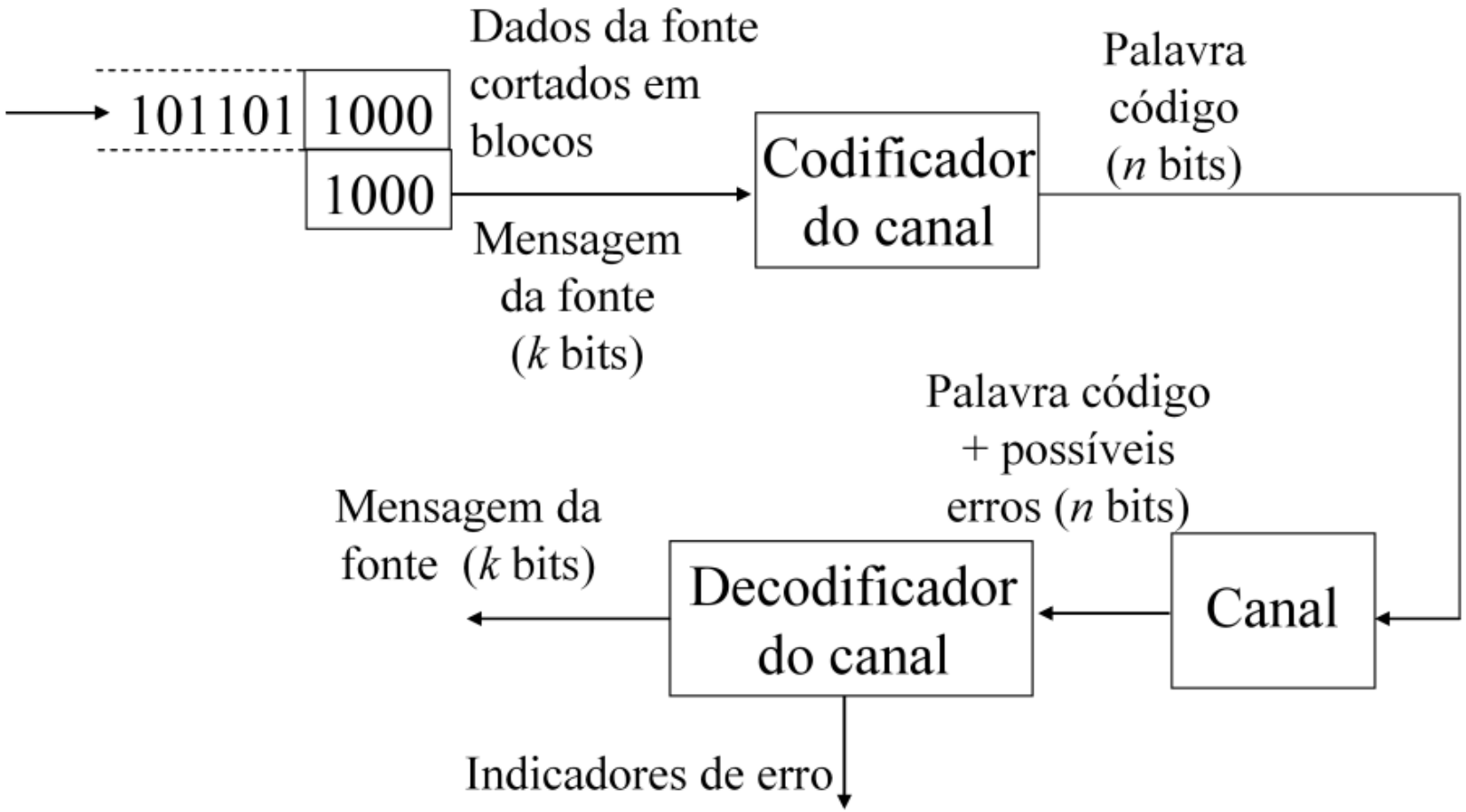
Códigos de bloco

- A mensagem é denotada como $\mathbf{m} = \{m_0, m_1, ..., m_{k-1}\}$
  - Existem 2^k blocos distintos.
- A palavra código é denotada como $\mathbf{c} = \{c_0, c_1, ..., c_{n-1}\}$
  - De todas as 2^n combinações possíveis, somente 2^k são realmente palavras código, logo existem $2^n - 2^k$ combinações, que se recebidas, são identificadas como um erro.
- Existem diversas maneiras de obter os n bits da palavra código a partir dos k bits da mensagem da fonte. Nós vamos nos concentrar em uma classe particular de blocos que reduz as complexidade de codificação. O *Códigos de bloco lineares*

