

CD Teste 2 - 43280 André Joray
Codificação de Canal

FEC → Forward Error Correction
↳ mal de correção

ARQ → Automatic Repeat Request
↳ detecção e pedido de retransmissão

Códigos de bloco (n, k)

k = # bits mensagem

n = # bits de palavra decodificação

$g = n-k$ = # bits redundantes

++ controle de erros

++ diminuição do BER

++ aumento da QoS

-- maior tempo de transmissão e correção

-- maior complexidade

2^o palavras de código

Codrate $\rightarrow R = \frac{k}{n}$

d_{min} = menor peso de Hamming

$\ell = d_{min} - 1 \rightarrow$ detecta

$t = \lfloor \frac{d_{min}-1}{2} \rfloor \rightarrow$ corrige

bloco → todos os pulsos têm a mesma duração

Linear → todos que pertencem ao código
↳ XOR de pulsos decodifica o outra palavra de código

Código de Repetição

repetição de mensagem

deteta e corrige

Código de bit paridade

bit extra é o XON

nenhum correção

Código de Hamming

$d_{min} = 3$

$n = 2^k - 1$

$R = (2^k - 1) - k$

$\ell = 2$; $t = 1$

CRC *

Em rotas → cada vez de uma palavra de código é ainda uma palavra...

$c(x) = m(x) \cdot g(x)$

$c(x)$ = palavra de cod. → grau $n-1$

$m(x)$ = mensagem → grau $k-1$

$g(x)$ = polinômio gerador → grau $n-k$

$c(x) = m(x)X^{n-k} + b(x)$

$b(x) = \text{resto } \left[\frac{m(x)X^n}{g(x)} \right] = \text{CRC}$

Descodificador

recebe a palavra

estima a palavra decodificada \hat{n}

ativa a mensagem \hat{m}

calcula o síndrome, s , se for nulo, não há erros

$s(x) = \text{resto } \left[\frac{c(x)}{g(x)} \right]$

detetar erros

devido capacidade de detecção, exp. anejado

Matriz Geradora de Códigos
 $G = [I \times I^T] \rightarrow k \times n$

Cada coluna de G é uma
seq. de paridade (p_1, p_2, \dots, p_k)

$P \rightarrow k \times q$

Cada linha de G é um palavrão
de código

Matriz de controle de Paridade

$$H^T = \begin{bmatrix} P \\ I_q \end{bmatrix}$$

$$A = (H^T) \times H$$

Aplicações

bit paridade → com nível ambiente.

memória RAM

repetição → bluetooth

Hamming → TeleText, circuitos integrados

→ IEEE 802.3, bluetooth

CATV → Ethernet 802.3

Localização de futebol na TV

Banda Base

colmito ciganos de freq. em torno
do 2.4 GHz (quadriplex)

distância

nível horível e ruído / interferência

NRZ-Absolute

Unipolar $\rightarrow E_b = \frac{V^2}{2} T_b$

Bipolar (melhor desempenho) $\rightarrow E_b = V^2 T_b$

Sinal de relógio separado

perda de sincronismo em longo

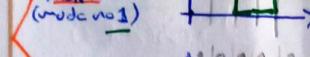
seq. de mesmo bit

inversão dos níveis, (tracer sobre)

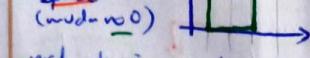
NRZ-Diferencial

cria transições para evitar perda de
sincronismo

Morse (modo 1)



Space (modo 0)



perda de sinc. embora seq. de
1s nos e 0s no M.

A2-B → código binário

contração → código binário

dobro de LB

menor energia média por bit

Unipolar

$E_b = \frac{V^2}{2} T_b$

Bipolar

$E_b = \frac{V^2}{2} T_b$

AMI

técnica aplicada a NRZ em RZ

sinal da PC $\rightarrow 0$

alternar 101010101010

NRZ-B

$E_b = \frac{V^2}{2} T_b$

A2-B

$E_b = \frac{V^2}{2} T_b$

Manchester (código bônico)

valor médio nulo

mesma EB e NRZ-B-polar

mesma IB e RZ

nenhuma transição a nível de tipo de bit

codigo ZB1Q - 2bit / Query

codifica 2 bits por cada Tb

níveis organizados em código de Gray para o BÉR

aumentar ritmo binário

manter a largura de banda

Aplicações

NRZ-U - níveis TTL; interligação de periféricos

IEEE 802.3 Ethernet a fibra - 5 bits

NRZ-B - interface RS-232

NRZ-S - USB

NRZ-M - IEEE Fast Ethernet, fibra óptica

AMI - código de certa telefônica por cabo de cobre

A2-T - infravermelho

Manchester - IEEE 802.3 Ethernet com cabo de cobre

ZB1Q - MDIS em ISDN

Digital - destrô - audios perturbados no SCD

Lembre-se que todos os Tb

Precedor

correlador - determina semelhança entre o pulso

recebido e o de referência

$n(t) \rightarrow \int_{t_0}^{t_1} n(t) dt \rightarrow$ pulso de bit

</div

SCD André Soares 48280

Codificações binária:

- OOK (On-Off Keying) - amplitude
- FSK (Frequency-Shift Keying) - frequência
- PSK (Phase Shift Keying) - fase
- QAM (Quadrature Amplitude Modulation)

Indicadores

- T_b - tempo de bit [s] = $\frac{1}{R_b}$
- R_b - ritmo binário [bit/s] = $\frac{1}{T_b}$
- BER - bit error rate = $\frac{\# \text{ bits errados}}{\# \text{ bits}}$
- T_{err} - tempo médio entre erros [s] = $\frac{T_b}{BER} = \frac{1}{R_b \times BER}$
- T_x - duração da transmissão [s] = $\frac{\# \text{ bits}}{R_b} = \# \text{ bits} \times T_b$

Características

- Topologia
 - Ponto a ponto
 - Ponto a Multiponto
 - Multiponto a Multiponto
- Directo
 - Simples
 - Duplex
 - Half-Duplex
 - Full-Duplex
- Tipo de Sinal
 - Análogico
 - Digital
- Banda
 - Base - ondas quadradas
 - Canal - ondas sinusoides

Meios de Transmissor

- Pares entrelaçados
 - UTP (unshielded twisted pair)
 - STP (shielded " ")
 - Quadrado
- Cabo coaxial
 - sinusoidal
 - paralelo
 - micro
 - small-core
 - normatice
- Fibra óptica - condutor através da luz
 - cor
 - Amarola - monomodo (1 modo de luz)
 - Laranja/Azul - multimodo (vários modos de luz)
 - gradual (pode ser gradual)

Atenuação - perda de amplitude [dB/km]
 Da b6l - ratio logarítmico entre dois resultados

Formas de Transmissão

- Série - sequencial
 vários distâncias
- Paralela - simultânea
 curta distância
- Síncrona - clock sincronizado
- Assíncrona - sem clock
 - bit-stuffing
 - corta distância

CAN (Controller Area Network)

- two-wire (STP)
- half-duplex
- alta velocidade
- tempo paridade de mensagens
- NRZ com bit-stuffing

Teoria da Informação

Informação própria

$$I(x_i) = \log_2 \frac{1}{P(x_i)} = -\log_2 P(x_i) \text{ [bit]}$$

- $P(x_i) = 1 \Rightarrow I(x_i) = 0$
- $P(x_i) < P(x_k) \Rightarrow I(x_i) > I(x_k)$

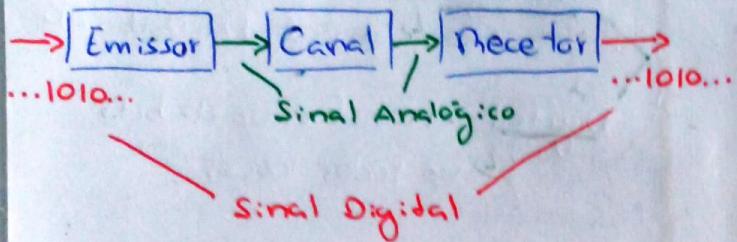
Entropia

$$H(x) = -\sum_x P(x) \log_2 P(x) \text{ [bit/simb]}$$

$$0 \leq H(x) \leq \log_2 M \quad \begin{matrix} 0 \text{ 1 símbolo cor } P(x) = 1 \\ \text{Mas todos com a mesma } P(x) \end{matrix}$$

KB	10^3	KiB	2^{10}	mil.	000
MB	10^6	MiB	2^{20}	10^{-6}	micro μ
GB	10^9	GiB	2^{30}	10^{-9}	nano n

Sistema de Comunicação Digital (SCD)



- Sinal - Codifica a sequência binária
- Emissor, canal e receptor são sistemas
- Sistemas transformam um sinal de entrada num sinal de saída

Exemplos de codificações binária:

- OOK → On-Off keying
 - ↳ caso particular de Amplitude Shift Keying
 - ↳ tem por base a amplitude
- FSK → Frequency-Shift keying
 - ↳ frequência
- PSK → Phase Shift Keying
 - ↳ fase
- QAM → Quadrature Amplitude Modulation

Indicadores sobre SCD

- T_b → tempo de bit (segundos)
 - ↳ tempo q o sinal corresponde a cada bit está na linha

- R_b → ritmo binário (bit/s)
 - ↳ taxa de bits por segundo

$$R_b = \frac{1}{T_b}$$

↳ inverso de T_b

BEP → Bit Error Rate

- ↳ taxa de erro de bit
- ↳ valores típicos: 10⁻⁴, 10⁻⁶, ...

