

UNIVERSIDADE FEDERAL DE SANTA CATARINA
(U F S C)

DISTRIBUIÇÃO DE PESO DOS CÓDIGOS

Waldemar Bernardi

Florianópolis, março de 1986.

DISTRIBUIÇÃO DE PESOS DOS CÓDIGOS

por

WALDEMAR BERNARDI

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

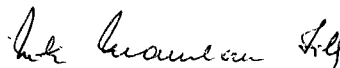
BANCA EXAMINADORA:



Prof. Gur Dial, Ph.D.
Orientador



Prof. Paul James Otterson, Ph.D.



Prof. Nelson Maculan Filho, Ph.D.

AGRADECIMENTOS

A todos que, de alguma forma, colaboraram na realização deste trabalho, em especial:

- Ao Professor Gur Dial (Ph. D.), pela orientação segura e precisa.
- Ao Professor Antônio de Souza Rauen, pelo apoio e colaboração.
- À Doroti, pela paciência e compreensão.
- Ao Wagner, Cristian e Rafael, que neste período não tiveram a atenção merecida.

À Doroti

ÍNDICE

CAPÍTULO I - Conceitos Preliminares		págs.
1.1	- Introdução	06
1.2	- A Álgebra de Grupo	06
1.3	- Resíduos Quadráticos	07
1.4	- Caracteres	09
1.5	- Matrizes do Tipo Hadamard e Conferência.	10
1.6	- Polinômios de Krawtchouk	17
CAPÍTULO II - Códigos Lineares e Não Lineares.		
2.1	- Introdução	21
2.2	- Códigos Lineares	21
2.3	- Descrição dos Códigos Lineares pelas Matrizes.	22
2.4	- Algumas Construções de Códigos Lineares.	26
2.5	- Códigos não Lineares	28
2.6	- Códigos de Hadamard	31
2.7	- Códigos Não Lineares Usando Matr. de Conferência	33
CAPÍTULO III - Enumeradores de Peso.		
3.1	- Introdução	35
3.2	- Códigos Homogêneos e Distribuição de Pesos	36
3.3	- Distribuição de Peso do Dual de um Código Linear Binário	38
3.4	- Momentos de Distribuição de Pesos	42
3.5	- Generalização do Teorema de MacWilliams para Códigos Lineares	44
3.6	- Teorema de Mac Williams para Códigos Não Lineares.	48
CAPÍTULO IV - Probabilidade de Erro Não Detectado.		
4.1	- Introdução	50
4.2	- Probabilidade de Erro Não Detectado	50
4.3	- Probabilidade de Erro Não Detectado para Códigos Lineares Não Binários	56
	- Conclusão	60
	- Bibliografia	61

RESUMO

A parte essencial do nosso trabalho trata da distribuição de peso dos códigos. Para isto, definimos o enumerador de peso dos códigos, a fim de estabelecer uma relação importante entre a distribuição de pesos de um código e a distribuição de pesos do seu código dual.

O nosso trabalho está dividido em quatro capítulos. No primeiro, vemos alguns conceitos básicos necessários para o desenvolvimento deste trabalho. Damos uma noção sobre álgebra de grupo, resíduos quadráticos, caracteres, matrizes do tipo Hadamard e Conferência e polinômios de Krawtchouk.

No segundo capítulo definimos códigos lineares, suas propriedades, matriz geratriz, matriz de verificação de paridade e dual dos códigos lineares. Além disso, definimos códigos não lineares e vimos algumas construções para esses códigos.

No capítulo três estudamos os enumeradores de pesos dos códigos. Nesse capítulo estabelecemos alguns resultados sobre a distribuição de pesos. Vimos as equações de MacWilliams que dão uma relação surpreendente e importante entre a distribuição de pesos de um código C e a distribuição de pesos do seu código dual (C^\perp). Estudamos também, as equações de momentos determinadas por Pless, que são uma família infinita de equações equivalentes às equações de MacWilliams.

No capítulo quatro aplicamos os enumeradores de peso para a determinação da probabilidade de erro não detectado na transmissão de dados.

CAPÍTULO I

CONCEITOS PRELIMINARES:

1.1 - Introdução - O problema da transmissão confiável de informação tem representado um desafio constante para engenheiros e pesquisadores em comunicações. A confiabilidade a que nos referimos diz respeito à ação do ruído e de outras interferências.

Frequentemente, no contexto das comunicações digitais ocorrem erros. Os códigos corretores de erro foram inventados para detectar e/ou corrigir possíveis erros que tenham ocorrido durante uma transmissão. Muitos tipos de códigos já foram desenvolvidos junto com processos de decodificação que torna possível a implementação dos mesmos.

Os objetivos da teoria de codificação, são basicamente:

- (i) - encontrar códigos longos e eficientes,
- (ii) - encontrar métodos práticos de codificação e decodificação eficientes.

Os desenvolvimentos recentes na tecnologia de "hardware" digital tornaram possível o uso de esquemas de codificação bastante complexos.

Neste capítulo veremos alguns conceitos básicos que serão necessários para o desenvolvimento deste trabalho.

1.2 Álgebra de Grupo. [02]

Uma n-upla binária sobre o corpo binário $GF(2)$, é um conjunto ordenado de n elementos do corpo e será denotado por (a_1, a_2, \dots, a_n) , onde $a_i = 0$ ou 1 , $i = 1, 2, \dots, n$. Podemos representar as n-uplas binárias por polinômios em z_1, z_2, \dots, z_n . A n-upla $1\ 0\ 0\ \dots\ 0$ será representada por z_1 ; $0\ 1\ 0\ \dots\ 0$, por z_2 ; $1\ 0\ 1\ 0\ 0\ \dots\ 0$ por $z_1 z_3$ e assim sucessivamente. Em geral $a = (a_1, a_2, \dots, a_n)$ será representado por $z_1^{a_1} z_2^{a_2} \dots z_n^{a_n} = z^a$. É possível ver, com facilidade, que dado z^a podemos determinar a.

Usaremos a convenção que $z_i^2 = 1, \forall i$. Usando esta estrutura, o conjunto de todos os z^v torna-se um grupo multiplicativo e será denotado por G.

Seja F_2^n o grupo de todas as n-uplas binárias. Então, podemos ver que F_2^n e G são grupos isomórficos. Com adição em F_2^n

$$v + w = (v_1, v_2, \dots, v_n) + (w_1, w_2, \dots, w_n) = (v_1 + w_1, v_2 + w_2, \dots, v_n + w_n)$$

correspondente a multiplicação em G,

$$z^V \cdot z^W = (z_1^V \cdot z_2^V \dots z_n^V) \cdot (z_1^W \cdot z_2^W \dots z_n^W) = z_1^{V+W} \cdot z_2^{V+W} \dots z_n^{V+W} \\ = z^{V+W}$$

Definição 1.2.1 - A álgebra de grupo QG, de G sobre os números racionais (Q), consiste de todas as somas:

$$\sum_{v \in F_2^n} a_v z^v, \quad a_v \in Q, \quad z^v \in G \tag{1.2.1}$$

A adição e multiplicação em QG são definidas por:

$$\sum_{v \in F_2^n} a_v z^v + \sum_{v \in F_2^n} b_v z^v = \sum_{v \in F_2^n} (a_v + b_v) z^v.$$

$$r \sum_{v \in F_2^n} a_v z^v = \sum_{v \in F_2^n} r a_v z^v, \quad r \in Q$$

$$e \sum_{v \in F_2^n} a_v z^v \cdot \sum_{w \in F_2^n} b_w z^w = \sum_{v, w \in F_2^n} (a_v \cdot b_w) z^{v+w}.$$

OBSERVAÇÃO. - A álgebra de grupo QG fornece uma notação algébrica para códigos, que veremos no capítulo III.

1.3 - Resíduos Quadráticos. [02]

Para a construção de códigos não-lineares (serão definidos no capítulo II) precisamos alguns conceitos sobre resíduos quadráticos.

Definição 1.3.1 - Seja p um primo ímpar. Os quadrados não nulos mód p são chamados resíduos quadráticos mód p.

Exemplo 1.3.1 .

Seja p = 11. Os resíduos quadráticos mód 11 são dados por:

$1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 \equiv 5, 5^2 = 25 \equiv 3$, i.é., 1, 3, 4, 5, 9 são resíduos quadráticos mód 11.

OBSERVAÇÃO 1.

Para achar os resíduos quadráticos ou simplesmente os resíduos mód p é suficiente considerar os quadrados dos números de 1 até $p-1$.

OBSERVAÇÃO 2.

Há $(1/2)(p-1)$ resíduos mód p . Os $(1/2)(p-1)$ números restantes são chamados não resíduos.

OBSERVAÇÃO 3.

Zero não é nem resíduo, nem não resíduo.

OBSERVAÇÃO 4.

O produto de dois resíduos quadráticos ou de dois não resíduos é um resíduo quadrático, enquanto que o produto de um resíduo quadrático por um não resíduo quadrático é um não resíduo.

Definição 1.3.2. - Seja p um primo ímpar. Então a função ϕ_p chamada símbolo de Legendre, é definida sobre os inteiros, por:

$$\phi_p(i) = \begin{cases} 0, & \text{se } i \text{ é múltiplo de } p \\ 1, & \text{se o resto é um resíduo mód } p, \text{ quando } i \text{ é dividido por } p \\ -1, & \text{se o resto não é resíduo.} \end{cases}$$

Exemplo 1.3.2.

Seja $p = 11$. Então,

$$\phi(6) = -1$$

$$\phi(12) = 1$$

$$\phi(3) = 1$$

$$\phi(22) = 0$$

Teorema 1.3.1. - Para todo $c \not\equiv 0 \pmod{p}$,

$$\sum_{b=0}^{p-1} \phi(b) \phi(b+c) = -1$$

Demonstração. - Sabemos que,

$$\phi(xy) = \phi(x) \phi(y), \quad 0 \leq x \leq p-1 \text{ e } 0 \leq y \leq p-1$$

Quando $b = 0$ a soma não se altera. Consideremos então, $b \neq 0$.
 Seja $m = \left(\frac{b+c}{b}\right) \pmod{p}$. Para cada b existe um único inteiro m , $0 \leq m \leq p-1$.
 Como b varia de 1 a $p-1$, m toma os valores $0, 2, 3, \dots, p-1$, mas, não 1. En-
 tão

$$\begin{aligned} \sum_{b=1}^{p-1} \phi(b) \phi(b+c) &= \sum_{b=1}^{p-1} \phi(b) \phi(bm) \\ &= \sum_{b=1}^{p-1} [\phi(b)]^2 \phi(m) \\ &= \sum_{\substack{m=0 \\ m \neq 1}}^{p-1} \phi(m) \end{aligned}$$

Usando a observação 2, temos que

$$\sum_{m=0}^{p-1} \phi(m) = 0.$$

Portanto,

$$\sum_{\substack{m=0 \\ m \neq 1}}^{p-1} \phi(m) = 0 - \phi(1) = -1.$$

logo,

$$\sum_{b=0}^{p-1} \phi(b) \phi(b+c) = -1.$$

1.4 - Caracteres. [02]

Definição 1.4.1 - Seja a transformação ψ_u de G para para os números racionais Q , dada por

$$\psi_u(z^v) = (-1)^{u \cdot v}, \text{ para todo } u \in F_2^n,$$

onde, $u \cdot v$ é o produto escalar dos vetores u e v sobre Q . ψ_u é chamado "caracter" de G .

Usando a linearidade, ψ_u pode ser estendida sobre QG , i.é.,

$$\psi_u\left(\sum_{v \in F_2^n} a_v z^v\right) = \sum_{v \in F_2^n} a_v \psi_u(z^v) = \sum_{v \in F_2^n} a_v (-1)^{u \cdot v} \quad (1.4.1)$$

OBSERVAÇÃO.

$$\psi_u(z^v) = \begin{cases} 1, & \text{se } u \text{ e } v \text{ são ortogonais} \\ -1, & \text{caso contrário.} \end{cases}$$

No próximo teorema veremos algumas propriedades de ψ_u .

Teorema 1.4.1.

- (i) $\psi_u(z^v) = \psi_v(z^u)$
- (ii) $\psi_u(z^v) \psi_u(z^w) = \psi_u(z^{v+w})$
- (iii) $\psi_u(z^w) \psi_v(z^w) = \psi_{u+v}(z^w)$.

Demonstração.

- (i) $\psi_v(z^u) = (-1)^{u \cdot v} = (-1)^{v \cdot u} = \psi_u(z^v)$
- (ii) $\psi_u(z^v) \psi_u(z^w) = (-1)^{u \cdot v} \cdot (-1)^{u \cdot w} = (-1)^{u \cdot (v+w)} = \psi_u(z^{v+w})$
- (iii) $\psi_u(z^w) \cdot \psi_v(z^w) = (-1)^{u \cdot w} \cdot (-1)^{v \cdot w} = (-1)^{u \cdot v + v \cdot w} = (-1)^{(u+v) \cdot w} =$
 $= \psi_{u+v}(z^w)$.

1.5 - Matrizes do Tipo Hadamard e Conferência. [02]

Definição 1.5.1. - Uma matriz de Hadamard H , de ordem n , é uma matriz $n \times n$ formada por 1's e -1's, tais que:

$$HH^t = nI, \tag{1.5.1}$$

onde I é a matriz identidade de ordem n .

A equação (1.5.1) implica que o produto interno de quaisquer duas linhas distintas de H é zero, i.é., as linhas distintas são ortogonais. Além disso, o produto interno de qualquer linha por ela mesma é n .

