

Introdução à Teoria da Informação

E J Nascimento

Universidade Federal do Vale do São Francisco

www.univasf.edu.br/~edmar.nascimento

July 24, 2019

- 1 Conceitos Básicos
- 2 Codificação de Fonte
- 3 Codificação de Canal

Introdução

- A teoria da informação foi estruturada por Claude Elwood Shannon em seu artigo **A Mathematical Theory of Communication** publicado em 1948

Reprinted with corrections from *The Bell System Technical Journal*,
Vol. 27, pp. 379–423, 623–656, July, October, 1948.

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist¹ and Hartley² on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

Introdução

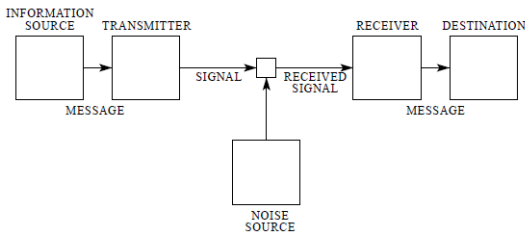
- Antes do trabalho de Shannon, vários sistemas de comunicação já se encontravam em operação, embora sem um arcabouço ou fundamentação matemática
 - Telégrafo (a partir de 1830), telefone (1870)
 - Telégrafo sem fio (1890)
 - Rádio AM (1900), modulação SSB (1920)
 - Televisão (1930), teletipo (1930)
 - Modulação FM (1930), PCM (1930)
 - Espalhamento espectral (1940)
- Shannon era graduado em engenharia elétrica e matemática
- Na sua dissertação de mestrado no MIT, ele formalizou o uso da lógica booleana na síntese de circuitos digitais

Introdução

- No período da Segunda Guerra Mundial, Shannon trabalhou no Bell Labs em assuntos relacionados à criptografia
- Antes de Shannon, o conceito de informação associado a probabilidades foi abordado por Nyquist em 1924
 - Utilizava-se o termo quantidade de **conhecimento** (intelligence) enviada através de um cabo
- Além disso, no código Morse, as letras mais frequentes eram codificadas com menos símbolos a fim de agilizar o processo de digitação
 - Algo que foi formalizado por Shannon ao introduzir o conceito de entropia de uma fonte de informação

Introdução

- Uma das grandes sacadas da teoria da informação foi reduzir sistemas de comunicação complexos a modelos simples



- O nível de abstração adotado por Shannon permitiu separar informação e semântica de uma mensagem
 - *The semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages*

Medida de Informação

- Quanto mais improvável é um evento, mais informação ele contém
 - O sol vai brilhar em Petrolina amanhã
 - O Brasil vai ser hexacampeão em 2022
 - Vai nevar em Juazeiro neste inverno
- A informação é ligada a incerteza, ou seja, quanto mais improvável um evento é, mais informação ele carrega

$$P \rightarrow 1, I \rightarrow 0, \quad P \rightarrow 0, I \rightarrow \infty$$

- Isto sugere como medida de informação

$$I \sim \log \frac{1}{P}$$

Medida de Informação

- Considerando que se deseja transmitir mensagens representadas por dígitos binários, em que cada mensagem possui uma probabilidade de ocorrência P , a informação em bits é dada por

$$I = \log_2 \frac{1}{P} \text{ bits}$$

- n mensagens equiprováveis $P = 1/n$ resultam em $\log_2 n$ bits de informação
- I pode ser interpretado como o número mínimo de bits necessário para codificar a mensagem
- Como a codificação não é necessariamente binária, a base do logaritmo pode ser diferente, uma base r correspondendo a sinais r -ários

Medida de Informação

- A unidade mais comum de informação é o bit, assim é comum omitir-se o 2 do logaritmo a fim de simplificar a notação
- Considera-se uma fonte sem memória que emite mensagens $m_1, m_2, \dots, m_n$ com probabilidades $P_1, P_2, \dots, P_n$, com $P_1 + P_2 + \dots + P_n = 1$
- O conteúdo de informação em cada mensagem m_i é dado por

$$I_i = \log \frac{1}{P_i} \text{ bits}$$

- A informação média por mensagem é chamada de **entropia da fonte** e é dada por

$$H(m) = \sum_{i=1}^n P_i I_i = \sum_{i=1}^n P_i \log \frac{1}{P_i} = - \sum_{i=1}^n P_i \log P_i \text{ bits}$$