$$BEP = \frac{\# \text{bits em erro}}{\# \text{bits totais}}$$

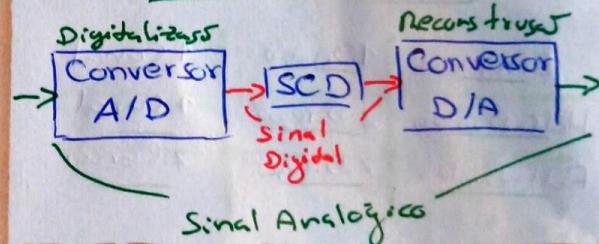
- Terr → tempo médio entre erros consecutivos (s)

$$Terr = \frac{T_b}{BEP} = \frac{1}{R_b \cdot BEP}$$

- T_x → duração da transmissão

$$T_x = \frac{\# \text{bits}}{R_b} = \# \text{bits} \cdot T_b$$

Sinal Analógico sobre SCD



⚠ Não é possível transmitir um sinal digital através de um canal analógico

Exemplares de Aplicações

- ADSL - Asymmetric Digital Subscriber Line
- medes LAN (Local Area Network)
- WAN (Wide .., ..)
- Wi-Fi
- Bluetooth
- GPS
- IrDA - Infrared Data Association
- NFC - Near Field Communication
- TDT - TV Digital Terrestre

Características de SCD

Tipo de Ligação

↳ topologia das interconexões no processo de comunicação

Ponto a ponto

Ponto a multi-ponto

Multiponto a multi-ponto

Direção da transmissão

Simplex → num só sentido

Elo: TV, rádio

Half-Duplex → num sentido de cada vez; elo: Walkie-Talkie

Full-Duplex → dois sentidos simultaneamente; elo: Telefone

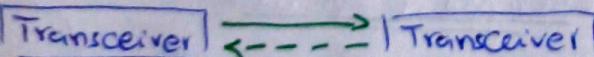
em 2 sentidos

Simplex	1 Direção	1 Canal
Half-Duplex	2 Direções	1 Canal
Full-Duplex	2 Direções	2 Canais

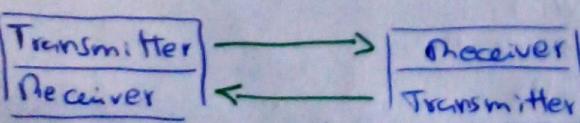
Simplex:



Half-Duplex



Full-Duplex



Tipo de Sinal

Análogo → envio de sinal analógico

↳ Ex: Rádio FM, Rádio AM

Digital → transferência de bits

↳ Ex: Redes locais

Inteligente

Banda de frequência

banda base

bands canal

Banda Base

↳ códigos de linha ("ondas quadradas")

↳ meios de transmissão satélites (ou fibra)

↳ não é possível ser transmitido no meio wireless

Banda Canal

↳ modulações digitais

↳ uso de sinusoides para posicionar o espectro em determinadas freqüências

↳ aproveitamento eficiente da largura de banda

↳ os meios de transmissão satélites, fibra óptica

Meios de Transmissão

- Pares entrelaçados (telefone)
- cabo coaxial (TV por cabo)
- Fibra ótica (rede de alta velocidade)
- ar (espaço livre) (televisões)

Pares entrelaçados

- dois condutores elétricos entrelaçados

fazem um par

- um cabo tem vários pares

UTP - unshielded twisted pair

STP - shielded twisted pair

- aplicações: redes telefônicas, redes locais

Cabo coaxial

- um condutor central isolado da malha exterior

isolamento através de ar ou plástico

malha protege o condutor de interferência

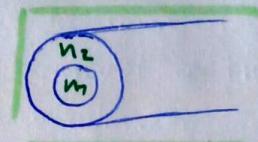
- aplicações: redes locais, sinal de TV

Fibra óptica

- condutor de luz, construído a partir de vidro ou plástico
- conversão de sinal elétrico em luz através de LED (light-emitting diode) ou de ILD (injection-laser diode)
- conversão de luz em sinal elétrico (photo-diode / optical transceiver)

constitui-se:

- núcleo de vidro puro, transparente
- casca envolve o núcleo; feita de material com menor refrate



n₁ - núcleo
n₂ - revestimento

- aplicações: MAN (metropolitano, áreas metropolitanas, interligação de redes)

- largura de banda elevada

- fibras monomodo, multimodo e multimodo gradual (ver slide 18)

- Cor
 - Amarelo - monomodo (1 fibra fino delgado)
 - Laranja - multimodo (muitas fibras finas)
 - (ou Áqua/Azul)

Ocupação do Espaço

- Ver tabela completa no slide 26
- monitorizada pela ANACOM

Atenuação

- perda gradual de intensidade
- medida em dB/km
- fibra tem menor atenuação que o cabô coaxial

Formas de Transmissão

Transmissão série

- bits transmitidos de forma sequencial
- usado em comunicação curta, longa e média distância

Transmissão paralela

- vários bits transmitidos simultaneamente
- usado em comunicação a curta distância
- ex: teclado de computador, processador

Transmissão síncrona

- o receptor tem mechanismo de sincronização relativamente ao Fluxo de dados proveniente do emissor
- este mecanismo é um clock presente no dispositivo de receptor
- clock enviado no cabo também

Transmissão assíncrona

- não é usado no receptor nenhum mecanismo de sincronização
- as sequências de bits transmitidos têm de ter marcas que indicam o fim e o inicio: Start bit e Stop bit
- a descodificação é feita no receptor
- usado em corta distância
- usa bit-stuffing
 - coloca bits de enximento para o sistema perceber onde está o T_b e não se perder

Sistemas de transmissão (Série)

RS-232 (Recommended Standard - 232)

- usado maioria das vezes em ports em série de computadores
- DTE (Data terminal equipment) - como um PC

- DCE (Data circuit-terminating equipment ou data communication equipment) - como um modem



SPI (Serial Peripheral Interface)

- especificado para comunicação síncrona em série usado a corta distância (sistemas embutidos)
- full duplex using master-slave architecture
- o dispositivo master origina a frame de escrita/leitura
- cada dispositivo slave é selecionado pelo CS (Chip Select) thru combinado com SS (Slave Select)
- 4 wire serial bus

Notas

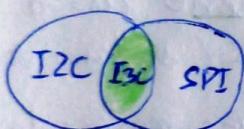
- Distância é inversamente proporcional a T_b e proporcional a I_b
 - + Distância => + Atenção
 - Cables metálicos conduzem mais

I²C (Inter-Integrated Circuit)

- síncrono serial computer bus
- multi-master e multi-slave
- packet switched
- single-ended
- short distance communications

I3C (MIPI I3C, ou SenseWire)

- multidrop serial data buses
- evolução do I²C, adicionando um número significante de fechaduras, mantendo compatibilidade com os I²C slaves



- multi-máster e multi-slaves

CAN (Controller Area Network)

- two-wire, half-duplex de alta velocidade; STP ou UTP
- utilizado em comunicações entre bichos para microcontroladores
- Modo em dispositivos inteligentes (ex: veículos, elevadores, instrumentos médicos)
- existe prioridades de mensagens
- NMII com bit-stuffing

USB (Universal Serial Bus)

- industry standard
- estabelece especificações para cabos, conectores e protocolos de conexão e comunicação e de power supply
- 4 Gerações de USB Specification:
USB 1.0, USB 2.0, USB 3.0 e USB 4

Modos de Sincronização

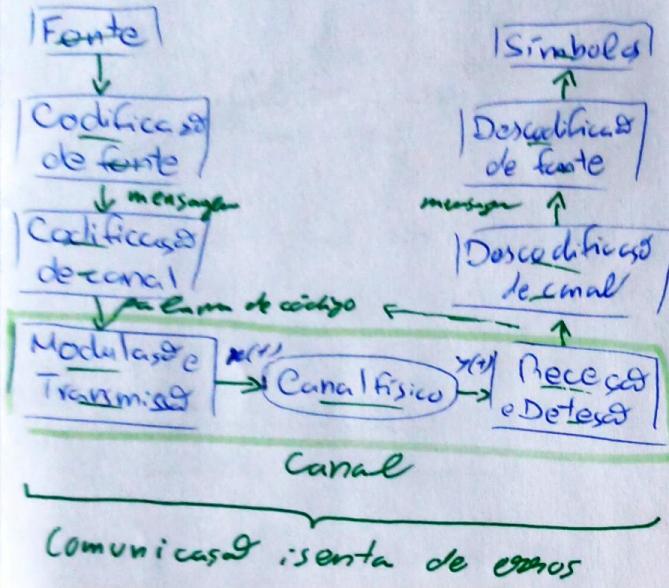
- assíncrono - the ADC / DAC não é sincronizado com o clock do PC
- síncrono - the PC clock é sincronizado com o USB start-of-frame (SOF)
- adaptativo - o clock é sincronizado pela quantidade de dados enviada por frame pelo host

Direção da transmissão

- Low-speed (LS) e Full-speed (FS) usam um par de dados únicos, D+ e D-, em half-duplex
- High-speed (HS) nesse caso usa canais diferentes
- SuperSpeed (SS) adds two additional pairs of shielded twisted wire; full-duplex
- Super Speed+ (SS+) - increased data rate and / or a new adjacent lane in USB-C