OBSERVAÇÃO 1.

Como $H^{-1} = (1/n)H^t$ temos também que $H^t H = nI$, i. é., as colunas de H têm as mesmas propriedades.

OBSERVAÇÃO 2.

Multiplicando-se qualquer linha ou coluna de H por -1 obtém-se uma outra matriz de Hadamard. Desta maneira podemos tornar a primeira linha e a primeira coluna de H em +1's.

Definição 1.5.2. - A matriz H de Hadamard em que a primeira linha e a primeira coluna são formadas por +1's é chamada matriz de Hadamard normalizada.

Exemplo 1.5.2.

As matrizes normalizadas de ordem 1, 2, 4 e 8 são:

Para n = 1, $H_1 = [1]$. Para n = 2, $H_2 = \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix}$. Para n = 4,

$H_4 = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{vmatrix}$. Para n = 8,

$H_8 = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{vmatrix}$

OBSERVAÇÃO 1.

O traço significa -1, ou seja "-" = -1.

OBSERVAÇÃO 2.

Estas matrizes são chamadas matrizes de Hadamard do tipo Sylvester.

Se a matriz de Hadamard existe, qual seria o valor de n? Veremos isto no teorema seguinte.

Teorema 1.5.1 - Se a matriz de Hadamard de ordem n existe, então n é 1, 2 ou um múltiplo de 4.

Demonstração.

Sem perda de generalidade supomos que H é normalizada. Suponha que n = 3. Sejam as três primeiras linhas como segue:

$$\begin{array}{cccc} 1 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & - & - & \dots & - & - & - & \dots & - \\ 1 & 1 & 1 & \dots & 1 & - & - & \dots & - & 1 & 1 & \dots & 1 & - & - & \dots & - \end{array}$$

$\underbrace{\hspace{1.5em}}_1 \quad \underbrace{\hspace{1.5em}}_1 \quad \underbrace{\hspace{1.5em}}_1 \quad \underbrace{\hspace{1.5em}}_1$

Como as linhas são ortogonais, temos que:

$$i + j - k - l = 0$$

$$i - j + h - l = 0$$

$$i - j - k + l = 0$$

o que implica que $i = j = k = l$, e, portanto, $n = 4i$. Logo n é um múltiplo de 4.

Várias construções de matrizes de Hadamard são conhecidas. Veremos duas delas, as quais são importantes para a construção de códigos:

CONSTRUÇÃO 1. - Se H_n é uma matriz de Hadamard de ordem n , então:

$$H_{2n} = \begin{vmatrix} H_n & H_n \\ H_n & -H_n \end{vmatrix}$$

é a matriz de Hadamard de ordem $2n$.

Usando esta construção podemos determinar todas as matrizes de Hadamard cuja ordem é uma potência de 2. Começando com $H_1 = [1]$, obtemos H_2, H_4, H_8 e assim por diante. Na literatura estas matrizes são chamadas matrizes de Siyvester.

CONSTRUÇÃO II. - (Construção de Paley). - Esta construção se baseia no conceito de resíduo quadrático mód p e, dá a matriz de Hadamard de ordem $n = p+1$, o qual é um múltiplo de 4 (ou $n = p^m + 1$ se utilizarmos resíduos quadráticos de um corpo de Galois de ordem p^m , i.é., $GF(p^m)$).

Primeiro definimos a matriz de Jacobsthal.

Definição 1.5.3 - (Matriz de Jacobsthal). - A matriz $Q = (q_{ij})$, de Jacobsthal, é uma matriz $p \times p$ cujas linhas e colunas são enumeradas de 0 a $p-1$ e $q_{ij} = \phi(j-1)$.

Exemplo 1.5.2

Seja $p = 7$

$$Q = \begin{matrix} & \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} & \begin{vmatrix} 0 & 1 & 1 & -1 & - & - & - \\ - & 0 & 1 & 1 & -1 & - & - \\ - & - & 0 & 1 & 1 & -1 & - \\ 1 & - & - & 0 & 1 & 1 & - \\ - & 1 & - & - & 0 & 1 & 1 \\ 1 & - & 1 & - & - & 0 & 1 \\ 1 & 1 & - & 1 & - & - & 0 \end{vmatrix} \end{matrix}$$

OBSERVAÇÃO.

$q_{ij} = -q_{ji}$, i.é., Q é anti-simétrica, pois p é da forma $4k-1$.

Lema 1.5.2 - $QQ^t = pI - J$ e $QJ = JQ = 0$, onde J é a matriz cujos elementos são todos iguais a 1.

Demonstração.

Seja $P = [p_{ij}] = QQ^t$. Então, se $i = j$, temos que:

$$p_{ii} = \sum_{k=0}^{p-1} q_{ik}^2 = p-1.$$

para $i \neq j$, temos que

$$p_{ij} = \sum_{k=0}^{p-1} q_{ik}q_{jk} = \sum_{k=0}^{p-1} \phi(k-i)\phi(k-j) = \sum_{k=0}^{p-1} \phi(b)\phi(b+c) = -1,$$

onde, $b = k-i$ e $c = i-j$.

Logo, $QQ^t = pI - J$.

Tendo em vista que cada linha e cada coluna de Q contém um número de +1's igual a $(1/2)(p-1)$ e um número igual de -1's, temos que

$$QJ = JQ = 0$$

Teorema 1.5.3 - (Construção de Paley). - Seja,

$$H = \begin{vmatrix} 1 & \underline{1} \\ \underline{1}^t & Q-I \end{vmatrix},$$

onde H é uma matriz de Hadamard. O $\underline{1}^t$ é um vetor coluna com cada componente igual a 1.

Demonstração.

$$HH^t = \begin{vmatrix} 1 & \underline{1} \\ \underline{1}^t & Q-I \end{vmatrix} \begin{vmatrix} 1 & \underline{1} \\ \underline{1}^t & Q^t-I \end{vmatrix} = \begin{vmatrix} p+1 & 0 \\ 0 & J+(Q-I)(Q^t-I) \end{vmatrix}$$

Mas pelo lema (1.5.2), $J+(Q-I)(Q^t-I) = J + pI - J - Q - Q^t + I = (p+1)I$. Portanto, $HH^t = (p+1)I_{p+1}$. Logo, H é uma matriz de Hadamard, de ordem $p+1$.

OBSERVAÇÃO.

Esta matriz é dita do tipo Paley.

Exemplo 1.5.3

Seja $p = 7$ e $p = 11$. Então, as matrizes de Hadamard de ordem 8 e 12, são, respectivamente, dadas por:

$$H_8 = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & 1 & - & 1 & - & - \\ 1 & - & - & 1 & 1 & - & 1 & - \\ 1 & - & - & - & 1 & 1 & - & 1 \\ 1 & 1 & - & - & - & 1 & 1 & - \\ 1 & - & 1 & - & - & - & 1 & 1 \\ 1 & 1 & - & 1 & - & - & - & 1 \\ 1 & 1 & 1 & - & 1 & - & - & - \end{vmatrix}$$

$$H_{12} = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - \\ 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 \\ 1 & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - \\ 1 & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - \\ 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 \\ 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 \\ 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - \\ 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 \\ 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - \end{vmatrix}$$

As matrizes de conferência são semelhantes às matrizes de Hadamard, mas tem uma pequena diferença na definição.

Definição 1.5.4 - (Matriz de Conferência). - Uma matriz de conferência C , de ordem n é uma matriz com os elementos da diagonal principal todos nulos e os outros são $+1$ ou -1 , satisfazendo:

$$C.C^t = (n - 1)I \tag{1.5.2}$$

Como as matrizes de Hadamard, podemos normalizar C de modo que tenha a forma:

$$C = \begin{vmatrix} 0 & 1 \\ \underline{1}^t & S \end{vmatrix} \tag{1.5.3}$$

onde S é uma matriz quadrada de ordem $n-1$ satisfazendo,

$$SS^t = (n - 1)I - J, \quad SJ = JS = 0 \quad (1.5.4)$$

Exemplo 1.5.4.

As matrizes normalizadas de conferência de ordem 2 e 4, são

$$C_2 = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \quad e \quad C_4 = \begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & - \\ 1 & - & 0 & 1 \\ 1 & 1 & - & 0 \end{vmatrix}$$

Várias construções são conhecidas. A mais útil para o desenvolvimento dos códigos é a seguinte:

CONSTRUÇÃO (Paley)

Definição 1.5.5 - Seja $n = p^m + 1 = 2 \pmod{4}$, onde p é um primo ímpar. Definimos a matriz $p^m \times p^m$ de Jacosthal como sendo a matriz

$Q = (q_{ij})$, onde $q_{ij} = \phi(j - i)$. Como $p^m = 1 \pmod{4}$ implica que Q é simétrica. Então,

$$C = \begin{vmatrix} 0 & \underline{1} \\ \underline{1}^t & Q \end{vmatrix}$$

é a matriz de conferência simétrica de ordem n .

Exemplo 1.5.5

Seja $n = 6$, então $p^m = 5$

$$C_6 = \begin{matrix} & & & 0 & 1 & 2 & 3 & 4 \\ & & & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & & & 1 & 0 & 1 & - & - & 1 \\ 1 & & & 1 & 1 & 0 & 1 & - & - \\ 2 & & & 1 & - & 1 & 0 & 1 & - \\ 3 & & & 1 & - & - & 1 & 0 & 1 \\ 4 & & & 1 & 1 & - & - & 1 & 0 \end{matrix}$$

Exemplo 1.5.6.

Seja $n = 14$, então $p^m = 13$.

OBSERVAÇÃO.

Estes polinômios têm a função geratriz:

$$(1 + \gamma z)^{n-x} (1-z)^x = \sum_{k=0}^{\infty} P_k(x) z^k \quad (1.6.2)$$

Se x é um inteiro ($0 \leq x \leq n$), então, no lado direito de (1.6.2) o limite superior pode ser substituído por n .

No seguinte teorema daremos duas expressões alternativas para polinômios de Krawtchouk.

Teorema 1.6.1 - (Expressões Alternativas).

$$(i) - P_k(x) = \sum_{j=0}^k (-q)^j \gamma^{k-j} \binom{n-j}{k-j} \binom{x}{j} \quad (1.6.3)$$

$$(ii) - P_k(x) = \sum_{j=0}^k (-1)^j q^{k-j} \binom{n-k+j}{j} \binom{n-x}{k-j} \quad (1.6.4)$$

Demonstração.

$$\begin{aligned} (i) - (1 + \gamma z)^{n-x} (1 - z)^x &= (1 + \gamma z)^n \left(1 - \frac{qz}{1 + \gamma z}\right)^x \\ &= (1 + \gamma z)^n \sum_{j=0}^{\infty} \binom{x}{j} \frac{(-qz)^j}{(1 + \gamma z)^j} \\ &= \sum_{j=0}^{\infty} (-qz)^j (1 + \gamma z)^{n-j} \binom{x}{j} \\ &= \sum_{j=0}^{\infty} (-q)^j z^j \binom{x}{j} \sum_{j=0}^k \binom{n-j}{k-j} (\gamma z)^{k-j} \\ &= \sum_{j=0}^{\infty} \sum_{j=0}^k (-q)^j z^j \binom{x}{j} \binom{n-j}{k-j} \gamma^{k-j} z^{k-j} \\ &= \sum_{j=0}^{\infty} \sum_{j=0}^k (-q)^j \gamma^{k-j} \binom{n-j}{k-j} \binom{x}{j} z^k. \end{aligned}$$

O coeficiente de z^k é:

$$\sum_{j=0}^k (-q)^j \gamma^{k-j} \binom{n-j}{k-j} \binom{x}{j}.$$

Logo,

$$P_k(x) = \sum_{j=0}^k (-q)^j \gamma^{k-j} \binom{n-j}{k-j} \binom{x}{j}.$$

$$\begin{aligned}
 \text{(ii) } - (1 + \gamma z)^{n-x} (1-z)^x &= (1-z)^n \left(1 + \frac{\gamma z}{1-z}\right)^{n-x} \\
 &= (1-z)^n \sum_{j=0}^{\infty} \binom{n-x}{k-j} \left(\frac{\gamma z}{1-z}\right)^{k-j} \\
 &= \sum_{j=0}^{\infty} \binom{n-x}{k-j} \gamma^{k-j} z^{k-j} (1-z)^{n-k+j} \\
 &= \sum_{j=0}^{\infty} \binom{n-x}{k-j} \gamma^{k-j} z^{k-j} \sum_{j=0}^k \binom{n-k+j}{j} (-1)^j z^j \\
 &= \sum_{j=0}^{\infty} \sum_{j=0}^k \binom{n-x}{k-j} \binom{n-k+j}{j} \gamma^{k-j} (-1)^j z^k
 \end{aligned}$$

O coeficiente de z^k é,

$$\sum_{j=0}^k (-1)^j \gamma^{k-j} \binom{n-x}{k-j} \binom{n-k+j}{j} = P_k(x).$$

Teorema 1.6.2 - Os polinômios de Krawtchok satisfazem a fórmula de recorrência:

$$(k+1)P_{k+1}(x) = [(n-k)\gamma + k - \gamma x]P_k(x) - \gamma(n-k+1)P_{k-1}(x) \quad (1.6.5)$$

com $k = 1, 2, \dots$, e com as condições iniciais $P_0(x) = 1, P_1(x) = \gamma n - \gamma x$

Demonstração.

