

UNIVERSIDADE FEDERAL DE SANTA CATARINA

C Ó D I G O S   L I N E A R E S

NOME: DARIO NOLLI

ORIENTADOR: PROF. GUR DIAL, Ph. D.

DATA: FLORIANÓPOLIS, 08 DE AGOSTO DE 1985

C Ó D I G O S   L I N E A R E S

por

D A R I O   N O L L I

Esta dissertação foi julgada adequada para a obtenção do título de

" M E S T R E   E M   C I Ê N C I A S "

especialidade em Matemática e aprovada em sua forma final pelo curso de pós-graduação em Matemática da Universidade Federal de Santa Catarina.



---

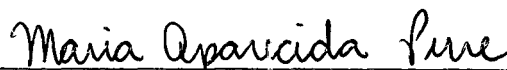
Prof. William Glenn Whitley, Ph. D.  
Coordenador

Banca Examinadora:



---

Prof. Guir Dial, Ph. D.  
Orientador



---

Profª Maria Aparecida Perre, Dra.



---

Prof. Adalberto Luiz Verani Depizolatti, Dr.

## A G R A D E C I M E N T O S

A meus pais, Pedro e Olímpia, pela vida e formação.

A minha esposa Dilma, pelo apoio, incentivo e dedicação.

Ao Professor Gur Dial, pela orientação e paciência na realização deste trabalho.

Aos colegas de curso, pela amizade e apoio.

Ao Jânio Pedro e Osvaldina, pelo trabalho de correção da linguagem e datilografia.

Aos funcionários Aldo, Nilda e Jussara, que de alguma forma deram sua colaboração.

A minha esposa Dilma

## R E S U M O

Este trabalho, trata de um estudo dos códigos lineares corretores de erros aleatórios e pedaços de erro.

No primeiro capítulo estão introduzidos os conceitos fundamentais sobre os códigos lineares corretores de erro aleatório.

O segundo e o terceiro capítulo tratam do estudo dos códigos lineares corretores e detectores de pedaços de erro, com a restrição de pêso, tanto ao código quanto ao pedaço. É apresentada ainda a construção de alguns destes códigos.

## A B S T R A C T

This work deals with a study of linear correcting codes for random and burst errors.

In the first chapter the fundamental concepts about linear correcting codes for random errors are introduced.

The second and third chapter deal with the study of linear detecting and correcting codes for burst errors with weight constraint on the code as well as on the burst. Some codes of these type are constructed.

# Í N D I C E

Pag.

## 1 - CONCEITOS RELEVANTES SOBRE CÓDIGOS LINEARES

1.1 - Introdução	1
1.2 - Matriz Geratriz	8
1.3 - Matriz de Verificação de Paridade	13
1.4 - Propriedades de um Código Linear	19
1.5 - Arranjo Padrão	21
1.6 - Síndrome e suas Propriedades	25
1.7 - Limite sobre a Distância Mínima para Códigos	29

## 2 - ESTUDO DOS CÓDIGOS LINEARES CORRETORES DE PEDAÇOS DE ERRO

2.1 - Códigos Corretores de Pedacos de Erro	42
2.2 - Resultados sobre o Pêso dos Pedacos	50
2.3 - Limites sobre o Pêso Mínimo dos Pedacos	59
2.4 - Funções Geratrizes de $W_b$ e $W_b^T$	62

## 3 - ESTUDO DOS CÓDIGOS LINEARES CORRETORES DE PEDAÇOS DE ERROS COM CRITÉRIO PÊSO

3.1 - Limite de Varsharmov-Gilbert Extendido	68
3.2 - Códigos Detectores de Pedacos de Erro	74
3.3 - Códigos com Pêso Mínimo Corretores de Pedacos de Erro	78
3.4 - Códigos Corretores de Pedacos de Erros e Erros Aleatórios	82

CONCLUSÃO	88
-----------	----

BIBLIOGRAFIA	89
--------------	----

## CAPÍTULO I

### CONCEITOS RELEVANTES SOBRE CÓDIGOS LINEARES

#### 1.1 - INTRODUÇÃO

Nas últimas três décadas a busca de eficientes e confiáveis sistemas de transmissão de dados digitais tem sido acelerada pelo uso crescente de processos automáticos de dados e a necessidade crescente para a comunicação de longo alcance.

Um dos sérios problemas em qualquer sistema de transmissão de dados é a ocorrência de erros. O problema de como controlar esses erros é de uma importância básica e os códigos foram inventados para correção desses erros.

Na literatura da teoria de codificação vários tipos de códigos tem sido inventados, tais como, códigos lineares, não lineares e convolucionais.

#### OBSERVAÇÕES:

- 1) Em nosso estudo nos ateremos apenas aos códigos lineares.
- 2) Os códigos lineares são importantes para aplicações práticas.

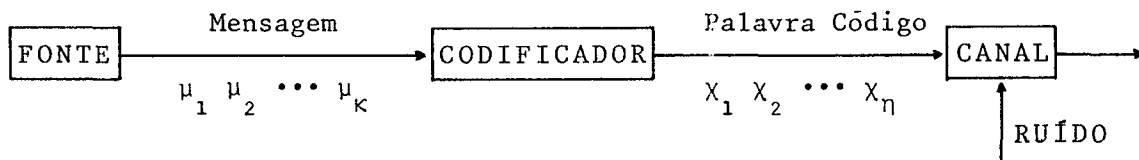


ticas e de fácil compreensão porque tem estrutura matemática.

Na maioria dos sistemas de comunicação de dados digitais, a informação é usualmente composta na forma binária, isto é, o canal utiliza dígitos binários, "0" ou "1", ou na forma decimal, ou ainda alguma forma de informação alfabética.

De um modo geral, consideramos  $q$  como sendo o número de dígitos (ou símbolos) distintos e arbitrários empregados num canal.

Consideremos a seguinte figura:



A **Fonte**, que pode ser uma pessoa ou uma máquina, produz as mensagens.

O **Codificador** transforma estas mensagens (informações) em palavras que vão ser transmitidas.

O **Canal** é o meio pelo qual as palavras são transmitidas.

O processo de codificação consiste de duas etapas básicas:

- (1) A sequência de informações é segmentada em blocos mensagens, cada bloco consistindo de  $k$  dígitos sucessivos de informação;
- (2) O codificador de acordo com certas regras, transforma um bloco mensagem em um bloco de  $n$  ( $n \geq k$ ) dígitos (uma  $n$ -upla) que o denominamos uma palavra código.

Como cada bloco mensagem consiste de  $k$  dígitos, teremos  $q^k$  possíveis blocos distintos, conseqüentemente teremos  $q^k$  possíveis palavras código, produzidas pelo codificador, correspondentes aos  $q^k$  possíveis blocos mensagem.

Ao conjunto de  $q^k$  palavras código é que denominamos de um bloco código, ou simplesmente código.

### Definição 1.1.1

Um bloco código é um conjunto de  $q^k$  sequências de símbolos utilizados no canal, cada uma das quais de comprimento  $n$ .

## OBSERVAÇÕES:

- 1) Frequentemente uma palavra código é também chamada um vetor código, porque esta é uma  $n$ -upla do espaço vetorial,  $V_n$ , de todas as  $n$ -uplas tomadas sobre um corpo de  $q$  elementos.
- 2) Em nosso estudo sempre que nos referimos a um corpo, subentende-se um corpo finito de  $q$  elementos e assim,  $q$  será primo ou uma potência de um primo.
- 3)  $GF(q)$  denotará um corpo de Galois com  $q$  elementos.

Vamos considerar códigos cuja estrutura é tal que, os  $q^k$  vetores códigos formam um subespaço vetorial  $k$ -dimensional de todas as  $n$ -uplas.

### Definição 1.1.2

O conjunto de todos os  $q^k$  vetores de comprimento  $n$  ( $n$ -uplas) é dito um **Código Linear** se, e somente se ele é um subespaço do espaço vetorial  $V_n$  de todas as  $n$ -uplas.

### Notação:

Denotaremos por  $[n,k]$  o código linear de comprimento  $n$  com  $k$  dígitos de informação ( $k$  é também dito dimensão do código) e  $n-k$  dígitos de verificação.

### Exemplo 1.1.1

Código Binário  $[5,3]$  em que o codificador transforma uma sequência de três dígitos em vetores código de cinco dígitos, assim:

Mensagem	Codificador	Vetor Código
000	←————→	00000
100	←————→	10011
010	←————→	01010
001	←————→	00101
110	←————→	11001
101	←————→	10110
011	←————→	01111
111	←————→	11100

Neste caso, há  $2^3 = 8$  mensagens distintas, portanto, 8 vetores código distintos. Cada mensagem é transformada pelo codificador em um vetor código de cinco dígitos.

OBSERVAÇÃO:

Podemos notar que o conjunto de vetores código forma um subespaço 3-dimensional do espaço vetorial de todas as 5-uplas. Portanto, é um código linear.

Definição 1.1.3

O **Pêso de Hamming** de um vetor  $x$ , denotado por  $W(x)$ , é definido como o número de componentes não nulas de  $x$ .

Exemplo 1.1.2

a)  $q = 2$ . Seja  $x = (10011101)$ , então,  $W(x) = 5$ .

b)  $q = 3$ . Seja  $x = (121201001)$ , então,  $W(x) = 6$ .

Definição 1.1.4

A **Distância de Hamming** entre dois vetores  $u$  e  $v$ , denotada por  $d(u,v)$ , é definida como o número de componentes em que eles diferem.

Exemplo 1.1.3

$q = 2$ . Sejam  $u = (100101100)$  e  $v = (110010101)$ , então,  $d(u,v) = 5$ .

OBSERVAÇÃO:

Seja  $q = 2$ , a distância entre dois vetores código  $u$  e  $v$  de um código linear é igual ao pêso de seu vetor soma  $u + v$ , isto é,  $d(u,v) = W(u + v)$ .

De fato, fazendo uma indução sobre  $n$  teremos: se  $n = 1$ , então,  $u = 0$  e  $v = 1$  e  $d(u,v) = W(u + v) = 1$ .

Supondo válido para um determinado  $n$ , isto é

$d(u,v) = W(u + v) = n$  , vamos provar para um  $n + 1$  .

Sejam  $u = u_1 u_2 \dots u_n z_1$  e  $v = v_1 v_2 \dots v_n z_2$  , temos então, duas possibilidades:

1ª) Se  $z_1 = z_2$  , não há o que provar, isto é,

$$d(u,v) = W(u + v) = n .$$

2ª) Se  $z_1 \neq z_2$  , então,  $d(u,v) = n + 1$  e como

$$u + v = u_1 + v_1, \dots, z_1 + z_2, \text{ onde } z_1 + z_2 \neq 0, \text{ temos que } W(u + v) = n + 1, \text{ logo } d(u,v) = W(u + v) = n + 1 .$$

Portanto,

$$d(u, v) = W(u + v) .$$

#### Exemplo 1.1.4

Consideremos os vetores  $u$  e  $v$  do Exemplo 1.1.3 .

$$u + v = (010111001)$$

$$W(u + v) = 5 = d(u,v)$$

Dado um código linear, podemos calcular a distância entre todos os pares de vetores código, a menor destas distâncias é denominada **Distância Mínima do Código** e é denotada por,  $d_{\min}$ , ou simplesmente  $d$  .

Se  $u$  e  $v$  são dois vetores código de um código linear, então,  $u - v$  também é um vetor código. Portanto, por definição, a distância entre quaisquer dois vetores código é igual ao peso de um terceiro vetor código. Assim, a distância mínima de um código linear é igual ao peso mínimo de seus vetores código não nulos.

#### OBSERVAÇÕES:

- 1) A noção de distância mínima ou peso mínimo é importante na análise da capacidade de correção de erro de um código linear.
- 2) Um código linear de comprimento  $n$  , dimensão  $k$  e distância mínima  $d$  será denotada por  $[n,k,d]$  .

#### Exemplo 1.1.5

Continuação do Exemplo 1.1.1 .

O p̄eso m̄inimo ẽ 2 e, portanto, a dist̄ancia m̄inima  $d = 2$ .

Alẽm dessa definiç̄ao de p̄eso e dist̄ancia de Hamming existe outra definiç̄ao que ẽ devida a Lee.

### Definiç̄ao 1.1.5

O **P̄eso de Lee** de uma  $n$ -upla  $(a_{n-1}, \dots, a_1, a_0)$ ,  $a_i$  esco-  
lhida do conjunto  $\{0, 1, 2, \dots, q - 1\}$ , onde  $q$  ẽ um inteiro  
positivo arbitr̄ario, ẽ definido como

$$W_L = \sum_{i=0}^{n-1} |a_i|$$

onde

$$|a_i| = \begin{cases} a_i, & 0 \leq a_i \leq \frac{q}{2} \\ q - a_i, & \frac{q}{2} < a_i \leq q - 1 \end{cases}$$

### Exemplo 1.1.6

Seja  $q = 5$  e  $n = 6$ , a 6-upla (013424).

$$\begin{aligned} \text{Entãõ, } W_L &= \sum_{i=0}^5 |a_i| \quad \text{onde } |a_i| = a_i, \quad 0 \leq a_i \leq \frac{5}{2} \\ &= 5 - a_i, \quad \frac{5}{2} < a_i \leq 4 \end{aligned}$$

$$W_L = 0 + 1 + 2 + 1 + 2 + 1 = 7$$

### Definiç̄ao 1.1.6

A **Dist̄ancia de Lee** entre duas  $n$ -uplas ẽ definida como o p̄e-  
so de Lee de sua diferenç̄a.

### Exemplo 1.1.7

Seja  $q = 5$ ,  $n = 6$  e as 6-uplas  $u = (400234)$  e  $v = (104210)$ .

A diferenç̄a m̄odulo-5 ẽ  $u - v = (301024)$ .

$$\text{A Dist̄ancia de Lee ẽ } W_L(u - v) = \sum_{i=0}^5 |u_i - v_i| \quad \text{onde}$$

$$|u_i - v_i| = u_i - v_i, \quad 0 \leq u_i - v_i \leq \frac{5}{2}$$

$$= 5 - (u_i - v_i), \quad \frac{5}{2} < u_i - v_i \leq 4$$

$$W_L(u - v) = 2 + 0 + 1 + 0 + 2 + 1 = 6$$

OBSERVAÇÕES:

- 1) Para os casos binário e ternário as distâncias de Lee e Hamming coincidem, para  $q > 3$ , a distância de Lee entre duas n-uplas é maior ou igual a distância de Hamming entre as mesmas duas n-uplas.
- 2) Em nosso estudo usaremos somente a distância e o peso no sentido de Hamming.

## 1.2 - MATRIZ GERATRIZ

Um código linear  $[n,k]$  é um subespaço do espaço vetorial de todas as  $n$ -uplas,  $V_n$ , portanto pode ser dado por uma base. Para este subespaço é possível encontrar um conjunto de  $k$   $n$ -uplas linearmente independentes (L.I.).

Sejam  $v_1, v_2, \dots, v_k$  os vetores L.I. Qualquer outro vetor do subespaço pode ser escrito da seguinte forma:

$V = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k$ , onde  $\alpha_i = 0, 1, \dots, q - 1$  para  $i = 1, 2, \dots, k$ .

Podemos, desta forma, descrever um código linear  $[n,k]$  por meio de um conjunto de  $k$  vetores código linearmente independentes.

Consideremos este conjunto  $v_1, v_2, \dots, v_k$  de  $k$  vetores código linearmente independentes como  $k$  linhas de uma matriz  $k \times n$ , denotada por  $G$ ,

$$G = \begin{pmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ \cdot \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdot & \cdot & \cdot & v_{1n} \\ v_{21} & v_{22} & \cdot & \cdot & \cdot & v_{2n} \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ v_{k1} & v_{k2} & & & & v_{kn} \end{pmatrix} \quad (1)$$

onde

$$v_i = (v_{i1}, v_{i2}, \dots, v_{in}), \quad i = 1, 2, \dots, k.$$

Seja  $u = (u_1, u_2, \dots, u_k)$  um bloco mensagem. Então, o vetor código correspondente pode ser dado por:

$$\begin{aligned} x = (x_1, x_2, \dots, x_n) &= u G \\ &= (u_1, u_2, \dots, u_k) \begin{pmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ \cdot \\ v_k \end{pmatrix} \\ &= u_1 v_1 + u_2 v_2 + \dots + u_k v_k \end{aligned}$$

Isto é, o vetor código  $x$ , correspondente a mensagem  $u$  é uma combinação linear das linhas de  $G$ . Portanto, o conjunto de todas as combinações lineares das linhas de  $G$  forma um subespaço  $k$ -dimensional de  $V_n$ , e o chamamos de **espaço linha de  $G$** .

Assim, as linhas de  $G$  geram um código linear e a matriz  $G$  é chamada **Matriz Geratriz do Código**.

OBSERVAÇÕES:

- 1) Como um subespaço pode ter mais que uma base, assim, um código linear pode ter mais que uma matriz geratriz.
- 2) Como um código linear é completamente especificado pela matriz geratriz o tamanho da armazenagem do codificador é reduzido.
- 3) O codificador precisa armazenar  $k$  linhas de  $G$  em lugar de armazenar os  $q^k$  vetores código do código.

Exemplo 1.2.1

Continuação do Exemplo 1.1.1, o código  $[5,3]$  é gerado por qualquer uma das duas matrizes seguintes:

$$G_1 = \begin{pmatrix} 10011 \\ 01010 \\ 00101 \end{pmatrix} \qquad G_2 = \begin{pmatrix} 10011 \\ 11001 \\ 11100 \end{pmatrix}$$

O vetor código  $x$  correspondente a mensagem  $u = (110)$  usando  $G_1$  é:

$$\begin{aligned} x = (110) \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} &= 1 \cdot v_1 + 1 \cdot v_2 + 0 \cdot v_3 = \\ &= 1 \cdot (10011) + 1 \cdot (01010) + 0 \cdot (00101) = \\ &= (11001) \end{aligned}$$

O vetor código  $x$  correspondente a mensagem  $u = (110)$  usando  $G_2$  é:

$$x = (110) \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = (01010)$$

E assim procedendo com todos os demais blocos mensagem obteremos os 8 vetores código do código.

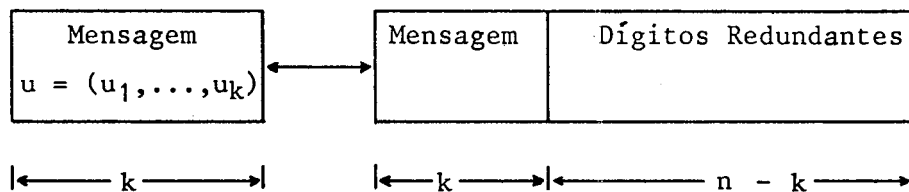
Podemos observar que usando a matriz geratriz  $G_1$  os primeiros 3 (três) dígitos de cada vetor código obtido, são os 3 (três)



dígitos da mensagem, transformada pelo codificador, fato este que nem sempre ocorre usando a matriz geratriz  $G_2$ .

Assim, é possível codificar cada bloco mensagem em um vetor código de tal modo que os primeiros  $k$  dígitos do vetor código são exatamente os mesmos do bloco mensagem e os últimos  $n - k$  dígitos são dígitos redundantes (dígitos de verificação de paridade) que são funções dos dígitos de informação.

Podemos ilustrar da seguinte maneira:



### Definição 1.2.1

Um código cujos vetores código assumem esta forma é dito um **Código Sistemático**.

Um  $[n, k]$  código linear sistemático pode ser descrito por uma matriz geratriz  $k \times n$  da forma:

$$G' = \begin{pmatrix} 100 \dots 0 & a_{11} & a_{12} & \dots & a_{1, n-k} \\ 010 \dots 0 & a_{21} & a_{22} & \dots & a_{2, n-k} \\ 001 \dots 0 & a_{31} & a_{32} & \dots & a_{3, n-k} \\ \cdot & \cdot & \cdot & & \\ \cdot & \cdot & \cdot & & \\ \cdot & \cdot & \cdot & & \\ 000 \dots 1 & a_{k1} & a_{k2} & \dots & a_{k, n-k} \end{pmatrix} \quad (2)$$

onde  $a_{ij} = 0, 1, 2, \dots, q-1$ .

Seja  $I_k$  a matriz identidade  $k \times k$  e seja  $A$  a matriz  $k \times (n - k)$  de  $a_{ij}$ . Então a matriz geratriz de um código sistemático pode ser escrita na forma seguinte:

$$G' = [I_k \vdots A] \quad (3)$$

Esta matriz  $G'$  pode ser obtida da matriz geratriz  $G$ , definida anteriormente, pela combinação de operações elementares das

linhas e permutações das colunas de  $G$ . Portanto  $G$  e  $G'$  são matrizes ditas combinatoriamente equivalentes.

Assim, existe uma matriz do tipo  $G'$  (da forma (2)) que é combinatoriamente equivalente a cada matriz geratriz  $G$  (da forma (1)), e todo código linear é equivalente a um código linear sistemático.

Agora, seja um bloco mensagem  $u = (u_1, u_2, \dots, u_k)$ . Usando a matriz geratriz  $G'$  da equação (2), o vetor código correspondente é

$$\begin{aligned} x &= (x_1, x_2, \dots, x_n) \\ &= (u_1, u_2, \dots, u_k) G' \\ &= (u_1, u_2, \dots, u_k) \begin{pmatrix} 100 \dots 0 & a_{11} & \dots & a_{1,n-k} \\ 010 \dots 0 & a_{21} & \dots & a_{2,n-k} \\ 001 \dots 0 & a_{31} & \dots & a_{3,n-k} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 000 \dots 1 & a_{k1} & \dots & a_{k,n-k} \end{pmatrix} \end{aligned} \quad (4)$$

$$\text{Assim, } x_i = u_i \text{ para } i = 1, 2, \dots, k \quad (5)$$

$$\text{e } x_{k+j} = a_{1j}u_1 + a_{2j}u_2 + \dots + a_{kj}u_k \quad (6)$$

para  $j = 1, 2, \dots, n-k$

Ou mais resumidamente

$$x = (u_1, u_2, \dots, u_k, y_1, y_2, \dots, y_{n-k}) \quad (7)$$

onde

$$y_j = \sum_{i=1}^k u_i a_{ij} \quad , \quad j = 1, 2, \dots, n-k \quad (8)$$

Das equações (5) e (6), ou mais resumidamente (7) e (8), podemos ver que as primeiras  $k$  componentes do vetor código são justamente os dígitos de informação; as últimas  $n - k$  componentes são funções dos dígitos de informação, ou seja, cada uma das últimas  $n - k$  componentes é uma combinação linear das primeiras  $k$  componentes.