Teoria da Informação

- criada / estudiada por Claude Shannon
- estudo de medidas de informação
- modelo de comunicação de Shannon:



Fonte produz uma sequência de símbolos a codificar

Codificação de fonte realiza a codificação eficiente desses símbolos

Cifra encripta os bits a transmitir

Codificação de canal introduz redundância de forma a efetuar controlo de erros

Quantidade de Informação

- Seja X uma v.a. q toma um conjunto de valores finitos de acordo com a f.m.p. $p(x)$
- Define-se auto-informação ou informação própria de uma ocorrência x_i :

$$I(x_i) = \log_2 \frac{1}{p(x_i)} = -\log_2 p(x_i) \quad [\text{bit}]$$

Propriedades:

- $I(x_i) = 0$ se $p(x_i) = 1$
- $I(x_i) \geq 0$ se $0 < p(x_i) \leq 1$
- $I(x_i) > I(x_k)$ se $p(x_i) < p(x_k)$
- $I(x_i, x_k) = I(x_i) + I(x_k)$ se x_i, x_k são independentes

Base do logaritmo:

- base 2, unidade é "bit" ou "shannon"
- base natural, unidade é "nat"
- base 10, unidade "hartley" ou "dits" (decimal digits)

Entropia

medida da quantidade de informação necessária, em média, para descrever a v.a. X

valor médio da informação própria:

$$\hookrightarrow H(X) = E[-\log_2 p(x)] \quad [\text{bit/symbol}]$$

$$0 \leq H(X) \leq \log_2 M, M = n^{\circ} \text{ de símbolos}$$

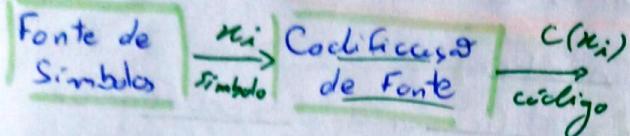
O quando um dos símbolos tem probabilidade 1

O limite superior acontece quando todos são equiprováveis

$$H(X) = \sum_n p(x) \log_2 (p(x))$$

Codificação de Fonte ("source coding")

- procura-se minimizar o comprimento do código
- descarga de acidente produzida por determinado fonte



- caracterizada pela sua entropia, $H(x)$
- produz um código cujas palavras têm comprimento médio L
- os códigos mais eficientes são aqueles que minimizam o valor de L

Teorema da codificação de fonte

- é possível codificar uma fonte de entropia H, usando um média L bits por símbolo:

$$L = H(x) + \epsilon \quad , \quad L \geq H$$

- o valor de ϵ deve ser o mais pequeno possível, idealmente 0
- a eficiência da codificação é dada por:

$$\frac{H(x)}{L} = \frac{H(x)}{H(x) + \epsilon}$$

- ϵ é a redundância do código
- com ϵ ideal, a eficiência é 100%

Codificação entrópica ou estatística

- consiste em codificar uma fonte de forma a que o seu bit rate médio seja $H(x)$ bits/s
- o valor de L deve tender para $H(x)$
- o comprimento da palavra de código a representar um símbolo x é $I(x_i)$

Comprimento Médio

- representa o nº médio de dígitos utilizado para representar cada símbolo:

$$L = E[I(c(x_i))] = \sum_{i=1}^N p(x_i) I(c(x_i))$$

Código ótimo e ideal

- um código fonte é ótimo se:

$$H(x) \leq L \leq H(x) + 1$$

- quando $L = H(x)$, o código é ideal e a eficiência é 100%

Algoritmo de código único (run-length code)

1. Ordenar os símbolos por probabilidade decrescente
2. Atribuir sucessivamente as sequências consecutivas binárias:

0
10
110
1110
(...)

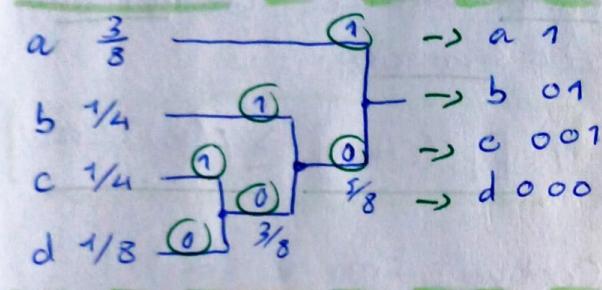


Algoritmo de Huffman

1. Ordenar os símbolos por probabilidade decrecente e considerá-los numa árvore

2. Enquanto houverem nós:
 - agrupar os 2 nós de menor probabilidade e formar um nó com a soma das 2
 - atribuir a cada nó 0 e 1

Exemplo:



O ótimo e ideal

Código de Shannon-Fano

1. Ordenar por probabilidade decrecente
2. De forma recursiva, dividir os símbolos em 2 partes, aproximadamente com o mesmo peso) e atribuir 0 ou 1 a cada parte

Exemplo:

a	0,35	0	00	00
b	0,17	0	01	01
c	0,17	1	10	10
d	0,16	1	11	110
e	0,15	=	11	111

Considerações

Huffman → bottom - up

Shannon-Fano → top - down

- Huffman → regra geral, mais eficiente

Formas de Compressão

Estática

- codificador e descodificador usam o mesmo modelo estabelecido à priori

- modelo não é calculado em função do ficheiro e não é modificado ao longo do processo

Semi-Adaptativa

- modelos determinados pelo codificador, em função do ficheiro

- O modelo é escrito no ficheiro para o descodificador obter

Adaptativa

- O codificador e o descodificador são atualizados o modelo, à medida que o processo decorre

Considerações:

- a forma estática é mais simples, mas menos eficiente
- a forma semi-adaptativa exige dados anteriores pelo ficheiro (two-pass approach):
 - 1) → estimar o modelo
 - 2) → codificar
- a forma adaptativa é mais exigente em tempo e memória mas e a que tem melhor taxa de compressão

Codificação baseada em dicionário

- designada por Lempel-Ziv (LZ)
- sequências de símbolos são codificados através de tokens / tipos
- cada token:
 - codifica um nº variável de símbolos
 - ocupa um nº fixo de bits
- não contam modelos de probabilidade, ou alfabeto de símbolos
- o dicionário pode ter vazio no inicio

Lempel-Ziv 77 (1977)

- baseado em sliding - window com:
 - dicionário (anterior)
 - Look-ahead buffer (LAB) (Texto a codificar)
- procura-se sobre o dicionário, a ocorrência do texto presente no início de LAB
- estrutura do token:

(position, length, innovation-symbol)

- position → posição da substring no dicionário
- length → nº de símbolos em comum
- innovation-symbol → próx. símbolo & quatro apag.

Nota: caso não exista quaisquer ocorrências:

$(0, 0, \text{innovation-symbol})$

- cada token ocupa:

$$\log_2(1D1) + \log_2(1S1) + 8 \text{ bit}$$

1D1 - nº de posição do dicionário

1S1 - nº de posição de LAB

Lempel-Ziv Storer-Szymanski

- mais eficiente em termos de compressão
- formato do token é modificado para:
 - Flag-bit (position, length)
 - Flag-bit & innovation-symbol

Aplicações

- Formatos ZIP, RAR, JAR, CAB (Cabinet), .DOCX, .PPTX, XLSX

Conceitos gerais - Codificação

- codificação eficiente \Rightarrow compressão de informação
- motivos:
 - menor espaço
 - menor tempo de transmissão

desperdício (lossless encoding, deduplicação)
com perda (lossy encoding)

Métricas de compressão

- medida de compressão (4 medidas)
- tempo de codificação
- tempo de decodificação
- memória utilizada na codificação
- memória utilizada na decodificação

do → dimensão do ficheiro original

dc → " codificado

Medidas de compressão

Prazos / Taxa de compressão

$$\frac{dc}{do} \times 100\% \quad \leftarrow$$

Percentagem de movimentação

$$(1 - \frac{dc}{do}) \times 100\% \quad \leftarrow$$

Bit por byte \downarrow

$$\frac{dc}{do} \times 8 \text{ [bpb] } \quad \leftarrow$$

N:1

\hookrightarrow proporção de N símbolos do ficheiro original que são codificados com 1 símbolo do ficheiro de saída, ou seja:

$$\frac{1}{N} = \frac{dc}{do} \quad \leftarrow$$

Sistemas Criptográficos

Tipos

- De acordo com Shannon, existem 3 tipos:

- Concealment system
- Privacy systems
- "True" secrecy system → Cifra

Objetivos

- realizar comunicações secretas, para tornar as mensagens seguras
- confidencialidade na comunicação

Cifra

- A mensagem original (plain text) é codificada para um texto cifrado (cipher text)
- O processo inverso é chamado de decifra
- Requer uma chave secreta, partilhada entre as duas partes
- quintuploto (P, C, K, E, D):

- P - Plain text - conjunto de plain texts
- C - Cipher text - " " cipher texts
- K - Key Space - " " chaves
- E - Encipher - " " regras de cifra
- D - Decipher - " " " " decifra

Diagrama:

