UNIVERSIDADE FEDERAL DE SANTA CATARINA

UM ESTUDO DOS CÓDIGOS DE REED-MULLER

NOME: ANTONIO GONSALVES VICENTE

ORIENTADOR: PROFESSOR GUR DIAL (Ph.D.)

DATA: FLORIANÓPOLIS, 24 DE SETEMBRO DE 1985.

UM ESTUDO DOS CÓDIGOS DE REED-MULLER

por

ANTÔNIO GONÇALVES VICENTE

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. Gurdial, Ph.D.

Prof. Wagner de Souza Borges, Ph.D.

Prof. Paul James Otterson, Ph

AGRADECIMENTOS

Externo, os meus sinceros agradecimentos, a todos àqueles que de qualquer modo contribuiram para a conclusão deste meu trabalho, em especial:

- À UFMT - Universidade Federal do Mato Grosso;
- Ao Departamento de Ciências do Centro Pedagógico de RAO;
- Ao Professor Gur Dial (Ph.D.) Orientador
- à Secretaria do Curso de Pós Graduação em Matemática da UFSC;
- A todos os meus colegas de estudo.

Aos meus Pais:
João Gonsalves Vicente e
Theodolina Adami Vicente
A minha eterna gratidão!

Ã

CIDA,TATIANA, THÉO e TALITA.

INDICE

RESUMO

No primeiro capítulo introduzimos os conceitos preliminares de um código linear, definimos o que é uma matriz geratriz e uma matriz de verificação de paridade, e, damos as propriedades básicas de um código linear. Definimos também os códigos de Hamming e o código dual e mostramos alguns processos de construção de um novo código através de um código velho, dando também o método de construção de um código produto.

No segundo capítulo estudamos os códigos de Reed-Muller, as propriedades básicas, sua construção e o produto entre dois códigos de Reed-Muller. Mostramos Também, através de exemplos que o produto de dois códigos de Reed-Muller, nem sempre é um código de Reed-Muller, mas que pode ser considerado como um subcódigo de Reed-Muller de ordem maior.

No terceiro capítulo vemos sob qual condição o dual de um código de peso par está contido no seu código próprio. Além disso, estudamos os códigos lineares de ordem $r+(r+1)_{m,s}$, que são obtidos pela anexação de alguns vetores básicos de Reed-Muller de ordem r. Mostramos ainda, que o código produto de Reed - Muller é um código linear de ordem $r+(r+1)_{m,s}$.

C A P I T U L O I

CÓDIGOS LINEARES.

1.INTRODUÇÃO: - Em qualquer sistema de comunicação podem ocorrer distúrbios na transmissão de dados ou mensagens. Estes distúrbios, muitas vezes são provocados por ruidos naturais ou feitos pelo homem. Por exemplo, numa linha telefônica, o distúrbio pode vir a ser ruido termal, relâmpago, ou conversa cruzada de outras linhas.

Os códigos foram inventados para corrigir erros em canais de comunicação com distúrbios.

Nós aqui, supomos uma mensagem como um bloco de símbolos sobre um conjunto finito. No geral, seja a mensagem 1001, que pode estar representando um número, uma letra ou até uma frase completa. Essa mensagem é então transmitida sobre um canal de comunicação que está sujeito a ruidos que poderão prejudicar a transmissão. Consideremos o diagrama do canal de comunicação

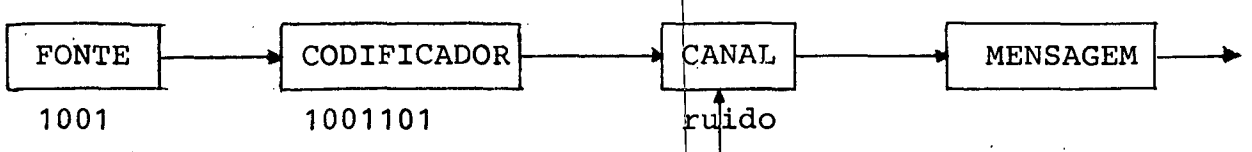


Fig. 1.1.1 - O canal de Comunicação.

A primeira caixa contém a mensagem, em nosso caso 1001 . Esta mensagem, então, entra no codificador onde os dígitos redundantes 101 são adicionados tal que a mensagem, quando comunicada , possa ser corrigida se ficou prejudicada. A mensagem é então transmitida sobre o canal, onde está sujeita a ruido. Quando um ruido prejudica a mensagem, um "0" é trocado por "1" ou um "1" por um "0", o que altera a mensagem. O objetivo dos códigos é detectar e corrigir os erros ocorridos durante a transmissão de mensagens.

OBSERVAÇÕES: 1)- Podemos pensar no canal de comunicação como um canal de comunicação real, ou como os dados armazenados no computador que se deterioram no tempo. Embora a confiabilidade do canal é muito boa, nossa necessidade para uma comunicação confiável é grande.

2)- Devido a presença de ruidos, ocorrem erros durante a transmissão. Estes erros podem ser esporádicos e independentes, neste caso são chamados erros aleatórios. No nosso trabalho trataremos somente desse tipo de erro.

2. CONCEITOS PRELIMINARES. [09]

Nós assumiremos que a informação vinda de um canal de informação está na forma binária (uma sequência de dígitos binários). O processo de codificação consiste de duas etapas básicas.
-1) a sequência de informação é segmentada em blocos mensagens, e cada bloco consiste de k sucessivos dígitos de informação;
-2) o codificador, de acordo com certas normas transforma um bloco mensagem em um bloco de n, (n >k) dígitos binários (uma n-upla binária) que nós chamamos de palavra código. Desde que cada bloco mensagem consiste de k dígitos binários, existem 2^k mensagens possíveis, isto é, existem 2^k palavras código possíveis a serem produzidas pelo codificador. Este conjunto de 2^k palavras código recebe o nome de código bloco. Uma palavra código é frequentemente chamada de vetor código, porque ela é uma n-upla de um espaço vetorial, V_n, de todas as n-uplas.

Para um código bloco, citado acima, a menos que tenha uma certa estrutura especial, o mecanismo de codificação seria exorbitantmente complexo para k grande, visto que, teríamos que armazenar os 2^k vetores código em um dicionário. Portanto, nós devemos restringir a nossa atenção para os códigos que podem ser mecanizados de maneira prática. A seguir, nós consideraremos códigos com a estrutura que os 2^k vetores código de cada código, que formam um subespaço K dimensional de todas as n-uplas.

Veremos que com esta estrutura em um código, a codificação complexa será consideravelmente reduzida.

Definição 1.2.1 - Um conjuto de 2^k n-uplas é chamado um código linear se, e somente se, for um subespaço do espaço vetorial V_n de todas as n-uplas.

Observação - Trabalharemos apenas com n-uplas binárias, isto é, códigos lineares binários.

Exemplo 1.2.1 - Seja k=3 e n=6. Suponhamos que o codificador transforme a mensagem de 3 dígitos em um vetor código de 6 dígitos da seguinte forma:

Mensagem	Codificador	Palavra-código
000	⟷	000000
001	⟷	001101
010	⟷	010011
011	⟷	011110
100	⟷	100110
101	⟷	101011
110	⟷	110101
111	⟷	111000

Observação - Trabalharemos com corpo binário GF(2) de dois elementos 0 e 1.

Desde que k=3, existem $2^3=8$ mensagens distintas possíveis. Cada mensagem é transformada em uma palavra código de seis dígitos pelo codificador. Todas as palavras código são distintas. Nós podemos facilmente ver que o conjunto das palavras código forma um subespaço tridimensional do espaço vetorial de todas as 6-uplas. Portanto, ele é um código linear.

1.2.2 - Matriz Geratriz.

Para um subespaço k dimensional, S de V_n, é possível achar um conjunto de k n-uplas linearmente independentes. Indicamos as k n-uplas por $v_1, v_2, \ldots, v_k$, tal que cada n-upla de S seja uma combinação linear de $v_1, v_2, \ldots, v_k$ na seguinte forma

$$x = u_1v_1+u_2v_2+ \ldots +u_kv_k \qquad (1.1.2a)$$

onde $u_i = 0$ ou 1 para i= 1, 2, ..., k.

Como um código linear é um subespaço e um subespaço pode ser dado por uma base, nós podemos então descrever um código linear de 2^k vetores código por um conjunto de k palavras código linearmente independentes. Seja a matriz G formada pelos k vetores código como linhas dela. Como podemos obter qualquer palavra código usando as linhas da matriz, esta matriz será chamada de matriz geratriz. Estes k vetores determinam o espaço linha de G, assim

$$G = \begin{vmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot\cdot \\ \cdot \\ v_k \end{vmatrix} = \begin{vmatrix} v_{11} & v_{12} & v_{13} & \cdots & v_{1n} \\ v_{21} & v_{22} & v_{23} & \cdots & v_{2n} \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ v_{k1} & v_{k2} & v_{k3} & \cdots & v_{kn} \end{vmatrix} \qquad (1.2.2b)$$

onde $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, para i= 1, 2, ..., k. Se $u = (u_1, u_2, \ldots, u_k)$ é um bloco mensagem, então a palavra código correspondente pode ser dada como segue:

$$x = uG$$

$$= (u_1, u_2, \ldots, u_k) \begin{vmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ \cdot \\ v_k \end{vmatrix} \qquad (1.2.2c)$$

$= u_1v_1+u_2v_2+ \ldots +u_kv_k$, isto é, a palavra código correspondente a mensagem $(u_1, u_2, \ldots, u_k)$ é uma combinação linear das linhas de G.

Observações: 1) - O código linear descrito acima é denotado por um $[n,k]$ código.

2) - O código linear é completamente especificado pela matriz geratriz dele.

3) - O espaço linha de G é definido como todas as combinações lineares das linhas de G.

A razão R = k/n é chamada a taxa do código; - uma vez

que um código é completamente especificado pela matriz geratriz G, o número de armazenagem da codificação é grandemente reduzido. O codificador tem unicamente que armazenar as k linhas de G em vez de armazenar os 2^k vetores código, do código.

Exemplo 1.2.2 - O código dado no exemplo 1.2.1 é o código [6,3] com a matriz geratriz

$$G = \begin{vmatrix} v_1 \\ v_2 \\ v_3 \end{vmatrix} = \begin{vmatrix} 1\ 0\ 0\ 1\ 1\ 0 \\ 0\ 1\ 0\ 0\ 1\ 1 \\ 0\ 0\ 1\ 1\ 0\ 1 \end{vmatrix}$$

A palavra código correspondente a mensagem u= (1 0 1) é

$$x = (1\ 0\ 1) \begin{vmatrix} v_1 \\ v_2 \\ v_3 \end{vmatrix}$$

$$= 1.v_1 + 0.v_2 + 1.v_3$$

$$= 1(1\ 0\ 0\ 1\ 1\ 0) + 0(0\ 1\ 0\ 0\ 1\ 1) + 1(0\ 0\ 1\ 1\ 0\ 1)$$

$$= 1\ 0\ 1\ 0\ 1\ 1$$

É possível codificar cada bloco mensagem em uma palavra código de tal forma que os primeiros k dígitos da palavra código sejam axatamente isuais aos blocos mensagem e os últimos (n-k) dígitos são dígitos redundantes, que são as funções de informação como ilustra a figura 1.2.1

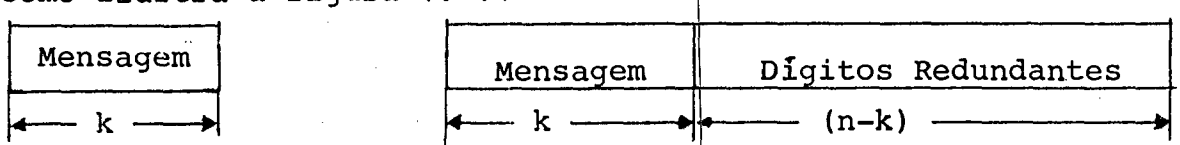


Fig.1.2.1

Um código desta forma é chamado um código sistemático. A redundância deveria ter a habilidade de combatar erros introduzidos durante a transmissão sobre um canal ruidoso, ou, em outras palavras, a redundância DEVERIA TER A CAPACIDADE DE PROTEGER A MENSAGEM. Agora o problema da codificação é para compor estes dígitos redundantes. Um [n,k] código linear sistemático pode ser descrito por uma kxn matriz da seguinte forma:

$$G = \begin{vmatrix} 1\,0\,0\,0\,\ldots\,0 & a_{11} & a_{12} & \cdots & a_{1,n-k} \\ 0\,1\,0\,0\,\ldots\,0 & a_{21} & a_{22} & \cdots & a_{2,n-k} \\ 0\,0\,1\,0\,\ldots\,0 & a_{31} & a_{32} & \cdots & a_{3,n-k} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ 0\,0\,0\,0\,\ldots\,1 & a_{k1} & a_{k2} & \cdots & a_{k,n-k} \end{vmatrix} \qquad (1.2.2d)$$

onde $a_{ij} = 0$ ou 1.

