



Lý thuyết thông tin

Phần 2

Lý thuyết thông tin thống kê

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



dinhptit@gmail.com



A. Đo lường thông tin

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



Nguyên tắc đo lường thông tin

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

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

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

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

- **Đơn vị đo**

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

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



Entropy của nguồn rời rạc không nhớ (DMS)

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

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

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

$H(A)$: Entropy của A (bit/symbol)

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



Tính chất của entropy của nguồn rời rạc

- Tính chất 1:

$$H_1(A) \geq 0$$

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

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

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

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

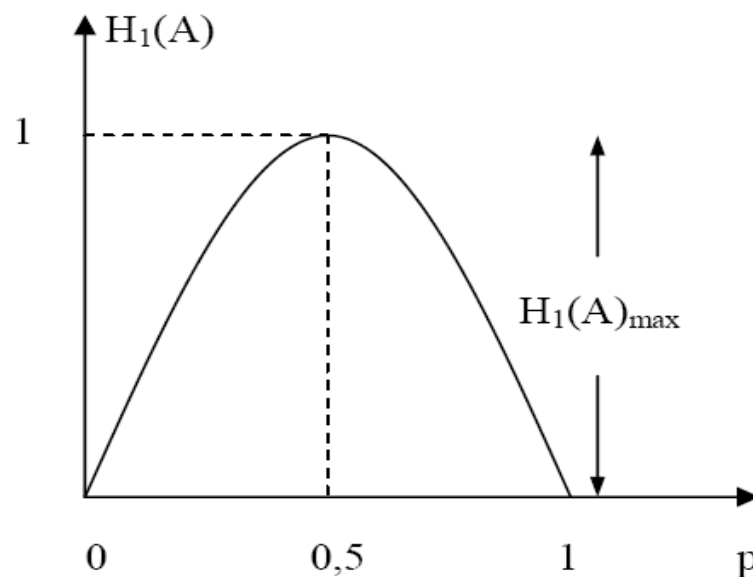


Khảo sát entropy của nguồn nhị phân

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

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

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





Thông tin tương hỗ

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

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

- **Tính chất:**

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

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

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

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

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

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

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

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

❑ Truyền tin không nhiễu (kênh lý tưởng):

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

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

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

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

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

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

- Dạng bảng

	a_1	a_2	a_s	
b_1	$p(a_1, b_1)$	$p(a_2, b_1)$				$p(a_s, b_1)$	
b_2	$p(a_1, b_2)$	$p(a_2, b_2)$				$p(a_s, b_2)$	
...							
b_t	$p(a_1, b_t)$	$p(a_2, b_t)$				$p(a_s, b_t)$	

- Dạng trường

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



Entropie của trường biến cố đồng thời

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

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

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

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

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

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



Entropy có điều kiện (conditional entropy)

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

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

(Partial conditional entropy)

- Tương tự:

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



Entropy có điều kiện (tt)

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

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

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



Entropy có điều kiện (tt)

- Tương tự:

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

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

- Chú ý: $H(A/B) \neq H(B/A)$



Mối quan hệ của các Entropy

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

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

- **Tính chất 2:**

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

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

- $H(A/B)=0, H(B/A)=0$: khi A và B là đồng nhất (kênh hoàn hảo, không nhiễu).
- $H(A/B) = H(A), H(B/A) = H(B)$: khi A và B là độc lập (kênh bị đứt).

- **Tính chất 3:** Cho DMS $X=\{x_k\}$, $k=1,N$. Một hàm toán học $f(X)$ mô tả mối quan hệ xác định của f và X . Khi đó:

$$H(f(X)|X) = 0$$

$$H(X|f(X)) \geq 0; \quad H(X) \geq H(f(X))$$

- Dấu "=" xảy ra chỉ khi $f(X)$ là quan hệ ánh xạ 1-1.