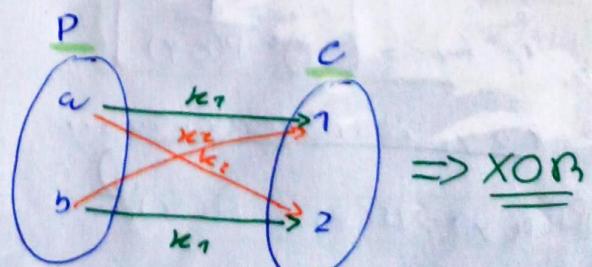


Segurança

- Segurança Computacional
- define-se em termos do número de operações ou do tempo
- Segurança incondicional (perfeita)
- o sistema não pode ser quebrado, mesmo com recursos infinitos

Sistema One Time Pad (OTP)

- Proposto por Gilbert Vernam
- tem segurança perfeita, nas seguintes condições:
 - a chave é do mesm comprimento que o plain text
 - a chave é aleatória e não é reutilizada
 - a chave é montada secreta



Análise de Sistema Criptográfico

Sendo as seguintes v.a.:

- X - conjunto de plain text
- K - conjunto de chaves
- Y - conjunto de criptogramas
- X e Y sejam independentes

Um sistema tem segurança perfeita se:

$$P(x|y) = P(x)$$



ou seja, não se ganha informação do texto por observação do criptograma

\Rightarrow

$$H(x|y) = H(x)$$

Entropia

$$H(x) = E \left[\log_2 \frac{1}{P(x)} \right]$$

Entropia Conjunta

$$H(x,y) = E \left[\log_2 \frac{1}{P(x,y)} \right]$$

Se x e y sejam independentes, ...

$$H(x,y) = H(x) + H(y)$$

Logo

$$0 \leq H(x,y) \leq H(x) + H(y)$$

Entropia Condicionada

$$H(x|y) = E \left[\log_2 \frac{1}{P(x|y)} \right]$$

\Leftrightarrow

$$H(x|y) = H(x,y) - H(y)$$

Logo, no caso de x e y serem independentes ...

$$H(x|y) = H(x)$$

$$\text{Logo } H(x|y) \leq H(x)$$

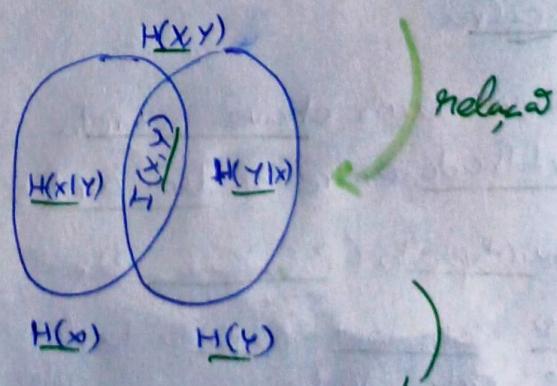
Informação Mútua

medida da quantidade de informação que a v.a. x carrega acerca da v.a. y

$$I(x,y) = I(y,x)$$

$$I(x,y) = H(x) - H(x|y)$$

Se x e y sejam independentes, $I(x,y) = 0$



$$0 \leq I(x,y) \leq H(x)$$

$$I(x,y) = 0 \Rightarrow H(x) \leq H(x)$$

Equivocos em Criptografia

Equivoco da mensagem $H(x|y)$

- mede a incerteza relativamente ao texto plain quando se conhece o criptograma

$$H(x|y) = H(x) - I(x,y)$$

Equivoco da chave $H(k|y)$

- mede a incerteza relativamente à chave quando se conhece o criptograma
- mede quanta informação acerca da chave é revelada pelo criptograma

$$H(k|y) = H(k) \rightarrow H(x) - H(y)$$

- assume-se que:

K e x determinam um único x
K e y " " " x

Condições de Segurança Perfeita

$$I(x,y) = 0 \Rightarrow H(x) \leq H(k)$$

$$H(k|y) \leq H(k)$$

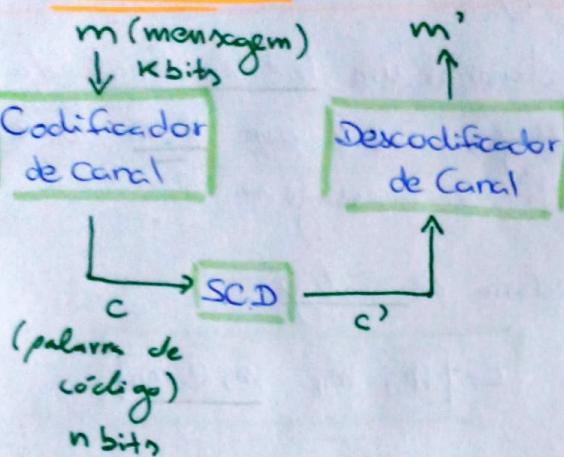
$$H(x,k,y) = H(x,y)$$

- Chaves equiprováveis

- Centro Ideal: Plain texto equiprovável

Se $H(k|y) < H(k)$, na redução de incerteza

Codificações de Canal



- A probabilidade de erro define o BER (Bit Error Rate) do canal

b) taxa de erros por bit

Códigos de controlo de erros

- A deteção/correcção são obtidos pela introdução de redundância na mensagem original

FEC → Forward Error Correction
 L) modo de correcção de erros
 L) o receptor recebe as palavras, deteta e corrige eventuais erros

ARQ → Automatic Repeat Request
 L) modo de deteção de erros
 L) o receptor recebe as palavras, deteta erros e solicita retransmissão

correcção - $d_{\min} \geq 3$

deteção e correcção - $d_{\min} \geq 4$

Códigos lineares de bloco

- bloco - todas as palavras têm a mesma dimensão (n)
- linear - o vetor nulo pertence ao código
 a soma modular de 2 palavras de código é uma palavra de código

$$(n, k)$$

- k - nº de bits da mensagem
- n - nº de bits da palavra de código ($n > k$)
- q - nº de bits redundantes

$$q = n - k$$

- 2^n palavras possíveis
- 2^k palavras de código

Propriedades

- Code rate: $R = \frac{k}{n}$
- Distância de Hamming (d_H)
 nº de bits q diferem duas palavras de código
- Distância mínima (d_{\min})
 menor distância de Hamming
 $d_{\min} \leq 1+q$

Capacidade de deteção (ℓ)

deteta até ℓ erros

$$\ell \leq d_{\min} - 1$$

Capacidade de Correção (t)

corrige até t erros

$$t \leq \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

Nota: $\lfloor \cdot \rfloor$ é floor(), ou seja, o maior inteiro menor que o valor

Detecta ℓ erros e corrige t erros

$$d_{\min} \geq \ell + t + 1$$

Código de Repetição (3,1)

repetição da mensagem

m	c
0	000
1	111

$2^k = 2$ palavras

$2^n = 8$ palavras possíveis

$d_{\min} = 3$

$\ell = 2$ - detecta erros de 1 ou 2 bits

$t = 1$ - corrige erros de 1 bit

Código de bit paridade par (3,2)

adicionar um bit no final da mensagem, que é um XOR dos 2 bits da mensagem

palavra de código:

$$C = [m_0 \ m_1 \ m_0 \oplus m_1]$$

$d_{\min} = 2$

$\ell = 1$ - detecta erros de 1 bit

$t = 0$ - ~~corrige~~ não tem correção

Peso de Hamming

nº de dígitos não nulos numa palavra

$$d_{\min} = \min w(c_k)$$

sendo c_k uma palavra de código diferente do vetor nulo

Código de Hamming

tem sempre $d_{\min} = 3$

$$n = 2^9 - 1$$

$$k = (2^9 - 1) - 9$$

$\ell = 2$ - detecta erros de 1 ou 2 bits

$t = 1$ - corrige erros de 1 bit

Códigos Ciclicos - CMC

- a rotas de qualquer palavra de código é ainda uma palavra de código

$$c(x) = m(x)g(x)$$

- $c(x)$ - palavra de código
polinômio de grau $n-1$
- $m(x)$ - mensagem
polinômio de grau $k-1$
- $g(x)$ - polinômio gerador de grau q
- Ao palavras de código
 $c = [c_{n-1} \ c_{n-2} \ \dots \ c_1 \ c_0]$ podem ser analisadas como polinômios:

$$c(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \dots + c_1x + c_0$$

- O nº de bits redundantes é o grau do polinômio gerador (g)

CMC - Cycle Redundancy Check

- As palavras têm a seguinte organização:

$$\boxed{\begin{array}{|c|c|} \hline & \rightarrow c(x) \text{ (n bits)} \\ \hline m(x) & b(x) \\ \hline k \text{ bits} & q \text{ bits} \\ \hline \end{array}}$$

- Os bits $b(x)$ constituem um polinômio de grau $q-1$ e designam CMC.