$$(1 + \gamma z)^{n-x} (1-z)^x = \sum_{k=0}^{\infty} P_k(x) z^k \quad (1.6.2)$$

Derivando em relação a z , temos:

$$(n-x)(1 + \gamma z)^{n-x-1} \gamma (1-z)^x - (1 + \gamma z)^{n-x} x(1-z)^{x-1} = \sum_{k=1}^{\infty} P_k(x) k z^{k-1}$$

Multiplicando por $(1 + \gamma z)(1-z)$, temos:

$$(n-x)\gamma(1-z)^{x+1} (1 + \gamma z)^{n-x} - x(1 + \gamma z)^{n-x+1} (1-z)^x = \sum_{k=1}^{\infty} P_k(x) k z^{k-1} (1 + \gamma z)(1-z).$$

Donde,

$$(1 + \gamma z)^{n-x} (1-z)^x [(n-x)\gamma(1-z) - x(1 + \gamma z)] = \sum_{k=1}^{\infty} P_k(x) k z^{k-1} [1 - z + \gamma z - \gamma z^2]$$

$$(1 + \gamma z)^{n-x} (1-z)^x [\gamma n - \gamma n z - \gamma x + \gamma x z - x - \gamma x z] = \sum_{k=1}^{\infty} P_k(x) k z^{k-1} [1 + z(\gamma - 1) - \gamma z^2].$$

$$\sum_{k=0}^{\infty} P_k(x) z^k [\gamma n - \gamma n z - x(1 + \gamma)] = \sum_{k=1}^{\infty} P_k(x) k z^{k-1} [1 + z(\gamma - 1) - \gamma z^2].$$

$$[\gamma n - \gamma n z - x(1 + \gamma)] [P_0(x) + P_1(x)z + P_2(x)z^2 + \dots] = [P_1(x)z^0 + 2P_2(x)z + 3P_3(x)z^2 + \dots] \cdot [1 + z(\gamma - 1) - \gamma z^2].$$

$$P_0(x) \gamma^{n-x} (1+\gamma) P_0(x) - P_0(x) \gamma^n z - P_1(x) x (1+\gamma) z + \gamma^n P_1(x) z - \gamma^n P_1(x) z^2 + \gamma^n P_2(x) z^2 -$$

$$x (1+\gamma) P_2(x) z^2 - \gamma^n P_2(x) z^3 + \dots = P_1(x) + P_1(x) (\gamma-1) z - \gamma P_1(x) z^2 + 2P_2(x) z +$$

$$+ 2P_2(x) (\gamma-1) z^2 - 2P_2(x) \gamma z^3 + 3P_3(x) z^2 + \dots$$

$$\gamma^n P_0(x) - x (1+\gamma) P_0(x) + [\gamma^n P_1(x) - x P_1(x) (1+\gamma) - P_0(x) \gamma^n] z + [\gamma^n P_2(x) - \gamma^n P_1(x) -$$

$$x (1+\gamma) P_2(x)] z^2 - \gamma^n P_2(x) z^3 + \dots =$$

$$P_1(x) + [(\gamma-1) P_1(x) + 2P_2(x)] z + [\gamma P_1(x) + 2(\gamma-1) P_2(x) + 3P_3(x)] z^2 + \dots$$

Comparando os termos de igual grau, temos:

$$\gamma^n P_0(x) - x (1+\gamma) P_0(x) = P_1(x) \longrightarrow P_1(x) = \gamma^n - qx$$

$$\gamma^n P_1(x) - x P_1(x) (1+\gamma) - P_0(x) \gamma^n = (\gamma-1) P_1(x) + 2P_2(x).$$

$$2P_2(x) = [\gamma^n - qx - (\gamma-1)] P_1(x) - \gamma^n P_0(x) = [\gamma(n-1) + 1 - qx] P_1 - \gamma^n P_0(x).$$

$$\gamma^n P_2(x) - \gamma^n P_1(x) - x (1+\gamma) P_2(x) = -\gamma P_1(x) + 2(\gamma-1) P_2(x) + 3P_3(x).$$

$$3P_3(x) = [\gamma^n - qx - 2\gamma + 2] P_2(x) - (\gamma^n - \gamma) P_1(x).$$

$$3P_3(x) = [(n-2)\gamma - qx + 2] P_2(x) - \gamma(n-1) P_1(x), \text{ e assim sucessivamente.}$$

Logo,

$$(k+1) P_{k+1}(x) = [(n-k)\gamma + k - qx] P_k(x) - \gamma(n-k+1) P_{k-1}(x).$$

No próximo capítulo estudaremos códigos lineares e não lineares. Primeiro introduziremos os códigos lineares e seus duais através da matriz geratriz de verificação de paridade. Depois os códigos não lineares serão discutidos. Além disso, algumas construções para estes códigos serão dadas.

CAPÍTULO II

CÓDIGOS LINEARES E NÃO LINEARES.

2.1 - Introdução. - O conceito de linearidade tem sido muito útil e iluminante na teoria da codificação, bem como em outras áreas da matemática aplicada. A linearidade, não somente simplifica a construção de códigos, mas também a implementação deles sem restringir seriamente a capacidade de corrigir erros dos códigos.

2.2 - Códigos Lineares. [01], [02], [03].

Seja F_2^n o espaço vetorial de todas as n-uplas binárias sobre GF(2) e F^n o espaço vetorial de todas as n-uplas sobre GF(q).

OBSERVAÇÕES:

- 1) - GF(2) é o corpo binário de Galois.
- 2) - GF(q) é o corpo finito de Galois, de q elementos, onde q é primo ou uma potência de primo.

Definição 2.2.1 - Um conjunto de vetores de F^n será chamado código linear, C, se, e só se, ele for um subespaço vetorial de F^n .

OBSERVAÇÃO.

Os elementos de C são chamados vetores código ou palavras código.

Definição 2.2.2 - O peso de Hamming, $wt(u)$, de um vetor u, de comprimento n é definido como sendo o número de componentes não nulas de u.

Exemplo 2.2.1

Seja $u = 1\ 0\ 0\ 1\ 1\ 0\ 1$, então $wt(u) = 4$

Seja $u = 1\ 2\ 0\ 3$, então $wt(u) = 3$.

Definição 2.2.3 - A distância de Hamming entre dois vetores u e v , de comprimento n , é o número de posições em que eles diferem.

Exemplo 2.2.2

Sejam $u = 1\ 0\ 1\ 1\ 1$ e $v = 0\ 0\ 1\ 0\ 1$, então $dist(u,v) = 2$.

Se v_1 e v_2 são duas palavras código, então $v_1 - v_2$ também é. Entretanto, a distância entre quaisquer duas palavras código é igual ao peso de uma outra palavra código, ou seja, $dist(u_1, u_2) = wt(u_1 - u_2)$. Portanto, a distância mínima de um código linear é igual ao peso mínimo de todos os vetores códigos não nulos. Esta afirmação é muito importante para analisar a capacidade de corrigir erros de um código linear.

Exemplo 2.2.3

Seja $q=2$, $n=5$. O conjunto de vetores:

$0\ 0\ 0\ 0\ 0$, $1\ 0\ 0\ 1\ 1$, $0\ 1\ 0\ 1\ 0$, $0\ 0\ 1\ 0\ 1$, $1\ 0\ 1\ 1\ 0$, $1\ 1\ 0\ 0\ 1$,
 $0\ 1\ 1\ 1\ 1$ e $1\ 1\ 1\ 1\ 0$, forma um espaço vetorial, V_1 , e é um código linear. O peso mínimo é 2.

2.3 - Descrição dos Códigos Lineares pelas Matrizes. [01], [02], [03]

Como um código linear é definido como um subespaço vetorial, então pode ser dado por uma base. Sabemos que um espaço vetorial pode ter mais de uma base. Então, qualquer conjunto dos vetores da base de um código linear pode ser considerado como linha de uma matriz G .

A matriz G , definida acima é chamada a matriz geratriz porque podemos gerar todas as palavras código pela combinação linear das linhas de G .

Definição 2.3.1 - O espaço linha de G , é o código linear C , ou seja, uma n -upla é uma palavra código de C , se, e somente se, é uma combinação linear das linhas de G .

Seja k a dimensão do código linear C , i.é., a dimensão do espaço vetorial. O número de linhas de G será exatamente k e as linhas de G são linearmente independentes. Como cada combinação linear dá um vetor código distinto, então há q^k vetores código em um código linear. Além disso, se d é a distância mínima deste código então este código será denotado por $[n,k,d]$, onde: n é o comprimento do código linear, k é a dimensão do código linear, d é a distância mínima do código.

OBSERVAÇÃO.

Se q e k têm valores grandes esta descrição dos códigos lineares é muito compacta porque temos que armazenar somente k linhas da matriz geratriz.

Exemplo 2.3.1

O código do exemplo 2.2.3 é um código linear $[5, 3, 2]$ e tem a matriz geratriz,

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

pois, as $2^3 = 8$ palavras código são as possíveis combinações lineares de G .

Há uma maneira alternativa para descrever códigos lineares através de matrizes. Sabemos que se C é um subespaço de dimensão k , o espaço nulo é um espaço vetorial, C^\perp , de dimensão $n-k$. Uma matriz H de posto $n-k$, cujo espaço linha é C^\perp , pode ser construída tomando como linha os vetores de uma base de C^\perp . Então, C é o espaço nulo de C^\perp .

Definição 2.3.2 - Uma n -upla a será vetor código de C , se, e somente se, for ortogonal a cada linha de H , i.é., se, e somente se,

$$Ha^t = 0 \tag{2.3.1}$$

Se $a = (a_1, a_2, \dots, a_n)$ e h_{ij} é o elemento de H na i -ésima linha e j -ésima coluna, então, pela equação (2.3.1),

$$\sum_{j=0}^n h_{ij} a_j = 0, \quad i = 1, 2, \dots, n-k \tag{2.3.2}$$

A equação (2.3.2) implica que as componentes de a satisfazem um conjunto de $n-k$ equações. Estas equações são chamadas equações generalizadas de verificação de paridade. A matriz H é chamada matriz de verificação de paridade.

Como a equação é verdadeira para toda a palavra código de C , então, em particular, vale para os k vetores da base da matriz G . Então, temos que;

$$GH^t = 0 \quad (2.3.3)$$

onde, 0 denota a matriz nula de ordem $k \times n-k$.

Exemplo 2.3.2

O código $C = [5, 3, 2]$ do exemplo 2.3.1 tem matriz de verificação de paridade:

$$H = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{vmatrix}$$

e,

$$GH^t = \begin{vmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{vmatrix} = \begin{vmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{vmatrix} = 0$$

OBSERVAÇÕES:

- 1) C e C^\perp são subespaço de F^n e ambos são códigos lineares.
- 2) C e C^\perp são denominados códigos duais (ou ortogonais).
- 3) Se C é um código $[n,k]$ então C^\perp é um código $[n, n-k]$.
- 4) Se um código é o espaço linha da matriz G , o dual dele é o espaço nulo, e vice versa.

No seguinte teorema provaremos uma propriedade importante dos códigos lineares.

Teorema 2.3.1 - Seja C um código linear que é o espaço nulo de uma matriz H . Então, para toda a palavra código de peso w , há uma relação de dependência entre w colunas de H , e, reciprocamente, para cada relação de dependência linear entre w colunas de H , há uma palavra código de peso w .

Demonstração.

Um vetor $a = (a_1, a_2, \dots, a_n)$ é uma palavra código se, e somente se,

$$aH^t = 0,$$

ou se h_i é a i -ésima coluna de H , então

$$\sum_{i=1}^n h_i a_i = 0 \tag{2.3.3}$$

Mas, a equação (2.3.3) é exatamente uma relação de dependência linear entre colunas de H . O número de colunas de H que aparecem com coeficientes não nulos é o número de componentes de a_i não nulos de a , que é exatamente o peso de a .

Reciprocamente, os coeficientes de qualquer relação de dependência entre w colunas de H são componentes de um vetor que deve estar no espaço nulo de H . Isto, prova o teorema.

Corolário. - Um código linear que é o espaço nulo da matriz H têm peso mínimo (distância mínima) w , se, e somente se, toda a combinação de $w-1$ colunas de H é linearmente independente e algumas w colunas são linearmente dependentes.

OBSERVAÇÃO.

Usando este corolário podemos construir códigos através da matriz H .

2.4 Algumas Construções de Códigos Lineares. [02]

Vamos ver aqui duas construções de códigos lineares, a partir de códigos conhecidos. Existem outras construções, mas, estas duas interessam ao nosso trabalho.

(i) Código Estendido. (Acréscimo de uma verificação de paridade global).

Seja C um código binário $[n, k, d]$ que tem algumas palavras de peso ímpar. Acrescentando um zero no final de cada palavra código de peso par e um 1 (um) no final de cada palavra código de peso ímpar formamos um novo código \tilde{C} com a propriedade de que toda palavra código de \tilde{C} tem peso par. \tilde{C} é um código $[n+1, k, d+1]$.