Se I_k é a kxk matriz identidade e se A é a kx(n-k) matriz de a_{ij}. Então a matriz geratriz de um código sistemático pode ser escrita como:

$$G = [I_k/A]$$

Considere um bloco mensagem $u = (u_1, u_2, \ldots, u_k)$. Usando a matriz geratriz da equação (1.2.2d) a palavra código correspondente é

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

$$= (u_1, u_2, \ldots, u_k) \cdot G$$

$$= (u_1, u_2, \ldots, u_k) \cdot \begin{vmatrix} 1000\ldots\ldots0 & a_{11} & a_{12} \cdots & a_{1,n-k} \\ 0100\ldots\ldots0 & a_{21} & a_{22} \cdots & a_{2,n-k} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0000\ldots\ldots1 & a_{k1} & a_{k2} \cdots & a_{k,n-k} \end{vmatrix}$$

(1.2.2e)

Por multiplicação de matrizes, podemos ver que

$$x_i = u_i, \text{ para } i = 1,2,\ldots,k \qquad (1.2.2f)$$

e

$$x_{k+j} = a_{1j}u_1 + a_{2j}u_2 + \ldots + a_{kj}u_k \qquad (1.2.2g)$$

para $j = 1,2,\ldots,n-k$. Pelas equações (1.2.2f) e (1.2.2g) nós vemos facilmente que os primeiros k dígitos de uma palavra código são justamente os dígitos de informação que foram transmitidos, os últimos n-k dígitos são funções lineares dos dígitos de informação. Nós chamamos os últimos n-k dígitos redundantes de x, os dígitos de verificação de paridade de uma palavra código. As equações de (1.2.2g) são chamadas de equações de verificação de pariade de um código.

Exemplo 1.2.3 - Considere a matriz geratriz do exemplo 1.2.2. A palavra código correspondente ao bloco mensagem $(u_1\ u_2\ u_3)$ é,

$$x = (x_1, x_2, \ldots, x_6)$$

$$= (u_1, u_2, u_3) \begin{vmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{vmatrix}$$

$$= (u_1, u_2, u_3, u_1+u_3, u_1+u_2, u_2+u_3),$$

então, $u_1 = x_1$, $u_2 = x_2$, $u_3 = x_3$,

e $x_4 = u_1+u_3$

$x_5 = u_1+u_2$

$x_6 = u_2+u_3$

Para um código na forma sistemática a complexidade de verificação pode ser facilmente reduzida, porque ele tem que armazenar somente kx(n-k) dígitos a_{ij} da matriz A em vez de armazenar kxn dígitos da matriz G.

1.2.3 - Matriz de Verificação de Paridade.

Para qualquer kxn matriz geratriz G (não necessariamente na forma 1.2.2d) cujas k linhas são linearmente independentes, existe uma (n-k)xn matriz H com n-k linhas

$$H = \begin{vmatrix} h_1 \\ h_2 \\ \cdot \\ \cdot \\ \cdot \\ h_{n-k} \end{vmatrix} = \begin{vmatrix} h_{11}\ h_{12}\ h_{13} \cdots h_{1n} \\ h_{21}\ h_{22}\ h_{23} \cdots h_{2n} \\ \cdot \\ \cdot \\ \cdot \\ h_{n-k,1} h_{n-k,2} \cdots h_{n-k,n} \end{vmatrix}$$

com $h_j = (h_{j1}, h_{j2}, \ldots, h_{jn})$, $j = 1,2,\ldots,n-k$, tal que as n-k linhas sejam linearmente independentes e cada vetor v no espaço linha de G seja ortogonal a todas as linhas de H, isto é, o produto interno $vh_j = 0$, para $1 \leq j \leq n-k$.

Seja g_i um vetor no espaço linha de G, então $g_i h_j = 0$, para $1 \leq i \leq k$ e $1 \leq j \leq n-k$. Suponha que um vetor no espaço

linha de H. Então u é uma combinação linear das linhas de H.

Seja $u = d_1h_1+d_2h_2+\ldots+d_{n-k}h_{n-k}$, onde $d_i = 0$ ou 1 para $1 \leq i \leq n-k$.

O produto interno de v e u é

$$v.u = v(d_1h_1+d_2h_2+\ldots+d_{n-k}h_{n-k})$$

$$= d_1(vh_1)+d_2(vh_2) +\ldots+d_{n-k}(vh_{n-k}) \qquad (1.2.3a)$$

Como $vh_j = 0$, então $v.u = 0$. Assim, o espaço linha de G é chamado o espaço nulo de H e vice-versa. Portanto, se $x=(x_1,x_2,\ldots,x_n)$ é um vetor nulo no espaço linha de G, então

$$x.H^t = (0\ 0\ 0\ .\ .\ .\ 0) \qquad (1.2.3b)$$

ou,

$$x.h_i = x_1h_{i1}+x_2h_{i2}+\ldots+x_nh_{in}, \qquad (1.2.3c)$$

para $i = 1,2,\ldots, n-k$.

Podemos portanto, descrever um código linear gerado por G em uma maneira alternada como segue: x é uma palavra código, no código gerado por G se, e somente se, $x.H^t = 0$ ou, $H.x^t = 0$. A matriz H é chamada de matriz de verificação de paridade de código.

Se a matriz geratriz de um código sistemático é da forma da equação (1.2.2d), então a matriz de verificação de paridade deste código é

$$H = \left|\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1k} & 1 & 0 & 0 & 0 \\ a_{21} & a_{22} & \cdots & a_{2k} & 0 & 1 & 0 & 0 \\ \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n-k,1} & \cdots & a_{n-k,k} & & 0 & 0 & 0 & 0 \end{array}\right| \begin{array}{c} \\ \\ \\ \\ \\ \\ \end{array} \qquad (1.2.3d)$$

$$\begin{array}{cccc} . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ . & . & . & 1 \end{array}$$

$= [A^t/I_{n-k}]$, onde A^t é a transposta da matriz A.

As equações de verificação de paridade de (1.2.2g) podem também ser obtidas de H. Isto pode ser visto como segue. Se $x = (x_1, x_2, \ldots, x_n)$ é a palavra código correspondente à mensagem $u = (u_1, u_2, \ldots, u_k)$, onde $u_i = x_i$, para $i=1,2,\ldots,k$.

Desde que $x.H^t = 0$ ou $H.x^t = 0$, então nós temos:

$$x_{k+j} = a_{1j}x_1+a_{2j}x_2+\ldots+a_{kj}x_k$$

$$= a_{1j}u_1+a_{2j}u_2+\ldots+a_{kj}u_k \qquad (1.2.3e)$$

para $j=1,2,\ldots,n-k$ que é exatamente o conjunto de todas as equações de (1.2.2g).

Exemplo 1.2.4 - Considere a matriz geratriz do exemplo 1.2.2. A matriz H é dada por

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

Como $H.x^t = 0$ então as equações de verificação são dadas por

$$\begin{vmatrix} x_1+x_3+x_4 = 0 \\ x_1+x_2+x_5 = 0 \\ x_2+x_3+x_6 = 0 \end{vmatrix}$$

Se a mensagem é (1 1 1), então a palavra código correspondente será (1 1 1 0 0 0).

Observação. - A matriz geratriz G e a matriz de verificação de paridade de H, de um código podem ser escritas também na forma

$$G = [I_k/A^t] \quad \text{e} \quad H = [A/I_{n-k}].$$

1.2.4 - Propriedades de um Código Linear.

(i) $x = x_1, x_2, \ldots, x_n$ é uma palavra código se, e somente se,

$$H.x^t = 0 \qquad (1.2.4a)$$

(ii) Usualmente a matriz de verificação de paridade H é uma (n-k)xn matriz da forma

$$H = [A/I_{n-k}] \qquad (1.2.4b)$$

e como nós já vimos, existem 2^k palavras código satisfazendo a equação (1.2.4a). (isto é verdadeiramente igual embora que H não tenha esta forma, contanto que H tenha n colunas e n-k linhas linearmente independentes). Quando H tem a forma (1.2.4b) as palavras código aparecerão assim:

$$x = \underbrace{x_1 x_2 x_3 \ldots x_k}_{\textit{mensagens}} \underbrace{x_{k+1} x_{k+2} \ldots x_n}_{\textit{dígitos redundantes}}$$

(iii) A matriz Geratriz.

Seja a mensagem $u = u_1, u_2, \ldots, u_k$, cuja palavra código correspondente é $x = x_1 x_2 \ldots x_n$. Primeiro, $x_i = u_i$ para $i=1,2,\ldots,k$, ou,

$$\begin{vmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_k \end{vmatrix} = I_k \begin{vmatrix} u_1 \\ u_2 \\ \cdot \\ \cdot \\ \cdot \\ u_k \end{vmatrix}, \quad I_k = \text{matriz identidade} \qquad (1.2.4c)$$

Então de (1.2.4a) e (1.2.4b) temos que

$$[A/I_{n-k}] \cdot \begin{vmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{vmatrix} = 0, \qquad \text{e} \qquad \begin{vmatrix} x_{k+1} \\ x_{k+2} \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{vmatrix} = -A \begin{vmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_k \end{vmatrix}$$

usando (1.2.4c), temos

$$\begin{vmatrix} x_{k+1} \\ x_{k+2} \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{vmatrix} = -A \begin{vmatrix} u_1 \\ u_2 \\ \cdot \\ \cdot \\ \cdot \\ u_k \end{vmatrix} \qquad (1.2.4d)$$

No caso binário $-A = A$.

Colocando (1.2.4c) no topo de (1.2.4d), temos que

$$\begin{vmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{vmatrix} = \begin{vmatrix} I_k \\ \hline A \end{vmatrix} \begin{vmatrix} u_1 \\ u_2 \\ \cdot \\ \cdot \\ \cdot \\ u_k \end{vmatrix}$$

e transpondo, obtemos.

$$x = u.G \qquad (1.2.4e)$$

onde, $G = [I_k / A^t]$ (1.2.4f)

(iv) Os parâmetros de um código.

A palavra código $x = x_1x_2...x_n$ é dita de comprimento n, onde n também é chamado de comprimento do bloco código. Se H tem n-k linhas linearmente independentes, existem 2^k palavras código, k é chamado de dimensão do código.

(v) Outras matrizes geratriz e de verificação de paridade.

Um código pode ter várias matrizes geratriz diferentes, pois um subespaço pode ter mais de uma base.Por exemplo:

$$\left|\begin{array}{cccc} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right|, \quad \left|\begin{array}{cccc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right|$$

Ambas são matrizes geratriz do código [4,2] embora uma esteja na forma sistemática e a outra não, as duas geram códigos [4,2] equivalentes. De fato, algum conjunto máximo de palavras código linearmente independentes tomadas de um dado código, pode ser usado como as linhas de uma matriz geratriz para esse código.

Uma verificação de paridade num código ϕ é algum vetor linha h tal que $h.x^t = 0$ para todas as palavras código de $x\varepsilon\phi$. Então, similarmente, algum conjunto máximo de verificação de paridade linearmente independente pode ser usado como as linhas da matriz de verificação de paridade H de ϕ.

Por exemplo,

$$\left|\begin{array}{cccc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right|, \quad \left|\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{array}\right|$$

ambas são matrizes de verificação de paridade do código [4,2].

(vi) Linearidade.

Se x e y são palavras de um código, então x+y também o são, porque $H(x+y)^t = H.x^t+H.y^t = 0$. Se c é algum elemento do corpo binário, então cx é também uma palavra código, porque $H(cx)^t = cHx^t = 0$.

Definição 1.2.2 - O peso de um vetor código é o número de posições não nulas do mesmo e é denotado por Wt(x).

Exemplo 1.2.5- Wt(1011) = 3, Wt(01011111)=6.

Definição 1.2.3 - A distância(de Hamming)entre dois vetores com o mesmo número de componentes, é o número de posições onde os dois vetores diferem, e é denotado por dist(x,y), onde x e y são vetores.

Exemplo 1.2.6 - Se x = 1011 e y = 0101 então, temos que a distânicia dada por dist(x,y) = 3.

Observações: 1) - O código [n,k] com distância mínima d será denotado por [n,k,d].

2) - A distância mínima de um código linear é o peso mínimo de qualquer palavra código (não nula).

3) - dist(x,y) = Wt(x-y).

Definição 1.2.4 -A intersecção de vetores binários x e y é um vetor dado por $x*y = (x_1y_1, x_2y_2, \ldots, x_ny_n)$

Exemplo 1.2.7 - Se x = (1011) e y = (0110), então x*y = 0010.

3. CÓDIGOS DE HAMMING. [05]

Os códigos de Hamming de correção de um único erro, formam uma classe importante de códigos que são fáceis de codificar e decodificar. Veremos apenas os códigos de Hamming binários.

Definição 1.3.1 - Um código de Hamming binário ζ_r, de comprimento $n = 2^r-1$ ($r \geq 2$) tem matriz de verificação de paridade H, cujas colunas consistem de todos os vetores binários não nulos, de comprimento r, cada um usado uma vez. ζ_r é um $[n = 2^r-1, k = 2^r-1-r, d= 3]$ código.

Exemplo 1.3.1 - O código de Hamming [7,4,3] ou ζ_r tem a matriz de verificação de paridade

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

Observamos que se H tem r linhas, existe apenas 2^r-1 colunas disponíveis, a saber os 2^r-1 vetores binários não nulos de comprimento r. Podemos obter H na forma $H = [A/I_{n-k}]$, basta pegarmos as colunas numa ordem diferente.

$$H' = \left|\begin{array}{ccccccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right|$$

No geral $H' = [A/I_r]$, onde A contém todas as colunas com pelo menos dois 1's. Então H e H', nos dão códigos equivalentes. A matriz geratriz G é dada por

$$G = \left|\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right|$$

É fácil de ver que a distância mínima do código é 3.