1. Códigos de bloco lineares
2. Códigos sistemáticos
3. Síndrome
4. Distância de Hamming
5. Arranjo padrão e decodificação de síndrome
6. Código de Hamming

Introdução

- Somente o *Galois Field* binário vai ser considerado $GF(2)$.
- A palavra da fonte contém k bits.
- A palavra do código contém n bits.
- A redundância é então de $n - k$.
- O código é conhecido como código de bloco (n, k)
- A taxa do código é então $R = k/n$


101101
1000
1000
Dados da fonte cortados em blocos
Mensagem da fonte (k bits)
Codificador do canal
Palavra código (n bits)
Palavra código + possíveis erros (n bits)
Canal
Decodificador do canal
Mensagem da fonte (k bits)
Indicadores de erro

Sumário

- O código (n, k) é linear se as 2^k palavras código formam um subespaço C de k dimensões do espaço vetorial V_n que contém todas as n-uplas no campo $GF(2)$, $GF(2^n)$. Existem então k palavras código que são linearmente independentes. Essas palavras códigos são denotadas $\mathbf{g}_j = \{g_{j0}, g_{j1}, ..., g_{jn-1}\}$, $0 \leq j \leq k-1$.
- O código de bloco é linear se a soma módulo-2 de duas palavras código também é uma palavra código. Cada bit da mensagem da fonte é denotado m_{ij}, i para representar a posição do bit de $0 \leq i \leq k-1$ e j para representar a mensagem de $0 \leq j \leq 2^k - 1$. Em C cada palavra código $\mathbf{c}_j = \{c_{j0}, c_{j1}, ..., c_{jn-1}\}$ é uma combinação linear dessas k palavras código:

$$\mathbf{c}_j = m_{j0}\mathbf{g}_0 + m_{j1}\mathbf{g}_1 + \cdots + m_{jk-1}\mathbf{g}_{k-1}$$

- O processo de codificação pode ser representado de maneira matricial:

$$\mathbf{c}_j = \mathbf{m}_j \cdot G$$

$$= (m_{j0}, m_{j1}, \cdots, m_{jk-1}) \cdot \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix}$$

$$= m_{j0}\mathbf{g}_0 + m_{j1}\mathbf{g}_1 + \cdots + m_{jk-1}\mathbf{g}_{k-1}$$

- Desenvolvendo a matriz G:

$$G = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

- Como $\mathbf{g}_j$ gera $\mathbf{c}_j$, a matriz G é chamada de **matriz geradora**.

- Exemplo de código linear $(7, 4)$, com a seguinte matriz geradora:

$$G = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} =$$

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

Mensagens	Palavras código
(0 0 0 0)	(0 0 0 0 0 0 0)
(1 0 0 0)	(1 1 0 1 0 0 0)
(0 1 0 0)	(0 1 1 0 1 0 0)
(1 1 0 0)	(1 0 1 1 1 0 0)
(0 0 1 0)	(1 1 1 0 0 1 0)
(1 0 1 0)	(0 0 1 1 0 1 0)
(0 1 1 0)	(1 0 0 0 1 1 0)
(1 1 1 0)	(0 1 0 1 1 1 0)
(0 0 0 1)	(1 0 1 0 0 0 1)
(1 0 0 1)	(0 1 1 1 0 0 1)
(0 1 0 1)	(1 1 0 0 1 0 1)
(1 1 0 1)	(0 0 0 1 1 0 1)
(0 0 1 1)	(0 1 0 0 0 1 1)
(1 0 1 1)	(1 0 0 1 0 1 1)
(0 1 1 1)	(0 0 1 0 1 1 1)
(1 1 1 1)	(1 1 1 1 1 1 1)

