

UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELETRICA
DEPARTAMENTO DE TELEMÁTICA

CÓDIGOS CORRETORES DE ERROS E ALGORITMOS DE
DECODIFICAÇÃO PARA O CANAL ADITIVO T-USUÁRIOS
DE MÚLTIPLO ACESSO

Por: João Bosco Batista ^{autor} Lacerda

Comissão Julgadora:

- Prof. Dr. Walter da Cunha Borelli - DT/FEE/UNICAMP/CAMPINAS - SP
- Prof. Dr. Trajano Pires da Nóbrega Neto - DM/UNESP/SJRP-SP
- Prof. Dr. Noraf Romeu Rocco - DM/UNB/BRASÍLIA - DF
- Prof. Dr. Renato Baldini Filho - DECOM/FEE/UNICAMP/CAMPINAS - SP
- Prof. Dr. Jaime Portugheis - DECOM/FEE/UNICAMP/CAMPINAS - SP

SUPLENTE:

- Prof. Dr. Lee Luan Ling - DECOM/FEE/UNICAMP/CAMPINAS - SP
- Prof. Dr. Ivanil Sebastião Bonatti - DT/FEE/UNICAMP/CAMPINAS - SP

Tese apresentada à Faculdade de Engenharia
Elétrica da Universidade Estadual de Campinas,
como parte dos requisitos exigidos para a
obtenção do título de Doutor em Engenharia
Elétrica.

Final da tese
para Comissão
Maio/1994

BIBLIOTECA DA ÁREA DE ENGENHARIA
UNICAMP

BIBLIOTECA CENTRAL

Comissão Julgadora em 27 de Maio de 1994
Lacerda
@fredell orientador

Agradecimentos

Ao prof. Dr. Walter da Cunha Borelli pela orientação e apoio no desenvolvimento do meu doutorado;

À CAPES/PICD pela bolsa de estudo;

À UFPb e, em particular, ao Departamento de Ciências Exatas e da Natureza - CFP/Campus V pelos afastamentos concedidos que permitiram a realização deste trabalho;

Ao prof. Dr. Trajano Pires da Nóbrega Neto - DM/UNESP/SJRP pelas sugestões feitas nas demonstrações apresentadas no apêndice deste trabalho;

Ao Departamento de Telemática pela utilização de seu laboratório e facilidades computacionais;

Finalmente gostaria de deixar os meus agradecimentos para todos aqueles que de uma forma ou de outra contribuíram para a realização do meu doutorado, em particular ao meu amigo Leonardo e aos funcionários Elza Aoki, Airton Ramos e Ana Flavia da Silva.

Resumo

O sistema de comunicação múltiplo acesso considerado neste trabalho é o sistema T - usuários onde T fontes estatisticamente independentes transmitem símbolos binários para T destinatários através de um mesmo canal aditivo sem memória. Os primeiros estudos para a obtenção de códigos para este tipo de sistema de comunicação foram no sentido de maximizar o número de palavras códigos de um dado comprimento para o caso particular de dois usuários independentes. Chang e Weldon [1] apresentaram uma outra abordagem no sentido de obter uma classe de códigos univocamente decodificável para o caso T - usuários, $T > 2$.

John H. Wilson [3] generalizou os códigos de Chang e Weldon e apresentou uma classe de códigos corretores de erros para o canal T - usuários.

Neste trabalho apresentamos uma classe de códigos corretores de erros para o sistema T - usuários, $T > 2$, que é obtida a partir de códigos 2 - usuários δ - decodificáveis. Também generalizamos estes novos códigos via a noção de classes de equivalência, segundo Thomas J. Ferguson [2].

Novas técnicas de decodificação baseada no table look-up, numa adaptação para os novos códigos do algoritmo de Wilson e numa combinação destas duas técnicas de decodificação são apresentadas. Resultados de simulações para o canal discreto sem memória (DMC) e para o canal AWGN T - usuários são mostrados.

Curvas de desempenhos comparando os vários esquemas de decodificação propostos e os esquemas de decodificação por decisão suave (S/D) e por decisão abrupta (H/D) também são mostradas.

*À memória do meu avô
José Batista de Araújo*

Aos meus pais Luiz Lacerda e
Maria José Batista Lacerda,
pela minha educação e a
Divina Maria da Cruz,
companheira que nos momentos
mais difíceis sempre me
incentivou à continuidade
deste trabalho.

Glossário

BAC	Canal Aditivo Binário
MAC	Canal Múltiplo Acesso
DMC	Canal Discreto sem Memória
AWGN	Canal Aditivo Gaussiano com Ruído Branco
QSBAC	Canal Aditivo Binário sem Ruído Quase Sincronizado
QSUD	Código Univocamente Decodificável Quase Sincronizado
NBSOFT	Número de bits de confiança
GF(2)	Corpo finito com dois elementos
GL(N,2)	Conjunto das matrizes não singulares sobre GF(2)
SNR	Relação sinal/ruído
S/D	Decisão suave
H/D	Decisão abrupta
T	Número de usuários do canal T - usuários
N	Comprimento das palavras-código
\otimes	Produto de Kronecker
+	Soma real
-	Subtração real
\equiv	Congruência módulo 2
{ 0, 1 }	Conjunto de símbolos na entrada do canal 2 - usuários
{ 0, 1, ..., T }	Conjunto de símbolos na entrada do canal T - usuários
{ 0, 1, -1 } ^T	Conjunto de todas as r-uplas sobre { 0, 1, -1 }
z _i - z' _i	Valor absoluto de z _i - z' _i
[x]	Maior inteiro menor ou igual a x
$\binom{T}{i}$	Número binomial
D	Matriz diferença
D ₀	Matriz diferença do código dois usuários
N ₀	Comprimento do código dois usuários
d _i	i - ésima linha de D
H _q	Matriz de Hadamard de ordem q
I _{j-1}	Matriz identidade de ordem 2 ^{j-1}
O _{j-1}	Matriz nula de ordem 2 ^{j-1}
P, Q	Matrizes de permutações generalizadas
[·] ^t	Matriz transposta
C	Código T - usuários
(C ₁ , C ₂ , ..., C _T)	Código T - usuários
C _i	i - ésimo código constituinte

$ C_1 , M_1$	Cardinalidade de C_1
X_1, Y_1	Palavras-códigos de C_1
R_1	Taxa de C_1
(R_1, R_2)	Par de taxas dos códigos constituintes do código dois usuários
$R(T)$	Taxa do código T - usuários
$C(T)$	Capacidade do canal T - usuários
Z	Vetor transmitido
z_i	i - ésima coordenada de Z
U	Vetor recebido
E	Vetor erro
e_i	i - ésima coordenada de E
$e(Z,U)$	Quantidade de erros de transmissão
S	Síndrome
λ	Vetor binário de comprimento T
$d_L(a, b)$	L - distância entre as palavras-códigos a e b
d_{\min}	L - distância mínima de um código T - usuários
δ	L - distância mínima de um código dois usuários δ -deco- dificável
$\ a - b\ $	Norma de $a - b$
Y_{AWGN}	Vetor na saída do canal AWGN
Y_Q	Vetor quantizado
y_{q_j}	j - ésima coordenada de Y_Q
P_e	Probabilidade de erro por palavra código

Índice

1. Introdução	1
2. Sistemas de Comunicação de Usuários Múltiplos	3
2.1. Introdução	3
2.2. O Canal Aditivo Binário Dois Usuários sem Ruído	4
2.3. O Canal Aditivo Binário Dois Usuários com Ruído	8
2.4. O Canal Aditivo T - Usuários	10
2.4.1. A Capacidade do Canal Aditivo T - Usuários	11
2.5. Conclusão	18
3. Códigos e Algoritmos de Decodificação para o Canal Aditivo T - Usuários	19
3.1. Introdução	19
3.2. Os Códigos de Chang e Weldon	19
3.3. Generalização dos Códigos de Chang e Weldon	33
3.4. Os Códigos de Wilson	36
3.5. Algoritmos de Decodificação	40
3.5.1. Algoritmo de Decodificação de Chang e Weldon	40
3.5.2. Algoritmo de Decodificação de Wilson	46
3.6. Conclusão	49
4. Uma Classe de Códigos Corretores de Erro para o Canal Aditivo T - Usuários	50
4.1. Introdução	50
4.2. A Classe de Códigos	50
4.3. Generalização da Classe de Códigos do Corolário	
4.1 via a Noção de Classes de Equivalência	56
4.4. Conclusão	60

5. Algoritmos de Decodificação e Resultados de Simulações	61
5.1. Introdução	61
5.2. Algoritmos de Decodificação	61
5.2.1. Técnica de Decodificação Baseada no Table Look-up	61
5.2.2. Algoritmo de Wilson Adaptado para os Novos Códigos	65
5.2.3. Técnica de Decodificação Combinada	71
5.2.4. Técnicas de Decodificação por Decisão Suave e Abrupta	71
5.3. Desempenho dos Novos Códigos	72
5.3.1. Simulação para o Canal Discreto sem Memória	72
5.3.2. Simulação para o Canal AWGN T - Usuários	75
5.4. Comparação entre Esquemas de Decodificações	78
5.4.1. Table Look-up versus o Algoritmo de Wilson	78
5.4.2. Table Look-up versus o Algoritmo de Wilson Adaptado para os Novos Códigos	79
5.4.3. Técnica de Decodificação Combinada versus o Algoritmo de Wilson	81
5.4.4. Técnica de Decodificação Combinada versus o Algoritmo de Wilson Adaptado para os Novos Códigos	82
5.4.5. Table Look-up versus Técnica de Decodificação Combinada	84
5.4.6. Comparações entre os Esquemas de Decodificação por Decisão Suave e por Decisão Abrupta	87
5.5. Conclusão	92
6. Conclusões Finais	93
Apêndice	97
Referências	106

Capítulo I

Introdução

As primeiras abordagens para a obtenção de códigos para o Canal Aditivo Binário T - Usuários de Múltiplo Acesso foram no sentido de maximizar o número de palavras códigos de um dado comprimento para o caso particular de dois usuários independentes. Neste trabalho apresentamos uma classe de códigos corretores de erros para o canal T - Usuários, $T > 2$, dando continuidade aos estudos feitos por Chang e Weldon [1], Ferguson [2] e Wilson [3].

No capítulo 2 apresentamos o sistema de comunicação T - Usuários. Em particular tratamos dos canais aditivos binários dois usuários com e sem ruído e enfocamos os esquemas de codificações existentes na literatura para este tipo de sistema de comunicação. Particular ênfase é dada à demonstração da expressão algébrica para a capacidade do canal aditivo binário T - Usuários.

No capítulo 3 são descritas as técnicas de codificação propostas por Chang e Weldon, Ferguson e Wilson bem como algumas técnicas conhecidas de decodificação para estas classes de códigos. Na secção 3.2 mostramos a classe de códigos univocamente decodificável apresentada por Chang e Weldon [1]. Na secção 3.3 enfocamos a generalização dada por Ferguson [2] para a classe de códigos de Chang e Weldon. Na secção 3.4 apresentamos a classe de códigos corretores de erros proposta por Wilson [3]. Na secção 3.5 descrevemos os algoritmo de decodificação para as classe de códigos apresentadas por Chang e Weldon e Wilson.