As equações (6) ou (8) são chamadas as equações de verificação de paridade do código.

**Exemplo 1.2.2**

(Continuação do Exemplo 1.1.1 .)

O código  $[5,3]$  tem a matriz geratriz,

$$G = \begin{pmatrix} 10011 \\ 01010 \\ 00101 \end{pmatrix}$$

O vetor código correspondente ao bloco mensagem  $u = (u_1, u_2, u_3)$  é

$$\begin{aligned} \mathbf{x} &= (x_1, x_2, x_3, x_4, x_5) \\ &= (u_1 \ u_2 \ u_3)G = (u_1 \ u_2 \ u_3) \begin{pmatrix} 10011 \\ 01010 \\ 00101 \end{pmatrix} \\ &= (u_1, u_2, u_3, u_1 + u_2, u_1 + u_3) \end{aligned}$$

Assim,  $x_1 = u_1$ ,  $x_2 = u_2$ ,  $x_3 = u_3$ ,  $x_4 = u_1 + u_2$  e  $x_5 = u_1 + u_3$ .  
Escrevendo os  $2^3 = 8$  vetores códigos correspondentes aos 8 blocos mensagens, temos:

<b>u</b>		<b>x</b>
000	←————→	00000
100	←————→	10011
010	←————→	01010
001	←————→	00101
110	←————→	11001
101	←————→	10110
011	←————→	01111
111	←————→	11100

### 1.3 - MATRIZ DE VERIFICAÇÃO DE PARIDADE

Sejam  $u$  e  $v \in V_n$  sobre  $GF(q)$ . Definimos o produto interno de  $u$  e  $v$  como

$$u \cdot v = u_1v_1 + u_2v_2 + \dots + u_nv_n \pmod{q}$$

Se  $u \cdot v = 0$ , então,  $u$  e  $v$  são ditos ortogonais.

Para qualquer  $k \times n$  matriz  $G$  com  $k$  linhas linearmente independentes existe uma  $(n - k) \times n$  matriz  $H$  com  $n - k$  linhas

$$h_j = (h_{j1}, h_{j2}, \dots, h_{jn})$$

linearmente independentes,

$$H = \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_{n-k} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k,1} & h_{n-k,2} & \dots & h_{n-k,n} \end{pmatrix} \quad (9)$$

e qualquer vetor  $v$  no espaço linha de  $G$  é ortogonal a todas as linhas de  $H$ , isto é, o produto interno  $v \cdot h_j = 0$  para  $1 \leq j \leq n-k$ .

Desde que  $g_i$  é um vetor no espaço linha de  $G$ , o produto interno

$$g_i \cdot h_j = 0, \text{ para } 1 \leq i \leq k \text{ e } 1 \leq j \leq n-k$$

Seja  $t$  um vetor no espaço linha de  $H$ . Então,  $t$  é uma combinação linear das linhas de  $H$ ,

$$t = d_1h_1 + d_2h_2 + \dots + d_{n-k}h_{n-k}$$

onde  $d_i = 0, 1, 2, \dots, q-1$  para  $1 \leq i \leq n-k$ .

O produto interno de  $t$  por  $v$  é

$$\begin{aligned} t \cdot v &= (d_1h_1 + d_2h_2 + \dots + d_{n-k}h_{n-k}) \cdot v \\ &= d_1(h_1 \cdot v) + d_2(h_2 \cdot v) + \dots + d_{n-k}(h_{n-k} \cdot v) \end{aligned}$$

Desde que,  $h_j \cdot v = 0$ , temos que  $t \cdot v = 0$ . Isto é, qualquer vetor  $v$  no espaço linha de  $G$  e qualquer vetor  $t$  no espaço linha de  $H$  são ortogonais, isto é,  $t \cdot v = 0$ .

O espaço linha de  $G$  é chamado espaço nulo de  $H$ , ou vice-versa.

Portanto, para qualquer  $k \times n$  matriz  $G$  existe uma  $(n-k) \times n$  matriz  $H$  tal que o espaço linha de  $G$  é ortogonal a  $H$ .

Consideremos a matriz  $H$  da equação (9) e seja

$$x = (x_1, x_2, \dots, x_n)$$

um vetor no espaço linha de  $G$ . Então,

$$\mathbf{xH}^T = (00 \dots 0) \quad (10)$$

onde  $\mathbf{H}^T$  é a matriz transposta da matriz  $\mathbf{H}$ . As equações (10) podem ainda ser escritas como

$$\mathbf{x} \cdot \mathbf{h}_j = x_1 h_{j1} + x_2 h_{j2} + \dots + x_n h_{jn} = 0 \quad (11)$$

para  $j = 1, 2, \dots, n - k$ .

Assim, o significado das equações (10) é que as componentes de  $\mathbf{x}$  devem satisfazer um conjunto de  $n - k$  equações linearmente independentes. Naturalmente, qualquer combinação linear das equações (11) também dá uma equação que as componentes de  $\mathbf{x}$  devem satisfazer, e isto corresponde ao fato que  $\mathbf{x}$  é ortogonal a cada vetor do espaço linha de  $\mathbf{H}$ . Estas equações são chamadas equações generalizadas de verificação de paridade, porque no caso binário elas são simplesmente para verificar a paridade par sobre certos conjuntos de símbolos na palavra código.

Podemos definir o código linear, também, da seguinte maneira:

### Definição 1.3.1

$\mathbf{x}$  é um vetor código, se, e somente se,  $\mathbf{xH}^T = 0$ .

A matriz  $\mathbf{H}$  é chamada **Matriz de Verificação de Paridade** do código.

### OBSERVAÇÃO:

As operações nas equações (10) e (11) são efetuadas módulo  $q$ .

Seja a matriz geratriz  $G$ , de um código linear, que está na forma (2). Então, existe uma maneira simples para encontrar a matriz de verificação de paridade  $\mathbf{H}$ , conforme o teorema seguinte:

### Teorema 1.3.1

Se  $V$  é o espaço linha da matriz  $G = [I_k \vdots A]$ , onde  $I_k$  é uma  $k \times k$  matriz identidade e  $A$  é uma  $k \times (n - k)$  matriz, então,  $V$  é o espaço nulo da matriz  $H = [-A^T \vdots I_{n-k}]$ , onde  $I_{n-k}$  é uma  $(n-k) \times (n-k)$  matriz identidade e  $A^T$  é a  $(n - k) \times k$  matriz transposta da matriz  $A$ .

Demonstração:

Vimos que qualquer vetor  $g_i$  no espaço linha de  $G$  é ortogonal a todas as linhas de  $H$ , isto é, o produto interno  $g_i \cdot h_j = 0$  para  $1 \leq i \leq k$  e  $1 \leq j \leq n - k$ . Isto quer dizer que qualquer vetor no espaço linha de  $G$  e qualquer vetor no espaço linha de  $H$  são ortogonais. Ou seja, as linhas de  $G$  e  $H$  são ortogonais umas as outras.

É claro que  $G$  tem posto  $k$  e  $H$  tem posto  $n - k$ , logo

$$H = [ -A^T : I_{n-k} ]$$

Assim,  $H$  é dada por:

$$H = \begin{pmatrix} -a_{11} & -a_{21} & \dots & -a_{k1} & 1 & 0 & \dots & 0 \\ -a_{12} & -a_{22} & \dots & -a_{k2} & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot & \cdot & \dots & \cdot \\ -a_{1,n-k} & -a_{2,n-k} & \dots & -a_{k,n-k} & 0 & 0 & \dots & 1 \end{pmatrix} \quad (12) \quad \square$$

As equações de verificação de paridade (6) ou (8) podem ser obtidas de  $H$ .

De fato, se  $x = (x_1, x_2, \dots, x_n)$  é um vetor código, correspondente a mensagem  $u = (u_1, u_2, \dots, u_k)$ , onde  $x_i = u_i$  para  $1 \leq i \leq k$  desde que  $xH^T = 0$ , então temos:

$$\begin{aligned} x_{k+j} &= a_{1j}x_1 + a_{2j}x_2 + \dots + a_{kj}x_k \\ &= a_{1j}u_1 + a_{2j}u_2 + \dots + a_{kj}u_k \end{aligned}$$

para  $j = 1, 2, \dots, n - k$ , que é exatamente o mesmo conjunto de equações (6).

OBSERVAÇÃO:

É conveniente, mas não essencial, que  $H$  tenha a forma mostrada em (12), pois, neste caso, os primeiros  $k$  dígitos em cada palavra código são dígitos de informação (mensagem), e os últimos  $n - k$  são dígitos de verificação de paridade.

Como a equação (10) vale para cada um dos  $k$  vetores da base da matriz  $G$ , estas  $k$  equações podem ser expressadas por:

$$HG^T = 0, \quad \text{ou} \quad GH^T = 0.$$

Exemplo 1.3.1

(Continuação do Exemplo 1.1.1 .)

Sabemos que a matriz geratriz  $\bar{e}$

$$G = [I_k \vdots A] = \begin{pmatrix} 10011 \\ 01010 \\ 00101 \end{pmatrix}$$

Segundo o Teorema 1.3.1 , a matriz de verificação de paridade  $\bar{e}$

$$H = [ -A^T \vdots I_{n-k} ] = [ A^T \vdots I_{n-k} ] = \begin{pmatrix} 11010 \\ 10101 \end{pmatrix}$$

OBSERVAÇÃO:

No caso binário  $-A^T = A^T$  .

O vetor código  $\mathbf{x}$  correspondente ao bloco mensagem

$$\mathbf{u} = (u_1 \ u_2 \ u_3) \ \bar{e} \ \text{tal que} \ \mathbf{xH}^T = \mathbf{0}$$

$$\text{Seja } \mathbf{x} = (x_1, x_2, x_3, x_4, x_5) \ \text{e} \ H^T = \begin{pmatrix} 11 \\ 10 \\ 01 \\ 10 \\ 01 \end{pmatrix}$$

$$\text{então, } (x_1, x_2, x_3, x_4, x_5) \begin{pmatrix} 11 \\ 10 \\ 01 \\ 10 \\ 01 \end{pmatrix} = 0$$

de onde temos:

$$\begin{cases} x_4 = x_1 + x_2 \\ x_5 = x_1 + x_3 \end{cases} \quad \text{onde } x_1 = u_1; \ x_2 = u_2 \ \text{e} \ x_3 = u_3 .$$

Agora escrevendo os  $2^3 = 8$  vetores código correspondentes aos 8 blocos mensagem, temos:

<b>u</b>		<b>x</b>
000	←————→	00000
100	←————→	10011
010	←————→	01010
001	←————→	00101
110	←————→	11001
101	←————→	10110
011	←————→	01111
111	←————→	11100

que são os vetores código do Exemplo 1.2.2 .

### Exemplo 1.3.2

Seja o código ternário  $[4,2]$  cuja matriz geratriz  $\bar{e}$ :

$$G = \begin{bmatrix} 1022 \\ 0121 \end{bmatrix}$$

Hã  $3^2 = 9$  vetores código.

A matriz de verificação de paridade  $\bar{e}$   $H = \begin{bmatrix} 1110 \\ 1201 \end{bmatrix}$

Os vetores código  $x$  são tais que  $xH^T = 0$  e dados por:

<b>u</b>		<b>x</b>
00	←————→	0000
01	←————→	0121
02	←————→	0212
10	←————→	1022
11	←————→	1110
12	←————→	1201
20	←————→	2011
21	←————→	2102
22	←————→	2220



Provaremos no teorema seguinte uma relação de dependência linear entre as colunas de  $\mathbf{H}$  e os vetores código de um código linear.

### Teorema 1.3.2

Seja  $C$  um código linear que é o espaço nulo de uma matriz  $\mathbf{H}$ . Então, para cada vetor código com peso Hamming  $W$ , existe uma relação de dependência linear entre  $W$  colunas de  $\mathbf{H}$ , e reciprocamente, para cada relação de dependência linear envolvendo  $W$  colunas de  $\mathbf{H}$ , existe um vetor código de peso  $W$ .

#### Demonstração:

Um vetor  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  é um vetor código se, e somente se,  $\mathbf{x}\mathbf{H}^T = \mathbf{0}$ , ou se o  $i$ -ésimo vetor coluna na matriz  $\mathbf{H}$  é denotado por  $\mathbf{h}_i$ , então

$$\sum_{i=1}^n x_i \mathbf{h}_i = \mathbf{0}.$$

Isto é exatamente uma relação de dependência linear entre colunas de  $\mathbf{H}$ , e o número de colunas de  $\mathbf{H}$  que aparece com coeficientes não nulos é o número de componentes não nulos  $x_i$  de  $\mathbf{x}$ , que é exatamente o peso de  $\mathbf{x}$ . Portanto, para cada vetor código com peso de Hamming  $W$ , existe uma relação de dependência linear entre  $W$  colunas de  $\mathbf{H}$ .

Analogamente, os coeficientes de qualquer relação de dependência linear entre colunas de  $\mathbf{H}$  são componentes de um vetor que deve estar no espaço nulo de  $\mathbf{H}$ . Portanto, para cada relação de dependência linear envolvendo  $W$  colunas de  $\mathbf{H}$ , existe um vetor código de peso  $W$ . □

### Corolário 1.3.3

O código linear  $C$  tem peso mínimo  $d$  se, e somente se,  $d$  é o maior número tal que, cada  $d - 1$  colunas de qualquer matriz de verificação de paridade  $\mathbf{H}$  de  $C$  são independentes.

#### Demonstração:

Segue imediatamente do Teorema 1.3.2.

## 1.4 - PROPRIEDADES DE UM CÓDIGO LINEAR

1.4.1 -  $x$  é um vetor código se, e somente se  $xH^T = 0$ , ou  $Hx^T = 0$ .

### 1.4.2 - Matriz Geratriz e Matriz de Verificação de Paridade

Usualmente a matriz geratriz é uma  $k \times n$  matriz da forma  $G = [I_k \mid A]$  e a matriz de verificação de paridade é uma  $(n - k) \times n$  matriz da forma  $H = [-A^T \mid I_{n-k}]$ , e o código tem  $q^k$  palavras código satisfazendo (10).

#### OBSERVAÇÕES:

- 1) O fato de  $q^k$  palavras no código ainda é correto se  $H$  não está na forma acima, desde que  $H$  tenha  $n$  colunas e  $n - k$  linhas linearmente independentes.
- 2) Quando  $H$  tem a forma acima, os vetores código são da forma:

$$X = \underbrace{x_1 \cdot \cdot \cdot x_k}_{\substack{\text{dígitos de} \\ \text{informação}}} \underbrace{x_{k+1} \cdot \cdot \cdot x_n}_{\substack{\text{dígitos de} \\ \text{verificação}}}$$

### 1.4.3 - Os Parâmetros de um Código Linear $[n, k, d]$

$n$  = comprimento do código.

$k$  = dimensão do código.

$d$  = distância mínima do código.

A Taxa ou Eficiência do Código é definida por  $R = \frac{k}{n}$ .

#### Exemplo 1.4.1

O código  $[5,3]$  tem taxa  $R = \frac{3}{5}$

### 1.4.4 - Outras matrizes geratriz e de verificação de paridade

Um código linear pode ter mais de uma matriz geratriz. De fato, qualquer conjunto máximo de vetores código linearmente independentes, tomados de um dado código, pode ser usado como as linhas de uma matriz geratriz para aquele código.

Uma verificação de paridade sobre um código é qualquer vetor linha  $\mathbf{h}$  tal que  $\mathbf{xh}^T = 0$  para todo vetor código  $\mathbf{x}$  pertencente ao código.

Analogamente, qualquer conjunto máximo de verificações de paridade linearmente independentes pode ser usado como as linhas de uma matriz de verificação de paridade  $\mathbf{H}$  para o código.

#### 1.4.5 - Linearidade

Se  $\mathbf{x}$  e  $\mathbf{y}$  são vetores código de um dado código, então,  $\mathbf{x} - \mathbf{y}$  é também um vetor código, porque  $(\mathbf{x} - \mathbf{y})\mathbf{H}^T = \mathbf{xH}^T - \mathbf{yH}^T = 0$ .

Se  $\mathbf{a}$  é qualquer elemento do corpo de  $q$  elementos, então,  $\mathbf{ax}$  também é um vetor código, porque  $(\mathbf{ax})\mathbf{H}^T = \mathbf{axH}^T = \mathbf{a} \cdot \mathbf{0} = \mathbf{0}$ .

#### OBSERVAÇÃO:

Um código linear é também um grupo aditivo e um espaço vetorial sobre o corpo.

## 1.5 - ARRANJO PADRÃO

Consideremos um código linear  $[n,k]$  com  $q^k$  vetores código.

Para qualquer vetor código que é transmitido em um canal ruidoso o vetor recebido  $r$  pode ser qualquer uma das  $q^n$   $n$ -uplas.

Qualquer esquema de decodificação usado no decodificador é uma regra (lei) para dividir as  $q^n$   $n$ -uplas em  $q^k$  subconjuntos disjuntos  $D_1, D_2, \dots, D_{q^k}$  tais que o subconjunto  $D_i$  contém somente um vetor código  $x_i$ . Assim, cada subconjunto  $D_i$  está em correspondência biunívoca com um vetor código  $x_i$ .

Desta forma, se o vetor recebido  $r$  é encontrado no subconjunto  $D_i$ , então, o decodificador identifica  $x_i$  como o vetor código transmitido.

A decodificação correta é feita se o vetor recebido está no subconjunto  $D_i$  que corresponde ao vetor código transmitido.

Uma decodificação incorreta resulta se o vetor recebido está no subconjunto que não corresponde ao vetor código transmitido.

Uma maneira para dividir as  $q^n$   $n$ -uplas é descrita como segue. E este processo de divisão é conhecido como **arranjo padrão**.

Todos os  $q^k$  vetores código são colocados numa linha com o vetor nulo  $x_1 = (0,0,\dots,0)$  como o primeiro elemento (à esquerda).

De todas as  $q^n - q^k$   $n$ -uplas, uma  $n$ -upla  $e_2$  é escolhida e é colocada debaixo do vetor código  $x_1$ . Então, a segunda linha é completada somando  $e_2$  a cada vetor código  $x_i$ , isto é, colocando debaixo de cada vetor código  $x_i$  o vetor soma  $e_2 + x_i$ .

Analogamente, entre todas as  $n$ -uplas restantes, não usadas, uma  $e_3$  é escolhida e é colocada na primeira coluna, e a terceira linha é completada. O processo continua até que todas as  $n$ -uplas são usadas, isto é, até que cada  $n$ -upla apareça em algum lugar na tabela abaixo. Então, obtemos um arranjo de linhas e colunas, em que cada linha consiste de  $q^k$   $n$ -uplas, conforme a tabela:

$$\begin{array}{cccccc}
 x_1 & & x_2 & \dots & x_i & \dots & x_{qk} \\
 e_2 & & e_2 + x_2 & \dots & e_2 + x_i & \dots & e_2 + x_{qk} \\
 e_3 & & e_3 + x_2 & \dots & e_3 + x_i & \dots & e_3 + x_{qk} \\
 \cdot & & \cdot & & \cdot & & \cdot \\
 \cdot & & \cdot & & \cdot & & \cdot \\
 \cdot & & \cdot & & \cdot & & \cdot \\
 e_\ell & & e_\ell + x_2 & \dots & e_\ell + x_i & \dots & e_\ell + x_{qk} \\
 \cdot & & \cdot & & \cdot & & \cdot \\
 \cdot & & \cdot & & \cdot & & \cdot \\
 \cdot & & \cdot & & \cdot & & \cdot \\
 e_{qn-k} & & e_{qn-k} + x_2 & \dots & e_{qn-k} + x_i & \dots & e_{qn-k} + x_{qk}
 \end{array}$$

Provaremos no Teorema seguinte algumas propriedades do arranjo padrão.

### Teorema 1.5.1

- (1) Duas n-uplas na mesma linha do arranjo não são idênticas.
- (2) Nenhuma n-upla aparece em linhas diferentes.

### Demonstração:

(1) Suponhamos que duas n-uplas na  $\ell$ -ésima linha são idênticas, isto é:  $e_\ell + x_i = e_\ell + x_j$  com  $i \neq j$ . Então, temos  $x_i = x_j$  que é impossível, pois  $x_i$  e  $x_j$  são vetores código. Portanto, duas n-uplas na mesma linha do arranjo não são idênticas.

(2) Suponhamos que uma n-upla aparece na  $\ell$ -ésima linha e na  $t$ -ésima linha, com  $\ell < t$ . Então, esta n-upla deve ser igual a  $e_\ell + x_i$  para algum  $i$  e deve ser igual a  $e_t + x_j$  para algum  $j$ . Portanto,  $e_\ell + x_i = e_t + x_j$  de onde obtemos  $e_t = e_\ell + (x_i - x_j)$  desde que  $x_i$  e  $x_j$  são vetores código, também o é  $x_i - x_j$ . Seja  $x_m = x_i - x_j$ . Então,  $e_t = e_\ell + x_m$ . O que implica que a n-upla  $e_t$  está na  $\ell$ -ésima linha, o que contradiz a regra de construção do arranjo que diz ser  $e_t$  o primeiro elemento da  $t$ -ésima linha que não apareceu em nenhuma linha anterior. Portanto, concluímos que nenhuma n-upla aparece em linhas diferentes.  $\square$

Deste teorema concluímos que cada linha do arranjo consis-

te de  $q^k$  n-uplas distintas e portanto, todas as linhas são disjuntas. Isto é, cada n-upla aparece uma e somente uma vez no arranjo. Assim há  $\frac{q^n}{q^k} = q^{n-k}$  linhas distintas..