- A palavra de código é dada por:

$$c(x) = m(x)x^q + b(x)$$

$$\underline{\text{CMC}} \rightarrow \text{resto} \left[\frac{m(x)x^q}{g(x)} \right]$$

- Típicamente usado na deteção, mas também suporta corret

- têm elevada capacidade de deteção, especialmente de burst de erros (rajada)

Decodificador de Canal

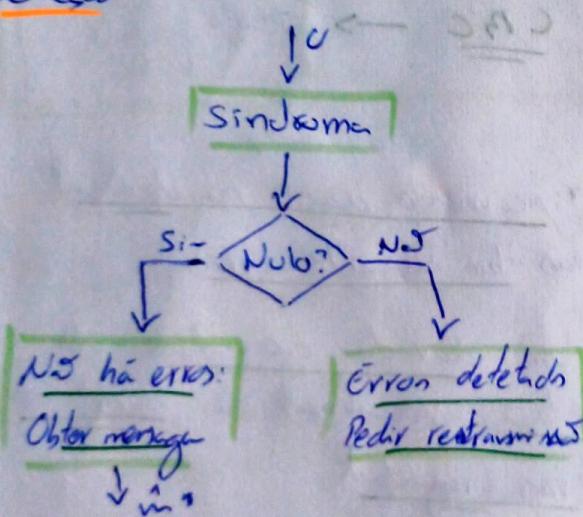
- recebe a mensagem y (palavra)
- estima a palavra de código se que she ola origem

- estima a mensagem m̂

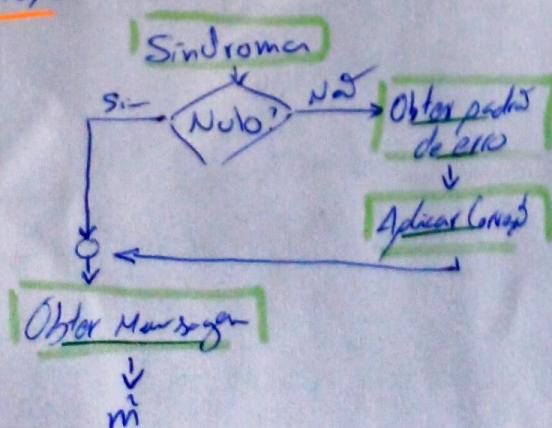
Faz a detectar e corrigir

- Síndrome - resultado da comparação bit a bit da bits de paridade transmitida e recalculada no descodificador

Detectar



Corrigir



NO CMC

- Seja $y(x) = c(x) + e(x)$ a palavra recebida, em que $e(x)$ é o padrão de erro:

- se $e(x) = 0 \Rightarrow$ síndrome é nula:

$$s(x) = \text{resto} \left[\frac{y(x)}{g(x)} \right] = \text{resto} \left[\frac{c(x)}{g(x)} \right]$$

$$= \text{resto} \left[\frac{m(x) g(x) + e(x) g(x)}{g(x)} \right] = 0$$

- se $e(x)$ não for nula \Rightarrow síndrome não é nula e depende de $e(x)$

$$s(x) = \text{resto} \left[\frac{m(x) g(x) + e(x) g(x)}{g(x)} \right]$$

$$= \text{resto} \left[\frac{e(x) g(x)}{g(x)} \right]$$

Matriz Geradora

$$C = m \times G$$

C - palavras de código: $1 \times n$

m - vetor mensagem: $n \times 1$

G - matriz geradora do código
matriz $k \times n$

$$G = [I_k | P] \text{ ou } G = [P | I_{n-k}]$$

P - sub-matriz geradora de paridade, ou seja, a matriz que estabelece as relações de paridade do código

dimensão $k \times q$

cada coluna constitui uma equação de paridade

Cada linha de G é uma palavra de código

A matriz de controlo de paridade

H :

$$H = [P^T | I_{n-k}]$$

permite verificar se existem erros na palavra recebida C , através do cálculo do síndrome:

$$\hookrightarrow S = C \times H^T$$

$S = 0 \Rightarrow$ não se detetam erros

$S \neq 0 \Rightarrow$ existem erros detetados

$$H^T = \begin{bmatrix} P \\ I_q \end{bmatrix}$$

Descodificação

É necessário recalcular a paridade entre os bits de mensagem recebidos e comparar esta com os bits de paridade recebidos

Para tal usa-se H :

$$\begin{aligned} S &= CH^T = mGH^T = \\ &= m[I_k \ P] \begin{bmatrix} P \\ I_q \end{bmatrix} \\ &= [S_0 \ S_1 \ \dots \ S_{q-1}] \end{aligned}$$

Cada bit do síndrome corresponde à verificação de erros no respetivo bit de paridade

O síndrome só depende do padrão de erro e; não depende da palavra de código

Aplicações

• Bit Paridade e Hamming:

↳ comunicação série assíncrona

↳ máquinas IBM

↳ televisão

↳ disco rígido

• Bit Paridade, repetição e Hamming

↳ RAID

↳ Blue tooth

• CMOS

↳ Norma Ethernet

↳ condicionador de fonte WinBar

Transmissão em Banda Base

- meio de transmissão admite frequência em torno de 0 Hz
- uso de códigos de linha (ondas quadradas)
- cota distância (tipicamente)

Códigos de Linha

- uso de pulsos elétricos para codificar os bits "0" e "1"
- estes pulsos são colocados diretamente no meio de transmissão
- tipos:
 - NRZ
 - RZ
 - Bifáricos

NRZ - Non-Return to Zero Absoluto

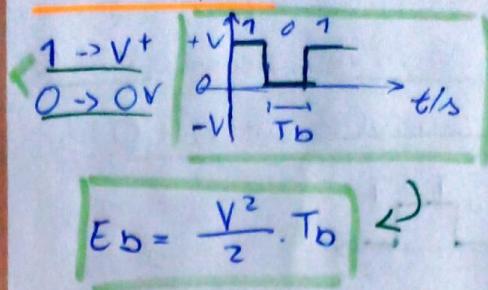
- não retorna a zero dentro de T_b
- formato binário
- transmite a cota distância com eficiência de 100%
- necessita de clock em separado
- problemas:

- perda de sincronismo para longas sequências do mesmo bit
- inversão da nível (troca dos fios)

Unipolar

Bipolar / Polar

NRZ Unipolar

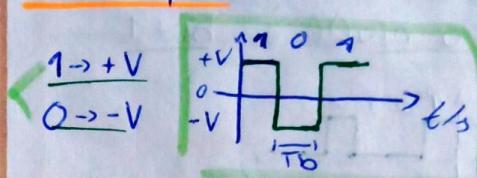


• DC (valor médio) não é nulo

• diretamente proporcional ao nº de 1s

• codificação TTL

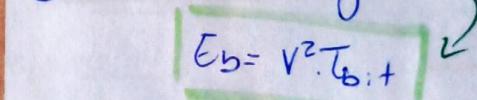
NRZ Bipolar



• DC é nulo grd nº de 1s = nº de 0s

• melhor desempenho que unipolar

• gasta mais energia



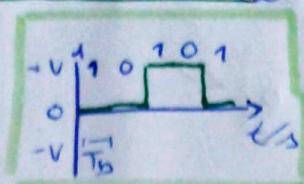
NRZ Diferencial

- bito codificados com alternação de nível (transições)
- minimizar perdas de sincronismo
- pode ser Unipolar ou bipolar

• NRZ-U (Norte)
• NRZ-S (Space)

NMZ-Mark

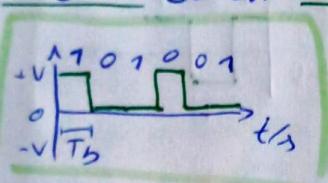
- mudança de nível para o bit+1
- mantém o nível em bit 0



- perda de sincronismo em longas sequências de 0s

NMZ-Space

- mudança de nível para o bit 0
- mantém o nível em bit+1

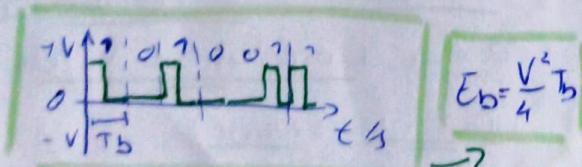


- perda de sincronismo em longas sequências de 1s

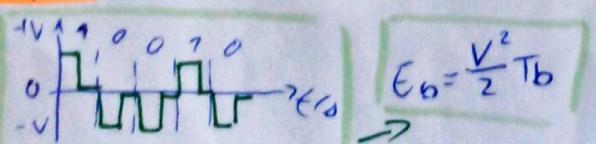
Códigos RZ

- return to zero
- gera mais transições que NMZ
- dobro da largura de banda q NMZ

Unipolar

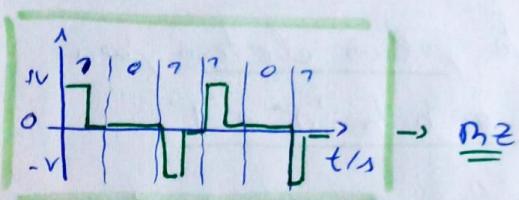
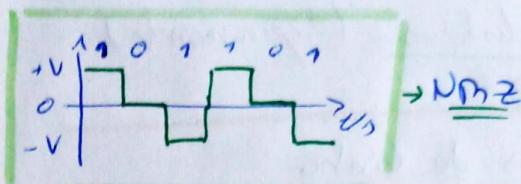


Bipolar



Código ANI

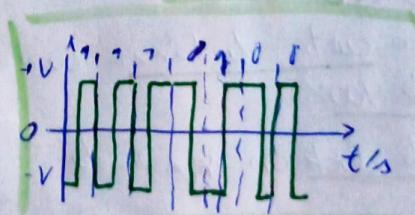
- Alternate Mask Inversion
- NMZ e RZ
- gera sinal q não tem perda de sincronismo
- 1s consecutivos alternam os am OV



Código Manchester

- tem sempre valor médio nulo
- código binário-transfere a meio do bit
- dobro da largura de banda de NMZ
- mesma energia média q NMZ

$$E_b = V^2 T_b$$



Código 2B1Q (2 níveis)

- 2bit → quaternary
- por cada Tb, codifica 2bits
- símbolos organizados em código de Gray para minimizar BEM
- amplitude simétricas entre si para DC tender para 0