No capítulo 4 apresentamos uma classe de códigos corretores de erros para o canal T-usuários [28, 29] obtida a partir de códigos dois usuários δ -decodificáveis e generalizamos esta classe de códigos via a noção de classe de equivalência.

No capítulo 5 são propostas algumas técnicas de decodificação para os códigos T - usuários bem como resultados de simulações para o Canal Discreto sem Memória e para o Canal AWGN. Estes resultados são

apresentados em forma de curvas de desempenho da probabilidade de erro versus a relação sinal/ruído (P_e x SNR). As curvas de desempenho são usadas na comparação das técnicas de decodificação propostas para diversos códigos T - usuários.

O capítulo 6 apresenta as considerações finais sobre todo o trabalho.

Capítulo II

Sistemas de Comunicações de Usuários Múltiplos

2.1 Introdução

Neste capítulo descrevemos os tipos de sistemas de comunicações T - Usuários; em particular tratamos dos sistemas de comunicações 2 - Usuários. Outros sistemas de comunicações de acesso múltiplo o leitor poderá encontrar em P. G. Farrell [5], Shin - Chun Chang e Jack K. Wolf [6], Laszlo Gyorfí e István Kerekes [22], Edward C. VAN DER Meulen [30], Imre Csísfár e János Körner [31], Thomas M. Cover e Abbas A. El Gamal [32], Boris S. Tsybakov [33] e Robert G. Gallager [34].

Na seção 2.2 tratamos do canal aditivo binário 2 - usuários sem ruído e apresentamos algumas classes de códigos univocamente decodificáveis para este tipo de sistema. Na seção 2.3 apresentamos o canal aditivo binário dois usuários com ruído e algumas classes de códigos para este tipo de canal denominados de códigos dois usuários δ - decodificáveis. Finalmente na seção 2.4 consideramos o canal T - Usuários e desenvolvemos a expressão algébrica que determina a capacidade do canal T - Usuários para o sistema sem ruído.

O canal de múltiplo acesso (MAC), fig. 2.1 tem duas ou mais entradas e uma saída. As entradas, suas fontes associadas e codificadores podem ter diferentes alocações físicas. Durante a transmissão sobre o canal, os dois ou mais sinais são superpostos ou combinados em um mesmo caminho. O trabalho do decodificador é decifrar e liberar as mensagens para seus destinos correspondentes, se possível sem erros. As fontes são assumidas serem estatisticamente independentes e o canal sem memória.

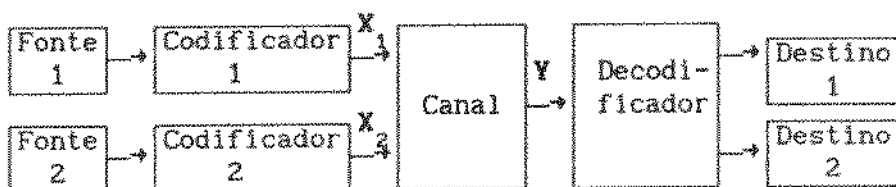


Fig. 2.1. Canal Múltiplo Acesso 2-usuários

2.2 O Canal Aditivo Binário 2 - Usuários sem Ruído

Para este particular MAC os valores dos símbolos na saída do canal é a soma aritmética dos valores dos símbolos na entrada, na ausência de ruído. No caso 2-usuários, se os símbolos na entrada são $\{0, 1\}$, então os símbolos na saída são $\{0, 1, 2\}$, como na figura 2.2, onde as linhas flechadas representam a probabilidade condicional $P(Y/X_1, X_2)$.

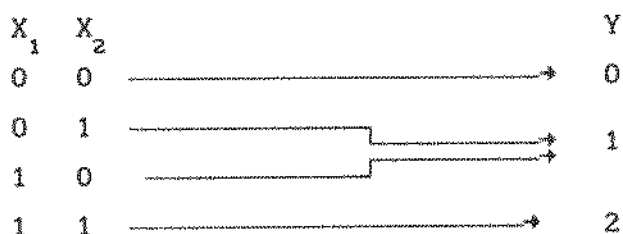


Fig. 2.2. Canal Aditivo Binário sem Ruído

O canal aditivo binário sem ruído é também conhecido como canal múltiplo acesso binário apagador porque o símbolo 1 na saída não pode ser decodificado sem ambiguidade mesmo no caso da ausência de ruído, pois o símbolo 1 pode ter sido produzido por $x_1 = 1$ e $x_2 = 0$ ou $x_1 = 0$ e $x_2 = 1$.

O problema da codificação para este modelo de canal é construir pares de códigos (C_1, C_2) tais que,

1) O decodificador seja capaz de decodificar os vetores binários transmitidos pelos usuários 1 e 2.

2) O par de taxas (R_1, R_2) seja um ponto que insida sobre a região de capacidade do canal e esteja, se possível, próximo da fronteira.

Um par de códigos que satisfaça a primeira propriedade é dito ser univocamente decodificável.

É claro que um código dois usuários (C_1, C_2) é univocamente decodificável se e somente se para quaisquer dois pares distintos de palavras códigos (c_1, c_2) , (c'_1, c'_2) pertencentes a (C_1, C_2) tenhamos,

$$c_1 + c_2 \neq c'_1 + c'_2$$

A região de capacidade para este tipo de canal é mostrada na figura 2.3, [5].

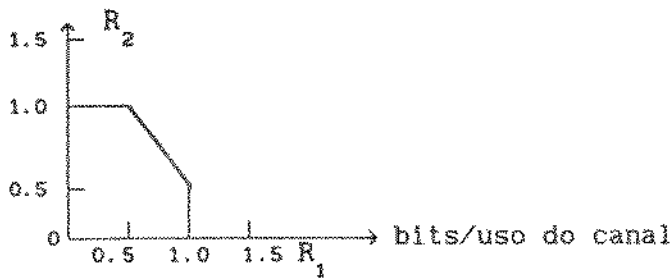


Fig. 2.3. Capacidade do MAC Aditivo Binário

Kasami e Lin, [7], 1976 apresentam um esquema muito simples de códigos de blocos de comprimento 2 univocamente decodificável para o caso 2 - usuários, supondo que os dois usuários operem com sincronismo de símbolos e blocos. Para este esquema o usuário 1 tem como palavras-código { 00, 11 } e o usuário 2 as palavras-código { 00, 01, 10 }, como mostrado na tabela 2.1.

Tabela 2.1

	C_1	0 0	1 1
	C_2		
0 0		0 0	1 1
0 1		0 1	1 2
1 0		1 0	2 1

Desde que todas as palavras recebidas são distintas, o decodificador pode decodificar as duas mensagens sem ambiguidade. As taxas dos códigos C_1 e C_2 são, respectivamente, $R_1 = (\log_2 |C_1|)/N$ e $R_2 = (\log_2 |C_2|)/N$, onde $|C_1|$ e $|C_2|$ são, respectivamente, as cardinalidades dos códigos C_1 e C_2 e N é o comprimento de ambos os códigos. O par de taxas realizável para este esquema é $(R_1, R_2) = (0.5, 0.792)$ e a soma de taxa total é $R = R_1 + R_2 = 1.292$.

Este esquema simples de codificação pode ser estendido [7,15] para códigos de blocos de comprimento N da seguinte maneira. Seja V_N o espaço vetorial de todas as N -uplas sobre $GF(2)$ e seja C_1 o código formado pelas duas N -uplas 000...0 e 111...1. Então C_2 é formado pela N -upla 000...0 e todas as outras N -uplas do espaço vetorial V_N , exceto a N -upla 111...1. Desta forma o par de códigos (C_1, C_2) é um código dois

usuários univocamente decodificável e o par de taxas realizável para este esquema é $(R_1, R_2) = (1/N, (\log_2(2^N - 1)/N))$.

Por exemplo, para $N = 3$, $C_1 = \{000, 111\}$ e $C_2 = \{000, 001, 010, 011, 100, 101, 110\}$. A tabela de decodificação para este código é,

Tabela 2.2

C_2	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0
C_1							
0 0 0	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0
1 1 1	1 1 1	1 1 2	1 2 1	1 2 2	2 1 1	2 1 2	2 2 1

Uma outra classe de códigos dois usuários univocamente decodificáveis é descrita por Kasami e Lin, [7], da seguinte maneira: seja C_1 um código linear (N, K) que contém o vetor $(111\dots 1)$ e seja S um coset de C_1 tal que $S \neq C_1$. Seja v o líder do coset S e v' o complemento de v . Incluímos v e v' em C_2 . Procedendo desta maneira para os demais cosets e desde que existem $2^{N-K} - 1$ cosets de C_1 que não são iguais a C_1 , podemos escolher $2^{N-K+1} - 2$ vetores e incluí-los em C_2 . Também podemos escolher a N -upla $(000 \dots 0)$ de C_1 e incluí-la em C_2 . Desta forma C_2 contém $2^{N-K+1} - 1$ vetores. O par de códigos (C_1, C_2) assim obtido é univocamente decodificável, [15].

Por exemplo, para $N = 4$ o par de códigos (C_1, C_2) é mostrado na tabela 2.3.

Tabela 2.3

C_1	0000	0011	1100	1111
C_2	0000			
	0001			1110
	0100			1011
	1010			0101

As taxas para estes códigos são $R_1 = 0.5$ e $R_2 = (\log_2 7)/4 = 0,702$ e a taxa soma é $R = 1.202$.

Em um sistema de comunicação de múltiplo acesso, o sincronismo entre os codificadores e entre os decodificadores e o decodificador afeta o desempenho dos códigos. Um canal aditivo binário (BAC) dois usuários é dito ser sincronizado [14] se os sincronismos de bits e de blocos são

mantidos entre os codificadores e o decodificador; caso contrário, é dito sem sincronismo.

Um caso particular deste sistema, [14], é obtido quando os codificadores não mantêm sincronismo de blocos, embora o decodificador mantenha sincronismo de bloco com cada codificador. É assumido que sincronismo de bits é mantido entre os codificadores e entre os codificadores e o decodificador. Neste caso o canal é chamado Canal Aditivo Binário sem ruído quase sincronizado, QSBAC.

Uma classe de códigos univocamente decodificáveis não homogêneos para o QSBAC é apresentada em [9]. Um código binário não homogêneo é um código de treliça no qual as quantidades de ramos que saem de cada nó não são iguais. Em um BAC quase sincronizado a diferença de fases "s" entre os blocos de palavras códigos dos dois codificadores é chamado de "slippage", fig. 2.4.