Lượng thông tin tương hỗ trung bình

- Lượng tin tương hỗ trung bình về tập phát A do tập thu B mang lại.

$$I(A; B) \stackrel{\Delta}{=} E[I(a_i; b_j)] = \sum_{a_i \in A} \sum_{b_j \in B} p(a_i, b_j) \log \frac{p(a_i | b_j)}{p(a_i)}$$

- **Ý nghĩa:**
 - $I(A; B)$: Đo lượng tin thu được về một biến ngẫu nhiên A thông qua giá trị của một biến ngẫu nhiên B.
 - Nó là lượng thông tin trung bình được truyền qua kênh có nhiễu (lượng tin không bị nhiễu phá hủy)



Một số tính chất

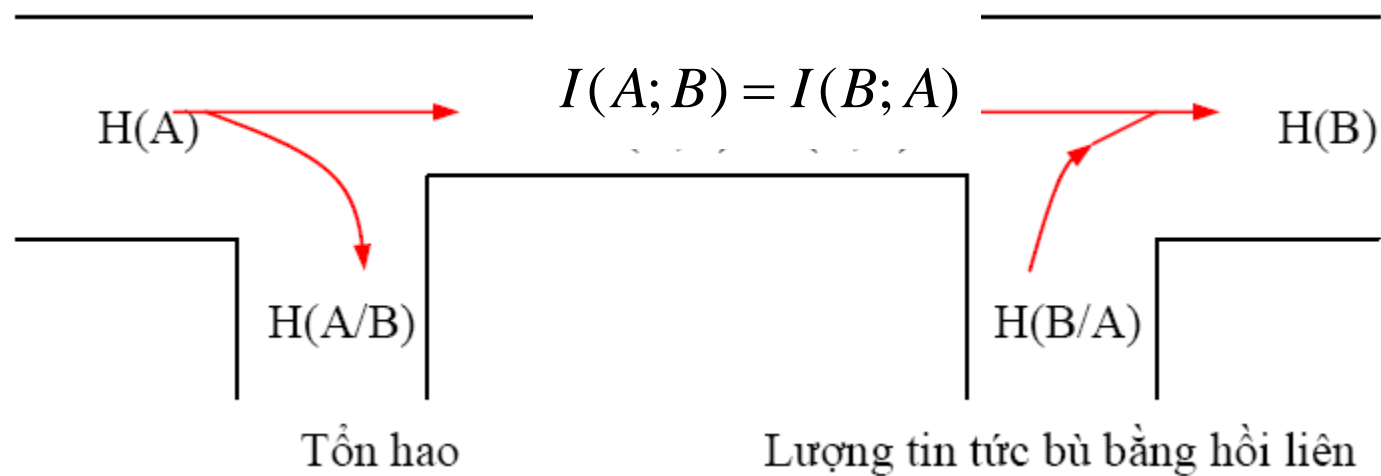
- Tính chất 1: $I(A; B) \geq 0$ $I(A; B) = 0$ khi A độc lập với B, kênh bị đứt.
- Tính chất 2: $I(A; A) = H(A)$
- Tính chất 3: $I(A; B) = I(B; A)$
- Tính chất 4: $I(A; B) \leq H(A) \rightarrow I(A; B) = H(A) = H(B)$ khi kênh không nhiễu.
- Tính chất 5:

$$I(A; B) = H(A) - H(A|B) = H(B) - H(B|A) = H(A) + H(B) - H(A, B)$$

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

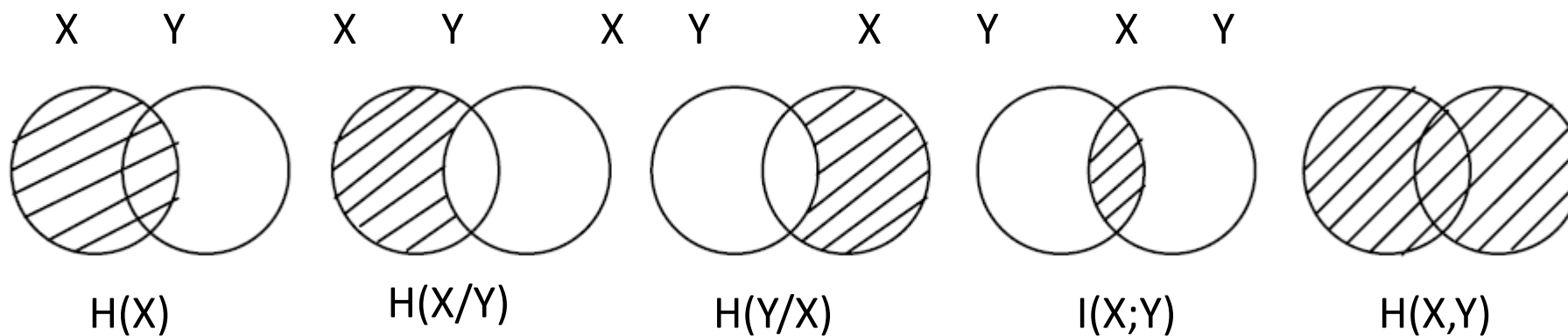
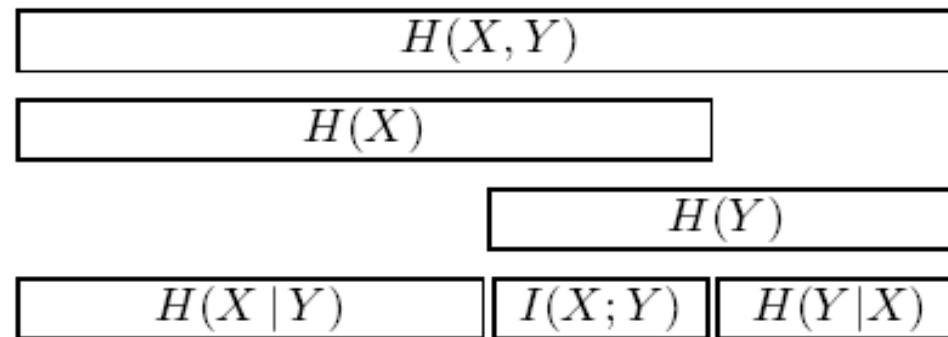


Mô hình kênh





Lược đồ Venn





B. Các tham số đặc trưng cho Nguồn và kênh rời rạc

dinhptit@gmail.com

- **Tốc độ baud của nguồn rời rạc (tốc độ truyền tín hiệu):** số symbol nguồn phát ra trong một đơn vị thời gian. (Một symbol có thể là biểu diễn của mức biên độ, tần số hoặc pha... của tín hiệu).

$$\upsilon_n = \frac{1}{T_n} \quad [Baud]$$

T_n : Thời hạn trung bình của mỗi dấu của nguồn phát.

- **Tốc độ bit /Khả năng phát của nguồn rời rạc (tốc độ truyền thông tin):** Là lượng tin trung bình do nguồn phát ra trong một đơn vị thời gian.

$$R_n = \upsilon_n H(A) = \frac{H(A)}{T_n} \quad [bps]$$

R_n đạt max khi $H(A) \max = H_0(A) = \log S$

- **Độ thừa (redundancy) của nguồn rời rạc:** $D = 1 - \mu$

$$\mu = \frac{H(A)}{H_0(A)} \quad \text{he so nen tin}$$



Các tham số của kênh rời rạc

- Tập các xác suất chuyển: $p(b_j / a_i)$
- Khả năng thông qua của kênh \mathbf{C}' (hoặc dung lượng kênh \mathbf{C}).
- Biểu diễn kênh rời rạc
 - Giảm đồ kênh
 - Hoặc ma trận chuyển: $P = [p(b_j | a_i)] = \begin{bmatrix} p(b_1 | a_1) & . & . & . & p(b_t | a_1) \\ . & . & . & . & . & . & . & . & . \\ p(b_1 | a_s) & . & . & . & p(b_t | a_s) \end{bmatrix}$
- Nếu một kênh có $p(b_j/a_i) \notin t$ ($\forall i, j$): gọi là kênh đồng nhất (hay bất biến); Ngược lại kênh không đồng nhất;
- Nếu một kênh có $p(b_j/a_i) \notin$ vào đầu đã phát trước nó: gọi là kênh không nhớ (Discrete memoryless channels); ngược lại kênh có nhớ (Discrete channels with memory)



Tốc độ bit của kênh

•**Định nghĩa:** Tốc độ bit của kênh là lượng thông tin trung bình truyền qua kênh trong một đơn vị thời gian:

$$R_k = v_k I(A; B) \quad [\text{bps}]$$

v_K : Tốc độ baud của kênh (dấu/s). Biểu thị số dấu được truyền qua kênh trong một đơn vị thời gian.

$$v_K = \frac{1}{T_K}$$

T_K : thời gian trung bình để truyền một dấu qua kênh

Nếu kênh giãn tin: $T_K > T_n$

Nếu kênh nén tin: $T_K < T_n$

Thông thường: $T_K = T_n$

- **Khả năng thông qua của kênh rời rạc:** là giá trị cực đại của R_k (ứng với một phân bố tối ưu của các xác suất tiên nghiệm $p(a_i)$, $\forall a_i \in A$).

$$C' = \max_A R_k = \nu_k \max_A I(A; B) = \nu_k C \quad [\text{bit/s}]$$

$$\text{Với: } C = \max_A I(A; B) \quad [\text{bit/symbol}]$$

C: Dung lượng kênh : Channel capacity (khả năng thông qua của kênh với mỗi dấu).