Se C tem matriz de verificação de paridade H , \tilde{C} tem matriz de verificação de paridade,

$$\hat{H} = \left| \begin{array}{cccccc} 1 & 1 & \dots & 1 & & \\ & & & & 0 & \\ & & & & \cdot & \\ & H & & & \cdot & \\ & & & & 0 & \end{array} \right|$$

Exemplo 2.4.1

Acrescentando uma verificação de paridade no código de Hamming [7,4,3] obtemos o código de Hamming estendido [8,4,4], com a matriz de verificação de paridade

$$\hat{H} = \left| \begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array} \right|$$

(ii) Código Furado. (Eliminação de uma Coordenada). -

É o processo inverso do código estendido. Eliminando uma coordenada de um código $C = [n, k, d]$ formamos um novo código $(n-1, k, d' \geq d-1)$

Exemplo 2.4.2

Eliminando a última coordenada no código [3, 2, 2] cujas palavras código são

0 0 0
0 1 1
1 0 1
1 1 1

temos o código furado [2, 2, 1] com as palavras código

0 0
0 1
1 0
1 1

2.5 Códigos Não Lineares. [02], [03]

Um dos objetivos principais dos códigos é corrigir (detectar) erros ocorridos durante a transmissão através de canais de comunicação com ruído. Para este objetivo os códigos lineares têm muitas vantagens práticas. Mas, se quisermos determinar o maior número possível de palavras código com uma determinada distância mínima, então, às vezes são usados códigos não lineares, que são definidos como segue:

Definição 2.5.1 - Um código linear (n, M, d) é um conjunto de M vetores de comprimento n (com componentes em $GF(q)$), tais que, quaisquer dois vetores diferem em pelo menos d posições e d é o maior número com esta propriedade.

OBSERVAÇÃO.

Trataremos somente de códigos não lineares binários.

Exemplo 2.5.1

Seja $n = 4$, $d = 2$, $M = 8$. Então o código $C(4, 8, 2)$ tem as palavras código:
0 0 0 0, 0 0 1 1, 0 1 1 0, 1 1 0 0, 1 0 0 1, 1 0 1 0, 0 1 0 1, 1 1 1 1.

Usualmente assumiremos que não há nenhuma posição na qual toda a palavra código é zero (senão seria um código $(n-1, M, d)$, porque podemos eliminar esta coordenada sem afetar a distância mínima e o número de palavras código). Também, visto que as distâncias entre as palavras código não se alteram se adicionarmos um vetor constante a todas as palavras código, podemos, se quisermos, assumir que o código contém o vetor nulo.

Teorema 2.5.1 - Se $A(n, d)$ denota o número de palavras código em qualquer código (n, M, d) , então,

$$A(n, 2r-1) = A(n+1, 2r) \quad (2.5.1)$$

Demonstração.

Seja C um código $(n, M, 2r-1)$. Acrescentando uma verificação de paridade global, temos um código $(n+1, M, 2r)$, assim,

$$A(n, 2r-1) \leq A(n+1, 2r).$$

Reciprocamente, dado um código $(n+1, M, 2r)$, eliminando uma coordenada temos um código $(n, M, d \geq 2r - 1)$, assim,

$$A(n, 2r-1) \geq A(n+1, 2r).$$

Logo,

$$A(n, 2r-1) = A(n+1, 2r).$$

OBSERVAÇÃO.

Este teorema diz que basta achar $A(n, d)$ para valores pares de d .

Teorema 2.5.2 - (O limite de Plotkin).

Se d é par e $2d \geq n$, então

$$A(n, d) \leq 2 \left\lfloor \frac{d}{2d-n} \right\rfloor \tag{2.5.2}$$

e,

$$A(2d, d) \leq 4d \tag{2.5.3}$$

Se d é ímpar e $2d + 1 > n$, então

$$A(n, d) \leq 2 \left\lfloor \frac{d+1}{2d+1-n} \right\rfloor \tag{2.5.4}$$

e,

$$A(2d+1, d) \leq 4d + 4 \tag{2.5.5}$$

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

Demonstração.

Seja C um código (n, M, d) . Calculamos a soma

$$\sum_{u \in C} \sum_{v \in C} \text{dist}(u, v), \text{ de duas maneiras.}$$

Primeiro, visto que $\text{dist}(u, v) \geq d$, se $u \neq v$ a soma é $\geq M(M-1)d$. Por outro lado, seja A a matriz $M \times n$ cujas linhas são as palavras código C . Suponha que a i -ésima coluna de A contenha x_i 0's e $m-x_i$ 1's. Então, esta coluna contribui $2x_i(M-x_i)$ para a soma, de modo que a soma é igual a:

$$\sum_{i=1}^n 2x_i(M-x_i).$$

Se M é par esta expressão é maximizada quando $x_i = \frac{1}{2}M$, e a soma é $\frac{1}{2}nM^2$. Assim, temos:

$$M(M-1)d \leq \frac{nM^2}{2}, \quad \text{ou} \quad M \leq \frac{2d}{2d-n}.$$

Mas M é par, assim:

$$M \leq 2 \left[\frac{d}{2d-n} \right]$$

Por outro lado, se M é ímpar, a soma é

$$\leq \frac{n(M^2-1)}{2}, \text{ e, portanto,}$$

$$M(M-1) \leq \frac{n(M^2-1)}{2}, \text{ ou } M \leq \frac{n}{2d-n} = \frac{2d}{2d-n} - 1.$$

Assim,

$$M \leq \left[\frac{2d}{2d-n} \right] - 1 \leq 2 \left[\frac{d}{2d-n} \right]. \quad (\text{Usando, } [2x] \leq 2[x] + 1).$$

Portanto,

$$M \leq 2 \left[\frac{d}{2d-n} \right].$$

Logo,

$$A(n, d) \leq 2 \left[\frac{d}{2d-n} \right]$$

Vamos dividir as palavras código de C em duas classes, uma começando com o zero e outra começando com 1. Uma classe deve conter pelo menos a metade das palavras código, assim,

$$A(n-1, d) \geq \frac{1}{2} A(n, d)$$

Portanto,

$$A(n, d) \leq 2A(n-1, d) \tag{2.5.6}$$

Das equações (2.5.6) e (2.5.2), temos:

$$A(4r, 2r) \leq 2A(4r-1, 2r) \leq 8r$$

Logo,

$$A(2d, d) \leq 4d \tag{2.5.3}$$

Se d é ímpar, então, pelo teorema 2.5.1 e por (2.5.2), temos:

$$A(n, d) = A((n+1, d+1)) \leq 2 \left[\frac{d+1}{2d+1-n} \right]$$

o que demonstra (2.5.4). E,

$$A(2d+1, d) = A(2d+2, d+1) \leq 2A(2d+1, d+1).$$

$$\text{Mas, } A(2d+1, d+1) \leq 2 \left[\frac{d+1}{2d+2-(2d+1)} \right] = 2d+2$$

Portanto;

$$2A(2d+1, d+1) \leq 4d+4.$$

Logo,

$$A(2d+1, d) \leq 4d+4 \tag{2.5.5}$$

2.6 - Códigos de Hadamard. [02]

Seja H_n uma matriz de Hadamard normalizada de ordem n . Se +1's forem trocados por 0's e -1's por 1's, H_n torna-se uma matriz de Hadamard binária A_n . Visto que as linhas de H_n são ortogonais, qualquer duas linhas de A_n concorrem a $(1/2^n)$ posições e diferem em $(1/2^n)$ posições, e assim, têm distância igual a $(1/2^n)$.

A matriz A_n dá origem a três códigos de Hadamard:

(i) - Um código $(n-1, n, (1/2^n))$, B_n , consistindo das linhas de A_n , eliminando a primeira coluna.

Exemplo 2.5.1

Seja $n=12$, $M = 12$, $d = 6$. Então, o código $(11, 12, 6)$ de Hadamard é:

$$B_{12} = \left\{ \begin{array}{cccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & \end{array} \right\}$$

(ii) - Um código $(n-1, 2n, (1/2^n))$, C_n , consistindo de B_n mais os complementos de todas as suas palavras código.

Exemplo 2.6.2

Seja $n = 12$, $M = 24$, $d = 5$

Então, o código de Hadamard $(11, 24, 5)$, é:

$$C_{12} = \left\{ \begin{array}{cccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \end{array} \right\}$$

(iii) - Um código $(n, 2n, (1/2^n))$, D_n , constituído de todas as linhas de A_n e seus complementos.

Exemplo 2.6.3

O código de Hadamard $(12, 24, 6)$, é:

$$D_{12} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

2.7 - Códigos Não Lineares Usando Matrizes de Conferência.[02]

Seja C uma matriz de conferência de ordem n (asim, $n = 2 \bmod 4$).
 Seja C normalizada na forma

$$C = \begin{pmatrix} 0 & \underline{1} \\ \underline{1}^t & S \end{pmatrix}$$

Onde a matriz S é quadrada de ordem n-1, satisfazendo

$$SS^t = (n-1)I - J, \quad SJ = JS = 0.$$

Então, as linhas de $\frac{1}{2}(S + I + J)$, $\frac{1}{2}(-S + I + J)$ mais o vetor nulo e o vetor com todas as componentes iguais a 1 formam um código não linear $(n-1, 2n, \frac{1}{2}(n-2))$.

Exemplo 2.7.1

0	0	0	0	0	0	0	0	0
1	1	1	0	0	1	0	1	0
1	1	1	1	0	0	0	0	1
1	1	1	0	1	0	1	0	0
0	1	0	1	1	1	0	0	1
0	0	1	1	1	1	1	0	0
1	0	0	1	1	1	0	1	0
0	0	1	0	1	0	1	1	1
1	0	0	0	0	1	1	1	1
0	1	0	1	0	0	1	1	1
1	0	0	1	1	0	1	0	1
0	1	0	0	1	1	1	1	0
0	0	1	1	0	1	0	1	1
1	0	1	1	0	0	1	1	0
1	1	0	0	1	0	0	1	1
0	1	1	0	0	1	1	0	1
1	1	0	1	0	1	1	0	0
0	1	1	1	1	0	0	1	0
1	0	1	0	1	1	0	0	1
1	1	1	1	1	1	1	1	1

No próximo capítulo estudaremos o problema da distribuição de pesos para códigos lineares e não lineares.

CAPÍTULO III

ENUMERADORES DE PESO.

3.1 - Introdução. - Em muitos sistemas de comunicação utilizando os códigos para a correção e detecção de erros, a distância mínima entre duas palavras código é um importante parâmetro. Muita atenção tem sido dada para construir códigos que tenham uma distância mínima dada. O peso de uma palavra código é a distância dela à origem (vetor nulo). A distância entre duas palavras código é o peso de outra palavra código, se o código for linear. Assim, o conjunto de inteiros especificando o peso de toda a palavra código é, então, exatamente a mesma coleção de números inteiros especificando a distância entre cada par de palavras código. Assim, é costume determinar as propriedades do peso em vez das propriedades da distância de códigos lineares. Em muitos casos, praticamente o que é conhecido explicitamente sobre a distribuição de pesos num código é que o peso tem certo valor mínimo. Mas, os estudos já revelaram que seria interessante saber mais informações sobre o código, tal como a distribuição de pesos das palavras código. Embora, sendo esta tarefa difícil, tem sido grande o esforço para determinar a distribuição de pesos de determinados códigos. Os códigos maiores requerem um conhecimento extra para obter a sua distribuição de pesos.

Neste capítulo veremos alguns resultados sobre a distribuição de pesos.

3.2 - Códigos Homogêneos e Distribuição de Pesos. [01]

Definição 3.2.1 - Seja C um código (n, M, d) e A_i o número de palavras código de peso i . Os números A_0, A_1, \dots, A_n são denominados distribuição de pesos de C .

OBSERVAÇÃO.

É óbvio que $A_0 + A_1 + \dots + A_n = M$.

Definição 3.2.2 - Seja C um código de comprimento n e seja M_i a matriz cujas linhas são os vetores de C de peso i , se existir algum. Então, C é homogêneo se para cada peso i , cada coluna de M_i em o mesmo peso.

No próximo teorema determinaremos uma relação entre o número de vetores de peso i em C e o número de vetores de peso i em C' (Código furado de C).

Teorema 3.2.1 - Seja C um código homogêneo de comprimento $n+1$ e A_i o número de vetores de peso i em C . Seja C' um código furado de C e a_i o número de vetores de peso i de C' . Então teremos:

$$(i) \quad a_i = \frac{(n+1-i)A_i}{n+1} + \frac{(i+1)A_{i+1}}{n+1} \quad (3.2.1)$$

Se B é um subcódigo de C obtido pela exigência de que alguma coordenada seja zero e se b_i denota o número de vetores de peso i em B , então temos:

$$(ii) \quad b_i = \frac{(n+1-i)A_i}{n+1} \quad (3.2.2)$$

Se acrescentarmos ainda a hipótese de que C é um código binário com somente vetores de peso par, então temos:

$$(iii) \quad A_{2j} = a_{2j} + a_{2j-1} \quad (3.2.3)$$

$$(iv) \quad a_{2j-1} = \frac{2j}{n+1} A_{2j} \quad (3.2.4)$$

$$(v) \quad a_{2j} = \frac{(n+1-2j)}{n+1} A_{2j} \quad (3.2.5)$$

$$(vi) \quad 2ja_{2j} = (n+1-2j)a_{2j-1} \quad (3.2.6)$$

Demonstração.

Seja M_i a matriz cujas linhas são vetores de peso i em C . O número de elementos não nulos na matriz M_i é iA_i , pois, M_i tem A_i linhas de peso i , e, cada coluna de M_i tem o mesmo peso, r . Portanto, $(n+1)r = iA_i$.

