Introdução aos Códigos Corretores de Erro

Bartolomeu F. Uchôa Filho, Ph.D

Grupo de Pesquisa em Comunicações – GPqCom
Departamento de Engenharia Elétrica
Universidade Federal de Santa Catarina
E-mail: uchoa@eel.ufsc.br

Introdução aos Códigos Corretores de Erro

1. Introdução
2. Decodificação de Máxima Verossimilhança
3. A Distância de Hamming
4. Códigos de Bloco Lineares
5. O Código de Hamming
6. A Matriz Geradora
7. A Matriz de Verificação de Paridade

8. A Distância Mínima de Hamming de um Código Linear

9. As Capacidades de Detecção e de Correçao de um Código

10. Detecção e Correção de Erros
    - O Conceito de Síndrome
    - O Arranjo Padrão

11. Códigos Convolucionais

12. Exemplo

13. A Representação em Treliças

14. O Algoritmo de Decodificação de Viterbi

Introdução

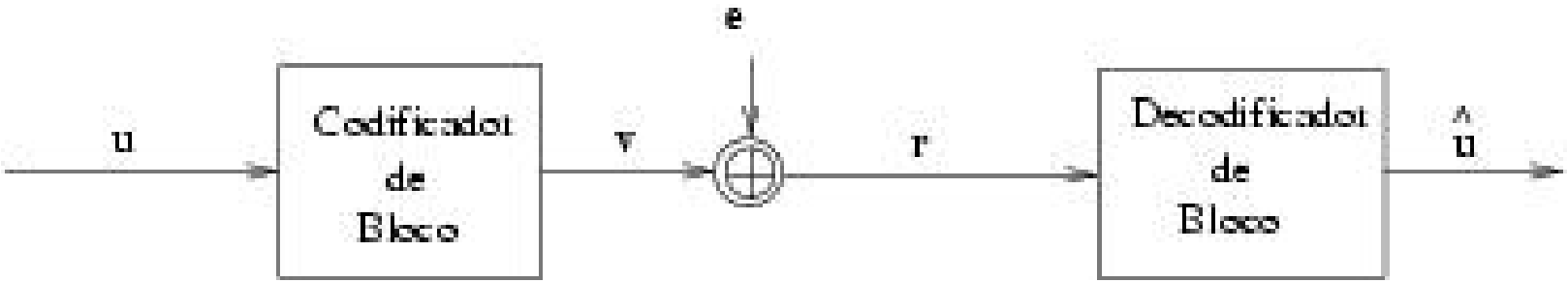


Figura 1: Sistema de comunicação binária com código de bloco.

Objetivo

OBJETIVO: O papel deste codificador é o de introduzir redundância controlada ou estruturada com o objetivo de detectar e/ou corrigir erros.

Definições Básicas

A seqüência de informação produzida pela fonte binária é subdividididade em blocos de k bits cada, que serão denotados pelo vetor $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$.

Como cada $u_i \in \{0, 1\}$, $0 \leq i \leq k-1$, existem 2^k possíveis vetores de informação.

A cada um desses vetores, o codificador de bloco associará um vetor binário $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ com n bits, onde $n > k$.

O vetor $\mathbf{v}$ será chamado de palavra-código.

Como cada vetor de informação é associado a uma única palavra-código, teremos exatamente 2^k palavras-código.

O conjunto dessas 2^k palavras-código é chamado de código de bloco.

Um código de bloco é um subconjunto do conjunto de todas os 2^n vetores binários. . .

Note que poderíamos ter 2^n possíveis vetores binários de comprimento n. Mas apenas 2^k vetores (justamente as palavras-código) são utilizados pelo codificador. Portanto, um código de bloco é nada mais que um subconjunto C do conjunto de todas os 2^n vetores binários.

O Canal BSC para a Transmissão de uma Palavra-Código

O canal que iremos considerar é o canal binário simétrico, ou BSC, que transmite 1 dígito binário por vez.

Como a palavra-código é formada por n dígitos binários, o canal BSC deverá ser usado n vezes para a transmissão de uma palavra-código.

Devemos notar se a fonte binária transmite 0's e 1's com igual probabilidade, então cada dígito binário produzido pela fonte contém 1 bit de informação.

Como o vetor de informação é formado por k dígitos binários, e a transmissão da palavra-código correspondente usa o canal n vezes, então a taxa de transmissão é

$$R = k/n$$

bits por uso do canal.

O Vetor Erro

Se transmitirmos o dígito binário $v = 1$ e houver ruído, dizemos que o sinal erro $e = 1$ foi adicionado (módulo 2) ao dígito transmitido, produzindo o dígito recebido $r = v \oplus e = 1 \oplus 1 = 0$. A operação $\oplus$ é também chamada de "ou exclusivo", ou seja, $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ e $1 \oplus 1 = 0$.

Podemos modelar o canal ruidoso pela adição de um vetor erro

$$\mathbf{e} = (e_0, e_1, \ldots, e_{n-1})$$

à palavra-código transmitida $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$.

O Vetor Recebido

Assim, o vetor recebido, que é uma versão ruidosa do vetor transmitido, é dado por

$$\begin{aligned}
\mathbf{r} &= \mathbf{v} \oplus \mathbf{e} \\
&= (v_0, v_1, \ldots, v_{n-1}) \oplus (e_0, e_1, \ldots, e_{n-1}) \\
&= (v_0 \oplus e_0, v_1 \oplus e_1, \ldots, v_{n-1} \oplus e_{n-1}) \\
&= (r_0, r_1, \ldots, r_{n-1}).
\end{aligned}$$

O Decodificação

O papel do decodificador de canal é obter uma estimativa $\hat{\mathbf{u}}$ para o vetor de informação $\mathbf{u}$, ou equivalentemente, uma estimativa $\hat{\mathbf{v}}$ para a palavra-código transmitida $\mathbf{v}$.

Exemplo: o Código de Paridade

Vamos considerar um código de bloco de taxa $R = 2/3$, ou seja, com $k = 2$ e $n = 3$. Os possíveis vetores de informação são:
u$= (0,0), (0,1), (1,0), (1,1)$.

Note que podemos ter as seguintes triplas binárias:

$$000 \;\; 001 \;\; 010 \;\; 011 \;\; 100 \;\; 101 \;\; 110 \;\; 111$$

Escolhemos as seguintes triplas para formar o código de bloco:

$$000 \;\; 011 \;\; 101 \;\; 110$$

Exemplo: o Código de Repetição

Consideremos agora um código de bloco de taxa $R = 1/5$. Os possíveis vetores de informação são: **u**=(0) e (1). Dos $2^5 = 32$ possíveis vetores binários, escolhemos os seguinte vetores para formar o código de bloco: 00000 e 11111. Por razões óbvias, este código é chamado de código de repetição

Decodificação de Máxima Verossimilhança e a Distância de Hamming

Vamos supor que $\mathbf{u}$ seja o vetor de informação e que a palavra $\mathbf{v}$ tenha sido transmitida.

O decodificador deverá estimar $\hat{\mathbf{u}}$, ou $\hat{\mathbf{v}}$, a partir da observação $\mathbf{r}$. Dizemos que um erro de palavra-código acontece quando $\hat{\mathbf{u}} \neq \mathbf{u}$ (ou $\hat{\mathbf{v}} \neq \mathbf{v}$).

Denotemos por E o evento erro de palavra-código. Assim, a probabilidade de erro de palavra-código dado que o vetor recebido foi $\mathbf{r}$ é dada por:

$$Prob\{E|\mathbf{r}\} \triangleq Prob\{\hat{\mathbf{v}} \neq \mathbf{v}|\mathbf{r}\}$$

A probabilidade de erro de palavra-código média é dada por:

$$Pr\{E\} = \sum_{\mathbf{r}} Pr\{E|\mathbf{r}\} \times P(\mathbf{r})$$

O decodificador deverá se empenhar para que a estimativa $\hat{\mathbf{v}}$ seja aquela que minimize a probabilidade condicionada de erro $Pr\{E|\mathbf{r}\}$.

Manipulando $Pr\{E|\mathbf{r}\}$

Usando a regra de Bayes, podemos reescrever a probabilidade $Pr\{\mathbf{v}|\mathbf{r}\}$ da seguinte maneira:

$$\begin{aligned} P(\mathbf{v}|\mathbf{r}) &= \frac{P(\mathbf{v},\mathbf{r})}{P(\mathbf{r})} \\ &= \frac{P(\mathbf{r}|\mathbf{v})P(\hat{\mathbf{v}})}{P(\mathbf{r})} \end{aligned} \tag{1}$$

Supondo-se que os 2^k vetores de informação $\mathbf{u}$ sejam eqüiprováveis, tem-se que as 2^k palavras-código também são eqüiprováveis: $P(\mathbf{v}) = \frac{1}{2^k}$, ou seja, $P(\mathbf{v})$ não depende de $\mathbf{v}$.

Por outro lado, $P(\mathbf{r})$ na equação (1) também não depende de $\mathbf{v}$. Assim, maximizar a equação (1) é equivalente a maximizar:

$$P(\mathbf{r}|\mathbf{v})$$

que é a função de verossimilhança.