Um arranjo assim construído é chamado **Arranjo Padrão** para um dado código linear  $[n,k]$ , onde as  $q^{n-k}$  linhas são chamadas "cosets" e as n-uplas da primeira coluna do arranjo são ditas representantes dos "cosets" (ou "coset líderes").

### Exemplo 1.5.1

Consideremos o código linear binário  $[5,3]$  do Exemplo 1.1.1. O arranjo padrão para este código é:

"coset líder"							
00000	10011	01010	11001	00101	10110	01111	11100
00001	10010	01011	11000	00100	10111	01110	11101
00010	10001	01000	11011	00111	10100	01101	11110
10000	00011	11010	01001	10101	00110	11111	01100

O "coset líder" em cada linha, sempre foi escolhido o vetor de menor peso entre os restantes.

Todas as  $2^5 = 32$  5-uplas aparecem no arranjo padrão.

No arranjo padrão do código  $[n,k]$  denotemos a  $j$ -ésima coluna como  $D_j$ , então

$$D_j = \{x_j; e_2 + x_j; e_3 + x_j; \dots; e_{q^{n-k}} + x_j\} \quad (13)$$

onde  $x_j$  é o  $j$ -ésimo vetor código e  $e_2, e_3, \dots, e_{q^{n-k}}$  são os "cosets líderes". Portanto, o arranjo padrão divide as  $q^n$  n-uplas em  $q^k$  subconjuntos disjuntos  $D_1; D_2; \dots; D_{q^k}$ .

Suponhamos que o vetor  $x_j$  é transmitido por um canal ruidoso. Pela equação (13), vimos que o vetor recebido  $r$  está em  $D_j$  se o vetor de erro causado pelo canal é um "coset líder". Então, o vetor recebido será decodificado corretamente em  $x_j$ . Por outro lado, se o vetor de erro causado pelo canal não é um "coset líder" resultará uma decodificação incorreta. Assim, o vetor de erro  $e$  causado pelo canal deve estar em algum "coset" e debaixo de algum vetor código, seja o  $\ell$ -ésimo "coset" e debaixo do vetor código  $x_j$ . Então,  $e = e_\ell + x_j$  e o vetor recebido será

$$r = x_i + e = e_\ell + (x_i + x_j) = e_\ell + x_s$$

O vetor recebido está em  $D_s$  e é decodificado em  $x_s$  que é uma decodificação incorreta. Portanto, quando um arranjo padrão é usado para a decodificação, a decodificação é correta se, e somente se o vetor de erro causado pelo canal é um "coset líder".

Sejam  $e_i$  e  $e_j$  dois vetores de erro com peso  $W(e_i)$  e  $W(e_j)$  respectivamente. Para um canal simétrico binário, se  $W(e_i) < W(e_j)$ , então  $e_i$  ocorre mais provavelmente que  $e_j$ . Portanto, em cada caso, o "coset líder" seria escolhido como um vetor com peso mínimo entre os vetores restantes.

## 1.6 - SÍNDROME E SUAS PROPRIEDADES

### 1.6.1 - Síndrome

Consideremos um código linear com matriz geratriz  $G$  e matriz de verificação de paridade  $H$ .

Seja  $x$  um vetor código que é transmitido através do canal.

No receptor obtemos um vetor  $r = (r_1, r_2, \dots, r_n)$  que pode ser diferente de  $x$ . Seja  $r$  a soma do vetor código original  $x$  e um vetor de erro  $e$ , isto é:

$$r = x + e \quad \text{ou} \quad e = r - x$$

O objetivo do decodificador é recuperar  $x$  de  $r$ .

Para decodificar  $r$  introduziremos o conceito de síndrome.

#### Definição 1.6.1.1

O vetor  $S = rH^T$  é chamado a **síndrome** do vetor recebido  $r$ .

#### OBSERVAÇÃO:

A síndrome de um vetor recebido será usada para correção e detecção de erros.

#### Exemplo 1.6.1.1

Consideremos o código linear binário  $[5,3]$  do Exemplo 1.3.1

$$G = \begin{pmatrix} 10011 \\ 01010 \\ 00101 \end{pmatrix} \quad \text{e} \quad H = \begin{pmatrix} 11010 \\ \\ 10101 \end{pmatrix}$$

Seja o vetor recebido  $r = (11110)$  que não é um vetor código. A síndrome deste vetor é:

$$S = (11110) \begin{pmatrix} 11 \\ 10 \\ 01 \\ 10 \\ 01 \end{pmatrix} = (10)$$

Seja o vetor recebido  $r = (11001)$  que é um vetor código correspondente a mensagem  $u = (110)$ . Então:



$$S = (11001) \begin{pmatrix} 11 \\ 10 \\ 01 \\ 10 \\ 01 \end{pmatrix} = (00)$$

### 1.6.2 - Propriedades da Síndrome

1.6.2.1 -  $S$  é um vetor de comprimento  $n-k$ .

1.6.2.2 - A síndrome de  $r$ ,  $S = rH^T$ , é zero se, e somente se  $r$  é um vetor código (pela definição do código).

1.6.2.3 - Se nenhum erro ocorreu, a síndrome de  $r$  é zero (mas, a recíproca não é verdadeira).

1.6.2.4 - Para um código binário, a síndrome é igual a soma das colunas de  $H$  onde ocorreram erros. (Assim,  $S$  é chamado a síndrome porque dá os sintomas de erros.)

#### Demonstração:

Sejam  $x$  um vetor código transmitido,  $e$  um vetor de erro e  $r$  o vetor recebido, então:

$$r = x + e$$

Pela definição de síndrome

$$S = rH^T = (x + e)H^T = xH^T + eH^T = eH^T \quad (14)$$

Se ocorreram erros nas posições  $a, b, c, \dots$ , de tal modo que

$$e = 0 \dots 0 \frac{1}{a} 0 \dots \frac{1}{b} \dots \frac{1}{c} \dots 0,$$

então, da equação (14), temos:

$$\begin{aligned} S &= \sum_i e_i h_i \quad (h_i = i\text{-ésima coluna de } H) \\ &= h_a + h_b + h_c + \dots \end{aligned}$$

Portanto, a síndrome é igual a soma das colunas de  $H$  onde ocorreram erros.

### 1.6.3 - Vantagens da Síndrome

Uma vantagem do uso da síndrome é que ela simplifica o processo de decodificação descrito anteriormente, senão vejamos.

Se  $C$  é um código de comprimento  $n$ , então, o arranjo padrão consistirá de  $q^n$  elementos, que teríamos de armazenar e investigar para localizar um vetor recebido. O uso da síndrome, isto é, calculando a síndrome do vetor recebido tem-se o "coset líder", isto é, o vetor de erro provável causado pelo canal, que subtraindo-o do vetor recebido tem-se o vetor código que provavelmente foi transmitido.

Provaremos no teorema seguinte, com uso da síndrome, uma propriedade muito importante do arranjo padrão que pode ser usada para simplificar o processo de decodificação.

### Teorema 1.6.3.1

- (1) Todas as  $q^k$  n-uplas de um "coset" tem mesma síndrome.
- (2) As síndromes para diferentes "cosets" são diferentes.

### Demonstração:

Consideremos uma matriz de verificação de paridade  $H$  para um dado código linear  $[n,k]$ .

(1) Consideremos o  $\ell$ -ésimo "coset" cujo "coset líder" é  $e_\ell$ . Uma n-upla neste "coset" é igual a  $e_\ell + x_i$  para algum  $i$ . A síndrome desta n-upla é

$$(e_\ell + x_i)H^T = e_\ell H^T + x_i H^T$$

Desde que  $x_i$  é um vetor código que está no espaço nulo de  $H$ , então  $x_i H^T = 0$ . Assim  $(e_\ell + x_i) H^T = e_\ell H^T$ . Isto é, a síndrome de qualquer n-upla num "coset" é igual a do "coset líder". Portanto, todas as n-uplas de um "coset" tem a mesma síndrome.

(2) Suponhamos que as síndromes do  $\ell$ -ésimo "coset" e do  $t$ -ésimo "coset" ( $\ell < t$ ) são iguais. Da parte (1) temos que

$$e_\ell H^T = e_t H^T.$$

Então,  $(e_t - e_\ell) H^T = 0$ . O que implica que a n-upla  $(e_t - e_\ell)$  deve ser um vetor código, qual seja  $x_j$ . Assim,  $e_t = e_\ell + x_j$ . Isto é,  $e_t$  está no  $\ell$ -ésimo "coset", o que contradiz a regra de construção do arranjo padrão que segundo a qual o "coset líder" não seria usado anteriormente. Portanto, concluímos que

$$l \neq t \quad , \quad e_l H^T \neq e_t H^T \quad ,$$

isto é, as síndromes de diferentes "cosets" são diferentes.

□

OBSERVAÇÃO:

Pelo Teorema 1.6.3.1 , existe uma correspondência biunívoca entre um "coset líder" e uma síndrome.

## 1.7 - LIMITES SOBRE A DISTÂNCIA MÍNIMA PARA CÓDIGOS

É importante saber a capacidade e limitação dos códigos correctores de erros. Esta informação juntamente com o conhecimento, o que é praticamente atingível, indica quais os problemas que estão resolvidos e quais ainda precisam de mais investigação.

Provaremos inicialmente três lemas que usaremos na dedução de alguns limites inferiores e superiores sobre a distância mínima atingível com um código linear.

### Lema 1.7.1

Se todos os vetores código em um código linear  $[n, k]$  são arrumados como linhas de uma matriz, e se nenhuma coluna consiste toda de "0's (toda nula), então, cada elemento do corpo aparece  $q^{k-1}$  vezes em cada coluna.

### Demonstração:

Provaremos o resultado para uma coluna qualquer. Escolhemos a primeira. Vamos escrever os vetores código da seguinte maneira,

os que começam por

$$\begin{array}{l} 0 \longrightarrow 0 \dots ; 0 \dots ; \dots \\ 1 \longrightarrow 1 \dots ; 1 \dots ; \dots \\ \cdot \\ \cdot \\ \cdot \\ q-1 \longrightarrow q-1 \dots ; q-1 \dots ; \dots \end{array}$$

Consideremos os elementos da primeira coluna.

Sabemos que os  $q^k$  vetores código formam um espaço vetorial sobre o corpo de  $q$  elementos. O conjunto dos vetores código que comecem por 0 ou 1 ou 2 ou ... ou  $q-1$ , formam cada um, um subespaço vetorial do espaço vetorial das  $q^k$  n-uplas sobre o corpo de  $q$  elementos.

Consideremo-los como "cosets", temos portanto um total de  $q$  "cosets".

Como todos os "cosets" tem o mesmo número de elementos, chamemos de  $x$  o número de elementos de cada "coset". Então, o produto do número de "cosets" pelo número de elementos de cada "coset" dá o número total de vetores código do código, isto é:

$qX = q^k \Rightarrow X = q^{k-1}$ , portanto, cada "coset" tem  $q^{k-1}$  elementos.

Escrevendo cada elemento do "coset" como uma linha de uma matriz  $M$  temos:

$$M = \begin{pmatrix} 0 & \dots & \dots \\ \vdots & & \\ \vdots & & \\ \vdots & & \\ \vdots & & \\ 0 & \dots & \dots \\ 1 & \dots & \dots \\ \vdots & & \\ \vdots & & \\ \vdots & & \\ \vdots & & \\ 1 & \dots & \dots \\ \vdots & & \\ \vdots & & \\ \vdots & & \\ q-1 & \dots & \dots \\ \vdots & & \\ \vdots & & \\ \vdots & & \\ q-1 & \dots & \dots \end{pmatrix}$$

Portanto, cada elemento do corpo aparece na primeira coluna  $q^{k-1}$  vezes. Como a primeira coluna foi escolhida arbitrariamente, vale o resultado para todas as colunas.  $\square$

### Exemplo 1.7.1

Seja o código linear binário  $[6,3]$  com matriz geratriz

$$G = \begin{pmatrix} 100011 \\ 010101 \\ 001110 \end{pmatrix}$$

Escrevendo os 8 vetores código como linhas de uma matriz  $M$  temos:

$$M = \begin{pmatrix} 000000 \\ 001110 \\ 010101 \\ 011011 \\ 100011 \\ 101101 \\ 110110 \\ 111000 \end{pmatrix}$$

Cada elemento 0 e 1 do corpo aparece  $2^{k-1} = 2^2 = 4$  vezes em cada coluna.

### Exemplo 1.7.2

Seja o código linear ternário  $[4,2]$  com matriz geratriz

$$G = \begin{pmatrix} 1022 \\ 0121 \end{pmatrix}$$

Escrevendo os  $3^2 = 9$  vetores código como linhas de uma matriz  $M$ , temos:

$$M = \begin{pmatrix} 0000 \\ 0121 \\ 0212 \\ 1022 \\ 1110 \\ 1201 \\ 2011 \\ 2102 \\ 2220 \end{pmatrix}$$

Cada elemento 0, 1 e 2 do corpo aparece  $q^{k-1} = 3^{2-1} = 3$  vezes em cada coluna.

### Lema 1.7.2

A soma dos pesos de todos os vetores código em um código linear  $[n,k]$ , quando arrumados como linhas de uma matriz  $M$  onde nenhuma coluna é toda nula, é

$$n(q-1)q^{k-1}$$

**Demonstração:**

Escrevendo os vetores código do código linear  $[n, k]$  como linhas de uma matriz  $M$ , conforme Lema 1.7.1, temos:

$$M = \begin{pmatrix} 0 & \dots & \dots & \dots \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ 0 & \dots & \dots & \dots \\ 1 & \dots & \dots & \dots \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ 1 & \dots & \dots & \dots \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ q-1 & \dots & \dots & \dots \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ q-1 & \dots & \dots & \dots \end{pmatrix}$$

O número de dígitos não nulos em cada linha é exatamente  $i$  igual ao número de dígitos não nulos em cada elemento do "coset". Cada elemento do "coset" é uma  $n$ -upla, o que nos permite afirmar que a matriz  $M$  tem  $n$  colunas. Cada "coset" tem  $q^{k-1}$  elementos, conforme Lema 1.7.1. Em cada coluna da matriz  $M$  temos  $q-1$  dígitos não nulos, onde cada um deles aparece  $q^{k-1}$  vezes, conforme Lema 1.7.1 e por hipótese, nenhuma coluna é toda nula. Portanto, na matriz  $M$  temos um total de  $n(q-1)q^{k-1}$  dígitos não nulos. Por definição, o peso de um vetor código, no sentido de Hamming é dado pelo número de dígitos não nulos do mesmo. Assim, a soma dos pesos de todos os vetores código de um código linear  $[n, k]$  é dada pela soma do número de dígitos não nulos de todos os vetores código do mesmo, que é igual ao número de dígitos não nulos da matriz  $M$  que é

$$n(q-1)q^{k-1}$$

□

**Exemplo 1.7.3**

Continuação do Exemplo 1.7.1 .

Vetores Código	Pêso
000000	0
001110	3
010101	3
011011	4
100011	3
101101	4
110110	4
111000	3

A soma total dos pesos dos vetores código é:

$$24 = 6(2 - 1) 2^{3-1} = n(q - 1) q^{k-1}$$

### Lema 1.7.3

Num código linear binário ou todos os vetores código tem peso par ou metade tem peso par e metade ímpar.

#### Demonstração:

Basta mostrar que os vetores código de peso par formam um subgrupo.

O conjunto  $C$  dos vetores código do código  $[n, k]$  formam um grupo com respeito a adição.

Consideremos somente o conjunto  $P$  dos vetores código de peso par. Para mostrar que  $P$  é um subgrupo de  $C$  basta mostrar que  $P$  é fechado e que a inversa existe no conjunto  $P$ .

No conjunto  $P$  a adição é fechada, pois o que resulta é sempre um vetor código de peso par.

Como o corpo é binário, o inverso de cada vetor código é ele mesmo, logo a inversa existe no conjunto  $P$ . Portanto, o conjunto  $P$  de todos os vetores código de peso par forma um subgrupo do grupo de todos os vetores código do código.

Diante disto, temos duas situações a examinar:

$$P = C \quad \text{ou} \quad P \subset C$$

Se  $P = C$ , então, todos os vetores código tem peso par.

Se  $P \subset C$ , consideremos um vetor código  $c \in C$  tal que  $c \notin P$ , então  $(c + P) = Q \not\subset P$ , isto é,  $(c + p_i) \notin P$  para todo



$p_i \in P$ , formam um conjunto  $Q$  de vetores de p̄eso ímpar contido em  $C$ . Portanto,  $C = P \cup Q$ .

Como  $P$  e  $Q$  tem o mesmo número de elementos, temos que, a metade dos vetores código tem p̄eso par e a metade tem p̄eso ímpar.

Logo, no código linear binário  $[n,k]$  todos os vetores código tem p̄eso par ou a metade tem p̄eso par e metade ímpar.  $\square$

#### Exemplo 1.7.4

No código binário  $[6,3]$  do Exemplo 1.7.1, consideremos os vetores código de p̄eso par e chamemos ao conjunto destes de:

$$P = \{000000 ; 011011 ; 101101 ; 110110\} .$$

A adição é fechada em  $P$ , isto é

$$011011 + 101101 = 110110 \in P$$

$$011011 + 110110 = 101101 \in P$$

$$110110 + 101101 = 011011 \in P$$

O inverso de cada vetor código é ele mesmo, consequentemente a identidade  $(000000) \in P$ . ji

Logo,  $P$  é um subgrupo do código binário  $[6,3]$  com respeito a adição.

#### **Lema 1.7.4**

O p̄eso m̄inimo de um vetor código em um código linear  $[n,k]$  é no máximo tão grande quanto o p̄eso médio

$$\frac{n(q-1)q^{k-1}}{q^k-1}$$

#### Demonstração:

Pelo Lema 1.7.2, a soma dos p̄esos de todos os vetores código de um código linear  $[n,k]$  cujos dígitos são tomados sobre um corpo de  $q$  elementos é  $n(q-1)q^{k-1}$ . Como num código  $[n,k]$  há  $q^k$  vetores código, sendo que  $q^k-1$  tem p̄eso não nulo, e o vetor código de p̄eso m̄inimo tem no máximo o p̄eso médio, denotemos por  $d_x$  o p̄eso m̄inimo do vetor código  $x$ , então

$$d_x \leq \frac{n(q-1)q^{k-1}}{q^k-1}$$

□

Seja  $B(n,d)$  o número máximo de vetores código possíveis em um código linear de comprimento  $n$  com peso mínimo pelo menos  $d$ .

#### Lema 1.7.5

$$\text{Se } n > d, B(n,d) \leq q B(n-1, d)$$

#### Demonstração:

Seja  $C$  um código de comprimento  $n$  e peso mínimo pelo menos  $d$  que tem  $B(n,d)$  vetores código. Seja o conjunto  $F$  de todos os vetores código de  $C$  em que o último dígito é "0".

Como a soma de quaisquer dois elementos de  $F$  está em  $F$ , e qualquer múltiplo escalar de um elemento de  $F$  está em  $F$ , então,  $F$  forma um subspaço de  $C$ .

$$F = \left\{ \begin{array}{l} 0 \quad . \quad . \quad . \\ . \\ . \\ . \\ 1 \quad . \quad . \quad . \\ . \\ . \\ . \\ 2 \quad . \quad . \quad . \\ . \\ . \\ . \\ q-1 \quad . \quad . \quad . \\ . \\ . \\ . \end{array} \right\}$$

Como cada elemento do corpo pode aparecer na última posição existem  $q$  "cosets" de  $F$  em  $C$ . Assim uma fração  $\frac{1}{q}$  dos elementos de  $C$  está em  $F$ .

Então, o subgrupo  $F$  é um código linear com  $\frac{1}{q} B(n,d)$  símbolos e peso mínimo pelo menos  $d$ , cujos vetores cada um tem a

última componente "0" .

Desprezando o último símbolo temos um código linear de  $n-1$  dígitos sem afetar o número de vetores código no subgrupo ou o peso mínimo. Pode existir outras colunas todas nulas no código resultante  $F$ , mas estas podem ser substituídas por qualquer outro tipo de coluna sem reduzir o peso mínimo. (Notar que  $B(n-1, n-1) = q$ , consistindo o código de  $n-1$  repetições de um único dígito de informação. Assim, com a suposição que  $n > d$ , são possíveis colunas não nulas no código de comprimento  $n-1$ .)

Portanto,

$$B(n-1, d) \geq \frac{1}{q} B(n, d), \quad \text{isto é:}$$

$$B(n, d) \leq q B(n-1, d)$$

### Teorema 1.7.6

Se  $n \geq \frac{qd - 1}{q - 1}$ , o número de dígitos de verificação requeridos para obter peso mínimo  $d$  em um código linear de comprimento  $n$  é pelo menos

$$\frac{qd - 1}{q - 1} - 1 - \log_q d .$$

### Demonstração:

Consideremos um código  $[i, k, d]$ .

Usando o Lema 1.7.4 temos que

$$d \leq \frac{i(q-1)q^{k-1}}{q^k - 1} \Rightarrow d(q^k - 1) \leq i(q-1)q^{k-1} \Rightarrow$$

$$\Rightarrow dq^k - d \leq iq^k - iq^{k-1} \Rightarrow dq^k - iq^k + iq^{k-1} \leq d \Rightarrow$$

$$\Rightarrow q^{k-1}(dq + i - iq) \leq d \Rightarrow q^k(dq + i - iq) \leq qd$$

e se  $dq + i - iq > 0$ , então,  $q^k \leq \frac{qd}{dq + i - iq}$ .