→ C' đánh giá năng lực tải tin tối đa của một kênh.

- **Tính chất:**

$$0 \leq C \leq \log S$$

$C = 0$ khi A và B độc lập (kênh đứt, Useless channel)

- **Độ thừa của kênh :** $D_k = 1 - \eta_k$
$$\eta_k = \frac{R_k}{C'}$$
 Hiệu suất sử dụng kênh
 - \rightarrow Hiệu suất sử dụng kênh phụ thuộc tính chất thống kê của nguồn.
 - Thông thường độ thừa của kênh được lợi dụng để xây dựng mã chống nhiễu kênh.
 - **Định lý mã hóa thứ hai của Shannon đối với kênh rời rạc :**
 - Nếu khả năng phát R_n của nguồn bé hơn khả năng thông qua của kênh: ($R_n < C'$) thì tồn tại một phép mã hoá và giải mã sao cho việc truyền tin có xác suất lỗi bé tùy ý khi độ dài từ mã đủ lớn. Nếu $R_n > C'$ thì không tồn tại phép mã hoá và giải mã như vậy.
- Nhận xét:** Định lý chỉ ra sự tồn tại, không chỉ ra cách thiết lập mã cụ thể nào.



Một số loại kênh rời rạc đặc biệt

- Kênh đối xứng (symmetric channel):
- Lossless channel (Kênh không tổn hao):
- Deterministic channel (Kênh đơn định):
- Noiseless channel: Kênh không nhiễu (Kênh hoàn hảo)
- Useless channel: Kênh vô dụng (kênh đứt)



C. Nguồn & kênh liên tục không nhớ

dinhptit@gmail.com

- **Nguồn liên tục:**

Lực lượng của nguồn là vô hạn

- **Mô hình nguồn liên tục S:**

- Nguồn liên tục S là một biến ngẫu nhiên, phát ra những tin s có thể nhận các giá trị liên tục trong khoảng $s_{\min} \div s_{\max}$ với hàm mật độ phân bố xác suất *probability density function* $W_1(s)$.

- **Entropie** (*differential entropy*) của nguồn S:

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

Chú ý:

- ✓ $h(S)$ có thể nhận các giá trị dương, âm (hữu hạn).
- ✓ $h(S)$ còn gọi là entropy tương đối

Entropy của nguồn ngẫu nhiên X có phân bố chuẩn

$$X \approx N(\mu, \sigma^2)$$

- Xét nguồn ngẫu nhiên $X=\{x(t)\}$, có phân bố chuẩn (Gaussian distribution), tức có hàm mật độ phân bố xác suất:

$$W_1(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(x-\mu)^2}{2\sigma^2}\right\}$$

$\mu = E(X)$ kỳ vọng của X.

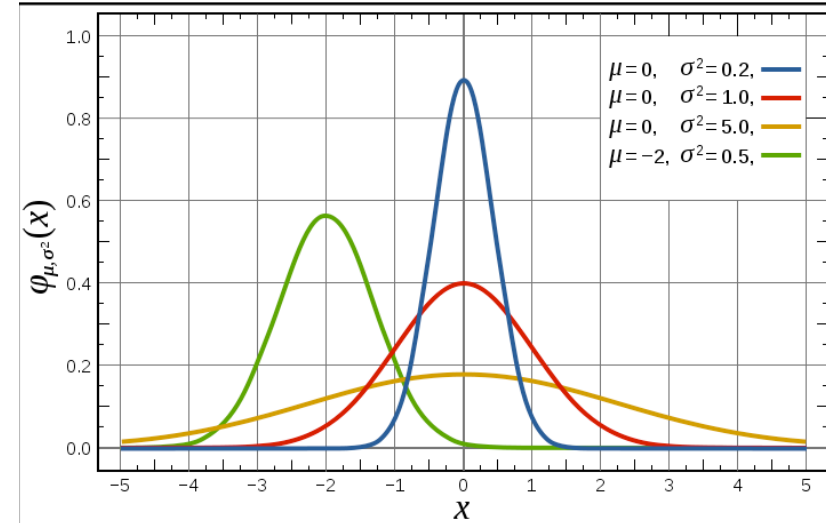
$E(X^2) = \sigma^2$ phương sai của X (Công suất của X)