Medida de Informação

- Pode-se observar que a entropia de uma fonte é função das probabilidades das mensagens e não da natureza das mensagens
- Fontes com distribuições distintas vão possuir entropias diferentes
- A fonte com entropia máxima possui a máxima incerteza
- Através de um procedimento de maximização, pode-se verificar que a distribuição uniforme maximiza a entropia (máxima incerteza)
- Nesse caso, $P_1 = P_2 = \dots = P_n = 1/n$ e $H(m) = \log n$

Codificação de Fonte

- Assim, se a fonte for equiprovável, o número mínimo de bits para codificar a fonte é $\log(1/P)$
- Quando a fonte não for equiprovável, o número mínimo de bits por mensagem é dado por $H(m)$
- Para chegar a esse resultado, considera-se uma sequência de N mensagens quando $N \rightarrow \infty$
- Se k_i é o número de vezes que a mensagem m_i ocorre na sequência, então

$$\lim_{N \rightarrow \infty} \frac{k_i}{N} = P_i$$

- Se $N \rightarrow \infty$, m_i ocorre NP_i vezes na sequência de N mensagens

Codificação de Fonte

- Em uma **sequência típica** de N mensagens
 - m_1 ocorre NP_1 vezes, m_2 ocorre NP_2 vezes, etc.
- Composições diferentes são extremamente improváveis (atípicas)
- Em uma sequência típica, a proporção de ocorrências das mensagens é a mesma, embora a ordem seja diferente
- A probabilidade ocorrência de uma sequência típica é dada por

$$P(S_N) = (P_1)^{NP_1} (P_2)^{NP_2} \dots (P_n)^{NP_n}$$

- Todas as possíveis sequências típicas são equiprováveis com probabilidade $P(S_N)$

Codificação de Fonte

- Para codificar uma sequência típica é necessário

$$\begin{aligned} L_N &= \log \frac{1}{P(S_N)} \text{ bits} \\ &= N \sum_{i=1}^n P_i \log \frac{1}{P_i} = NH(m) \text{ bits} \end{aligned}$$

- Assim, o número médio de dígitos binários por mensagem é dado por

$$L = \frac{L_N}{N} = H(m) \text{ bits}$$

- $H(m)$ representa o número mínimo de bits necessário para codificar a fonte

Código de Huffman

- Idealmente, para se alcançar o mínimo de $H(m)$ bits por mensagem, é necessário uma sequência de comprimento infinito
- Existem métodos que alcançam resultados próximos do valor ótimo com sequências de comprimento finito
 - Huffman, Shannon-Fano, aritmética, etc.
- Com o código de Huffman, uma fonte com 6 mensagens e probabilidades $(0,3; 0,25; 0,15; 0,12; 0,10; 0,08)$ é codificada com $(00, 10, 010, 011, 110, 111)$
- Nesse caso $L = 2,45$ e $H(m) = 2,418$ e a eficiência do código é $\eta = H(m)/L = 0,976$
- A redundância do código é dada por $\gamma = 1 - \eta = 0,024$

Código de Huffman

- Apesar do código ser de comprimento variável, ele não apresenta ambiguidades
- É possível construir um código r -ário usando o mesmo procedimento
- Pode ser necessário incluir uma mensagem de probabilidade nula
- Com o código de Huffman quaternário, a fonte com 6 mensagens e probabilidades $(0,3; 0,25; 0,15; 0,12; 0,10; 0,08)$ é codificada como $(0,2,3,10,11,12)$
- Nesse caso $L = 1,3$ dígitos quaternários, $H_4(m) = 1,209$ unidades quaternárias e $\eta = 0,936$
- Para melhorar a eficiência, é necessário ir além de $N = 1$