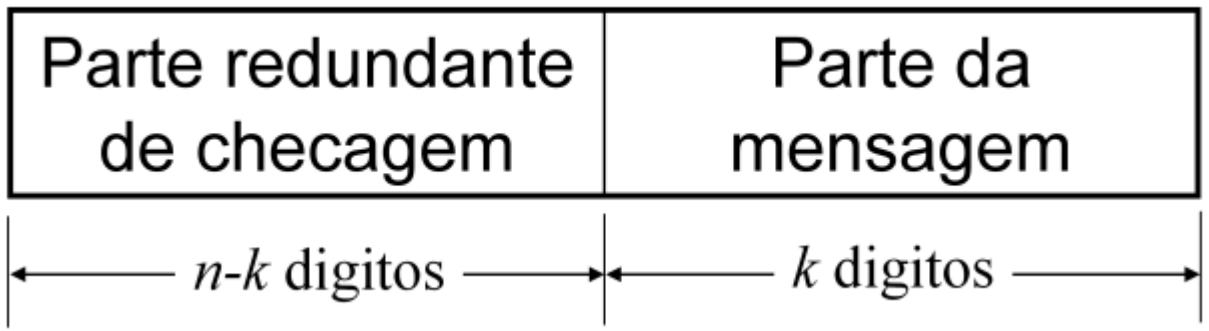
- Se $\mathbf{m}_{13} = (1101)$ é a mensagem a ser codificada, a palavra chave correspondente é:

$$\mathbf{c}_{13} = 1 \cdot \mathbf{g}_0 + 1 \cdot \mathbf{g}_1 + 0 \cdot \mathbf{g}_2 + 1 \cdot \mathbf{g}_3$$
$$= 1 \cdot (1101000) + 1 \cdot (0110100) + 0 \cdot (1110010) + 1 \cdot (0001101) =$$
$$(1101000) +$$
$$(0110100) +$$
$$(1010001) =$$
$$(0001101)$$

Sumário

Códigos sistemáticos

- Uma característica desejável do código para que ele seja mais fácil de decodificar é que ele seja sistemático.
- Definição de sistemático:
  - É um código que as palavras códigos contém uma repetição da mensagem da fonte com k bits mais a parte de checagem redundante de $n - k$ bits, que são chamados bits de paridade.



sistemático

- Primeiro criar a matriz $\mathbf{P}$ que cria os bits de paridade. Ela é de dimensão $k \times (n - k)$
- Depois a parte que constrói a repetição da mensagem da fonte na parte direita da palavra código.

  Matriz identidade $k \times k$

- $G = [P \vdots I_k]$

$$
\overbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}^{\text{Matriz } p}
\qquad
\overbrace{\qquad\qquad\qquad\qquad}^{\substack{\text{Matriz} \\ \text{identidade } k \times k}}
$$

$$
G = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} =
$$

$$
\left[\begin{array}{cccc|ccccc}
p_{00} & p_{01} & \cdots & p_{0,n-k-1} & 1 & 0 & 0 & \ldots & 0 \\
p_{10} & p_{11} & \cdots & p_{1,n-k-1} & 0 & 1 & 0 & \ldots & 0 \\
p_{20} & p_{21} & \cdots & p_{2,n-k-1} & 0 & 0 & 1 & \ldots & 0 \\
 & & & & & & & & \\
p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & 0 & \ldots & 1
\end{array}\right]
$$

exemplo de código sistemático

$$\mathbf{c} = (m_0, m_1, m_2, m_3) \cdot \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- Nós vamos calcular $\mathbf{c}$ em função de $\mathbf{m}$:

- $(c_0, c_1, c_3, c_4, c_5, c_6) =$

- $c_0 = m_0 + m_2 + m_3$
  $c_1 = m_0 + m_1 + m_2$
  $c_2 = m_1 + m_2 + m_3$
  $c_3 = m_0$
  $c_4 = m_1$
  $c_5 = m_2$
  $c_6 = m_3$

Matriz de verificação de paridade

- Existe uma outra matriz ainda mais interessante para a decodificação. Ela é menor que a matriz G e serve para indicar a paridade do sinal recebido. O resultado do sinal recebido multiplicado por essa matriz dá zero quando não há erros de transmissão.
- Vamos definir a *matriz de verificação de paridade* dada por $H = [I_{n-k} \vdots P^T]$, onde P^T é a matriz transposta de P. Veja que a matriz H é menor que a matriz G.
- Vamos verificar o resultado de HG^T:

$$HG^T = [I_{n-k} \vdots P^T] \begin{bmatrix} P^T \\ \dots \\ I_k \end{bmatrix} = P^T + P^T$$