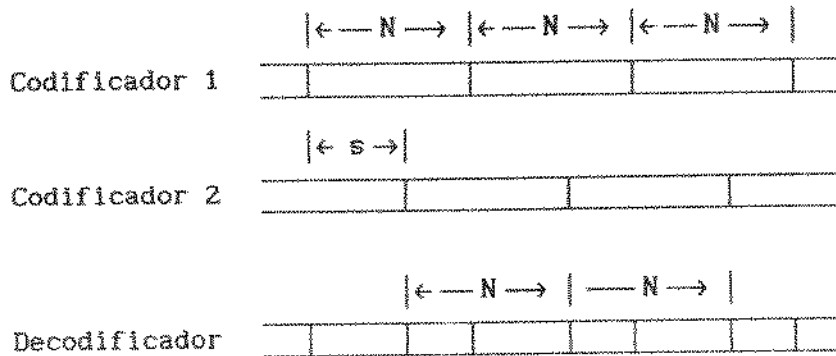


Fig. 2.4. Transmissão de Palavras Códigos em um BAC Quase Sincronizado

Se o comprimento de C_1 e C_2 é "N" então $0 \leq s < N$. O par de códigos (C_1, C_2) é chamado de código univocamente decodificável quase sincronizado (QSUD).

O BAC sem sincronismo pode ser transformado em um BAC quase sincronizado através do seguinte esquema, [14]: no início da transmissão de dados cada um dos dois codificadores enviam uma sequência de sincronismo para o decodificador. Estas sequências de sincronismos tem a propriedade de que após a recepção de uma delas por parte do decodificador, este pode estabelecer sincronismo de bloco com o codificador que a enviou independente da palavra-código transmitida pelo outro codificador durante o mesmo intervalo de tempo. Após a recepção das sequências de sincronismos de ambos os codificadores, o

decodificador estabelece sincronismo com cada codificador individualmente e o BAC sem sincronismo é transformado em um BAC quase sincronizado. Desta forma, o problema para o BAC sem sincronismo é dividido em duas partes: a definição de uma sequência de sincronismo e a construção de códigos QSUD.

2.3 O Canal Aditivo Binário 2 - Usuários com Ruído

O MAC aditivo binário com ruído pode ser representado pelo modelo discreto da figura 2.5.

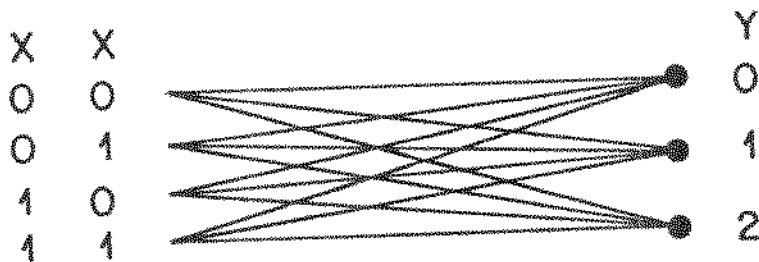


Fig 2.5 Canal Aditivo Binário com Ruído

As condições de erros são definidas pelas seguintes regras:

- i) Se o ruído causa uma transição de erro de (0,0) para 1 ou de (1,1) para 1, então um único erro ocorreu;
- ii) Se o ruído causa uma transição de erro de (0,1) ou (1,0) para 0 ou 2, então um único erro ocorreu;
- iii) Se o ruído causa uma transição de erro de (0,0) para 2 ou de (1,1) para 0 então um duplo erro ocorreu.

Códigos para o Canal Aditivo Binário com ruído dois usuários foram estudados por Tadao Kasami e Shu Lin, [7], Henk C. A. van Tilborg [16, 17] e E. J. Weldon, [15]. Algoritmos de decodificação são apresentados por Tadao Kasami e Shu Lin, [18] e G. H. Khachatrian, [19].

Esta classe de códigos, denominada de δ - decodificável, tem a capacidade de corrigir $t = \lfloor (\delta - 1)/2 \rfloor$ erros, onde o símbolo $\lfloor x \rfloor$ denota o maior inteiro menor ou igual a x .

Um código dois usuários (C_1, C_2) é dito ser δ - decodificável se para quaisquer dois pares distintos de palavras-códigos (c_1, c_2) ,

(c'_1, c'_2) em (C_1, C_2) tivermos,

$$d_L(c_1 + c_2, c'_1 + c'_2) \geq \delta$$

onde,

$$d_L(a, b) = \sum_{i=1}^n |b_i - a_i| = \|a - b\|$$

é definida como a L - distância, [1, 17] entre as palavras-código a e b . O sinal "-" denota a subtração real, $|b_i - a_i|$ é o valor absoluto de $b_i - a_i$, "n" é o comprimento das palavras-código dos códigos C_1 e C_2 e $\|a - b\|$ é a norma de $a - b$.

Por exemplo, para $\delta = 4$ o código dois usuários de comprimento $N = 4$ (C_1, C_2) onde $C_1 = \{ 0000, 1111 \}$ e $C_2 = \{ 1100, 0011 \}$ é 4 - decodificável, conforme podemos ver da tabela abaixo.

Tabela 2.4

C_1	0 0 0 0	1 1 1 1
C_2		
1 1 0 0	1 1 0 0	2 2 1 1
0 0 1 1	0 0 1 1	1 1 2 2

O problema de codificação para este tipo de canal, [19], pode ser formulado da seguinte maneira: dados N , δ e a taxa R_1 do código do primeiro usuário, construir códigos C_1, C_2 tais que (C_1, C_2) seja δ - decodificável e a taxa R_2 do código C_2 seja máxima. Este é um problema combinatorial bastante complicado e uma série de trabalhos tem sido desenvolvidos para investigar tais códigos, [7, 14, 15, 16, 17, 18, 20, 21].

Van Tilborg [17], usando métodos combinatoriais, obteve uma cota superior para $|C_1| \cdot |C_2|$, onde (C_1, C_2) é um código dois usuários δ - decodificável para o canal aditivo binário com ruído. Assintoticamente esta cota se reduz a,

$$R_1 + R_2 \leq 3/2 + e(\log_2 e) - (1/2 + e) \cdot \log_2(1 + 2e)$$

$$= 1/2 - e + H(1/2 - e) - (1/2)H(2e)$$

onde,

$$e = \lfloor (\delta - 1)/2 \rfloor / n$$

R_1, R_2 são, respectivamente, as taxas dos códigos C_1 e C_2 e $H(x)$ é a função entropia de x :

$$H(x) = -x \cdot \log_2 x - (1 - x) \cdot \log_2(1 - x)$$

2.4 O Canal Aditivo T - Usuários

- A figura 2.6 mostra o sistema de comunicação, motivação deste trabalho, denominado sistema de comunicação múltiplo acesso, [1].

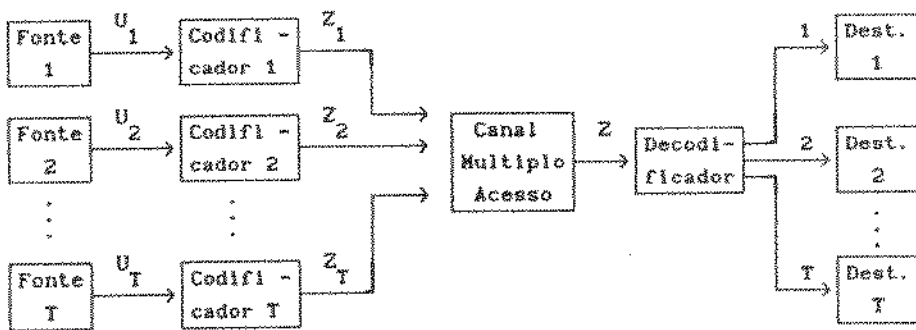


Fig. 2.6. Sistema de Comunicação Múltiplo Acesso

A cada um dos T - usuários é atribuído um código binário C_i , de comprimento N denominado de código constituinte. Um vetor $Z_i \in C_i$ é escolhido e transmitido por cada usuário. Se o canal é sem ruído, a saída é o vetor $Z = Z_1 + Z_2 + \dots + Z_T$, onde o sinal "+" indica a soma real coordenada a coordenada. Seja M_i o número de palavras códigos do i - ésimo código constituinte C_i , então a taxa deste código é,

$$R_1 = (\log_2 M_1) / N$$

e a taxa soma do código T - usuários (C_1, C_2, \dots, C_T) é definida conforme [1], como sendo,

$$R(T) = R_1 + R_2 + \dots + R_T$$

As primeiras abordagens para a obtenção de códigos para o canal aditivo binário T - usuários foram no sentido de maximizar o número de palavras códigos de um dado comprimento para dois usuários independentes. Em [1], Chang e Weldon descrevem uma classe de códigos T - usuários univocamente decodificável para o canal múltiplo acesso aditivo binário sem ruído e apresentam um algoritmo de decodificação para essa classe de códigos. Thomas J. Ferguson [2] generaliza os códigos de Chang e Weldon via dois caminhos. O primeiro é uma generalização da construção iterativa apresentada em [1] e o segundo é via a noção de classes de equivalências de tais códigos. John H. Wilson em [3] desenvolve uma extensão dos códigos de Chang e Weldon, apresenta uma classe de códigos corretores de erros para o canal aditivo binário com ruído T - usuários e ilustra através de um exemplo um algoritmo de decodificação para tais códigos.

2.4.1. A Capacidade do Canal Aditivo T - Usuários

- A capacidade do Canal Discreto sem Memória (DMC) com alfabeto de entrada X , alfabeto de saída Y e probabilidade de transição $p(y = j / x = i)$ é dada por,

$$C = \text{Max}_{\{p(x_i)\}} I(X; Y)$$

onde a maximização é feita sobre todas as possíveis distribuições de probabilidades de entrada $\{p(x_i)\}$ em X ,

$$I(X; Y) = \sum_{i=0}^{I-1} \sum_{j=0}^{J-1} p(x = i, y = j) \log_2 \frac{p(y = j / x = i)}{p(y = j)}$$

é a informação média mútua do canal,

$$p(x = i, y = j) = p(y = j/x = i).p(x = i) \quad (2.1)$$

e,

$$p(y = j) = \sum_{i=0}^{I-1} p(y = j/x = i).p(x = i)$$

A capacidade do canal aditivo binário T - usuários sem ruído com alfabeto de entrada X igual ao alfabeto de saída Y = { 0, 1, 2, ..., T } é obtida [12] quando todos os usuários transmitem símbolos binários igualmente prováveis e estatisticamente independentes. A distribuição de probabilidade das T + 1 superposições é binomial conforme mostraremos a seguir.

Sejam Z = (z₁, z₂, ..., z_k), z_i ∈ { 0, 1, ..., T } e X a variável aleatória: X = a k - ésima coordenada de Z ser igual a i, i ∈ { 0, 1, ..., T }.

Este evento é provável se na escolha dos k - ésimos símbolos binários de cada um dos T - códigos constituintes tivermos i uns e desta forma temos que o número de maneiras distintas possíveis para a realização deste evento é,

$$\binom{T}{i}$$

Por outro lado, cada código constituinte possui duas palavras-código e portanto para cada código constituinte temos duas possibilidades de escolhermos o k - ésimo símbolo. Além disto cada usuário transmite símbolos binários estatisticamente independentes, logo o número de eventos possíveis no processo de escolha para a formação do k - ésimo símbolo de Z, isto é, a cardinalidade do espaço amostral é 2^T.