4. O CÓDIGO DUAL. [11]

Definição 1.4.1 - Se $u = u_1u_2u_3\ldots u_n$, $v = v_1v_2v_3\ldots v_n$ são vetores (com comprimento sobre o corpo F) o produto escalar é definido como $u.v = u_1v_1+u_2v_2+\ldots+u_nv_n$, (avaliado em F),

Exemplo 1.4.1 - Seja u = 1101, v= 1111, então, temos que u.v = 1+1+0+1 = 1.

Observações: 1) - Se u.v = 0, u e v são chamados ortogonais.

2) - Para vetores binários u.v=0 se, e somente se, Wt(x*y) é par, u.v = 1 se, e somente se, Wt(x*y) é ímpar. Também, u.u = 0 se, e somente se, Wt(u) é par ($x*y=(x_1y_1,\ldots,x_ny_n)$).

Definição 1.4.2 - Se ϕ é um [n,k] código linear sobre F, seu código dual ou ortogonal $\phi^{\perp}$ é o conjunto de vetores que são ortogonais a toda palavra código de ϕ.

$$\phi^{\perp} = \{u/u.v = 0, \forall v \in \phi\}.$$

Então pelas propriedades de um código linear $\phi^{\perp}$ é exatamente o conjunto de todas as verificações de paridade em ϕ. Se ϕ tem a matriz geratriz G e a matriz de verificação de paridade H, então $\phi^{\perp}$ tem a matriz geratriz igual a H e a matriz de verificação de paridade igual a G, pois $G.H^{t} = 0$. Então $\phi^{\perp}$ é um [n,n-k] código e é o subespaço ortogonal de ϕ.

Exemplo 1.4.1 - Seja ϕ = [7,4] que possue a seguinte matriz de verificação de paridade

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

e a matriz geratriz

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

com as seguintes palavras código:

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

O seu dual $\phi^{\perp}$ = [7,3] tem a seguinte matriz de verificação de paridade H' = G e matriz geratriz G' = H com as seguintes palavras código.

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

5. CONSTRUÇÃO DE NOVOS CÓDIGOS ATRAVÉS DE CÓDIGOS VELHOS. [11].

Dados um ou mais códigos, podemos então, construir outros novos códigos através dos códigos dados. Veremos alguns casos de construção.

1.5.1 - A Construção $|u|.|u+v|$.

Dado um código $\phi_1 = [n,k_1]$ e um código $\phi_2 = [n,k_2]$ de mesmo comprimento, nós podemos formar um novo código ϕ_3 consistindo de todos os vetores $|u||u+v|$, $u\varepsilon\phi_1$, $v\varepsilon\phi_2$.

Observação. - Se $u = u_1u_2...u_n$ e $v = v_1v_2v_3...v_n$, então $|u||v|$ denota o vetor $u_1u_2...u_nv_1v_2...v_n$ de comprimento 2n.

Exemplo 1.5.1 - Seja $\phi_1 = [4,3]$ código de peso par, $\phi_2 = [4,1]$ código repetitivo. Sejam G_1 e G_2 as matrizes geratrizes de ϕ_1 e ϕ_2, respectivamente,

$$G_1 = \left|\begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right| \quad \text{e} \quad G_2 = [1\ 1\ 1\ 1]$$

As palavras código de ϕ_1 e ϕ_2 são respectivamente,

ϕ_1	ϕ_2
0 0 0 0	0 0 0 0
1 0 0 1	1 1 1 1
0 1 0 1	
0 0 1 1	
1 1 0 0	
1 0 1 0	
0 1 1 0	
1 1 1 1	

Pela construção $|u||u+v|$, $u\varepsilon\phi_1$ e $v\varepsilon\phi_2$ obteremos um código com as seguintes palavras código.

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

que é código $\phi_3 = [8,4]$.

1.5.2 - Adição de uma Verificação de Paridade Global.

Suponha que temos $\phi = [n,k,d]$ código binário, em que algumas palavras código tem peso ímpar. Nós podemos formar um novo código $\hat{\phi}$, adicionando um zero no final de toda palavra código de peso par, e 1 no final de toda palavra código de peso ímpar. Desta forma, obteremos um novo código $\hat{\phi}= [n+1,k,d+1]$ em que todas as palavras código tem peso par, isto é, satisfaz a nova equação de verificação de paridade $x_1+x_2+x_3+\ldots+x_{n+1} = 0$.

Se ϕ tem a matriz de verificação de paridade H, $\hat{\phi}$ tem a matriz de verificação de paridade

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

Exemplo 1.5.2 - Seja ϕ = [7,4,3] que é ζ_3 com

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

então

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

com as equações de verificação de paridade

$$\begin{cases} x_1+x_2+x_3+x_4+x_5+x_6+x_7+x_8 = 0 \\ x_2+x_3+x_4+x_5 = 0 \\ x_1+x_3+x_4+x_6 = 0 \\ x_1+x_2+x_4+x_7 = 0 \end{cases}$$

Observamos que o novo código $\hat{\phi}$ é o [8,4,4] código, chamado de código extendido de Hamming.

Observação.- Num código binário, ou todas as palavras código tem peso par, ou metade tem peso par e metade peso ímpar.

1.5.3 -Furando um Código pela Eliminação de Coordenadas.

Este processo é considerado o inverso da extensão de um código, e consiste em eliminar uma ou mais coordenadas de cada palavra código, de um código.

Observação. - O código furado é denotado por ϕ^*.

Exemplo 1.5.3 - Seja o código ϕ= [3,2,2], cujas palavras código são:

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

Eliminando as últimas coordenadas de cada palavra código obtemos o código ϕ^* = [2,2,1] cujas palavras código são:

0 0
0 1
1 0
1 1

Observação. - No geral, cada vez que uma coordenada de cada palavra código é eliminada, n diminui para 1 e o número de palavras código permanece o mesmo, sendo que a distância mínima d em geral diminui por 1.

1.5.4 - Expurgando pela Eliminação de Palavras Código.

Seja um código ϕ= [n,k,d] linear binário e tenha as palavras código de peso par e ímpar. Se expurgarmos ϕ pela eliminação de palavras código de peso par, então obteremos um código ϕ' = [n,k-1,d'], onde d' $\geq$ d.

Exemplo 1.5.4 - Seja ζ_3 = [7,4,3] um código, onde H está na forma sistemática, este código possui as seguintes palavras código:

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

se tirarmos as palavras código de peso ímpar, obteremos um ϕ' =[7,3,4] código.

1.5.5 - Incrementando pela Adição de Novas Palavras Código.

Este método consiste em acrescentar a palavra código 1 (cujos comprimento são "1"), desde que ela não esteja no código, da seguinte maneira: - Pegamos as palavras código, do código velho e a seguir fazemos a união com o conjunto de palavras código que iremos obter, adiconando a cada palavra código, do código velho, a palavra 1, isto é o mesmo que acrescentar uma linha de 1's na matriz geratriz. Então $\phi^{(a)} = \phi \cup \{1 + \phi\}$.

Desta forma, se tínhamos um $\phi = [n,k,d]$ código, então, obteremos um $\phi^{(a)} = [n,k+1,d^{(a)}]$ código, onde $d^{(a)} = \min\{d, n-d'\}$ e d' é o peso maior de qualquer palavra código de ϕ.

Exemplo 1.5.3 - Seja o código $\phi = [3,2,2]$, cujas palavras código são:

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

Incrementando o código com a palavra código 1 1 1 obteremos o código

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

1.5.6 - Prolongamento pela Adição de Símbolos Mensagens.

A maneira usual para prolongar um código é incrementar, adiconando a palavra código 1, e então extender adicionando uma verificação de paridade global. É o mesmo que adicionar mais um símbolo mensagem.

Exemplo 1.5.6 - O código [16,11,4] é o prolongamento do código [15,10,4].

1.5.7 - Redução de um Código pelo Corte Transversal.

É a operação inversa do processo de prolongamento, basta pegar as palavras código que começam com $x_i = 0$ e eliminar a coordenada x_i.

Exemplo 1.5.7 - O código [15,10,4] é a redução do código [16,11,4].

Nós ilustraremos estas seis últimas operações na Figura. 1.5.7, usando um código de Hamming.

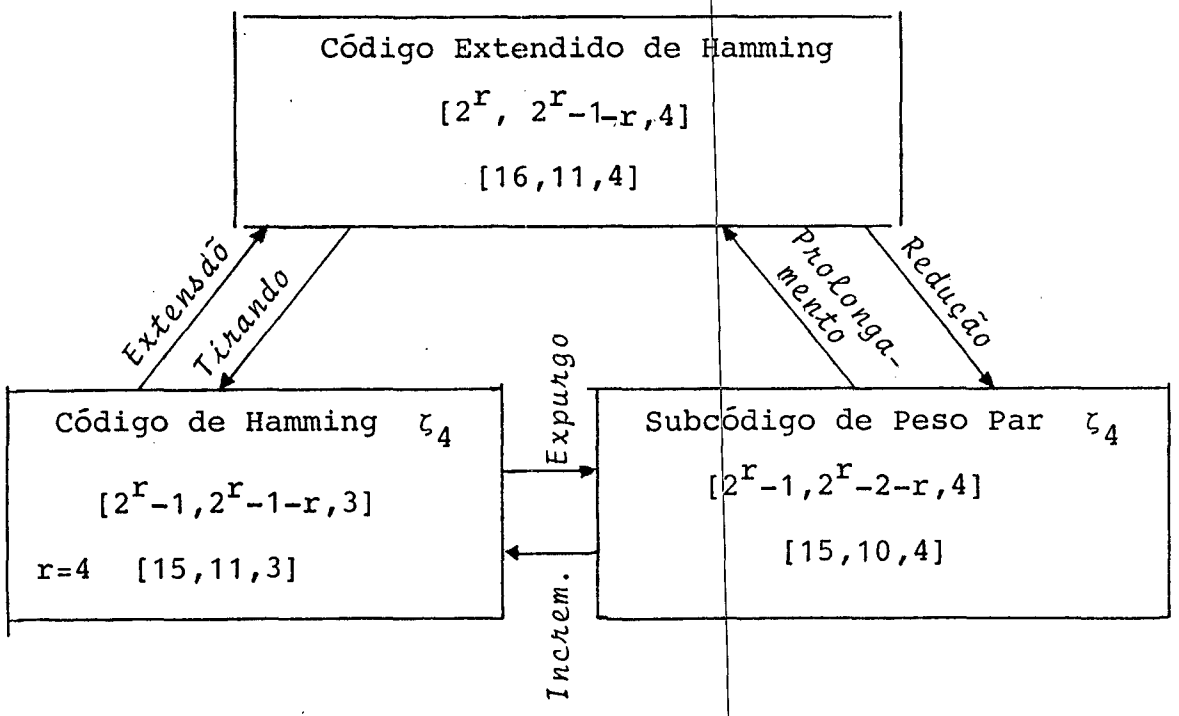


Fig.1.5.7 - Variações sobre um Código de Hamming.

6 - CÓDIGOS PRODUTO. [11]

Definição 1.6.1 - Se $A = (a_{ij})$ é uma matriz mxm e $B = (b_{ij})$ é uma matriz nxn sobre algum corpo, o produto de Kronecker de A e B é a matriz mn x mn obtida substituindo cada elemento a_{ij} por $a_{ij}.B$. Este produto é escrito por $A \otimes B$. Simbolicamente, nós temos $A \otimes B = (a_{ij}B)$.

Por exemplo, se $A = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$ e $B = \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}$

$$A \otimes B = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{vmatrix} \quad \text{e} \quad B \otimes A = \begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix}$$

Isto mostra, que no geral $A \otimes B \neq B \otimes A$.

É possível pela combinação de dois ou mais códigos, obter um código mais poderoso, isto é, código com capacidade maior para detecção e correção de erro. Uma destas combinações entre códigos nos dá o código produto, que tem a vantagem de poder corrigir erros aleatórios ou em pedaços.

Um dígito de verificação de paridade sobre um vetor é capaz de detectar todos os erros únicos. Este tipo de verificação de paridade é muito usado em computadores. Agora, consideremos os dígitos de informação escritos na forma retangular como está mostrado na figura abaixo, com um dígito global de verificação de paridade sobre cada linha e cada coluna.

Dígitos de Informação	Verificação Sobre Linhas
Verificação sobre Colunas	Verificação Sobre Verificação

Esta iteração de um código com uma verificação de paridade, é capaz de corrigir todos os erros únicos, porque, se um único erro ocorre, as linhas e colunas em que o erro ocorreu é indicado pela falha de verificação de paridade.

Este código tem a distância mínima 4 e é capaz de corrigir um único erro e detectar dois erros. Este código é usado nas unidades de fitas magnéticas utilizadas em computadores.

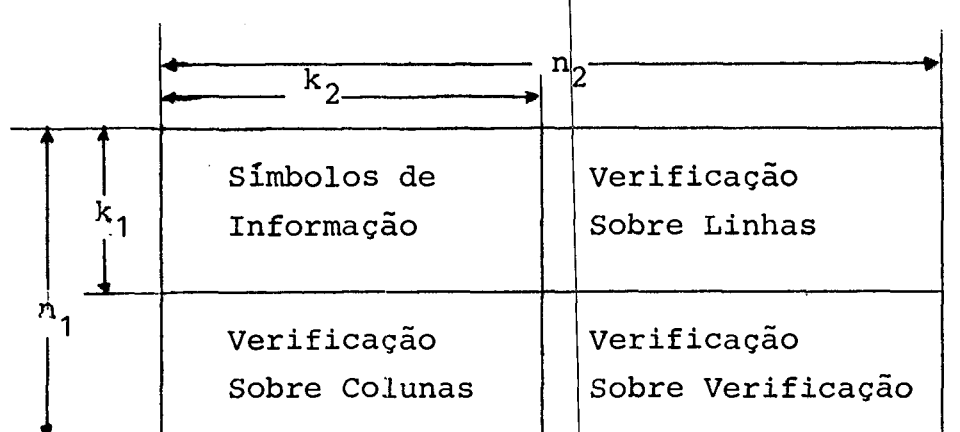
Exemplo 1.6.1

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

O código produto desta forma é um código linear.