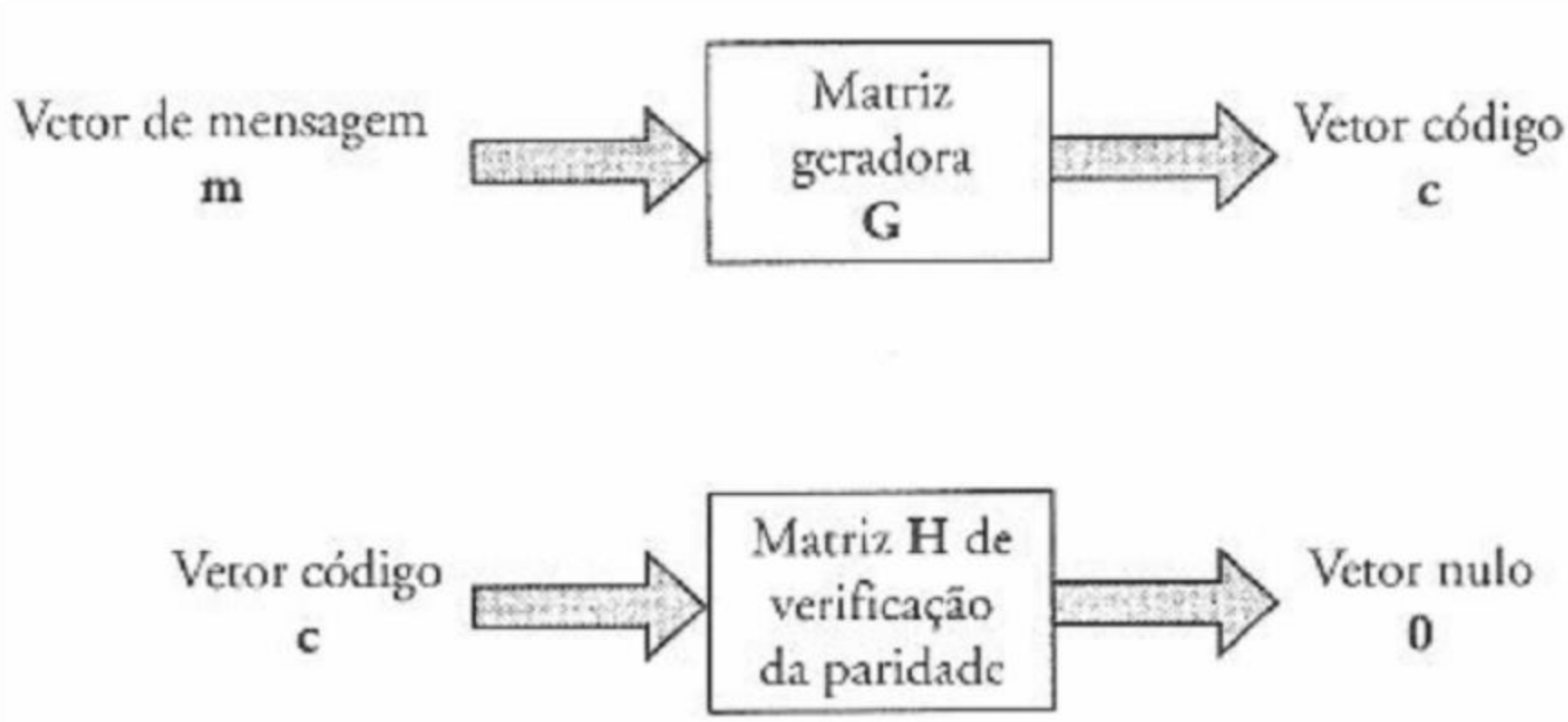
- Em binário a soma $P^T + P^T = 0$, sendo 0 nesse caso uma matriz $(n-k)$xk nula.
- Multiplicando o sinal codificado $\mathbf{c}$ sem erros pela matriz H:

$$\mathbf{c}H^T = \mathbf{m}GH^T = 0$$

- $$\mathbb{H} = [\mathbb{I}_{n-k}\mathbb{P}^T] = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & p_{00} & p_{10} & \cdots & p_{k-1,0} \\ 0 & 1 & 0 & \cdots & 0 & p_{01} & p_{11} & \cdots & p_{k-1,1} \\ 0 & 0 & 1 & \cdots & 0 & p_{02} & p_{12} & \cdots & p_{k-1,2} \\ \vdots & & & & & & & & \\ 0 & 0 & 0 & \cdots & 1 & p_{0,n-k-1} & p_{1,n-k-1} & \cdots & p_{k-1,n-k-1} \end{bmatrix}$$