Assim,

$$r = \frac{i}{n+1}A_i$$

Podemos ver então, que cada coluna de M_i tem $A_i - \frac{i}{n+1}A_i = \frac{(n+1-i)A_i}{n+1}$ zeros. Um vetor de peso i em C' resulta, ou de um vetor de peso i em C com zero na coordenada furada, ou de um vetor de peso $i+1$ em C com 1 na coordenada furada. Logo,

$$a_i = \frac{(n+1-i)A_i}{n+1} + \frac{(i+1)A_{i+1}}{n+1} \quad (3.2.1)$$

Visto que um vetor de peso i em B é um vetor de peso i em C com zero numa coordenada fixa, (3.2.2) vale.

Consideremos o caso especial onde C é um código binário, somente com vetores de peso para e C' é um código furado. Então, o código furado pode ter vetores de peso $2j$ e $2j-1$ e estes resultam cancelando uma coordenada de um vetor de peso par. Logo,

$$A_{2j} = a_{2j} + a_{2j-1} \quad (3.2.3)$$

Se fizermos $i = 2j-1$ em (3.2.1) temos $A_{2j-1} = 0$ e,

$$a_{2j-1} = \frac{2j}{n+1}A_{2j} \quad (3.2.4)$$

Se fizermos $i = 2j$ em (3.2.1), então $A_{2j+1} = 0$ e,

$$a_{2j} = \frac{(n+1-2j)A_{2j}}{n+1} \quad (3.2.5)$$

Finalmente, de (3.2.5) temos,

$$A_{2j} = \frac{a_{2j}(n+1)}{n+1-2j} \quad \text{e de (3.2.4), temos} \quad A_{2j} = \frac{a_{2j-1}(n+1)}{2j} .$$

Portanto,

$$\frac{a_{2j-1}(n+1)}{2j} = \frac{a_{2j}(n+1)}{n+1-2j} .$$

Logo,

$$2ja_{2j} = (n+1-2j)a_{2j-1} \quad (3.2.6)$$

3.3 - Distribuição de Peso do Dual de um Código Binário. [01], [02], [06].

Sabemos que se C é um código $[n, k]$, C^\perp é um código $[n, n-k]$.

Definição 3.3.1 - O polinômio,

$$W_C(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i \quad (3.3.1)$$

é chamado "enumerador de peso" de C , onde A_i é o número de palavras código de peso i em C .

OBSERVAÇÕES.

1) $W_C(x, y)$ também pode ser escrito como

$$W_C(x, y) = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} \quad (3.3.2)$$

2) Podemos ter somente uma variável fazendo $x = 1$, e ainda, ter um bom enumerador de peso:

$$W_C(x, y) = W_C(y) = \sum_{i=0}^n A_i y^i \quad (3.3.3)$$

Definição 3.3.2 - Se B_i denota o número de palavras código de peso i de C^\perp (dual de C), o enumerador de peso de C^\perp é:

$$W_C(x, y) = \sum_{i=0}^n B_i x^{n-i} y^i = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} \quad (3.3.4)$$

Exemplo 3.3.1

Seja C um código $[6, 3, 3]$ cujas palavras código são:

0 0 0 0 0 0, 0 0 1 1 1 0, 0 1 1 0 1 1, 1 0 0 0 1 1, 0 1 0 1 0 1, 1 0 1 1 0 1, 1 1 0 1 1 0 e 1 1 1 0 0 0. O dual de C é C^\perp , que é:

$$C^\perp = \{0 0 0 0 0 0, 1 1 0 0 0 1, 1 0 1 0 1 0, 0 1 1 1 0 0, 0 1 1 0 1 1, 1 0 1 1 0 1, 1 1 0 1 1 0, 0 0 0 1 1 1\}.$$

Pela definição (3.3.1), o enumerador de peso de C é:

$$W_C(x, y) = x^6 + 4x^3y^3 + 3x^2y^4.$$

E o enumerador de peso de seu dual é:

$$W_{C^\perp}(x, y) = x^6 + 4x^3y^3 + 3x^2y^4.$$

As equações de MacWilliams dão um resultado surpreendente e importante, entre a distribuição de peso de um código C e a distribuição de peso de C^\perp .

Estas equações valem para códigos sobre corpos finitos, mas mostraremos inicialmente para códigos binários porque nos dará uma noção muito boa sobre a sua utilidade.

Para determinar isso, precisaremos da definição e lema seguinte:

Definição 3.3.5 - Se F_2^n é o conjunto de todos os vetores de comprimento n, seja f uma transformação definida sobre F_2^n . A transformada de Hadamard \tilde{f} de f é definida por

$$\tilde{f}(u) = \sum_{v \in F_2^n} (-1)^{u \cdot v} f(v), \quad u \in F_2^n \quad (3.3.5)$$

onde $u \cdot v$ é o produto interno de u por v.

Lema 3.3.1 - Se $C = [n, k]$ é um código linear binário, então,

$$\sum_{c \in C^\perp} f(c) = \frac{1}{|C|} \sum_{u \in C} \tilde{f}(u) \quad (3.3.6)$$

onde $|C| = 2^k$ é o número de palavras código em C.

Demonstração.

$$\sum_{u \in C} \tilde{f}(u) = \sum_{u \in C} \sum_{v \in F_2^n} (-1)^{u \cdot v} f(v) = \sum_{v \in F_2^n} f(v) \sum_{u \in C} (-1)^{u \cdot v}$$

Mas, se $v \in C^\perp$, então $u \cdot v = 0$ e, $\sum_{u \in C} (-1)^{u \cdot v} = 2^k$. Se $v \notin C^\perp$, então $u \cdot v = 0$ e $u \cdot v = 1$ em igual número, e, $\sum_{u \in C} (-1)^{u \cdot v} = 0$. Portanto,

$$\sum_{u \in C} \tilde{f}(u) = \sum_{v \in C^\perp} f(v) 2^k. \text{ Logo,}$$

$$\sum_{c \in C^\perp} f(c) = \frac{1}{2^k} \sum_{u \in C} \tilde{f}(u) \quad (3.3.6)$$

Teorema 3.3.1 - (Teorema de MacWilliams para Códigos Lineares Binários). - Se C é um código linear binário $[n, k]$ com dual C^\perp , então,

$$W_{C^\perp}(x, y) = \frac{1}{2^k} W_C(x+y, x-y) \quad (3.3.7)$$

Equivalentemente,

$$\sum_{k=0}^n B_k x^{n-k} y^k = \frac{1}{2^k} \sum_{i=0}^n A_i (x+y)^{n-i} (x-y)^i \quad (3.3.8)$$

ou,

$$\sum_{u \in C^\perp} x^{n-wt(u)} y^{wt(u)} = \frac{1}{2^k} \sum_{u \in C} (x+y)^{n-wt(u)} (x-y)^{wt(u)} \quad (3.3.9)$$

Demonstração.

Seja $f(u) = x^{n-wt(u)} y^{wt(u)}$. Então, temos:

$$\hat{f}(u) = \sum_{v \in F_2^n} (-1)^{u \cdot v} x^{n-wt(u)} y^{wt(u)} \quad (3.3.10)$$

Tomando $u = (u_1 \cdot u_2 \cdot \dots \cdot u_n)$ e $v = (v_1 \cdot v_2 \cdot \dots \cdot v_n)$, temos:

$$\begin{aligned} \hat{f}(u) &= \sum_{v \in F_2^n} (-1)^{u_1 v_1 + \dots + u_n v_n} \prod_{i=1}^n x^{1-v_i} y^{v_i} \\ &= \prod_{i=1}^n \sum_{v_i=0}^1 (-1)^{u_i v_i} x^{1-v_i} y^{v_i} \\ &= \prod_{i=1}^n \sum_{w=0}^1 (-1)^{u_i w} x^{1-w} y^w. \end{aligned}$$

Assim,

$$\hat{f}(u) = (x + y)^{n-wt(u)} (x-y)^{wt(u)} \quad (3.3.11)$$

Pelo lema (3.3.1), temos:

$$\sum_{u \in C^\perp} x^{n-wt(u)} y^{wt(u)} = \frac{1}{2^k} \sum_{u \in C} (x+y)^{n-wt(u)} (x-y)^{wt(u)}.$$

OBSERVAÇÃO.

As equações (3.3.7), (3.3.8) e (3.3.9) são conhecidas como identidade de MacWilliams.

Exemplo 3.2.2

Seja $C = [7, 4, 3]$ dado pela matriz geratriz:

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

Então,

$$C = \{0\ 0\ 0\ 0\ 0\ 0\ 0, 0\ 0\ 0\ 1\ 1\ 1\ 1, 0\ 0\ 1\ 0\ 1\ 1\ 0, \\ 0\ 1\ 0\ 0\ 1\ 0\ 1, 1\ 0\ 0\ 0\ 0\ 1\ 1, 0\ 0\ 1\ 1\ 0\ 0\ 1, 0\ 1\ 0\ 1\ 0\ 1\ 0, \\ 1\ 0\ 0\ 1\ 1\ 0\ 0, 0\ 1\ 1\ 0\ 0\ 1\ 1, 1\ 0\ 1\ 0\ 1\ 0\ 1, 1\ 1\ 0\ 0\ 1\ 1\ 0, \\ 0\ 1\ 1\ 1\ 1\ 0\ 0, 1\ 0\ 1\ 1\ 0\ 1\ 0, 1\ 1\ 0\ 1\ 0\ 0\ 1, 1\ 1\ 1\ 0\ 0\ 0\ 0, \\ 1\ 1\ 1\ 1\ 1\ 1\ 1\}$$

$$C^\perp = \{0\ 0\ 0\ 0\ 0\ 0\ 0, 1\ 1\ 0\ 1\ 0\ 0\ 1, 1\ 0\ 1\ 1\ 0\ 1\ 0, \\ 0\ 1\ 1\ 1\ 1\ 0\ 0, 0\ 1\ 1\ 0\ 0\ 1\ 1, 1\ 0\ 1\ 0\ 1\ 0\ 1, 1\ 1\ 0\ 0\ 1\ 1\ 0, \\ 0\ 0\ 0\ 1\ 1\ 1\ 1\}$$

Portanto,

$$W_C(x, y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7,$$

e,

$$W_{C^\perp}(x, y) = x^7 + 7x^3y^4.$$

Logo,

$$\frac{1}{16}W_C(x+y, x-y) = \frac{1}{16}[(x+y)^7 + 7(x+y)^4(x-y)^3 + 7(x+y)^3(x-y)^4 \\ + (x+y)^7] = x^7 + 7x^3y^4 = W_{C^\perp}(x, y),$$

e,

$$\frac{1}{8}W_{C^\perp}(x+y, x-y) = \frac{1}{8}[(x+y)^7 + 7(x+y)^3(x-y)^4] \\ = x^7 + 7x^4y^3 + 7x^3y^4 + y^7 = W_C(x, y).$$

No teorema seguinte obteremos uma relação entre as distribuições de peso $\{B_i\}$ e $\{A_i\}$ Obtidas em (3.3.8).

Teorema 3.3.2 -

$$\text{Se } (x+y)^{n-i}(x-y)^i = \sum_{k=0}^n P_k(i)x^{n-k}y^k, \quad (3.3.12)$$

onde $P_k(i)$ é um polinômio de Krawtchouk, então,

$$B_k = \frac{1}{|C|} \sum_{i=0}^n A_i P_k(i) \quad (3.3.13)$$

Demonstração. - Pelo teorema 3.3.1, temos

$$\sum_{k=0}^n B_k x^{n-k} y^k = \frac{1}{|C|} \sum_{i=0}^n A_i (x+y)^{n-i} (x-y)^i.$$

Portanto,

$$\sum_{k=0}^n B_k x^{n-k} y^k = \frac{1}{|C|} \sum_{i=0}^n A_i \sum_{k=0}^n P_k(i) x^{n-k} y^k.$$

Donde,

$$\sum_{k=0}^n B_k x^{n-k} y^k = \sum_{k=0}^n \frac{1}{|C|} \sum_{i=0}^n A_i P_k(i) x^{n-k} y^k.$$

Logo,

$$B_k = \frac{1}{|C|} \sum_{i=0}^n A_i P_k(i).$$

3.4 - Momentos da Distribuição de Pesos. [01], [02]

Até agora obtemos as equações de MacWilliams para códigos lineares binários. Mas existem as equações de momentos, determinadas por Pless, que são uma família infinita de equações relacionando a distribuição de pesos de C à distribuição de pesos de C^\perp . Esta família de equações é equivalente as equações de MacWilliams e têm a vantagem de que a solução única para estas equações em geral, é evidente.

Nesta seção obteremos as potências de momentos de Pless.

Fazendo $x = 1$ na equação (3.3.8), temos:

$$\sum_{i=0}^n A_i y^i = \frac{1}{2^k} \sum_{i=0}^n B_i (1+y)^{n-i} (1-y)^i \quad (3.4.1)$$

Tomando, $y = 1$, temos:

$$\sum_{i=0}^n \frac{A_i}{2^k} = 1. \quad (3.4.2)$$

Esta é a primeira equação, no caso binário, da potência de momentos.

Derivando (3.4.1) em relação a y , temos:

$$\sum_{i=1}^n i A_i y^{i-1} = \frac{1}{2^{n-k}} [B_0 n (1+y)^{n-1} + B_1 ((n-1)(y+1)^{n-2} (1-y) - (1+y)^{n-1}) + B_2 ((n-2)(1+y)^{n-3} (1-y)^2 - 2(1-y)(1+y)^{n-2}) + B_3 ((n-3)(1+y)^{n-4} (1-y)^3 -$$

Fazendo $y = 1$, temos:

$$\sum_{i=1}^n iA_i = \frac{1}{2^{n-k}} [B_0 n 2^{n-1} - B_1 2^{n-1}].$$

Mas, $B_0 = 1$. Portanto,

$$\sum_{i=1}^n iA_i = \frac{1}{2^{n-k}} 2^n 2^{-1} (n - B_1),$$

ou,

$$\sum_{i=1}^n iA_i = \frac{1}{2^{-k}} \frac{1}{2} (n - B_1).$$

Portanto,

$$\sum_{i=1}^n \frac{iA_i}{2^k} = \frac{1}{2} (n - B_1) \quad (3.4.3)$$

que é a segunda equação da potência de momentos (ou, o primeiro momento).