Se A e B são respectivamente, $[n_1,k_1,d_1]$ e $[n_2,k_2,d_2]$ códigos lineares sobre GF(q) (GF(q) é um corpo finito com q elementos, onde q é um número primo ou uma potência de primo). Suponha por simplicidade, que os símbolos de informação são os primeiros k_1 símbolos de A e os primeiros k_2 símbolos de B.

Definição 1.6.2 - O produto direto $A \otimes B$ é um $[n_1n_2,k_1k_2,d_1d_2]$ código, cujas palavras código consistem de todos n_1xn_2 arranjos construído como segue:



O canto superior esquerdo contém os k_1k_2 símbolos de informação. As primeiras k_2 colunas são escolhidas de modo que pertença a A, e em seguida as linhas são complementadas de modo que pertença a B. Isto,é também chamado o produto de Kronecker de A e B e é simplesmente chamado de código produto. As colunas são palavras código de A, e as linhas são palavras código de B. Também

podemos construir os arranjos de modo contrário, isto é, primeiro as linhas e depois as colunas.

Exemplo 1.6.2 - O produto direto do código binário [3,2,2] com ele mesmo é o código [9,4,4] consistindo dos 16 arranjos mostrados a seguir:

[3,2,2] x [3,2,2] = [9,4,4]

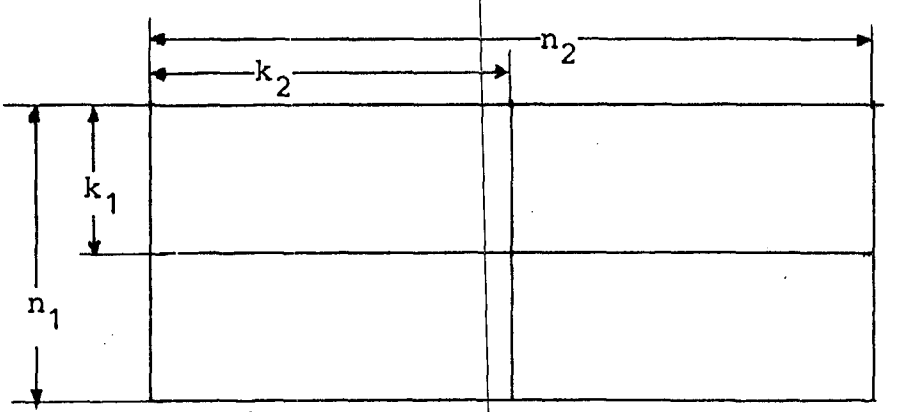
0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 1 1	1 0 1	1 1 0
0 0 0	0 1 1	1 0 1	1 1 0

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

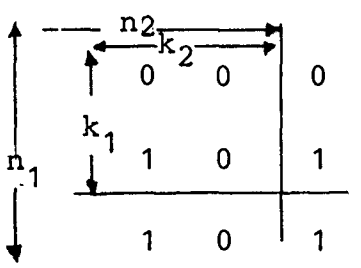
1 0 1	1 0 1	1 0 1	1 0 1
0 0 0	0 1 1	1 0 1	1 1 0
1 0 1	1 1 0	0 0 0	0 1 1

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

onde cada arranjo é da forma:



Por exemplo.



Observamos que cada arranjo corresponde a uma palavra código, assim temos as seguintes palavras código:

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

Calculemos agora a matriz geratriz de $G = A \otimes B$, onde A = B. Temos que

$$G_1 = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix}$$

então

$$G = G_1 \otimes G_2 = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{vmatrix}$$

Se calcularmos as palavras código utilizando a matriz geratriz do código produto, isto é, utilizando a equação x =u.G, verificaremos que as palavras código, serão as mesmas obtidas utilizando os arranjos.

Exemplo 1.6.3 - Seja A = [3,2], B = [4,3], onde

$$G_1 = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} \qquad G_2 = \begin{vmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{vmatrix}$$

as palavras código de A e B são respectivamente,

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

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

Os 64 arranjos são:

0000	0000	0000	0000	0000	0000	0000	0000
0000	0110	0101	1001	0011	1100	1010	1111
0000	0110	0101	1001	0011	1100	1010	1111
1111	1111	1111	1111	1111	1111	1111	1111
0000	1111	0110	1010	1100	0011	0101	1001
1111	0000	1001	0101	0011	1100	1010	0110
0110	0110	0110	0110	0110	0110	0110	0110
0000	1111	0110	1010	1100	0011	0101	1001
0110	1001	0000	1100	1010	0101	0011	1111
1010	1010	1010	1010	1010	1010	1010	1010
0000	1111	0110	1010	1100	0011	0101	1001
1010	0101	1100	0000	0110	1001	1111	0011
1100	1100	1100	1100	1100	1100	1100	1100
0000	1111	0110	1010	1100	0011	0101	1001
1100	0011	1010	0110	0000	1111	1001	0101
0011	0011	0011	0011	0011	0011	0011	0011
0000	1111	0110	1010	1100	0011	0101	1001
0011	1100	0101	1001	1111	0000	0110	1010
0101	0101	0101	0101	0101	0101	0101	0101
0000	1111	0110	1010	1100	0011	0101	1001
0101	1010	0011	1111	1001	0110	0000	1100
1001	1001	1001	1001	1001	1001	1001	1001
0000	1111	0101	1010	1100	0011	0101	1001
1001	0110	1100	0011	0101	1010	1100	0000

Como cada arranjo é uma palavra código, então temos as seguintes palavras código:

000000000000	110000001100
000011001100	110011110011
000001010101	110001101010
000010011001	110010100110
000000110011	110011000000
000011001100	110000111111
000010101010	110001011001
000011111111	110010010101
111100001111	001100000011
111111110000	001111111100
111101101001	001101100101
111110100101	001110101001
111111000011	001111001111
111100111100	001100110000
111101011010	001101010110
111110010110	001110011010
011011111001	010100000101
011000000110	010111111010
011001100000	010101100011
011010101100	010110101111
011011001010	010111001001
011000110101	010100110110
011001010011	010101010000
011010011111	010110011100
101000001010	100100001001
101011110101	100111110110
101001101100	100101101111
101010100000	100110100011
101011000110	100111000101
101000111001	100100111010
101001011111	100101011100
101010010011	100110010000

Calculemos agora a matriz geratriz $G = G_1 \otimes G_2$

$$G = \left\| \begin{array}{cccccccccccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{array} \right\|$$

Também podemos notar que: - se calcularmos as palavras código utilizando a matriz geratriz do código produto obtermos as mesmas palavras código obtidas com os arranjos.

Poranto, o produto $A \otimes B$ é definido como sendo o código $[n_1n_2, k_1k_2, d_1d_2]$ cujas palavras código consistem de todos os $n_1 x n_2$ arranjos em que as colunas pertencem a A e as linhas pertencem a B.

Teorema 1. [09] - O peso mínimo do produto de dois códigos é o produto dos pesos mínimos destes códigos.

Prova. - Se um código tem peso mínimo w_1 e outro tem peso mínimo w_2, um vetor no código produto deve ter pelo menos w_1 elementos não nulos em cada linha que contém um elemento não nulo, e pelo menos w_2 elementos não nulos em cada coluna, que contém um elemento não nulo, portanto, o código produto, pelo menos tem w_1w_2 elementos não nulos.

No próximo capítulo estudaremos uma família de códigos lineares que são chamados de Códigos de Reed-Muller.

CAPÍTULO II

OS CÓDIGOS DE REED-MULLER.

1. Introdução. - Os códigos de Reed-Muller formam uma família de códigos antigos e bem conhecidos na literatura da Teoria da Codificação e têm como vantagem, a facilidade de codificação.

Neste capítulo estudaremos os códigos de Reed-Muller ou (RM), as propriedades básicas, sua construção e o produto entre dois códigos de Reed-Muller. Será mostrado através de exemplo, também neste capítulo que o produto de dois códigos RM, nem sempre é um código RM, mas que pode ser considerado como um subcódigo de um código de RM de ordem maior.

2. Funções Booleanas. - Definiremos os códigos de Reed-Muller em termos de funções Booleanas.

Seja $v = (v_1, v_2, \ldots, v_m)$ uma m-upla binária escolhida sobre V_m que é o conjunto de todas as m-uplas binárias.

Definição 2.2.1 - Uma função $f(v) = f(v_1, v_2, \ldots, v_m)$ que toma os valores 0 ou 1 é chamada de função Booleana. Tal função pode ser expecificada por uma tabela verdadeira que dá os valores de f em todos os 2^m argumentos.

Exemplo 2.2.1 - Seja $m = 3$, uma função Booleana que é especificada pela seguinte tabela verdadeira.

$v_3 = 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1$
$v_2 = 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1$
$v_1 = 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1$
$f = 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0$

A última linha da tabela dá valores tomados por f, e é um valor binário de comprimento $n = 2^m$ que é denotado por f.

Um código consistirá de todos os vetores f, onde a função f pertence a uma certa classe.

Observação. - Como a última linha da tabela verdadeira pode ser satisfeita arbitrariamente, temos que existem 2^{2^m} funções Booleanas de m variáveis.

As operações de lógica usuais podem ser usadas para funções Booleanas. Sabemos que as operações usuais são:

$$\begin{aligned} &f \text{ EXCLUSIVO OU } g = f + g \\ &f \quad E \quad g = f.g \\ &f \quad OU \quad g = f + g + f.g \\ &\quad NÃO \quad f = \bar{f} = 1 + f \end{aligned} \qquad (2.2.1)$$

O lado direito destas equações define as operações em termos de funções binárias.

A função Booleana f do exemplo 2.2.1 pode ser escrita da seguinte maneira:

$f = v_1v_2\bar{v}_3$ OU $\bar{v}_1\bar{v}_2v_3$, usando as equações 2.2.1, temos:

$$\begin{aligned} f &= v_1v_2\bar{v}_3 + v_3\bar{v}_1\bar{v}_2 + v_1v_2\bar{v}_3v_3\bar{v}_1\bar{v}_2 \\ &= v_1v_2(1 + v_3) + v_3(1 + v_1)(1 + v_2) \\ &= v_1v_2 + v_1v_2v_3 + v_3 + v_3v_2 + v_3v_1 + v_1v_2v_3 \\ &= v_3 + v_1v_2 + v_3v_2 + v_3v_1 \end{aligned}$$

Observações: - 1) Note que $v_i^2 = v_i$, $\forall i$

2) è claro que qualquer função Booleana pode ser escrita como a soma de 2^m funções.

$$1, v_1, v_2, \ldots, v_m, v_1v_2, v_1v_3, \ldots, v_{m-1}v_m, v_1v_2\ldots v_m \qquad (2.2.2)$$

com os coeficientes que são 0 e 1. Como existem um total de 2^{2^m} funções Booleanas, todas estas funções devem ser distintas. Em outras palavras, os 2^m vetores correspondentes às funções (2.2.2) são linearmente independentes.

Definição 2.2.2 - A forma normal disjuntiva de uma função Booleana é dada por

$$f(v_1,\ldots,v_m) = \sum_{i_1=0}^{1} \ldots \sum_{i_m=0}^{1} f(i_1,\ldots,i_m) w_1^{i_1} \ldots w_m^{i_m} \text{ , onde}$$

$w_r^1 = w_r$, $w_r^0 = \bar{v}_r$.

Exemplo 2.2.2 - $f = v_3+v_1v_2+v_3v_2+v_3v_1$ está na forma normal disjuntiva.

Teorema 1. - Qualquer função Booleana f pode ser extendida em potências de v_i como

$$f(v_1,\ldots,v_m) = \sum_{a \varepsilon v_m} g(a) v_1^{a_1} \ldots v_m^{a_m} \qquad (2.2.3)$$

onde os coeficientes são dados por

$$g(a) = \sum_{b \subset a} f(b_1,\ldots,b_m) \qquad (2.2.4)$$

onde $b \subset a$ significa que os 1's em b são um subconjunto dos 1's em a.

Verificando para m = 2.

$$f(v_1,v_2) = f(0,0)(1+v_1)(1+v_2)+f(0,1)(1+v_1)v_2+f(1,0)v_1(1+v_2)+$$
$$+f(1,1)v_1v_2$$
$$= f(0,0)1+\{f(0,0)+f(1,0)\}v_1+\{f(0,0)+f(0,1)\}v_2+$$
$$+\{f(0,0)+f(1,0)+f(1,1)\}v_1v_2,$$

3. Códigos de Reed-Muller. [09]

Definição 2.3.1 - O código binário de Reed-Muller de r-ésima ordem, R(r,m) de comprimento $n=2^m$, para $0 \leq r \leq m$ é o conjunto de todos os vetores f, onde $f(v_1,v_2,\ldots,v_m)$ é uma função Booleana, que é um polinômio de grau no máximo r.

Exemplo 2.3.1 - Seja m=3, r=1. Então o código de Reed-Muller de primeira ordem de comprimento n = 8, consiste em 16 palavras código.

$a_0,1+a_1v_1+a_2v_2+a_3v_3$, $a_i = 0$ ou 1, i = 0,1,2,3.