Canal sem Memória

$$
\begin{aligned}
P(\mathbf{r}|\mathbf{v}) &= P[(r_0, r_1, \ldots, r_{n-1})|(v_0, v_1, \ldots, v_{n-1})] \\
&= \prod_{i=0}^{n-1} P(r_i|v_i)
\end{aligned}
\tag{2}
$$

Para o canal BSC temos as seguintes probabilidades condicionadas:

$$
P(r_i|v_i) = \begin{cases} 1-p & \text{para } r_i = v_i \\ p & \text{para } r_i \neq v_i \end{cases}
\tag{3}
$$

A Distância de Hamming

Para dois vetores $\mathbf{v}$ e $\mathbf{v}'$ quaisquer, definimos a distância de Hamming entre $\mathbf{v}$ e $\mathbf{v}'$ como:

$$d_H(\mathbf{v}, \mathbf{v}') = \text{ número de posições em que } \mathbf{v} \text{ e } \mathbf{v}' \text{ diferem}$$

Example Considere os vetores binários $\mathbf{v} = (1, 1, 0, 1, 0)$ e $\mathbf{v}' = (1, 0, 0, 0, 1)$. A distância de Hamming entre $\mathbf{v}$ e $\mathbf{v}'$ é $d_H(\mathbf{v}, \mathbf{v}') = 3$.

Substituições. . .

$$
\begin{aligned}
P(\mathbf{r}|\mathbf{v}) &= \prod_{i=0}^{n-1} P(r_i|v_i) \qquad (4)\\
&= p^{d_H(\mathbf{r},\mathbf{v})} \times (1-p)^{n-d_H(\mathbf{r},\mathbf{v})}\\
&= \left(\frac{p}{1-p}\right)^{d_H(\mathbf{v},\mathbf{r})} \times (1-p)^n
\end{aligned}
$$

Note que o termo $(1-p)^n$ não depende de $\mathbf{v}$. Logo, maximizar (4) é equivalente a maximizar a seguinte expressão:

$$\left(\frac{p}{1-p}\right)^{d_H(\mathbf{v},\mathbf{r})} \qquad (5)$$

Como normalmente $p < 1/2$, temos que

$$\left(\frac{p}{1-p}\right) < 1$$

e concluimos que maximizar (5) é equivalente a escolher a palavra-código $\mathbf{v}$ que minimize a distância de Hamming entre $\mathbf{v}$ e $\mathbf{r}$, ou seja, $d_H(\mathbf{v}, \mathbf{r})$.

Decodificação de Máxima Verossimilhança para Códigos de Bloco

1. Observar a saída do canal $\mathbf{r}$

2. Calcular $d_H(\mathbf{v}, \mathbf{r})$ para todas as 2^k palavras-código do código C

3. Escolher a palavra $\hat{\mathbf{v}}$ mais próxima de $\mathbf{r}$ como a estimativa da palavra-código transmitida, ou seja, escolher $\hat{\mathbf{v}} \in C$ tal que $d_H(\hat{\mathbf{v}}, \mathbf{r}) \leq d_H(\mathbf{v}, \mathbf{r})$ para qualquer $\mathbf{v} \neq \hat{\mathbf{v}} \in C$

Exemplo

Considere o código de taxa $R = 1/5$. Vamos supor que o vetor recebido seja $\mathbf{r} = (1, 0, 0, 1, 1)$. Realizando a decodificação de máxima verossimilança, devemos obter primeiramente as distâncias de Hamming

$$d_H((0,0,0,0,0),(1,0,0,1,1)) = 3 \text{ e } d_H((1,1,1,1,1),(1,0,0,1,1)) = 2.$$

Note que a palavra-código $\hat{\mathbf{v}} = (1, 1, 1, 1, 1)$ está mais próxima de $\mathbf{r}$ do que a palavra-código (0,0,0,0,0). Logo, a palavra decodificada, ou seja, dada como correta, é a palavra $\hat{\mathbf{v}} = (1, 1, 1, 1, 1)$.

Base

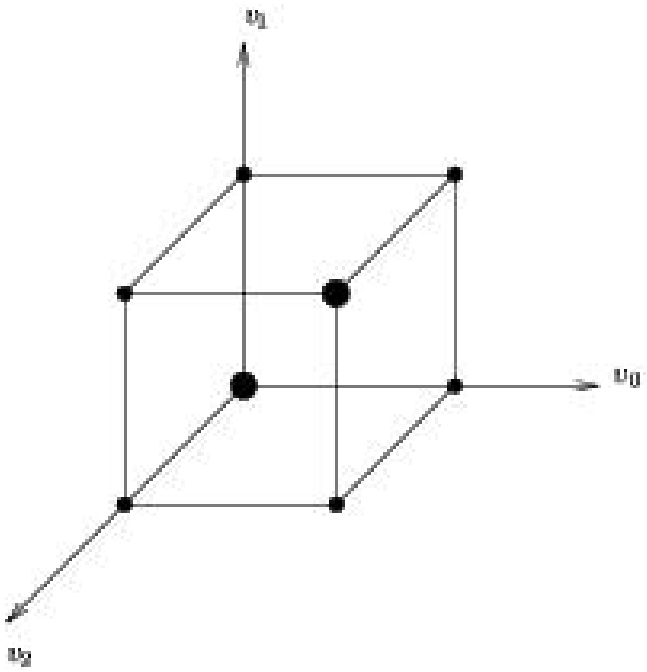


Figura 2: Espaço tridimensional contendo as 8 triplas binárias (pontos) possíveis e as 2 palavras-código (pontos grandes) do código de taxa $R = 1/3$ do exemplo anterior.

Códigos de Bloco Lineares

Um código de bloco de taxa $R = k/n$, ou seja, com 2^k palavras-código de comprimento n bits é dito ser um código **linear** se e somente se suas 2^k palavras-código formam um subespaço linear de dimensão k do espaço de todas as n-uplas binárias.

Ou seja, um código de bloco binário C é linear se e somente se para quaisquer palavras-código $\mathbf{v} \in C$ e $\mathbf{v}' \in C$ tivermos que

$$\mathbf{v} \oplus \mathbf{v}' = \mathbf{v}'' \in C$$

Exemplo

Consideremos o código de bloco de taxa $R = 2/3$ cujas palavras-código são

$$\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$$

Podemos verificar facilmente que a soma de quaisquer duas palavras-código resulta numa outra palavra-código. Por exemplo,

$$(0,1,1) \oplus (1,1,0) = (1,0,1)$$

Tabela 1: Código de Hamming de Taxa $R = 4/7$.

u	**v**
0000	0000000
1000	1101000
0100	0110100
1100	1011100
0010	1110010
1010	0011010
0110	1000110
1110	0101110
0001	1010001
1001	0111001
0101	1100101
1101	0001101
0011	0100011
1011	1001011
0111	0010111
1111	1111111

O Código de Hamming de Taxa 4/7 é Linear . . .

Para quaisquer palavras-código, digamos

$$\mathbf{v} = (1, 1, 0, 1, 0, 0, 0)$$

e

$$\mathbf{v}' = (1, 0, 1, 0, 0, 0, 1)$$

temos que a soma

$$\mathbf{v} \oplus \mathbf{v}' = (1, 1, 0, 1, 0, 0, 0) \oplus (1, 0, 1, 0, 0, 0, 1) = (0, 1, 1, 1, 0, 0, 1)$$

também é uma palavra-código.

Linearidade

Uma conseqüência da linearidade do código é que podemos sempre escolher k palavras-código linearmente independentes, formando uma base de um espaço linear k-dimensional, de tal modo que qualquer palavra código possa ser escrita como uma combinação linear das k palavras-código da base.

Exemplo

Considere o código de taxa $R = 2/3$. Se escolhermos as palavras-código $(1, 0, 1)$ e $(0, 1, 1)$ para formar a base, e considerarmos todos os possíveis valores do vetor de informação $\mathbf{u} = (u_0, u_1)$, poderemos escrever qualquer palavra-código $\mathbf{v}$ na forma:

$$\mathbf{v} = (u_0 \times (1, 0, 1)) \oplus (u_1 \times (0, 1, 1))$$

Por exemplo, para $\mathbf{u} = (u_0, u_1) = (1, 1)$, temos a palavra-código (1,1,0).

Na Forma Matricial . . .

Podemos expressar a equação acima na forma matricial. Definindo a matriz

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

escrevemos

$$\begin{aligned} \mathbf{v} &= \mathbf{u}\,\mathbf{G} \\ (v_0, v_1, v_2) &= (u_0, u_1) \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \end{aligned}$$

Assim, para $\mathbf{u} = (1, 1)$, teremos

$$\mathbf{v} = (1, 1) \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = (1, 1, 0)$$

A Matriz Geradora de um Código Linear

A matriz $\mathbf{G}$ é chamada a *matriz geradora* de um código de bloco.

Apenas os códigos de bloco lineares possuem matriz geradora.

A matriz geradora não é única. Por exemplo, se trocarmos uma linha pela outra na matriz $\mathbf{G}$ ainda geraremos o mesmo código, porém os vetores de informação serão associados às palavras-código numa ordem diferente.