- Exercício:
  - Encontre H, a partir de G do código $(7, 4)$

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


Vetor de mensagem
m
Matriz
geradora
G
Vetor código
c
Vetor código
c
Matriz H de
verificação
da paridade
Vetor nulo
0

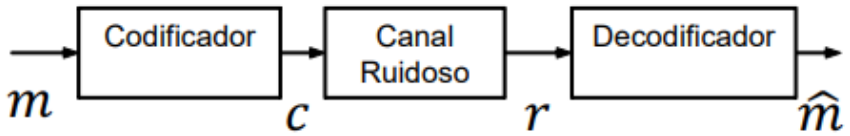
Exercício

- Encontre a matriz geradora e a matriz verificadora de paridade de um código de repetição $(n, 1)$, criando n bits idênticos para cada bit da mensagem. Faça para $n = 5$
  - $G = \left[\begin{array}{cccc:c} 1 & 1 & 1 & 1 & 1 \end{array}\right]$
  - $H = \left[\begin{array}{cccc:c} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right]$

Sumário

Síndrome

- $\mathbf{r} = \mathbf{c} + \mathbf{e}$



- O sinal recebido através de um canal com ruído é o sinal enviado mais o erro.
- Para identificar a posição em que houve um erro:

$$e_i(1 \leq i \leq n) = \begin{cases} 1 & \text{se houver erro na } i\text{-ésima posição} \\ 0 & \text{se não houver erro} \end{cases}$$

O vetor síndrome é: $\mathbf{s} = \mathbf{r} \cdot H^T = (s_0, s_1, \ldots, s_{n-k-1})$ vale zero quando não há erro

Os síndromes diferentes de zero são provindos de vários padrões de erro.

O erro mais provável é o considerado.

Propriedades da síndrome

1. A síndrome depende somente do padrão do erro, e não da palavra-código transmitida.

$$\mathbf{s} = \mathbf{r} \cdot H^T = (\mathbf{c} + \mathbf{e})H^T = \mathbf{c}H^T + \mathbf{e}H^T = \mathbf{e}H^T$$

2. A síndrome é uma combinação linear dos padrões de erro. Mas havendo 2^k mensagens da fonte, existem 2^k erros que dão a mesma síndrome.
3. Nesse caso é necessário haver um critério para identificar qual é o erro mais provável de ter ocorrido. No caso do código binário sistemático, é o padrão de erro que possua menos itens não nulos.

Exemplo de um circuito de cálculo de síndrome

- Considerando o código $(7, 4)$ utilizado no slide 9, nós criamos a matriz H^T:

$$\mathbf{s} = (s_0, s_1, s_2) = (r_0, r_1, r_2, r_3, r_4, r_5, r_6) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

- Os dígitos da síndrome são:

$$\begin{aligned} s_0 &= r_0 + r_3 + r_5 + r_6 \\ s_1 &= r_1 + r_3 + r_4 + r_5 \\ s_2 &= r_2 + r_4 + r_5 + r_6 \end{aligned}$$

Sumário

Distância de Hamming

- O *peso de Hamming* é definido como o número de elementos não nulos numa palavra código, $w(\mathbf{c})$ (*w* para *weight*).
- A *distância de Hamming* é o número de lugares onde duas palavras códigos diferem.
- A distância mínima d_{min} é a menor distância de Hamming observada entre duas palavras código diferentes dentro de um grupo do código de bloco $\mathbf{C}$.

$$d_{min} \triangleq \{d(\mathbf{c}, \mathbf{d}) : \mathbf{c}, \mathbf{d} \in \mathbf{C}, \mathbf{c} \neq \mathbf{d}\}$$

- Num código linear, a soma de duas palavras chave é outra palavra chave. Logo a distância entre duas palavras chave é o peso de uma terceira. Como qualquer palavra chave é a soma de duas outras palavras-chave, a distância mínima e o peso do código são os mesmos em um código linear.

$$\begin{aligned} d_{min} &= \{w(\mathbf{c} + \mathbf{d}) : \mathbf{c}, \mathbf{d} \in \mathbf{C}, \mathbf{c} \neq \mathbf{d}\} \\ &= \{w(\mathbf{x}) : \mathbf{x} \in \mathbf{C}, \mathbf{x} \neq 0\} \\ &\triangleq w_{min} \end{aligned}$$