As 16 palavras código são escritas na Fig.2.3.1,abaixo,

0	0 0 0 0 0 0 0 0
v_3	0 0 0 0 1 1 1 1
v_2	0 0 1 1 0 0 1 1
v_1	0 1 0 1 0 1 0 1
v_2+v_3	0 0 1 1 1 1 0 0
v_1+v_3	0 1 0 1 1 0 1 0
v_1+v_2	0 1 1 0 0 1 1 0
$v_1+v_2+v_3$	0 1 1 0 1 0 0 1
1	1 1 1 1 1 1 1 1
$1+v_3$	1 1 1 1 0 0 0 0
$1+v_2$	1 1 0 0 1 1 0 0
$1+v_1$	1 0 1 0 1 0 1 0
$1+v_2+v_3$	1 1 0 0 0 0 1 1
$1+v_1+v_3$	1 0 1 0 0 1 0 1
$1+v_1+v_3$	1 0 0 1 1 0 0 1
$1+v_1+v_2+v_3$	1 0 0 1 0 1 1 0

Fig. 2.3.1 - Palavras código de R(1,3).

Observação.- Podemos notar que R(1,m) é sempre dual de um código extendido de Hamming, e que todas as palavras código de R(1,m) exceto 0 e 1 tem peso 2^{m-1}.

No geral o código RM de r-ésima ordem consiste de todas as combinações lineares dos vetores correspondentes aos produtos $1, v_1, \ldots, v_m, v_1v_2, \ldots, v_2v_3, \ldots, v_{m-1}v_m, \ldots$ (até o grau de ordem r). Então estes vetores formam uma base do código.

Existem $k = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r} = \sum_{i=0}^{r} \binom{m}{i}$ vetores binários, e são linearmente independentes. Então k é a dimensão do código.

Exemplo 2.3.1 - Seja m = 4 então os 16 possíveis veto - res básicos para os códigos de Reed-Muller de comprimento 16 são mostrados na figura 2.3.2.

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
v_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
v_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
v_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
v_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
v_3v_4	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
v_2v_4	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1
v_1v_4	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1
v_2v_3	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1
v_1v_3	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1
v_1v_2	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
$v_2v_3v_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
$v_1v_3v_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
$v_1v_2v_4$	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
$v_1v_2v_3$	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
$v_1v_2v_3v_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Fig.2.3.2 - Vetores básicos para códigos de Reed-Muller de comprimento 16.

Os vetores básicos para códigos de Reed-Muller de r-ésima ordem de comprimento 16, R(r,4), são:

Ordem r	Linhas de Fig.2.3.2
0	1
1	1 a 5
2	1 a 11
3	1 a 15
4	todas

Exemplo 2.3.2 - R(2,4) tem como matriz geratriz G, as linhas de 1 a 11 da Fig.2.3.2 e possui 2^{11} palavras código que são obtidas, fazendo todas as possíveis combinações lineares com as linhas de G.

Exemplo 2.3.3 - O código R(2,3) possui a seguinte matriz geratriz G.

$$G = \left|\begin{array}{cccccccc|c} 1&1&1&1&1&1&1&1 & 1 \\ 0&0&0&0&1&1&1&1 & v_3 \\ 0&0&1&1&0&0&1&1 & v_2 \\ 0&1&0&1&0&1&0&1 & v_1 \\ 0&0&0&1&0&0&0&1 & v_1v_2 \\ 0&0&0&0&0&1&0&1 & v_1v_3 \\ 0&0&0&0&0&0&1&1 & v_2v_3 \end{array}\right|$$

possuindo 2^7 palavras código, que são obtidas fazendo todas as possíveis combinações lineares com as linhas de G.

Os códigos de Reed-Muller de comprimento 2^{m+1} podem ser obtidos simplesmente de códigos de Reed-Muller de comprimento 2^m, usando a construção $|u||u+v|$ (veja 1.5.1).

Observemos que o código ϕ_3 construído no exemplo 1.5.1 usando os códigos $\phi_1 = [4,3]$ e $\phi_2 = [4,1]$ é o código $\phi_3 = [8,4] = R(1,3)$, código de Reed-Muller de primeira ordem.

Teorema 2. $R(r+1,m+1) = \{|u||u+v| : u \in R(r+1,m), v \in R(r,m)\}$

Prova. - Pela definição, uma palavra código típica f em R(r+1,m+1) vem de um polinômio $f(v_1,..,v_{m+1})$ de grau no máximo r+1. Nós podemos escrever:

$f(v_1,...,v_{m+1}) = g(v_1,...,v_m)+v_{m+1}h(v_1,...,v_m)$, onde grau(g) ≤ r+1 e grau(h) ≤ r. Sejam g e h os vetores (de comprimento 2^m) correspondendo a $g(v_1,...,v_m)$ h $(v_1,...,v_m)$. Naturalmente $g \in R(r+1,m)$ e $h \in R(r,m)$. Mas agora, considere $g(v_1,...,v_m)$ e $v_{m+1}h(v_1,...,v_m)$ como polinômios em $v_1,...,v_{m+1}$. Os vetores correspondentes (agora de comprimento 2^{m+1}) são $|g||g|$ e $|0||h|$. Pois se $f(v_1,...,v_m)$ é uma função Booleana de m variáveis e se f é o vetor binário correspondente de comprimento 2^m, então os vetores de comprimento 2^{m+1} correspondente a $g(v_1,...,v_{m+1})=f(v_1,...,v_m)$ e $h(v_1,...,v_{m+1}) = v_{m+1}f(v_1,...,v_m)$ são $|f||f|$ e $|0||f|$ respectivamente. Portanto, $f = |g||g|+|0||h|$.

Observação.- Existe uma relação equivalente em termos de matriz geratriz. Se G(r,m) é uma matriz geratriz para R(r,m). Então o teorema diz que:

$$G(r+1,m+1) = \left|\begin{array}{cc} G(r+1,m) & G(r+1,m) \\ 0 & G(r,m) \end{array}\right|$$

Realmente uma palavra código gerada por esta matriz tem a forma $|u||u+v|$, onde $u\varepsilon R(r+1,m)$, $v\varepsilon R(r,m)$.

Exemplo 2.3.4 - Seja $r = 1$, $m = 3$, então

$$G(2,4) = \begin{vmatrix} G(2,3) & G(2,3) \\ 0 & G(1,3) \end{vmatrix}$$

e

$$G(2,3) = \begin{vmatrix} 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&1&0&1 \\ 0&0&0&1&0&0&0&1 \end{vmatrix}$$

$$G(1,3) = \begin{vmatrix} 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1&1 \end{vmatrix}$$

Assim,

$$G(2,4) = \begin{vmatrix} 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \end{vmatrix}$$

Observemos que as linhas da matriz G(2,4) são as linhas de 1 a 11 da Fig.2.3.2.

<u>Observação</u> - R(r,m) tem a distância mínima 2^{m-r}.

A figura 2.3.3 mostra as dimensões de alguns dos primeiros [n,k,d] códigos RM:

Comprimento n	4	8	16	32	64	128	256	512
m	2	3	4	5	6	7	8	9
Distância d	Dimensão k							
1	4	8	16	32	64	128	256	512
2	3	7	15	31	63	127	255	511
4	1	4	11	26	57	120	247	502
8		1	5	16	42	99	219	466
16			1	6	22	64	163	382
32				1	7	29	93	256
64					1	8	37	130
128						1	9	46
256							1	10
512								1

Fig. 2.3.3 - Códigos de Reed-Muller.

Teorema 3. - $R(m-r-1,m)$ é o código dual do $R(r,m)$ para $0 \leq r \leq m-1$.

Prova. - Seja $a \in R(m-r-1,m)$, $b \in R(r,m)$. Então $a(v_1,\ldots,v_m)$ é um polinômio de grau $\leq m-r-1$, $b(v_1,\ldots,v_m)$ tem grau $\leq r$, e seu produto ab tem grau $\leq m-1$. Portanto, ab $\in R(m-1,m)$ e tem peso par. Como $ab \equiv 0 \pmod 2$, então $R(m-r-1,m) \subset R(r,m)^{\perp}$. Mas,

$$\dim R(m-r-1,m) + \dim R(r,m) = 1 + \binom{m}{1} + \ldots + \binom{m}{m-r-1} + 1 + \binom{m}{1} + \ldots + \binom{m}{r} = 2^m,$$

que implica $R(m-r-1,m) = R(r,m)^{\perp}$.

Exemplo 2.3.5 - Seja $R(2,3) = [8,7]$, então $R^{\perp} = R(m-r-1,m) = R(0,3) = [8,1]$.

4. Códigos Produto de Reed-Muller. [10]

Vimos no item 3 que o código de Reed-Muller de r-ésima ordem é formado usando os vetores básicos $v_0, v_1, \ldots, v_m$ e todos os produtos destes vetores tomando r ou menos, ao mesmo tempo, onde $v_1, v_2, \ldots, v_m$ são as linhas da matriz que tem todas as possíveis m-uplas binárias como colunas e v_o tendo todas as componentes com 1.

Sabemos que, se A é um $[n_1, k_1, d_1]$ código e B é um $[n_2, k_2, d_2]$ código, então o código produto A.B é o $[n_1 n_2, k_1 k_2, d_1 d_2]$ código.

De fato A.B consiste dos $n_1 x n_2$ arranjos cujas linhas são elementos de A e as colunas são elementos de B. Vimos também, no item 3 que o código R(r,m) tem comprimento $n = 2^m$, dimensão $k = \sum_{i=0}^{r} \binom{m}{i}$ e a distância mínima $d = 2^{m-r}$.

Assim, se A = R(r,m) e B = $R(r_2, m_2)$ então o código produto A.B é um código de comprimento $n = n_1 n_2 = 2^{m_1+m_2}$ e dimensão $k = k_1 k_2 = \left(\sum_{i=0}^{r_1} \binom{m_1}{i}\right)\left(\sum_{i=0}^{r_2} \binom{m_2}{i}\right)$ e a distância mínima $d = 2^{m_1+m_2-(r_1+r_2)}$.

A seguir examinaremos a relação entre $R(r_1, m_1)$ $R(r_2, m_2)$ e $R(r_1+r_2, m_1+m_2)$.

Para mostrar isto, provaremos o seguinte lema:

Lema 1.

$$\left(\sum_{i=0}^{r_1} \binom{m_1}{i}\right)\left(\sum_{i=0}^{r_2} \binom{m_2}{i}\right) \leq \sum_{i=0}^{r_1+r_2} \binom{m_1+m_2}{i} \qquad (2.4.1)$$

com a igualdade se, e somente se, $r_1 = m_1$ e $r_2 = m_2$.

Prova. - Sabemos que

$$(1 + x)^{m_1+m_2} = \sum_{i=0}^{m_1+m_2} \binom{m_1+m_2}{j} x^j,$$

e

$$(1 + x)^{m_1}(1 + x)^{m_2} = \left(\sum_{k=0}^{m_1} \binom{m_1}{k} x^k\right)\left(\sum_{l=0}^{m_2} \binom{m_2}{l} x^l\right).$$

Comparando os coeficientes de potências semelhantes de x nos desenvolvimentos $(1 + x)^{m_1+m_2}$ e $(1 + x)^{m_1}(1+ x)^{m_2}$, nós temos

$$\sum_{r_1=0}^{n} \binom{m_1}{r_1}\binom{m_2}{n-r_1} = \binom{m_1+m_2}{n} \qquad (2.4.2)$$

com $0 \leq r_1 \leq n \leq m_1+m_2$

Seja, $A = \sum_{i=0}^{r_1}\binom{m_1}{i}$, $B = \sum_{i=0}^{r_2}\binom{m_2}{i}$ e $C = \sum_{i=0}^{r_1+r_2}\binom{m_1+m_2}{i}$. Agora,

$$A.B = \sum_{\substack{0\leq j\leq r_2 \\ 0\leq i\leq r_1}} \binom{m_1}{i}\binom{m_2}{j} = \sum_{k=0}^{r_1+r_2} \cdot \sum_{i+j=k} \binom{m_1}{i}\binom{m_2}{j}.$$

$$i\leq r_1, j\leq r_2$$

Usando 2.4.2, C pode ser escrito da seguinte forma:

$$C = \sum_{i=0}^{r_1+r_2}\binom{m_1+m_2}{i} = \sum_{k=0}^{r_1+r_2} \sum_{i+j=k} \binom{m_1}{i}\binom{m_2}{j}.$$

Mas,

$$\sum_{\substack{i+j=k \\ i\leq r_1, j\leq r_2}} \binom{m_1}{i}\binom{m_2}{j} \leq \sum_{i+j=k} \binom{m_1}{i}\binom{m_2}{j}. \quad \text{Então, } A.B \leq C.$$

A igualdade em 2.4.1 é satisfeita, quando

$$\sum_{\substack{i+j=k \\ i\leq r_1, j\leq r_2}} \binom{m_1}{i}\binom{m_2}{j} = \sum_{i+j=k} \binom{m_1}{i}\binom{m_2}{j}, \quad k\leq r_1+r_2.$$

Escolhendo $k = r_1+ 1$, com $i = r_1$, nós vemos que a igualdade garante que $\binom{m_1}{r_1+1} = 0$, isto é, $r_1 + 1 > m_1$. Assim $r_1 = m_1$.

Similarmente pode ser visto que a igualdade em 2.4.1 garante $r_2 = m_2$.