Como  $q^k = B(i, d)$  então,  $q^k = B(i, d) \leq \frac{qd}{dq + i - iq}$ .

Escolhendo  $i$  tal que  $\frac{qd - 1}{q - 1} = i + f$  onde  $i$  é um inteiro e

$0 \leq f < 1$ , temos

$$qd - 1 = (q - 1)i + (q - 1) \Rightarrow qd - i(q - 1) = 1 + (q - 1)$$

Então,

$$q^k = B(i, d) \leq \frac{qd}{qd + i - iq} = \frac{qd}{1 + f(q-1)} \quad (15)$$

Se  $n \geq i$ , por  $(n - i - 1)$  aplicações do Lema 1.7.5, temos

$$B(n, d) \leq q^{n-i} B(i, d)$$

Usando (15) vem que

$$\begin{aligned} B(n, d) &\leq q^{n-i} B(i, d) \leq \frac{q^{n-i} \cdot qd}{1 + (q-1)f} = \frac{q^n - \frac{qd-1}{q-1} + f}{1 + (q-1)f} \cdot qd = \\ &= \frac{q^n - \frac{qd-1}{q-1} \cdot q^f \cdot qd}{1 + (q-1)f} \end{aligned} \quad (16)$$

Para simplificar (16) mostremos que  $q^f \leq 1 + f(q-1)$ .  
Considera-se a função  $F(q) = 1 + f(q-1) - q^f$ .

Esta função é contínua e diferenciável, então,

$$\frac{dF(q)}{dq} = f - f q^{f-1} = f(1 - q^{f-1}) = f \left(1 - \frac{1}{q^{1-f}}\right)$$

Como  $\frac{1}{q^{1-f}} \leq 1 \quad \forall q \geq 1$  e  $0 \leq f < 1$  temos que

$$f(1 - q^{f-1}) \geq 0 \quad \text{isto é} \quad \frac{dF(q)}{dq} \geq 0, \text{ portanto}$$

$F(q)$  é crescente.

Mas  $F(1) = 0$  e  $\forall q \geq 1 \quad F(q) \geq F(1) \Rightarrow 1 + f(q-1) - q^f \geq 0 \Rightarrow$   
 $\Rightarrow 1 + f(q-1) \geq q^f$ .

Portanto,  $q^f \leq 1 + f(q-1)$ . Substituindo em (16) temos

$$B(n, d) \leq \frac{q^n - \frac{qd-1}{q-1} \cdot [1 + f(q-1)] qd}{1 + f(q-1)} = q^n - \frac{qd-1}{q-1} \cdot qd$$

isto é

$$B(n, d) \leq q^n - \frac{qd-1}{q-1} \cdot qd$$

Desde que  $B(n, d) = q^k$  para o código com máxima distância mínima onde  $K$  é o número de símbolos de informação para aquele código, temos, então,

$$q^k \leq q^n - \frac{qd-1}{q-1} qd$$

tomando logarítmo com base  $q$  , temos que

$$K \leq n - \frac{qd - 1}{q - 1} + 1 + \log_q d$$

Como  $n \geq \frac{qd - 1}{q - 1}$  , temos, que o número de dígitos de verificação

$n - k$  será

$$n - k \geq \frac{qd - 1}{q - 1} - 1 - \log_q d$$

□

### OBSERVAÇÃO:

Se  $d$  é muito grande, os últimos dois termos na expressão acima podem ser desprezados.

### Exemplo 1.7.5

Seja  $n = 4$  ,  $q = 3$  e  $d = 3$  . Se  $n \geq \frac{qd - 1}{q - 1} \Rightarrow 4 \geq 4$ .

Então  $n - k \geq \frac{qd - 1}{q - 1} - 1 - \log_q d \Rightarrow n - k \geq 4 - 1 - \log_3 3 =$

$$= 2 \Rightarrow n - k \geq 2$$

Portanto, o código necessita de pelo menos 2 dígitos de verificação de paridade.

Provaremos no Teorema seguinte o limite superior de Hamming sobre  $d$  .

### Teorema 1.7.7

Para qualquer código linear  $[n,k]$  com peso mínimo maior ou igual a  $2t + 1$  , o número de dígitos de verificação satisfaz

$$n - k \geq \log_q [1 + \binom{n}{1} (q - 1) + \binom{n}{2} (q - 1)^2 + \dots + \binom{n}{t} (q - 1)^t] .$$

### Demonstração:

Consideremos um código linear  $[n,k]$  .

Se o código é para corrigir todas as combinações de  $t$  ou menos erros, então todos os vetores de peso menor ou igual a  $t$  devem ser "coset líderes". Mas o número de "cosets" é  $q^{n-k}$  . Assim, o número de vetores de peso menor ou igual a  $t$  deve ser não maior que o número de "cosets", isto é:

$$q^{n-k} \geq 1 + \binom{n}{1} (q-1) + \binom{n}{2} (q-1)^2 + \dots + \binom{n}{t} (q-1)^t .$$

Tomando logaritmo vem que:

$$n - k \geq \log_q [1 + \binom{n}{1} (q-1) + \binom{n}{2} (q-1)^2 + \dots + \binom{n}{t} (q-1)^t] \quad \square$$

### Teorema 1.7.8

(O limite de Singleton.)

Se  $C$  é um código linear  $[n, k, d]$ , então  $n - k \geq d - 1$ .

### Demonstração:

Uma palavra código com somente um dígito não nulo de informação tem peso no máximo  $n - k + 1$ . Assim

$$d \leq n - k + 1 \quad \text{ou}$$

$$n - k \geq d - 1$$

### Exemplo 1.7.6

Seja o código linear binário  $[6, 3, 3]$ , então

$$n - k \geq d - 1 \Rightarrow 6 - 3 \geq 3 - 1 \Rightarrow 3 > 2$$

Este Teorema prova um limite superior para o tamanho do código com uma dada distância mínima. No Teorema seguinte provaremos um limite inferior que diz que bons códigos lineares existem.

### Teorema 1.7.9

(Varsharmov - Gilbert.)

É possível construir um  $[n, k]$  código com distância mínima pelo menos  $d$  para o qual a seguinte inequação vale:

$$\sum_{i=0}^{d-2} \binom{n}{i} (q-1)^i \geq q^{n-k}$$

### Demonstração

Pelo Teorema 1.3.2, se uma matriz  $H$ , de verificação de paridade, pode ser determinada de tal modo que nenhum conjunto de  $d - 1$  colunas, ou menos, é linearmente independente, o espaço nulo

da matriz é um código linear com distância mínima pelo menos  $d$ .

Isto sugere o seguinte método para a construção de um código com  $r$  símbolos de verificação de paridade e peso mínimo  $d$ .

Selecionar qualquer  $r$ -upla não nula como a primeira coluna de uma matriz de verificação de paridade. Então, selecionar qualquer  $r$ -upla não nula, exceto múltipla da primeira, como uma segunda coluna na matriz de verificação de paridade. A terceira coluna deve ser qualquer  $r$ -upla que não é uma combinação linear das duas primeiras. Em geral, a  $i$ -ésima coluna é escolhida como qualquer  $r$ -upla que não é combinação linear de quaisquer  $d - 2$ , ou menos colunas anteriores.

Esta construção assegura que nenhuma combinação linear de  $d - 1$  colunas, ou menos, será zero.

Assim, o conjunto de todas as combinações lineares de  $d - 2$  ou menos, colunas não inclui todas as  $r$ -uplas, outra coluna pode ser adicionada.

No pior caso possível, todas estas combinações lineares podem ser distintas. Há  $q - 1$  possíveis coeficientes não nulos, e assim, há

$$\binom{j-1}{1} (q - 1) + \binom{j-1}{2} (q - 1)^2 + \dots + \binom{j-1}{d-2} (q - 1)^{d-2} \quad (17)$$

combinações lineares de  $d - 2$ , ou menos, colunas do total de  $j - 1$  colunas. Se isto é menor que o número total de  $r$ -uplas, então, existe certamente mais uma coluna que pode ser adicionada a matriz. Isto é, se

$$\binom{j-1}{1} (q - 1) + \binom{j-1}{2} (q - 1)^2 + \dots + \binom{j-1}{d-2} (q - 1)^{d-2} < q^r - 1 \quad (18)$$

existe um código com  $j$  dígitos e no máximo  $r$  dígitos de verificação de paridade (e portanto pelo menos  $k = j - r$  dígitos de informação) com distância mínima  $d$ . O código é o espaço nulo da  $r \times j$  matriz que é formada das colunas escolhidas. Agora, seja  $n$  o maior valor de  $j$  para o qual vale a inequação (18). Então, existe um  $[n, k]$  código com distância mínima  $d$  que satisfaz a inequação

$$\binom{n}{1} (q - 1) + \binom{n}{2} (q - 1)^2 + \dots + \binom{n}{d-2} (q - 1)^{d-2} \geq q^r - 1$$

fazendo  $r = n - k$  temos:

$$1 + \binom{n}{1} (q - 1) + \binom{n}{2} (q - 1)^2 + \dots + \binom{n}{d-2} (q - 1)^{d-2} \geq q^{n-k}$$

ou seja

$$\sum_{i=0}^{d-2} \binom{n}{i} (q-1)^i \geq q^{n-k} \quad (19)$$

### Exemplo 1.7.7

Vamos construir um código linear ternário  $[n, k]$  com distância mínima 3 e que tenha 2 dígitos de verificação de paridade, isto é,  $q = 3$ ,  $d = 3$  e  $n - k = 2$ .

A matriz de verificação de paridade  $H$  é uma  $2 \times n$  matriz. As 2-uplas são: 00 ; 01 ; 02 ; 10 ; 11 ; 12 ; 20 ; 21 ; 22 .

Escolhendo as colunas de  $H$  :

$$h_1 = 10$$

$$h_2 = 01$$

$h_3$  não pode ser 20 nem 02 pois são múltiplas de  $h_1$  e  $h_2$ , respectivamente. Desta forma, temos que  $h_3$  pode ser 11 ou 12 ou 21 ou 22 .

Se  $h_3 = 11$ , então,  $h_4$  não pode ser 20 nem 02 nem 22, pois são múltiplas de  $h_1$ ,  $h_2$  e  $h_3$ , respectivamente.

Assim,  $h_4$  pode ser 12 ou 21. Escolhemos  $h_4 = 12$ . Como  $n = 4$  é o maior valor de  $j$  para o qual vale a inequação (18), existe, então, o código  $[4, 2]$  com as especificações acima.

Portanto:

$$H = \begin{pmatrix} 1011 \\ 0112 \end{pmatrix}, \text{ ou seja } H = \begin{pmatrix} 1110 \\ 1201 \end{pmatrix}$$

Os vetores código são dados no Exemplo 1.3.2 .

### OBSERVAÇÃO:

Para outras escolhas de  $h_3$  e  $h_4$  obteremos códigos equivalentes.

No próximo Capítulo, estudaremos os Códigos Lineares Corretores de Pedacos de Erro.



## CAPÍTULO II

### ESTUDO DOS CÓDIGOS LINEARES CORRETORES DE PEDAÇOS DE ERRO

#### 2.1 - CÓDIGOS CORRETORES DE PEDAÇOS DE ERRO

No Capítulo I, os códigos estudados corrigem os erros que ocorrem aleatoriamente. Mas, em certos sistemas de comunicação, os canais são afetados por distúrbios que produzem erros predominantemente reunidos em pedaços. Esses distúrbios que introduzem pedaços de erro usualmente operam de uma maneira tal que, sobre um comprimento dado, alguns dígitos são recebidos corretamente enquanto outros são errados. Por exemplo, em linhas telefônicas o som de um raio, ou um distúrbio elétrico provocado pelo homem frequentemente afetam vários dígitos, adjacentes dos dígitos transmitidos, ou em fitas magnéticas, os defeitos usualmente afetam mais que um dígito. Nestes casos, em geral, os códigos corretores de erros aleatórios não são eficientes para a correção de pedaços de erros, é necessário se ter códigos específicos para este fim. Para construir estes códigos apresentamos aqui a definição de um pedaço.

#### Definição 2.1.1

Um pedaço de comprimento  $b$  é um vetor cujas únicas compo

nentes não nulas estão entre  $b$  posições sucessivas, a primeira e a última das quais são não nulas.

### Exemplo 2.1.1

Uma sequência de erro no sistema binário pode ter a seguinte aparência:

00010110011000010111100  $b = 18$

Nesta sequência temos  $b = 18$ .

### Definição 2.1.2

Um código linear  $[n, k]$  que é capaz de corrigir todos os pedaços de erro de comprimento menor ou igual a  $b$  (mas, nem todos os pedaços de comprimento  $b + 1$ ) é chamado um **código corretor-de- $b$ -pedaços-de-erro** ou o código é dito ter  $b$ -capacidade de corrigir pedaços de erro.

Vejamos algumas restrições sobre  $n-k$  para um dado  $b$ , ou restrições sobre  $b$  para um dado  $n-k$ .

### Teorema 2.1.1

O número de dígitos de verificação de paridade de um código linear  $[n, k]$  que não tem pedaço de comprimento menor ou igual a  $b$  como um vetor código é pelo menos  $b$ , isto é,  $n-k \geq b$ .

### Demonstração:

Consideremos o conjunto dos vetores cujas componentes não nulas são confinadas às primeiras  $b$  posições. Há um total de  $q^b$  destes vetores. Quaisquer dois vetores deste conjunto não podem estar num mesmo "coset" de um arranjo padrão para este código, porque se eles estão, sua diferença, que é um pedaço de comprimento menor ou igual a  $b$ , será um vetor código. Portanto, estes  $q^b$  vetores devem estar em  $q^b$  "coset" distintos. Como há um total de  $q^{n-k}$  "cosets" para um código  $[n, k]$ , temos que  $n-k$  deve ser pelo menos igual a  $b$ , isto é:

$$n - k \geq b$$

□

### Teorema 2.1.2

Para detectar todos os pedaços de comprimento menor ou igual a  $b$  com um código linear de comprimento  $n$ , são necessários e suficientes  $b$  dígitos de verificação de paridade.

#### Demonstração:

No Teorema 2.1.1, vimos que são necessários pelo menos  $b$  dígitos de verificação de paridade para um código linear  $[n, k]$  detectar todos os pedaços de comprimento menor ou igual a  $b$ . Portanto, a condição necessária segue.

Para demonstrarmos a condição suficiente, consideremos o seguinte fato: Todos os pedaços de comprimento menor ou igual a  $b$  são detectados por um código no qual os primeiros  $n-b$  dígitos são dígitos de informação e os últimos  $b$  dígitos são dígitos de verificação de paridade. Todos esses dígitos são escolhidos de modo tal que, a soma de cada um dos  $b$  conjuntos de dígitos que contém "um" nas primeiras  $b$  posições, com todo o  $b$ -ésimo dígito seguinte é zero. Portanto, no máximo um dos dígitos não nulos de um pedaço de comprimento menor ou igual a  $b$  pode aparentar alguma verificação de paridade peculiar e desta forma, todo o pedaço será detectado juntamente com muitos outros vetores de erro.

□

### Teorema 2.1.3 [12]

(1) Para corrigir todos os pedaços de erro de comprimento menor ou igual a  $b$ , um código linear deve ter pelo menos  $2b$  dígitos de verificação de paridade.

(2) Para corrigir todos os pedaços de erro de comprimento menor ou igual a  $b$  e simultaneamente detectar todos os pedaços de erro de comprimento menor ou igual a  $\ell \geq b$ , o código deve ter pelo menos  $b + \ell$  dígitos de verificação de paridade.

#### Demonstração:

(1) Suponhamos que existe um pedaço  $v$  de comprimento menor ou igual a  $2b$  como um vetor código. Este vetor pode ser escrito como um vetor diferença de dois pedaços  $u$  e  $w$  de comprimento menor ou igual a  $b$  (exceto o caso degenerado em que  $v$  é um pedaço consistindo de um único elemento não nulo). Para este código linear

$u$  e  $w$  devem estar num mesmo "coset" do arranjo padrão.

Se um destes dois vetores é usado com um "coset líder" (vetor de erro corrigível), o outro será um pedaço de erro incorrigível. Como resultado, este código não poderá corrigir todos os pedaços de erro de comprimento menor ou igual a  $b$ . Portanto, nenhum pedaço de erro de comprimento menor ou igual a  $2b$  pode ser um vetor código. Logo, pelo Teorema 2.1.1, para corrigir todos os pedaços de erro de comprimento menor ou igual a  $b$ , um código linear deve ter pelo menos  $2b$  dígitos de verificação de paridade.

(2) Analogamente, todo pedaço de comprimento menor ou igual a  $b + \ell$  pode ser escrito como a diferença de um pedaço de comprimento menor ou igual a  $\ell$  e um pedaço de comprimento menor ou igual a  $b$ .

Se o código é para corrigir simultaneamente pedaços de comprimento menor ou igual a  $b$  e para detectar todos os pedaços de comprimento  $\ell$ , então, o pedaço de comprimento  $b$  e o pedaço de comprimento  $\ell$  devem estar em diferentes "cosets", e sua soma não deve ser uma palavra código. Logo, pelo Teorema 2.1.1, Para corrigir todos os pedaços de erro de comprimento menor ou igual a  $b$  e simultaneamente detectar todos os pedaços de erro de comprimento menor ou igual a  $\ell \geq b$ , o código deve ter pelo menos  $b + \ell$  dígitos de verificação de paridade.  $\square$

Um outro limite inferior sobre o número de verificações de paridade requerido para um código linear que corrige todos os pedaços de comprimento menor ou igual a  $b$  é provado no Teorema seguinte:

#### Teorema 2.1.4

O número de dígitos de verificação de paridade em qualquer código linear de comprimento  $n$  que corrige todos os pedaços de comprimento menor ou igual a  $b$  é pelo menos

$$b - 1 + \log_q [ (q - 1) (n - b + 1) + 1 ]$$

#### Demonstração:

Notemos que, cada pedaço de comprimento menor ou igual a  $b$  deve estar em "coset" diferente, e o número de "cosets" é pelo menos tão grande quanto o número de pedaços de erro de comprimento menor ou igual a  $b$ . Há  $(q - 1)n$  pedaços de comprimento 1 (um)

diferentes, desde que a cada componente não nula possa aparecer em qualquer um dos  $n$  símbolos e qualquer dos  $q-1$  elementos do corpo. Há  $(q-1)^2 (n-1)$  possíveis pedaços de comprimento 2 (dois), desde que cada duas componentes não nulas possam ser algum dos  $q-1$  elementos não nulos do corpo, e o pedaço pode começar em qualquer posição exceto a última. Para pedaços de comprimento  $i > 2$ , há,  $(q-1)^2 q^{i-2} (n-i+1)$  vetores desde que há  $q-1$  escolhas para cada dígito inicial e final e  $q$  escolhas para os dígitos entre eles e  $(n-i+1)$  possíveis posições intercaladas. O número total de vetores de erro, incluindo o vetor nulo é, portanto

$$1 + n(q-1) + \sum_{i=2}^b (q-1)^2 q^{i-2} (n-i+1)$$

isto é:

$$\begin{aligned} & 1 + n(q-1) + (q-1)^2 \sum_{i=2}^b (n-i+1) q^{i-2} = \\ & = 1 + n(q-1) + (q-1)^2 \sum_{j=0}^{b-2} [(n-1)-j] q^j = \\ & = 1 + n(q-1) + (q-1)^2 (n-1) \sum_{j=0}^{b-2} q^j - \\ & - (q-1)^2 q \sum_{j=0}^{b-2} j q^{j-1} \end{aligned} \quad (20)$$

Usando as duas identidades

$$\sum_{i=0}^n x^i = \frac{1-x^{n+1}}{1-x}$$

e

$$\sum_{i=0}^n i x^{i-1} = \frac{d}{dx} \left( \frac{1-x^{n+1}}{1-x} \right)$$

e substituindo em (20) a expressão para o número total de vetores de erro pode ser simplificada como

$$\begin{aligned} & 1 + n(q-1) + (n-1)(q-1)^2 \left[ \frac{1-q^{b-1}}{1-q} \right] - q(q-1)^2 \frac{d}{dq} \left[ \frac{1-q^{b-1}}{1-q} \right] = \\ & = 1 + n(q-1) - (n-1)(q-1)^2 \left[ \frac{1-q^{b-1}}{q-1} \right] + q(q-1)^2 \frac{d}{dq} \left[ \frac{1-q^{b-1}}{q-1} \right] = \\ & = 1 + n(q-1) - (n-1)(q-1)(1-q^{b-1}) + \\ & + q(q-1)^2 \left[ \frac{-(b-1)q^{b-2}(q-1) - 1 + q^{b-1}}{(q-1)^2} \right] = \end{aligned}$$

$$\begin{aligned}
&= 1 + n(q-1) - (n-1)(q-1)(1-q^{b-1}) + q[-(b-1)(q-1)q^{b-2} - 1 + q^{b-1}] = \\
&= 1 + n(q-1) + n(q-1)q^{b-1} - q^b + q^{b-1} - n(q-1) + q - 1 - (b-1)(q-1)q^{b-1} - \\
&\quad - q + q^b = \\
&= q^{b-1} [n(q-1) - (b-1)(q-1) + 1] = q^{b-1} [(q-1)(n-b+1) + 1].
\end{aligned}$$

Como o número de "cosets" é pelo menos tão grande quanto o número de pedaços de erro de comprimento menor ou igual a  $b$ , então, temos

$$q^{n-k} \geq q^{b-1} [(q-1)(n-b+1) + 1]$$

tomando logaritmo temos

$$n - k \geq b - 1 + \log_q [(q-1)(n-b+1) + 1] \quad \square$$

Um limite semelhante ao do Teorema 1.7.9 é provado no Teorema seguinte para códigos corretores de pedaços de erro.

