Instituto Federal de Santa Catarina

Curso superior de tecnologia em sistemas de telecomunicação

Comunicações móveis 2

Códigos de bloco

Prof. Diego da Silva de Medeiros

São José, maio de 2012

Codificação

- Modificação dos dados a serem transmitidos, apropriando-os à aplicação
- Codificação de fonte
    - Redução de redundância nos sinais transmitidos, com ou sem perdas
    - Ex:

Codificação

- Modificação dos dados a serem transmitidos, apropriando-os à aplicação
- Codificação de fonte
  - Redução de redundância nos sinais transmitidos, com ou sem perdas
  - Ex:
    - Padrão JPEG (com e sem perdas)
    - Geração do alfabeto baseado na frequência de ocorrência dos símbolos:

Símbolo	Frequência	Binário sem codificação	Binário com codificação
0	Muito frequente	00	0
1	Nunca	01	1110
2	Pouco frequente	10	110
3	Muito frequente	11	10

Codificação

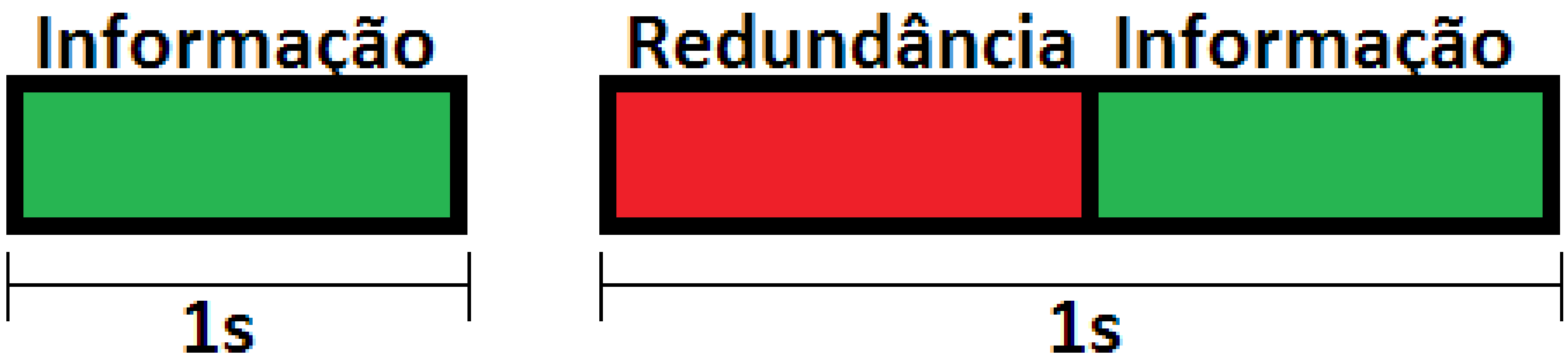
- Codificação de canal
  - Inclusão de redundância controlada na informação
  - Detecção/correção de erros na transmissão
  - Ex:

Codificação

- Codificação de canal
  - Inclusão de redundância controlada na informação
  - Detecção/correção de erros na transmissão
  - Ex:
    - Paridade
    - CRC - Cyclic Redundancy Check
    - Códigos de bloco
    - Códigos convolucionais
    - Códigos Turbo
    - Códigos LDPC
    - ...

Codificação de canal

- Inclusão de redundância controlada para auxiliar a detecção/correção de erros
- Reduz eficiência espectral, mas melhora a performance de BER
- Ex: bits de paridade



Códigos de bloco

- Conseguem **corrigir** um número determinado de erros sem retransmissão
- Bits de redundância são adicionados à blocos da mensagem para produzir **palavras-código**
- Referenciado como código (n,k), onde
  - n = número de bits da palavra codificada
  - k = número de bits do bloco de informação (2^k palavras-código)
  - n - k = número de bits de redundância adicionados na codificação
  - Rc = k/n = Taxa de código

Códigos de bloco - Propriedades

- Distância do código
  - Número de elementos diferentes entre duas palavras código

$$d\left(c_i, c_j\right) = \sum_{l=1}^{n} c_{i,l} \circ c_{j,l}$$

$$\left.\begin{matrix} 1\boxed{0}1\boxed{0}0 \\ 1\boxed{1}1\boxed{1}0 \end{matrix}\right\} \text{Distância} = 2$$

- Distância mínima de Hamming
  - Menor distância dentro do código

$$d_{min} = min\left\{d\left(c_i, c_j\right)\right\}$$

Info	Código	Distância	
000	0000		
		1	
001	0000		
		2	
010	0000		
		1	
011	0000		
		3	1
100	0000		
		1	
101	0000		
		2	
110	0000		
		1	
111	0000		