Derivando a 2ª vez, temos:

$$\begin{aligned} \sum_{i=2}^n i(i-1)A_i (y)^{i-2} &= \frac{1}{2^{n-k}} [n(n-1)(1+y)^{n-2} + B_1(n-1)((n-2)(1+y)^{n-3} \\ &\cdot (1-y) - (1+y)^{n-2}) - B_1(n-1)(1+y)^{n-2} + B_2(n-2)((n-3)(1+y)^{n-4}(1-y)^2 \\ &- 2(1-y)(1+y)^{n-3}) + 2B_2((1+y)^{n-2} - (1-y)(n-2)(1+y)^{n-3}) + 3B_3(2(1-y) \\ &\cdot (1+y)^{n-3} - (n-3)(1+y)^{n-4}(1-y)^2 + \dots]. \end{aligned}$$

Fazendo $y = 1$, temos:

$$\begin{aligned} \sum_{i=2}^n i(i-1)A_i &= \frac{1}{2^{n-k}} [n(n-1)2^{n-2} - B_1(n-1)2^{n-2} - B_1(n-1)2^{n-2} + 2B_2 2^{n-2}] \\ &= \frac{1}{2^{n-k}} [2^{n-2} (n(n-1) - 2B_1(n-1) + 2B_2)] \\ &= \frac{1}{2^{-k}} \frac{1}{4} (n(n-1) - 2B_1(n-1) + 2B_2). \end{aligned}$$

Portanto,

$$\sum_{i=2}^n \frac{i(i-1)A_i}{2^k} = \frac{1}{4} (n(n-1) - 2B_1(n-1) + 2B_2)$$

ou,

$$\sum_{i=2}^n \binom{i}{2} \frac{A_i}{2^k} = \frac{1}{4} \sum_{i=0}^2 (-1)^i \binom{n-i}{2-i} B_i \quad (3.4.4)$$

que é a terceira equação da potência de momento (ou segundo momento).

Continuando desta maneira obtemos a equação da potência dos momentos de distribuição de pesos:

$$\sum_{i=0}^n \binom{i}{v} \frac{A_i}{2^k} = \frac{1}{2^v} \sum_{i=0}^v (-1)^i \binom{n-i}{v-i} B_i \quad (3.4.5)$$

onde $v = 0, 1, 2, \dots, n$.

OBSERVAÇÕES:

1) - O lado esquerdo de (3.4.5) é chamado momento binomial dos A_i 's.

2) - Se a distância mínima do código dual é d' , então $B_1, B_2, \dots, B_{d'-1} = 0$, e, se $v < d'$,

$$\sum_{i=0}^n \binom{i}{v} \frac{A_i}{2^k} = \frac{1}{2^v} \binom{n}{v} \quad (3.4.6)$$

Da equação (3.4.6), podemos ver que o v -ésimo momento, para $v = 0, 1, 2, \dots, d'-1$, é independente do código e é igual a do código $[n, n, 1], F_2^n$.

3.5 - Generalização do Teorema de MacWilliams para Códigos Lineares. [02]

Vamos descrever alguns enumeradores de peso de códigos lineares sobre um corpo $F = GF(q) = GF(p^m)$, onde p é um primo. Denotaremos os elementos de $GF(q)$ por w_0, w_1, \dots, w_{q-1} , em alguma ordem fixa.

Definição 3.5.1 - Seja $u = (u_1, u_2, \dots, u_n) \in F^n$. A composição de u , denotada por $\text{comp}(u)$, é $(s_0, s_1, \dots, s_{q-1})$, onde, $s_i = s_i(u)$ é o número de componentes u_j iguais a w_i . É óbvio que $\sum_{i=0}^{q-1} s_i = n$.

Definição 3.5.2 - Seja C um código linear $[n, k]$ sobre $GF(q)$, e, $A(t)$ o número de palavras código $u \in C$ com $\text{comp}(u) = t = (t_0, t_1, \dots, t_{q-1})$. Então, o enumerador de peso completo de C , é:

$$\begin{aligned} W_C(z_0, z_1, \dots, z_{q-1}) &= \sum A(t) z_0^{t_0} z_1^{t_1} \dots z_{q-1}^{t_{q-1}} \\ &= \sum_{u \in C} z_0^{s_0} z_1^{s_1} \dots z_{q-1}^{s_{q-1}} \end{aligned} \quad (3.5.1)$$

Exemplo 3.5.1

Se C é um código ternário [4, 2, 3] dado por:

$C = \{0000, 0121, 0212, 1022, 1110, 2011, 2102, 2220\}$, então

$$\begin{aligned} W_C(z_0, z_1, z_2) &= z_0^4 + z_0 z_1^2 z_2 + z_0 z_1 z_2^2 + z_0 z_1 z_2^2 + z_0 z_1^3 + z_0 z_1^2 z_2 + \\ &\quad + z_0 z_1^2 z_2 + z_0 z_1 z_2^2 + z_0 z_2^3 \\ &= z_0^4 + z_0 z_1^3 + 3z_0 z_1^2 z_2 + 3z_0 z_1 z_2^2 + z_0 z_2^3 \\ &= z_0 (z_0^3 + (z_1 + z_2)^3). \end{aligned}$$

OBSERVAÇÃO.

Sabemos que todo elemento β de $GF(q)$ pode ser escrito na forma:

$$\beta = \beta_0 + \beta_1 \alpha + \beta_2 \alpha^2 + \dots + \beta_{m-1} \alpha^{m-1}, \text{ ou equivalentemente,}$$

$\beta = (\beta_0, \beta_1, \dots, \beta_{m-1})$, onde α é um elemento primitivo de $GF(q)$ e $0 \leq \beta_i \leq p-1$.

Seja

$\epsilon = e^{\frac{2\pi i}{p}} = \cos\left(\frac{2\pi}{p}\right) + i \operatorname{sen}\left(\frac{2\pi}{p}\right)$, que é a raiz p-ésima da unidade. Para cada $\beta = (\beta_0, \beta_1, \dots, \beta_{m-1}) \in GF(q)$, definimos a função de valores complexos, definida em $GF(q)$ por:

$$\phi(\gamma) = \epsilon^{\beta_0 \gamma_0 + \dots + \beta_{m-1} \gamma_{m-1}} \quad (3.5.2)$$

para,

$$\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{m-1}) \in GF(q).$$

Definição 3.5.3 - ϕ_β é chamado caracter de $GF(q)$.

Exemplo 3.5.2

Seja $q = p = 3$, $GF(3) = \{0, 1, 2\}$ e $\epsilon = w = e^{\frac{2\pi i}{3}}$.

Os três caracteres, são: $\phi_0(0) = 1, \phi_0(1) = 1, \phi_0(2) = 1$
 $\phi_1(0) = 1, \phi_1(1) = w, \phi_1(2) = w^2$
 $\phi_2(0) = 1, \phi_2(1) = w^2, \phi_2(2) = w^4 = w$

Lema 3.5.1 - Para todo $\beta \in GF(q)$, com $\beta \neq 0$,

$$\sum_{\gamma \in GF(q)} \phi_{\beta}(\gamma) = 0.$$

Demonstração.

$$\begin{aligned} \sum_{\gamma \in GF(q)} \phi_{\beta}(\gamma) &= \sum_{\gamma \in GF(q)} \beta_0 \gamma_0 + \dots + \beta_{m-1} \gamma_{m-1} \\ &= \prod_{j=0}^{m-1} \sum_{\gamma_j \in GF(q)} \beta_j \gamma_j \end{aligned}$$

Visto que $\beta \neq 0$, algum β_j é não nula, digamos $\beta_r \neq 0$. Então, o r -ésimo fator do produto acima é:

$$\sum_{\gamma_r \in GF(q)} \beta_r \gamma_r = \sum_{k=0}^{p-1} \epsilon^k = \frac{1 - \epsilon^p}{1 - \epsilon} = 0, \text{ pois, } \epsilon^p = 1. \text{ Logo,}$$

$$\sum_{\gamma \in GF(q)} \phi_{\beta}(\gamma) = 0.$$

Definição 3.5.4. - Para $u, v \in F^n$ seja $\phi_u(v) = \phi_1(u.v)$. A transformada \hat{f} da aplicação f definida sobre F^n é dada por

$$\hat{f}(u) = \sum_{v \in F^n} \phi_u(v) f(v).$$

Lema 3.5.2 - Se C é um código linear $[n, k]$ sobre $GF(q)$, então

$$\sum_{u \in C^{\perp}} f(u) = \frac{1}{q^k} \sum_{u \in C} \hat{f}(u) \quad (3.5.3)$$

Demonstração.

$$\sum_{u \in C} \hat{f}(u) = \sum_{u \in C} \sum_{v \in F^n} \phi_u(v) f(v) = \sum_{v \in F^n} f(v) \sum_{u \in C} \phi_1(u.v)$$

Se $v \in C^{\perp}$, então $u.v=0$, e, $\phi_1(u.v) = 1$, e, portanto, a soma interior é igual a q^k . Mas, se $v \notin C^{\perp}$, então pelo lema 3.5.1 esta soma é igual a zero. Portanto,

$$\sum_{u \in C} \hat{f}(u) = q^k \sum_{v \in C^{\perp}} f(v).$$

Logo,

$$\sum_{u \in C^{\perp}} f(u) = \frac{1}{q^k} \sum_{u \in C} \hat{f}(u).$$

O próximo teorema nos dá uma relação entre o enumerador de peso completo de um código e o enumerador de peso completo do seu dual. É o teorema de MacWilliams para enumeradores de peso completo.

Teorema 3.5.1. - Se C é um código linear $[n, k]$ sobre $GF(q)$ com enumerador de peso completo W_C , então o enumerador de peso completo do código dual C^\perp é

$$W_{C^\perp}(z_0, \dots, z_r, \dots, z_{q-1}) = \frac{1}{q^k} W_C \left(\sum_{s=0}^{q-1} \phi_1(w_0 w_s) z_s, \dots, \sum_{s=0}^{q-1} \phi_1(w_r w_s) z_s, \dots, \sum_{s=0}^{q-1} \phi_1(w_{q-1} w_s) z_s \right).$$

Demonstração.

Vamos aplicar o lema 3.5.2 com

$$f(u) = z_0^{s_0(u)} z_1^{s_1(u)} \dots z_{q-1}^{s_{q-1}(u)}.$$

Portanto,

$$\begin{aligned} \hat{f}(u) &= \sum_{v \in GF^n} (v) z_0^{s_0(v)} z_1^{s_1(v)} \dots z_{q-1}^{s_{q-1}(v)} \\ &= \prod_{r=0}^{q-1} \sum_{s=0}^{q-1} \phi_1(w_r w_s) z_s^{s_r(u)} \end{aligned}$$

Aplicando o lema 3.5.2, temos:

$$\sum_{u \in C^\perp} (z_0^{s_0(u)} \dots z_{q-1}^{s_{q-1}(u)}) = \frac{1}{q^k} \sum_{u \in C} \prod_{r=0}^{q-1} \sum_{s=0}^{q-1} \phi_1(w_r w_s) z_s^{s_r(u)}$$

Logo,

$$W_{C^\perp}(z_0, \dots, z_r, \dots, z_{q-1}) = \frac{1}{q^k} \left(\sum_{s=0}^{q-1} \phi_1(w_0 w_s) z_s, \dots, \sum_{s=0}^{q-1} \phi_1(w_r w_s) z_s, \dots, \sum_{s=0}^{q-1} \phi_1(w_{q-1} w_s) z_s \right)$$

Exemplo 3.5.3

Para um código sobre $GF(3)$, temos:

$$W_{C^\perp}(z_0, z_1, z_2) = \frac{1}{3^k} W_C(z_0+z_1+z_2, z_0+wz_1+w^2z_2, z_0+w^2z_1+wz_2)$$

onde, $w = e^{\frac{2\pi i}{3}}$

3.6 - Teorema de MacWilliams para Códigos Não Lineares. [2], [1]

Até agora vimos as equações de MacWilliams para códigos lineares. Nesta seção veremos a identidade de MacWilliams para códigos não lineares. Para isto faremos uso da álgebra de grupo.

Definição 3.6.1 - Seja $C = \sum_{v \in F^n} C_v z^v$ um elemento arbitrário da álgebra de grupo QG, com a propriedade de que $M = \sum_{v \in F^n} C_v \neq 0$. A $(n+1)$ -úpla A_0, A_1, \dots, A_n , onde,

$$A_i = w(t) \sum_{v \in F^n} C_v t^{wt(v)}, \text{ é a chamada distribuição de peso.}$$

OBSERVAÇÃO.

Isto é uma generalização natural da distribuição de peso de um código. É claro que $\sum A_i = M$.