Código de Huffman

- Um valor de $N = 2$ é conhecido como uma extensão de segunda ordem
- Considere uma fonte com 2 mensagens m_1 e m_2 com probabilidades $(0,8; 0,20)$
- Ela é codificada com $(0,1)$ e nesse caso, $L = 1$, $H(m) = 0,72$ e a eficiência do código é $\eta = 0,72$
- Uma extensão de segunda ordem codifica as mensagens $m_1m_1, m_1m_2, m_2m_1, m_2m_2$ com probabilidades $(0,64; 0,16; 0,16; 0,04)$ como $(0,11, 100, 101)$
- Nesse caso, $L' = 1,56$ e $L = 0,78$, resultando em $\eta = 0,72/0,78 = 0,923$

Código de Huffman

- Uma extensão de terceira ordem codifica as mensagens $m_1 m_1 m_1$, $m_1 m_1 m_2$, $m_1 m_2 m_1$, $m_2 m_1 m_1$, $m_1 m_2 m_2$, $m_2 m_1 m_2$, $m_2 m_2 m_1$, $m_2 m_2 m_2$ com probabilidades $(0,512; 0,128; 0,128; 0,128; 0,032; 0,032; 0,032; 0,008)$ como $(0,100, 101, 110, 11100, 11101, 11110, 11111)$
- Nesse caso, $L' = 2,184$ e $L = 0,728$, resultando em $\eta = 0,72/0,728 = 0,989$

Codificação de Canal

- Como foi visto, as mensagens de uma fonte podem ser codificadas usando $H(m)$ dígitos
- Se o comprimento médio por mensagem for igual à entropia, a redundância é nula
- Nesse caso, as mensagens codificadas não podem ser transmitidas por um canal ruidoso
 - A falta de redundância não permite recuperar as mensagens da fonte
- Para que haja comunicação livre de erros em um canal ruidoso, é necessário introduzir redundância através da codificação de canal
- A maneira mais simples de fazer codificação de canal é através de um código de repetição

Codificação de Canal

- O código binário de repetição mais simples faz o seguinte mapeamento

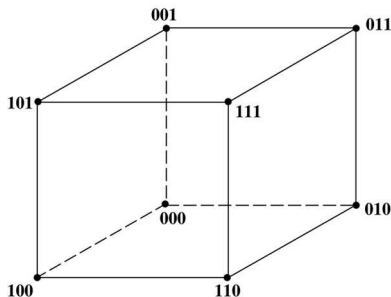
$$0 \rightarrow 000$$

$$1 \rightarrow 111$$

- 000 e 111 são chamados de palavras-código
- A decodificação é feita pela maioria, assim se forem recebidos os valores 001, 010, 100 e 000 se decide pelo 0, enquanto se forem recebidos 011, 101, 110 e 111 se decide pelo 1
- Definindo-se a distância de Hamming d_H como o número de valores em que as cadeias binárias diferem, pode-se dizer que o decodificador escolhe a palavra-código com a menor d_H

Codificação de Canal

- A distância de Hamming entre as palavras-código do código de repetição vale 3, o que permite corrigir 1 único erro
- No caso geral, um código com distância de Hamming mínima $d_{H(min)}$ pode corrigir $\lfloor d_{H(min)}/2 \rfloor$
- O valor $\lfloor d_{H(min)}/2 \rfloor$ é interpretado como o raio de uma esfera de Hamming em que não há sobreposição



Codificação de Canal

- O código de repetição não é eficiente e pode ser melhorado
- Admitindo-se que em um intervalo de T segundos se possui um bloco de αT dígitos binários e que se adiciona $(\beta - \alpha)T$ dígitos redundantes
 - São efetivamente transmitidos βT dígitos
 - Existem $2^{\alpha T}$ possíveis mensagens
 - Existem $2^{\beta T}$ possíveis mensagens transmitidas (vértices de um hipercubo βT -dimensional)
 - A fração ocupada dos vértices é $2^{-(\beta-\alpha)T}$ e tende a 0 se $T \rightarrow \infty$, o que faz a probabilidade de erro tender a zero
- A ligação entre α e β foi estabelecida por Shannon como

$$\frac{\alpha}{\beta} < C_s$$

- Em que C_s é a capacidade do canal

Capacidade de um Canal Discreto sem Memória

- Considere um canal com símbolos de entrada $x_1, x_2, \dots, x_r$ e símbolos de saída $y_1, y_2, \dots, y_s$
- Se o canal é ruidoso, $P(x_i|y_j)$ representa a probabilidade de que x_i foi transmitido dado que y_j foi recebido
- A incerteza sobre X dado Y é medida pela entropia condicionada $H(X|Y)$ dada por

