Introdução a Teoria da Informação TI0056 2014.1

Capacidade e Teorema da Capacidade de Canal

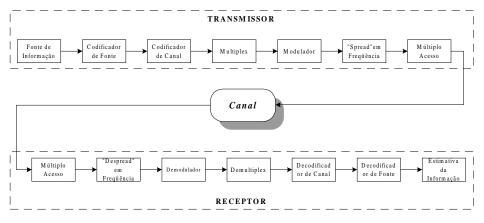
Prof. Walter C. Freitas Jr

walter@gtel.ufc.br

Grupo de Pesquisa em Telecomunicações Sem Fio (GTEL)
http://www.gtel.ufc.br/~walter
http://sites.google.com/site/walterjr/
http://sites.google.com/site/profwalterfreitas/

Curso de Graduação em Engenharia de Teleinformática (CGETI)

Sistema de comunicação - modelo geral



Introdução

A entropia representa a informação esperada por cada símbolo de fonte.

- Se tivermos duas fontes com iguais entropias, aquela que produzir mais símbolos por unidade de tempo vai colocar mais exigências no sistema de comunicações.
- ▶ O ritmo de informação mede a quantidade de informação produzida num certo intervalo de tempo.
- Existem limitações físicas fundamentais à transferência de informação (ruído, largura de banda, potência, ...), que se refletem na capacidade do canal.
- ► A capacidade do canal (em bits/s) mede a quantidade de informação que um canal pode transferir por unidade de tempo.
- Shannon relacionou estes dois conceitos através do teorema da codificação de canal, também chamado Teorema Fundamental da Teoria da Informação.

Considerações gerais

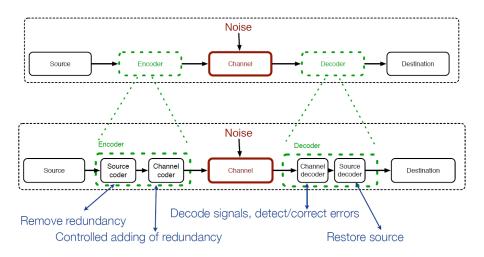
- Codificador de fonte retira redundância compactação da informação
- Canal insere perturbações/interferência
- Necessidade de inserção de redundância (conhecida) para evitar/minimizar os efeitos do canal
- Transferência de informação torna-se complicada
- ▶ Necessidade de inclusão de algum controle de qualidade na mensagem

Pergunta

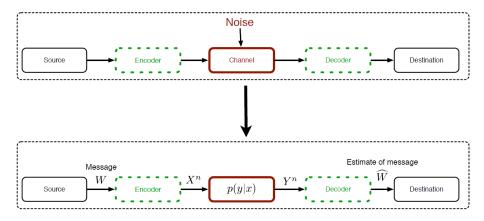
Qual o limite de informação que pode ser transmitida, sem erros, através de um canal que insere perturbação na mensagem?

Teorema da Capacidade de Canal

Sistema de comunicação - modelo geral simplificado



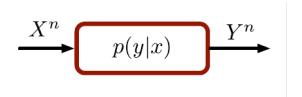
Sistema de comunicação - modelo geral simplificado



Canal discreto sem memória

Definição:

Um canal discreto é o meio (físico ou abstrato) de conexão entre a entrada $X\in\mathcal{X}$ e a saída $Y\in\mathcal{Y}$, descrito pela probabilidade condicional p(y|x) para a saída y quando a entrada é x



Teorema da Capacidade de Canal

Definição

A capacidade de informação de um canal é a quantidade máxima de informação capaz de ser transmitida, *bits por uso do canal*, sem erro de transmissão.