Códigos de bloco - Propriedades

- Peso de um código
  - Número de coordenadas não nulas da palavra-código
  - Em transmissões binárias, o peso do código é o número de bits 1 da palavra-código

$$W(c_i) = \sum_{l=1}^{n} c_{i,l}$$

- Capacidade de detecção de erros de um código

$$t_d = d_{min} - 1$$

- Capacidade de correção de erros de um código

$$t_c = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$$

Códigos de bloco - Propriedades

- Linearidade
  - Um código é linear se o código a seguir é uma palavra-código do conjunto

$$C = \alpha_1 c_i + \alpha_2 c_j$$

    onde α_1 e α_2 são dois elementos selecionados dentro do alfabeto e c_i e c_j são duas palavras código
  - O Código também precisa possuir a palavra-código de tudo zero
- Padrão de erros
  - Diferença entre o código transmitido e o recebido
  - Tem o mesmo comprimento que uma palavra-código

Linearidade - Exemplo

- Verificar se os seguintes códigos são lineares

$$A=\{[0\,0\,0] \quad [0\,0\,1] \quad [0\,1\,0] \quad [0\,1\,1] \quad [1\,0\,0] \quad [1\,0\,1] \quad [1\,1\,0] \quad [1\,1\,1]\}$$

$$B=\{[0\,0\,0] \quad [0\,0\,1] \quad [1\,0\,0] \quad [1\,0\,1]\}$$

$$C=\{[0\,0\,0] \quad [1\,0\,0] \quad [1\,1\,0] \quad [1\,1\,1]\}$$

$$D=\{[0\,0\,1] \quad [1\,0\,0] \quad [1\,0\,1]\}$$

Linearidade - Exemplo

- Verificar se os seguintes códigos são lineares

$$A=\{[0\,0\,0] \quad [0\,0\,1] \quad [0\,1\,0] \quad [0\,1\,1] \quad [1\,0\,0] \quad [1\,0\,1] \quad [1\,1\,0] \quad [1\,1\,1]\}$$
$$B=\{[0\,0\,0] \quad [0\,0\,1] \quad [1\,0\,0] \quad [1\,0\,1]\}$$
$$C=\{[0\,0\,0] \quad [1\,0\,0] \quad [1\,1\,0] \quad [1\,1\,1]\}$$
$$D=\{[0\,0\,1] \quad [1\,0\,0] \quad [1\,0\,1]\}$$

- Não lineares:
  - C → Soma de dois elementos não resulta em nenhum outro do conjunto
  - D → Não há a palavra-código de tudo zero

Códigos de bloco - Representação matricial

- Quando *k* é grande, a codificação através de tabelas se torna pouco prática
- Dá-se então através da operação genérica

$$\boldsymbol{c_i} = \boldsymbol{m_i}\,\boldsymbol{G}$$

onde

$$\boldsymbol{c_i} = \begin{bmatrix} c_{i0} & c_{i1} & \cdots & c_{i(n-1)} \end{bmatrix} = \textit{Palavra codificada}$$

$$\boldsymbol{m_i} = \begin{bmatrix} m_{i0} & m_{i1} & \cdots & m_{i(k-1)} \end{bmatrix} = \textit{Vetor de informação}$$

$$\boldsymbol{G} = \begin{bmatrix} g_{00} & g_{01} & \cdots & g_{0(n-1)} \\ g_{10} & g_{11} & \cdots & g_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ g_{(k-1)0} & g_{(k-1)1} & \cdots & g_{(k-1)(n-1)} \end{bmatrix} = \textit{Matriz geradora}$$

$$= \begin{bmatrix} \boldsymbol{g_0} \\ \boldsymbol{g_1} \\ \vdots \\ \boldsymbol{g_{(k-1)}} \end{bmatrix}$$

Códigos de bloco - Representação matricial

- Exemplo: verificar se a matriz **G** a seguir é a matriz geradora do código a seguir

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Mensagem	Palavra-código
000	0000
001	0011
010	0101
011	0110
100	1001
101	1010
110	1100
111	1111