$$H(X|Y) = \sum_i \sum_j P(x_i, y_j) \log \frac{1}{P(x_i|y_j)}$$

- O canal é caracterizado pela matriz de canal dada pelos elementos $P(y_j|x_i)$ que pode ser relacionada com $P(x_i|y_j)$ por

$$P(x_i|y_j) = \frac{P(y_j|x_i)P(x_i)}{\sum_i P(x_i)P(y_j|x_i)}$$

Capacidade de um Canal Discreto sem Memória

- A informação mútua de X para Y é definida como

$$I(X; Y) = H(X) - H(X|Y) \text{ bits por símbolo}$$

- Em termos das probabilidades, $I(X; Y)$ pode ser escrita como

$$\begin{aligned} I(X; Y) &= \sum_i \sum_j P(x_i, y_j) \log \frac{P(x_i, y_j)}{P(x_i)P(y_j)} \\ &= \sum_i \sum_j P(x_i, y_j) \log \frac{P(y_j|x_i)}{P(y_j)} \end{aligned}$$

- Pela simetria, tem-se que

$$I(X; Y) = I(Y; X) = H(Y) - H(Y|X)$$

Capacidade de um Canal Discreto sem Memória

- A capacidade do canal C_s é definida como

$$C_s = \max_{P(x_i)} I(X; Y) \text{ bits por símbolo}$$

- O canal BSC (Binary Symmetric Channel) possui $X \in \{0, 1\}$ e $Y \in \{0, 1\}$ com probabilidades de transição p_e
- A capacidade do canal BSC é

$$C_s = 1 - \mathcal{H}(p_e)$$

- Em que $\mathcal{H}(p_e)$ é a entropia binária da distribuição $(p_e, 1 - p_e)$, sendo alcançada quando $P(X = 0) = P(X = 1) = 1/2$

Capacidade de um Canal Discreto sem Memória

- A capacidade do canal C_s é interpretada como a máxima quantidade de informação possível de se transmitir para cada símbolo transmitido
- Se K símbolos são transmitidos por segundo, então $C = KC_s$ bits por segundo podem ser transmitidos
- A definição de um canal vai além do meio físico, pois ela pode levar em conta transmissores, receptores, uma degradação temporal, etc.
- Como $\mathcal{H}(p_e) \geq 0$, $C_s \leq 1$ para o canal BSC
- Como $H(X|Y) \geq 0$, $C_s \leq \max H(X) \leq 1$ em geral
- Para símbolos r-ários, $C_s \leq 1$ unidades r-árias por símbolo

Capacidade de um Canal Contínuo sem Memória

- No caso contínuo são consideradas funções densidades de probabilidade
- Entropias e informação mútua precisam ser definidas em função dessas densidades
- A entropia diferencial é definida como

$$h(X) = - \int_S p(x) \log p(x) dx$$

- Em que a integral é calculada sobre o suporte ($p(x) > 0$) e $p(x)$ é a fdp de X com $\int_{-\infty}^{\infty} p(x) dx = 1$

Capacidade de um Canal Contínuo sem Memória

- Para uma distribuição uniforme $X \sim [0, a]$, tem-se que

$$\begin{aligned} p(X) &= \frac{1}{a}, \quad 0 \leq X \leq a \\ h(X) &= \log a \end{aligned}$$

- Pode-se observar que a entropia diferencial pode ser negativa ($a \leq 1$) ao contrário da entropia discreta que é sempre não negativa
- Para uma distribuição gaussiana $X \sim \mathcal{N}(0, \sigma^2)$

$$\begin{aligned} p(X) &= \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} \\ h(X) &= \frac{1}{2} \log 2\pi e \sigma^2 \end{aligned}$$