Define-se então:

$$C = \max_{p_X(x)} \mathcal{I}(X, Y) \tag{1}$$

$$\mathcal{I}(X,Y) = \mathcal{H}(X) - \mathcal{H}(X|Y) = \mathcal{H}(Y) - \mathcal{H}(Y|X) \tag{2}$$

Capacidade de canal

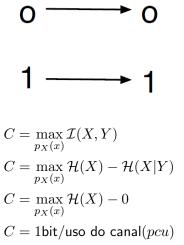
- ▶ Capacidade de canal é uma função apenas das probabilidades condicionais $P(y_k|x_i)$ que definem o canal
- ► A maximização em relação às probabilidades dos símbolos (codificados) da fonte é sujeita a
 - 1. $P(x_i) \ge 0$, para todo i
 - 2. $\sum_{i=0}^{K-1} P(x_i) = 1$



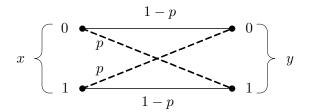
Capacidade de canal - propriedades

- 1. $C \ge 0$, uma vez que $\mathcal{I}(X,Y) \ge 0$
- 2. $C \leq \log[|X|]$, uma vez que $C = \max \ \mathcal{I}(X,Y) \leq \max \ \mathcal{H}(X) = \log[|X|]$
- $3. C \leq \log[|Y|]$
- 4. $\mathcal{I}(X,Y)$ é uma função contínua de $p_X(x)$
- 5. $\mathcal{I}(X,Y)$ é uma função côncava de $p_X(x)$

Canal sem ruído



Canal Binário Simétrico (BSC)



- Diagrama é unicamente definido pela probabilidade de transição
- A entropia é maximizada quando $Pr(x_0) = Pr(x_1) = 1/2$

Canal Binário Simétrico (BSC)

- $ightharpoonup \Pr(y_0|x_1) = \Pr(y_1|x_0) = p$
- $\Pr(y_0|x_0) = \Pr(y_1|x_1) = 1 p$
- Sabendo que

$$\mathcal{I}(X,Y) = \mathcal{H}(Y) - \mathcal{H}(Y|X)$$

A entropia $\mathcal{H}(Y)$ é máxima quando as saídas são equiprováveis \Rightarrow entradas equiprováveis. Nesse caso $\mathcal{H}(Y)=1$ bit/símbolo.

$$\mathcal{H}(Y|X) = \sum_{i=1}^{M} p(x_i)\mathcal{H}(Y|x_i)$$

$$\mathcal{H}(Y|X) = P(X=0)\mathcal{H}(Y|X=0) + P(X=1)\mathcal{H}(Y|X=1)$$

$$\mathcal{H}(Y|X) = P(X=0)\underbrace{\mathcal{H}(1-p,p)}_{\Omega(p)} + P(X=1)\underbrace{\mathcal{H}(1-p,p)}_{\Omega(p)} = \Omega(p)$$

$$C_{BSC} = 1 - \Omega(p)$$

$$C_{BSC} = 1 + p \cdot \log[p] + (1 - p) \cdot \log[1 - p]$$

Canal Binário Simétrico (BSC)

- $\Pr(y_0|x_1) = \Pr(y_1|x_0) = p$
- $\Pr(y_0|x_0) = \Pr(y_1|x_1) = 1 p$
- Sabendo que

$$\mathcal{I}(X,Y) = \sum_{k=0}^{K-1} \sum_{j=0}^{J-1} P(x_j, y_k) \cdot \log \left[\frac{P(y_k | x_j)}{P(y_k)} \right]$$

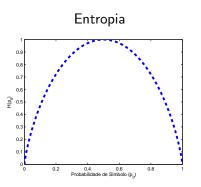
▶ Logo

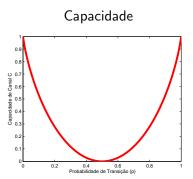
$$C = 1 + p \cdot \log[p] + (1 - p) \cdot \log[1 - p]$$

= 1 - \mathcal{H}(p, 1 - p)



Canal Binário Simétrico (BSC)



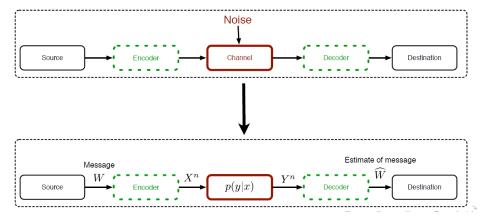


Canal Binário Simétrico (BSC)