Desta forma temos que,

$$P(X = i) = \frac{\binom{T}{i}}{2^T} \quad (2.2)$$

As probabilidades de transições, [1] são dadas por,

$$P(y = j/x = i) = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{caso contrário} \end{cases} \quad 0 \leq i, j \leq T \quad (2.3)$$

Desta forma temos a capacidade do canal T - usuários, a qual denotamos por C(T):

$$C(T) = \sum_{i=0}^T \sum_{j=0}^T p(x = i, y = j) \log_2 \frac{p(y = j/x = i)}{p(y = j)}$$

De (2.1) e (2.3) temos,

$$C(T) = \sum_{i=0}^T p(x = i) \cdot \log_2 \frac{1}{p(x=i)}$$

e, da equação (2.2) obtemos a seguinte expressão para a capacidade do canal aditivo binário T - usuários sem ruído,

$$C(T) = \sum_{i=0}^T \frac{\binom{T}{i}}{2^T} \log_2 \frac{2^T}{\binom{T}{i}}$$

Os seguintes lemas [1] determinam, respectivamente, um limitante inferior e um limitante superior para C(T).

Lemma 2.: C(T) é limitado inferiormente por $(1/2) \log_2 (\pi T/2)$.

Demonstração : É conhecido das propriedades dos números binomiais que,

$$\left\lfloor \frac{\binom{T}{i}}{2} \right\rfloor \geq \binom{T}{i}, \quad 0 \leq i \leq T$$

onde $\left\lfloor \frac{T}{2} \right\rfloor$ denota o maior inteiro menor ou igual a T/2. Então,

$$\sum_{i=0}^T \frac{\binom{T}{i}}{2^T} \log_2 \frac{2^T}{\binom{T}{i}} \approx \sum_{i=0}^T \frac{\binom{T}{i}}{2^T} \log_2 \frac{2^T}{\left\lfloor \frac{T}{2} \right\rfloor}$$

$$= \log_2 \frac{2^T}{\left\lfloor \frac{T}{2} \right\rfloor}$$

Por outro lado,

$$\left\lfloor \frac{T}{2} \right\rfloor > \sqrt{\frac{\pi T}{2}}$$

ver apêndice A.

Então,

$$\log_2 \frac{2^T}{\left\lfloor \frac{T}{2} \right\rfloor} > \log_2 \sqrt{\frac{\pi T}{2}} = (1/2) \log_2 (\pi T/2).$$

Portanto,

$$C(T) \geq (1/2) \log_2 (\pi T/2)$$

■

Lemma 2.2 : $C(T)$ é limitado superiormente por $(1/2) \log_2 (\pi T/2)$ para T par e por $(1/2) \log_2 \pi(T+1)/2$ para T ímpar.

Demonstração : Sejam,

$$P_1 = \frac{\binom{T}{1}}{2^T}, \quad a = \left\lfloor \frac{T+1}{2} \right\rfloor$$

e,

$$L_1 = \frac{1}{\sqrt{\pi a}} \exp(-(1-a)^2/a)$$

Então,

$$\begin{aligned} - \sum_{i=0}^T P_i \log_2 L_i &= - \sum_{i=0}^T P_i \log_2 \left(\frac{\exp(-(1-a)^2/a)}{\sqrt{\pi a}} \right) \\ &= - \sum_{i=0}^T P_i \left\{ -(1/2) \log_2(\pi a) - \frac{(1-a)^2}{a} \log_2 e \right\} \\ &= (1/2) \log_2(\pi a) + (1/a) \left[\log_2 e \right] \left(\frac{a}{2} \right) = (1/2) \log_2(\pi e a). \end{aligned}$$

Desde que,

$$C(T) = \sum_{i=0}^T P_i \log_2 \frac{1}{P_i}$$

temos,

$$C(T) - (1/2) \log_2(\pi e a) = \sum_{i=0}^T P_i \log_2 \frac{L_i}{P_i}$$

$$\leq \sum_{i=0}^T P_i \left(\frac{L_i}{P_i} - 1 \right) \log_2 e$$

$$= \log_2 e \left\{ \sum_{i=0}^T L_i - 1 \right\}$$

A desigualdade decorre das seguintes propriedades da função logarítmica,

$$1) \log_2 x = \log_e x \cdot \log_2 e$$

$$2) \log_e x \leq x - 1$$

Agora, para todo T seja,

$$\begin{aligned} A &= \sum_{i=0}^T L_i = \sum_{i=-a}^{T-a} \frac{\exp(-i^2/a)}{\sqrt{\pi a}} \leq \\ &\leq \sum_{i=-a}^a \frac{\exp(-i^2/a)}{\sqrt{\pi a}} \end{aligned} \quad (2.4)$$

Vamos mostrar que $A < 1$. De [14, pp. 11] temos,

$$\begin{aligned} \frac{1}{\sqrt{\pi a}} \sum_{i=-\infty}^{\infty} \exp(-i^2/a) &= \sum_{i=-\infty}^{\infty} \exp(-a\pi^2 i^2) \\ &= 1 + 2 \sum_{i=1}^{\infty} \exp(-a\pi^2 i^2) \end{aligned} \quad (2.5)$$

Esta última igualdade decorre do fato da função,

$$f(i) = \exp(-a\pi^2 i^2)$$

ser par, isto é, $f(i) = f(-i)$.

De (2.4) e (2.5) segue que,

$$\begin{aligned} A &\leq 1 + 2 \sum_{i=1}^{\infty} \exp(-a\pi^2 i^2) - \frac{2}{\sqrt{\pi a}} \sum_{i=a+1}^{\infty} \exp(-i^2/a) \\ &= 1 + 2 \sum_{i=1}^{\infty} \left\{ \exp(-a\pi^2 i^2) - \exp(-[(((i+a)^2/a) + \log_e \sqrt{\pi a}]) \right\} \\ &= 1 + 2 \sum_{i=1}^{\infty} \left(\exp(-E_{1i}) - \exp(-E_{2i}) \right) \end{aligned}$$

onde,

$$E_{11} = a\pi^2 i^2$$

$$E_{21} = (i + a)^2/a + \log_e \sqrt{\pi a}$$

Agora, para $a \geq 1$ o valor de "i" que minimiza $E_{11} - E_{21}$ é 1. Então para $i = 1$, $E_{11} - E_{21}$ cresce monotonicamente com "a". Além disto, $E_{11} - E_{21}$ é minimizada para $a = 1$.

Para $a = 1$, $i = 1$ temos,

$$E_{11} - E_{21} = \pi^2 - 2^2 + \log_e \sqrt{\pi}$$

e desde que $\pi^2 > 2^2 + \log_e \sqrt{\pi}$ segue que para $i \geq 1$ e $a \geq 1$,

$$E_{11} > E_{21}$$

então,

$$\exp(-E_{11}) - \exp(-E_{21}) < 0$$

desta forma temos que $A \leq 0$ e, portanto,

$$C(T) - (1/2)\log_2(\pi ea) \leq 0$$

isto é,

$$C(T) \leq (1/2)\log_2(\pi ea).$$

■

Definição 2.1 : Duas quantidades $g_1(t)$ e $g_2(t)$ são assintoticamente iguais se sua razão se aproxima da unidade quando t tende para o infinito.

Como consequência do lema 2.2 temos que $C(T)$ é assintoticamente igual a $(1/2)\log_2(\pi eT/2)$ quando T cresce. Este resultado é sintetizado no seguinte teorema, [1].

Teorema 2.1 : A taxa máxima de um código T-usuários univocamente decodificável para o Canal Aditivo Binário T-Usuários sem ruído é assintoticamente igual a $(1/2)\log_2(\pi e T/2)$ quando $T \rightarrow \infty$.

2.5 Conclusão

Neste capítulo foram apresentados os sistemas de comunicações T - Usuários, em particular tratamos do canal aditivo binário dois usuários com e sem ruído e apresentamos algumas classes de códigos para estes tipos de sistemas de comunicações. Também foi desenvolvida uma expressão algébrica que determina a capacidade do canal aditivo binário T - Usuários sem ruído. No próximo capítulo apresentaremos algumas classes de códigos para o Canal Aditivo Binário T - Usuários com e sem ruído, bem como alguns algoritmos de decodificações para estas classes de códigos.

Capítulo III

Códigos e Algoritmos de Decodificação para o Canal Aditivo T - Usuários

3.1 Introdução

Neste capítulo apresentaremos esquemas de codificação para o canal Aditivo T - Usuários bem como algumas técnicas de decodificação para esse tipo de sistema de comunicação. Na seção 3.2 descrevemos as classes de códigos univocamente decodificáveis propostas por Chang e Weldon [1,11]. Na seção 3.3 fazemos uma apresentação de como Ferguson [2] generalizou os códigos de Chang e Weldon. Esta generalização é feita via dois caminhos. O primeiro é uma generalização da construção iterativa proposta por Chang e Weldon [1] e o segundo é via a noção de classes de equivalência de tais códigos. Na seção 3.4 mostramos como Wilson [3] estendeu os códigos de Chang e Weldon [1] e obteve uma classe de códigos corretores de erros para o canal Aditivo T - Usuários. Finalmente na seção 3.5 serão mostradas algumas técnicas de decodificação para os códigos de Chang e Weldon [1] e de Wilson [3].

3.2 Os Códigos de Chang e Weldon, [1]

Os códigos de Chang e Weldon [1] são definidos via uma matriz D de ordem $T \times N$ com entradas no conjunto $\{0, 1, -1\}$ chamada matriz diferença da seguinte maneira: dado um código T - usuários (C_1, C_2, \dots, C_T) para o qual o i - ésimo código constituinte C_i , $i = 1, 2, \dots, T$ contém duas palavras-código X_i, Y_i , isto é, $C_i = \{X_i, Y_i\}$ a i - ésima linha de D é o vetor diferença $d_i = X_i - Y_i$. Reciprocamente, dada uma matriz diferença D de ordem $T \times N$ é possível construir um código T - usuários com duas palavras códigos por código constituinte através das seguintes regras:

1) Se a j - ésima coordenada da i - ésima linha de D é -1 , então as j - ésimas coordenadas de X_i e Y_i são 0 e 1, respectivamente;

2) Se a j - ésima coordenada da i - ésima linha de D é 1, então as j - ésimas coordenadas de X_i e Y_i são 1 e 0, respectivamente;

3) Se a j - ésima coordenada da i - ésima linha de D é 0, então as j - ésimas coordenadas de X_i e Y_i são 0.

Definição 3.1 : Um código T - usuário (C_1, C_2, \dots, C_T) é univocamente decodificável se e somente se todas as somas constituídas de uma palavra-código de cada código constituinte são distintas, isto é, se e somente se, para quaisquer $(Z_1, Z_2, \dots, Z_T) \neq (Z'_1, Z'_2, \dots, Z'_T)$ em (C_1, C_2, \dots, C_T) tivermos $Z_1 + Z_2 + \dots + Z_T \neq Z'_1 + Z'_2 + \dots + Z'_T$.