Capacidade de um Canal Contínuo sem Memória

- A relação entre a entropia discreta e a entropia diferencial é obtida através da discretização da variável contínua
- Se a distribuição $p(x)$ de X é discretizada em intervalos (bins) de tamanho Δ , então pelo teorema do valor médio

$$p(x_i)\Delta = \int_{i\Delta}^{(i+1)\Delta} p(x)dx$$

- Se a variável quantizada for denotada por

$$X^\Delta = x_i, \text{ se } i\Delta \leq X \leq (i+1)\Delta$$

- Então a probabilidade de $X^\Delta = x_i$ é

$$p_i = \int_{i\Delta}^{(i+1)\Delta} p(x)dx = p(x_i)\Delta$$

Capacidade de um Canal Contínuo sem Memória

- A entropia de X^Δ é dada por

$$\begin{aligned} H(X^\Delta) &= - \sum p_i \log p_i \\ &= - \sum \Delta p(x_i) \log p(x_i) - \log \Delta \end{aligned}$$

- Se $p(x)$ é integrável (Riemann), então se $\Delta \rightarrow 0$

$$H(X^\Delta) + \log \Delta \rightarrow h(X)$$

- A entropia de uma variável contínua quantizada com n bits é aproximadamente $h(x) + n$ bits

Capacidade de um Canal Contínuo sem Memória

- No cálculo da capacidade é de interesse saber as distribuições que maximizam a entropia sob determinadas restrições
- Se a variável aleatória contínua possui fdp $p(x)$, com a restrição de que $\overline{x^2} = \sigma^2$, então

$$h(X) = - \int_S p(x) \log p(x) dx$$

$$\int_{-\infty}^{\infty} p(x) dx = 1$$

$$\int_{-\infty}^{\infty} x^2 p(x) dx = \sigma^2$$

- Do cálculo das variações, tem-se que a distribuição que maximiza $h(X)$ é gaussiana

$$p(X) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}, \quad h(X) = \frac{1}{2} \log 2\pi e \sigma^2$$

Capacidade de um Canal Contínuo sem Memória

- Um processo de ruído branco com DEP $\mathcal{N}/2$ e banda B tem

$$R_n(\tau) = \mathcal{N}B \text{sinc}(2\pi B\tau)$$

- Dessa expressão, pode-se observar que amostras do ruído na taxa de Nyquist são descorrelacionadas $R_n(k/(2B)) = 0$ e pelo fato do ruído ser gaussiano, elas são independentes
- A entropia de uma amostra é dada por

$$h(n) = \frac{1}{2} \log 2\pi e \mathcal{N} B \text{ bit por amostra}$$

- Assim $2B$ amostras por segundo resultam em

$$h'(n) = B \log 2\pi e \mathcal{N} B \text{ bit/s}$$

- O ruído branco possui a máxima entropia por segundo dentre os processos com banda B e variância $\sigma^2 = \mathcal{N}B$

Capacidade de um Canal Contínuo sem Memória

- A informação mútua $I(X; Y)$ entre duas variáveis aleatórias contínuas X e Y pode ser definida em termos de entropias diferenciais
- Assim, tem-se que

$$\begin{aligned}
 I(X; Y) &= h(X) - h(X|Y) = h(Y) - h(Y|X) \\
 &= \int \int p(x, y) \log \frac{p(x, y)}{p(x)p(y)} dx dy \\
 &= \int \int p(x, y) \log \frac{p(y|x)}{p(y)} dx dy \\
 &= \int \int p(x, y) \log \frac{p(x|y)}{p(x)} dx dy, \\
 h(X|Y) &= - \int \int p(x, y) \log p(x|y) dx dy
 \end{aligned}$$

Capacidade de um Canal Contínuo sem Memória

- Outras expressões podem ser obtidas aplicando-se as relações

$$\begin{aligned}
 p(x, y) &= p(x)p(y|x) \\
 \frac{p(x|y)}{p(x)} &= \frac{p(y|x)}{p(y)} = \frac{p(y|x)}{\int_{-\infty}^{\infty} p(x, y) dx} \\
 &= \frac{p(y|x)}{\int_{-\infty}^{\infty} p(x)p(y|x) dx}
 \end{aligned}$$

- Dado um canal especificado pela fdp $p(y|x)$, a capacidade do canal contínuo é dada por

$$C_s = \max_{p(x)} I(X; Y) \text{ bits por símbolo}$$

Capacidade de um Canal Contínuo sem Memória

- Considerando o canal AWGN com limitação em banda B , a capacidade pode ser calculada considerando o fato que

$$\begin{aligned}y(t) &= x(t) + n(t) \\p(y|x) &= p_n(y - x) \\ \int p(y|x) \log p(y|x) dy &= \int p_n(y - x) \log p(y - x) dy\end{aligned}$$