Díbit	V
10	+3
11	+1
01	-1
00	-3

} simetria

$$P_b = 2 P_S \text{ [bit/s]}$$

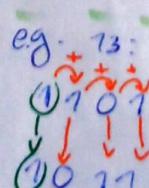
P_S - nº de símbolos enviados por segundo

- aumentar ritmo binário
- manter a largura de banda usada

Código de Gray

- código binário refletido
- muda apenas um bit entre configurações consecutivas

Binário	Gray
00	00
01	01
10	11
11	10



Binário → Gray:
 1) 1º dígito é igual
 2) outros são iguais à soma dos o anteriores

Aplicação

NMZ Unipolar	Ethernet, fibra
NMZ Bipolar	Interface RS-232
NMZ-S	USB
NMZ-M	Fest Ethernet, fibra
AMI	centrais telefônicas
B2I	infra-vermelhos
Manchester	Ethernet, cabo de cobre
2B1Q	BDJS ou ISDN

Nota:

USB e CAN → NMZ com bit-stuffing

Diagrama de Olho

- ferramenta de diagnóstico sobre o funcionamento do sistema
- avalia perturbação num SCP
- sobreposição de todos os Tb
- deteta
 - ↳ atrasos
 - ↳ ruído

Emissor, Meio e Receptor

Emissor

- codificador NMZ, RZ, ...
- meio de transmissão (cabos, fibra, ar)
- atenuação
- ruído
- interferência
- limitações da largura de banda

Receptor

- filtro de recusa
- regres de decisão binária

Detectar

• técnicas

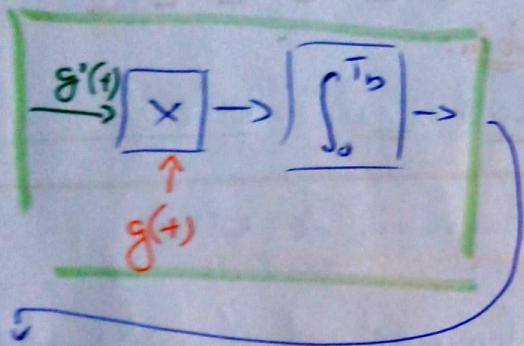
L correlador

L filtro adaptado

L demodulador coerente

• Correlador

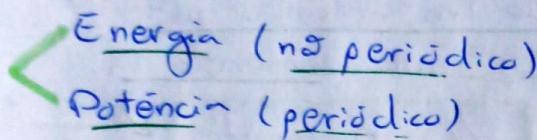
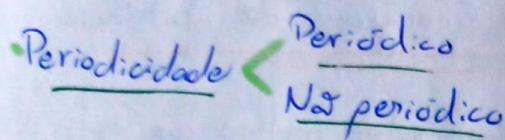
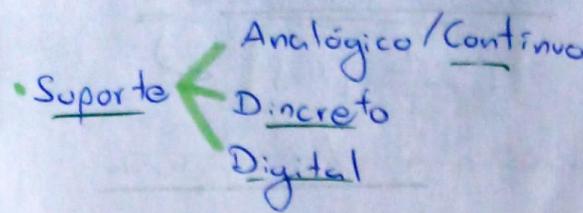
- O sinal usa como referência um pulso conhecido, $g(x)$



Regras de decisão

- determina a semelhança entre o pulso recebido e o referência
- após isto, aplica-se uma regra de decisão, para decidir o bit desejado

Sinais - Classificação



Sinais Contínuos e Discretos e Digitais

Sinal Contínuo

• f.r.v.r. $\rightarrow x(t): \mathbb{R} \rightarrow \mathbb{R}$

- Ex.: - microfone
- coluna
- monitor/impressora
- LED, ...

Sinal Discreto

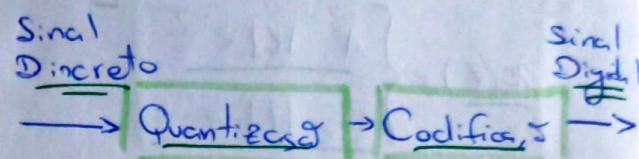
• f.r.v.i. $\rightarrow x[n]: \mathbb{Z}_0 \rightarrow \mathbb{R}$

- o eixo do tempo é discreto
• valor de amplitude obtidos:
 - por amostragem ao ritmo F_s (frequency of Sampling)
 - a cada T_s (time of sampling) é obtida uma nova amostra

Sinal Digital

f.i.v.i. $\rightarrow x[n]: \mathbb{Z}_0 \rightarrow \mathbb{R}$

- o eixo do tempo é discreto
• o eixo das amplitudes é discreto (cada amostra é um inteiro com n bits)



Nota: Sinais

- em termos gerais, é algo que codifica informação
• em termos físicos, representa uma corrente ou tensão elétrica utilizados no canal de transmissão na comunicação digital

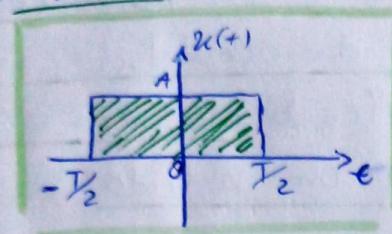
Sinais Periódicos e Não Periódicos

Sinais não periódicos (aperiódicos)

- não se repetem ao longo do tempo
• ex: - Pulso Retangular
- Pulso Sinusoidal

Pulso Retangular

- amplitude A
- duração T



$$x(t) = \begin{cases} A, & |t| < \frac{T}{2} \\ 0, & |t| \geq \frac{T}{2} \end{cases}$$

Pulso Sinusoidal

- produto de uma sinusóide por um pulso retangular

Sinais Periódicos

- repetem-se a cada período fundamental T_0

Ex.: sinusóides

onda quadrada

- T_0 - menor valor de tempo para o qual o sinal se repete

- Dominio Contínuo (período T_0)

$$x(t) = x(t + kT_0)$$

- Dominio Discreto (período de N amostras)

$$x[n] = x[n + kN]$$

- k - inteiro relativo

- o inverso do período fundamental é a frequência fundamental f_0

$$f_0 = \frac{1}{T_0} [\text{Hz}]$$

define a repetição do sinal

Sinais de Energia e de Potência

- A Lei de Joule indica que a potência instantânea $p(t)$ dissipada numa resistência R :

$$p(t) = R I^2 = \frac{U^2}{R}$$

Logo a potência para sinais...

$$p(t) = x^2(t)$$

- A energia é o romatório de todos os potências instantâneas.

No domínio Contínuo:

$$E_x = \int_{-\infty}^{+\infty} x^2(t) dt$$

No domínio Discreto:

$$E_x = \sum_{n=-\infty}^{+\infty} x^2[n]$$

Verifica-se que $0 \leq E_x \leq +\infty$

- A potência é dada pelo energia média num intervalo temporal de duração T

$$P_x = \lim_{T \rightarrow +\infty} \frac{1}{T} E_x$$

Tipicamente...

- Sinais não periódicos são caracterizados pela energia:
energia finita; potência nula

- Sinais periódicos são caracterizados pela potência:
energia infinita; potência finita

- Sinais limitados à esquerda e à direita se sempre de energia

- Para sinal periódico, ...

$$P_x = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} x^2(t) dt$$

a potência corresponde à energia média por período

Unidades SI:

energia - Joule [J]

potência - Watt [W]

Potência:

- No domínio contínuo:

$$P_x = \frac{1}{T_0} \int_{T_0} x^2(t) dt$$

- No domínio discreto:

$$P_x = \frac{1}{N} \sum_N x^2[n]$$

0 < P < ∞

Se o sinal tem energia finita e não nula diz-se

sinal de energia

Têm potência nula

se o sinal tem potência finita e não nula diz-se ~~sinal~~
sinal de potência

Têm energia infinita

Sinal de Potência (periódico)

vári médio, ou componente DC (Direct Current)

No domínio contínuo:

$$m_x = \frac{1}{T_0} \int_{T_0} x(t) dt$$

No domínio discreto:

$$m_x = \frac{1}{N} \sum_N x[n]$$

Aplicações

Sinais biometrícios

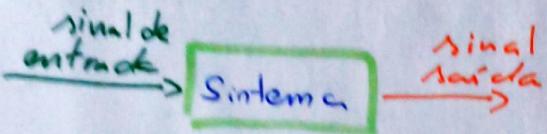
Sismógrafo

código de linha (banda base)

pulsos sinusoidais (banda canal)

Sistema e Operações

- Sistema é um objeto que manipula um ou mais sinais para realizar certa função, produzindo um novo sinal



Tipos de Operações

- Sobre variável dependente (Amplitude)

- Amplificação ou atenuação
- Adição (subtração)
- Multiplicador

- Sobre variável independente (Tempo)

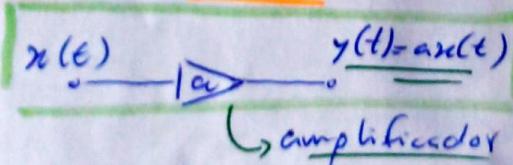
Exalação

- comprimento e expansão
- reflexos (caso particular)

Deslocamento

- avanço
- atraso

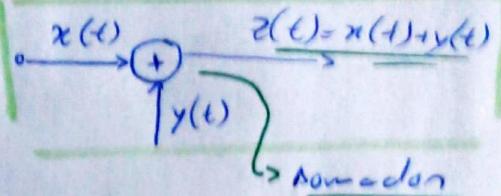
Amplificação ou Atenuação



- $|a| > 1 \rightarrow$ amplificação
- $|a| < 1 \rightarrow$ atenuação

$$E_y = a^2 E_x$$

Soma (subtração)