Definição 3.6.2. - O enumerador de peso de C é o polinômio:

$$W_C(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i$$

ou seja,

$$W_C(x, y) = \sum_{v \in F^n} C_v x^{n-wt(v)} y^{wt(v)}$$

Definição 3.6.3 - O elemento C' de QG dado por

$$C' = \frac{1}{M} \sum_{u \in F^n} \phi_u(C) z^u \tag{3.6.1}$$

é a transformada de C.

$$\text{Suponha que } C' = \sum_{u \in F^n} C'_u z^u.$$

Assim,

$$C'_u = \frac{1}{M} \phi_u(C) = \frac{1}{M} \sum_{v \in F^n} (-1)^{u \cdot v} C_v, \quad u, v \in F^n \tag{3.6.2}$$

Definição 3.6.4 - A distribuição de peso de C' é A'_0, A'_1, \dots, A'_n , onde

$$A'_i = wt(u) \sum_{u \in F^n} \phi_u(C) \tag{3.6.3}$$

Definição 3.6.5 - O enumerador de peso de C' é,

$$W_{C'}(x, y) = \sum_{i=0}^n A_i' x^{n-i} y^i.$$

O teorema seguinte nos diz que $W_{C'}$ é dado por uma transformação linear de W_C .

Teorema 3.6.1 - (Teorema de MacWilliams para Códigos Não Lineares).

$$W_{C'}(x, y) = \frac{1}{M} W_C(x+y, x-y) \quad (3.6.4)$$

ou equivalentemente,

$$\sum_{v \in F^n} C'_v x^{n-wt(v)} y^{wt(v)} = \frac{1}{M} \sum_{u \in F^n} C_u (x+y)^{n-wt(u)} (x-y)^{wt(u)}.$$

Demonstração.

De (3.6.2), temos que,

$$\sum_{v \in F^n} C'_v x^{n-wt(v)} y^{wt(v)} = \frac{1}{M} \sum_{v \in F^n} (-1)^{u \cdot v} x^{n-wt(v)} y^{wt(v)}.$$

Mas,

$$\sum_{v \in F^n} (-1)^{u \cdot v} x^{n-wt(v)} y^{wt(v)} = (x+y)^{n-wt(u)} (x-y)^{wt(u)},$$

por (3.3.10) e (3.3.11). Logo,

$$\sum_{v \in F^n} C'_v x^{n-wt(v)} y^{wt(v)} = \frac{1}{M} \sum_{u \in F^n} C_u (x+y)^{n-wt(u)} (x-y)^{wt(u)}.$$

No próximo capítulo veremos uma aplicação da distribuição de pesos de um código para a determinação da probabilidade de erro não detectado.

CAPÍTULO IV

PROBABILIDADE DE ERRO NÃO DETECTADO.

4.1 - Introdução. - Vimos no capítulo III que as identidades de MacWilliams relacionam a distribuição de pesos de um código com a distribuição de pesos do código dual. Apresentamos neste capítulo uma derivação muito simples destas identidades, requerendo somente um conhecimento elementar da teoria da probabilidade. Para isso, utilizaremos o conceito de probabilidade de erro não detectado.

4.2 - Probabilidade de Erro Não Detectado para Códigos Lineares Binários. [06], [07]

Suponhamos que sejam empregados códigos detectores de erro para o controle de erros na transmissão de dados. Seja x um vetor código transmitido e erros ocorrem de tal forma que não são detectáveis pelo processo de controle de erros. Nesta seção veremos como computar tal evento, isto é, a probabilidade de um erro não detectado. Para computar esta probabilidade é necessário definir primeiro o modelo probabilístico que descreve o processo de transmissão. Suponhamos que o canal binário simétrico é empregado para a transmissão de dados. Este canal tem a probabilidade ϵ ($0 \leq \epsilon \leq 1$) de receber o dígito transmitido trocado e a probabilidade $1 - \epsilon$ de receber o dígito corretamente. Além disso, suponhamos que em dígitos sucessivos os erros ocorram independentemente.

Para definir a probabilidade de erro não detectado definiremos o seguinte:

Definição 4.2.1 - Seja x um vetor binário de comprimento n , e peso $w = wt(x)$. A probabilidade deste vetor, $P(x)$, é definida por,

$$P(x) = \epsilon^w (1 - \epsilon)^{n-w}, \quad 0 \leq \epsilon \leq 1 \quad (4.2.1)$$

Definição 4.2.2 - Se A_i é o número de palavras código de peso i , $i=0, 1, 2, \dots, n$, então a probabilidade de erro não detectado é definida por

$$P_{nd} = \sum_{i=0}^n A_i \epsilon^i (1 - \epsilon)^{n-i} \quad (4.2.2)$$

Seja $A(y) = \sum_{i=0}^n A_i y^i$ o enumerador de peso do código. Usando esta equação, (4.2.2) torna-se,

$$P_{nd} = (1 - \epsilon)^n A\left(\frac{\epsilon}{1 - \epsilon}\right) - (1 - \epsilon)^n$$

Definição 4.2.3 - Seja H a matriz de verificação de paridade de do código linear binário $[n, k]$. A síndrome de um vetor x , de comprimento n , é definida como sendo

$$S = Hx^t \quad (4.2.3)$$

OBSERVAÇÕES:

- 1) S é um vetor de comprimento $n-k$.
- 2) S é um vetor nulo se, e somente se, x é uma palavra código.
- 3) Se S é o vetor nulo não implica necessariamente, que não ocorreu erro.

Definição 4.2.4 - Uma matriz de verificação de paridade expandida de um código linear $[n, k]$ é uma matriz H^* cujas linhas são todos os vetores do espaço linha de H .

OBSERVAÇÕES:

- 1) Assim, H^* contém 2^{n-k} linhas, incluindo o vetor nulo.
- 2) Estas linhas são as palavras código do código dual.

Definição 4.2.5 - Para qualquer vetor binário x , de comprimento n , a síndrome de x , é

$$S^* = H^*x^t \quad (4.2.4)$$

Exemplo 4.2.1

A matriz de verificação de paridade, H, do código [7, 4] de Hamming é dada por

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Então,

$$H^* = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Seja $x = (1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1)$, então $S(x) = 0$ e $S^*(x) = 0$, e

$$x = (1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0), \text{ então } S(x) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \text{ e } S^*(x) = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Lema 4.2.1 - $S^*(x) = 0$, se, e somente se, $S(x) = 0$.
Se $S^*(x) \neq 0$, então $S^*(x)$ contém metade zeros e metade 1's.

Demonstração. - Seja $[n, k]$ um código linear binário, com a matriz de verificação de paridade H, e seja x um vetor binário de comprimento n.

Sabemos que $S^*(x) = H^*x^t$, onde H^* é uma matriz cujas linhas são todos os vetores do espaço linha de H. Portanto, as linhas de H^* são todas as possíveis combinações lineares das linhas de H. Como $S(x) = Hx^t$, então os elementos de S^* são obtidos tomando todas as combinações lineares dos elementos de S. Logo, o lema é verdadeiro.

Para provar o próximo teorema necessitamos do seguinte lema:

Lema 4.2.2

$$\sum_{i=0}^n \binom{n}{i} \epsilon^i (1 - \epsilon)^{n-i} = \frac{1}{2} - \frac{1}{2} (1 - 2\epsilon)^n \quad (4.2.5)$$

i , ímpar

Demonstração.

Sabemos que pela teoria da probabilidade,

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

i , ímpar

Fazendo $a = \epsilon$ e $b = 1 - \epsilon$ temos que

$$\begin{aligned} \sum_{i=0}^n \binom{n}{i} \epsilon^i (1 - \epsilon)^{n-i} &= \frac{1}{2} \sum_{i=0}^n \binom{n}{i} (1 - \epsilon)^{n-i} \epsilon^i - \\ &\quad \frac{1}{2} \sum_{i=0}^n \binom{n}{i} (-\epsilon^i) (1 - \epsilon)^{n-i} \\ &= \frac{1}{2} - \frac{1}{2} (1 - 2\epsilon)^n \end{aligned}$$

Seja B_i o número de linhas de H^* de peso i , $i = 0, 1, \dots, n$, ou seja, B_i é o número de palavras código de peso i , do código dual, e seja E_j o evento que a j -ésima componente de $S^*(x) = 1$.

Teorema 4.2.1 -

$$P_{nd} = 2^{-(n-k)} \sum_{i=0}^n B_i (1 - 2\epsilon)^i - (1 - \epsilon)^n \quad (4.2.6)$$

Demonstração.

$$P_{nd} = 1 - P(E_1 \cup E_2 \cup \dots \cup E_{2^{n-k}}) - (1 - \epsilon)^n$$

Pelo lema (4.2.1), se $S^*(x) \neq 0$, então exatamente 2^{n-k-1} dos eventos E_j ocorrem, enquanto que se $S^*(x) = 0$ nenhum deles ocorre. Assim, a soma

$\sum_{j=1}^{2^{n-k}} P(E_j)$ é igual a 2^{n-k-1} vezes a probabilidade de uma síndrome não nula. Então,

$$P_{nd} = 1 - \frac{1}{2^{n-k-1}} \sum_{j=1}^{2^{n-k}} P(E_j) - (1 - \epsilon)^n \quad (4.2.7)$$

Tomemos a j -ésima linha de H^* tendo peso w_j . Então, $P(E_j)$ é justamente a probabilidade que se tenha um número ímpar de 1's nas w_j posições correspondentes às componentes não nulas da j -ésima linha de H^* . Assim,

$$\sum_{k \equiv 0}^{w_j} \epsilon^k (1 - \epsilon)^{w_j - k} \quad (4.2.8)$$

k , ímpar

Mas, pelo lema (4.2.2), temos que

$$P(E_j) = \frac{1}{2} - \frac{1}{2}(1 - 2\epsilon)^{w_j}$$

Portanto,

$$\begin{aligned} P(E_1 \cup \dots \cup E_{2^{n-k}}) &= \frac{1}{2^{n-k-1}} \sum_{j=1}^{2^{n-k}} \left(\frac{1}{2} - \frac{1}{2}(1 - 2\epsilon)^{w_j} \right) \\ &= 1 - 2^{-(n-k)} \sum_{i=0}^n B_i (1 - 2\epsilon)^i \end{aligned}$$

Logo,

$$P_{nd} = 2^{-(n-k)} \sum_{i=0}^n B_i (1 - 2\epsilon)^i - (1 - \epsilon)^n$$

Veremos agora uma derivação simples da identidade de MacWilliams, utilizando o conceito de probabilidade de erro não detectado.

De (4.2.2) e (4.2.6), temos que

$$\begin{aligned} P_{nd} &= (1 - \epsilon)^n \sum_{i=0}^n A_i \left(\frac{1}{1 - \epsilon} \right)^i - (1 - \epsilon)^n \\ &= 2^{-(n-k)} \sum_{i=0}^n B_i (1 - 2\epsilon)^i - (1 - \epsilon)^n. \end{aligned}$$

Portanto,

$$(1 - \epsilon)^n \sum_{i=0}^n A_i \left(\frac{1}{1 - \epsilon} \right)^i = 2^{-(n-k)} \sum_{i=0}^n B_i (1 - 2\epsilon)^i.$$

Fazendo $y = 1 - 2\epsilon$, ou seja, $\epsilon = \frac{1-y}{2}$ e $1 - \epsilon = \frac{1+y}{2}$, temos

que, $\sum_{i=0}^n B_i (1 - 2\epsilon)^i = \sum_{i=0}^n B_i y^i = B(y)$

e,

$$\begin{aligned} (1 - \epsilon)^n \sum_{i=0}^n A_i \left(\frac{1}{1 - \epsilon} \right)^i &= \frac{(1+y)^n}{2^n} \sum_{i=0}^n A_i \left(\frac{1-y}{1+y} \right)^i \\ &= \frac{(1+y)^n}{2^n} A\left(\frac{1-y}{1+y}\right), \end{aligned}$$

onde $B(y)$ é o enumerador de pesos do código dual e $A(y)$ é o enumerador de pesos do código. Portanto,

$$2^k B(y) = (1+y)^n A\left(\frac{1-y}{1+y}\right)$$

a qual, é a identidade de MacWilliams.

Exemplo 4.2.2

Consideremos o código [7,4] de Hamming, cuja matriz de verificação de paridade é

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

Portanto,

$$C = \{00000000, 10001111, 01001110, 00101011, 00010111, 10100101, 10011000, 01100111, 11000001, 01011011, 00111110, 11101000, 10110001, 11010101, 01110000, 11111111\},$$

e,

$$C^\perp = \{00000000, 11101000, 11010101, 10110001, 00111110, 01011011, 01100111, 10001111\}.$$

Portanto,

$$A_0 = 1, A_1 = 0, A_2 = 0, A_3 = 7, A_4 = 7, A_5 = 0, A_6 = 0 \text{ e } A_7 = 1,$$

e,

$$B_0 = 1, B_1 = 0, B_2 = 0, B_3 = 0, B_4 = 7, B_5 = 0, B_6 = 0, \text{ e } B_7 = 0.$$

De (4.2.2), temos

$$\begin{aligned} P_{nd} &= (1-\vartheta)^7 [1+0+0+7\left(\frac{\varepsilon}{1-\varepsilon}\right)^3+7\left(\frac{\varepsilon}{1-\varepsilon}\right)^4+0+0+\left(\frac{\varepsilon}{1-\varepsilon}\right)^7] - (1-\vartheta)^7 \\ P_{nd} &= (1-\vartheta)^7 [1+7\left(\frac{\varepsilon}{1-\varepsilon}\right)^3+7\left(\frac{\varepsilon}{1-\varepsilon}\right)^4+\left(\frac{\varepsilon}{1-\varepsilon}\right)^7] - (1-\vartheta)^7 \end{aligned} \quad (4.2.8)$$

e de (4.2.6), temos que

$$\begin{aligned} P_{nd} &= 2^{-3} [1+0+0+7(1-2\vartheta)^4+0+0+0] - (1-\vartheta)^7 \\ &= \frac{1}{8} (1+7(1-2\vartheta)^4) - (1-\vartheta)^7 \end{aligned} \quad (4.2.9)$$

Igualando (4.2.8) e (4.2.9), temos que

$$(1-\vartheta)^7 [1+7\left(\frac{\varepsilon}{1-\varepsilon}\right)^3+7\left(\frac{\varepsilon}{1-\varepsilon}\right)^4+\left(\frac{\varepsilon}{1-\varepsilon}\right)^7] - (1-\vartheta)^7 = \frac{1}{8} (1+7(1-2\vartheta)^4) - (1-\vartheta)^7$$

Fazendo $y = 1 - 2\vartheta$, temos que

$$\left(\frac{1+y}{2}\right)^7 [1+7\left(\frac{1-y}{1+y}\right)^3+7\left(\frac{1-y}{1+y}\right)^4+\left(\frac{1-y}{1+y}\right)^7] = \frac{1}{8} (1+7y^4),$$

ou,

$$2^{-7} [(1+y)^7+7(1-y)^3(1+y)^4+7(1-y)^4(1+y)^3+(1-y)^7] = \frac{1}{8} (1+7y^4),$$

que é a identidade de MacWilliams para este código.