Capacidade de correção de um código de bloco

- O sinal recebido $\mathbf{r}$ com erro e distância l do sinal $\mathbf{c}$ enviado.
- Como duas palavras código diferem de d_{min}, nenhum padrão de erro com com $d_{min} - 1$ ou menos erros erros muda uma palavra código em outra.
- Um código d_{min} garante detecção de erros $d_{min} - 1$.
- Existem $2^n - 1$ padrões de erro possíveis, dentro desses, $2^k - 1$ são palavras código. Portanto, existem $2^n - 2^k$ erros detectáveis , alguns contendo um peso superior a $d_{min} - 1$. Por isso existem $2^k - 1$ erros não detectáveis.

Capacidade de correção de erro e probabilidade de detecção errônea

- Considere um erro de peso t

$$2t + 1 \leq d_{min} \leq 2t + 2$$

- Se o erro tem peso t ou menos, ele será mais próximo da palavra código transmitida que qualquer outra palavra código.
- No entanto, se $l > t$ o vetor de erro será mais próximo de uma palavra código incorreta, do que a palavra código transmitida.
- O código garante correção para erros onde $t = \lfloor (d_{min} - 1)/2 \rfloor$ ou menos.
- Probabilidade de detecção errônea:

$$P(E) \leq \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

- Um código de bloco linear com distância mínima d_{min} é denotado (n, k, d_{min}).

Sumário

Arranjo padrão de decodificação de síndrome

- O arranjo padrão é uma tabela que contém todas as combinações de sinais recebidos. Ele contém a combinação de cada palavra código com cada padrão de erro.
- As palavras código possíveis são denominadas c_i, que vai de c_1 até c_{2^k}.
- Os padrões de erro denominados e_i, de e_2 até $e_{2^{n-k}}$, e_1 não é marcado é zero erro.

$\mathbf{c}_1 = \mathbf{0}$	$\mathbf{c}_2$	$\mathbf{c}_3$	$\cdots$	$\mathbf{c}_i$	$\cdots$	$\mathbf{c}_{2^k}$
$\mathbf{e}_2$	$\mathbf{c}_2 + \mathbf{e}_2$	$\mathbf{c}_3 + \mathbf{e}_2$	$\cdots$	$\mathbf{c}_i + \mathbf{e}_2$	$\cdots$	$\mathbf{c}_{2^k} + \mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{c}_2 + \mathbf{e}_3$	$\mathbf{c}_3 + \mathbf{e}_3$	$\cdots$	$\mathbf{c}_i + \mathbf{e}_3$	$\cdots$	$\mathbf{c}_{2^k} + \mathbf{e}_3$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\mathbf{e}_j$	$\mathbf{c}_2 + \mathbf{e}_j$	$\mathbf{c}_3 + \mathbf{e}_j$	$\cdots$	$\mathbf{c}_i + \mathbf{e}_j$	$\cdots$	$\mathbf{c}_{2^k} + \mathbf{e}_j$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\mathbf{e}_{2^{n-k}}$	$\mathbf{c}_2 + \mathbf{e}_{2^{n-k}}$	$\mathbf{c}_3 + \mathbf{e}_{2^{n-k}}$		$\mathbf{c}_i + \mathbf{e}_{2^{n-k}}$		$\mathbf{c}_{2^k} + \mathbf{e}_{2^{n-k}}$

- As linhas do conjunto padrão são os *conjuntos complementares*, e os primeiros elementos $e_2, ..., e_{2^{n-k}}$ são os *conjuntos complementares principais*.

- Usando um código $(6, 3)$ de matriz geradora:

$$\mathbf{G} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$ temos o seguinte arranjo padrão:

000000	011100	101010	110001	110110	101101	011011	000111
100000	111100	001010	010001	010110	001101	111011	100111
010000	001100	111010	100001	100110	111101	001011	010111
001000	010100	100010	111001	111110	100101	010011	001111
000100	011000	101110	110101	110010	101001	011111	000011
000010	011110	101000	110011	110100	101111	011001	000101
000001	011101	101011	110000	110111	101100	011010	000110
100100	111000	001110	010101	010010	001001	111111	100011

- Decodificando:
  1. Calcular a síndrome $s = r\,H^T$
  2. Dentro do *conjunto complementar* encontre o *conjunto complementar principal* que gera a síndrome. O padrão de erro com maior probabilidade de ocorrência é aquele com o menor peso. Denomine de e_0
  3. $\mathbf{c} = \mathbf{r} + e_0$

Código dual

- Com um código de bloco linear:

$$GH^T = 0$$

- O código tem matriz geradora G e matriz de verificação de paridade H, sendo um código (n, k). Existe um *código dual* com parâmetros $(n, n-k)$, com matriz geradora H e verificação de paridade G.