→ Entropie vi phân của X: $h(X) = \frac{1}{2} \log 2\pi e \sigma^2 = \log \sqrt{2\pi e \sigma^2}$ bit

- Định lý:** Let X be a random variable with mean μ and variance σ^2 .

$$\rightarrow h(X) \leq \log \sqrt{2\pi e \sigma^2}$$

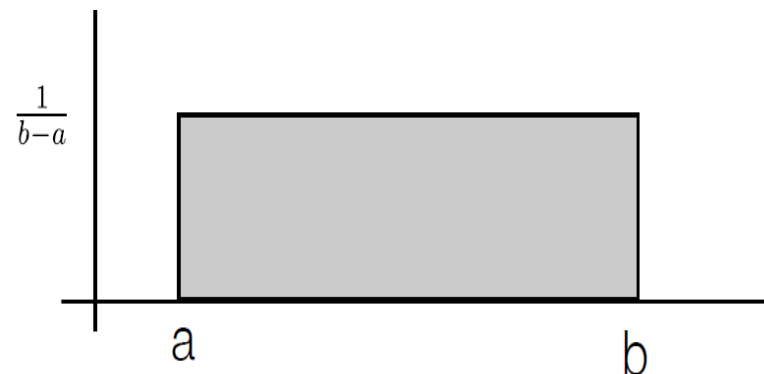
“=” only when X has a gaussian distribution



Entropy của nguồn ngẫu nhiên có phân bố đều

- Uniform distribution: $X \sim U(a, b)$

$$W(X) = \begin{cases} \frac{1}{b-a} & \text{for } x \in (a, b) \\ 0 & \text{elsewhere} \end{cases}$$



$$h(X) = - \int_a^b \frac{1}{b-a} \log \frac{1}{b-a} dx = \log(b-a)$$

– Note that $h(X) < 0$ if $(b-a) < 1$

- Định lý:**

Xét X trong một khoảng hữu hạn (a,b), với:

$$\int_a^b W_1(x) dx = 1$$

Thì: $h(X) \leq \log(b-a)$

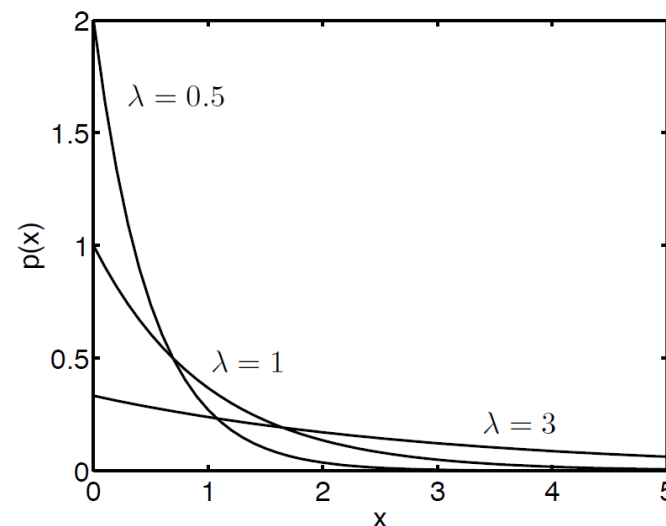
“=” chỉ xảy ra khi X có phân bố đều.

- For the exponential distribution:

$$W(x) = \begin{cases} \lambda e^{-\lambda x} & \text{for } x \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

the differential entropy for this exponential distribution:

$$h(X) = \log \frac{e}{\lambda}$$



- Định lý:**

Trong số tất cả các đại lượng ngẫu nhiên X liên tục dương có cùng kỳ vọng m:

$$\int_0^{\infty} W_1(x) dx = 1 \quad \text{và} \quad \int_0^{\infty} x W_1(x) dx = m$$

Đại lượng ngẫu nhiên phân bố luật hàm mũ có entropy lớn nhất.



