Introducción a la Teoría de la Información

El Canal Gaussiano

Facultad de Ingeniería, UdelaR

Año 2023

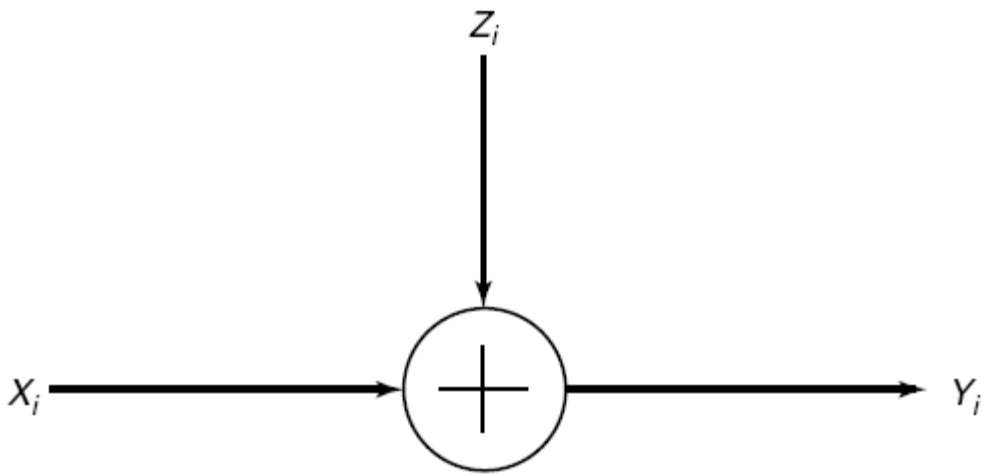
Definición

Definición (Canal Gaussiano)

Canal de tiempo discreto cuya salida en el tiempo i está dada por

$$Y_i = X_i + Z_i$$

donde X_i es una señal continua y $Z_i \sim \mathcal{N}(0, N)$ es i.i.d. e independiente de X_i para todo i.



Restricciones

- Si no se incorpora ningún tipo de restricción, la capacidad de este canal es infinita.
- En general se restringe la potencia media de X

$$\frac{1}{n}\sum_{i}^{n} x_i^2 \leq P$$

Capacidad de Información

Definición

La capacidad de información de un canal con restricción de potencia P es

$$C = \max_{f:E_f\left[X^2\right]\leq P} I(X;Y)$$

Definición informacional

Capacidad de Información del Canal Gaussiano

Teorema

Para un canal Gaussiano, se cumple $C = \frac{1}{2}\log\left(1+\frac{P}{N}\right)$

Demostración.

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) = h(Y) - h(X+Z|X) \\ &= h(Y) - h(Z|X) \\ &= h(Y) - h(Z) \end{aligned}$$

$$\text{var}(Y) = E\left[Y^2\right] - E\left[Y\right]^2 \leq E\left[Y^2\right]$$

$$E\left[Y^2\right] = E\left[(X+Z)^2\right] = E\left[X^2\right] + 2E\left[X\right]E\left[Z\right] + E\left[Z^2\right] \leq P + N$$

Como $h(Y) \leq \frac{1}{2}\log(2\pi e\sigma^2)$, donde $\sigma^2 = \text{var}(Y) \leq P+N$, obtenemos

$$h(Y) \leq \frac{1}{2}\log(2\pi e(P+N))$$

□

Es una cota.

Capacidad de Información del Canal Gaussiano (2)

Demostración.

Para $X \sim \mathcal{N}(0, P)$, Y es la suma de dos variables independientes, X, Z, cada una con distribución normal. Por lo tanto

$$Y \sim \mathcal{N}(0, P + N) \ ,$$

con lo cual se alcanza el máximo, $h(Y) = \frac{1}{2}\log(2\pi e(P+N))$.

$$\begin{aligned} I(X;Y) &= h(Y) - h(Z) \\ &= \frac{1}{2}\log(2\pi e(P+N)) - \frac{1}{2}\log(2\pi eN) \\ &= \frac{1}{2}\log\left(1 + \frac{P}{N}\right) \end{aligned}$$

□

Es alcanzable.