- Assim,

$$\begin{aligned}h(Y|X) &= - \int \int p(x, y) \log p(y|x) dx dy \\ &= - \int p(x) dx \int p(y|x) \log p(y|x) dy \\ &= - \int p(x) dx \int p_n(y - x) \log p(y - x) dy = h(n)\end{aligned}$$

Capacidade de um Canal Contínuo sem Memória

- Assim, para o canal AWGN com limitação em banda B

$$I(X; Y) = h(Y) - h(n) \text{ bits por símbolo}$$

- Para obter a capacidade do canal é necessário maximizar $h(Y)$ sob a restrição em $\overline{y^2}$ dada por

$$\overline{y^2} = S + N, \quad S = \overline{x^2}, \quad N = \mathcal{N}B$$

- Nesse caso,

$$\begin{aligned} h(Y)_{\max} &= \frac{1}{2} \log [2\pi e(S + N)] \\ h(n) &= \frac{1}{2} \log 2\pi eN \end{aligned}$$

Capacidade de um Canal Contínuo sem Memória

- A capacidade do canal AWGN com limitação de banda e potência é dada por

$$C_s = \max_{p(x)} I(X; Y) = \frac{1}{2} \log \left(1 + \frac{S}{N} \right) \text{ bit/símbolo}$$

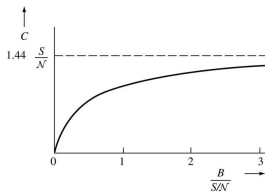
- Esta capacidade é alcançada para um processo gaussiano branco na entrada, cujas variáveis aleatórias X possuem média nula e variância S
- A capacidade em bits por segundo é dada por

$$C = B \log \left(1 + \frac{S}{N} \right) \text{ bit/s}$$

Capacidade de um Canal Contínuo sem Memória

- É útil conhecer o limite na capacidade quando a largura de banda é infinita

$$\begin{aligned}
 C &= B \log \left(1 + \frac{S}{\mathcal{N}B} \right) \\
 \lim_{B \rightarrow \infty} C &= \lim_{B \rightarrow \infty} B \log \left(1 + \frac{S}{\mathcal{N}B} \right) \\
 &= \lim_{B \rightarrow \infty} \frac{S}{\mathcal{N}} \left[\frac{\mathcal{N}B}{S} \log \left(1 + \frac{S}{\mathcal{N}B} \right) \right] \\
 &= (\log_2 e) \frac{S}{\mathcal{N}} = 1,44 \frac{S}{\mathcal{N}} \text{ bit/s}
 \end{aligned}$$



Capacidade de Canais Seletivos em Frequência

- Canais de comunicação sem fio tendem a ser seletivos em frequência
 - Efeito de multipercurso
- Se o canal for do tipo AWGN sem distorção (ganho constante H sobre a banda), a capacidade em bits/s pode ser escrita como

$$C = B \log \left(1 + |H|^2 \frac{S}{N} \right) \text{ bit/s}$$

- Esta capacidade independe do canal ser passa-baixa ou passa-faixa
- Se for considerada uma largura de banda infinitesimal Δf centrada em f_i , tem-se que

$$\begin{aligned} C(f_i) &= \Delta f \cdot \log \left(1 + |H(f_i)|^2 \frac{S_x(f_i) \Delta f}{S_n(f_i) \Delta f} \right) \\ &= \log \left(1 + \frac{|H(f_i)|^2 S_x(f_i)}{S_n(f_i)} \right) \Delta f \text{ bit/s} \end{aligned}$$

Capacidade de Canais Seletivos em Frequência

- Assim, um canal seletivo em frequência pode ser dividido em pequenos canais não seletivos do tipo AWGN com largura de banda Δf
- A capacidade aproximada é a soma das capacidades, ou seja

$$\hat{C} = \sum_i \log \left(1 + \frac{|H(f_i)|^2 S_x(f_i)}{S_n(f_i)} \right) \Delta f \text{ bit/s}$$