Como o código C é o conjunto formado por todas as palavras-código, e não tem nenhuma relação com a ordem em que estas palavras-código são listadas, um matriz geradora equivalente, obtida por exemplo permutando-se linhas de $\mathbf{G}$, gera exatamente o mesmo código, apesar de modificar a relação entre $\mathbf{u}$ e $\mathbf{v}$.

A Matriz Geradora do Código de Hamming

Considerando agora o código de Hamming da Tabela, teremos a seguinte matriz geradora:

$$\mathbf{G} = \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{bmatrix} \tag{6}$$

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

Assim, se $\mathbf{u} = (1, 1, 0, 1)$, teremos

$$\begin{aligned}
\mathbf{v} &= \mathbf{u}\,\mathbf{G} \\
&= (1, 1, 0, 1) \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{bmatrix} \\
&= g_0 \oplus g_1 \oplus g_3 \\
&= (0, 0, 0, 1, 1, 0, 1)
\end{aligned}$$

Generalização

Em geral, para k e n quaisquer, teremos:

$$\mathbf{v} = \mathbf{u}\,\mathbf{G}$$

onde

$$\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$$
$$\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$$

e

$$\mathbf{G} = \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ g_{20} & g_{21} & g_{22} & \cdots & g_{2,n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix} \quad (7)$$

Códigos Sistemáticos

Um código de bloco linear é dito ser **sistemático** se os k bits de informação aparecem inalterados na palavra-código, ou seja, a palavra-código é escrita como:

$$\mathbf{v} = (v_0, v_1, \cdots, v_{n-k-1}, u_0, u_1, \cdots, u_{k-1})$$

A Matriz Geradora de um Código Sistemático

A matriz geradora de um código sistemático é dada por

$$\mathbf{G} = \left[\mathbf{P}_{k\times(n-k)} : \mathbf{I}_k\right]$$

onde $\mathbf{I}_k$ é a matriz identidade de ordem k. Escrevendo esta matriz na forma expandida, temos:

$$\mathbf{G} = \begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0,n-k-1} & 1 & & \\ p_{10} & p_{11} & \cdots & p_{1,n-k-1} & & 1 & \\ \vdots & \vdots & & \vdots & & & \ddots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,,n-k-1} & & & 1 \end{bmatrix} \tag{8}$$

onde os espaços vazios na matriz denotam zeros.

A Matriz Geradora do Código de Hamming na Forma Sistemática

Devemos notar que o código de Hamming de taxa 4/7 apresentado na Tabela é sistemático. Observe que as suas palavras-código são obtidas por $\mathbf{v} = \mathbf{u}\,\mathbf{G} = [u_0, u_1, u_2, u_3]\,\mathbf{G}$. Ou seja,

$$\begin{aligned} v_0 &= u_0 + u_2 + u_3 \\ v_1 &= u_0 + u_1 + u_2 \\ v_2 &= u_1 + u_2 + u_3 \\ v_3 &= u_0 \\ v_4 &= u_1 \\ v_5 &= u_2 \\ v_6 &= u_3 \end{aligned}$$

O Codificador

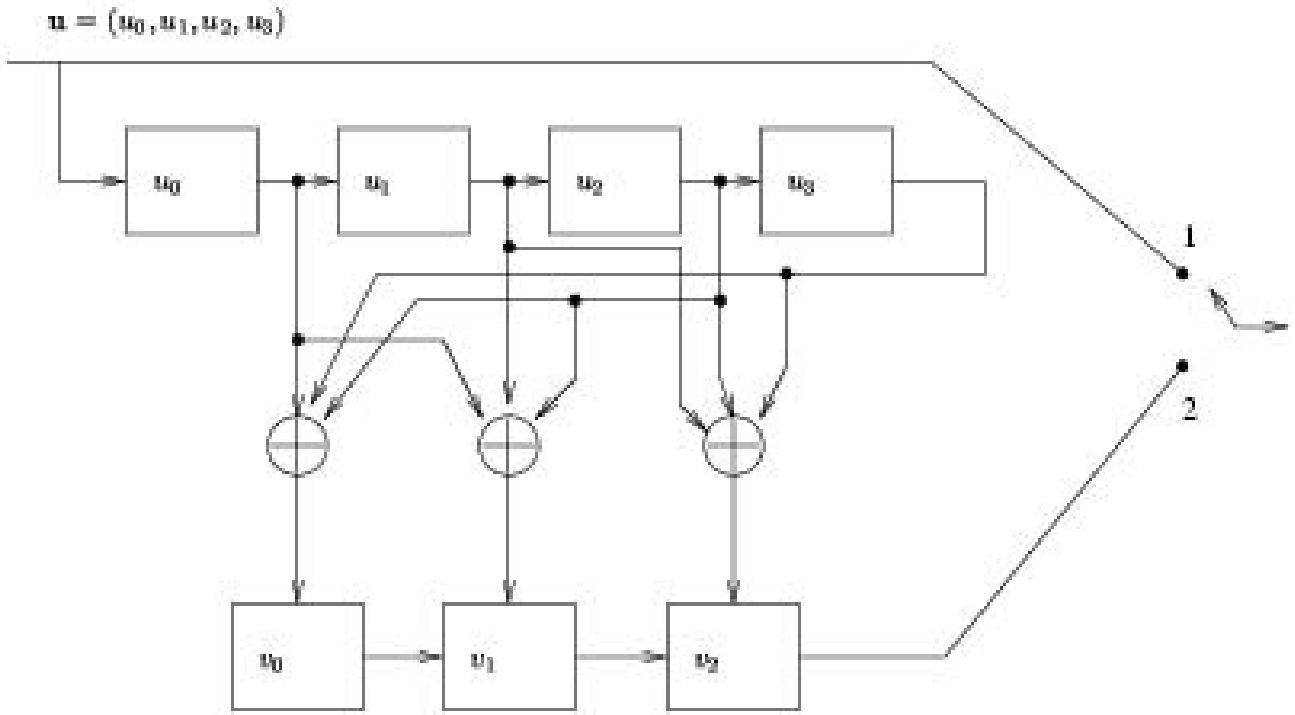


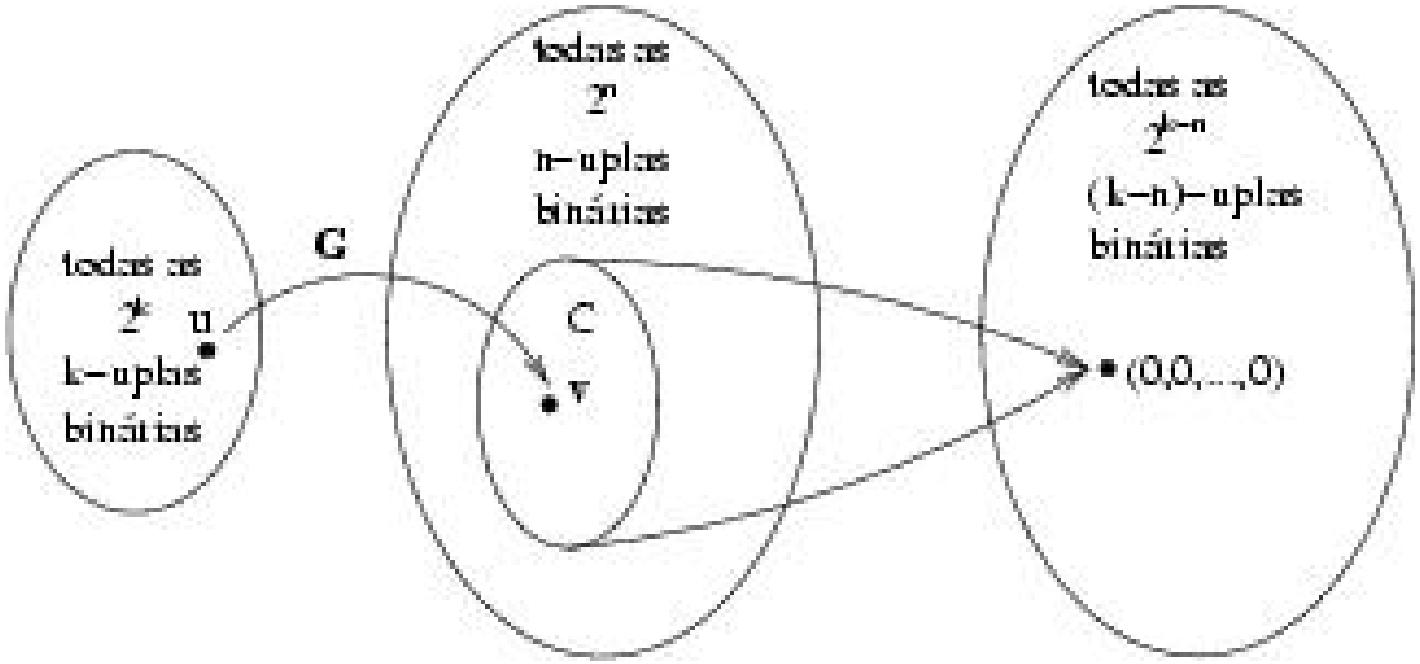
Figura 3: Codificador para o Código de Hamming Sistemático de Taxa 4/7.