Entropy của trường sự kiện đồng thời

- Entropy vi phân của trường biến cố liên tục đồng thời của S và U.

$$h(S, U) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(s, u) \log[W(s, u)] ds du$$

Về mặt hình thức, so với nguồn rời rạc, $h(S, U)$ đóng vai trò của $H(A, B)$

- Tính chất:

$$h(U, S) = h(S, U) = h(S) + h(U|S) = h(U) + h(S|U)$$

$$h(U|S) \leq h(U); \quad h(S|U) \leq h(S) \quad \text{Dấu} = \text{khi } S, U \text{ độc lập.}$$



Entropy có điều kiện

- Entropie vi phân có điều kiện của nguồn S khi đã biết nguồn U.

$$h(S|U) = - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(s, u) \log[W(s|u)] ds du$$

Về mặt hình thức, so với nguồn rời rạc, $h(S/U)$ đóng vai trò của $H(A/B)$.

- Lượng tin tương hỗ giữa các nguồn liên tục S và U:

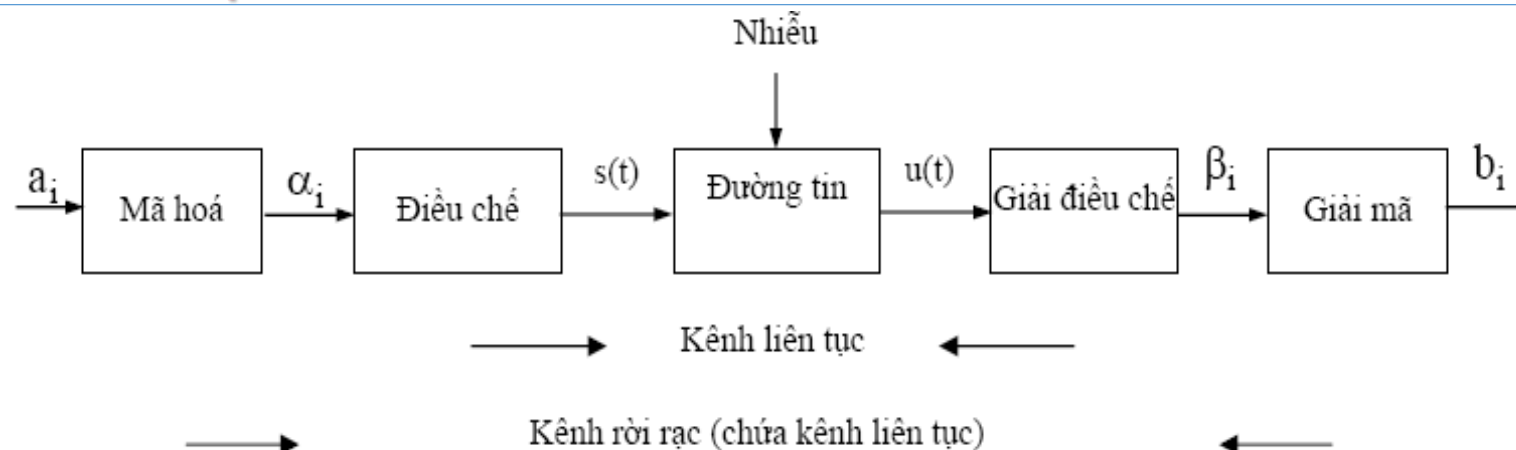
$$I(S;U) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} W(s,u) \log \left[\frac{W(s,u)}{W(s)W(u)} \right] ds du$$

- Một số tính chất

$$I(S;U) = I(U;S) = h(U) - h(U|S) = h(S) - h(S|U)$$

$$I(S;U) \geq 0 \quad \text{Dấu} = \text{là khi S độc lập với U}$$

Nếu kênh không nhiễu thì $I(S;U) \rightarrow$ vô cùng.



- **Các đặc trưng của kênh liên tục:**

- Trường dấu lối vào (sau bộ điều chế): $S = \{s(t), w_1(s)\}$
- Trường dấu lối ra (trước bộ giải điều chế): $U = \{u(t), w_1(u)\}$
- Hàm mật độ phân bố để xuất hiện $U_j(t)$ khi đã phát $s_i(t)$: $W(U_j(t)/s_i(t))$
- Khả năng thông qua của kênh.