- Esta situação ocorre em sistemas como o OFDM
- A capacidade total é obtida fazendo $\Delta f \rightarrow 0$

$$C = \int_{-\infty}^{\infty} \log \left(1 + \frac{|H(f)|^2 S_x(f)}{S_n(f)} \right) df$$

Capacidade de Canais Seletivos em Frequência

- A capacidade de um canal seletivo em frequência depende da DEP do sinal de entrada $S_x(f)$
- É portanto de interesse conhecer a distribuição de potência $S_x(f)$ que maximize a capacidade sujeita a restrição

$$\int_{-\infty}^{\infty} S_x(f) df \leq P_x$$

- O procedimento de otimização leva ao valor ótimo de $S_x(f)$ dado por

$$S_x(f) = \max\left(W - \frac{S_n(f)}{|H(f)|^2}, 0\right)$$

- A constante W é obtida de modo que

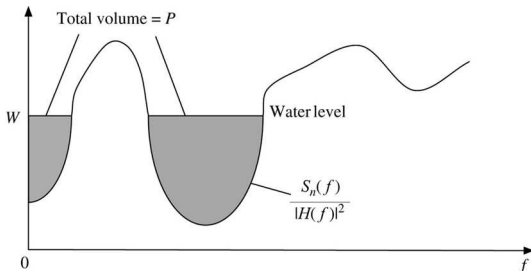
$$P = \int_{-\infty}^{\infty} S_x(f) df = \int_{\{f: W - \frac{S_n(f)}{|H(f)|^2} > 0\}} \left(W - \frac{S_n(f)}{|H(f)|^2}\right) df$$

Capacidade de Canais Seletivos em Frequência

- Com a capacidade máxima dada por

$$C_{max} = \int_{\{f: W - \frac{S_n(f)}{|H(f)|^2} > 0\}} \log\left(\frac{W|H(f)|^2}{S_n(f)}\right) df$$

- Este processo de alocação de potência é melhor entendido com a interpretação do enchimento de água



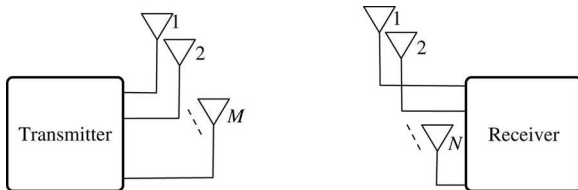
Capacidade de Canais Seletivos em Frequência

- Pode-se observar que um W maior corresponde a um $S_n(f)/|H(f)|^2$ menor (ou uma SNR de canal $|H(f)|^2/S_n(f)$ maior)
 - Mais potência é alocada nas frequências em que a SNR de canal é maior
 - Pouca ou nenhuma potência é alocada nas frequências em que a SNR de canal é ruim
- Essa é uma abordagem similar à utilizada no esquema DMT (OFDM)
- O processo para encontrar W envolve o uso de um algoritmo iterativo
- Em sistemas OFDM (DMT), o espectro é dividido em intervalos de largura de banda Δf e a potência alocada para cada subportadora f_i é dada por

$$S_i = \Delta f \cdot \max\left(W - \frac{S_n(f_i)}{|H(f_i)|^2}, 0\right), \quad \sum S_i = P$$

Capacidade de Canais MIMO

- Como foi observado anteriormente, para aumentar a capacidade de um canal é necessário usar mais potência ou largura de banda
- Outra maneira de aumentar a capacidade é utilizar múltiplas entradas e saídas (MIMO - Multiple Input Multiple Output)
- A tecnologia MIMO está incorporada nos mais recentes padrões Wi-Fi e nas tecnologias 4G e 5G



Capacidade de Canais MIMO

- Um sistema com M entradas e N saídas pode ser representado por vetores através da relação

$$\mathbf{y}_{(N \times 1)} = \mathbf{H}_{(N \times M)} \cdot \mathbf{x}_{(M \times 1)} + \mathbf{w}_{(N \times 1)}$$

- Entropias de um vetor podem calculadas considerando que cada elemento possui uma probabilidade p_i
- Da mesma forma, a informação mútua entre a entrada e a saída é dada por

$$\begin{aligned} I(\mathbf{x}; \mathbf{y}) &= h(\mathbf{y}) - h(\mathbf{y}|\mathbf{x}) \\ &= h(\mathbf{y}) - h(\mathbf{H} \cdot \mathbf{x} + \mathbf{w}|\mathbf{x}) \\ &= h(\mathbf{y}) - h(\mathbf{w}) \end{aligned}$$