Teorema 4. - Para $0 < r_1 \leq m_1$ e $0 < r_2 \leq m_2$ o código produto $R(r_1,m_1)R(r_2,m_2)$ é um subcódigo de $R(r_1+r_2,m_1+m_2)$.

Prova. - Sejam G_1 e G_2 as matrizes geratrizes de $R(r_1,m_1)$ e $R(r_2,m_2)$, respectivamente, e sejam as linhas da matriz G_1 os vetores $u_1,u_2,\ldots,u_m,u_0$ e seus produtos tomando r_1 ou menos, ao mesmo tempo, e as linhas da matriz G_2 os vetores $v_1,v_2,\ldots,v_{m_2},v_0$ e seus produtos tomando r_2 ou menos, ao mesmo tempo. É claro que $u_1,u_2,\ldots,u_{m_1}$ são as linhas de uma matriz contendo todas as m_1-uplas como colunas e u_0 é um vetor cujas 2^{m_1} componentes são 1. Similarmente $v_1,v_2,\ldots,v_{m_2}$ são as linhas de uma matriz cujas colunas são todas as m_2-uplas e v_0 é um vetor cu

jos 2^{m_2} componentes são 1. Além disso, a matriz geratriz de $R(r_1+r_2,m_1+m_2)$ tem como suas linhas $w_1,w_2,\ldots,w_{m_1+m_2},w_0$ e os seus produtos tomando r_1+r_2 ou menos, ao mesmo tempo.

Seja a matriz geratriz do código produto $R(r_1,m_1)R(r_2,m_2)$, então $G = G_1 \otimes G_2$.

Seja,

$$G_1 = \begin{vmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_1 \end{vmatrix}$$

onde cada a_j $(1 \leq j \leq 1)$ é um produto de u_i's tomando r_1 ou menos, ao mesmo tempo. Então.

$$G = \begin{vmatrix} a_1*G_2 \\ a_2*G_2 \\ \cdot \\ \cdot \\ \cdot \\ a_1*G_2 \end{vmatrix}$$

Supondo $a_j = u_{j1}u_{j2}\ldots u_{jk}$, $1 \leq k \leq r_1$ e seja a t-ésima linha de G_2; $v_{t_1},v_{t_2},\ldots,v_{t_q}$, $1 \leq q \leq r_2$. Então a t-ésima linha de um bloco a_j*G_2 em $G_1 \otimes G_2$ como uma linha em G é

$w = w_{m_2+j_1}w_{m_2+j_2}\ldots w_{m_2+j_k}w_{t_1}\ldots w_{t_q}$, $k \leq r_1$, $q \leq r_2$.

É claro que o número de produtos em w é menor ou igual que r_1+r_2. Desta forma, cada linha de G, é um elemento de $R(r_1+r_2,m_1+m_2)$. Também de acordo com o lema acima $\dim R(r_1,m_1)R(r_2,m_2) \leq \dim R(r_1+r_2,m_1+m_2)$. Portanto, $R(r_1,m_1)R(r_2,m_2)$ é um subcódigo de $R(r_1+r_2,m_1+m_2)$.

Agora consideremos o exemplo de código produto de Reed-Muller.

Exemplo 2.4.1 - Para algum m_1,m_2 $R(1,m_1+m_2)$"C" $R(1,m_1)$. $R(1,m_2)$"C" $R(2,m_1+m_2)$, onde "C" representa o"subcódigo de".

Seja $A = R(1,m_1)$, $B = R(1,m_2)$, $C = R(2,m_1+m_2)$ e $C' = R(1,m_1+m_2)$, claramente $\dim C = 1 + \binom{m_1+m_2}{1}\binom{m_1+m_2}{2}$, e $\dim C' = 1 + (m_1+m_2)$, $\dim AB = (1+m_1)(1+m_2)$ e $1 + m_1 + m_2 < (1+m_1)(1+m_2) \leq 1 + \binom{m_1+m_2}{1}\binom{m_1+m_2}{2}$. Sejam G_1 e G_2 as matrizes geratrizes de A e B, respectivamente. Então,

$$G_1 = \begin{vmatrix} u_{m_1} \\ u_{m_1-1} \\ \vdots \\ u_2 \\ u_1 \\ u_0 \end{vmatrix} = \left| \begin{array}{cc} \overbrace{\cdots\cdots\cdots}^{2^{m_1-1}} & \overbrace{\text{---}\cdots\text{---}}^{2^{m_1-1}} \\ \overbrace{\cdots\cdots}^{2^{m_1-2}}\overbrace{\text{---}\cdots\text{---}}^{2^{m_1-2}} & \overbrace{\cdots\cdots}^{2^{m_1-2}}\overbrace{\text{---}\cdots\text{---}}^{2^{m_1-2}} \\ & \\ & \\ & \\ & \\ 0\,1\,0\,1\,0\,1\,0\,1\,\ldots\ldots & \ldots\ldots\,0\,1\,0\,1\,0\,1 \\ 1\,1\,1\,1\,1\,1\,1\,1\,\ldots\ldots & \ldots\ldots\,1\,1\,1\,1\,1\,1 \end{array} \right|$$

$$G_2 = \begin{vmatrix} v_{m_2} \\ v_{m_2-1} \\ \vdots \\ v_2 \\ v_1 \\ v_0 \end{vmatrix} = \left| \begin{array}{cc} \overbrace{\cdots\cdots\cdots}^{2^{m_2-1}} & \overbrace{\text{---}\cdots\text{---}}^{2^{m_2-1}} \\ \overbrace{\cdots\cdots}^{2^{m_2-2}}\overbrace{\text{---}\cdots\text{---}}^{2^{m_2-2}} & \overbrace{\cdots\cdots}^{2^{m_2-2}}\overbrace{\text{---}\cdots\text{---}}^{2^{m_2-2}} \\ & \\ & \\ & \\ & \\ 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,\ldots & \ldots\ldots\,0\,1\,0\,1\,0\,1\,0 \\ 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,\ldots & \ldots\ldots\,1\,1\,1\,1\,1\,1\,1 \end{array} \right|$$

onde $\ldots\overset{r}{\ldots}\ldots$ indicam r zeros consecutivos e $\_\_\_\overset{r}{\_}\_\_\_$ indicam os r uns consecutivos. A matriz geratriz G do código produto AB é então,

$$G = G_1 \otimes G_2 = \left| \begin{array}{cc} \overbrace{0\,0\,0\,0\,0\,0\,0\,0}^{2^{m_1-1}} & \overbrace{G_2\,G_2\,G_2\,G_2\,G_2\,G_2}^{2^{m_1-1}} \\ \overbrace{0\,0\,0\,0}^{2^{m_1-2}}\overbrace{G_2G_2G_2G_2}^{2^{m_1-2}} & \overbrace{0\,0\,0\,0}^{2^{m_1-2}}\overbrace{G_2G_2G_2G_2G_2}^{2^{m_1-2}} \\ 0\;G_2\;0\;G_2\;\ldots\ldots\ldots & \ldots\;0\;G_2\;0 \\ G_2\;G_2\;\ldots\ldots\ldots & \ldots\;G_2\;G_2G_2 \end{array} \right|$$

onde 0 em G é uma (m_2+1) x 2^{m_2} matriz nula.

Seja,

$$\begin{cases} w_{m_1+m_2} = \overbrace{\cdots\cdots\cdots}^{2^{m_1+m_2-1}}\overbrace{\cdots\cdots\cdots}^{2^{m_1+m_2-1}} \\ w_{m_1+m_2-1} = \overbrace{\cdots\cdots\cdots}^{2^{m_1+m_2-2}}\overbrace{\cdots\cdots\cdots}^{2^{m_1+m_2-2}}\overbrace{\cdots\cdots\cdots}^{2^{m_1+m_2-2}}\overbrace{\cdots\cdots\cdots}^{2^{m_1+m_2-2}} \\ \vdots \\ w_1 = \overbrace{0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,\ldots\ldots\,0\,1\,0\,1\,0\,1}^{2^{m_1+m_2}} \\ w_0 \quad \overbrace{1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,\ldots\ldots\,1\,1\,1\,1\,1}^{2^{m_1+m_2}} \end{cases}$$

Claramente $R(2,m_1+m_2)$ é gerado por $w_0,w_1,\ldots,w_{m_1+m_2}$ e $R(2,m_1+m_2)$ é gerado por $w_0,w_1,\ldots,w_{m_1+m_2}$ e seus produtos tomados dois a dois ao mesmo tempo. Se R_i denota a i-ésima linha de G, $0 \leq i \leq (m_1+1)(m_2+1)$, então podemos verificar facilmente o seguinte

$$\begin{cases} R_1 = w_{m_1+m_2}w_{m_2} \\ R_2 = w_{m_1+m_2}w_{m_2-1} \\ \vdots \\ R_{m_2+1} = w_{m_1+m_2} \end{cases}$$

$$\begin{cases} R_{m_2+2} = w_{m_1+m_2-1}w_{m_2} \\ R_{2(m_2+1)} = w_{m_1+m_2-1} \end{cases}$$

$$\vdots$$

$$\begin{cases} R_{m_1(m_2+1)+1} = w_{m_2} \\ R_{(m_1+1)(m_2+1)} = w_0 \end{cases}$$

Então o conjunto de linhas de G é um subconjunto das bases de $R(2,m_1+m_2)$. Portanto, $A.B \subset C$.

Além disso, a matriz geratriz de $C' = R(1,m_1+m_2)$ é

$$\begin{vmatrix} w_{m_1+m_2} \\ \cdot \\ \cdot \\ \cdot \\ w_1 \\ w_0 \end{vmatrix}$$

Mas,

$$w_0 = R_{(m_1+1)(m_2+1)}$$
$$w_1 = R_{(m_1+1)(m_2+1)-1}$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$w_{m_2} = R_{m_1(m_2+1)+1}$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$w_{m_1+m_2} = R_{m_2+1}$$

Poranto, $C' \subset$ A.B.

Exemplo 2.4.2 - Seja agora R(1,2) e R(1,3), verifiquemos então de R(1,2)R(1,3)"C" R(2,5). A matriz geratriz do código R(2,5) é

$$G(2,5) = \left|\begin{array}{l}
00000000000000001111111111111111 \quad v_5 \\
00000000111111110000000011111111 \quad v_4 \\
00001111000011110000111100001111 \quad v_3 \\
00110011001100110011001100110011 \quad v_2 \\
01010101010101010101010101010101 \quad v_1 \\
11111111111111111111111111111111 \quad v_0 \text{ ou } 1 \\
00010001000100010001000100010001 \quad v_1v_2 \\
00000101000001010000010100000101 \quad v_1v_3 \\
00000000010101010000000001010101 \quad v_1v_4 \\
00000000000000000101010101010101 \quad v_1v_5 \\
00000011000000110000001100000011 \quad v_2v_3 \\
00000000001100110000000000110011 \quad v_2v_4 \\
00000000000000000011001100110011 \quad v_2v_5 \\
00000000000011110000000000001111 \quad v_3v_4 \\
00000000000000000000111100001111 \quad v_3v_5 \\
00000000000000000000000011111111 \quad v_4v_5
\end{array}\right|$$

As matrizes geratrizes dos códigos R(1,2) e R(1,3) são respectivamente,

$$G(1,2) = \left|\begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{array}\right| \qquad G(1,3) = \left|\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right|$$

Portanto,

$$G(1,2) \otimes G(1,3) = \left|\begin{array}{l}
00000000000000000000111100001111 \\
00000000000000000011001100110011 \\
00000000000000000101010101010101 \\
00000000000000001111111111111111 \\
00000000000011110000000000001111 \\
00000000001100110000000000110011 \\
00000000010101010000000001010101 \\
00000000111111110000000011111111 \\
00001111000011110000111100001111 \\
00110011001100110011001100110011 \\
01010101010101010101010101010101 \\
11111111111111111111111111111111
\end{array}\right|$$

Observemos que todas as linhas da matriz do código produto $R(1,2)R(1,3) = [32,12]$ que são palavras código, pertencem ã matriz geratriz do código $R(2,5) = [32,12]$. Portanto, $R(1,2)R(1,3)$"C" $R(2,5)$.

Pelo exemplo precedente poderia ser pensado que $R(r_1+r_2-1, m_1+m_2)$ é um subcódigo de $R(r_1,m_1)R(r_2,m_2)$. Mas o teorema seguinte mostra que isto nem sempre é verdadeiro.