A Matriz de Verificação de Paridade

Seja C o espaço (conjunto de n-uplas) formado por todas as palavras-código de um código linear de taxa $R = k/n$ com matriz geradora **G**. Da Teoria de Espaços Lineares, existe uma matriz **H** de dimensões $(n-k) \times n$ cujas linhas são linearmente independentes tal que qualquer vetor em C é ortogonal às linhas de **H**, e que qualquer vetor binário de comprimento n que é ortogonal às linhas de **H** pertence a C. Desta maneira, este código C pode também ser descrito com base na matriz **H** da seguinte maneira:

> Uma n-upla **v** é uma palavra-código do código C gerado por **G** se e somente se
>
> $$\mathbf{v}\,\mathbf{H}^T = \mathbf{0}$$
>
> onde **H** é a matriz de verificação de paridade do código.

O Efeito das Matrizes G e H de um Código de Bloco Linear



A Matriz de Verificação de Paridade na Forma Sistemática

No caso de o código de bloco linear ser sistemático, a matriz de verificação de paridade $\mathbf{H}$ terá a forma:

$$\mathbf{H} = [\mathbf{I}_{n-k} \ \mathbf{P}^T] \tag{9}$$

$$= \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & p_{00} & p_{10} & \cdots & p_{k-1,0} \\ 0 & 1 & 0 & \cdots & 0 & p_{01} & p_{11} & \cdots & p_{k-1,1} \\ 0 & 0 & 1 & \cdots & 0 & p_{02} & p_{12} & \cdots & p_{k-1,2} \\ \cdot & & & & & & & & \\ \cdot & & & & & & & & \\ \cdot & & & & & & & & \\ 0 & 0 & 0 & \cdots & 1 & p_{0,n-k-1} & p_{1,n-k-1} & \cdots & p_{k-1,n-k-1} \end{bmatrix}$$

Exemplo

Considere o código de Hamming de taxa 4/7 apresentado na Tabela. A partir de (6), reconhecemos que a matriz $\mathbf{P}$ é dada por:

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

Logo, a matriz de verificação de paridade para o código é dada por:

$$\begin{aligned} \mathbf{H} &= [\mathbf{I}_3 \ \ \mathbf{P}^T] \\ &= \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

Tomemos como exemplo a palavra-código $\mathbf{v} = (1,1,0,0,1,0,1)$. Podemos verificar que:

$$
\begin{aligned}
\mathbf{v}\,\mathbf{H}^T &= (1,1,0,0,1,0,1) \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}^T \\
&= (1,1,0,0,1,0,1) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \\
&= (0,0,0)
\end{aligned}
$$

Exemplo

Consideremos a mesma palavra-código do exemplo anterior, mas agora supondo que o vetor erro tenha sido $\mathbf{e} = (0, 0, 0, 0, 0, 0, 1)$. Ou seja, teremos o vetor recebido $\mathbf{r} = (1, 1, 0, 0, 1, 0, 0)$. Podemos verificar que:

$$\begin{aligned} \mathbf{r}\,\mathbf{H}^T &= (1,1,0,0,1,0,0) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \\ &= (1,0,1) \end{aligned}$$

O Código Dual

É importante observar que a matriz de paridade **H** tem $k' = n - k$ linhas linearmente independentes, e que cada linha de **H** tem comprimento n.

Pela definição de matriz geradora de um código linear, podemos concluir que **H** é a matriz geradora de um código linear de taxa $R' = k'/n$.

Seja C o código gerado pela matriz geradora **G** e que tem como matriz de verificação de paridade a matriz **H**. Então o código C_d, chamado de **código dual** de C, é aquele código cuja matriz geradora é **H** e que tem como matriz de verificação de paridade a matriz **G**.

Devemos notar que, para qualquer $\mathbf{v} \in C$ e qualquer $\mathbf{w} \in C_d$, temos que $\mathbf{v}\,\mathbf{w}^T = 0$.

Exemplo

Considere o código (sistemático) de repetição de taxa $R = k/n = 1/3$. A matriz geradora desse código é $\mathbf{G} = [\mathbf{P}\ \mathbf{I}_1] = [1, 1, 1]$ e a matriz de verificação de paridade é

$$\begin{aligned} \mathbf{H} &= [\mathbf{I}_2\ \mathbf{P}^T] \\ &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \end{aligned}$$

O código dual do código de repetição de taxa $R = 1/3$ é o código de taxa $R' = (n - k)/n = 2/3$ geradado pela matriz geradora

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

que é o código de verificação de paridade de taxa 2/3.

O Código Dual do Código de Repetição de Taxa $1/n$

Estendendo o resultado deste exemplo, dizemos que o código dual do código (sistemático) de repetição de taxa $R = 1/n$ é o código de verificação de paridade de taxa $R' = (n-1)/n$.

A Distância e o Peso de Hamming

Seja $d_H(\mathbf{v}, \mathbf{v}')$ a distância de Hamming entre as n-uplas $\mathbf{v}$ e $\mathbf{v}'$.

Vamos também considerar o *peso de Hamming* de uma n-upla $\mathbf{v}$, ou seja, o número de elementos (ou coordenadas) de $\mathbf{v}$ que são diferentes de zero. Denotemos por $w_H(\mathbf{v})$ o peso de Hamming de $\mathbf{v}$.

Por exemplo, dado que $\mathbf{v} = (1, 1, 0)$ temos que $w_H(\mathbf{v}) = 2$.

Propriedade: Distância versus Peso

É facil verificar que, para quaisquer n-uplas binárias $\mathbf{v}$ e $\mathbf{v}'$, temos que:

$$d_H(\mathbf{v}, \mathbf{v}') = w_H(\mathbf{v} \oplus \mathbf{v}') \tag{10}$$

Exemplo

Consideremos as duas n-uplas $\mathbf{v} = (1, 1, 0, 1, 0, 0, 1)$ e

$$\mathbf{v}' = (1, 0, 0, 0, 1, 1, 0)$$

A distância de Hamming é

$$d_H(\mathbf{v}, \mathbf{v}') = 5$$

e o peso de Hamming da soma é

$$w_H((1, 1, 0, 1, 0, 0, 1) \oplus (1, 0, 0, 0, 1, 1, 0)) = w_H((0, 1, 0, 1, 1, 1, 1)) = 5$$

Logo,

$$d_H(\mathbf{v}, \mathbf{v}') = w_H(\mathbf{v} \oplus \mathbf{v}')$$

A Distância de Hamming Mínima

A *distância de Hamming mínima* de um código de bloco linear C, denotada por $d_{\min}(C)$, ou simplesmente $d_{\min}$, é definida da seguinte maneira:

$$d_{\min} \stackrel{\Delta}{=} \min \{d_H(\mathbf{v}, \mathbf{v}') | \mathbf{v} \in C, \mathbf{v}' \in C, \mathbf{v} \neq \mathbf{v}'\} \tag{11}$$

Exemplo

Considere o código de bloco linear de taxa $R = 2/3$, cujas palavras-código são:

$$\mathbf{v}_1 = (0,0,0), \mathbf{v}_2 = (0,1,1), \mathbf{v}_3 = (1,0,1) \text{ e } \mathbf{v}_4 = (1,1,0)$$

Formando-se todos os 6 possíveis pares de palavras-código, quais sejam,

$$(\mathbf{v}_1, \mathbf{v}_2), (\mathbf{v}_1, \mathbf{v}_3), (\mathbf{v}_1, \mathbf{v}_4), (\mathbf{v}_2, \mathbf{v}_3), (\mathbf{v}_2, \mathbf{v}_4) \text{ e } (\mathbf{v}_3, \mathbf{v}_4)$$

tem-se que as respectivas distâncias de Hamming são, 2, 2, 2, 2, 2 e 2. Logo, a distância mínima deste código é $d_{\min} = 2$.

A Distância de Hamming Mínima para Códigos de Bloco Lineares

Vamos agora supor que o código em questão seja linear. Neste caso, temos que

$$d_{\min} = \min\{d_H(\mathbf{v}, \mathbf{v}') | \mathbf{v} \in C, \mathbf{v}' \in C, \mathbf{v} \neq \mathbf{v}'\} \quad (12)$$

$$= \min\{w_H(\mathbf{v}'') | \mathbf{v}'' \in C, \mathbf{v}'' \neq \mathbf{0}\} \quad (13)$$

onde a segunda igualdade segue do fato de que a soma de duas palavras-código é uma palavra-código se o código for linear.

Assim, para um código de bloco linear, **a distância de Hamming mínima é igual ao peso de Hamming mínimo de suas palavras-código não nulas**.

Exemplo

No exemplo anterior, bastaria ter verificado o peso de Hamming de todas as palavras-código não nulas, quais sejam, (0,1,1), (1,0,1) e (1,1,0). Como os pesos de Hamming são 2, 2 e 2, o peso de Hamming mínimo (ou distância de Hamming mínima) do código é 2.

Tabela 2: Código de Hamming de Taxa $R = 4/7$.

u	**v**
0000	0000000
1000	1101000
0100	0110100
1100	1011100
0010	1110010
1010	0011010
0110	1000110
1110	0101110
0001	1010001
1001	0111001
0101	1100101
1101	0001101
0011	0100011
1011	1001011
0111	0010111
1111	1111111

Exemplo: Código de Hamming de Taxa $R = 4/7$

Neste caso, como são 16 palavras-código, há $\binom{16}{2} = 120$ pares distintos de palavras-código.