A condição de decodificação única pode ser expressa em termos da matriz diferença pelo seguinte teorema, conforme [1].

Teorema 3.1 : (Condição de Decodibilidade unívoca): Uma matriz D $T \times N$ sobre $\{0, 1, -1\}$ define um código univocamente decodificável se e somente se o único vetor M de comprimento T sobre $\{0, 1, -1\}$ tal que $M \cdot D = 0^N$ é o vetor $M = 0^T$, onde 0^N e 0^T denotam os vetores zeros de comprimentos N e T , respectivamente.

Demonstração : Seja D a matriz diferença $T \times N$ que define um código binário T - usuários univocamente decodificável (C_1, C_2, \dots, C_T) para o qual o i - ésimo código constituinte C_i , contém duas palavras códigos X_i e Y_i , isto é, $C_i = \{X_i, Y_i\}$. Então,

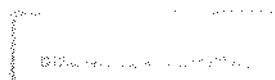
$$D = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_T \end{bmatrix}$$

onde $d_i = X_i - Y_i$.

Sejam (Z_1, Z_2, \dots, Z_T) e $(Z'_1, Z'_2, \dots, Z'_T)$ duas T - uplas distintas em (C_1, C_2, \dots, C_T) , então,

$$(Z_1 - Z'_1) + (Z_2 - Z'_2) + \dots + (Z_T - Z'_T) \neq 0^N$$

e desde que $Z_i - Z'_i$ é 0^N , d_i ou $-d_i$, segue da equação acima que o código T - usuários é univocamente decodificável se e somente se,



$$m_1 d_1 + m_2 d_2 + \dots + m_T d_T = M.D \neq 0^N$$

para todo $M \neq 0^N$, $M \in \{0, 1, -1\}^T$.

O teorema seguinte apresenta um método iterativo para construir uma classe de códigos T - usuários univocamente decodificáveis para o canal aditivo binário sem ruído T - usuários. A idéia é baseada na anexação de mais colunas (i.é., bits/palavras) na matriz diferença de um dado código univocamente decodificável e, simultaneamente, aumentar o número de linhas (i.é., usuários) tal que a nova matriz seja a matriz diferença para um novo código T' - usuários univocamente decodificável, onde $T' > T$.

Teorema 3.2 : Para um inteiro não negativo j a matriz

$$D_j = \begin{bmatrix} D_{j-1} & D_{j-1} \\ D_{j-1} & -D_{j-1} \\ I_{j-1} & 0_{j-1} \end{bmatrix} \quad (3.1)$$

define um código $(j+2).2^{j-1}$ - usuários univocamente decodificável de comprimento 2^j , onde I_{j-1} é a matriz identidade de ordem 2^{j-1} , 0_{j-1} é a matriz zero de ordem 2^{j-1} e $D_0 = [1]$.

Demonstração : A prova é por indução em j . Para $j = 0$, $D_0 = [1]$ define o código trivial um usuário univocamente decodificável de comprimento 1. Suponha que D_{j-1} defina um código $2^{j-2}.(j+1)$ - usuários univocamente decodificável de comprimento 2^{j-1} , $j \geq 1$. Agora considere a $T_j \times N_j$ matriz D_j de 3.1. É claro que $T_j = 2.[2^{j-2}.(j+1)] + 2^{j-1} = (j+2).2^{j-1}$ e $N_j = 2^{j-1}.2 = 2^j$. Agora devemos mostrar que D_j é a matriz diferença para um código T_j - usuários univocamente decodificável de comprimento N_j .

Seja $m = (m_1, m_2, m_3)$ o vetor solução da equação $m.D_j = 0^j$ sobre $\{0, 1, -1\}$, onde $m_1, m_2 \in \{0, 1, -1\}^{j-1}$, $m_3 \in \{0, 1, -1\}^{j-1}$. De 3.1 temos,

$$m_1 D_{j-1} + m_2 D_{j-1} + m_3 = 0^{j-1} \quad (3.1a)$$

$$m_1 D_{j-1} - m_2 D_{j-1} = 0^{j-1} \quad (3.1b)$$

o que implica que,

$$2m_1 D_{j-1} = -m_3 \quad (3.1c)$$

$$m_1 D_{j-1} = m_2 D_{j-1}$$

As componentes de $2m_1 D_{j-1}$ devem ser inteiros pares ou zero. Desde que as componentes de m_3 são elementos do conjunto $\{0, 1, -1\}$, segue que $m_3 = 0^{N_{j-1}}$. Então de 3.1c temos,

$$\begin{aligned} m_1 D_{j-1} &= 0^{N_{j-1}} \\ m_2 D_{j-1} &= 0^{N_{j-1}} \end{aligned} \quad (3.1d)$$

Por hipótese de indução D_{j-1} é a matriz diferença para um código T_{j-1} - usuários univocamente decodificável e segue do teorema 3.1 que $m_1 = m_2 = 0^{N_{j-1}}$. Então $m = (m_1, m_2, m_3) = 0^N$ e, portanto, aplicando novamente o teorema 3.1, temos que D_j é a matriz diferença de um código T_j - usuários univocamente decodificável de comprimento N_j . ■

Exemplo 3.1 : Para $j = 1$ a matriz diferença é da forma,

$$D_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 0 \end{bmatrix}$$

e o código T_1 - usuários, $T_1 = (1 + 2).2^0 = 3$ de comprimento 2^1 , tem os seguintes códigos constituintes:

$$\begin{aligned} C_1 &= \{ X_1 = (1, 1), Y_1 = (0, 0) \} \\ C_2 &= \{ X_2 = (1, 0), Y_2 = (0, 1) \} \\ C_3 &= \{ X_3 = (1, 0), Y_3 = (0, 0) \} \end{aligned}$$

A tabela 3.1 apresenta uma listagem (não exaustiva) de parâmetros dos códigos do teorema 3.2.

Tabela 3.1

J	T_J	N_J	d_{\min}	$R_{\text{sum}}(T_J)$
1	3	2	1	1.5
2	8	4	1	2
3	20	8	1	2.5
4	48	16	1	3
5	112	32	1	3.5
6	256	64	1	4
7	576	128	1	4.5
8	1280	256	1	5
9	2816	512	1	5.5
10	6144	1024	1	6

- A taxa do i - ésimo código constituinte é,

$$R_i = (\log_2 2)/N_J = 1/N_J$$

e a taxa soma é,

$$R(T_J) = T_J/N_J = 1 + J/2 = 1 + (1/2)\log_2 N_J.$$

onde $T_J = (J + 2) \cdot 2^{J-1}$ e $N_J = 2^J$.

- Os Códigos T_J - Usuários Unicamente Decodificáveis especificados pelo teorema 3.2 tem taxa soma $R(T_J)$ assintoticamente igual a taxa soma máxima $C(T_J)$ quando T_J cresce, [1].

Definição 3.2 : (Produto de Kronecker - [4]): Sejam $A = (a_{ij})$ uma matriz $m \times m$ e $B = (b_{ij})$ uma matriz $n \times n$ sobre um corpo qualquer. O produto de Kronecker de A e B , denotado por $A \otimes B$ é a matriz $mn \times mn$ obtida multiplicando toda entrada da matriz A , a_{ij} por B , isto é, $A \otimes B = (a_{ij} B)$.

Por exemplo, se

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{e} \quad H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

então,

$$I_2 \otimes H_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

O teorema abaixo [1] apresenta uma classe de códigos obtida por Chang e Weldon com distância mínima, $d_{\min} = 2^i$, $i \geq 0$.

Teorema 3.3 : Seja $D_1^{(j)}$ uma matriz sobre $\{0, 1, -1\}$ da seguinte forma:

$$D_1^{(j)} = \begin{bmatrix} D_{1-1}^{(j)} & D_{1-1}^{(j)} \\ D_{1-1}^{(j)} & -D_{1-1}^{(j)} \end{bmatrix}$$

onde $D_0^{(j)}$ é a matriz D_j do teorema 3.2. Então $D_1^{(j)}$ define um código T-usuários de comprimento N e distância mínima $d_{\min} = 2^i$, onde $T = (j+2) \cdot 2^{j-1+i}$, $N = 2^{j+1}$. A taxa soma destes código é,

$$R(T) = T/N = 1 + (1/2) \log(N/d_{\min})$$

Demonstração : Por indução em i. Para $i = 0$, $D_0^{(j)}$ é a matriz D_j do teorema 3.2 e define um código com os seguintes parâmetros:

$$T = (j + 2) \cdot 2^{j-1}; \quad N = 2^j; \quad d_{\min} = 2^0$$

Agora suponha que a matriz $D_{1-1}^{(j)}$ defina um código com parâmetros:

$$\begin{aligned} T &= (j + 2) \cdot 2^{j-1+(i-1)} \\ N &= 2^{j+(i-1)} \\ d_{\min} &= 2 \end{aligned}$$

A matriz $D_1^{(j)}$ define um código $(j+2) \cdot 2^{j-1+i}$ - usuários de comprimento 2^{j+1} . Para completar a prova indutiva devemos mostrar que este código tem distância mínima igual a 2^i .

Seja m a $[(j+2) \cdot 2^{j-1+i}]$ - upla sobre $\{0, 1, -1\}$. Particionemos m em duas $[(j+2) \cdot 2^{j-1+(i-1)}]$ - uplas iguais (m_1, m_2) . Considere a 2^{j+1} - upla,

$$mD_1^{(j)} = (m_1 D_{1-1}^{(j)} + m_2 D_{1-1}^{(j)}, m_1 D_{1-1}^{(j)} - m_2 D_{1-1}^{(j)})$$

Então,

$$\|mD_1^{(j)}\| = \|m_1 D_{1-1}^{(j)} + m_2 D_{1-1}^{(j)}\| + \|m_1 D_{1-1}^{(j)} - m_2 D_{1-1}^{(j)}\|.$$

Agora, desde que $\|a + b\| + \|a - b\| \geq 2 \cdot \max(\|a\|, \|b\|)$ e, por hipótese de indução $\|m_1 D_{1-1}^{(j)}\| \geq 2^{i-1}$, para $i = 1, 2$, temos que,

$$\begin{aligned} \|mD_1^{(j)}\| &= \|m_1 D_{1-1}^{(j)} + m_2 D_{1-1}^{(j)}\| + \|m_1 D_{1-1}^{(j)} - m_2 D_{1-1}^{(j)}\| \\ &\geq 2 \cdot \max(\|m_1 D_{1-1}^{(j)}\|, \|m_2 D_{1-1}^{(j)}\|) \geq 2 \cdot 2^{i-1} = 2^i. \end{aligned}$$

Então para concluir a demonstração é necessário mostrar que existe m tal que $\|m \cdot D_{1-1}^{(j)}\| = 2^i$. É fácil verificar que a última linha da matriz $D_0^{(j)}$ tem um único 1, a última linha de $D_1^{(j)}$ tem dois uns e a última linha de $D_i^{(j)}$ tem 2^i uns. Então o vetor $m = (0 \ 0 \ \dots \ 0 \ 1)$ satisfaz esta propriedade. ■

Para $i = 0$, $D_0^{(j)}$ é a matriz D_j do teorema 3.2. Para $i = 1$, $D_1^{(j)}$ é o produto de Kronecker da matriz de Hadamard de ordem 2, isto é,

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

pela matriz D_j do teorema 3.2. Em geral, o seguinte resultado é verdadeiro.