Teorema 5. - Seja $r_1 = 2$, $r_2 = 2$. Então:

(i) - $\dim R(r_1+r_2-1, m_1+m_2) > \dim R(r_1,m_1)R(r_2,m_2)$, se $m_1=2$, $m_2 > 5$

(ii) - $\dim R(r_1+r_2-1, m_1+m_2) = \dim R(r_1,m_1)R(r_2,m_2)$, se $m_1=2$, $m_2 = 5$

(iii)- $\dim R(r_1+r_2-1, m_1+m_2) < \dim R(r_1,m_1)R(r_2,m_2)$, se $m_1=2$, $m_2 < 5$

Prova.

$$\dim R(2,m_1)R(2,m_2) = [\binom{m_1}{0}+\binom{m_1}{1}+\binom{m_1}{2}][\binom{m_2}{0}+\binom{m_2}{1}+\binom{m_2}{2}]$$

$$= \underbrace{\binom{m_1}{0}\binom{m_2}{0}}_{x} + \underbrace{\binom{m_1}{0}\binom{m_2}{1}+\binom{m_1}{1}\binom{m_2}{0}}_{y} + \underbrace{\binom{m_1}{0}\binom{m_2}{0}+\binom{m_1}{1}\binom{m_2}{1}}_{z}$$

$$+ \underbrace{\binom{m_1}{2}\binom{m_2}{0}+\binom{m_1}{2}\binom{m_2}{1}+\binom{m_1}{1}\binom{m_2}{2}+\binom{m_1}{2}\binom{m_2}{2}}_{t}, \quad \text{e}$$

$$\dim R(3,m_1+m_2) = \underbrace{\binom{m_1+m_2}{0}}_{x} + \underbrace{\binom{m_1+m_2}{1}}_{y} + \underbrace{\binom{m_1+m_2}{2}}_{z} + \binom{m_1+m_2}{3}. \quad \text{Então,}$$

$$\dim R(3,m_1+m_2) - \dim R(2,m_1)R(2,m_2) = \binom{m_2+m_1}{3} - t =$$

$$= \binom{m_1+m_2}{3} - \binom{m_1}{2}\binom{m_2}{1} - \binom{m_1}{1}\binom{m_2}{2} - \binom{m_2}{2}\binom{m_1}{2}$$

$$= \binom{m_1}{0}\binom{m_2}{3}+\binom{m_1}{1}\binom{m_2}{2}+\binom{m_1}{2}\binom{m_2}{1}+\binom{m_1}{3}\binom{m_2}{0}-[\binom{m_1}{2}\binom{m_2}{1}+\binom{m_1}{1}\binom{m_2}{2}+\binom{m_1}{2}\binom{m_2}{2}]$$

$$= \binom{m_2}{3} + \binom{m_1}{3} + \binom{m_2}{2}\binom{m_1}{2}$$

Tomando $m_1 = 2$, nós obtemos:

$$\dim R(3,2+m_1) - \dim R(2,2)R(2,m_2) = \binom{m_2}{3} - \binom{m_2}{2}$$

$$\begin{cases} > 0, \text{ se } m_2 > 5 \\ = 0, \text{ se } m_2 = 5 \\ < 0, \text{ se } m_2 < 5 \end{cases}$$

É interessante notar que a distância mínima de $R(r_1+r_2-1,m_1+m_2)$ é $2[2^{m_1+m_2-(r_1+r_2)}]$ que é duas vezes a distância mínima do código produto $R(r_1,m_1)R(r_2,m_2)$, mas, em alguns casos, a dimensão é igual a do $R(r_1+r_2-1,m_1+m_2)$. A tabela 2.4.1, abaixo nos dá a dimensão dos códigos $R(r_1+r_2-1,m_1+m_2)$, $R(r_1,m_1)R(r_2,m_2)$ e $R(r_1+r_2,m_1+m_2)$ para alguns valores de m_1,m_2, r_1 e r_2.

m_1	r_1	m_2	r_2	$R(r_1+r_2,m_1+m_2)$	$R(r_1,m_1)R(r_2,m_2)$	$R(r_1+r_2,m_1+m_2$
2	2	2	2	15	16	16
2	2	3	2	26	28	31
2	2	6	2	93	88	163
3	3	5	3	219	209	247
3	3	6	3	382	336	466
3	3	4	3	120	120	127
3	3	3	3	63	64	64
4	3	5	4	466	465	502
4	3	4	4	247	240	255

Tabela 2.4.1

Mostraremos agora que o produto de dois códigos de Reed-Muller no geral, não é um código de Reed-Muller.

Seja $R(r_1,m_1) = A = [n_1,k_1]$, onde $n_1 = 2^{m_1}$ e $k_1 = \sum_{i=0}^{r_1} \binom{m_1}{i}$ e seja $R(r_2,m_2) = B = [n_2,k_2]$, onde $n_2 = 2^{m_2}$ e $k_2 = \sum_{i=0}^{r_1} \binom{m_2}{i}$. Então o código produto $R(r_1,m_1)R(r_2,m_2) = A.B = [n_1n_2,k_1k_2]$ é um código de comprimento $n = n_1n_2 = 2^{m_1+m_2}$, $\dim k = k_1k_2 = \left(\sum_{i=0}^{r_1} \binom{m_1}{i}\right).\left(\sum_{i=0}^{r_2} \binom{m_2}{i}\right)$. Mas será que existe um certo r tal que $R(r_1,m_1)R(r_2,m_2) = R(r,m_1+m_2)$? Vejamos isto através de um exemplo. Seja $R(2,3) = A = [8,7]$ e $R(3,4) = B = [16,15]$, então $R(2,3)R(3,4) = A.B = [128,105]$. Verifiquemos então se existe um r tal que $105 = \sum_{i=0}^{r} \binom{7}{i}$. Sabemos que $r \leq m$, assim, os possíveis valores de r serão 1,2,3,4,5,6 e 7. Então se tomarmos r = 4 ou r = 5 que são os possíveis valores de r pois

$R(2,3)R(3,4)$"C" $R(5,7)$ obteremos os valores 99 e 130 que são diferentes de 105. Portanto, não existe r tal que $105 = \sum_{i=0}^{r} \binom{7}{i}$.

Logo, $R(r_1,m_1)R(r_2,m_2)$ não é um código de Reed-Muller.

Podemos verificar através do exemplo 2.4.1, onde $R(1,2)R(1,3)$"C" $R(2,5)$ que o código $R(1,2)R(1,3)$ não é um código de Reed-Muller de 1ª ordem, pois, na sua matriz geratriz aparecem os produtos v_1v_4, v_2v_4, v_3v_4, v_1v_5, v_2v_5, v_3v_5, mas também não é um código de Reed-Muller de 2ª ordem pois faltam os produtos v_1v_2, v_1v_3, v_2v_3, v_4v_5.

Mostraremos no próximo capítulo que o código produto de Reed-Muller é um tipo de código que será definido no capítulo seguinte.

CAPÍTULO III

CÓDIGOS AUTO DUAIS E CÓDIGOS DE ORDEM $r+(r+1)_{m,s}$.

1. Introdução. - Estudaremos neste capítulo, sob qual condição o dual de um código de peso par está contido no seu código próprio. Além disso, estudaremos os códigos lineares de ordem $r+(r+1)_{m,s}$, que são obtidos pela anexação de alguns vetores básicos de um código de Reed-Muller de ordem r.

Mostraremos que o código produto de Reed-Muller é um código linear, citado acima.

2. Códigos Auto Duais. [01]

Como já vimos no ítem 4 do capítulo I, se ϕ é um [n,k] código linear sobre F, então o seu dual $\phi^{\perp}$ é um [n,n-k] código, que é o conjunto de vetores que são ortogonais a toda palavra código de ϕ , isto é,

$$\phi^{\perp} = \{u/u.v = 0, \quad \forall v \in \phi\}$$

Definição 3.2.1 - Seja ϕ um [n,k] código linear binário e $\phi^{\perp}$ o seu [n,n-k] código dual. Se $\phi \subset \phi^{\perp}$, então ϕ é chamado auto dual fracamente.

Definição 3.2.2 - Se $\phi = \phi^{\perp}$ o código é dito auto dual.

Observações: - 1) ϕ é auto dual fracamente, se u.v = 0 para todo par (não cencessariamente distinto) de palavras código de ϕ.

2)- ϕ é auto dual se ϕ é auto dual fracamente e tem dimensão k = n/2(n deve ser par).

Exemplo 3.2.1 - Seja n= 4, k = 2 e ϕ = {0000,0101,1010,1111} podemos verificar facilmente, que ϕ é auto dual.

Teorema 1. - Se ϕ é um código auto dual com a matriz geratriz (I/A), então ϕ também tem $(-A^t/I)$ como uma matriz geratriz.

Prova. - Qualquer matriz geratriz de verificação do código auto dual ϕ é uma matriz geratriz de $\phi^{\perp} = \phi$.

Na seguinte proposição determinaremos sob quais condições $\phi^{\perp} \subset \phi$

Proposição 1. - Se n é par e ϕ é um código linear binário [n,n-1] de peso par, então $\phi^{\perp} \subset \phi$

Prova. - Se ϕ= [n,n-1] então $\phi^{\perp}$= [n,1] que é o código repetitivo, possuindo apenas as palavras código 0 0 0 . . . 0 e 1 1 1 . . . 1 1 1 de comprimento n.

Provemos então, que estas duas palavras código pertencem a ϕ.

(i) o vetor nulo pertence a ϕ porque ϕ é linear.

(ii) Seja G a matriz geratriz de ϕ, na forma $G = [I_{n-1}/-A^t]$, isto é,

$$G = \left|\begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \ldots \ldots \ldots 0\ 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \ldots \ldots \ldots 0\ 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \ldots \ldots \ldots 0\ 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \ldots \ldots \ldots 0\ 1 \\ & & & \vdots & & \\ & & & \vdots & & \\ & & & \vdots & & \\ 0 & 0 & 0 & 0 & 0 & 0 \ldots \ldots \ldots 1\ 1 \end{array}\right|$$

A palavra código formada pela soma de todas as linhas da matriz G, é exatamente o vetor código cujas componentes são todas iguais a 1. Logo, $\phi^{\perp} \subset \phi$

Exemplo 3.2.1 - Seja $\phi = [4,3]$, então $\phi^{\perp} = [4,1]$ e a matriz geratriz de ϕ é,

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

cujas palavras código são:

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

O seu dual $\phi^{\perp} = [4,1]$ possue a seguinte matriz geratriz $G = [\ 1\ 1\ 1\ 1\ ]$, cujas palavras código são:

0 0 0 0
1 1 1 1

Portanto, $\phi^{\perp} \subset \phi$

Exemplo 3.2.2 - Seja $\phi = [3,2]$ com n ímpar, temos $\phi^{\perp} = [3,1]$ onde a matriz geratriz de ϕ é,

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

cujas palavras código são:

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

o seu dual $\phi^{\perp} = [3,1]$ possue a matriz geratriz $G' = [1\ 1\ 1]$, cujas palavras código são:

0 0 0
1 1 1

Observemos que a palavra código 1 1 1 $\notin \phi$. Portanto, $\phi^{\perp} \subset \phi$.

Observação: - Nesta secção provamos que, se n é par e ϕ é um código [n,n-1] binário, então o dual de ϕ está contido em ϕ.

Seria interessante determinar se em outros códigos, este fato acontece, e quais são os códigos. Estamos estudando este fato para outros códigos.

3. Código de Ordem $r+(r+1)_{m,s}$. [02],[04]

Sabemos que os códigos de Reed-Muller de ordem r são formados usando os vetores básicos $v_0, v_1, \ldots, v_m$ e todos os vetores produto destes vetores tomando r ou menos, ao mesmo tempo, onde $v_1, v_2, \ldots, v_m$ são as linhas de uma matriz geratriz que tem todas as m-uplas possíveis como colunas e v_0 tendo todos os componentes como sendo 1.

Estudaremos agora os códigos de ordem $r+(r+1)_{m,s}$ que são formados usando os vetores básicos $v_0, v_1, \ldots, v_m$ juntamente com alguns vetores produto r+1 vetores ao mesmo tempo. Estes códigos podem ser usados nos sistemas com problemas de armazenagem.

Definição 3.3.1 - Um código é dito de ordem $r+(r+1)_{m,s}$ se é formado pelos vetores básicos $v_0, v_1, \ldots, v_m$ e todos os vetores produto destes vetores tomando r ou menos, ao mesmo tempo, juntamente com alguns s vetores produto ($1 \leq s < \binom{m}{r+1}$) de r+1 vetores.

Notação. - Um código de ordem $r+(r+1)_{m,s}$ é denotado por R(r,m,s).

Se G(r,m) denota a matriz para um código RM de ordem r, então a matriz geratriz do código R(r,m,s) pode ser escrita como:

$$G(r+(r+1)_{m,s},m) = \begin{vmatrix} G(r,m) \\ X \end{vmatrix}$$

onde X é uma matriz contendo alguns s vetores produtos de $v_1, v_2, \ldots v_m$ tomando r+1, ao mesmo tempo.

Exemplo 3.3.1 - Para m = 3, r=2 a matriz geratriz do código RM de segunda ordem pode ser escrita como:

$$G(2,3) = \begin{vmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_1v_2 \\ v_1v_3 \\ v_2v_3 \end{vmatrix} = \begin{vmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&1&0&1 \\ 0&0&0&1&0&0&0&1 \end{vmatrix}$$

As matrizes geratrizes dos códigos de ordem $1+(2)_{3,1}$ podem ser tomados como quaisquer das seguintes:

a) $G(1+(2)_{3,1},3) = \begin{vmatrix} G(1,3) \\ v_1v_2 \end{vmatrix} = \begin{vmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&1&1 \end{vmatrix}$

b) $G(1+(2)_{3,1},3) = \begin{vmatrix} G(1,3) \\ v_1v_3 \end{vmatrix} = \begin{vmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&1&0&1 \end{vmatrix}$

c) $G(1+(2)_{3,1},3) = \begin{vmatrix} G(1,3) \\ v_2v_3 \end{vmatrix} = \begin{vmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&0&1&0&0&0&1 \end{vmatrix}$

As matrizes geratrizes dos códigos de ordem $1+(2)_{3,2}$ podem ser quaisquer das seguintes:

d) $G(1+(2)_{3,2},3) = \begin{vmatrix} G(1,3) \\ v_1v_2 \\ v_1v_3 \end{vmatrix} = \begin{vmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&1&0&1 \end{vmatrix}$

$$e)\quad G(1+(2)_{3,2},3) = \begin{vmatrix} G(1,3) \\ v_1v_2 \\ v_2v_3 \end{vmatrix} = \begin{vmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&1&0&0&0&1 \end{vmatrix}$$

$$f)\quad G(1+(2)_{3,2},3) = \begin{vmatrix} G(1,3) \\ v_1v_3 \\ v_2v_3 \end{vmatrix} = \begin{vmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&1&0&1 \\ 0&0&0&1&0&0&0&1 \end{vmatrix}$$

Exemplo 3.3.2 - Para m=4, r=1 uma matriz geratriz para um código de ordem $1+(2)_{4,1}$ pode ser tomada como:

$$G(1+(2)_{4,1},3) = \begin{vmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ X \end{vmatrix}$$

onde X é algum dos vetores v_1v_2, v_1v_3, v_1v_4, v_2v_3, v_2v_4, v_3v_4.