Portanto, seriam necessários 120 cálculos de distância para se chegar à distância mínima.

Devido à linearidade deste código, podemos verificar facilmente que o peso mínimo de uma palavra-código não nula (há apenas 15 delas) na Tabela é 3.

Logo este código tem $w_{\min} = d_{\min} = 3$.

As capacidades de Detecção e de Correção de um Código Linear

Dado um código de bloco de taxa $R = k/n$ e cuja distância mínima é $d_{\min}$, até quantos erros de bit ele é capaz de detectar?

E quanto a correção de erros, qual a capacidade do código?

Qual a razão para se dizer que o código de taxa $2/3$ é capaz de detectar um único erro, e não tem capacidade para corrigir nenhum erro?

Por outro lado, o que nos permite afirmar que o código de Hamming é capaz de corrigir um erro de bit?

A Capacidade de Detecção

Dizemos que um código tem *capacidade de detecção* de N_D erros de bit se ele for capaz de detectar qualquer padrão de erro $\mathbf{e}$ tal que $w_H(\mathbf{e}) \leq N_D$, e houver pelo menos um padrão de erro $\mathbf{e}$ com $w_H(\mathbf{e}) = N_D + 1$ tal que o código não seja capaz de detectar.

É importante observar que detectamos a presença de erro no canal quando o vetor recebido $\mathbf{r}$ não for uma palavra-código, pois apenas palavras-código são transmitidas através do canal.

Porém, há a possibilidade de o vetor recebido $\mathbf{r}$ ser uma palavra-código, mas não ser a palavra-código transmitida.

Isso acontece se e somente se o vetor erro $\mathbf{e}$ for uma palavra-código não nula.

Note que se o vetor erro $\mathbf{e}$ for uma palavra-código não nula, então teremos que $\mathbf{r} = \mathbf{v} \oplus \mathbf{e} \neq \mathbf{v}$ também será uma palavra-código, pois o código é linear.

CONCLUSÃO: Podemos afirmar que os erros não detectáveis são aqueles vetores $\mathbf{e}$ que pertencem ao código, ou seja, que são palavras-código.

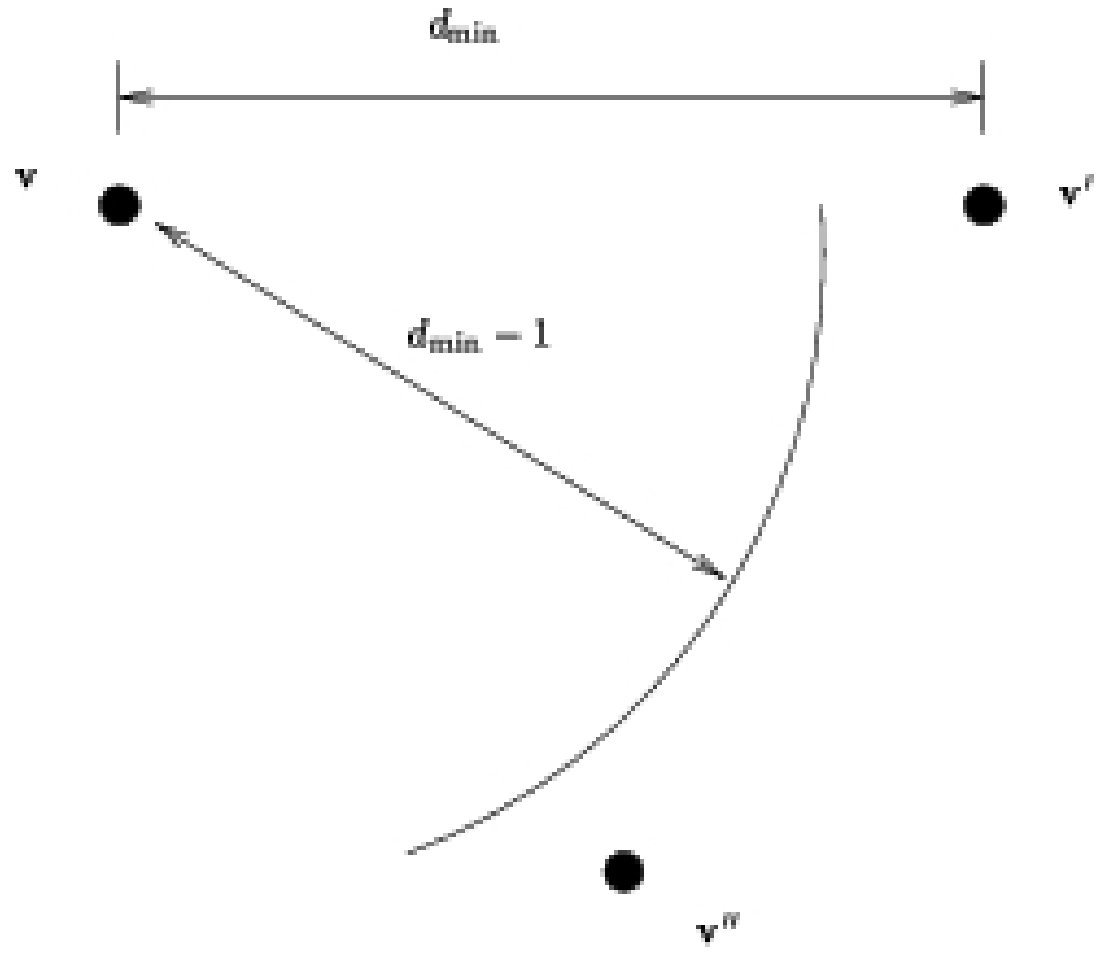


Figura 4: Espaço contendo três palavras-código de um código de bloco.

A Capacidade de Detecção

A capacidade de detecção de um código de bloco é $d_{\min} - 1$.

Por exemplo, para o código de taxa $2/3$, como $d_{\min} = 2$ temos que o código detecta até $d_{\min} - 1 = 1$ erro de bit.

A Capacidade de Correção

Dizemos que um código tem *capacidade de correção* de N_C erros de bit se ele for capaz de corrigir qualquer padrão de erro $\mathbf{e}$ tal que $w_H(\mathbf{e}) \leq N_C$, e houver pelo menos um padrão de erro $\mathbf{e}$ com $w_H(\mathbf{e}) = N_C + 1$ tal que o código não seja capaz de corrigir.

Diferente do caso da detecção, no processo de correção o decodificador tentará corrigir o(s) erro(s) quando o vetor recebido $\mathbf{r}$ não for uma palavra-código.

Porém, se o número de erros ultrapassar a capacidade de correção do código, haverá uma decodificação errônea. Estes são chamados de os padrões de erro não corrigíveis.