### Teorema 2.1.5

Existe um código linear  $[n, k]$  que corrige qualquer pedaço único de comprimento menor ou igual a  $b_g$  ( $< \frac{n}{2}$ ), para o qual a inequação é satisfeita

$$n - k \leq 2 b_g + \log_q [(q-1)(n - 2 b_g - 1) + 1].$$

### Demonstração:

Suponhamos que a matriz  $H$  de verificação de paridade está sendo construída para um código que corrige qualquer pedaço único de comprimento menor ou igual a  $b$ . É necessário e suficiente que nenhum vetor código consista da soma de dois pedaços de comprimento menor ou igual a  $b$ . Assim, pelo Teorema 1.3.2, é necessário e suficiente que nenhuma combinação linear envolvendo dois conjuntos de  $b$  ou menos colunas consecutivas de  $H$  seja zero. Suponhamos que  $n-1$  colunas  $h_1, h_2, \dots, h_{n-1}$  foram escolhidas. Então, qualquer coluna  $h_n$  pode ser adicionada, com a condição de que não seja uma combinação linear das últimas  $b-1$  colunas  $h_{n-b+1}, \dots, h_{n-1}$  e qualquer conjunto de  $b$  colunas consecutivas entre as  $h_1, h_2, \dots, h_{n-b}$ ; isto é,

$$h_n \neq (a_{n-1} h_{n-1} + \dots + a_{n-b+1} h_{n-b+1}) + (b_{n-b-i} h_{n-b-i} + \dots +$$

$$+ b_{n-b-i-b+1} h_{n-b-i+b+1} ) \quad (21)$$

O pior caso concebível seria o de que, para cada escolha de coeficientes  $a_j$  e  $b_j$  se tenha uma soma distinta na equação (21). Há  $q^{b-1}$  escolhas para os  $a_j$ . Os coeficientes  $b_j$  formam um pedaço de comprimento menor ou igual a  $b$  num vetor de comprimento  $n - b$ , e pelo argumento do Teorema 2.1.4, podemos ver que há

$$q^{b-1} [ (q-1) (n-2b+1) + 1 ]$$

escolhas para estes coeficientes, incluindo o caso em que eles são todos nulos. Assim, o número total de escolhas dos coeficientes é  $q^{b-1} [ (q-1) (n - 2b + 1) + 1 ]$ . Se o número de vetores possíveis de comprimento  $n - k$  é maior que este, certamente de verá existir um vetor  $h_n$  satisfazendo a inequação (21) para todas as escolhas dos coeficientes, e assim, é possível construir um código de comprimento  $n$  que corrige todos os pedaços de comprimento menor ou igual a  $b$ . Desde que existam  $q^{n-k}$  vetores de comprimento  $n - k$ , isto é possível se

$$q^{n-k} > q^{2(b-1)} [ (q-1) (n - 2b + 1) + 1 ] .$$

Agora, seja  $b_g$  o maior valor de  $b$  satisfazendo esta inequação. Então, para  $b = b_g + 1$ , o oposto da inequação é satisfeita, isto é

$$q^{n-k} \leq q^{2b_g} [ (q-1) (n - 2b_g - 1) + 1 ]$$

tomando logaritmo, temos

$$n - k \leq 2b_g + \log_q [ (q-1) (n - 2b_g - 1) + 1 ] .$$

□

### Exemplo 2.1.2

Vamos construir um código linear binário  $[n, k]$  que tenha 3 dígitos de verificação de paridade com pedaço único de comprimento menor ou igual a 2. Isto é:  $n - k = 3$ ,  $q = 2$ ;  $b_g = 2$ .

As 8 3-uplas são: 000 ; 100 ; 010 ; 001 ; 110 ; 101 ; 011 ; 111 .

$$h_1 = 100$$

$$h_2 = 010$$

$$h_3 = 001$$

$h_4$  não pode ser 001 nem 110 pois são combinações lineares de  $h_3$  e  $h_1 + h_2$ . Portanto,  $h_4$  pode ser: 011 ou 111 ou 101. Se  $h_4 = 011$ , então,  $h_5$  não pode ser 011

nem 110 pois são combinações lineares de  $h_4$  e  $h_1 + h_2$ .  
 Portanto,  $h_5$  pode ser 101 ou 111. Se  $h_5 = 101$ , então,  
 $h_6$  não pode ser 101 nem 010. Portanto,  
 $h_6 = 111$ .

Assim,  $n = 6$  e  $k = 3$ . Logo, existe o código [6,3] com  
 as especificações acima, e

$$H = \begin{pmatrix} 100011 \\ 010101 \\ 001111 \end{pmatrix} \quad \text{ou} \quad H = \begin{pmatrix} 011100 \\ 101010 \\ 111001 \end{pmatrix}$$



## 2.2 - RESULTADOS SOBRE O PÊSO DOS PEDAÇOS

Consideremos  $W_b$  o pêsso total de todos os pedaços de comprimento  $b$  no espaço de todas as  $n$ -uplas.

Nesta seção obteremos resultados com respeito ao pêsso de todos os pedaços de comprimento  $b$  (fixo) e com respeito ao pêsso de todos os pedaços de comprimento menor ou igual a  $b$  [15].

No Lema seguinte obteremos o número de pedaços de comprimento  $b$  com pêsso  $W$ .

### Lema 2.2.1

O número total de pedaços de comprimento  $b > 1$  com pêsso  $W$  no espaço de todas as  $n$ -uplas é

$$\binom{b-2}{W-2} (n - b + 1) (q - 1)^W \quad (22)$$

### Demonstração:

Consideremos um pedaço de comprimento  $b$ . Suas únicas componentes não nulas estão entre  $b$  componentes sucessivas, a primeira e a última das quais são não nulas. Cada uma destas, a primeira e a última componentes, pode ser quaisquer um dos  $q - 1$  elementos não nulos do corpo. Como estamos considerando pedaços de comprimento  $b$  que são de pêsso  $W$ , portanto, entre  $b - 2$  componentes restantes  $W - 2$  componentes tem que ser não nulas, que podem ser escolhidas de  $\binom{b-2}{W-2}$  maneiras e cada uma destas  $W - 2$  componentes pode assumir  $q - 1$  valores não nulos.

Além disso, há  $n - b + 1$  posições possíveis começando por um pedaço de comprimento  $b$  em uma  $n$ -upla. Portanto, o número total de pedaços de comprimento  $b > 1$  com pêsso  $W$  é

$$(q-1)^2 \binom{b-2}{W-2} (q-1)^{W-2} (n - b + 1) = \binom{b-2}{W-2} (q-1)^W (n - b + 1).$$

□

### Exemplo 2.2.1

Consideremos o código linear binário do Exemplo 1.1.1 com  $b = 3$  e  $W = 2$ . Então, o número total de pedaços de comprimento  $b = 3$  e com pêsso  $W = 2$  é:

$$\binom{b-2}{W-2} (n - b + 1) (q-1)^W = \binom{1}{0} (5 - 3 + 1) = 3.$$

No Teorema seguinte obteremos  $W_b$  em termos de  $n$ ,  $q$  e  $b$ .

### Teorema 2.2.1

Para  $n \geq b$

$$W_1 = n (q-1) \quad (23)$$

e

$$W_b = (n - b + 1) [b (q-1) + 2] (q-1)^2 q^{b-3}, \quad (24)$$

para  $b > 1$ .

### Demonstração:

O valor de  $W_1$  segue considerando todos os pedaços de comprimento "um" cujo número é exatamente  $n(q-1)$ .

Para  $b > 1$ , usando o Lema 2.1.1, o peso total dos pedaços de comprimento  $b$  é dado por:

$$\begin{aligned} & \sum_{W=2}^b W \binom{b-2}{W-2} (n - b + 1) (q-1)^W = \\ & = (n - b + 1) (q-1)^2 \sum_{W=2}^b W \binom{b-2}{W-2} (q-1)^{W-2} = \\ & = (n - b + 1) (q-1)^2 \sum_{j=0}^{b-2} \binom{b-2}{j} (j+2) (q-1)^j = \\ & = (n - b + 1) (q-1)^2 \left[ \frac{1}{q-1} \sum_{j=0}^{b-2} \binom{b-2}{j} (j+2) (q-1)^{j+1} \right] = \\ & = (n - b + 1) (q-1)^2 \left[ \frac{1}{q-1} \sum_{j=0}^{b-2} \binom{b-2}{j} \frac{d}{dq} (q-1)^{j+2} \right] = \\ & = (n - b + 1) (q-1)^2 \left[ \frac{1}{q-1} \frac{d}{dq} \sum_{j=0}^{b-2} \binom{b-2}{j} (q-1)^{j+2} \right] = \\ & = (n - b + 1) (q-1) \frac{d}{dq} \left[ (q-1)^2 \sum_{j=0}^{b-2} \binom{b-2}{j} (q-1)^j \right] \end{aligned} \quad (25)$$

Usando a Série Binomial  $(a + b)^n = \sum_{m=0}^n \binom{n}{m} a^{n-m} b^m$ ,

fazendo  $a = 1$  e  $b = q - 1$  temos  $[1 + (q-1)]^n = \sum_{m=0}^n \binom{n}{m} (q-1)^m$ , que

substituindo em (25) obtemos:

$$\begin{aligned}
&= (n - b + 1) (q-1) \frac{d}{dq} \left[ (q-1)^2 [1 + (q-1)]^{b-2} \right] = \\
&= (n - b + 1) (q-1) \frac{d}{dq} \left[ (q-1)^2 q^{b-2} \right] = \\
&= (n - b + 1) (q-1) \left[ 2(q-1) q^{b-2} + (q-1)^2 (b-2) q^{b-3} \right] = \\
&= (n - b + 1) (q-1)^2 \left[ 2 q^{b-2} + b q^{b-2} - b q^{b-3} - 2 q^{b-2} + 2 q^{b-3} \right] = \\
&= (n - b + 1) (q-1)^2 q^{b-3} \left[ b(q-1) + 2 \right]
\end{aligned}$$

Portanto,

$$W_b = (n - b + 1) (q-1)^2 [ b (q-1) + 2 ] q^{b-3}$$

□

No teorema seguinte obteremos uma relação de recorrência em  $W_b + 1$ .

### Teorema 2.2.2

Para  $n > 1$

$$n W_2 = 2 (n - 1) (q - 1) W_1 \quad (26)$$

e para  $n > b > 1$

$$(n - b + 1) [ b(q-1) + 2 ] W_{b+1} = (n - b) [ b(q-1) + q + 1 ] q W_b \quad (27)$$

### Demonstração:

Para  $b > 1$  da equação (24) obtemos

$$\begin{aligned}
W_2 &= (n - 1) [ 2(q-1) + 2 ] (q-1)^2 q^{-1} = \\
&= (n - 1) 2(q-1)^2
\end{aligned}$$

ou

$$n W_2 = 2(n - 1) (q-1) (q-1) n$$

Portanto,

$$n W_2 = 2(n - 1) (q-1) W_1$$

No Teorema 2.2.1 fazendo  $b = b + 1$  e substituindo na equação (24) obtemos

$$\begin{aligned} W_{b+1} &= (n - b - 1 + 1) [ (b+1) (q-1) + 2 ] (q-1)^2 q^{b-2} \\ &= (n - b) [ b(q-1) + q + 1 ] (q-1)^2 q^{b-2} \end{aligned}$$

ou

$$(n - b + 1) [ b(q-1) + 2 ] W_{b+1} =$$

$$= (n - b) [ b(q-1) + q + 1 ] q(q-1)^2 q^{b-3} (n-b+1) [ b(q-1) + 2 ]$$

portanto,

$$(n - b + 1) [ b(q-1) + 2 ] W_{b+1} =$$

$$= (n - b) [ b(q-1) + q + 1 ] q W_b \quad \square$$

Denotaremos por  $W_b^T$  o pêsô total de todos os pedaços de comprimento menor ou igual a  $b$  no espaço de todas as  $n$ -uplas.

No Teorema seguinte, obteremos  $W_b^T$  em termos de  $n$ ,  $q$  e  $b$ .

### Teorema 2.2.3

Para  $n \geq b$

$$W_b^T = b(n - b + 1) q^b + [ n - 2b(n - b + 1) ] q^{b-1} + (n-b)(b-1) q^{b-2} \quad (28)$$

### Demonstração:

No Teorema 2.2.1 fazendo  $b = j$  e escrevendo agora  $W_b^T$  em termos de  $W_j$  obtemos:

$$\begin{aligned} W_b^T &= \sum_{j=1}^b W_j \\ &= n(q-1) + \sum_{j=2}^b (n-j+1) [ j(q-1) + 2 ] (q-1)^2 q^{j-3} \\ &= n(q-1) - (q-1)^3 \sum_{j=2}^b j^2 q^{j-3} + (q-1)^2 [ (n+1)(q-1) - 2 ] \sum_{j=2}^b j q^{j-3} + \\ &\quad + 2(n+1)(q-1)^2 \sum_{j=2}^b q^{j-3} \quad (29) \end{aligned}$$

Calculando separadamente os três somatôrios

$$1a) \sum_{j=2}^b q^{j-3} = q^{-1} + \sum_{j=3}^b q^{j-3} = q^{-1} + [ 1 + q + q^2 + q^3 + \dots + q^{b-3} ] =$$

$$= q^{-1} + \frac{q^{b-2} - 1}{q - 1}$$

Portanto,

$$\sum_{j=2}^b q^{j-3} = \frac{1}{q} + \frac{q^{b-2} - 1}{q - 1} \quad (30)$$

$$\begin{aligned} 2a) \quad \sum_{j=2}^b j q^{j-3} &= 2q^{-1} + 3q^0 + 4q^1 + 5q^2 + 6q^3 + \dots + bq^{b-3} = \\ &= 2q^{-1} + (2+1)q^0 + (2+2)q^1 + (2+3)q^2 + \dots + (2+b-2)q^{b-3} = \\ &= \sum_{i=0}^{b-2} (2+i)q^i = \sum_{i=0}^{b-2} 2q^i + \sum_{i=0}^{b-2} iq^i = \\ &= 2(q^{-1} + q^0 + q^1 + q^2 + \dots + q^{b-3}) + \sum_{i=0}^{b-2} iq^i = \\ &= 2\left(\frac{1}{q} + \frac{q^{b-2} - 1}{q-1}\right) + \sum_{i=0}^{b-2} iq^i = 2\left(\frac{q^{b-1} - 1}{q(q-1)}\right) + \sum_{i=0}^{b-2} iq^i \quad (I) \end{aligned}$$

Usando a identidade

$$\sum_{i=0}^n ix^{i-1} = \frac{d}{dx} \left[ \frac{1 - x^{n+1}}{1 - x} \right]$$

em (I) obtemos:

$$\begin{aligned} &= 2 \frac{q^{b-1} - 1}{q(q-1)} + \frac{d}{dq} \left[ \frac{1 - q^{b-1}}{1 - q} \right] = \\ &= 2 \frac{q^{b-1} - 1}{q(q-1)} + \frac{bq^{b-2}(q-1) + q^{b-2} - 2q^{b-1} + 1}{(q-1)^2} = \\ &= \frac{2q^{b-2}}{q-1} - \frac{2}{q(q-1)} + \frac{bq^{b-2}}{q-1} + \frac{q^{b-2} - 2q^{b-1} + 1}{(q-1)^2} = \\ &= \frac{bq^{b-2}}{q-1} - \frac{2}{q(q-1)} + \frac{2q^{b-1} - 2q^{b-2} + q^{b-2} - 2q^{b-1} + 1}{(q-1)^2} = \\ &= \frac{bq^{b-2}}{q-1} - \frac{2}{q(q-1)} + \frac{1 - q^{b-2}}{(q-1)^2} \end{aligned}$$

Portanto,

$$\sum_{j=2}^b j q^{j-3} = \frac{bq^{b-2}}{q-1} - \frac{2}{q(q-1)} + \frac{1 - q^{b-2}}{(q-1)^2} \quad (31)$$

$$\begin{aligned}
3a) \quad \sum_{j=2}^b j^2 q^{j-3} &= q^{-2} \sum_{j=2}^b j j q^{j-1} = q^{-2} \sum_{j=2}^b j \frac{d}{dq} q^j = \\
&= q^{-2} \frac{d}{dq} \sum_{j=2}^b j q^j = q^{-2} \frac{d}{dq} \left[ q \sum_{j=2}^b j q^{j-1} \right] = \\
&= q^{-2} \frac{d}{dq} \left[ q \sum_{j=2}^b \frac{d}{dq} q^j \right] = \\
&= q^{-2} \frac{d}{dq} \left[ q \frac{d}{dq} \sum_{j=2}^b q^j \right] = \\
&= \frac{1}{q^2} \frac{d}{dq} \left[ q \frac{d}{dq} q^2 \sum_{j=2}^b q^{j-2} \right] = \\
&= \frac{1}{q^2} \frac{d}{dq} \left[ q \frac{d}{dq} \left( q^2 \sum_{i=0}^{b-2} q^i \right) \right] \quad (II)
\end{aligned}$$

Usando a identidade

$$\sum_{i=0}^n x^i = \frac{1 - x^{n+1}}{1 - x}$$

em (II) temos

$$\begin{aligned}
&= \frac{1}{q^2} \frac{d}{dq} \left[ q \frac{d}{dq} \left( q^2 \frac{1 - q^{b-1}}{1 - q} \right) \right] = \frac{1}{q^2} \frac{d}{dq} \left[ q \frac{d}{dq} \left( \frac{q^2 - q^{b+1}}{1 - q} \right) \right] = \\
&= \frac{1}{q^2} \frac{d}{dq} \left[ q \cdot \frac{[2q - (b+1)q^b](1-q) + q^2 - q^{b+1}}{(1-q)^2} \right] = \\
&= \frac{1}{q^2} \frac{d}{dq} \left[ \frac{2q^2 - (b+1)q^{b+1}}{1-q} + \frac{q^3 - q^{b+2}}{(q-1)^2} \right] = \\
&= \frac{1}{q^2} \left[ \frac{4q - 4q^2 - (b+1)^2 q^b + (b+1)^2 q^{b+1} + 2q^2 - (b+1)q^{b+1} + 3q^2 - (b+2)q^{b+1}}{(q-1)^2} + \right. \\
&\quad \left. + \frac{2(q^{b+2} - q^3)}{(q-1)^3} \right] \\
&= \frac{4}{q(q-1)^2} + \frac{1 - (b+1)^2 q^{b-2} + [(b+1)^2 - (2b+3)] q^{b-1}}{(q-1)^2} + \frac{2(q^b - q)}{(q-1)^3} \\
&= \frac{4}{q(q-1)^2} + \frac{b^2 q^{b-1} - (b^2 + 2b + 1) q^{b-2} + 1}{(q-1)^2} + \frac{2(q^b - q)}{(q-1)^3} - \frac{2q^{b-1}}{(q-1)^2}
\end{aligned}$$

Portanto,

$$\sum_{j=2}^b j^2 q^{j-3} = \frac{4}{q(q-1)^2} + \frac{b^2 q^{b-1} - (b^2 + 2b + 1) q^{b-2} + 1}{(q-1)^2} + \frac{2q(q^{b-2}-1)}{(q-1)^3} \quad (32)$$

Substituindo os resultados (30), (31) e (32) na equação (29), temos:

$$\begin{aligned} W_b^T &= n(q-1) - (q-1)^3 \left[ \frac{4}{q(q-1)^2} + \frac{b^2 q^{b-1} - (b+1) q^{b-2} + 1}{(q-1)^2} + \frac{2q(q^{b-2}-1)}{(q-1)^3} \right] + \\ &+ [(n+1)(q-1) - 2] (q-1)^2 \left[ \frac{bq^{b-2}}{q-1} - \frac{2}{q(q-1)} - \frac{q^{b-2}-1}{(q-1)^2} \right] + \\ &+ 2(n+1)(q-1)^2 \left[ \frac{1}{q} + \frac{q^{b-2}-1}{q-1} \right] \\ &= n(q-1) - (q-1)^3 \left[ \frac{4(q-1) + b^2(q-1)q^b - (b+1)^2(q-1)q^{b-1} + q(q-1) + 2q^2(q^{b-2}-1)}{q(q-1)^3} \right] + \\ &+ [(n+1)(q-1) - 2] (q-1)^2 \left[ \frac{b(q-1)q^{b-1} - 2(q-1) - q^{b-1} + q}{q(q-1)^2} \right] + \\ &+ 2(n+1)(q-1)^2 \left[ \frac{q^{b-1}-1}{q(q-1)} \right] \\ &= n(q-1) - \left[ \frac{4}{q} (q-1) + b^2(q-1)q^{b-1} - (b+1)^2(q-1)q^{b-2} + q-1 + 2q(q^{b-2}-1) \right] + \\ &+ [(n+1)(q-1) - 2] \left[ b(q-1)q^{b-2} - \frac{2}{q}(q-1) - q^{b-2} + 1 \right] + \\ &+ 2(n+1)(q-1)(q^{b-2} - q^{-1}) \\ &= n(q-1) - \frac{4}{q} (q-1) - b^2(q-1)q^{b-1} + (b+1)^2(q-1)q^{b-2} - q + 1 - \\ &- 2q(q^{b-2}-1) + (n+1)(q-1)^2 b q^{b-2} - \frac{2}{q} (n+1)(q-1)^2 - \\ &- (n+1)(q-1)q^{b-2} + (n+1)(q-1) - 2b(q-1)q^{b-2} + \frac{4}{q}(q-1) + \\ &+ 2(q^{b-2}-1) + 2(n+1)(q-1)q^{b-2} - \frac{2}{q}(n+1)(q-1) \end{aligned}$$

$$\begin{aligned}
W_b^T &= nq - n - b^2 q^b + b^2 q^{b-1} + (b+1)^2 q^{b-1} - (b+1)^2 q^{b-2} - q + 1 - 2q^{b-1} + 2q + \\
&+ (n+1) [ b q^b - 2b q^{b-1} + b q^{b-2} ] - 2nq + 4n - \frac{2n}{q} - 2q + 4 - \frac{2}{q} - \\
&- (n-1) [ q^{b-1} - q^{b-2} ] + nq - n + q - 1 - 2b [ q^{b-1} - q^{b-2} ] + 2q^{b-2} - 2 + \\
&+ 2(n+1) [ q^{b-1} - q^{b-2} ] - 2n - 2 + \frac{2n}{q} + \frac{2}{q} =
\end{aligned}$$

$$\begin{aligned}
&= q^b [-b^2 + b(n+1)] + q^{b-1} [b^2 + b^2 + 2b + 1 - 2 - 2bn - 2b - n - 1 - 2b + \\
&+ 2n + 2] + q^{b-2} [-b^2 - 2b - 1 + bn + b + n + 1 + 2b + 2 - 2n - 2] \\
&= b [ n - b + 1 ] q^b + [ 2b(b - n - 1) + n ] q^{b-1} + [ b(n - b + 1) - n ] q^{b-2}
\end{aligned}$$

$$W_b^T = b [ n - b + 1 ] q^b + [ n - 2b(n - b + 1) ] q^{b-1} + [(n-b)(b-1)] q^{b-2}$$

□

### OBSERVAÇÃO 1

Este resultado aparece em [15] e o somatório da equação (32) aqui desenvolvida, apresenta em [15], dois erros no resultado. Um erro de potência na segunda parcela e outro, erro de sinal, na terceira parcela da soma.