- Curva simétrica (esperado!)
- ightharpoonup Quando não há ruído (p=0) a capacidade de canal é máxima, com um bit por uso do canal. Neste mesmo valor, a entropia atinge seu valor mínimo
- ▶ Com a probabilidade de erro p=1/2, a capacidade atinge o menor valor enquanto a entropia atinge o máximo. Nestes casos, o canal é dito ser **sem utilidade** (useless)
- ightharpoonup Com a probabilidade de erro p=1, o canal inverte o símbolo transmitido de maneira determinística, logo, a inversão pode ser realizada no receptor atingindo também nesse caso capacidade máxima

Exemplo Ilustrativo - Transmissão de Imagens

- Imagens lena e xadrez
- ► Luminância valores dos pixels [0-255]
- ▶ Canal BSC probabilidade de erro p
- ▶ Source code: comprimento fixo $\lceil \log_2 256 \rceil$

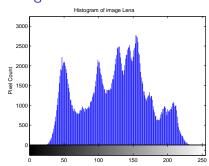


Exemplo Ilustrativo - Lena

Imagem Transmitida



Histograma



Exemplo Ilustrativo - Lena

Imagem Transmitida



Imagem Recebida p = 0.2

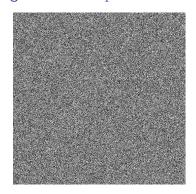


Exemplo Ilustrativo - Lena

Imagem Transmitida



Imagem Recebida p = 0.5



Exemplo Ilustrativo - Lena

Imagem Transmitida



Imagem Recebida p = 0.8



Exemplo Ilustrativo - Lena

Imagem Transmitida



Imagem Recebida p=1



Exemplo Ilustrativo - Lena

Imagem Transmitida

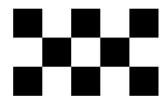


 $\label{eq:magem_posterior} \mbox{Imagem Recebida} \ p=1 \ \mbox{e}$ $\mbox{Invertida}$

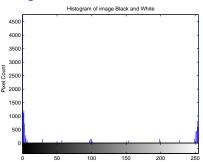


Exemplo Ilustrativo - bw

Imagem Transmitida



Histograma



Exemplo Ilustrativo - bw

Imagem Transmitida

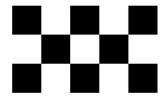
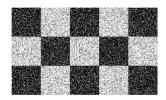


Imagem Recebida p = 0.2



Exemplo Ilustrativo - bw

Imagem Transmitida

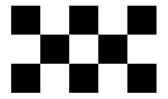
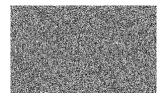


Imagem Recebida p=0.5



Exemplo Ilustrativo - bw

Imagem Transmitida

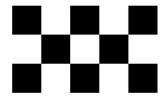
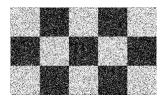


Imagem Recebida p = 0.8



Exemplo Ilustrativo - bw

Imagem Transmitida

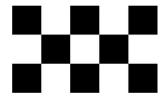
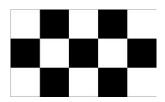


Imagem Recebida p=1



Exemplo Ilustrativo - bw

Imagem Transmitida

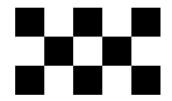
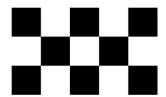


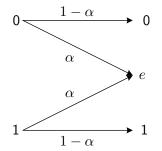
Imagem Recebida p=1 e Invertida



Capacidade de canal - outros exemplos

Canal binário com apagamento

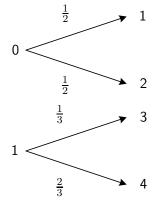
$$C = \max \mathcal{I}(X, Y) = 1 - \alpha$$
 bits



Capacidade de canal - outros exemplos

Canal com ruído com saídas não superpostas (não é canal com ruído!)