Corolário 3.1 : A matriz $D_i^{(j)}$ do teorema 3.3. é o produto de Kronecker da matriz de Hadamard de ordem 2^i com a matriz D_j do teorema 3.2.

Demonstração : Usaremos indução sobre i . É fácil ver que para $i = 1$ $D_1^{(j)}$ é o produto de Kronecker da matriz de Hadamard de ordem 2 com a matriz D_j do teorema 3.2. Suponha que o resultado seja verdadeiro para todo $r < n$. Então $D_{n-1}^{(j)}$ é o produto de Kronecker da matriz de Hadamard de ordem 2^{n-1} com a matriz D_j . Mostraremos que é verdade para $r = n$.

Temos que,

$$D_n^{(j)} = \begin{bmatrix} D_{n-1}^{(j)} & D_{n-1}^{(j)} \\ D_{n-1}^{(j)} & -D_{n-1}^{(j)} \end{bmatrix}$$

$$= H_2 \otimes D_{n-1}^{(j)}$$

onde H_2 é a matriz de Hadamard de ordem 2.

Por hipótese de indução temos,

$$D_{n-1}^{(j)} = H_{2^{n-1}} \otimes D_j$$

onde $H_{2^{n-1}}$ é a matriz de Hadamard de ordem 2^{n-1} . Desta forma temos,

$$D_n^{(j)} = H_2 \otimes (H_{2^{n-1}} \otimes D_j)$$

finalmente pela associatividade do produto de Kronecker temos,

$$D_n^{(j)} = H_{2^n} \otimes D_j$$

Um caso particular é obtido quando $j = 0$. Neste caso $D_1^{(j)}$ é simplesmente a matriz de Hadamard de ordem 2^1 .

A tabela 3.2 nos mostra alguns parâmetros desta classe de códigos.

Tabela 3.2

Códigos de Weldon					
i	j	T	N	d_{\min}	$R_{\text{sum}}(T)$
1	0	2	2	2	1
1	1	6	4	2	1.5
1	2	16	8	2	2
1	3	40	16	2	2.5
⋮	⋮	⋮	⋮	⋮	⋮
2	0	4	4	4	1
2	1	12	8	4	1.5
2	2	32	16	4	2
2	3	80	32	4	2.5
⋮	⋮	⋮	⋮	⋮	⋮
3	0	8	8	8	1
3	1	24	16	8	1.5
3	2	64	32	8	2
3	3	160	64	8	2.5
⋮	⋮	⋮	⋮	⋮	⋮

Exemplo 3.4 : Para $i = 1$ e $j = 1$ temos:

$$D_1^{(1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 0 & -1 & 0 \end{bmatrix}$$

que é a matriz diferença de um código T-usuários, $T = (1+2) \cdot 2^{1-1+1} = 6$, comprimento $N = 2^{1+1} = 4$ e distância mínima $d_{\min} = 2$.

Shin-Chun Chang em [11] apresenta outros resultados de códigos univocamente decodificáveis para o Canal Múltiplo Acesso T-Usuários. A construção destes códigos é baseado no seguinte teorema.

Teorema 3.4 : Considere a matriz diferença obtida usando o método iterativo:

$$D_i = \begin{bmatrix} D_{i-1} & D_{i-1} \\ D_{i-1} & -D_{i-1} \\ I_{i-1} & O_{i-1} \end{bmatrix}$$

Esta matriz especifica um Código T_i - Usuários univocamente decodificável de comprimento $N_i = 2^i$ onde,

$$T_i = (1 + 2)2^{i-1}$$

Seja D'_{is} a matriz obtida de D_i apagando as primeiras S colunas da submatriz

$$B_i = \begin{bmatrix} D_{i-1} \\ D_{i-1} \\ I_{i-1} \end{bmatrix}$$

e removendo todas as linhas da submatriz

$$H_i = \begin{bmatrix} D_{i-1} & -D_{i-1} \\ I_{i-1} & O_{i-1} \end{bmatrix}$$

exceto as linhas com componentes iguais a zero nas posições das colunas apagadas. Então D'_{is} é a matriz diferença de um código múltiplo-usuários

univocamente decodificável de comprimento $2^i - S$ onde $1 \leq S \leq 2^{i-1}$.

Demonstração : Seja $D_{i-1} = (\tilde{V}_1, \tilde{V}_2, \dots, \tilde{V}_{N_{i-1}})$ onde \tilde{V}_k , $k = 1, 2, \dots, N_{i-1}$ é a k -ésima coluna da matriz D_{i-1} . Então a matriz D_i definida no teorema 3.4 pode ser escrita na seguinte forma,

$$D_i = \begin{bmatrix} \tilde{V}_1 & \tilde{V}_2 & \dots & \tilde{V}_{N_{i-1}} & \tilde{V}_1 & \tilde{V}_2 & \dots & \tilde{V}_{N_{i-1}} \\ \tilde{V}_1 & \tilde{V}_2 & \dots & \tilde{V}_{N_{i-1}} & -\tilde{V}_1 & -\tilde{V}_2 & \dots & -\tilde{V}_{N_{i-1}} \\ & & & I_{i-1} & & & & O_{i-1} \end{bmatrix}$$

e

$$B_i = \begin{bmatrix} D_{i-1} \\ D_{i-1} \\ I_{i-1} \end{bmatrix} = \begin{bmatrix} \tilde{V}_1 & \tilde{V}_2 & \dots & \tilde{V}_{N_{i-1}} \\ \tilde{V}_1 & \tilde{V}_2 & \dots & \tilde{V}_{N_{i-1}} \\ & & & I_{i-1} \end{bmatrix}$$

$$H_i = \begin{bmatrix} D_{i-1} & -D_{i-1} \\ I_{i-1} & O_{i-1} \end{bmatrix} = \begin{bmatrix} \tilde{V}_1 & \tilde{V}_2 & \dots & \tilde{V}_{N_{i-1}} & -\tilde{V}_1 & -\tilde{V}_2 & \dots & -\tilde{V}_{N_{i-1}} \\ & & & I_{i-1} & & & & O_{i-1} \end{bmatrix}$$

Sem perda de generalidade, podemos assumir que as primeiras S colunas da matriz B_i são apagadas e todas as linhas em H_i são removidas, exceto aquelas que tem componentes iguais a zero nas primeiras S posições. Então podemos obter a $T_{iS} \times (N_{i-1} - S)$ matriz sobre $\{0, 1, -1\}$.

$$D'_i = \begin{bmatrix} \tilde{V}_{S+1} \dots \tilde{V}_{N_{i-1}} & \tilde{V}_1 \dots \tilde{V}_S & \tilde{V}_{S+1} \dots \tilde{V}_{N_{i-1}} \\ \tilde{V}'_{S+1} \dots \tilde{V}'_{N_{i-1}} & \tilde{O} \dots \tilde{O} & -\tilde{V}'_{S+1} \dots -\tilde{V}'_{N_{i-1}} \\ & & I'_{i-1} & & & O'_{i-1} \end{bmatrix} \quad (3.2)$$

onde \tilde{V}'_j é \tilde{V}_j após a remoção das linhas, I'_{i-1} é a matriz identidade de ordem $N_{i-1} - S$, O'_{i-1} é a matriz nula de ordem $(N_{i-1} - S) \times N_{i-1}$ e \tilde{O} representa o vetor coluna nulo.

Seja m uma T_{iS} - upla sobre $\{0, 1, -1\}$ tal que,

$$m \cdot D'_1 = 0^{N_{1-1} - S} \quad (3.3)$$

Podemos agrupar as componentes de m em tres vetores (m_1, m_2, m_3) onde m_1 é o vetor das primeira N_{1-1} componentes de m , m_3 é o vetor das últimas $(N_{1-1} - S)$ componentes de m e m_2 é o vetor das demais componentes de m .

De (3.2) e (3.3) temos,

$$\begin{cases} m_1 \tilde{V}_{S+1} + m_2 \tilde{V}'_{S+1} + m_{3,1} = 0 \\ \vdots \\ m_1 \tilde{V}_{N_{1-1}} + m_2 \tilde{V}'_{N_{1-1}} + m_{3, N_{1-1} - S} = 0 \end{cases} \quad (3.4)$$

$$\begin{cases} m_1 \tilde{V}_{1-1} = 0 \\ \vdots \\ m_1 \tilde{V}_S = 0 \end{cases} \quad (3.5)$$

$$\begin{cases} m_1 \tilde{V}_{S+1} - m_2 \tilde{V}'_{S+1} = 0 \\ \vdots \\ m_1 \tilde{V}_{N_{1-1}} - m_2 \tilde{V}'_{N_{1-1}} = 0 \end{cases} \quad (3.6)$$

de (3.4) e (3.6) temos,

$$\begin{cases} 2m_1 \tilde{V}_{S+1} = -m_{3,1} \\ \vdots \\ 2m_1 \tilde{V}_{N_{1-1}} = -m_{3, N_{1-1} - S} \end{cases}$$

isto é, as componentes de m_3 são todas nulas ou números pares. Desde que $m_3 \in \{0, 1, -1\}^{N_{1-1} - S}$, temos que $m_3 = 0^{N_{1-1} - S}$. Desta forma obtemos o seguinte sistema,

$$\begin{cases} m_1 \tilde{V}_{S+1} = -m_2 \tilde{V}'_{S+1} \\ \vdots \\ m_1 \tilde{V}_{N_{1-1}} = -m_2 \tilde{V}'_{N_{1-1}} \end{cases} \quad (3.7)$$

de (3.7) e (3.6) temos,

$$\mathbf{m}_2' \mathbf{D}'_{1-1} = \mathbf{0}^{N_{1-1}-S} \quad (3.8)$$

onde,

$$\mathbf{D}'_{1-1} = (\tilde{\mathbf{V}}'_{S+1}, \dots, \tilde{\mathbf{V}}'_{N_{1-1}})$$

De (3.6) e (3.8) temos,

$$\begin{cases} \mathbf{m}_1' \tilde{\mathbf{V}}'_{S+1} = 0 \\ \vdots \\ \mathbf{m}_1' \tilde{\mathbf{V}}'_{N_{1-1}} = 0 \end{cases} \quad (3.9)$$