Muito embora esses erros não afetam o resultado do Teorema 2.2.3, qual seja, a equação (28).

### OBSERVAÇÃO 2

Da equação (28), podemos notar que

$$W_b^T - W_{b-1}^T = W_b$$

De fato, na equação (28) fazendo  $b = b - 1$  obtemos:

$$W_{b-1}^T = (b-1)(n-b+1+1) q^{b-1} + [n-2(b-1)(n-b+1+1)] q^{b-2} + [(b-1)(n-b+1+1)-n] q^{b-3}$$

Então,

$$\begin{aligned}
W_b^T - W_{b-1}^T &= q^b [b(n-b+1)] + q^{b-1} [n-2b(n-b+1) - (b-1)(n-b+1+1)] + \\
&+ q^{b-2} [b(n-b+1) - n - n + 2(b-1)(n-b+1+1)] - q^{b-3} [(b-1)(n-b+1+1) - n]
\end{aligned}$$



$$\begin{aligned}
&= q^b [b(n-b+1)] + q^{b-1} [n-2b(n-b+1) - (b-1)[(n-b+1) + 1]] + \\
&\quad + q^{b-2} [b(n-b+1) - 2n + 2(b-1)[(n-b+1) + 1]] - q^{b-3} [(b-1)[(n-b+1)+1]-n] \\
&= q^b [b(n-b+1)] + q^{b-1} [-2b(n-b+1) - (b-1)(n-b+1) - b + 1 + n] + \\
&\quad + q^{b-2} [b(n-b+1)+2(b-1)(n-b+1)+2b-2-2n] - q^{b-3} [(b-1)(n-b+1)+b-1-n] \\
&= q^b [b(n-b+1)] + q^{b-1} [-2b(n-b+1) - b(n-b+1) + 2(n-b+1)] + \\
&\quad + q^{b-2} [b(n-b+1) + 2b(n-b+1) - 2(n-b+1) - 2(n-b+1)] - \\
&\quad - q^{b-3} [(b-1)(n-b+1) - (n-b+1)] \\
&= (n-b+1) [b q^b + [-2b-b+2] q^{b-1} + [b+2b-2-2] q^{b-2} + [1-(b-1)] q^{b-3}] \\
&= (n-b+1) [b q^b + (2-3b) q^{b-1} + (3b-4) q^{b-2} + (2-b) q^{b-3}] \\
&= (n-b+1) [b q^3 + (2-3b) q^2 + (3b-4) q + (2-b)] q^{b-3} \\
&= (n-b+1) [b(q-1) + 2] (q-1)^2 q^{b-3} = w_b
\end{aligned}$$

Portanto,

$$w_b^T - w_{b-1}^T = w_b$$

### OBSERVAÇÃO 3

O resultado do Teorema 2.2.3, pode ser usado para determinar o peso total de todas as  $n$ -uplas. Isto pode ser obtido fazendo  $b = n$  de modo que, obtemos  $w_n^T = n(q-1) q^{n-1}$ .

De fato, no Teorema 2.2.3, fazendo  $b = n$  temos:

$$\begin{aligned}
w_n^T &= n(n-n+1) q^n + [n-2n(n-n+1)] q^{n-1} + (n-n)(n-1) q^{n-2} \\
&= n q^n - n q^{n-1} = n(q-1) q^{n-1}
\end{aligned}$$

Portanto,

$$w_n^T = n(q-1) q^{n-1}$$

## 2.3 - LIMITES SOBRE O PÊSO MÍNIMO DOS PEDAÇOS

Nos dois Teoremas seguintes obteremos limites sobre o maior peso mínimo atingível por um pedaço de comprimento  $b$  e por um pedaço de comprimento menor ou igual a  $b$  no espaço de todas as  $n$ -uplas.

Plotkin [11], obteve um limite similar sobre o maior peso mínimo atingível por um vetor código em um código linear  $[n, k]$ .

### Teorema 2.3.1

O peso mínimo de um pedaço de comprimento  $b > 1$  no espaço de todas as  $n$ -uplas é no máximo

$$b - \frac{b-2}{q} \quad (33)$$

### Demonstração:

Sabemos que o número de pedaços de comprimento  $b$  no espaço de todas as  $n$ -uplas com dígitos tomados sobre o corpo de  $q$  elementos é

$$(n - b + 1) (q - 1)^2 q^{b-2}$$

Pelo Teorema 2.2.1, o peso total de todos os pedaços de comprimento  $b$ , no espaço de todas as  $n$ -uplas é

$$(n - b + 1) [b(q - 1) + 2] (q - 1)^2 q^{b-3}$$

É pelo Lema 1.7.4, desde que, o elemento de peso mínimo pode ter no máximo a média dos pesos, um limite superior sobre o peso mínimo de um pedaço de comprimento  $b$  é dado por

$$\frac{(n-b+1) [b(q-1) + 2] (q-1)^2 q^{b-3}}{(n-b+1) (q-1)^2 q^{b-2}} = [b(q-1) + 2] q^{-1} = b - \frac{b-2}{q}$$

Portanto, o peso mínimo de um pedaço de comprimento  $b > 1$  no espaço de todas as  $n$ -uplas é

$$b - \frac{b-2}{q}$$

□

### OBSERVAÇÃO:

É interessante notar que o limite obtido no Teorema 2.3.1 é independente de  $n$ .

Assim, o limite permanece inalterável para todo  $n$  contanto que,  $n \geq b > 1$ .

### Teorema 2.3.2

O pêsso m̃nimo de um pedaço de comprimento menor ou igual a  $b$  no espaço de todas as  $n$ -uplas  $\bar{e}$  no m̃ximo

$$\frac{b(n-b+1) q^b + [n - 2b(n-b+1)] q^{b-1} + (b-1)(n-b) q^{b-2}}{[(n-b+1)(q-1) + 1] q^{b-1} - 1} \quad (34)$$

### Demonstraçãõ:

O ñmero de pedaços de comprimento menor ou igual a  $b$  no espaço de todas as  $n$ -uplas  $\bar{e}$

$$[(n - b + 1)(q - 1) + 1] q^{b-1} - 1$$

Pelo Teorema 2.2.3, o pêsso total de todos os pedaços de comprimento menor ou igual a  $b$  no espaço de todas as  $n$ -uplas  $\bar{e}$

$$b(n-b+1) q^b + [n - 2b(n-b+1)] q^{b-1} + (b-1)(n-b) q^{b-2}.$$

Entãõ, o pêsso m̃nimo de um pedaço de comprimento menor ou igual a  $b$   $\bar{e}$  dado por

$$\frac{b(n-b+1) q^b + [n - 2b(n-b+1)] q^{b-1} + (b-1)(n-b) q^{b-2}}{[(n-b+1)(q-1) + 1] q^{b-1} - 1} \quad \square$$

### OBSERVAÇãõ:

O pêsso m̃nimo de um vetor cõdigo em um cõdigo linear  $[n, k]$  segundo o Lema 1.7.4,  $\bar{e}$  no m̃ximo tãõ grande como a m̃dia dos pêsos

$$\frac{n(q-1) q^{k-1}}{q^k - 1}$$

Se considerarmos o espaço de todas as  $n$ -uplas, entãõ, o pêsso m̃nimo de uma  $n$ -upla serã no m̃ximo

$$\frac{n(q-1) q^{n-1}}{q^n - 1}$$

Este resultado tambẽm pode ser obtido fazendo  $b = n$  no Teorema 2.3.2, isto  $\bar{e}$ :

$$\frac{n(n-n+1) q^n + [n - 2n(n-n+1)] q^{n-1} + (n-1)(n-n) q^{n-2}}{[(n-n+1)(q-1) + 1] q^{n-1} - 1} =$$

$$= \frac{n q^n - n q^{n-1}}{q \cdot q^n - 1} = \frac{n(q-1) q^{n-1}}{q^n - 1} .$$

## 2.4 - FUNÇÕES GERATRIZES DE $w_b$ E $w_b^T$

MacWilliams [7] definiu funções geratrizes para códigos lineares. Estas funções tem sido de grande utilidade na enumeração das palavras código de um dado peso.

Sharma e Dass [13], calcularam as funções geratrizes de  $w_b$  e  $w_b^T$  que poderão ser úteis na enumeração de palavras código.

No dois Teoremas seguintes provaremos resultados obtidos por Sharma e Dass [13].

### Teorema 2.4.1

Para  $n \geq b \geq 1$ ,  $w_b$  é o coeficiente de  $x^b$  em

$$n(q-1)x + [n(q+1)qx^2 - \{n(3q+1) - 2\}x + 2(n-1)]x^2(q-1)^2(1-qx)^{-3} \quad (35)$$

### Demonstração:

A expressão tendo  $w_b$  como coeficiente de  $x^b$ , pode geralmente ser escrita como

$$\sum_{i=1}^n w_i x^i.$$

Usando o Teorema 2.2.1, obtemos:

$$\begin{aligned} \sum_{i=1}^n w_i x^i &= n(q-1)x + \sum_{i=2}^n (n-i+1) [i(q-1)+2] (q-1)^2 q^{i-3} x^i = \\ &= n(q-1)x + (q-1)^2 x^3 \sum_{i=2}^n \{-i^2(q-1) + i[(n+1)(q-1) - 2] + \\ &+ 2(n+1)\} (qx)^{i-3} = \\ &= n(q-1)x + (q-1)^2 x^3 \{- (q-1) \sum_{i=2}^n i^2 (qx)^{i-3} + [(n+1)(q-1) - 2] \\ &\quad \sum_{i=2}^n i (qx)^{i-3} + 2(n+1) \sum_{i=2}^n (qx)^{i-3}\} \end{aligned} \quad (36)$$

Substituindo as expressões (30); (31) e (32) na equação

(36) temos:

$$\begin{aligned}
\sum_{i=1}^n W_i x^i &= n(q-1) x + (q-1)^2 x^3 \left\{ - (q-1) \left[ \frac{4}{q x (qx-1)^2} + \right. \right. \\
&+ \frac{2q x [(qx)^{n-2} - 1]}{(qx-1)} + \left. \frac{n^2 (qx)^{n-1} - (n+1)^2 (qx)^{n-2} + 1}{(qx-1)^3} \right] + \\
&+ [ (n+1) (q-1) - 2 ] \left[ \frac{n(qx)^{n-2}}{qx-1} - \frac{2}{qx(qx-1)} - \right. \\
&- \left. \frac{(qx)^{n-2} - 1}{(qx-1)^2} \right] + 2(n+1) \left[ \frac{1}{qx} - \frac{(qx)^{n-2} - 1}{qx-1} \right] \left. \right\} = \\
&= n(q-1) x + (q-1)^2 x^3 \left\{ - (q-1) \left[ \frac{4(qx-1)}{qx(qx-1)^3} + \frac{2(qx)^n}{qx(qx-1)^3} - \right. \right. \\
&- \frac{2(qx)^2}{qx(qx-1)^3} + \frac{n^2 (qx)^n (qx-1)}{qx(qx-1)^3} - \frac{(n+1)^2 (qx)^{n-1} (qx-1)}{qx(qx-1)^3} + \\
&+ \left. \frac{qx(qx-1)}{qx(qx-1)^3} \right] + [ (n+1)(q-1) - 2 ] \left[ \frac{n(qx)^{n-1} (qx-1)}{qx(qx-1)^2} - \right. \\
&- \frac{(qx)^{n-1}}{qx(qx-1)^2} + \frac{2 - qx}{qx(qx-1)^2} \left. \right] + 2(n-1) \left[ \frac{(qx)^{n-1}}{qx(qx-1)} - \right. \\
&- \left. \frac{1}{qx(qx-1)} \right] \left. \right\} = \\
&= n(q-1) x + \frac{(q-1)^2 x^2}{q(qx-1)^3} \left\{ (qx)^{n+1} \{ [ - n^2 + n(n+1) ] (q-1) - 2n + 2n + 2 \} + \right. \\
&+ \{ (qx)^n [ - 2 + n^2 + (n+1)^2 - 2n(n+1) - (n+1) ] (q-1) + 4n + 2 - \\
&- 4(n+1) \} + (qx)^{n-1} \{ [ -(n+1)^2 + n(n+1) + n + 1 ] (q-1) - 2n - \\
&- 2 + 2(n+1) \} + (qx)^2 \{ [ 1 - (n+1) ] (q-1) + 2 - 2(n+1) \} + \\
&+ qx \{ [ - 3 + 3(n+1) ] (q-1) - 6 + 4n + 4 \} + 4(q-1) - 2(n+1) \\
&(q-1) + 4 - 2(n+1) \left. \right\} = \\
&= n(q-1) x + \frac{(q-1)^2 x^2}{q(qx-1)^3} \left\{ (qx)^{n+1} [ n(q-1) + 2 ] + (qx)^n [ -nq - 2q + n ] + \right. \\
&+ (qx)^2 [ -n(q-1) - 2n ] + qx [ 3nq + n - 2 ] + 2q - 2nq \left. \right\} =
\end{aligned}$$

$$\begin{aligned}
&= n(q-1) x + \frac{(q-1)^2 x^2}{q(qx-1)^3} \left\{ (qx)^{n+1} [n(q-1)+2] + (qx)^n [-n(q-1)-2q]- \right. \\
&\quad \left. - (qx)^2 n(q-1) + qx [n(3q+1) - 2] + 2q(1 - 2n) \right\} = \\
&= n(q-1) x + \frac{(q-1)^2 x^2}{(qx-1)^3} \left\{ q^n x^{n+1} [n(q-1)+2] - q^{n-1} x^n [n(q-1)+2q]- \right. \\
&\quad \left. - nq(q+1) x^2 + [n(3q+1) - 2] x + 2 - 2n \right\} \\
&= n(q-1) x + \frac{(q-1)^2 x^2}{(qx-1)^3} \left\{ q^{n-1} x^n \{ [n(q-1)+2]qx - [n(q-1)+2q] \} - \right. \\
&\quad \left. - n(q+1) qx^2 + [n(3q+1)-2] x + 2 - 2n \right\} \tag{37}
\end{aligned}$$

A expressão (37), contém termos envolvendo  $x^{n+2}$  e ordens maiores. Visto que, o comprimento de um pedaço não pode exceder  $n$ , este termo pode ser abandonado totalmente e obtemos a função geratriz de  $W_b$  como estabelecida em (35), isto é:

$$\sum_{i=1}^n W_i x_i = n(q-1) x + \frac{(q-1)^2 x^2}{(qx-1)^3} \left\{ -n(q+1)qx^2 + [n(3q+1)-2] x + 2 - 2n \right\}$$

ou

$$= n(q-1) x + \frac{(q-1)^2 x^2}{(1-qx)^3} \left[ n(q+1)qx^2 - [n(3q+1)-2] x - 2 + 2n \right] \quad \square$$

**OBSERVAÇÃO:**

Como esperado, os coeficientes de todas as potências de  $x$  maiores que  $n$  desaparecem em (37).

### Teorema 2.4.2

Para  $n \geq b \geq 1$ ,  $W_b^T$  é o coeficiente de  $x^b$  em

$$(q-1) x [n q x^2 - \{ (n+2)(q-1)+2n \} x + n] (1 - qx)^{-3} \tag{38}$$

**Demonstração:**

A expressão tendo  $W_b^T$  como coeficiente de  $x^b$ , pode geralmente ser escrita como

$$\sum_{i=1}^n W_i^T x^i .$$

Usando o Teorema 2.2.3 , obtemos:

$$\begin{aligned} \sum_{i=1}^n W_i^T x^i &= \sum_{i=1}^n [i(n-i+1) q^i + \{n - 2i(n-i+1)\} q^{i-1} + (n-i)(i-1)q^{i-2}] x^i = \\ &= -(q-1)^2 x^2 \sum_{i=1}^n i^2 q^{i-2} x^{i-2} + (n+1)(q-1)^2 x^2 \sum_{i=1}^n i q^{i-2} x^{i-2} + \\ &\quad + n(q-1) x^2 \sum_{i=1}^n q^{i-2} x^{i-2} = \\ &= -(q-1)^2 x^2 qx \sum_{i=1}^n i^2 (qx)^{i-3} + (n+1)(q-1)^2 x^2 qx \sum_{i=1}^n i (qx)^{i-3} + \\ &\quad + n(q-1) x^2 qx \sum_{i=1}^n (qx)^{i-3} = \\ &= -(q-1)^2 x^2 qx \left[ \frac{1}{(qx)^2} + \sum_{i=2}^n i^2 (qx)^{i-3} \right] + (n+1)(q-1)^2 x^2 qx \\ &\quad \left[ \frac{1}{(qx)^2} + \sum_{i=2}^n i (qx)^{i-3} \right] + n(q-1) x^2 qx \left[ \frac{1}{(qx)^2} + \sum_{i=2}^n (qx)^{i-3} \right] \end{aligned} \quad (39)$$

Substituindo as expressões (30) , (31) e (32) na expressão (39) , temos:

$$\begin{aligned} \sum_{i=1}^n W_i^T x^i &= -(q-1)^2 x^2 qx \left[ \frac{1}{(qx)^2} + \frac{4}{qx(qx-1)^2} + \frac{2qx [(qx)^{n-2}-1]}{(qx-1)^3} + \right. \\ &\quad \left. + \frac{n^2 (qx)^{n-1} - (n+1)^2 (qx)^{n-2} + 1}{(qx-1)^2} \right] + \\ &\quad + (n+1)(q-1)^2 x^2 qx \left[ \frac{1}{(qx)^2} + \frac{n(qx)^{n-2}}{qx-1} - \frac{2}{qx(qx-1)} - \right. \\ &\quad \left. - \frac{(qx)^{n-2}-1}{(qx-1)^2} \right] + n(q-1) x^2 qx \left[ \frac{1}{(qx)^2} + \frac{1}{qx} - \frac{(qx)^{n-2}-1}{qx-1} \right] = \\ &= - \frac{(q-1)^2 x^2 qx}{(qx)^2} + \frac{(n+1)(q-1)^2 x^2 qx}{(qx)^2} + \frac{n(q-1) x^2 qx}{(qx)^2} - \\ &\quad - (q-1)^2 x^2 qx \left[ \frac{4}{qx(qx-1)^2} + \frac{2qx [(qx)^{n-2}-1]}{(qx-1)^3} + \right. \end{aligned}$$



$$\begin{aligned}
& + \frac{n^2 (qx)^{n-1} - (n+1)^2 (qx)^{n-2} + 1}{(qx-1)^2} \Big] + \\
& + (n+1)(q-1)^2 x^2 qx \left[ \frac{n(qx)^{n-2}}{qx-1} - \frac{2}{qx(qx-1)} - \frac{(qx)^{n-2}-1}{(qx-1)^2} \right] + \\
& + n(q-1) x^2 qx \left[ \frac{1}{qx} - \frac{(qx)^{n-2}-1}{qx-1} \right] = \\
= & n(q-1) x - \frac{(q-1)^2 x^2}{(qx-1)^3} \left[ 4qx - 4 + 2(qx)^n - 2(qx)^2 + n^2 (qx)^{n+1} - \right. \\
& - 2n^2 (qx)^n + n^2 (qx)^{n-1} - 2n(qx)^n + 2n(qx)^{n-1} - (qx)^n + (qx)^{n-1} + \\
& \left. + (qx)^2 - qx \right] + \frac{(n+1)(q-1)^2 x^2}{(qx-1)^3} \left[ n(qx)^{n-1} (qx-1)^2 - 2(qx-1)^2 - \right. \\
& \left. - [(qx)^{n-1} - qx] (qx-1) \right] + \frac{n(q-1)x^2}{(qx-1)^3} \left[ [(qx)^{n-1}-1] (qx-1)^2 \right] = \\
= & n(q-1) x + \frac{(q-1)x^2}{(qx-1)^3} \left[ - [3qx - 4 - (qx)^2] (q-1) + [3qx - 2 - (qx)^2] \right. \\
& \left. (n+1)(q-1) + [2qx - 1 - (qx)^2] n \right] + \frac{(q-1)x^2}{(qx-1)^3} (qx)^{n-1} \\
& \left[ - (q-1)(n+1)^2 - n^2 (q-1)(qx)^2 + (2n^2 + 2n - 1)(q-1) qx + \right. \\
& \left. + n(qx)^2 - 2n qx + n + (n+1)(q-1) [n(qx)^2 - (2n+1) qx + n + 1] \right] \\
= & n(q-1) x + \frac{(q-1)x^2}{(qx-1)^3} \left[ (qx)^2 [(q-1)-(n+1)(q-1)-n] + qx [-3(q-1) + \right. \\
& \left. + 3(n+1)(q-1)+2n] + [4(q-1)-2(n+1)(q-1)-n] \right] + \\
& + \frac{(q-1)x^2}{(qx-1)^3} (qx)^{n-1} \left[ (qx)^2 [-n^2 (q-1)+n(n+1)(q-1)+n] + \right. \\
& \left. + [(n+1)^2 (q-1)-(n+1)^2 (q-1)+n] + qx [(2n^2 + 2n - 1)(q-1) - \right. \\
& \left. - (2n+1)(n+1)(q-1)-2n] \right] = \\
= & n(q-1) x + \frac{(q-1) x^2}{(qx-1)^3} \left[ -nq(qx)^2 + n(3q-1) qx + 2(q-1)+n(1-2q) \right] +
\end{aligned}$$

$$\begin{aligned}
& + \frac{(q-1)x^2}{(qx-1)^3} (qx)^{n-1} \left[ nq(qx)^2 + [-nq + n - 2q - 2 - 2n] qx + n \right] = \\
= & \frac{(q-1)x}{(qx-1)^3} \left[ n(qx-1)^3 - n(qx)^3 + 3n(qx)^2 - nqx^2 + 2qx - 2nqx - 2x - nx \right] + \\
& + \frac{(q-1)q^{n-1}x^{n+1}}{(qx-1)^3} \left[ nq(qx)^2 - [nq - n + 2q - 2 + 2n] qx + n \right] = \\
= & \frac{(q-1)x}{(qx-1)^3} \left[ -n(qx)^2 + (n+2)q^2x + (n-2)qx - nq \right] + \\
& + \frac{(q-1)q^{n-1}x^{n+1}}{(qx-1)^3} \left[ nq^3x^2 - [(n+2)(q-1) + 2n] qx + n \right] = \\
= & \frac{(q-1)x}{(qx-1)^3} \left[ -n(qx)^2 + [(n+2)(q-1) + 2n] qx - nq \right] + \\
& + \frac{(q-1)q^{n-1}x^{n+1}}{(qx-1)^3} \left[ nq^3x^2 - [(n+2)(q-1) + 2n] qx + n \right] \quad (40)
\end{aligned}$$

O último termo na expressão (40), contém termos envolvidos do  $x^{n+1}$  e de ordens maiores, pelas mesmas razões do Teorema 2.4.1, pode ser abandonado totalmente e obtemos a função geratriz de  $W_b^T$  como estabelecida em (38), isto é:

$$\sum_{i=1}^n W_i^T x^i = \frac{(q-1)x}{(qx-1)^3} \left[ -n(qx)^2 + [(n+2)(q-1) + 2n] qx - nq \right]$$

ou

$$= \frac{(q-1)x}{(1-qx)^3} \left[ n(qx)^2 - [(n+2)(q-1) + 2n] qx + nq \right]$$

□

## CAPÍTULO III

### ESTUDO DOS CÓDIGOS LINEARES CORRETORES DE PEDAÇOS DE ERRO COM CRITÉRIO PÊSO

#### 3.1 - LIMITE DE VARSHARMOV-GILBERT EXTENDIDO

No Capítulo II apresentamos o estudo dos códigos lineares corretores de pedaços de erro. Mas existem muitas situações em que os erros ocorrem na forma de pedaços e nem todos os dígitos no pedaço são afetados. Como exemplo, existem canais modelados por Elliot [4] e Gilbert [5] onde este tipo de situação ocorre.