Códigos de bloco - Forma sistemática da matriz geradora

- Forma obtida através de adições e/ou permutações de linhas da matriz original
- Forma sistemática consiste em uma das abaixo

$$G=\begin{bmatrix} I_k & P \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & p_{00} & p_{01} & \cdots & p_{0(n-k-1)} \\ 0 & 1 & 0 & \cdots & 0 & p_{10} & p_{11} & \cdots & p_{1(n-k-1)} \\ 0 & 0 & 1 & \cdots & 0 & p_{20} & p_{21} & \cdots & p_{2(n-k-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & p_{(k-1)0} & p_{(k-1)1} & \cdots & p_{(k-1)(n-k-1)} \end{bmatrix}$$

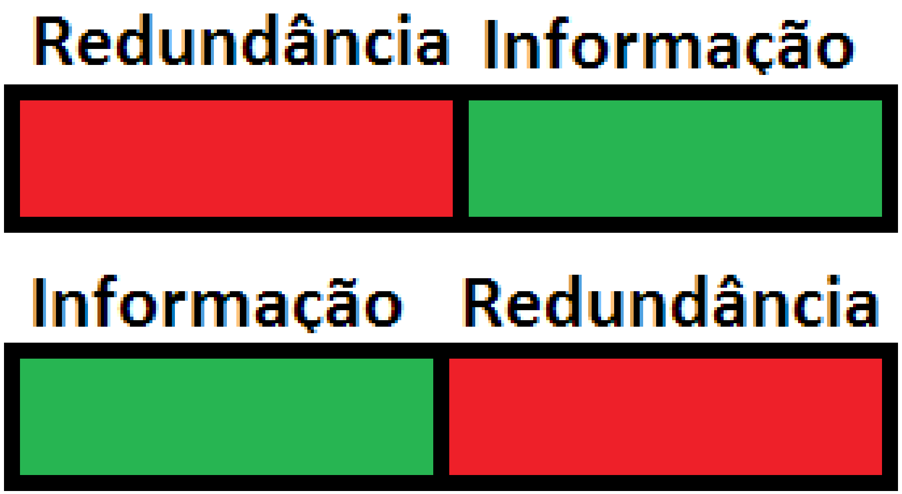
Onde

Ik = Matriz identidade de ordem **k**
P = *Matriz de paridade* **k** x (**n** - **k**)

$$G=\begin{bmatrix} P & I_k \end{bmatrix}=\begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0(n-k-1)} & 1 & 0 & 0 & \cdots & 0 \\ p_{10} & p_{11} & \cdots & p_{1(n-k-1)} & 0 & 1 & 0 & \cdots & 0 \\ p_{20} & p_{21} & \cdots & p_{2(n-k-1)} & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{(k-1)0} & p_{(k-1)1} & \cdots & p_{(k-1)(n-k-1)} & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Códigos de bloco - Forma sistemática da matriz geradora

- Matriz geradora na forma sistemática gera um ***código sistemático***
- Códigos sistemáticos possuem a mesma distância de Hamming de um código não sistemático de mesma ordem



$$G = \begin{bmatrix} P & I_k \end{bmatrix}$$

$$G = \begin{bmatrix} I_k & P \end{bmatrix}$$

Códigos de bloco - Forma sistemática da matriz geradora

- Exemplo: dada a matriz geradora a seguir, colocar na forma sistemática

$$\boldsymbol{G} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Códigos de bloco - Forma sistemática da matriz geradora

- Exemplo: dada a matriz geradora a seguir, colocar na forma sistemática

$$\boldsymbol{G} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

- L0 $\leftrightarrow$ L2
- (L0 + L1) $\rightarrow$ L0
- (L0 + L2) $\rightarrow$ L0

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Códigos de bloco - Matriz verificadora de paridade

- Matriz ***H*** cujas linhas são ortogonais às linhas da matriz ***G***
- Tem dimensão (**n**-**k**) x **n**

$$\boldsymbol{G} \cdot \boldsymbol{H}^{t} = \mathbf{0}$$

onde **0** = Matriz de zeros de dimensão **k** x (**n**-**k**)

- Para garantir a propriedade da ortogonalidade, a matriz ***H*** deve ser

$$\boldsymbol{H} = \begin{cases} \begin{bmatrix} \boldsymbol{P}^{t} & \boldsymbol{I}_{n-k} \end{bmatrix} & \text{para } \boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_{k} & \boldsymbol{P} \end{bmatrix} \\ \begin{bmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{P}^{t} \end{bmatrix} & \text{para } \boldsymbol{G} = \begin{bmatrix} \boldsymbol{P} & \boldsymbol{I}_{k} \end{bmatrix} \end{cases}$$

Matriz verificadora de paridade - Exemplo 1

- Dadas as matrizes abaixo, verificar se o produto resulta em zero

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_k & \boldsymbol{P} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{P}^t & \boldsymbol{I}_{n-k} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Matriz verificadora de paridade - Exemplo 1

- Dadas as matrizes abaixo, verificar se o produto resulta em zero

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_k & \boldsymbol{P} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{P}^t & \boldsymbol{I}_{n-k} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\boldsymbol{G} \cdot \boldsymbol{H}^t = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Matriz verificadora de paridade - Exemplo 2

- Seja a seguinte matriz geradora, encontrar a matriz de verificação de paridade e verificar se o vetor $\boldsymbol{m_i}$ = [1 1 0 1 0 1] pertence ao código.