De (3.5) e (3.9) obtemos,

$$\mathbf{m}_1' \mathbf{D}'_{1-1} = \mathbf{0}^{N_{1-1}} \quad (3.10)$$

Pelo teorema 3.1, $\mathbf{m}_1' = \mathbf{0}^{T_{1-1}}$. Agora, se \mathbf{m}_2 não é o vetor nulo, podemos formar um vetor \mathbf{m}_2' inserindo 0 nas posições do vetor \mathbf{m}_2 correspondente as posições que foram apagadas nos vetores $\tilde{\mathbf{V}}_j$ e desde que de (3.8) $\mathbf{m}_2' \mathbf{D}'_{1-1} = \mathbf{0}^{N_{1-1}-S}$ isto implica que $\mathbf{m}_2' \mathbf{D}'_{1-1} = \mathbf{0}^{N_{1-1}}$. Então do teorema 3.1, $\mathbf{m}_2' = \mathbf{0}^{T_{1-1}}$ e portanto \mathbf{m}_2 também é igual ao vetor nulo. Desta forma temos que $\mathbf{m} = \mathbf{0}^{T_{1S}}$ e, novamente do teorema 3.1, a matriz \mathbf{D}'_{1S} define um código univocamente decodificável. ■

Exemplo 3.5. : Considere a seguinte matriz diferença para um código 8 - usuários univocamente decodificável

$$\mathbf{D}_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 0 & 1 & 0 \\ 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 0 & -1 & 0 \\ 1 & -0 & -0 & -0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Seja $S = 1$. Apagando a segunda coluna de \mathbf{D}_2 , então de acordo com o

teorema 3.4 a 4^a, 5^a e 8^a linhas devem ser removidas. A matriz resultante é :

$$D'_{2,1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & 1 & 0 \\ 1 & -1 & -0 \\ 1 & 0 & 0 \end{bmatrix}$$

Um outro processo iterativo pode ser obtido da seguinte maneira. Seja $K_0 = [1]$, $M_0 = [1 0]$ e

$$K_{i-1} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1, N_{i-1}} \\ \vdots & \vdots & & \vdots \\ k_{T_{i-1}, 1} & k_{T_{i-1}, 2} & \dots & k_{T_{i-1}, N_{i-1}} \end{bmatrix}$$

$$M_{i-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ & & \vdots & & & & & \vdots & \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

$\xleftarrow{2^i}$

 \updownarrow
 2^{i-1}

então podemos definir um novo processo iterativo através da seguinte matriz,

$$K_i = \begin{bmatrix} k_{11} & k_{11} & k_{12} & k_{12} & \dots & k_{1, N_{i-1}} & k_{1, N_{i-1}} \\ k_{11} & -k_{11} & k_{12} & -k_{12} & \dots & k_{1, N_{i-1}} & -k_{1, N_{i-1}} \\ \vdots & & \vdots & & & \vdots & \\ k_{T_{i-1}, 1} & k_{T_{i-1}, 1} & k_{T_{i-1}, 2} & k_{T_{i-1}, 2} & \dots & k_{T_{i-1}, N_{i-1}} & k_{T_{i-1}, N_{i-1}} \\ k_{T_{i-1}, 1} & -k_{T_{i-1}, 1} & k_{T_{i-1}, 2} & -k_{T_{i-1}, 2} & \dots & k_{T_{i-1}, N_{i-1}} & -k_{T_{i-1}, N_{i-1}} \\ \hline & & & & & M_{i-1} & \end{bmatrix}$$

para $i \geq 1$.

Por exemplo, para $i = 1$ temos,

$$K_1 = \begin{bmatrix} k_{11} & k_{11} \\ k_{11} & -k_{11} \\ & M_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 0 \end{bmatrix}$$

A matriz K_1 é igual a matriz D_1 do teorema 3.2. Em geral as matrizes obtidas através deste processo iterativo são equivalentes às matrizes obtidas no teorema 3.2 por permutações de linhas e colunas.

O seguinte exemplo ilustra este fato. Para $i = 2$, K_2 é a seguinte matriz,

$$K_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

permutando a 2ª e 3ª colunas temos,

$$K'_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

permutando a 2ª e 3ª linhas temos,

$$K''_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

permutando a 3ª e 5ª linhas temos,

$$K_2''' = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

finalmente permutando-se a 4ª e 5ª linhas obtemos a matriz D_2 ,

$$K_2'''' = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = D_2$$

Desta forma as matrizes K_1 são matrizes diferenças que definem códigos T_1 - usuários univocamente decodificáveis de comprimento N_1 .

3.3 Generalização dos Códigos de Chang e Weldon [2]

O seguinte teorema, devido a Ferguson [2] generaliza, de modo iterativo os códigos de Chang e Weldon [1].

Teorema 3.5 : Seja D a matriz diferença de um códigos T - usuários univocamente decodificável de comprimento N . Sejam A e B matrizes $N \times N$ sobre $\{0, 1, -1\}$ tais que $\overline{A + B}$ é inversível, onde a barra se refere a soma modulo 2. Então,

$$\hat{D} = \begin{bmatrix} D & D \\ D & -D \\ A & B \end{bmatrix}$$

é a matriz diferença de um código $(2T + N)$ - usuários univocamente decodificável de comprimento $2.N$.

Demonstração : Seja m um vetor sobre o conjunto $\{0, 1, -1\}$ de com

primento $(2T + N)$ e vamos escreve-lo como $m = (m^1, m^2, m^3)$ onde m^1 e m^2 são vetores de comprimento T e m^3 é um vetor de comprimento N . Se $m.D = 0$ então,

$$0 = m^1 D + m^2 D + m^3 A \quad (3.11a)$$

$$0 = m^1 D - m^2 D + m^3 B \quad (3.11b)$$

Então $0 = 2m^1 D + m^3(A + B)$ e, desta forma, tomando a soma módulo 2, temos que $0 = \overline{m^3(A + B)}$. Desde que $\overline{A + B}$ é uma matriz binária inversível, temos que $\overline{m^3} = 0$ e, portanto, $m^3 = 0$ e segue de (3.11a) e (3.11b) que $m^1 D = 0$ e $m^2 D = 0$ e desde que D é uma matriz diferença de um código univocamente decodificável segue, do teorema 3.1 que $m^1 = m^2 = 0$. Então $m.\check{D} = 0$ implica $m = 0$, portanto, pelo teorema 3.1 temos que a matriz \check{D} define um código univocamente decodificável. ■

Tomando $D = D_j$ do teorema 3.2 obtemos o seguinte corolário.

Corolário 3.2 : Seja $D_0 = [1]$ e defina

$$D_j(D_{j-1}, A, B) = \begin{bmatrix} D_{j-1} & D_{j-1} \\ D_{j-1} & -D_{j-1} \\ A & B \end{bmatrix}$$

Para $\overline{A + B} \in GL(N, 2)$ obtemos um conjunto de códigos $\{((j + 2).2^{j-1}) - \text{usuários univocamente decodificáveis de comprimento } 2^j, \text{ onde } j \text{ é um inteiro não negativo e } GL(N, 2) \text{ denota o conjunto das matrizes não singulares sobre } GF(2)\}$.

Como exemplo, tome $j = 1$, $A = [0]$ e $B = [1]$, então,

$$D_1(D_0, A, B) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 1 \end{bmatrix}$$

A seguir mostraremos como Ferguson [2] generalizou os códigos de Chang e Weldon via a noção de classes de equivalência.

Definição 3.3 : Uma matriz P de ordem $K \times K$ é chamada de matriz de permutação generalizada se cada linha e coluna de P contém somente uma entrada não nula que pode ser 1 ou -1.

O conjunto de matrizes de permutações generalizadas de ordem $K \times K$ forma um grupo multiplicativo de ordem $K!.2^K$ conforme mostra o lema abaixo.

Lema 3.4 : O conjunto das matrizes de permutações generalizadas de ordem $K \times K$ forma um grupo multiplicativo de ordem $K!.2^K$.

Demonstração : É claro que o produto de duas matrizes de permutações generalizadas é uma matriz de permutação generalizada e, portanto, a multiplicação de matrizes é uma operação bem definida neste conjunto. A matriz identidade de ordem $K \times K$ é obviamente uma matriz de permutação generalizada. Além disto toda matriz de permutação generalizada de ordem $K \times K$ é inversível, pois tem $\text{rank} = K$. Para concluirmos a primeira afirmação do lema basta mostrarmos que a inversa de uma matriz de permutação generalizada é uma matriz de permutação generalizada. Seja P uma matriz de permutação generalizada de ordem $K \times K$ e seja P' a sua matriz simétrica, isto é, $P'_{ij} = P_{ji}$, $i, j = 1, 2, \dots, K$. É claro que P' é uma matriz de permutação generalizada e é fácil ver que $P.P' = P'.P = I$.

Para provarmos a segunda afirmação do lema veremos de quantas maneiras podemos formar uma matriz de permutação generalizada. Cada linha de uma matriz P pode ser preenchida de 2^K maneiras distintas e esta linha pode ser colocada em K posições diferentes, desta forma temos $2^K.K$ maneiras distintas para formar uma linha da matriz P . Escolhida uma posição para a primeira linha sobram $K - 1$ posições diferentes para colocarmos a segunda linha e, portanto existem $2^K.K.(K-1)$ distintas formas para formarmos duas linhas da matriz P . Continuando com este raciocínio vemos que existem $2^K.(K-1).(K-2). \dots . 2.1 = 2^K.K!$ maneiras distintas para obtermos o conjunto de matrizes de permutações generalizadas, isto é, este conjunto tem $K!.2^K$ elementos. ■

Teorema 3.6 : Seja D uma matriz diferença $T \times N$ de um código T - usuários univocamente decodificável. Sejam P e Q matrizes de permutações generalizadas de ordem $T \times T$ e $N \times N$, respectivamente. Então $D^1 = P.D.Q$ é uma matriz diferença $T \times N$ para um código T - usuários univocamente decodificável.

Demonstração : Desde que D tem entradas no conjunto $\{0, 1, -1\}$ e P e Q são matrizes de permutações generalizadas segue que D^1 também tem entradas no conjunto $\{0, 1, -1\}$ isto é, D^1 é uma matriz diferença. Para

determinar se D^1 define um código univocamente decodificável, seja \mathbf{m} um vetor sobre $\{0, 1, -1\}$ de comprimento T tal que $\mathbf{0} = \mathbf{m} \cdot D^1 = \mathbf{m} \cdot P \cdot D \cdot Q$, desde que Q é inversível, lema 3.4, segue que $\mathbf{0} = \mathbf{m} P D$. Agora D define um código univocamente decodificável e, portanto, do teorema 3.1 segue que $\mathbf{m} \cdot P = \mathbf{0}$ e, desta forma temos que $\mathbf{m} = \mathbf{0}$, logo do teorema 3.1 temos que D^1 define um código univocamente decodificável. ■

Exemplo 3.6 : Seja $D = D_1$ a matriz diferença do exemplo 3.1 e sejam P e Q matrizes de permutações generalizadas de ordem 3 e 2, respectivamente, dadas por,

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

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

então,

$$D^1 = P D_1 Q = \begin{bmatrix} 1 & 1 \\ 0 & -1 \\ -1 & 1 \end{bmatrix}$$

é a matriz diferença de um código 3 - usuários univocamente decodificável de comprimento 2. As matrizes D^1 e D_1 são chamadas matrizes equivalentes e os códigos por elas geradas, códigos equivalentes.