Wyner [16], Dass [2,3] e Sharma e Dass [15] realizaram o estudo dos códigos que são capazes de corrigir ou detectar pedaços de erro de comprimento  $b$  que são de peso menor ou igual a  $W$ , isto é, no pedaço de comprimento  $b$ ,  $W$  erros ou menos ocorrem.

Primeiro, introduziremos a idéia de peso relativo ao pedaço a ser corrigido bem como ao código. Suponhamos que temos um critério de peso sobre o código. No Teorema seguinte daremos uma extensão do limite de Varsharmov-Gilbert para um código que não tem pedaço de comprimento menor ou igual a  $b$  como um vetor código impondo ao código o critério peso. Este limite assegura a existência de um código que pode detectar todos os vetores de erro que são pe

daços de comprimento menor ou igual a  $b$ , ou tem p̄eso menor ou  $i$  igual a  $W - 1$ .

### Teorema 3.1.1

Existe um c̄odigo linear  $[n, k]$  com p̄eso m̄inimo pelo menos  $W$  que n̄o tem pedaço n̄o nulo de comprimento menor ou igual a  $b$  co mo um vetor c̄odigo ( $W \leq b$ ) satisfazendo a inequaç̄o

$$\sum_{i=0}^{W-2} \binom{n}{i} (q-1)^i + \sum_{j=W-1}^{b-1} \binom{b-1}{j} (q-1)^j \geq q^{n-k} \quad (41)$$

### Demonstraç̄o:

Provaremos o Teorema construindo uma  $(n - k) \times n$  matriz de verificaç̄o de paridade  $H$ . O p̄ocedimento ser̄a semelhante ao do Teorema 2.1.5. Suponhamos que uma  $(n - k)$ -upla ̄e escolhida co mo a primeira coluna de  $H$ . Colunas subsequentes s̄ao adicionadas de tal modo que, tendo selecionado  $j - 1$  colunas  $h_1, h_2, \dots, h_{j-1}$ , uma coluna  $h_j$  ̄e adicionada com a condiç̄o que ela n̄o ̄e uma combinaç̄o linear de quaisquer  $W - 2$  colunas ou menos entre as  $h_1, h_2, \dots, h_{j-1}$ , nem uma combinaç̄o linear de  $b - 1$  colunas ou menos, mas,  $W - 1$  colunas ou mais entre as

$$h_{j-b+1}, h_{j-b+2}, \dots, h_{j-1}$$

Na pior das hip̄oteses, todas estas combinaç̄oes lineares po dem ser distintas. O n̄mero total de combinaç̄oes lineares ̄e dado por

$$\sum_{i=1}^{W-2} \binom{j-1}{i} (q-1)^i + \sum_{j=W-1}^{b-1} \binom{b-1}{j} (q-1)^j$$

Mas, o n̄mero total de  $(n - k)$ -uplas n̄o nulas ̄e  $q^{n-k} - 1$ .

Se

$$\sum_{i=0}^{W-2} \binom{j-1}{i} (q-1)^i + \sum_{j=W-1}^{b-1} \binom{b-1}{j} (q-1)^j < q^{n-k},$$

isto ̄e, para  $j \leq n$ , o n̄mero de combinaç̄oes lineares ̄e menor que o conjunto de  $(n - k)$ -uplas n̄o nulas.

Se  $n$  ̄e o maior valor de  $j$  para o qual a inequaç̄o ante rior vale, ent̄o, o c̄odigo  $(n, k)$  existe satisfazendo (41).

□

OBSERVAÇÃO:

O resultado obtido vale para  $W \leq b$ . Contudo, se  $W > b$ , o critério p̄so é redundante e o limite resultante se reduz ao limite de Varsharmov - Gilbert sobre o p̄so mínimo conforme o Teorema 1.7.9.

Provaremos, a seguir, um Lema que determina o número total de pedaços de comprimento  $b > 1$  com p̄so menor ou igual a  $W$ .

Lema 3.1.2

O número total de pedaços de comprimento  $b (> 1)$  com p̄so menor ou igual a  $W$  é

$$(n - b + 1) (q - 1)^2 [1 + (q - 1)]^{(b-2, W-2)} \quad (42)$$

onde

$$[1 + (q - 1)]^{(m,r)}$$

denota a expansão binomial incompleta de  $(1 + x)^m$  até o termo  $x^r$  na potência ascendente de  $x$ .

Demonstração:

Pelo Lema 2.2.1, o número total de pedaços de comprimento  $b > 1$  com p̄so  $W$  no espaço de todas as  $n$ -uplas é

$$\binom{b-2}{W-2} (n-b+1) (q-1)^W = (n-b+1) (q-1)^2 \binom{b-2}{W-2} (q-1)^{W-2}.$$

Como nos interessam todos os pedaços de comprimento  $b > 1$  com p̄so menor ou igual a  $W$ , temos então que:

O número de pedaços de comprimento  $b > 1$  com p̄so 2 é:  $(n-b+1)(q-1)^2 \binom{b-2}{0} (q-1)^0$

O número de pedaços de comprimento  $b > 1$  com p̄so 3 é:  $(n-b+1)(q-1)^2 \binom{b-2}{1} (q-1)^1$

O número de pedaços de comprimento  $b > 1$  com p̄so 4 é:  $(n-b+1)(q-1)^2 \binom{b-2}{2} (q-1)^2$

.

.

.

O número de pedaços de comprimento  $b > 1$  com p̄so  $W$  é:  $(n-b+1)(q-1)^2 \binom{b-2}{W-2} (q-1)^{W-2}$

Assim, o número total de pedaços de comprimento  $b$  de p̄so  $W$  ou menos é

$$\begin{aligned}
(n-b+1)(q-1)^2 & \left[ \binom{b-2}{0}(q-1)^0 + \binom{b-2}{1}(q-1)^1 + \binom{b-2}{2}(q-1)^2 + \dots + \binom{b-2}{W-2}(q-1)^{W-2} \right] = \\
& = (n-b+1)(q-1)^2 \sum_{i=0}^{W-2} \binom{b-2}{i}(q-1)^i
\end{aligned} \tag{43}$$

Usando a Série Binomial

$$(a + b)^n = \sum_{m=0}^n \binom{n}{m} a^{n-m} b^m$$

e fazendo  $a = 1$  e  $b = q - 1$ , temos

$$[1 + (q - 1)]^n = \sum_{m=0}^n \binom{n}{m} (q - 1)^m.$$

Agora denotando o desenvolvimento incompleto, até a potência  $W - 2$ , da Série Binomial  $[1 + (q - 1)]^{(b-2, W-2)}$ , temos que

$$[1 + (q-1)]^{(b-2, W-2)} = \sum_{i=0}^{W-2} \binom{b-2}{i} (q-1)^i.$$

Substituindo em (43), obtemos que o número total de pedaços de comprimento  $b > 1$  com peso menor ou igual a  $W$  é

$$(n - b + 1) (q - 1)^2 [1 + (q - 1)]^{(b-2, W-2)}.$$

□

Usaremos o Lema para provar o seguinte Teorema.

### Teorema 3.1.3

O número de dígitos de verificação de paridade em qualquer código linear que corrige todos os pedaços de comprimento menor ou igual a  $b$  com peso menor ou igual a  $W$  ( $W \leq b$ ) é pelo menos

$$\log_q \left[ q^{W-1} [(q-1)(n - W + 1)] + (q-1)^2 \sum_{j=W+1}^b (n-j+1) [1 + (q-1)]^{(j-2, W-2)} \right] \tag{44}$$

### Demonstração:

Usando o Lema 3.1.2, o número total de pedaços de comprimento menor ou igual a  $b$  com peso menor ou igual a  $W$ , incluindo o vetor nulo e os vetores de erro único, é

$$\begin{aligned}
& 1 + n(q-1) + (q-1)^2 \sum_{j=2}^W (n-j+1) q^{j-2} + \\
& + (q-1)^2 \sum_{j=W+1}^b (n-j+1) [1+(q-1)]^{(j-2, W-2)} \quad (45)
\end{aligned}$$

que usando o Teorema 2.1.4 nos três primeiros termos da expressão (45), temos

$$q^{W-1} [(q-1)(n-W+1) + 1] + (q-1)^2 \sum_{j=W+1}^b (n-j+1) [1+(q-1)]^{(j-2, W-2)}$$

que é o número de "cosets" exigidos pelo arranjo padrão deste código, isto é:

$$q^{n-k} \geq q^{W-1} [(q-1)(n-W+1) + 1] + (q-1)^2 \sum_{j=W+1}^b (n-j+1) [1+(q-1)]^{(j-2, W-2)}$$

Tomando logaritmo temos que o número de dígitos de verificação de paridade deste código é

$$\begin{aligned}
n-k \geq \log_q \left[ q^{W-1} [(q-1)(n-W+1) + 1] + (q-1)^2 \sum_{j=W+1}^b (n-j+1) \right. \\
\left. [1+(q-1)]^{(j-2, W-2)} \right]
\end{aligned}$$

□

#### OBSERVAÇÃO:

Para  $W = b$ , o limite inferior sobre o número de verificação de paridade se transforma em

$$b - 1 + \log_q [(q-1)(n-b+1) + 1]$$

que coincide com o resultado do Teorema 2.1.4 .

No Teorema seguinte, provaremos o limite de empacotamento de esfera extendido para um código que é capaz de corrigir todos os pedaços de comprimento menor ou igual a  $b$  .

#### Teorema 3.1.4

Um código linear  $[n, k]$  capaz de corrigir todas as combinações de  $m$  erros ou menos e todos os pedaços de comprimento menor ou igual a  $b$  deve satisfazer

$$n-k \geq \log_q \left[ \sum_{i=0}^m \binom{n}{i} (q-1)^i + (q-1)^2 \sum_{i=m+1}^b (n-i+1) \{ q^{i-2} - [1+(q-1)]^{(i-2, m-2)} \} \right]$$

(46)

onde  $m < b$ .

### Demonstração:

Como o código  $\bar{e}$  é capaz de corrigir todos os erros de peso menor ou igual a  $m$ , todas as  $n$ -uplas de peso menor ou igual a  $m$  estarão em "cosets" diferentes, seu número é

$$[1 + (q - 1)]^{(n,m)} \quad (47)$$

Do mesmo modo, visto que o código corrige todos os pedaços de comprimento menor ou igual a  $b$ , cada pedaço de comprimento menor ou igual a  $b$  também deve estar em "coset" diferente, a não ser que, este  $\bar{e}$  também um erro aleatório de peso menor ou igual a  $m$  e em consequência são incluídos em (47).

Assim, necessitamos somente calcular o número de pedaços de comprimento  $m + 1$ ,  $m + 2$ , ...,  $b$  com peso maior que  $m$ . O número de pedaços de comprimento  $i$  ( $i > m$ ) com peso maior que  $m$  é

$$(n - i + 1) (q-1)^2 \{ q^{i-2} - [1 + (q-1)]^{(i-2, m-2)} \}$$

Assim, o número total de vetores de erro  $\bar{e}$

$$\sum_{i=0}^m \binom{n}{i} (q-1)^i + (q-1)^2 \sum_{i=m+1}^b (n-i+1) \{ q^{i-2} - [1 + (q-1)]^{(i-2, m-2)} \}$$

que é também o número mínimo de "cosets" exigidos pelo código, isto é:

$$q^{n-k} \geq \sum_{i=0}^m \binom{n}{i} (q-1)^i + (q-1)^2 \sum_{i=m+1}^b (n-i+1) \{ q^{i-2} - [1 + (q-1)]^{(i-2, m-2)} \}$$

Tomando logarítmo, temos que

$$n-k \geq \log_q \left[ \sum_{i=0}^m \binom{n}{i} (q-1)^i + (q-1)^2 \sum_{i=m+1}^b (n-i+1) \{ q^{i-2} - [1 + (q-1)]^{(i-2, m-2)} \} \right] \quad (48)$$

□

### OBSERVAÇÃO:

Para  $m \geq b$ , os dois últimos fatores em (48) desaparecem e o limite se reduz ao limite de empacotamento de esfera de Hamming.



### 3.2 - CÓDIGOS DETECTORES DE PEDAÇOS DE ERRO

Consideremos um código com peso mínimo pelo menos  $W_1$  tal que, nenhum vetor código é um pedaço de comprimento menor ou igual a  $b$  com peso menor ou igual a  $W_2$ .

No Teorema seguinte provaremos um limite superior sobre o número de dígitos de verificação de paridade exigidos para a construção de um tal código. Uma vantagem a mais de tais códigos é que podem ser usados para corrigir  $\lfloor \frac{W_1 - 1}{2} \rfloor$  ou menos erros aleatórios também.

#### OBSERVAÇÃO:

$\lfloor X \rfloor$  denota o inteiro maior ou igual a  $X$ .

#### Teorema 3.2.1

Existe um código linear  $[n, k]$  com peso mínimo pelo menos  $W_1$  que não tem pedaço de comprimento menor ou igual a  $b$  com peso menor ou igual a  $W_2$  como um vetor código ( $W_1 \leq W_2 \leq b$ ) satisfazendo a inequação

$$q^{n-k} \leq \sum_{i=0}^{W_1-2} \binom{n}{i} (q-1)^i + \sum_{j=W_1-1}^{W_2-1} \binom{b-1}{j} (q-1)^j \quad (49)$$

#### Demonstração:

A existência de um tal código será mostrada construindo uma matriz  $(n-k) \times n$  de verificação de paridade  $H$ , apropriada para o código. Usaremos um procedimento análogo ao do Teorema 2.1.5.

Uma  $(n-k)$ -upla não nula é escolhida como a primeira coluna da matriz de verificação de paridade  $H$ . Colunas subsequentes são adicionadas tais que, tendo selecionado  $j-1$  colunas  $c_1, c_2, \dots, c_{j-1}$ , uma coluna  $c_j$  é adicionada com a condição que, esta não é uma combinação linear de quaisquer  $W_1-2$  colunas ou menos e nem uma combinação linear de quaisquer  $W_2-1$  colunas ou menos entre as  $b-1$  colunas imediatamente precedentes

$$c_{j-b+1}, c_{j-b+2}, \dots, c_{j-1}$$

Esta construção assegura que o espaço nulo de tais matrizes será um código linear com peso mínimo pelo menos  $W_1$  e não terá qualquer pedaço de comprimento menor ou igual a  $b$  com peso menor ou igual a  $W_2$  como um vetor código.

Agora, entre as  $j - 1$  colunas há

$$\left[ \binom{j-1}{1} (q-1) + \binom{j-1}{2} (q-1)^2 + \dots + \binom{j-1}{W_1-2} (q-1)^{W_1-2} \right] + \\ + \left[ \binom{b-1}{W_1-1} (q-1)^{W_1-1} + \binom{b-1}{W_1} (q-1)^{W_1} + \dots + \binom{b-1}{W_2-1} (q-1)^{W_2-1} \right]$$

possíveis combinações lineares de

- (i)  $W_1-2$  colunas ou menos entre as  $j - 1$  colunas, e
- (ii)  $W_2-1$  colunas ou menos mas  $W_1-1$  colunas ou mais entre as  $b - 1$  colunas.

Na pior das hipóteses, todas estas combinações lineares podem ser distintas. Assim, uma coluna  $c_j$  ( $j \leq n$ ) pode ser adicionada a  $H$  se esta não esgotar todo o conjunto de  $q^{n-k} - 1$  das  $(n-k)$ -uplas não nulas, isto é, se

$$\sum_{i=1}^{W_1-2} \binom{j-1}{i} (q-1)^i + \sum_{i=W_1-1}^{W_2-1} \binom{b-1}{i} (q-1)^i < q^{n-k} - 1 \quad (50)$$

Seja  $n$  o maior valor de  $j$  para o qual a inequação precedente é válida.

Então, existe um código  $[n, k]$  com os requisitos exigidos e satisfazendo (49)

□

### Corolário 3.2.2

Se  $W_1 > W_2$  o limite obtido em (49) se reduz ao limite de Varsharmov-Gilbert para um código linear de peso mínimo pelo menos  $W_1$ .

Assim, nesta situação, os pedaços de comprimento  $b$  e  $W_2$  não tem papel a representar.

### Corolário 3.2.3

Para um código com peso mínimo pelo menos  $W_1$  que não tem

pedaço de comprimento menor ou igual a  $\mathbf{b}$  como um vetor código, as verificações de paridade satisfazem a inequação

$$\sum_{i=0}^{W_1-2} \binom{n}{i} (q-1)^i + \sum_{j=W_1-1}^{b-1} \binom{b-1}{j} (q-1)^j \geq q^{n-k}.$$

### Demonstração:

Pondo  $W_2 = \mathbf{b}$  em (49) o resultado segue. Este resultado é o mesmo apresentado no Teorema 3.1.1, ou seja, o limite extendido de Varsharmov-Gilbert.

### Corolário 3.2.4

Existe um código linear  $[\mathbf{n}, \mathbf{k}]$  que não tem pedaços de comprimento  $\mathbf{b}$  ou menos com peso  $\mathbf{W}$  ou menos como um vetor código, satisfazendo

$$\sum_{i=0}^{W-1} \binom{b-1}{i} (q-1)^i \geq q^{n-k}$$

### Demonstração:

Pondo  $W_1 = 1$  em (49), temos o resultado.

### OBSERVAÇÃO:

Para  $W_1 = 1$  e  $W_2 = \mathbf{b}$ , o Teorema 3.2.1 leva a existência de um código linear  $[\mathbf{n}, \mathbf{k}]$  que não tem pedaços de comprimento menor ou igual a  $\mathbf{b}$  como um vetor código com mais de  $\mathbf{b} - 1$  dígitos de verificação de paridade. Um tal código com exatamente  $\mathbf{b}$  verificações de paridade pode ser assim formado o qual detecta necessariamente todos os erros que são pedaços de comprimentos menores ou iguais a  $\mathbf{b}$ , conforme Teorema 2.1.2

### Exemplo 3.2.1

Consideremos um código linear binário  $[15, 11]$  cuja matriz

de verificação de paridade  $\bar{e}$

$$\begin{pmatrix} 1000011111001101 \\ 0100110011111100 \\ 001010101100111 \\ 000110010011111 \end{pmatrix}$$

Esta matriz foi construída adicionando 4-uplas como colunas subsequentes de acordo com o Teorema 3.2.1, tomando  $W_1=3$ ,  $W_2=3$  e  $b=4$ . O peso mínimo do código é 3 e nenhum pedaço de comprimento menor ou igual a 4 com peso menor ou igual a 3 é um vetor código, enquanto que um pedaço de comprimento 4 com peso 4 é um vetor código.

Exemplo: (011110000000000).

### 3.3 - CÓDIGOS COM PÊSO MÍNIMO CORRETORES DE PEDAÇO DE ERRO

Vamos impor uma condição de pêso mínimo para um código corretor de pedaços de erro.