Como já vimos no capítulo II, ítem 4, que o produto entre dois códigos de Reed-Muller R(1,2)R(1,3) não é um código de Reed-Muller, mostraremos agora que R(1,2)R(1,3) é um código do tipo R(1,5,6).

$$G(2,5) = \begin{vmatrix} v_5 \\ v_4 \\ v_3 \\ v_2 \\ v_1 \\ v_0 \\ v_1v_2 \\ v_1v_3 \\ v_1v_4 \\ v_1v_5 \\ v_2v_3 \\ v_2v_4 \\ v_2v_5 \\ v_3v_4 \\ v_3v_5 \\ v_4v_5 \end{vmatrix} = \begin{vmatrix} 00000000000000001111111111111111 \\ 00000000111111110000000011111111 \\ 00001111000011110000111100001111 \\ 00110011001100110011001100110011 \\ 01010101010101010101010101010101 \\ 11111111111111111111111111111111 \\ 00010001000100010001000100010001 \\ 00000101000001010000010100000101 \\ 00000000010101010000000001010101 \\ 00000000000000000101010101010101 \\ 00000011000000110000001100000011 \\ 00000000001100110000000000110011 \\ 00000000000000000011001100110011 \\ 00000000000011110000000000001111 \\ 00000000000000000000111100001111 \\ 00000000000000000000000011111111 \end{vmatrix}$$

Para m=5 e r = 1 temos que uma matriz geratriz para um código de ordem $1+(2)_{5,6}$ pode ser tomada como:

$$G(1+(2)_{5,6},5) = \begin{vmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ X \end{vmatrix}$$

onde X é uma das possíveis combinações de 6 vetores dos v_1v_2, v_1v_3, v_1v_4, v_1v_5, v_2v_3, v_2v_4, v_2v_5, v_3v_4, v_3v_5, v_4v_5. Por exemplo:

$$G(1+(2)_{5,6},5) = \begin{vmatrix} v_5 \\ v_4 \\ v_3 \\ v_2 \\ v_1 \\ v_0 \\ v_3v_5 \\ v_2v_5 \\ v_1v_5 \\ v_3v_4 \\ v_2v_4 \\ v_1v_4 \end{vmatrix} = \begin{vmatrix} 00000000000000001111111111111111 \\ 00000000111111110000000011111111 \\ 00001111000011110000111100001111 \\ 00110011001100110011001100110011 \\ 01010101010101010101010101010101 \\ 11111111111111111111111111111111 \\ 00000000000000000000111100001111 \\ 00000000000000000011001100110011 \\ 00000000000000000101010101010101 \\ 00000000000011110000000000001111 \\ 00000000001100110000000000110011 \\ 00000000010101010000000001010101 \end{vmatrix}$$

que é a matriz geratriz do código R(1,2)R(1,3). Portanto, R(1,2)R(1,3) é um código de ordem $r+(r+1)_{m,s}$, isto é, um R(1,5,6) código.

Teorema 1. - Para $0 < r_1 \leq m_1$ e $0 < r_2 \leq m_2$ o código produto $R(r_1,m_1)R(r_2,m_2)$ é um código de ordem $r+(r+1)_{m,s}$ para $R(r_1,m_1)R(r_2,m_2) \neq R(r_1+r_2,m_1+m_2)$.

Prova. O teorema 4 do capítulo II, nos diz que: para $0 < r_1 \leq m_1$ e $0 < r_2 \leq m_2$ o código produto $R(r_1,m_1)R(r_2,m_2)$ é um subcódigo de $R(r_1+r_2,m_1+m_2)$. Então, se temos a matriz geratriz $G(r_1+r_2,m_1+m_2)$, que é a matriz geratriz do código $R(r_1+r_2,m_1+m_2)$, e como as matrizes geratrizes para um código de ordem $r+(r+1)_{m,s}$ serão sempre submatrizes da matriz $G(r_1+r_2,m_1+m_2)$, pois $s \leq \binom{m}{r+1}$, e podemos pegar qualquer uma delas para formar um código de ordem $r+(r+1)_{m,s}$, resulta que, alguma destas matrizes será a matriz geratriz de $R(r_1,m_1)R(r_2,m_2)$.

Peso Mínimo de um Código R(r,m,s). [04]

Teorema 2. O peso mínimo de um código R(r,m,s), é $2^{m-(r+1)}$ que é o peso mínimo do código R(r+1,m).

Prova.- Se G(r,m) denota a matriz geratriz do código R(r,m), então a matriz geratriz do código R(r,m,s) poderá ser escrita como:

$$G(r+(r+1)_{m,s},m) = \begin{vmatrix} G(r,m) \\ X \end{vmatrix}$$

onde X é uma matriz contendo s vetores produtos $v_1,v_2,\ldots,v_m$, tomados r+1, ao mesmo tempo.

Se v é um vetor de R(r,m,s), então os seguintes casos são possíveis:

caso (i) - Se v é uma combinação linear envolvendo algumas linhas de G(r,m), então $wt(v) \geq \text{mín } wtR(r,m) = 2^{m-r}$;

caso (ii) - Se v é uma combinação linear envolvendo algumas linhas de X, então v é um elemento de R(r+1,m). Assim,

$$wt(v) \geq \text{mín}wtR(r+1,m) = 2^{m-(r+1)}.$$

Nós sabemos que cada $v_1,v_2,\ldots,v_m$ é de peso 2^{m-1}. por indução sobre r, pode ser mostrado que o peso de algum produto $v_1,v_2,\ldots,v_m$ tomando r, ao mesmo tempo, é 2^{m-r}. Assim, se v é uma das linhas de X, então wt(v) é $2^{m-(r+1)}$.

Assim, nós temos visto que o código R(r,m,s) contém palavras código, a saber, as linhas de X tendo peso $2^{m-(r+1)}$. Igualmente, qualquer outra palavra código é de peso maior ou igual que $2^{m-(r+1)}$. Portanto, o peso mínimo do código R(r,m,s) é $2^{m-(r+1)}$.

4. Dual do R(r,m,s). [04]

Teorema 3.- Para todo r, m e s ($0 \leq r \leq (m-2)$ e $1 \leq s < \binom{m}{r+1}$) o dual de R(r,m,s) é R(m-r-2,m,s'), onde $s' = \binom{m}{m-r-1} - s$.

Prova. - Se $\left|\begin{array}{c} G(r,m) \\ \hline X_1 \end{array}\right|$ é a matriz geratriz de R(r,m,s) e se $u_1, u_2, \ldots, u_s$, são as linhas de X_1, onde cada u_j é um produto de $v_1, v_2, \ldots, v_m$ tomados r+1, ao mesmo tempo.

Suponha $u_j = v_{j1} \cdot v_{j2} \ldots v_{jr+1}$ $(1 \leq j \leq s$ e $j \in \{1,2,\ldots,m\})$. Para cada u_j um vetor u_j' é definido como segue:

$u_j' = v_{p_1} \cdot v_{p_2} \ldots v_{p_{m-(r+1)}}$, onde

$$\{p_1, p_2, \ldots, p_{m-(r+1)}\} = \{1,2,\ldots,m\} - \{j_1, j_2, \ldots, j_{r+1}\}.$$

O produto de u_j e $u_j' \neq 0 \pmod 2$, porque, é conhecido que o vetor produto $v_1 \cdot v_2 \ldots v_m$ é de peso 1 de Hamming.

Suponha que X_2 é a matriz cujas linhas são os vetores obtidos tomando os produto de $v_1, v_2, \ldots, v_m$ tomados m-r-1, ao mesmo tempo, excluidos os vetores u_j', $j = 1,2,\ldots,s$.

Considere a Matriz

$$H = \left|\begin{array}{c} G((m-r-2),m) \\ \hline X_2 \end{array}\right|$$

Suponha que B é o código gerado por H. Claramente B é um código R(m-r-2,m,s'), onde $s' = \binom{m}{m-r-1} - s$. Seja $a \in R(r,m,s)$ e $b \in B$. Existem três possíveis casos, que são:

caso (i) - Suponha que o vetor $\underline{a}$ é uma combinação linear das linhas de G(r,m), isto é, $\underline{a} \in R(r,m)$. Sabemos que cada palavra código $a \in R(r,m)$ vem de um polinômio $a(v_1, v_2, \ldots, v_m)$ de grau no máximo r. Similarmente, $b(v_1, v_2, \ldots, v_m)$ é um polinômio de grau $\leq r+(m-r-1) = m-1$.

Portanto, $\underline{a}.\underline{b} \in R(m-1,m)$ e, como tal, é de peso par. Então o produto de $\underline{a}$ e $\underline{b}$ é igual a 0 (mod2):

caso(ii) - Suponha que $\underline{a}$ é qualquer palavra código de R(r,m,s) e $\underline{b}$ é uma combinação linear das linhas de G(m-r-2,m). Então, $b(v_1,v_2,\ldots,v_m)$ é um polinômio de grau $\leq$ m-r-2, $a(v_1,v_2,\ldots,v_m)$ de grau $\leq$ r+1 e seus produtos é um polinômio de grau $\leq$ (r+1) + (m-r-2,m) = m-1.

Assim, $\underline{a}.\underline{b} \in R(m-1,m)$ e como tal, é de peso par. Portanto, o produto de $\underline{a}$ e $\underline{b}$ é igual a 0 (mod2);

caso(iii) - Suponha que $\underline{a}$ é uma combinação linear das linhas de X_1 e $\underline{b}$ é uma combinação linear das linhas de X_2. Como nos dois casos previstos, pode ser mostrado que o produto de $\underline{a}$ e $\underline{b}$ é igual a 0 (mod2).

Assim, teremos mostrado que o código B está contido em $R(r,m,s)^{\perp}$. Mas,

$$\dim B+\dim R(r,m,s) = [1+\binom{m}{1}+\ldots+\binom{m}{m-r-2}+s]+[1+\binom{m}{1}+\ldots+\binom{m}{r}+s] = 2^m.$$

Logo, $R(r,m,s)^{\perp} = B = R(m-r-2,m,s')$.

EXemplo 3.4.1 - Seja R(1,4,1), o seu dual será o código R(1,4,5).

CONCLUSÃO

O problema de transmissão confiável de informação tem representado um desafio constante para os pesquisadores em comunicações. Frequentemente, no contexto das comunicações digitais, ocorrem problemas de detecção e/ou correção de possíveis erros que tenham ocorrido durante uma transmissão. O objetivo da teoria da codificação é encontrar códigos longos e eficientes procurando métodos práticos de codificação e decodificação eficientes.

Nesta Tese estudamos os códigos de Reed-Muller, códigos produto e generalização do código de Reed-Muller. Os códigos de Reed-Muller são fáceis de decodificar, e os códigos produtos são os mais poderosos. Os códigos generalizados podem tornar-se úteis porque são lineares, e ocupam menas memória.

Os desenvolvimentos recentes na tecnologia do hardware digital tornaram possível o uso de esquemas de codificação bastante complexos, e a medida que processadores mais complexos tornam-se disponíveis, graças a tecnologia da microeletrônica, a vantagem do uso dos códigos tornam-se ainda maiores.

BIBLIOGRAFIA

01 - BERLEKAMP, E.R. Algebraic Coding Theory. McGraw-Hill.NY.1968.

02 - DASS, B.K and MUTTO, S.K. A Note on Reed-Muller Codes.Discrete Appl.Maths. 2(1980), 345-348.

03 - DASS, B.K and SHARMA, B.D. Adjacent Error Correcting Perfect Codes. J.Cybernetics.1977.Vol 7, 9-13.

04 - DASS, B.K.and WASAN,S.K. On Codes of Order $r+(r+1)_{m,s}$. International J. Eletr.,54, nº 3,471-473.1983.

05 - HAMMING,R.W. Error Detecting and Error Correting Codes. Bell System Tec. Journal, 29,147-160. 1950.

06 - LIN, S. An Introdution to Error Correcting Codes. Prentice Hall. N.Y. 1970.

07 - LINT, J.H.Van, Coding Theory.Lecture Notes in Math. Springer Verlag. N.Y. 1970.

08 - NOMURA, T.,KAWA, H., IMAI, H. and FUKUDA, A. A Theory of two Dimensional Linear Recurring Arrays. IEEE-Trans Audio Inf. Theory Vol 18, nº 06, 775-785.1972.

09 - PETERSON, W.W. and WELDON, E.J. Error Correcting Codes. 2nd Edition. MIT Press. 1972.

10 - SPIEGEL,E. and WASAN, S.K. On a Product of Reed-Muller Codes. Journal of Inf. and Optimization Sciences. vol 3, nº 03. 1982.

11 - SLOANE, N.J.A. and MACWILLIAMS, F.J. The Theory of Error Correcting Codes. North Holland. 1977.