Capacidade de Canais MIMO

- De modo similar ao caso SISO (Single Input Single Output), a entropia é maximizada quando a distribuição da entrada é gaussiana
 - O correspondente MIMO é uma gaussiana M-dimensional
- A capacidade do canal (por vetor de símbolos transmitido) é dada por

$$C_s = \max_{p(\mathbf{x})} I(\mathbf{x}; \mathbf{y}) = \frac{1}{2} \log \det(\mathbf{I}_N + \mathbf{H}\mathbf{C}_x\mathbf{H}^T\mathbf{C}_w^{-1})$$

- Em que $\mathbf{C}_x$ e $\mathbf{C}_w$ representam as matrizes de covariância da entrada e do ruído, respectivamente
- A capacidade em bits/s é dada por

$$\begin{aligned} C(\mathbf{H}) &= B \log \det(\mathbf{I}_N + \mathbf{H}\mathbf{C}_x\mathbf{H}^T\mathbf{C}_w^{-1}) \\ &= B \log \det(\mathbf{I}_N + \mathbf{C}_x\mathbf{H}^T\mathbf{C}_w^{-1}\mathbf{H}) \end{aligned}$$

Capacidade de Canais MIMO

- A capacidade do canal MIMO depende de $\mathbf{C}_x$
 - O transmissor pode usar ou não o conhecimento do canal $\mathbf{H}^T \mathbf{C}_w^{-1} \mathbf{H}$ para escolher a melhor $\mathbf{C}_x$
 - O conhecimento do canal chega ao transmissor através de algum mecanismo de feedback
- Quando o transmissor não conhece o canal e o ruído é aditivo, tem-se que $\mathbf{C}_x = \sigma_x^2 \mathbf{I}$ e $\mathbf{C}_w = \sigma_w^2 \mathbf{I}$, de modo que

$$C = B \sum_{i=1}^r \log \left(1 + \frac{\sigma_x^2}{\sigma_w^2} \gamma_i \right)$$

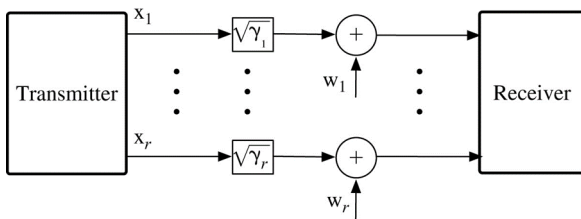
- Em que γ_i representa o autovalor não nulo da matriz $\mathbf{H}^T \mathbf{H}$ de posto r

Capacidade de Canais MIMO

- Quando os autovalores são idênticos ($\gamma_i = \gamma$), pode-se observar que a capacidade do canal MIMO é r vezes a de um canal SISO

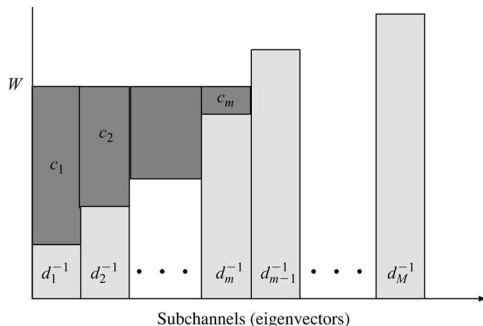
$$C_{MIMO} = r.B \sum_{i=1}^r \log\left(1 + \frac{\sigma_x^2}{\sigma_w^2} \gamma\right)$$

- O sistema MIMO é equivalente a r canais SISO em paralelo



Capacidade de Canais MIMO

- O transmissor pode usar o conhecimento do canal para distribuir a potência entre as entradas de modo similar aos esquemas com enchimento de água
- O ganho de potência c_i vai depender de um autovalor d_i resultante da decomposição de $\mathbf{H}^T \mathbf{C}_w^{-1} \mathbf{H}$



Capacidade de Canais MIMO

- Nesse caso, o diagrama de blocos do sistema é representado por