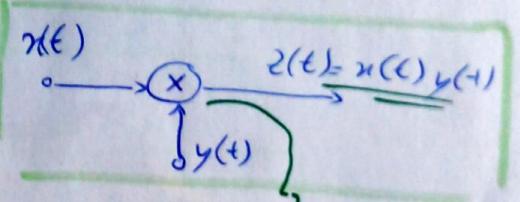


a subtração é com soma, mas $y(t)$ é negativo

$$E_z = \int_{-\infty}^{+\infty} x^2(t) dt + \int_{-\infty}^{+\infty} y^2(t) dt + 2 \int_{-\infty}^{+\infty} n(t) y(t) dt$$

na subtração

Produto



multiplicador

Escalamento

$$y(t) = x(at)$$

$|a| > 1$ - comprimento

$|a| < 1$ - expansão

altera a energia, mas não a potência:

$$E_y = \frac{1}{|a|} E_x \quad \text{e} \quad P_y = P_x$$

Nota:

deslocamento
não altera
energia
não potência

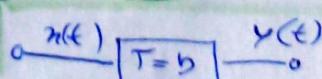
escalado
do deslocamento
ao escalamento

Deslocamento

$$y(t) = x(t - b)$$

$b > 0$ - atraso

$b \leq 0$ - avanço



Sinuso - Espectro

Sinuso Periódicos

- repetem-se a cada período fundamental T_0

continuo - $x(t) = x(t + kT_0)$

discreto - $x[t] = x[n + kN]$

Sinusoide

- tem valor médio nulo

$$x(t) = A \cos(2\pi f_0 t + \phi)$$

A - max. amplitude

f_0 - frequência fundamental

ϕ - fase inicial

a potência apenas depende da amplitude:

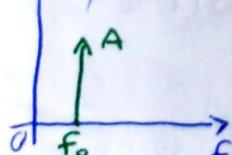
$$P_x = \frac{A^2}{2}$$

Espectro de Amplitude

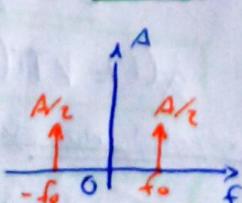
- indica a distribuição de potência pelas frequências

Espectro Unilateral

Amplitude



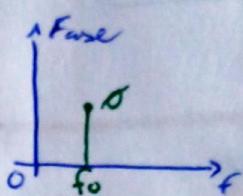
Espectro Bilateral



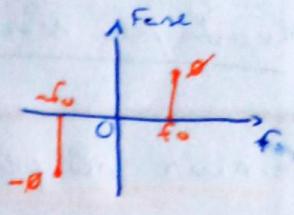
Espectro de Fase

- indica o desfasamento de cada componente de frequência

Unilateral



Bilateral



Notas:

- amplitude sempre positiva:

$$-\cos(x) = \cos(x + \pi)$$

- cossenos sempre:

$$\sin(x) = \cos(x - \frac{\pi}{2})$$

Indicações

$$x(t) = A_0 + \sum_{k=1}^{+\infty} A_k \cos(2\pi k f_0 t + \phi_k)$$

ou

$$x(t) = \sum_{k=-\infty}^{+\infty} |C_k| \cos(2\pi k f_0 t + \phi_k)$$

Potência [w]

$$P_x = A_0^2 + \sum_{k=1}^{+\infty} \frac{A_k^2}{2} \rightarrow \text{Espectro Unilateral (A)}$$

$$P_x = \sum_{k=-\infty}^{+\infty} |C_k|^2 \rightarrow \text{Espectro Bilateral (A)}$$

→ Teorema de Parseval

Valor Médio (DC)

$$m_\infty = A_0 = C_0 \rightarrow \text{frequência 0}$$

Largura de Bandeira

$$LB = \text{máx. } f - \text{mín. } f \text{ (positiva)} [\text{Hz}]$$

- largura da faixa de frequência ocupada pelo sinal

Sinais não periódicos

- não apresentam padrões de repetição
- caracterizados pela energia finita
- representados por um espetro contínuo no domínio da frequência

Pulso Retangular

- sinal estritamente limitado no tempo

$$E = A^2 T$$

$$v(t) = \begin{cases} A, & t \in [-\frac{T}{2}; \frac{T}{2}] \\ 0, & t \notin \end{cases}$$

$$v(t) = A \Pi\left(\frac{t}{T}\right)$$

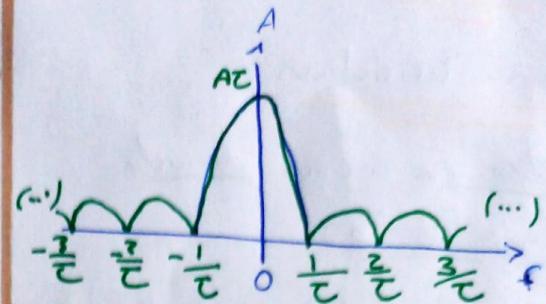
$$\Pi\left(\frac{t}{T}\right) = \begin{cases} 1, & |t| < \frac{T}{2} \\ 0, & |t| > \frac{T}{2} \end{cases}$$

Expressão do Espectro:

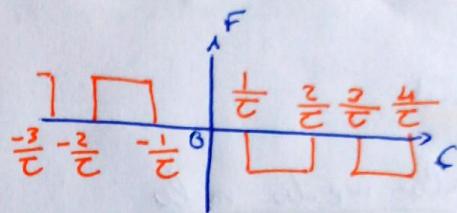
$$V(f) = \frac{A}{\pi f} \sin(fT) = AT \operatorname{sinc}(fT)$$

$$V(0) = AT$$

Espetro de Amplitude



Espetro de Fase



Nota: Transformada de Fourier

- sinal não periódico corresponde a sinal periódico com $T_0 \rightarrow \infty$
- assim $f_0, 2f_0, \dots \rightarrow 0$

$$v(t) = \int_{-\infty}^{+\infty} X(f) \exp(j2\pi f t) df$$

↳ transformada inversa

Pulso Sinenoidal

- no domínio do tempo, resulta do produto de uma sinusoide por um pulso retangular

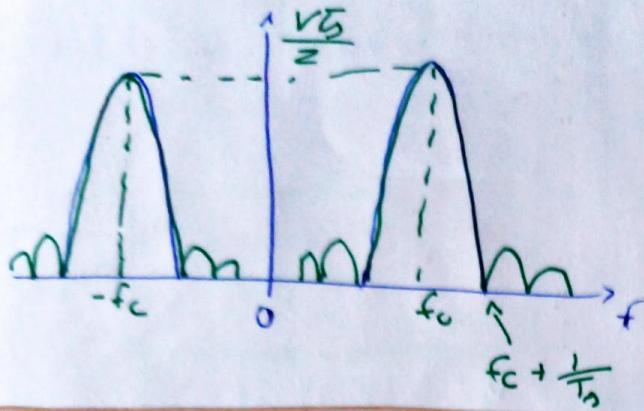
$$E = \frac{V^2}{2} T_0$$

$$g(t) = V \Pi\left(\frac{t}{T_0}\right) \cos(2\pi f_c t)$$

Expressão no espectro:

$$G(f) = V \frac{T_0}{2} \sin((f-f_c)T_0) + V \sum_{n=1}^{\infty} \sin((f+nf_c)T_0)$$

Espetro de Amplitude



Indicadores

Energia

- Teorema de Rayleigh
- relações idênticas ao teorema de potência de Parseval

$$E = \int_{-\infty}^{\infty} |V(f)|^2 df$$

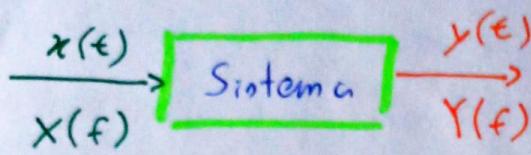
} densidade de
espectral de energia
[J/Hz]

Largura de Banda

- definida a partir dos zeros
espectrais

Resposta em Frequência H(f)

- caracteriza o comportamento no domínio da frequência



$$Y(f) = X(f)H(f)$$

Filtream

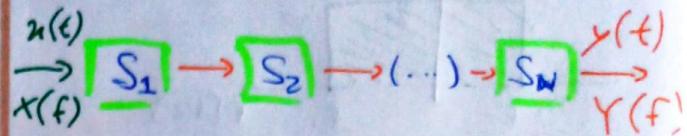
- os componentes que constam de $X(f)$ e não constam de $Y(f)$ são filtrados (eliminados) pelo sistema
- O tipo de filtragem é definido pelas funções $H(f)$

Tipos de filtragem:

- passa - baixo
- passa - banda
- passa - alto
- rejeita - banda

Associação de Sistemas

Associação Série / Cadeia

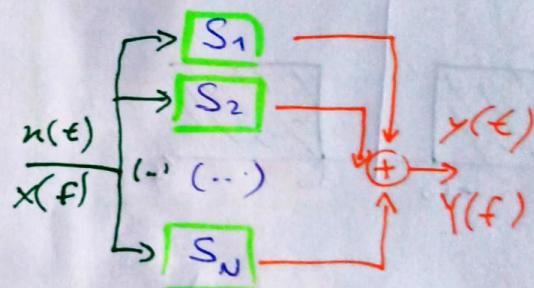


- a resposta em frequência equivalente é o produto das respostas em frequência individuais:

$$H_{eq}(f) = H_1(f)H_2(f) \dots H_N(f)$$

$$= \prod_{k=1}^N H_k(f)$$

Associação Paralelo

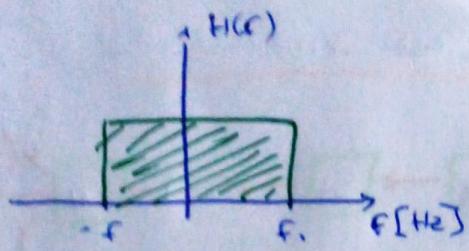


- a resposta em frequência equivalente é a soma das respostas individuais:

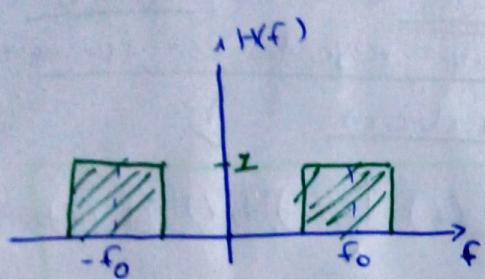
$$H_{eq}(f) = H_1(f) + H_2(f) + \dots + H_N(f)$$

$$= \sum_{k=1}^N H_k(f)$$

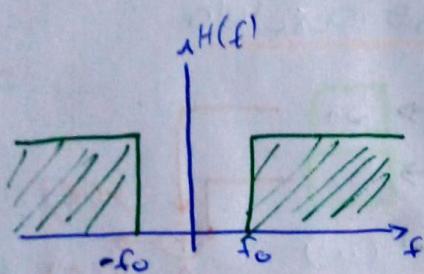
Passa-band ideal



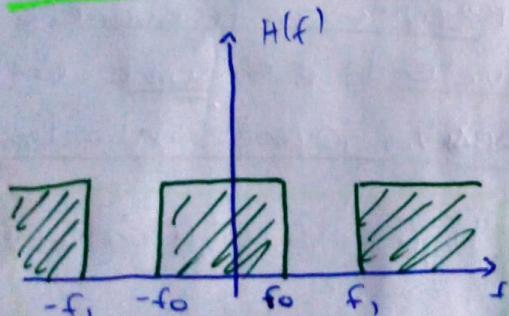
Passa-banda ideal



Passa-alto ideal



Rejeita-banda ideal



Banda Canal

- Pulso sinuoidal
- Espectro do tipo passa-banda
- f_c é dada pela sinuóide
- LB é dada pelo ritmo de transmissão

Modulações Digitais

- Várias de forma individual
 - 3 parâmetros dum sinuóide
- ASK (Amplitude Shift Keying)
 - ↳ OOK (On-Off keying) é o particular de ASK
- FSK (Frequency Shift Keying)
- PSK (Phase Shift Keying)

Modulação	Binária	Multíplica
ASK	✓	✓
OOK	✓	✓
PSK	✓	✓
FSK	✓	✓
QAM (APK)	✗	✓

Modulações M-árias

- aumentam o ritmo de transmissão, para a mesma LB (excepto M-FSK)
- usam $M \geq 2$ níveis e transmitem

$$k = \log_2(M) \text{ bit/simb}$$

- o ritmo binário é:

$$R_b = R_s \log_2(M) \text{ bit/segundo}$$

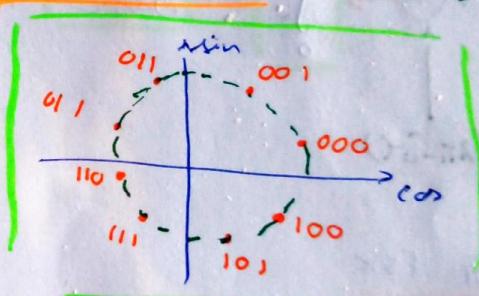
↙ $R_s = \text{nº de símbolos enviados por s.}$

M-PSK

- fase depende da seq. binária
- muda a fase entre síncronos, a amplitude e freq. são constantes
- todos os síncronos têm a mesma energia

$$v(t) = A \cos(2\pi f t + \phi)$$

Constelação 8-PSK

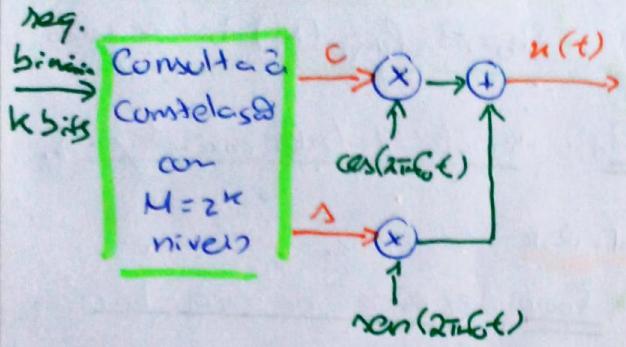


Codificação de Gray

QAM

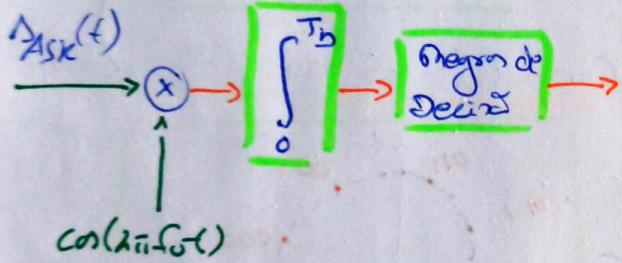
- amplitude e fase dependem da seq. binária
- diferentes constelações
- síncronos com diferentes energias

Emissor genérico M-PSK e QAM

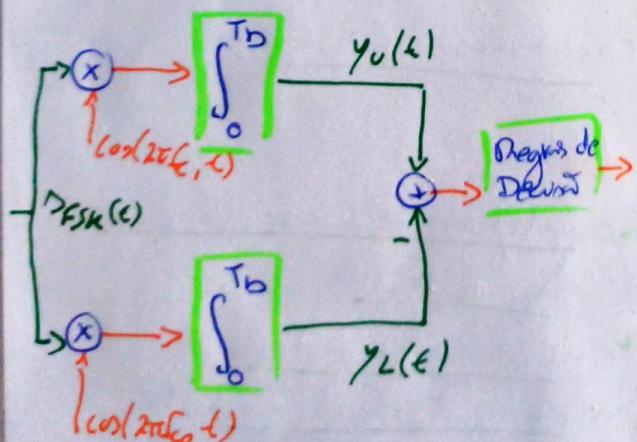


Receptor ASK/OOK/PSK

- diferença para cada modulação é nas regras de decisão binária

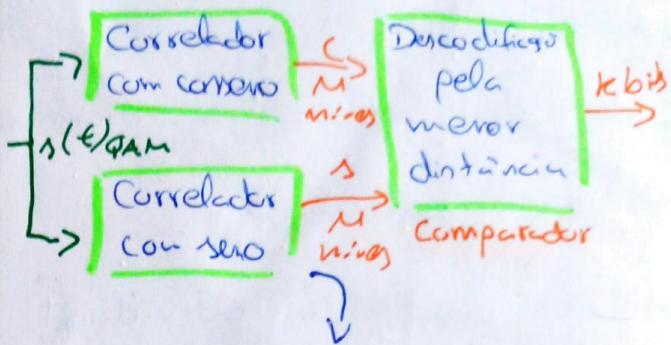


Receptor FSK

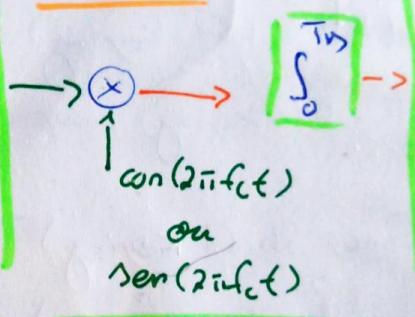


Receptor genérico M-PSK e QAM

- Para qualquer valor de M , basta usar dois correladores



Correlador:



Transmissão não ideal

- atenuação
- largura de banda limitada
- distorção
- delay (atraso)
- ruído
- mistura dos efeitos

Curvas de BER

- taxa de erro
- define a qualidade do serviço (QoS)
- BER aceitável
 - voz = 10^{-3}
 - dados = 10^{-6}
 - WLAN = 10^{-5}

Note: S/N - Signal-to-noise ratio

UBB - Unipolar Base Band \rightarrow NRZU

BBB - Bipolar " " \rightarrow NRZB

Teorema de capacidade de canal

- a probabilidade de erro do canal determina a capacidade C de transferência de info.
- Se $P \leq C$, com probabilidade de erro arbitrariamente pequena, é possível transmitir sem erros

Lei de Hartley-Shannon



$$C = B \log_2 (1 + S/N) \text{ [bit/seg]}$$

B - largura de banda

S/N - relação sinal/ruído

Aplicações

<u>Modulação</u>	<u>Aplicação</u>
OOK	transmissão em fibra ótica
ASK	NFC - Near Field Communication
GMSK	GSM - Global System Mobile
FSK	transmissão com MODEM
BPST e QPSK	Wi-Fi
	Wi-Fi ADSL DVB-T OFDM LTE
QAM	