Códigos para un Canal Gaussiano

Definición (Código (M, n) con restricción de potencia P)

1. Un conjunto de índices $\{1, 2 \dots M\}$
2. Una función de codificación $x : \{1, 2 \dots M\} \to \mathcal{X}^n$, $x(w) = x_1(w), x_2(w) \dots x_n(w)$, tal que

$$\frac{1}{n} \sum_{i=1}^{n} x_i^2(w) \leq P, \quad \forall w \in \{1, 2 \dots M\}$$

3. Una función de decodificación $g : \mathcal{Y}^n \to \{1, 2 \dots M\}$

Capacidad del Canal Gaussiano con Restricción de Potencia P

Definición (Tasa alcanzable)

Una tasa R es *alcanzable* para un canal Gaussiano con restricción de potencia P si existe una sucesión de códigos $(2^{nR}, n)$ que satisfacen la restricción de potencia P y tienen probabilidad máxima de error $\lambda^{(n)} \to 0$.

Definición (Capacidad)

La *capacidad* de un canal Gaussiano con restricción de potencia P es el supremo de las tasas alcanzables.

Definición operacional

Intuición - Empaquetado de Esferas

- Si emitimos $(x_1 \dots x_n)$, recibimos $(Y_1 \dots Y_n)$ con $Y_i = x_i + Z_i$ y tenemos que

$$\frac{1}{n}\sum (Y_i - x_i)^2 = \frac{1}{n}\sum Z_i^2 \to E\left[Z_i^2\right] = N\,.$$

  Con gran probabilidad, $\sum (Y_i - x_i)^2 \leq n(N+\epsilon)$, $(Y_1 \dots Y_n)$ está contenido en una esfera de radio $\sqrt{n(N+\epsilon)}$ y centro $(x_1 \dots x_n)$

- De forma similar,

$$\begin{aligned}\frac{1}{n}\sum Y_i^2 &= \frac{1}{n}\sum (X_i + Z_i)^2 = \frac{1}{n}\sum X_i^2 + 2X_iZ_i + Z_i^2 \\ &\leq P + \frac{1}{n}\sum 2X_iZ_i + \frac{1}{n}\sum Z_i^2\,.\end{aligned}$$

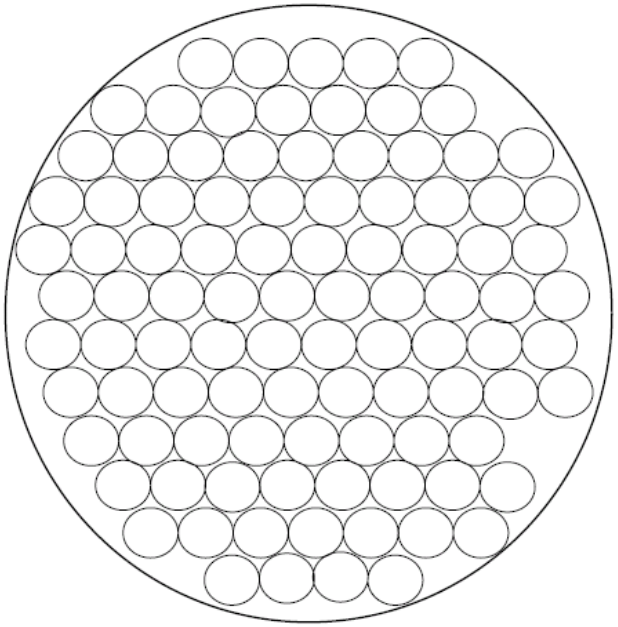
  Si $\{X_i\}$ son i.i.d., con gran probabilidad $(Y_1 \dots Y_n)$ está contenido en una esfera de radio $\sqrt{n(P+N+\epsilon)}$ y centro en cero.

Intuición - Empaquetado de Esferas

El volumen de una esfera de radio r es $C_n r^n$, por lo que la cantidad máxima de esferas de radio $\sqrt{nN}$ que pueden empaquetarse en una de radio $\sqrt{n(P+N)}$ es

$$\frac{C_n \Big(n(P+N)\Big)^{\frac{n}{2}}}{C_n \Big(nN\Big)^{\frac{n}{2}}} = \left(1+\frac{P}{N}\right)^{\frac{n}{2}} = 2^{n\frac{1}{2}\log\left(1+\frac{P}{N}\right)}$$

de donde surge que $R \sim \frac{1}{2}\log\left(1+\frac{P}{N}\right)$



Teorema de Capacidad del Canal Gaussiano

Teorema

La capacidad del canal Gaussiano con restricción de potencia P es $C = \frac{1}{2}\log\left(1 + \frac{P}{N}\right)$

Probamos primero que la tasa es alcanzable.

