

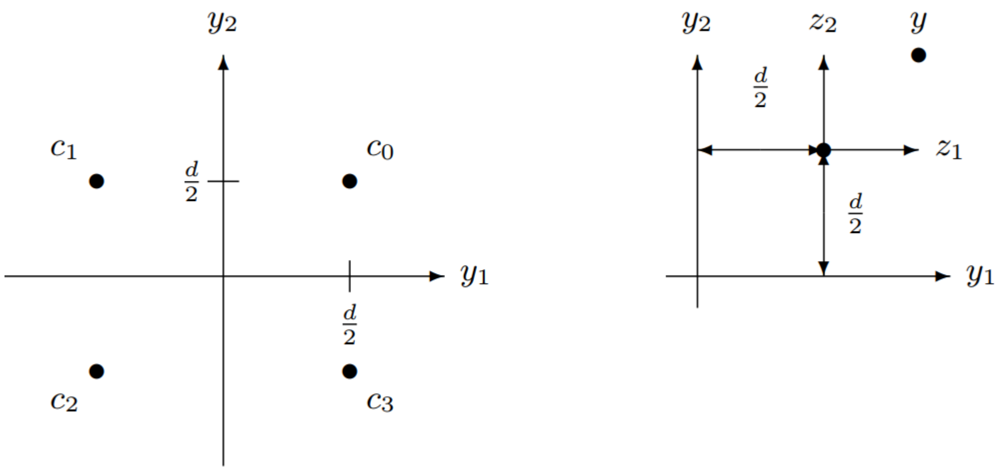
Cuối cùng, $P_e = \frac{2}{6}Q\left(\frac{d}{2\sigma}\right) + \frac{4}{6}2Q\left(\frac{d}{2\sigma}\right) = \frac{5}{3}Q\left(\frac{d}{2\sigma}\right)$. Kết quả này chúng ta dễ dàng mở rộng được. Đối với liên kết PAM của m điểm (m số nguyên dương), xác suất mắc lỗi là

$$P_e = \left(2 - \frac{2}{m}\right)Q\left(\frac{d}{2\sigma}\right)$$

Ví dụ 3.3.2. (QAM cỡ m) Hình 3.6 cho thấy bộ tín hiệu $\{c_0, c_1, c_2, c_3\} \subset \mathbb{R}^2$ cho bộ điều biến biên độ bậc hai (QAM) cỡ 4. Ta coi các tín hiệu là các điểm trong $\mathbb{R}^2$. Nhiễu là $Z \sim \mathcal{N}(0, \sigma^2 I_n)$ và quan sát thu được, với $H = i$ là $Y = c_i + Z$. Ta giả thiết rằng máy thu thực hiện quy tắc kiểm định ML, đối với kênh AWGN có nghĩa là giải mã khoảng cách tối thiểu. Miền giải mã cho c_0 là góc phần tư đầu tiên, cho c_1 góc phần tư thứ hai, v.v.. Khi $H = 0$, bộ giải mã đưa ra quyết định chính xác nếu $\left\{Z_1 > \frac{d}{2}\right\} \bigcap \left\{Z_2 \geq -\frac{d}{2}\right\}$, trong đó d là khoảng cách tối thiểu giữa các điểm tín hiệu. Đây là giao của các biến cố độc lập. Do đó, theo công thức nhân xác suất

$$P_e(i) = P_r\left\{\{Z \geq \frac{d}{2}\}\bigcap\{Z < -\frac{d}{2}\}\right\} = Q^2\left(\frac{d}{2\sigma}\right) = \left[1 - Q(\frac{d}{2\sigma})\right]^2$$

Theo tính đối xứng, với tất cả $i, P_c(i) = P_c(0)$. Do đó



Hình 3.6: Chòm sao QAM cỡ 4 trong $\mathbb{R}^2$.

$$P_c = P_e(0) = 1 - P_c(0) = 2Q\left(\frac{d}{2\sigma}\right) - Q^2\left(\frac{d}{2\sigma}\right)$$

m-QAM được định nghĩa cho tất cả các số m có dạng $(2j)^2$ với $j = 1, 2, \ldots$.

KẾT LUẬN

Kênh AWGN thời gian với rời rạc rất đáng chú ý vì nó đóng một vai trò quan trọng trong lý thuyết truyền tin. Bộ giải mã ML cho kênh AWGN có quy tắc kiểm định theo khoảng cách tối thiểu. Đối với các chùm tín hiệu thuộc họ PAM và QAM, xác suất mắc lỗi có thể được tính chính xác bằng hàm Q. Đối với các chùm khác, xác suất mắc lỗi có giới hạn trên cho bởi liên kết ràng buộc và hàm Q.

Một kỹ thuật khá chung và hữu ích để tìm giới hạn trên cho xác suất mắc lỗi là đánh giá Bhattacharyya. Lưu ý rằng nó áp dụng cho các kiểm định MAP gắn với các bài toán khái quát về kiểm định giả thuyết, không chỉ cho các bài toán thông tin. Đánh giá xác suất tổng Bhattacharyya chỉ phụ thuộc vào $f_{H|Y}$ và P_H (xem tài liệu tham khảo [2]).

Hầu hết các tiêu chuẩn truyền thông hiện tại sử dụng PAM, QAM hoặc PSK để tạo từ mã của chúng. Ý tưởng cơ bản là hình thành các từ mã dài với các thành phần thuộc tập hợp điểm PAM, QAM hoặc PSK, được gọi là bảng chữ cái. Chỉ một tập hợp con của các dãy như thế có thể nhận được theo cách đó được dùng làm từ mã. Trong tài liệu [2], một vài bộ giải mã hữu dụng đã được đưa ra: Bộ mã 5-PAM được dùng làm chùm của nền Ethernet; QAM được dùng trong các modem điện thoại và trong các tiêu chuẩn phát sóng video kỹ thuật số khác nhau (DVB-C2, DVB-T2); tùy thuộc vào tốc độ dữ liệu, PSK và QAM được sử dụng trong mạng LAN không dây (mạng cục bộ) IEEE 802.11, cũng như trong dự án hợp tác thế hệ thứ ba (3GPP) và các tiêu chuẩn cho mạng dữ liệu không dây (LTE); và PSK (với các biến thể) được dùng trong các chuẩn Bluetooth 2, ZigBee và EDGE.

Tài liệu tham khảo

Tài liệu Tiếng Việt

[1] Nguyễn Lâm Đông, Nhập môn xử lý tín hiệu số, NXB Khoa Học Và Kỹ Thuật, 2004

[2] TS. Nguyễn Đức Nhân, Mô phỏng hệ thống truyền thông, Học viện Công Nghệ Bưu Chính Viễn Thông, 2014

[3] Nguyễn Danh Sang, Mô phỏng máy thu tối ưu qua kênh AWGN sử dụng bộ tính tương quan cho hệ thống thông tin tín hiệu nhị phân gồm hai sóng mang trực giao cơ bản, đồ án tốt nghiệp, Đại học Hàng Hải Việt Nam, 2018

Tài liệu Tiếng Anh

[4] BixioRimoldi, Principles of Digital Communication A Top-Down Approach, NXB. Cambridge University Press, 2016.