$$C = \max \mathcal{I}(X,Y) = 1$$
 bit, para $p(x) = (\frac{1}{2}, \frac{1}{2})$



Capacidade de canal - outros exemplos

"Máquina de escrever" com ruído

$$C = \max \mathcal{I}(X,Y) = \log[13] \text{bits}$$

$$A \longrightarrow A \\ B \\ C \longrightarrow C \\ D \longrightarrow D$$

$$E \longrightarrow D$$

$$G \longrightarrow G$$

$$\vdots$$

$$\vdots$$
Saídas não ruidosas
$$C = \max \mathcal{I}(X,Y) = \log[13] \text{bits}$$

Codificação de canal - motivação

- Como melhorar a resistência do canal aos efeitos do ruído?
- Definição do limite de confiabilidade
- ▶ Idéia:
 - ▶ Transformar a seqüência de dados em uma seqüência de entrada do canal
 - Minimizar os efeitos do ruído (interferência)
 - Mapeamento inverso após o canal para recuperar seqüência de dados

Como fazer isso?

Inserção de redundância!

Codificação de canal - definições

- ► Simplificado para códigos de bloco
- ightharpoonup Mensagem é subdividida em blocos seqüenciais cada um com k bits, e cada bloco é mapeado em um block de n bits em que n>k
- Número de bits de redundância: n-k
- ► A taxa de código é denominada a razão

$$r = \frac{k}{n} \tag{3}$$

Codificação de canal - definições

 Acuracidade da recuperação requer probabilidade de erro tão pequena quanto possível

Questão importante

Existe algum método sofisticado de codificação de canal tal que a probabilidade de erro seja menor que um número arbitrário positivo ϵ , em caso afirmativo, o esquema de codificação é eficiente tal que a taxa de codificação não necessite ser muito pequena?

Resposta

SIM!

Codificação de canal - definições

- ► A resposta é dada pelo teorema da capacidade de canal
- ► Generalização necessidade de se incluir o *tempo* como uma variável a ser considerada
- ▶ Suposições: fonte com alfabeto $\mathcal A$ e entropia $\mathcal H(A)$, emitindo sinais a cada T_s segundos
- ► Taxa média de informação

$$R = \frac{\mathcal{H}(A)}{T_s} \tag{4}$$

Codificação de canal - definições

- ightharpoonup O decodificador tem de fornecer também símbolos do alfabeto ${\cal A}$ a uma taxa de T_s segundos
- lacktriangle Seja a capacidade do canal dada por C bits por transmissão
- ightharpoonup Supondo que o canal é capaz de ser utilizando uma vez a cada T_c segundos
- ► Então, a capacidade do canal por unidade de tempo, representa a máxima taxa de transferência de informação pelo canal

$$\frac{C}{T}$$
 (5)

Teorema da Codificação de Canal

Segundo teorema de Shannon

Primeira parte

Seja uma fonte discreta com alfabeto $\mathcal A$ e entropia $\mathfrak H(A)$ que produz símbolos a cada T_s segundos. Seja um canal discreto sem memória com capacidade de canal C e utilizado a cada T_c segundos. Então, se

$$\frac{\mathcal{H}(A)}{T_s} \le \frac{C}{T_c} \tag{6}$$

existe um esquema de codificação para o qual a saída da fonte pode ser transmitida pelo canal e ser reconstruída com a uma probabilidade de erro arbitrariamente pequena. O parâmetro C/T_c é chamado de taxa crítica.

Teorema da Codificação de Canal

Segundo teorema de Shannon

Segunda parte

Inversamente, se

$$\frac{\mathcal{H}(A)}{T_s} > \frac{C}{T_c} \tag{7}$$

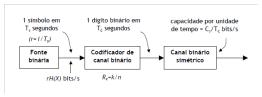
não é possível transmitir informação pelo canal e reconstruí-la com uma probabilidade de erro arbitrariamente pequena.