1. Generamos un código aleatoriamente sorteando $X_i(w) \sim \mathcal{N}(0, P - \epsilon)$, i.i.d, $i = 1, 2 \ldots n$, para las palabras $w = 1, 2 \ldots 2^{nR}$. El código es conocido tanto por el codificador como por el decodificador. Cada palabra es un vector n dimensional cuyas coordenadas son normales.
2. Codificación: El mensaje w se codifica como $X^n(w) = (X_1(w) \ldots X_n(w))$. Si $X^n(w)$ no satisface la restricción de potencia se emite una palabra arbitraria.
3. Decodificación: Se recibe Y^n. Si existe un único w tal que $X^n(w)$ satisface la restricción de potencia y es conjuntamente típica con Y^n, decodificamos $\hat{W} = w$. De lo contrario tomamos una decisión arbitraria.

Teorema de Capacidad del Canal Gaussiano

Consideramos un mensaje arbitrario, w, y los siguientes eventos:

$$\begin{aligned} B_w &= \left\{ \frac{1}{n} \sum_{j=1}^{n} X_j^2(w) > P \right\}, \\ E_{w,u} &= \left\{ (X^n(u), Y^n) \in A_\epsilon^{(n)} \right\}, 1 \leq u \leq 2^{nR}, \\ \mathcal{E}_w &= \{ \hat{W} \neq w \}. \end{aligned}$$

Observamos que

$$\mathcal{E}_w \subseteq B_w \cup E_{w,w}^c \cup \bigcup_{u \neq w} E_{w,u},$$

y por lo tanto, para $\mathcal{E} = \{\hat{W} \neq W\}$, se cumple que

$$P(\mathcal{E}|W = w) \leq P(B_w|W = w) + P(E_{w,w}^c|W = w) + \sum_{u \neq w} P(E_{w,u}|W = w)$$

Teorema de Capacidad del Canal Gaussiano

$$
\begin{aligned}
P(\mathcal{E}|W=w) &\leq P(B_w|W{=}w) + P(E_{w,w}^c|W{=}w) + \sum_{u\neq w} P(E_{w,u}|W{=}w) \\
&\leq \epsilon + \epsilon + \sum_{u\neq w} 2^{-n(I(X;Y)-3\epsilon)} \\
&\leq \epsilon + \epsilon + 2^{nR}2^{-n(I(X;Y)-3\epsilon)} \\
&= \epsilon + \epsilon + 2^{-n(I(X;Y)-3\epsilon-R)} \\
&\leq 3\epsilon
\end{aligned}
$$

para n grande y $R < I(X;Y) - 3\epsilon = \frac{1}{2}\log\left(1+\frac{P-\epsilon}{N}\right) - 3\epsilon$.

Teorema de Capacidad del Canal Gaussiano

Para cada w, $P(\mathcal{E}|W = w) \leq 3\epsilon$, entonces, promediando obtenemos

$$\frac{1}{2^{nR}} \sum_{w} P(\mathcal{E}|W = w) \leq 3\epsilon \,.$$

La probabilidad de error promediada sobre todos los códigos y todas las palabras de código está acotada por 3ϵ. Por lo tanto, existe algún código, $\mathcal{C}$, tal que

$$P_e^{(n)}(\mathcal{C}) \leq 3\epsilon \,,$$

donde $P_e^{(n)}(\mathcal{C})$ es la probabilidad de error promediada sobre todas las palabras de código, para el código $\mathcal{C}$.

Recíproco

Consideramos una secuencia de códigos $(2^{nR}, n)$ con $P_e^{(n)} \to 0$.
Con la distribución uniforme sobre W, podemos escribir

$$nR = H(W) = I(W; \hat{W}) + H(W|\hat{W})$$

Por Fano, $H(W|\hat{W}) \leq 1 + nRP_e^{(n)} = n\epsilon_n$, por lo que

$$nR \leq I(W; \hat{W}) + n\epsilon_n$$

Tenemos $W \to X^n(W) \to Y^n \to \hat{W}$ y por lo tanto

$$\begin{aligned} nR &\leq I(X^n; Y^n) + n\epsilon_n \\ &= h(Y^n) - h(Y^n|X^n) + n\epsilon_n \\ &= h(Y^n) - h(Z^n) + n\epsilon_n \\ &\leq \sum_{i=1}^{n} h(Y_i) - h(Z^n) + n\epsilon_n \\ &= \sum_{i=1}^{n} h(Y_i) - \sum_{i=1}^{n} h(Z_i) + n\epsilon_n \end{aligned}$$