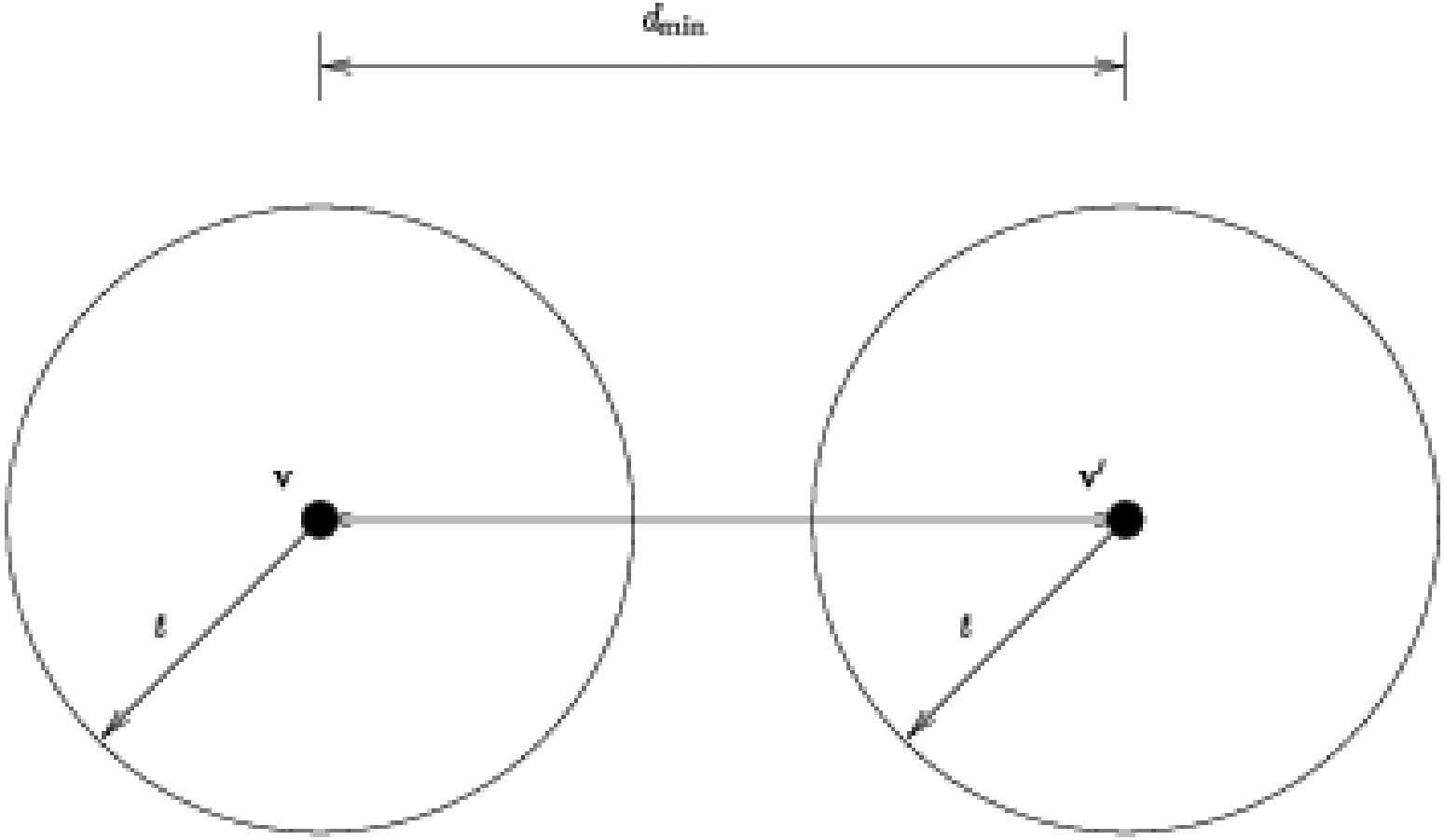


Figura 5: Espaço ilustrando a capacidade de correção de erro de um código de bloco.

A Regra de Decodificação

Vamos imaginar 2^k esferas de raio t soltas no espaço, com centros exatamente nos pontos correspondentes às palavras-código. Vamos supor que a palavra-código $\mathbf{v}$, que é o centro da esfera $E_{\mathbf{v}}$, tenha sido transmitida. O decodificador usará a seguinte regra de decodificação:

1. Se o vetor recebido $\mathbf{r}$ estiver dentro ou na superfície da esfera $E_{\mathbf{v}}$, então a palavra-código correspondendo ao centro desta esfera (ou seja, $\mathbf{v}$) será a palavra decodificada (dada como correta). Com esta regra, se o número de erros for $\leq t$, o decodificador será capaz de corrigir o(s) erro(s) com sucesso.

2. Se o vetor recebido $\mathbf{r}$ estiver dentro de uma outra esfera, digamos $E_{\mathbf{v}'}$, então a palavra decodificada será $\mathbf{v}'$, e a decodificação será errônea.

3. Se o vetor recebido **r** estiver fora de qualquer esfera, o decodificador poderá decidir-se por uma das palavras-código mais próximas, ou declarar apenas que houve erro na transmissão.

A Capacidade de Correção

Devemos notar que as esferas não podem se tocar, pois se isso acontecer, e o vetor recebido estiver neste ponto de toque, o decodificador ficaria na indecisão.

Por outro lado, quanto maior for o raio t das esferas, maior será o número de erros corrigíveis.

CONCLUSÃO: A distância entre as supefícies de duas esferas vizinhas deve ser pelo menos de 1 bit, ou seja,

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

A Capacidade de Correção

A capacidade de correção de um código de bloco é

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

onde $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x.

Por exemplo, para o código de Hamming, como $d_{\min} = 3$ temos que

$$t = \left\lfloor \frac{3 - 1}{2} \right\rfloor = 1$$

Note que, para o código de taxa $2/3$, temos $t = 0$, ou seja, aquele código não é um código corretor de erro, é apenas um código detector de erro.

Determinação da Distância Mínima via a Matriz H

Vamos supor que a palavra-código

$$\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$$

tenha peso de Hamming l, e que as l posições iguais a 1 nesta palavra sejam: $i_1, i_2, \ldots, i_l$, onde $0 \leq i_1 < i_2 < \ldots < i_l \leq n-1$.

Seja

$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-1}]$$

a matriz de verificação de paridade do código, onde $\mathbf{h}_i$ é a i-ésima coluna de $\mathbf{H}$.

Como $\mathbf{v}$ é uma palavra-código, então devemos ter:

$$
\begin{aligned}
\mathbf{v}\,\mathbf{H}^T &= 0 \\
(v_0, v_1, \ldots, v_{n-1}) \begin{bmatrix} \mathbf{h}_0^T \\ \mathbf{h}_1^T \\ \vdots \\ \mathbf{h}_{n-1}^T \end{bmatrix} &= [0, 0, \cdots, 0] \\
v_0\mathbf{h}_0^T + v_1\mathbf{h}_1^T + \cdots + v_{n-1}\mathbf{h}_{n-1}^T &= [0, 0, \cdots, 0] \\
v_{i_1}\mathbf{h}_{i_1}^T + v_{i_2}\mathbf{h}_{i_2}^T + \cdots + v_{i_l}\mathbf{h}_{i_l}^T &= [0, 0, \cdots, 0] \\
\mathbf{h}_{i_1}^T + \mathbf{h}_{i_2}^T + \cdots + \mathbf{h}_{i_l}^T &= [0, 0, \cdots, 0]
\end{aligned}
$$

Propriedade:

A partir da última equação acima podemos concluir que para cada $\mathbf{v} \in C$ de peso de Hamming l, existem l colunas de **H** cuja soma é zero, ou seja, existem l colunas de **H** que são linearmente dependentes.

Também é fácil verificar que para cada l colunas de **H** cuja soma é zero (linearmente dependentes), existe uma palavra-código **v** de peso de Hamming l cujas posições em que um 1 ocorrem coincidem com as posições destas l colunas de **H**.

Teorema

Seja C um código linear com matriz de verificação de paridade **H**. O peso mínimo (logo a distância mínima) de C é igual ao menor número de colunas de **H** cuja soma dá o vetor zero.

Exemplo

Considere o código de repetição de taxa 1/3, cujas palavras-código são: (0,0,0) e (1,1,1). A matriz geradora deste código é $\mathbf{G} = [1, 1, 1] = [\mathbf{P}\ \mathbf{I}_k]$. A matriz de verificação de paridade é

$$\mathbf{H} = [\mathbf{I}_{n-k}\ \mathbf{P}^T] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Como não há 2 colunas de **H** cuja soma é zero, e as 3 colunas de **H** somam zero, temos que $d_{\min} = 3$.

Exemplo

Considere agora o código de paridade de taxa $2/3$ cuja matriz geradora é

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

e cuja matriz de verificação de paridade é

$$\mathbf{H} = [1\ 1\ 1]$$

Como a soma de duas colunas quaisquer é zero, a distâcia mínima deste código é $d_{\min} = 2$.

Exemplo

Considere agora o código de Hamming de taxa 4/7. A matriz de verificação de paridade é

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Note que todas as colunas são não nulas, logo $d_{\min} > 1$. Também, não há duas colunas idênticas (ou seja, cuja soma seja zero), logo $d_{\min} > 2$. Porém, se escolhermos por exemplo as colunas 1, 2 e 4, teremos três colunas cuja soma é zero, logo $d_{\min} = 3$.

Construção de Códigos Ótimos: Exemplo

Vamos construir um código de bloco linear e sistemático ótimo de taxa $R = k/n = 3/6$. A matriz de verificação de paridade na forma sistemática é da forma:

$$\mathbf{H} = [\mathbf{I}_{n-k}\ \mathbf{P}^T] = \begin{bmatrix} 1 & 0 & 0 & p_{00} & p_{10} & p_{20} \\ 0 & 1 & 0 & p_{01} & p_{11} & p_{21} \\ 0 & 0 & 1 & p_{02} & p_{12} & p_{22} \end{bmatrix}$$

Note que temos 9 incógnitas, que correspondem aos elementos da matriz **P**. Portanto, há $2^9 = 512$ possíveis códigos de bloco lineares e sistemáticos de taxa $3/6$. As 3 primeiras colunas de **H** já foram escolhidas (a matriz $\mathbf{I}_{n-k}$). Devemos escolher as 3 colunas restantes. Como cada coluna tem 3 bits, temos 8 possibilidades para essas colunas. Obviamente, dentre essas 8 possibilidades devemos desconsiderar a coluna zero, pois caso contrário teríamos **uma** coluna "cuja soma" é zero, e ficaríamos com $d_{\min} = 1$. Também devemos eliminar as colunas que já foram utilizadas (ou seja, as colunas da matriz $\mathbf{I}_{n-k}$, caso contrário, com duas colunas idênticas, ficaríamos restritos a $d_{\min} = 2$.

Assim, devemos preencher as 3 colunas da direita de **H** a partir da seguinte lista de colunas:

$$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Agora devemos notar que como cada coluna de **H** é um vetor tridimensional, é impossível neste caso encontrarmos 4 colunas de **H** que sejam linearmente independentes. Logo, uma boa escolha seria:

$$\mathbf{H} = [\mathbf{I}_{n-k}\ \mathbf{P}^T] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

e teremos $d_{\min} = 3$, pois somando-se as colunas 2, 3, e 6, por exemplo, obtemos a coluna zero.