Teorema da Codificação de Canal - discussão

- ▶ O teorema da codificação de canal é o resultado isolado mais importante da teoria da informação
- ▶ O teorema especifica que a capacidade de canal C é um limite fundamental na taxa na qual a transmissão é confiável sem erros, através de um canal discreto sem memória
- O teorema não mostra como construir um "bom código"
- ▶ Resultado: se a Equação (6) é satisfeita então **um** bom código existe

Teorema da Codificação de Canal - aplicação Canal binário simétrico (BSC)

Considere-se uma fonte binária a gerar símbolos equiprováveis de duração T_s segundos, ou seja, a produzi-los à taxa de $r=1/T_s$ símbolos por segundo. Sendo os símbolos binários equiprováveis, a entropia da fonte vale $\mathcal{H}(X)=1$ bit/símbolo e a taxa de informação da fonte é $R=r\mathcal{H}(X)=1/T_s$ bits/s.



 $lackbox{O}$ Codificador (de canal!) produz um símbolo binário em cada T_c segundos, o qual é transmitido através de um canal binário simétrico (BSC) que, portanto, é usado uma vez em cada T_c segundos. Assim, a capacidade do canal por unidade de tempo é $C=C_s/T_c$ bits/s.

Teorema da Codificação de Canal - aplicação

Canal binário simétrico (BSC)

- Fonte: símbolos equiprováveis a cada T_s segundos, $\mathcal{H}(X)=1$ bit por símbolo
- lacktriangle Taxa de informação da fonte: $1/T_s$
- lacktriangle Codificador de canal com taxa de codificação R_c produzindo símbolos a cada T_c segundos
- lacktriangle Taxa de transmissão de símbolos codificados é $1/T_c$
- lacktriangle A capacidade de canal por unidade de tempo é C/T_c bits por segundo
- Logo, se

$$\frac{\mathcal{H}(X)}{T_s} \le \frac{C_s}{T_c} \Rightarrow \frac{1}{T_s} \le \frac{C_s}{T_c} \Rightarrow \frac{T_c}{T_s} \le C_s \tag{8}$$

a probabilidade de erro pode ser tão pequena quanto se deseje, usando uma codificação adequada

Teorema da Codificação de Canal - aplicação Canal binário simétrico (BSC)

► A taxa de codificação é igual à razão

$$R_c = T_c/T_s \tag{9}$$

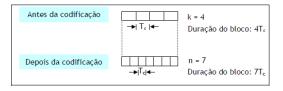
Então, pode-se escrever

$$R_c \le C_s \tag{10}$$

- Interpretação: para $R_c \leq C_s$ existe um código (com taxa de codificação menor ou igual a capacidade de canal) capaz de atingir uma taxa de erro arbitrariamente pequena
- ▶ Como a capacidade do canal BSC é $C_s = 1 \Omega(p) \Rightarrow R_c \leq 1 \Omega(p)$

Teorema da Codificação de Canal - aplicação

Porque é $\frac{T_c}{T_s} = R_C$



- A razão $\frac{k}{n} = R_c$ chama-se taxa de código
- lacktriangle Como a duração dos blocos é a mesma: $kT_s=nT_c$
- ▶ Nesse caso acima: $4T_s = 7T_c \Rightarrow T_c/T_s = 4/7 = R_c$

Em resumo, temos duas maneiras de exprimir o teorema da codificação de canal:

- ▶ Com a capacidade expressa em bits/símbolo, C_s : $R_c \le C_s$
- ▶ Com a capacidade expressa em bits/s, C: $R = r\mathcal{H}(X) \leq C$

$$C = \frac{C_s}{T_s}$$

Pergunta

Qual a capacidade de informação a ser transmitida por meio de um canal limitado em faixa, limitado em potência e gaussiano?

- ightharpoonup Seja X(t)
 - Processo estocástico estacionário
 - Média nula
 - Faixa limitada em B Hz
- As K amostras discretas amostradas na taxa de Nyquist (2B símbolos por segundo) são $X_k, k=1,2,\ldots,K$
- ► Amostras transmitidas a cada *T* segundos
- Canal limitado em faixa B Hertz
- Número de amostras

$$K = 2BT \tag{11}$$

- ▶ Canal inserção de ruído aditivo gaussiano branco de média zero e densidade espectral de potência $N_0/2$
- Ruído limitado em B Hertz
- ▶ Logo

$$Y_k = X_k + N_k, \qquad k = 1, 2, \dots, K$$
 (12)