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_k & \boldsymbol{P} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Matriz verificadora de paridade - Exemplo 2

- Seja a seguinte matriz geradora, encontrar a matriz de verificação de paridade e verificar se o vetor $\boldsymbol{m_i}$ = [1 1 0 1 0 1] pertence ao código.

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_k & \boldsymbol{P} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{P}^t & \boldsymbol{I}_{n-k} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Matriz verificadora de paridade - Exemplo 2

- Seja a seguinte matriz geradora, encontrar a matriz de verificação de paridade e verificar se o vetor ***mi*** = [1 1 0 1 0 1] pertence ao código.

$$G = \begin{bmatrix} I_k & P \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} P^t & I_{n-k} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$m_i \cdot H^t = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$$

- Como deu zero, significa que ***mi*** pertence ao código gerado pela matriz ***G***

Códigos de bloco - Teste da síndrome

- Vetor recebido

$$\boldsymbol{r} = \boldsymbol{m}_i + \boldsymbol{e}$$

onde ***e*** = vetor de erros ou padrão de erros

- Define-se o vetor de *síndrome de erro*, com **n**-**k** bits:

$$\begin{aligned} \boldsymbol{s} &= \boldsymbol{r} \cdot \boldsymbol{H}^t \\ &= \left(\boldsymbol{m}_i + \boldsymbol{e}\right) \cdot \boldsymbol{H}^t \\ &= \boldsymbol{e} \cdot \boldsymbol{H}^t \end{aligned}$$

- Ou seja, a síndrome ***s*** está associada à um padrão de erros
- Um padrão de erros corrigível pode ser associado à uma síndrome específica

Teste da síndrome - Exemplo 1

- Suponha que o vetor ***mi*** = [1 1 0 1 0 1] tenha sido transmitido e corrompido por ruído no canal, de forma que na recepção tenha sido detectado o vetor ***r*** = [0 1 0 1 0 1]. Determinar a síndrome de ***r*** e comparar com $\boldsymbol{e} \cdot \boldsymbol{H}^t$. Usar a mesma matriz ***H*** do exemplo anterior

$$
\begin{aligned}
\boldsymbol{s} &= \boldsymbol{r} \cdot \boldsymbol{H}^t \\
&= \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\
&= 0 \cdot \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} + 1 \cdot \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} + 0 \cdot \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} + 1 \cdot \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}
\end{aligned}
$$

Teste da síndrome - Exemplo 1

- O padrão de erros é

$$\begin{aligned} \boldsymbol{e} &= \boldsymbol{m}_i + \boldsymbol{r} \\ &= \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

- E a outra forma de encontrar a síndrome é:

$$\begin{aligned} \boldsymbol{s} &= \boldsymbol{e} \cdot \boldsymbol{H}^t \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= 1 \cdot \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} + 0 \cdot \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} + 0 \cdot \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} \end{aligned}$$

- Ou seja, o vetor de síndromes pode ser encontrado diretamente do vetor recebido, e pode ser associado à um padrão de erros específico!

Teste da síndrome x padrão de erros

- Quantos padrões de erros podem existir?

$$2^n$$

- Quantos vetores de síndrome de erros podem existir?

$$2^{n-k}$$

- Ou seja, há mais de um padrão de erros associado à uma síndrome

Teste da síndrome x padrão de erros - Exemplo

- Para a seguinte matriz de verificação de paridade, verificar as síndromes dos padrões de erro ***e1*** = [0 0 0 1 0 1] e ***e2*** = [0 1 0 0 0 0]

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{P}^t & \boldsymbol{I}_{n-k} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\boldsymbol{s}_1 = \boldsymbol{e}_1 \cdot \boldsymbol{H}^t = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1\,0\,1 \end{bmatrix}$$

$$\boldsymbol{s}_1 = \boldsymbol{e}_1 \cdot \boldsymbol{H}^t = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1\,0\,1 \end{bmatrix}$$

Mas há uma maior probabilidade de 1 erro de bit ocorrer do que 2.