4.3 - Probabilidade de Erro Não Detectado para Códigos Lineares Binários. [06], [07]

Seja $[n, k]$ um código linear sobre $GF(q)$. Suponhamos que o canal q -ário (fig. 4.3.1) seja empregado para a transmissão de dados. Este canal tem a probabilidade $(1-\epsilon)$ de receber o dígito corretamente, e probabilidade $(\epsilon/(q-1))$ de receber o dígito trocado.

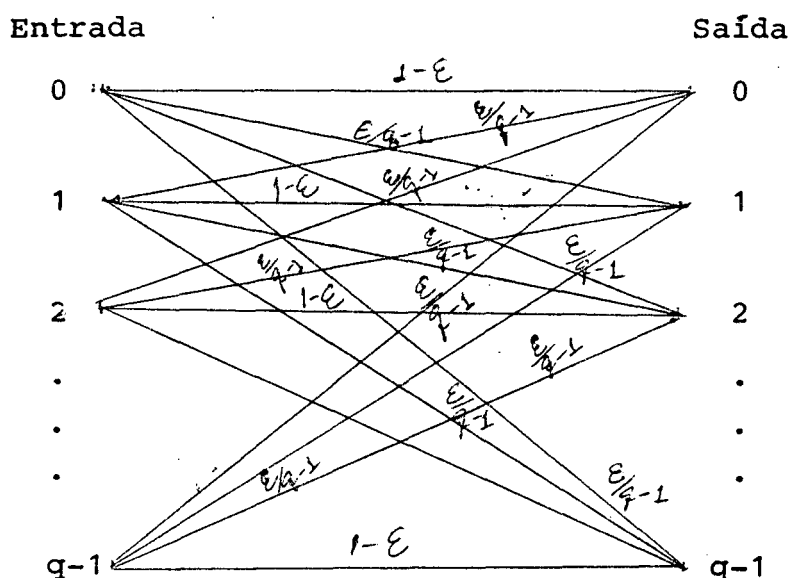


Figura 4.3.1 - Canal q -ário simétrico.

Definição 4.3.1 - Seja $[n, k]$ um código linear sobre $GF(q)$. Seja x um vetor de comprimento n sobre $GF(q)$, tendo peso de Hamming $w = wt(x)$. A probabilidade deste vetor é definida por

$$P(x) = \left(\frac{\epsilon}{q-1}\right)^w (1-\epsilon)^{n-w} \quad 0 \leq \epsilon \leq 1 \quad (4.3.1)$$

Definição 4.3.2 - Se A_i é o número de palavras código de peso i , $i = 0, 1, \dots, n$, então, a probabilidade de erro não detectado é dada por

$$P_{nd} = \sum_{i=1}^n A_i \left(\frac{\epsilon}{q-1}\right)^i (1-\epsilon)^{n-i} \quad (4.3.2)$$

ou seja,

$$P_{nd} = (1 - \epsilon)^n \left[A \left(\frac{\epsilon}{(q-1)(1-\epsilon)} \right) - 1 \right] \quad (4.3.3)$$

Se E_j é o evento que a j -ésima componente de $S^*(x)$ é não nula, $j = 1, 2, \dots, q^{n-k}$, então

$$P_{nd} = 1 - P(E_1 \cup E_2 \cup \dots \cup E_{q^{n-k}}) = (1 - \epsilon)^n \quad (4.3.4)$$

Se w_j é o peso da j -ésima linha da matriz de verificação de paridade expandida, H^* , então

$$P(E_j) = \sum_{k=1}^{w_j} \binom{w_j}{k} (1-\epsilon)^{w_j} \left(\frac{\epsilon}{q-1} \right)^k \left[(q-1)^k - (q-1)^{k-1} + (q-1)^{k-2} + \dots + (-1)^{k-1} (q-1) \right] \quad (4.3.5)$$

Mas,

$$\begin{aligned} & \sum_{k=1}^{w_j} \binom{w_j}{k} (1-\epsilon)^{w_j} \left(\frac{\epsilon}{q-1} \right)^k \left[(q-1)^k - (q-1)^{k-1} + \dots + (-1)^{k-1} (q-1) \right] \\ &= \sum_{k=1}^{w_j} \binom{w_j}{k} (1-\epsilon)^{w_j} \left[\epsilon^k \left(1 - \frac{1}{q-1} + \frac{1}{(q-1)^2} + \dots + (-1)^{k-1} \frac{1}{(q-1)^{k-1}} \right) \right] \\ &= \sum_{k=1}^{w_j} \binom{w_j}{k} (1-\epsilon)^{w_j} \epsilon^k \left(1 - \frac{1}{q-1} + \frac{1}{(q-1)^2} - \frac{1}{(q-1)^3} + \dots + \frac{(-1)^{k-1}}{(q-1)^{k-1}} \right) \\ &= \sum_{k=1}^{w_j} \binom{w_j}{k} \sum_{k=0}^{w_j} (-\epsilon)^k \left[\epsilon^k \left(1 - \frac{1}{q-1} + \frac{1}{(q-1)^2} - \dots + \frac{(-1)^{k-1}}{(q-1)^{k-1}} \right) \right] \\ &= \sum_{k=1}^{w_j} \binom{w_j}{k} \left(1 + \sum_{k=1}^{w_j} (-\epsilon)^k \frac{q^k}{q^k} \right) \left[\epsilon^k \left(1 - \frac{1}{q-1} + \frac{1}{(q-1)^2} - \dots + \frac{(-1)^{k-1}}{(q-1)^{k-1}} \right) \right] \\ &= \frac{q-1}{q} - \frac{q-1}{q} \sum_{k=1}^{w_j} \left(-\frac{q\epsilon}{q-1} \right)^k = \frac{q-1}{q} \left[1 - \left(1 - \frac{q\epsilon}{q-1} \right)^{w_j} \right]. \end{aligned}$$

Portanto,

$$P(E_j) = \frac{q-1}{q} \left[1 - \left(1 - \frac{q\epsilon}{q-1} \right)^{w_j} \right] \quad (4.3.6)$$

Portanto,

$$P(E_1 \cup \dots \cup E_{q^{n-k}}) = \frac{1}{(q-1)q^{n-k-1}} \sum_{j=1}^{q^{n-k}} P(E_j) \quad (4.3.7)$$

Seja B_i o número de linhas de H^* de peso i , $i = 0, 1, \dots, n$. Então

$$P_{nd} = q^{-(n-k)} \sum_{i=0}^n B_i \left(1 - \frac{q\epsilon}{q-1} \right)^i - (1 - \epsilon)^n \quad (4.3.8)$$

ou,

$$P_{nd} = q^{-(n-k)} B \left(1 - \frac{q\varepsilon}{q-1}\right) - (1 - \varepsilon)^n \quad (4.3.9)$$

Igualando (4.3.3) e (4.3.9), temos

$$(1 - \varepsilon)^n A \left(\frac{\varepsilon}{(q-1)(1-\varepsilon)} \right) = q^{-(n-k)} B \left(1 - \frac{q\varepsilon}{q-1}\right)$$

Fazendo,

$$y = \frac{\varepsilon}{(q-1)(1-\varepsilon)}, \text{ obtemos}$$

$$q^{n-k} A(y) = (1+(q-1)y)^n B \left(\frac{1-y}{1+(q-1)y} \right) \quad (4.3.10)$$

que é a identidade de MacWilliams para códigos lineares não binários.

Exemplo 4.3.1

Seja C o código ternário [5, 3, 2] dado pela matriz geratriz.

$$G = \begin{vmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 0 \end{vmatrix}$$

Então,

$$C = \{00000, 10012, 11020, 10102, 11110, 12001, 10222, 12211, 11200, 12121, 20021, 21002, 20111, 21122, 02201, 21212, 22100, 22220, 22010, 20201, 01011, 01101, 02022, 02112, 00210, 00120, 01221\}.$$

e,

$$C^\perp = \{00000, 22110, 12001, 01111, 12220, 21002, 10112, 20221, 02222\}.$$

Portanto,

$$A_0 = 1, A_1 = 0, A_2 = 2, A_3 = 14, A_4 = 6 \text{ e } A_5 = 4$$

e,

$$B_0 = 1, B_1 = 0, B_2 = 0, B_3 = 2, B_4 = 6 \text{ e } B_5 = 0.$$

De (4.3.2), temos

$$P_{nd} = (1 - \epsilon)^n \left[\sum_{i=0}^n A_i \left(\frac{\epsilon}{(q-1)(1-\epsilon)} \right)^i - 1 \right]$$

Portanto,

$$P_{nd} = (1-\epsilon)^5 \left[1+0+2 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^2 + 14 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^3 + 6 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^4 + 4 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^5 \right] - (1-\epsilon)^5$$

ou seja,

$$P_{nd} = (1-\epsilon)^5 \left[1+2 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^2 + 14 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^3 + 6 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^4 + 4 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^5 \right] - (1-\epsilon)^5$$

(4.3.11)

E de (4.3.8), temos:

$$P_{nd} = 3^{-2} \left(1+0+0+2 \left(1 - \frac{3\epsilon}{2} \right)^3 + 6 \left(1 - \frac{3\epsilon}{2} \right)^4 + 0 \right) - (1-\epsilon)^5$$

$$= \frac{1}{3^2} \left(1+2 \left(1 - \frac{3\epsilon}{2} \right)^3 + 6 \left(1 - \frac{3\epsilon}{2} \right)^4 \right) - (1-\epsilon)^5$$

(4.3.12)

Igualando (4.3.11) e (4.3.12), temos que

$$\begin{aligned} (1-\epsilon)^5 \left[1+2 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^2 + 14 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^3 + 6 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^4 + 4 \left(\frac{\epsilon}{2(1-\epsilon)} \right)^5 \right] &= \\ = \frac{1}{3^2} \left(1 + 2 \left(1 - \frac{3\epsilon}{2} \right)^2 + 6 \left(1 - \frac{3\epsilon}{2} \right)^4 \right). \end{aligned}$$

Fazendo $y = \frac{\epsilon}{2(1-\epsilon)}$, temos

$$3^2 (1+2y^2+14y^3+6y^4+4y^5) = (1+2y)^5 \left(1+2 \left(\frac{1-y}{1+2y} \right)^3 + 6 \left(\frac{1-y}{1+2y} \right)^4 \right).$$

que é a igualdade de MacWilliams para este código.

CONCLUSÃO

O problema da decodificação correta é um assunto que há muito vem preocupando os estudiosos do referido. Neste trabalho, fizemos um estudo sobre a distribuição de pesos dos códigos. É importante saber a probabilidade de decodificação correta, quando uma informação é transmitida utilizando-se um código. Para calcular isto na prática é necessário saber a distribuição de pesos dos códigos.

Um dos mais importantes resultados é que o enumerador de pesos do código dual, C^\perp , de um código binário, é unicamente determinado pelo enumerador de peso de C .

Este é um trabalho teórico e poderá ser útil aos estudantes interessados na teoria de decodificação.

BIBLIOGRAFIA

- [01] - PLESS, V. Introduction to the Theory of Error Correcting Codes. John Wiley and Sons, INC. USA. 1982
- [02] - MACWILLIAMS, F.J. and SLOANE, N.J.A. The Theory of Error Correcting Codes. North Holland Publ. Co. Amsterdam. 1977
- [03] - BERLEKAMP, E.R. Algebraic Coding Theory. McGraw-Hill. New York. 1968.
- [04] - PETERSON, W.W. and WELDON, E.J. Error Correcting Codes. MIT Press, Cambridge. Mass. 1972
- [05] - VAN LINT, J.H. Coding Theory. Springer. New York. 1971.
- [06] - GLEASON, A.M. Weight Polinomials of Self Dual Codes and the MacWilliams Identities. Actes Congress Intern. de Mathematique, 3. Gauthier-Villars. Paris. 1971.
- [07] - CHANG, S.C. and WOLF, J.K. A Simple Derivation of the MacWilliams' Identity for Linear Codes. IEEE Trans. on Information Theory. Vol 26, n° 4. July 1980.