Sumário

Código de Hamming

- Para qualquer inteiro positivo $m \geq 3$, existe um código de Hamming com os seguintes parâmetros:

Tamanho do código	$n = 2^m - 1$
Tamanho da mensagem da fonte	$k = 2^m - m - 1$
Número de bits de paridade	$n - k = m$
Capacidade de correção de erro	t=1 ($d_{min} = 3$)

Código de Hamming

EXEMPLO

A partir da matriz geradora do código , pede-se

a) Obter uma matriz geradora na forma sistemática
b) Construir uma tabela com os vetores mensagens e seus respectivos vetores códigos.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

c) Obter a matriz verificadora de paridade H.

d) Verificar a condição de ortogonalidade para o vetor código correspondente ao vetor mensagem m = 101.

Código de Hamming

Solução

A matriz na forma sistemática, **G'** correspondente à matriz **G**, é obtida a partir das seguintes operações a partir da matriz **G**

$$\mathbf{g_0'} = \mathbf{g_1} = 101100$$
$$\mathbf{g_1'} = \mathbf{g_1} + \mathbf{g_2} = 110010$$
$$\mathbf{g_2'} = \mathbf{g_0} + \mathbf{g_1} = 011001$$

$$\mathbf{G'} = \begin{bmatrix} \mathbf{g_0'} \\ \mathbf{g_1'} \\ \mathbf{g_2'} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Código de Hamming

b) Com a matriz **G'** obtém-se os vetores

Tabela - Vetores códigos gerados a partir da matriz G'

m	**c = m.G'**	**c**
000	$\mathbf{c}_0 = 0\ (101100) + 0\ (110010) + 0\ (011001)$	**000000**
100	$\mathbf{c}_1 = 1\ (101100) + 0\ (110010) + 0\ (011001)$	**101100**
010	$\mathbf{c}_2 = 0\ (101100) + 1\ (110010) + 0\ (011001)$	**110010**
110	$\mathbf{c}_3 = 1\ (101100) + 1\ (110010) + 0\ (011001)$	**011110**
001	$\mathbf{c}_4 = 0\ (101100) + 0\ (110010) + 1\ (011001)$	**011001**
101	$\mathbf{c}_5 = 1\ (101100) + 0\ (110010) + 1\ (011001)$	**110101**
011	$\mathbf{c}_6 = 0\ (101100) + 1\ (110010) + 1\ (011001)$	**101011**
111	$\mathbf{c}_7 = 1\ (101100) + 1\ (110010) + 1\ (011001)$	**000111**

Código de Hamming

c) Obter a matriz verificadora de paridade H.

A partir da matriz geradora na forma sistemática

$$\mathbf{G}' = \left[\mathbf{P}_{k\times(n-k)} \middle| \mathbf{I}_{k\times k}\right] = \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

obtém-se a matriz **H** na forma

$$\mathbf{H} = \left[\mathbf{I}_{(n-k)\times(n-k)} \middle| \mathbf{P}^T\right] = \left[\begin{array}{cccccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right].$$

Código de Hamming

d) Verificar a condição de ortogonalidade para o vetor código correspondente ao vetor mensagem m = 101.

$$\mathbf{c} = \mathbf{m} \cdot \mathbf{G}' = (101)\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = 1\,(101100) + 0\,(110010) + 1\,(011001) = 110101$$

A condição de ortogonalidade pode ser verificada a partir do resultado do produto interno entre o vetor código, **c**, e a matriz verificadora de paridade transposta $\mathbf{H}^T$, conforme mostrado a seguir.

$$\mathbf{c} \cdot \mathbf{H}^T = (110101)\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = 1\,(100) + 1\,(010) + 0\,(001) + 1\,(101) + 0\,(110) + 1(011) = 000\,.$$

Fonte: Prof. Luís Henrique Assumpção Lolis - UFPR