No Teorema seguinte uma extensão do limite de Varsharmov-Gilbert é provada para um código que corrige todos os pedaços de comprimento menor ou igual a  $b$ . Este limite assegura a existência de um código que corrige todos os pedaços de comprimento menor ou igual a  $b$  ou detecta todos os erros de pêso menor ou igual a  $W-1$ .

#### Teorema 3.3.1

Dados os dois inteiros positivos  $W$  e  $b$  tais que  $W \leq 2b$ , uma condição suficiente para que exista um código linear  $[n, k]$ ,  $n > 2b$ , com pêso mínimo pelo menos  $W$  que corrige todos os pedaços de comprimento menor ou igual a  $b$  é

$$q^{n-k} > [1 + (q-1)]^{(n-1, W-2)} + \sum_{\substack{r_1+r_2=2b-1 \\ r_1, r_2: \\ r_1+r_2=W-1}} [I(q, n; b, r_2) \binom{b-1}{r_1} (q-1)^{r_1}] \quad (51)$$

onde  $0 \leq r_1 \leq b-1$ ;  $0 \leq r_2 \leq b$ ,

$$I(q, n; b, r_2) = \begin{cases} \binom{n-b}{r_2} (q-1)^{r_2} & ; r_2 = 0, 1 \\ (q-1)^{r_2} \sum_{i=r_2}^b \binom{i-2}{i_2-2} (n-b-i+1) & ; r_2 \geq 2 \end{cases}$$

e

$$[1 + X]^{(m, r)} = \begin{cases} 0 & , r < 0 \\ 1 & , r = 0 \\ 1 + \binom{m}{1} X + \dots + \binom{m}{r} X^r & , 0 < r < m \end{cases}$$

#### Demonstração:

A existência de um tal código será mostrada construindo uma  $(n-k) \times n$  matriz de verificação de paridade apropriada.

Escolher uma  $(n-k)$ -upla não nula como a primeira colu-

na da matriz de verificação de paridade  $H$ .

Para adicionar apropriadamente colunas subsequentes a  $H$  vamos supor que temos escolhido  $j - 1$  colunas  $h_1; h_2; \dots; h_{j-1}$ . Ainda que adicionando a  $j$ -ésima devemos assegurar dois pontos:

- (i) que quaisquer  $W - 1$  colunas serão linearmente independentes
- (ii) que  $h_j$  não será uma combinação linear das  $b - 1$  colunas precedentes junto com quaisquer  $b$  colunas consecutivas das primeiras  $j - b$  colunas.

Em outras palavras:

$$h_j = (a_{i1} h_{i1} + a_{i2} h_{i2} + \dots + a_{iW-2} h_{iW-2}) \quad (52)$$

e

$$h_j = (b_{j-b+1} h_{j-b+1} + b_{j-b+2} h_{j-b+2} + \dots + b_{j-1} h_{j-1}) + (c_t h_t + c_{t+1} h_{t+1} + \dots + c_{t+b-1} h_{t+b-1}) \quad (53)$$

onde  $h_i$ 's são quaisquer  $W - 2$  colunas anteriores e  $h_t$ 's são quaisquer  $b$  colunas consecutivas entre  $h_1, h_2, \dots, h_{j-b}$ . Como há  $q - 1$  coeficientes não nulos, portanto, o número de maneiras em que os coeficientes  $a_i$ 's podem ser escolhidos é

$$[ 1 + (q - 1) ]^{(j-1, W-2)} - 1 \quad (54)$$

Todas as possíveis combinações de  $W - 2$  colunas ou menos são incluídas em (54) portanto os coeficientes  $b_j$ 's e  $c_t$ 's serão escolhidos de tal modo que pelo menos  $W - 1$  tomados ao mesmo tempo são não nulos.

Para fazer isto, escolhemos um número  $r_1$  de  $b_j$ 's e um número  $r_2$  de  $c_t$ 's tais que  $r_1 + r_2 \geq W - 1$ . (Os maiores valores que  $r_1$  e  $r_2$  podem alcançar são  $b - 1$  e  $b$ , respectivamente.)

Agora, o número  $r_1$  de  $b_j$ 's pode ser escolhido em

$$\binom{b-1}{r_1} (q - 1)^{r_1} \quad (55)$$

maneiras. Para escolher o número  $r_2$  de  $c_t$ 's é equivalente avaliar o número de pedaços de comprimento menor ou igual a  $b$  com peso  $r_2$  em um vetor de comprimento  $j - b$ . Este pode ser dado em

$$I(q, j; b, r_2) \tag{56}$$

maneiras, onde  $I(q, j; b, r_2)$  denota a expressão dada no enunciado do Teorema. De (54), (55) e (56), o número total de combinações lineares para as quais  $h_j$  não pode ser igual é

$$[1+(q-1)]^{(j-1, W-2)} - 1 + \sum_{\substack{r_1+r_2=2b-1 \\ r_1, r_2: \\ r_1+r_2=W-1}} [(b-1) \binom{r_1}{r_1} (q-1)^{r_1} I(q, j; b, r_2)] \tag{57}$$

O pior caso concebível seria o de que, cada escolha dos coeficientes  $a_i$ 's,  $b_j$ 's e  $c_t$ 's forneça uma soma distinta.

Portanto, uma coluna  $h_j$  pode ser adicionada a  $H$  com a condição de que o conjunto total de  $q^{n-k} - 1$   $(n - k)$ -uplas não nulas não é esgotado por todas essas combinações lineares, isto é a  $j$ -ésima coluna pode ser sempre adicionada se

$$q^{n-k} - 1 > [1+(q-1)]^{(j-1, W-2)} - 1 + \sum_{\substack{r_1+r_2=2b-1 \\ r_1, r_2: \\ r_1+r_2=W-1}} [(b-1) \binom{r_1}{r_1} (q-1)^{r_1} I(q, j; b, r_2)] \tag{58}$$

Mas para um código  $[n, k]$  existir, a inequação (58) será válida para  $j = n$  e assim obteremos (51).

□

OBSERVAÇÃO:

O resultado obtido acima tem sido provado para  $W \leq 2b$ .

Para  $W > 2b$ , o peso mínimo do código torna-se pelo menos  $2b + 1$  e então o código é capaz de corrigir todos os erros de peso menor ou igual a  $b$  cobrindo em particular a correção de todos os pedaços de comprimento menor ou igual a  $b$ .

O termo envolvendo o somatório sobre  $r_1$  e  $r_2$  em (57) desaparece reduzindo o limite obtido em (51) ao limite de Varsharmov-Gilbert.

Corolário 3.3.2

Se não levarmos em consideração o peso imposto sobre o código, isto é, se  $W = 1$ , então, o somatório na inequação

(51) se divide no produto de dois termos separados dando

$$\sum_{r_1=0}^{b-1} \binom{b-1}{r_1} (q-1)^{r_1} = q^{b-1}$$

e

$$\sum_{r_2=0}^b I(q, j; b, r_2) = q^{b-1} [(q-1)(n-2b+1) + 1]$$

Além disso, no lugar da expressão (54) obtemos - 1 .

Então, o limite toma a forma

$$q^{n-k} > q^{2(b-1)} [(q-1)(n-2b+1) + 1]$$

que é um resultado dado no Teorema 2.1.5 fazendo  $b = b_g + 1$ .

### Exemplo 3.3.1

Consideremos o código linear binário  $[8,2]$  construído conforme Teorema 3.3.1 tomando  $W = 5$  e  $b = 3$ , cuja matriz de verificação de paridade é

$$\begin{pmatrix} 10000010 \\ 01000001 \\ 00100001 \\ 00010010 \\ 00001011 \\ 00000111 \end{pmatrix}$$

O peso mínimo do código é 5 e as síndromes dos vetores que são pedaços de comprimento menor ou igual a 3 são todas diferentes.



### 3.4 - CÓDIGOS CORRETORES DE PEDAÇOS DE ERRO E ERROS ALEATÓRIOS

Vamos impor a um código corretor de pedaço de erro a condição de corrigir erro aleatório, e deduziremos no Teorema seguinte, um limite superior sobre o número suficiente de dígitos de verificação que asseguram a existência de um tal código que corrige todos os erros aleatórios de peso menor ou igual a  $m$  e todos os pedaços de comprimento menor ou igual a  $b$ .

#### Teorema 3.4.1

Dados dois inteiros positivos  $m$  e  $b$  tais que  $m < b$ , uma condição suficiente para que exista um código linear  $[n, k]$ ,  $n > 2b$ , que corrige todas as combinações de peso menor ou igual a  $m$  e todos os pedaços de comprimento menor ou igual a  $b$  é

$$q^{n-k} > [1 + (q-1)]^{\binom{n-1}{2m-1}} + \sum_{\substack{r_1+r_2=b+m-1 \\ r_1, r_2: \\ r_1+r_2=2m}} [K(q, n; b, r_1) \binom{n-1}{r_2} (q-1)^{r_2}] + \\ + \left[ \sum_{i=m}^{b-1} \binom{b-1}{i} (q-1)^i \right] \left[ \binom{n-b-1}{m} (q-1)^m + L(q, n; b, m) \right] \quad (59)$$

onde  $0 \leq r_1 \leq b$ ,  $0 \leq r_2 \leq m-1$ ,

$$K(q, n; b, r) = \begin{cases} \binom{n-1}{r} (q-1)^r, & r = 0, 1 \\ (q-1)^r \sum_{i=r}^b \binom{i-2}{r-2} (n-i), & r \geq 2 \end{cases}$$

e

$$L(q, n; b, m) = \begin{cases} q^{b-1} [(q-1)(n-2b+1)+1] - 1, & \text{se } m = 0 \\ (q-1)^2 \sum_{i=m+1}^b (n-b-i+1) \sum_{j=m-1}^{i-2} \binom{i-2}{j} (q-1)^j, & \\ & \text{se } m \neq 0 \end{cases}$$

**Demonstração:**

Como anteriormente, tendo escolhido  $j - 1$  colunas  $h_1, h_2, \dots, h_{j-1}$  da matriz de verificação de paridade  $H$ , a  $j$ -ésima coluna  $h_j$  pode ser adicionada se ela cumpre três exigências postas abaixo.

Como uma primeira exigência, visto que o código é para corrigir todas as combinações de pêso menor ou igual a  $m$ , a coluna  $h_j$  para ser adicionada deverá ser tal que, não é uma combinação linear de quaisquer  $2m - 1$  colunas anteriores ou menos. Quaisquer  $2m - 1$  colunas ou menos fora das  $j - 1$  colunas podem ser escolhidas em

$$[ 1 + (q - 1) ]^{(j-1, 2m-1)} - 1 \quad (60)$$

maneiras.

Em seguida, desde que, o código com vetores de erro de pêso menor ou igual a  $m$  exigido para corrigir simultaneamente todos os erros que são pedaços de comprimento menor ou igual a  $b$ , a sĩndrome de qualquer vetor de erro de pêso menor ou igual a  $m$  não será igual a de qualquer vetor de erro que é um pedaço de comprimento menor ou igual a  $b$ .

A inequação (61) abaixo, assegura que a sĩndrome de qualquer vetor de erro de pêso menor ou igual a  $m$  não é igual a de qualquer vetor de erro que é um pedaço de comprimento menor ou igual a  $b$  fora das  $j$  componentes exceto quando o pedaço inclui a ũltima componente, isto é, a  $j$ -ésima e o vetor de pêso  $m$  correto é escolhido das primeiras  $j - b - 1$  componentes que é agora cuidado pela inequação (62).

Assim, a segunda exigência sobre  $h_j$  é que

$$h_j \neq (a_s h_s + a_{s+1} h_{s+1} + \dots + a_{s+b-1} h_{s+b-1}) + (b_{t_1} h_{t_1} + b_{t_2} h_{t_2} + \dots + b_{t_{m-1}} h_{t_{m-1}}) \quad (61)$$

e

$$h_j \neq (c_{j-b+1} h_{j-b+1} + c_{j-b+2} h_{j-b+2} + \dots + c_{j-1} h_{j-1}) + (d_{i_1} h_{i_1} + d_{i_2} h_{i_2} + \dots + d_{i_m} h_{i_m}) \quad (62)$$

onde as  $h'_s$  são quaisquer  $b$  colunas consecutivas e  $h'_t$  são quaisquer  $m - 1$  colunas entre as  $h_1, h_2, \dots, h_{j-1}$  e  $h'_j$  são quaisquer  $m$  colunas entre as  $h_1, h_2, \dots, h_{j-b-1}$  com todos os  $d'_i$  não nulos. Visto que todas as combinações lineares de  $2m - 1$  colunas ou menos são incluídos em (60) escolheremos coeficientes em (61) e (62) tais que os últimos  $2m$   $a'_s$  e  $b'_t$  tomados ao mesmo tempo e os últimos  $m$   $c'_i$  são não nulos.

Com o fim de assim escolher  $r_1$   $a'_s$  e  $r_2$   $b'_t$  tais que  $r_1 + r_2 \geq 2m$ . (Os maiores valores que  $r_1$  e  $r_2$  podem atingir são  $b$  e  $m - 1$ , respectivamente.)

Agora,  $r_1$   $a'_s$  que de um pedaço de comprimento menor ou igual a  $b$  com peso  $r_1$  num vetor de comprimento  $j - 1$ , podem ser escolhidos em

$$K(q, j; b, r_1) \quad (63)$$

maneiras (onde,  $K(q, j; b, r_1)$  denota a expressão dada no enunciado do Teorema) e  $r_2$   $b'_t$  em

$$\binom{j-1}{r_2} (q - 1)^{r_2} \quad (64)$$

maneiras. Além disso, pelo menos  $m$   $c'_j$  podem ser escolhidos em

$$\sum_{i=m}^{b-1} \binom{b-1}{i} (q - 1)^i \quad (65)$$

maneiras, enquanto o número de opções em que todos os  $d'_i$  não nulos podem ser escolhidos é

$$\binom{j-b-1}{m} (q - 1)^m \quad (66)$$

Finalmente, a possibilidade da mesma síndrome de quaisquer dois vetores de erro cada um dos quais é um pedaço de comprimento menor ou igual a  $b$  está excluída. Portanto, a terceira exigência força que

$$h_j \neq (e_k h_k + e_{k+1} h_{k+1} + \dots + e_{k+b-1} h_{k+b-1}) + (f_{j-b+1} h_{j-b+1} + f_{j-b+2} h_{j-b+2} + \dots + f_{j-1} h_{j-1}) \quad (67)$$

onde  $h'_k$  são quaisquer  $b$  colunas consecutivas entre as  $h_1, h_2, \dots, h_{j-b}$ . Tendo em vista as situações consideradas anteriormente,

é claro que pelo menos  $m f_j^0$  juntamente com pelo menos

$$(m + 1) e_k^1$$

serão tornados não nulos. O número de maneiras em que pelo menos  $m f_j^1$  podem ser escolhidos já foi dado na expressão (65).

Do mesmo modo, pelo menos  $(m + 1) e_k^1$ , que formam um pedaço de comprimento menor ou igual a  $b$  tendo peso maior ou igual a  $m + 1$  em um vetor de comprimento  $j - b$ , podem ser escolhidos em

$$L(q, j; b, m) \quad (68)$$

maneiras (onde,  $L(q, j; b, m)$  denota a expressão dada no enunciado do Teorema).

De (60), (63), (64), (65), (66) e (67), o número total de combinações lineares é

$$\begin{aligned} & [1 + (q-1)]^{\binom{j-1, 2m-1}{-1}} + \sum_{\substack{r_1, r_2: \\ r_1+r_2=2m \\ r_1+r_2=b+m-1}} [K(q, j; b, r_2) \binom{j-1}{r_2} (q-1)^{r_2}] + \\ & + \left[ \sum_{i=m}^{b-1} \binom{b-1}{i} (q-1)^i \right] \left[ \binom{j-b-1}{m} (q-1)^m + L(q, j; b, m) \right] \end{aligned} \quad (69)$$

Logo, um vetor  $h_j$  para todas as escolhas dos coeficientes deve existir se

$$\begin{aligned} q^{n-k-1} & > [1 + (q-1)]^{\binom{j-1, 2m-1}{-1}} + \sum_{\substack{r_1, r_2: \\ r_1+r_2=2m \\ r_1+r_2=b+m-1}} [K(q, j; b, r_2) \binom{j-1}{r_2} (q-1)^{r_2}] + \\ & + \left[ \sum_{i=m}^{b-1} \binom{b-1}{i} (q-1)^i \right] \left[ \binom{j-b-1}{m} (q-1)^m + L(q, j; b, m) \right] \end{aligned} \quad (70)$$

Assim, um código  $[n, k]$  existirá se a inequação (70) é satisfeita para  $j = n$  e então obteremos (59).

□

#### OBSERVAÇÃO:

O Teorema acima foi provado para  $m < b$ . Contudo, se  $m \geq b$  a consideração de pedaço torna-se redundante e o segundo termo em (69), isto é, o somatório em  $r_1$  e  $r_2$  e a expres

são (65), isto é, o somatório em  $i$  desaparecem.

Então, o limite obtido em (59) se reduz ao limite de Varsharov-Gilbert.

### Corolário 3.4.2

Separando a condição correção de erro aleatório, isto é, pondo  $m = 0$ , o somatório na inequação (59) se divide no produto de dois termos separados a saber

$$\sum_{r_1=0}^b K(q, n; b, r_1)$$

e

$$\sum_{r_2=0}^{m-1} \binom{n-1}{r_2} (q-1)^{r_2} = [1 + (q-1)]^{\binom{n-1, m-1}} = [1 + (q-1)]^{\binom{n-1, -1}} = 0$$

Do mesmo modo, para  $m = 0$

$$[1 + (q-1)]^{\binom{n-1, 2m-1}} = 0$$

$$\sum_{i=m}^{b-1} \binom{b-1}{i} (q-1)^i = q^{b-1}$$

e

$$\begin{aligned} \binom{n-b-1}{m} (q-1)^m + L(q, n; b, m) &= 1 + L(q, n; b, 0) = \\ &= q^{b-1} [(q-1)(n-2b+1) + 1]. \end{aligned}$$

Assim, como no Corolário 3.3.2, o limite em (59) se reduz ao resultado dado no Teorema 2.1.5, fazendo  $b = b_g + 1$ .

### Exemplo 3.4.1

Consideremos um código linear binário  $[8,2]$  construído conforme Teorema 3.4.1, tornando  $m = 2$  e  $b = 3$  cuja matriz de verificação de paridade é

$$\begin{pmatrix} 1000010 \\ 0100011 \\ 0010001 \\ 00010010 \\ 00001011 \\ 00000101 \end{pmatrix}$$

As síndromes dos vetores de erro único, duplo e triplo adjacentes são diferentes, portanto, este código pode corrigir todos os erros aleatórios de peso menor ou igual a 2 e todos os pedaços de comprimento menor ou igual a 3, isto é, corrige todos os erros únicos, duplos e triplos adjacentes.

## C O N C L U S Ã O

Os cõdigos lineares podem ser usados para correção e detecção de erros aleatõrios e ou pedaços de erros.

Uma das vantagens destes cõdigos é que podem ser implementados facilmente.

Neste trabalho os cõdigos lineares foram desenvolvidos associando um critério de pêsos para o pedaço e sobre os cõdigos usados para correção de pedaços.

Esperamos com a utilização destes tipos de cõdigos poderemos economizar dígitos de verificação e, conseqüentemente, incrementar a taxa do cõdigo.

## B I B L I O G R A F I A

- [1] CHIEN, R.T. & TANG, D.T. On definitions of a burst. IBM J.Res. & Develop., Jul. : 292-3, 1965.
- [2] DASS, Bal Kishan. A bound of error detecting burst codes. J. of Comb. Inf. & Sys. Sci., 1:21-4, 1976.
- [3] \_\_\_\_\_. A sufficient bound for codes correcting burst with weight constraint. J. Assoc. Comptu. Mach., 22:501-3, 1975.
- [4] ELLIOT, E.O. A model of the switched telephone network for data communications. Bell Syst. Tech. J., 44:89-109, 1965.
- [5] GILBERT, E.N. Capacity of a burst-noise channel. Bell Syst. Tech. J., 39:1253-65, 1960.
- [6] LIN, Shu. An Introduction to error-correcting codes. New Jersey, Englewood Cliffs, 1970.
- [7] MAC WILLIAMS, F.J. A theorem of the distribution of weights in a systematic code. Bell Syst. Tech. J., 42:79-94, 1963.
- [8] MAC WILLIAMS, F.J. & SLOANE, N.J.A. The theory of error-correcting codes. North Holland, Publishing Co., 1977.
- [9] PETERSON, W.W. & WELDON JUNIOR, E.J. Error-correcting codes. Massachusetts, Massachusetts Institute of Technology, 1972. 2nd Edition.



- [10] PLESS, Vera. Introduction to the theory of error correcting codes. New York, John Wiley & Sons, 1982.
- [11] PLOTKIN, M. Binary codes with specified minimum distance. IRE Trans. Inf. Theory, 6:445-50. Also Research Division Report, 51-20, University of Pennsylvania. January, 1951.
- [12] RIEGER, S.H. Codes for the correction of "clustered" errors. IRE Trans., IT-6, 16-21, 1960.
- [13] SHARMA, Bhu Dev & DASS, Bal Kishan. Extended Varsharmov-Gilbert and sphere-packing bounds for burst-correcting codes. IEEE Trans. Inf. Theory, 20:291-2, 1974.
- [14] \_\_\_\_\_. \_\_\_\_\_. Bounds for burst-error and random-error correcting linear codes. Indian J. of Pure & Appl. Math., 6:294-302, 1975.
- [15] \_\_\_\_\_. \_\_\_\_\_. On weights of burst. Indian J. of Pure & Appl. Math., 8:1519-24, 1977.
- [16] WYNER, A.D. Low-density-burst-correcting codes. IEEE Trans. Inf. Th., IT-9:124, 1963.