O limitante de Singleton

Devemos observar que preenchendo a parte esquerda da matriz **H** com a matriz $\mathbf{I}_{n-k}$, estamos inicialmente selecionando $n-k$ colunas linearmente independentes de **H**, e com isso há a esperança de encontrarmos um código com $d_{\min} > n-k$. Mas não é possível incluirmos mais uma coluna e termos $n-k+1$ colunas linearmente independentes, pois as colunas de **H** são vetores de dimensão $(n-k)$, e no espaço $(n-k)$-dimensional não há $n-k+1$ vetores linearmente independentes. Assim, ficamos com o seguinte limitante superior para $d_{\min}$.

Teorema: O limitante de Singleton

Para um código de bloco linear de taxa $R = k/n$, temos que

$$d_{\min} \leq n - k + 1$$

que é o limitante de Singleton.

No exemplo anterior, temos que $d_{\min} \leq 6 - 3 + 1 = 4$. O melhor código de bloco de taxa $3/6$ tem $d_{\min} = 3 < 4$.

Detecção e Correção de Erros: Os Conceitos de Síndrome e Arranjo Padrão

A *síndrome* de um vetor recebido **r** é definida como o vetor:

$$\mathbf{s} \stackrel{\Delta}{=} \mathbf{r}\,\mathbf{H}^T = [s_0, s_1, \ldots, s_{n-k-1}]$$

Obviamente,

Se $\mathbf{r} \in C$, então $\mathbf{s} = [0, 0, \ldots, 0]$

Se $\mathbf{r} \notin C$, então $\mathbf{s} \neq [0, 0, \ldots, 0]$

A Síndrome Não Dependende de v

Vamos supor que a palavra-código **v** tenha sido transmitida e que o vetor erro tenha sido **e**. Assim, o vetor recebido será

$$\mathbf{r} = \mathbf{v} \oplus \mathbf{e}$$

e a síndrome será dada por

$$\begin{aligned} \mathbf{s} &= \mathbf{r}\,\mathbf{H}^T \\ &= (\mathbf{v} \oplus \mathbf{e})\,\mathbf{H}^T \\ &= \mathbf{v}\,\mathbf{H}^T \oplus \mathbf{e}\,\mathbf{H}^T \\ &= \mathbf{e}\,\mathbf{H}^T \end{aligned}$$

Exemplo

Vamos considerar o código de Hamming de taxa 4/7, cuja matriz de verificação de paridade é:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Seja $\mathbf{r} = (r_0, r_1, \ldots, r_6)$ o vetor recebido. Então, a síndrome

$\mathbf{s} = (s_0, s_1, s_2)$ será:

$$
\begin{aligned}
\mathbf{s} &= (s_0, s_1, s_2) \\
&= \mathbf{r}\,\mathbf{H}^T \\
&= (r_0, r_1, \ldots, r_6) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}
\end{aligned}
$$

Assim, obtemos o seguinte sistema de equações:

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

Das equações, podemos facilmente construir um circuito de cálculo de síndrome e de detecção de erro para o código de Hamming de taxa 4/7.

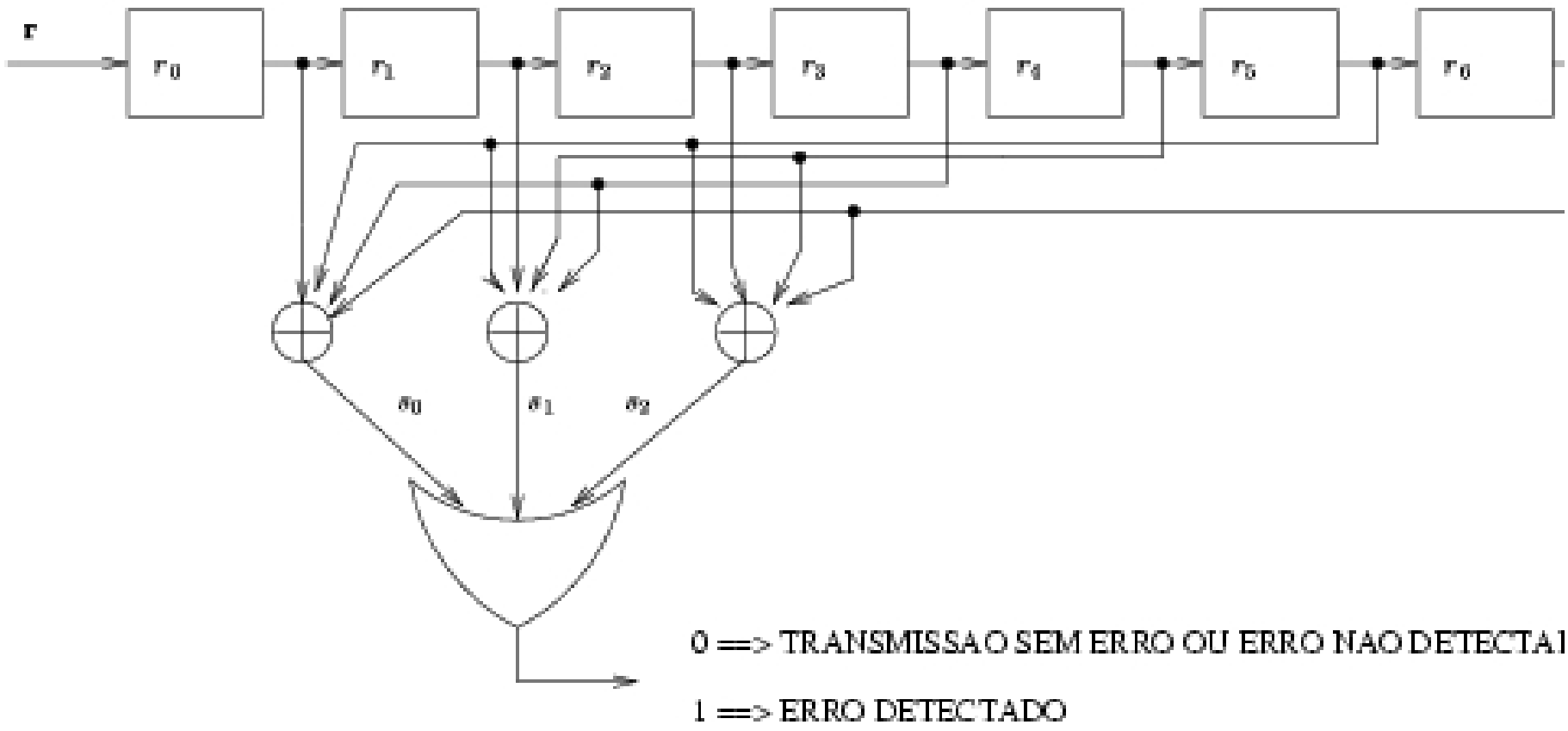


Figura 6: Circuito de cálculo de síndrome e de detecção de erros para o código de Hamming de taxa 4/7.

Correção de Erros

Seja C um código de bloco linear de taxa $R = k/n$ e sejam

$$\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^k}$$

as suas palavras-código.

Sabemos que independentemente da palavra-código transmitida, devido ao ruído o vetor recebido **r** pode ser qualquer n-upla binária.

Um esquema de decodificação (correção) de erro é uma regra para particionar o conjunto de todos os 2^n possíveis vetores recebidos em 2^k subconuntos disjuntos $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_{2^k}$, tal que a palavra-código $\mathbf{v}_i$ e mais nenhuma outra palavra-código pertença ao subconjunto $\mathbf{E}_i$, para $1 \leq i \leq 2^k$. Assim, cada subconjunto estará associado a uma única

palavra-código, e se o vetor recebido estiver no subconjunto $\mathbf{E}_i$, então a palavra-código decodificada (dada como correta) será $\mathbf{v}_i$.

Arranjo Padrão

$$
\begin{array}{lccccc}
\mathbf{v}_1 = \mathbf{0} & \mathbf{v}_2 & \cdots & \mathbf{v}_i & \cdots & \mathbf{v}_{2^k} \\
\mathbf{e}_2 & \mathbf{e}_2 + \mathbf{v}_2 & \cdots & \mathbf{e}_2 + \mathbf{v}_i & \cdots & \mathbf{e}_2 + \mathbf{v}_{2^k} \\
\mathbf{e}_3 & \mathbf{e}_3 + \mathbf{v}_2 & \cdots & \mathbf{e}_3 + \mathbf{v}_i & \cdots & \mathbf{e}_3 + \mathbf{v}_{2^k} \\
\vdots & & & & & \vdots \\
\mathbf{e}_l & \mathbf{e}_l + \mathbf{v}_2 & \cdots & \mathbf{e}_l + \mathbf{v}_i & \cdots & \mathbf{e}_l + \mathbf{v}_{2^k} \\
\vdots & & & & & \vdots \\
\mathbf{e}_{2^{n-k}} & \mathbf{e}_{2^{n-k}} + \mathbf{v}_2 & \cdots & \mathbf{e}_{2^{n-k}} + \mathbf{v}_i & \cdots & \mathbf{e}_{2^{n-k}} + \mathbf{v}_{2^k}
\end{array}
$$

Exemplo

Considere o código de taxa 3/6 projetado no na seção anterior, cuja matriz geradora é:

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

Tabela 3: Arranjo padrão para o código de taxa 3/6.

líderes							
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

Exemplo

Vamos supor que o vetor recebido seja $\mathbf{r} = (1, 1, 1, 0, 0, 1)$, que situa-se na quarta linha e na quarta coluna. O resultado da decodificação deve ser então que o vetor erro foi $\mathbf{e} = (0, 0, 1, 0, 0, 0)$, que é o líder do coset referente à quarta linha, e a palavra-código decodificada é $\hat{\mathbf{v}} = (1, 1, 0, 0, 0, 1)$. Se o erro tiver sido de fato $\mathbf{e} = (0, 0, 1, 0, 0, 0)$, então a decodificação estará correta, e o único erro ocorrido no terceiro bit (da esquerda para a direita) terá sido corrigido.