 Amostras de ruído são gaussianas, estatisticamente independentes, com média zero e variância

$$\sigma^2 = N_0 B \tag{13}$$

 Como o canal é limitado em potência, cada entrada do canal deve ter uma função custo

$$\mathbb{E}\left\{X_{k}^{2}\right\} = P, \qquad k = 1, 2, \dots, K$$
 (14)

em que P é a potência média de transmissão

- ▶ Capacidade de informação é definida como o máximo da informação mútua entre a entrada X_k e a saída Y_k sobre todas as distribuições de probabilidade de X_k que satisfazem a restrição da Equação (14)
- Matematicamente

$$C = \max_{p_X(x)} \left\{ \mathcal{I}(X_k, Y_k) : \mathbb{E}\left\{ X_k^2 \right\} = P \right\}$$
 (15)

Sabendo

$$\mathcal{I}(X_k, Y_k) = \mathcal{H}(Y_k) - \mathcal{H}(Y_k|X_k) \tag{16}$$

E como X_k e N_k são independentes e a soma é igual a Y_k , tem-se

$$\mathcal{I}(X_k, Y_k) = \mathcal{H}(Y_k) - \mathcal{H}(N_k) \tag{17}$$

- ightharpoonup Como $\mathcal{H}(N_k)$ é independente da distribuição de X_k , maximizar a Equação (17) é maximizar a entropia de Y_k
- Para uma variância fixa, Y_k terá máxima entropia se $p_Y(y)$ for uma distribuição gaussiana (será provado mais adiante!)
- lacktriangle Logo, X_k também dever ser gaussiano e atender à restrição de potência

Então, escreve-se

$$C = \mathcal{I}(X_k, Y_k) : X_k$$
 gaussiano, $\mathbb{E}\left\{X_k^2\right\} = P$ (18)

- Cálculos
 - 1. Variância de Y_k é $P + \sigma^2$, logo

$$\mathcal{H}(Y_k) = \frac{1}{2} \log \left[2\pi e(P + \sigma^2) \right] \tag{19}$$

2. Variância do ruído N_k é σ^2 , assim

$$\mathcal{H}(N_k) = \frac{1}{2} \log \left[2\pi e \sigma^2 \right] \tag{20}$$

▶ Substituindo as Equações (19) e (20) na Equação (17) tem-se

$$C = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right)$$
 bits por transmissão (21)

▶ Lembrando que o canal é usado K vezes para transmitir as K amostras em T segundos, tem-se que a informação é dada por capacidade por unidade de tempo (K/T). Também K=2BT, logo

$$C = B \log \left(1 + \frac{P}{N_0 B} \right)$$
 bits por segundo (22)

Lei de Shannon-Hartley

Terceiro teorema de Shannon

A capacidade de informação de um canal contínuo de largura de faixa B Hertz corrompido com ruído aditivo gaussiano branco de densidade espectral de potência $N_0/2$ e limitado em faixa em B Hertz é dado por

$$C = B \log \left(1 + \frac{P}{N_0 B} \right) \text{ bits por segundo}$$
 (23)

Teorema da capacidade de informação Discussão

- Resultado mais famoso de Shannon
- Interrelaciona os parâmetros chaves de um sistema de transmissão: largura de faixa do canal, potência média transmitida e densidade espectral de potência
- ightharpoonup O teorema implica que, para uma dada P e largura de faixa do canal B pode-se transmitir informação a uma taxa de C bits por segundo com uma probabilidade de erro arbitrariamente pequena, utilizando suficientemente complexos sistemas de codificação
- Não é possível transmitir a uma taxa maior que C bits por segundo usando nenhum sistema de codificação e ter uma probabilidade de erro arbitrariamente pequena
- ▶ Limite fundamental da transmissão sem erros
- ► Para se aproximar deste limite o sinal deve ter estatísticas próximas do ruído gaussiano branco

Exemplo

Considere o canal de uma linha telefônica com largura de banda de 3.4 KHz.

- 1. Calcule a capacidade do canal para uma SNR de 30 dB.
- 2. Calcule a SNR necessária para suportar uma taxa de 4800 bps.