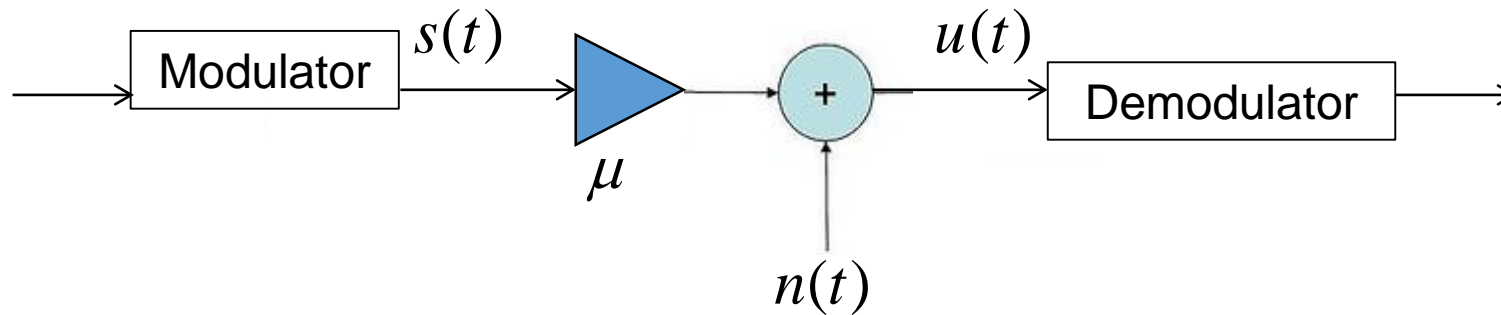
- **Tính chất kênh liên tục trong kênh rời rạc:**

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

$$C'_{lt} \geq C'_{rr \text{ chứa kênh liên tục}}$$

Kênh AWGN không nhớ

$$u(t) = \mu \cdot s(t) + n(t) \quad \mu = \text{const}, (\neq t).$$



AWGN Channel

$n(t)$ AWGN- Additive white Gaussian Noise: nhiễu cộng, mật độ phổ công suất không đổi rộng vô hạn (tạp âm trắng), biên độ ngẫu nhiên có phân bố chuẩn.



Khả năng thông qua của kênh AWGN

Là giá trị cực đại của lượng tin truyền qua kênh AWGN trong một đơn vị thời gian, lấy theo mọi khả năng có thể có của phân bố xác suất nguồn phát, trong đó có tính đến giới hạn công suất phát và công suất tạp nhiễu.

$$C' = \nu_k \cdot \max I(U; S)$$

ν_k Tốc độ truyền tin của kênh

- Dung lượng kênh AWGN: $C = \max I(U; S)$

- Nếu tín hiệu là hàm liên tục theo thời gian liên tục, khả năng thông qua của kênh AWGN với băng tần hữu hạn F và giới hạn công suất trung bình tín hiệu hữu ích nhận được $P_{\mu s}$, có nhiễu với mật độ phổ công suất hai phía $N_0/2$ được xác định bởi:

$$C' = F \log \left(1 + \frac{\mu^2 P_s}{N_0 F} \right) = F \cdot \log(1 + \text{SNR}) \quad \text{bps}$$

- F : BW của kênh
 - P_n : là công suất trung bình của nhiễu trong dải F .
 - $P_n = N_0 \cdot F$: với trường hợp nhiễu tạp âm trắng.
 - N_0 : Mật độ phổ công suất của nhiễu cộng.
- Nếu $F \rightarrow \infty$, tức là khi dải thông của kênh là vô hạn:

$$C'_\infty = \lim_{F \rightarrow \infty} C' = (\log_2 e) \left(\frac{\mu^2 P_s}{N_0} \right) = 1,443 \cdot \frac{P_{\mu s}}{N_0} \quad \text{bps}$$



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

Các nguồn tin 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 R_n của nguồn nhỏ hơn khả năng thông qua của kênh.

Ngược lại, không thể thực hiện được mã hoá và giải mã với xác suất sai bé tùy ý được.



Tài liệu tham khảo

- David J. C. Mackay, **Information Theory, Inference, and Learning Algorithms**, Cambridge University Press, 2003
- McEliece R.J., **The theory of Information and coding**, Cambridge University Press, 1985
- John Proakis & Masoud Salehi, **Digital Communication**, 2007