Esolher os líderes de coset de menor peso de Hamming

Para n transmissões pelo canal BSC com probabilidade de transição $p < 1/2$, os erros mais prováveis são os de menor peso de Hamming, pois a probabilidade de haver w erros em n transmissões pelo canal BSC é igual a $p^w(1-p)^{n-w}$. Quanto menor o número de erros w, maior será a probabilidade.

Decodificação por Síndrome

Step 1. Calcule a síndrome do vetor recebido $\mathbf{r}$, $\mathbf{r}\,\mathbf{H}^T$.

Step 2. Localize o líder de coset $\mathbf{e}_l$ cuja síndrome é igual a $\mathbf{r}\,\mathbf{H}^T$. Então $\mathbf{e}_l$ é tomado como o padrão de erro causado pelo canal.

Step 3. Decodifique o vetor recebido $\mathbf{r}$ pela palavra-código $\hat{\mathbf{v}} = \mathbf{r} \oplus \mathbf{e}_l$.

Exemplo

Vamos considerar mais uma vez o código de Hamming de taxa 4/7 mostrado na Tabela 1.

Teremos $2^{n-k} = 2^3 = 8$ líderes de coset para escolher.

Para minimizar a probabilidade de erro, escolheremos os líderes como sendo os padrões de erro mais prováveis, ou seja, o vetor todo zero e todos os 7 vetores (de comprimento 7) de peso de Hamming igual 1.

Tabela 4: Tabela de decodificação para o código de Hamming da Tabela 1.

Síndrome	Líderes de coset
(s_0, s_1, s_2)	$(e_0, e_1, e_2, e_3, e_4, e_5, e_6)$
(1,0,0)	(1,0,0,0,0,0,0)
(0,1,0)	(0,1,0,0,0,0,0)
(0,0,1)	(0,0,1,0,0,0,0)
(1,1,0)	(0,0,0,1,0,0,0)
(0,1,1)	(0,0,0,0,1,0,0)
(1,1,1)	(0,0,0,0,0,1,0)
(1,0,1)	(0,0,0,0,0,0,1)

Suponha que o vetor $\mathbf{v} = (1, 0, 0, 1, 0, 1, 1)$ seja a palavra-código transmitida e $\mathbf{r} = (1, 0, 0, 1, 1, 1, 1)$ seja o vetor recebido. Para decodificar **r**, nós computamos a síndrome de **r**,

$$\mathbf{s} = (1, 0, 0, 1, 1, 1, 1) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = (0, 1, 1)$$

A partir da Tabela, temos que (0,1,1) é à síndrome do líder de coset $\mathbf{e} = (0, 0, 0, 0, 1, 0, 0)$. Logo, o resultado da decodificação será:

$$\begin{aligned} \hat{\mathbf{v}} &= \mathbf{r} \oplus \mathbf{e} \\ &= (1, 0, 0, 1, 1, 1, 1) \oplus (0, 0, 0, 0, 1, 0, 0) \\ &= (1, 0, 0, 1, 0, 1, 1) \end{aligned}$$

que de fato foi a palavra-código transmitida.

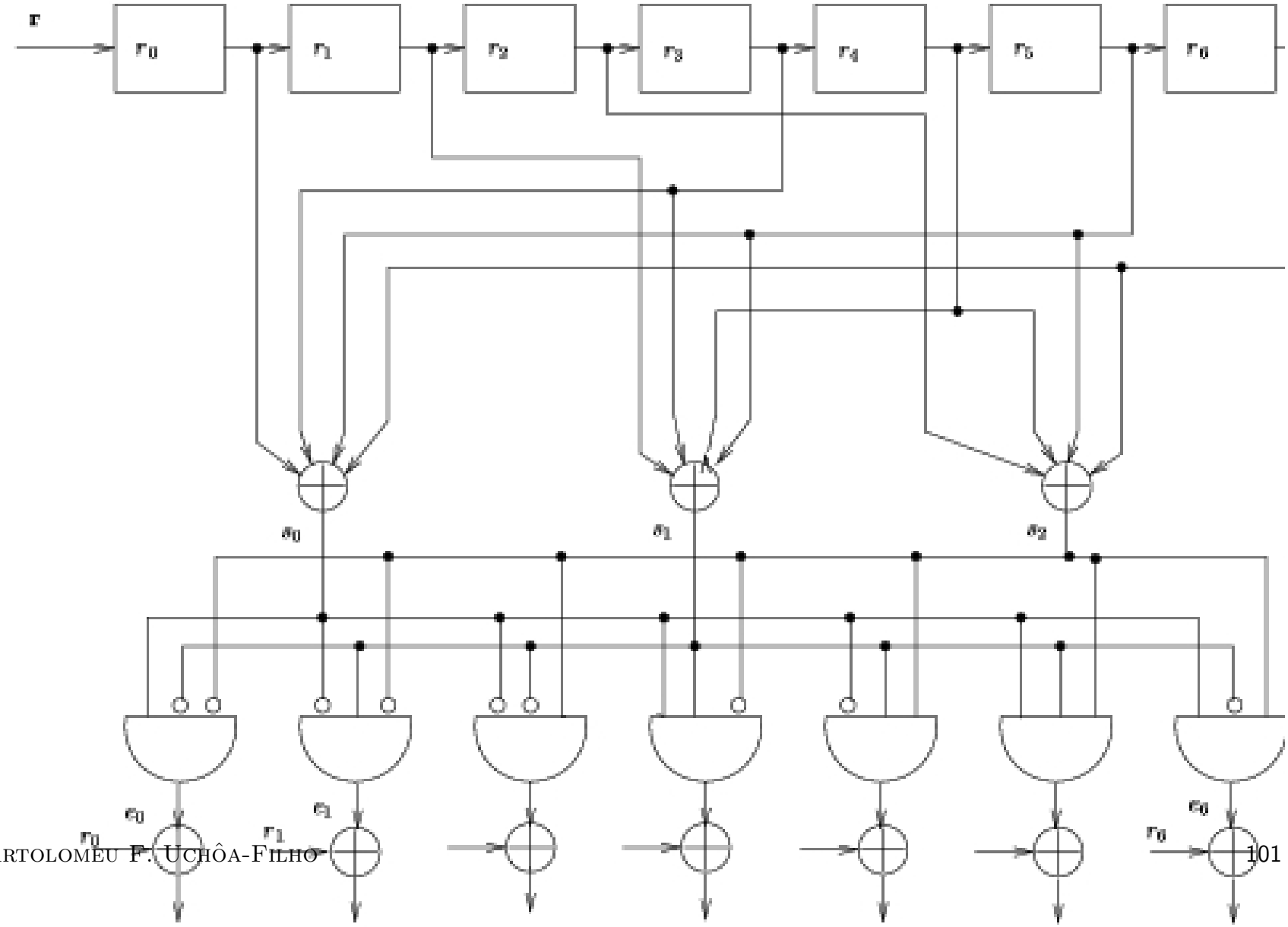
Códigos Perfeitos

O código de taxa $3/6$ tem $d_{\min} = 3$, logo corrige todos os padrões de erro de peso $t = 1$, e eventualmente algum (ou alguns) padrão (ou padrões) de peso maior que 1. De fato, a partir da Tabela, vimos que esta escolha de arranjo padrão permite corrigir 2 erros caso o padrão de erro seja especificamente $\mathbf{e} = (1, 0, 0, 1, 0, 0)$. Mas não garantimos a correção de todos os padrões de erro de peso 2.

Devemos notar que a mesma sorte não ocorre com o código de Hamming. Pelo fato de o código de Hamming ser um código capaz de corrigir todos os padrões de erro de peso até t, e mais nenhum outro padrão de erro, ele é dito ser um código **perfeito**.

Circuito de decodificação para o código de Hamming de taxa 4/7.

Como a síndrome de $\mathbf{r} = \mathbf{v} + \mathbf{e}$ é igual à síndrome de $\mathbf{e}$, a partir da Tabela, e seguindo o algoritmo da Decodificação por Síndrome apresentado acima, podemos facilmente construir um circuito lógico para o decodificador para o código de Hamming de taxa 4/7, que é capaz de corrigir qualquer padrão de 1 erro de bit.


r
r_0
r_1
r_2
r_3
r_4
r_5
r_6
s_0
s_1
s_2
e_0
e_1
e_0
r_0
r_1
r_0