Solução:

1. $SNR=30 \text{ dB} \rightarrow SNR = 1000 \text{ (em escala linear)}$

$$C = B\log_2(1 + SNR) \tag{24}$$

$$C = 3.4\log_2(1 + 1000)$$

$$C = 33.9 \text{kbps} \tag{26}$$

2. C = 4800 bps

$$SNR = 2^{C/B} - 1 (27)$$

$$SNR = 2^{4.8/3.4} - 1 \tag{28}$$

$$SNR = 1.66 = 2.2 dB$$
 (29)

(25)

- Sendo o canal limitado em faixa e potência, qual o impacto do teorema da capacidade de informação?
- ► Framework prático sistema ideal
- ightharpoonup Taxa de bits R_b igual à capacidade de informação C
- Potência média de transmissão

$$P = E_b C (30)$$

em que E_b é a **energia por bit**

▶ Logo, para o sistema ideal

$$\frac{C}{B} = \log\left(1 + \frac{E_b}{N_0} \frac{C}{B}\right) \tag{31}$$

Um sistema ideal com largura de banda infinita tem uma capacidade de canal finita:

$$C = B \log_2 \left(1 + \frac{S}{N_0 B} \right) \tag{32}$$

$$\lim_{B \to \infty} C = \lim_{B \to \infty} B \log_2 \left(1 + \frac{S}{N_0 B} \right) \tag{33}$$

$$= \lim_{B \to \infty} \frac{S}{N_0} \left[\frac{N_0 B}{S} \log_2 \left(1 + \frac{S}{N_0 B} \right) \right] \tag{34}$$

Como $\lim_{x \to \infty} x \log_2\left(1 + \frac{1}{x}\right) = \log_2 e = 1,44$. Portanto

$$C_{\infty} = \lim_{R \to \infty} C \approx \frac{S}{N_0} 1,44 \tag{35}$$

$$C_{\infty} = 1,44 \frac{S}{N_0} \tag{36}$$

Existe um valor limite de E_b/N_0 (limite de Shannon) abaixo do qual não pode haver comunicação sem erros, qualquer que seja o ritmo de transmissão. Sendo T a duração de cada bit, E_b a sua energia e R=1/Tbits/s, então

$$\frac{S}{N} = \frac{E_b/T}{N_0 B} = \frac{E_b}{N_0} \frac{R}{B} \Rightarrow C = B \log_2 \left(1 + \frac{S}{N} \right) = B \log_2 \left(1 + \frac{E_b}{N_0} \frac{R}{B} \right) \tag{37}$$

Mas
$$R \le C \Rightarrow \frac{R}{B} \le \frac{C}{B} = \left(1 + \frac{E_b}{N_0} \frac{R}{B}\right)$$

Se
$$B \to \infty \Rightarrow \frac{R}{B} \le \log_2\left(1 + \frac{E_b}{N_0} \frac{R}{B}\right) = \frac{\ln\left(1 + \frac{E_b}{N_0} \frac{R}{B}\right)}{\ln 2} \approx \frac{\frac{E_b}{N_0} \frac{R}{B}}{\ln 2}$$

Portanto.

$$\left| \frac{E_b}{N_0} \ge \ln 2 = 0.693 \ (-1.59 \mathrm{dB}) \right|$$
 Limite de Shannon

(38)

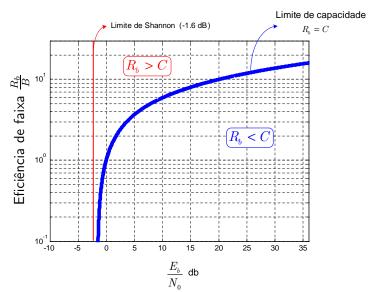


De maneira equivalente pode-se definir a relação energia do sinal por bit pela densidade espectral de potência em termos da eficiência de faixa como

$$\frac{E_b}{N_0} = \frac{2^{C/B} - 1}{C/B} \tag{39}$$

ightharpoonup Eficiência de faixa $\frac{C}{B}$

Curva de eficiência de faixa - limite de Shannon



Fim do Tópico