Recíproco

La distribución uniforme sobre W induce una distribución uniforme sobre las palabras de código. Por lo tanto, para $P_i = E\left[X_i^2\right]$,

$$P_i = E\left[X_i^2\right] = \frac{1}{2^{nR}} \sum_w x_i^2(w)$$

$$\text{var}(Y_i) = E\left[Y_i^2\right] - E\left[Y_i\right]^2 \leq E\left[Y_i^2\right]$$

$$E\left[Y_i^2\right] = E\left[(X_i + Z_i)^2\right] = E\left[X_i^2\right] + 2E\left[X_i\right]E\left[Z_i\right] + E\left[Z_i^2\right] = P_i + N$$

$$h(Y_i) \leq \frac{1}{2}\log 2\pi e(P_i + N)$$

$$\begin{aligned} nR &\leq \sum h(Y_i) - \sum h(Z_i) + n\epsilon_n \\ &\leq \sum \frac{1}{2}\log 2\pi e(P_i + N) - \sum \frac{1}{2}\log 2\pi eN + n\epsilon_n \\ &= \sum \frac{1}{2}\log\left(1 + \frac{P_i}{N}\right) + n\epsilon_n \end{aligned}$$

Recíproco

$$
\begin{aligned}
R &\leq \frac{1}{n}\sum_{i=1}^{n}\frac{1}{2}\log\left(1+\frac{P_i}{N}\right)+\epsilon_n \\
&\leq \frac{1}{2}\log\left(1+\frac{1}{n}\sum_{i=1}^{n}\frac{P_i}{N}\right)+\epsilon_n \qquad Jensen \\
&\leq \frac{1}{2}\log\left(1+\frac{P}{N}\right)+\epsilon_n
\end{aligned}
$$

Donde la última desigualdad surge de que

$$
\begin{aligned}
\frac{1}{n}\sum_{i=1}^{n}P_i &= \frac{1}{n}\sum_{i=1}^{n}\frac{1}{2^{nR}}\sum_{w}x_i^2(w) \\
&= \frac{1}{2^{nR}}\sum_{w}\frac{1}{n}\sum_{i=1}^{n}x_i^2(w) \\
&\leq \frac{1}{2^{nR}}\sum_{w}P = P
\end{aligned}
$$

Canal Gaussiano de Ancho de Banda Limitada W

- Canal de tiempo continuo.
- Por el Teorema de Muestreo existen $2W$ grados de libertad por segundo. El canal se puede discretizar sin pérdida de capacidad.
- En tiempo $(0, T)$ tenemos $2WT$ muestras con potencia media $PT/2WT = P/2W$
- Ruido blanco Gaussiano de ancho de banda W hertz y densidad espectral de potencia $N_0/2$. Cada muestra tiene ruido Gaussiano independiente de varianza $N_0/2$
- La capacidad por uso de canal es

$$C = \frac{1}{2}\log\left(1 + \frac{P/2W}{N_0/2}\right) = \frac{1}{2}\log\left(1 + \frac{P}{N_0 W}\right) \text{ bits por uso de canal}$$

- Como hay $2W$ muestras por segundo, la capacidad en bits/seg es

$$C = W\log\left(1 + \frac{P}{N_0 W}\right) \to \frac{P}{N_0}\log e \quad \text{cuando } W \to \infty$$

Consideraciones sobre la capacidad

La capacidad en bits/s es $C = W \log\left(1 + \frac{P}{N_0 W}\right)$.

- si $P \to \infty$, $C \to \infty$
- si $N_0 \to 0$, $C \to \infty$

Mediante transformaciones se puede transmitir en un ancho de banda diferente del de la señal original, como en FM por ejemplo.
A la entrada del detector se recibe:
$C_R = B_T \log\left(1 + \frac{P_R}{N_0 B_T}\right)$.

A la salida se reconstruye la señal de ancho de banda W. La tasa de transferencia de información es:
$R \leq W \log\left(1 + \frac{P_D}{N_D}\right)$.
El mejor caso es $C_R = R$.

$B_T \log[1 + \left(\frac{P}{N}\right)_R] = W \log[1 + \left(\frac{P}{N}\right)_D]$.

Si $B_T \gg W$ entra más ruido pero se puede mejorar la relación señal ruido detectada.