As operações de multiplicação descritas acima definem uma dupla ação de grupo sobre as matrizes diferença D , [5] pp. 104 e, portanto, uma relação de equivalência. É mostrado em [2] que o número de códigos distintos que são equivalentes ao código gerado pela matriz D é $T! \cdot (N - 1)! \cdot 2^{T+N-1}$.

3.4 Os Códigos de Wilson, [3]

Nesta seção é apresentada uma classe de códigos corretores de erros obtida por Wilson [3].

O canal aditivo com ruído pode ser modelado como o canal aditivo

T - usuários sem ruído, em cascata com um canal discreto sem memória (DMC) tendo probabilidades de transições diferentes de zero para todos os possíveis pares de entradas e saídas.

Seja

$$Z = (z_1, z_2, \dots, z_N) = \sum_{i=1}^N Z_i$$

onde $z_i \in \{0, 1, 2, \dots, T\}$ e Z_i é uma palavra código do i - ésimo código constituinte. Defina Z' similarmente com a restrição de que o conjunto de palavras-código binárias constituintes de Z' , isto é, $(Z'_1, Z'_2, \dots, Z'_T)$, seja distinto de Z , isto é, $\neq (Z_1, Z_2, \dots, Z_T)$.

A L-distância entre os dois vetores Z e Z' é:

$$d_L(Z, Z') = \sum_{i=1}^N |z_i - z'_i| = || Z - Z' ||$$

O L-peso de Z é simplesmente a soma dos valores absolutos de suas coordenadas.

A L-distância mínima, d_{\min} , de um código T - usuários é o menor valor de $d_L(Z, Z')$ sobre todos os pares (Z, Z') com $Z \neq Z'$.

O número de erros de transmissão é definido como sendo a L-distância entre a palavra código transmitida Z e a saída do canal U , isto é,

$$e(Z, U) = || Z - U ||$$

O seguinte teorema é uma generalização do teorema 3.3 e permitiu Wilson [3] obter uma classe de códigos corretores de erros para o canal aditivo binário T - usuáries.

Teorema 3.7 : Seja B uma matriz $q \times q$ sobre $\{0, 1, -1\}$ para a qual existe uma matriz A sobre $\{0, 1, -1\}$ tal que $A.B = dI$, onde d é um inteiro positivo e I é a matriz identidade. Seja D_0 a matriz diferença para um código T - usuários de comprimento N e distância mínima d_0 . Então o produto de Kronecker $B \otimes D_0$ é a matriz diferença para um código qT - usuários de comprimento qN com uma distância mínima de pelo menos $d \cdot d_0$.

Exemplo 3.7 : Seja D_1 a matriz diferença do código 3-usuários univocamente decodificável do exemplo 3.1, isto é,

$$D_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 0 \end{bmatrix}$$

e seja H_4 a matriz de Hadamard de ordem 4, dada por,

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

é fácil ver que $H_4 \cdot H_4^t = 4 \cdot I$, onde H_4^t denota a matriz transposta de H_4 e I é a matriz identidade de ordem 4. Então, segundo o teorema 3.5, o produto de Kronecker $H_4 \otimes D_1$ dada por,

$$H_4 \otimes D_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \end{bmatrix}$$

é a matriz diferença de um código 12 - usuários de comprimento $N = 8$ e distância mínima $d_{\min} = 4$, cujos códigos constituintes são:

$$\begin{aligned} C_1 &= \{ X_1 = (1, 1, 1, 1, 1, 1, 1, 1); Y_1 = (0, 0, 0, 0, 0, 0, 0, 0) \} \\ C_2 &= \{ X_2 = (1, 0, 1, 0, 1, 0, 1, 0); Y_2 = (0, 1, 0, 1, 0, 1, 0, 1) \} \\ C_3 &= \{ X_3 = (1, 0, 1, 0, 1, 0, 1, 0); Y_3 = (0, 0, 0, 0, 0, 0, 0, 0) \} \\ C_4 &= \{ X_4 = (1, 1, 0, 0, 1, 1, 0, 0); Y_4 = (0, 0, 1, 1, 0, 0, 1, 1) \} \\ C_5 &= \{ X_5 = (1, 0, 0, 1, 1, 0, 0, 1); Y_5 = (0, 1, 1, 0, 0, 1, 1, 0) \} \\ C_6 &= \{ X_6 = (1, 0, 0, 0, 1, 0, 0, 0); Y_6 = (0, 0, 1, 0, 0, 0, 1, 0) \} \\ C_7 &= \{ X_7 = (1, 1, 1, 1, 0, 0, 0, 0); Y_7 = (0, 0, 0, 0, 1, 1, 1, 1) \} \end{aligned}$$

$$C_8 = \{ X_8 = (1, 0, 1, 0, 0, 1, 0, 1); Y_8 = (0, 1, 0, 1, 1, 0, 1, 0) \}$$

$$C_9 = \{ X_9 = (1, 0, 1, 0, 0, 0, 0, 0); Y_9 = (0, 0, 0, 0, 1, 0, 1, 0) \}$$

$$C_{10} = \{ X_{10} = (1, 1, 0, 0, 0, 0, 1, 1); Y_{10} = (0, 0, 1, 1, 1, 1, 0, 0) \}$$

$$C_{11} = \{ X_{11} = (1, 0, 0, 1, 0, 1, 1, 0); Y_{11} = (0, 1, 1, 0, 1, 0, 0, 1) \}$$

$$C_{12} = \{ X_{12} = (1, 0, 0, 0, 0, 0, 1, 0); Y_{12} = (0, 0, 1, 0, 1, 0, 0, 0) \}$$

A tabela 3.3 apresenta uma lista de parâmetros não exaustiva para a classe de códigos de Wilson.

Tabela 3.3

J	q	T	N	d _{min}	R _{sum} (T)
0	2	2	2	2	1
0	4	4	4	4	1
0	8	8	8	8	1
0	12	12	12	12	1
0	16	16	16	16	1
0	24	24	24	24	1
⋮	⋮	⋮	⋮	⋮	⋮
1	2	6	4	2	1.5
1	4	12	8	4	1.5
1	8	24	16	8	1.5
1	12	36	24	12	1.5
1	16	48	32	16	1.5
1	24	72	48	24	1.5
⋮	⋮	⋮	⋮	⋮	⋮
2	2	16	8	2	2
2	4	32	16	4	2
2	8	64	32	8	2
2	12	96	48	12	2
2	16	128	64	16	2
2	24	192	96	24	2
⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮

3.5 Algoritmos de Decodificação

3.5.1. Algoritmo de decodificação de Chang e Weldon

Para os códigos iterativos do Teorema 3.2. Chang e Weldon [1] apresentam um método sistemático para decodificar o vetor transmitido do vetor recebido.

Seja $Z = Z_1 + Z_2 + \dots + Z_T$, $Z_i \in C_i$, onde C_i é o i -ésimo código constituinte e seja $Y = Y_1 + Y_2 + \dots + Y_T$, $Y_i \in C_i$. Então podemos representar a diferença $S = Z - Y$ em termos dos T vetores diferença, $d_i = X_i - Y_i$, $i = 1, 2, \dots, T$,

$$S = Z - Y = \sum_{i=1}^T (Z_i - Y_i) = \sum_{i=1}^T \lambda_i d_i$$

onde $C_i = \{ X_i, Y_i \}$ e,

$$\lambda_i = \begin{cases} 1, & \text{se } Z_i = X_i \\ 0, & \text{se } Z_i = Y_i \end{cases} \quad (3.12)$$

Isto pode ser expresso em termos da matriz diferença D da seguinte forma,

$$S = Z - Y = \lambda D \quad (3.13)$$

onde $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_T)$.

Desde que Y é um vetor fixado, cada saída Z tem um vetor S univocamente especificado por Z . O papel de S na decodificação do canal múltiplo-acesso é similar a síndrome do caso clássico a um usuário, por esta razão chamaremos S de síndrome.

Em virtude da existência de uma correspondência biunívoca entre as T -uplas binárias $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_T)$ e os conjuntos de palavras códigos (Z_1, Z_2, \dots, Z_T) que geram a palavra Z na saída do canal aditivo T -usuários, o seguinte lema é verdadeiro.

Lema 3.5 : Dado um código T -usuário univocamente decodificável o vetor Z na saída do canal aditivo T -usuários é univocamente determinado pela T -upla binária $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_T)$.

O problema de decodificação é achar o vetor binário λ que satisfaça a equação (3.13). O algoritmo de decodificação apresentado por Chang e Weldon se utiliza da estrutura simétrica dos códigos gerados pela matriz diferença dada em 3.1. A idéia básica é decodificar o código com índice J primeiro decodificando os dois códigos com índices $J-1$. Repetindo este processo J vezes decodificamos o código T_J - usuários. Este processo é apresentado a seguir.

Assuma que Z é a saída do canal e $S = Z - Y$ é a síndrome correspondente. Então Z pode ser decodificado usando-se o seguinte processo para resolver a equação $S^{(j)} = \lambda^{(j)} D_j$.

Seja $S = S^{(j)}$ a síndrome inicial, isto é,

$$S^{(j)} = S = Z - Y \quad (3.14)$$

então particionando $S^{(j)}$ em duas 2^{j-1} - uplas obtemos,

$$S^{(j)} = (S_1^{(j-1)}, S_2^{(j-1)}) \quad (3.15)$$

seja $\lambda^{(j)}$ o vetor solução da equação,

$$\lambda^{(j)} D_j = S^{(j)} \quad (3.16)$$

e particionemos $\lambda^{(j)}$ em três partes,

$$\lambda^{(j)} = (\lambda_1^{(j-1)}, \lambda_2^{(j-1)}, \lambda_3^{(j-1)}) \quad (3.17)$$

cujos comprimentos são, T_{j-1} , T_{j-1} e 2^{j-1} , respectivamente, onde $T_{j-1} = (j+1) \cdot 2^{j-2}$. Das equações (3.15), (3.16) e (3.17) obtemos o seguinte sistema de equações,

$$\begin{cases} \lambda_1^{(j-1)} D_{j-1} + \lambda_2^{(j-1)} D_{j-1} + \lambda_3^{(j-1)} I_{j-1} = S^{(j-1)} & (I) \\ \lambda_1^{(j-1)} D_{j-1} - \lambda_2^{(j-1)} D_{j-1} = S_2^{(j-1)} & (II) \end{cases}$$

somando as equações (I) e (II) obtemos,

$$2\lambda_1^{(j-1)} D_{j-1} + \lambda_3^{(j-1)} I_{j-1} = S_1^{(j-1)} + S_2^{(j-1)} \quad (3.18)$$

tomando a soma modulo 2 e observando que $\lambda_3^{(j-1)} I_{j-1} = \lambda_3^{(j-1)}$, obtemos,

$$\lambda_3^{(j-1)} \equiv S_1^{(j-1)} + S_2^{(j-1)} \pmod{2} \quad (3.19)$$

Por outro lado da equação (3.18) temos,

$$\lambda_1^{(j-1)} D_{j-1} = (S_1^{(j-1)} + S_2^{(j-1)} - \lambda_3^{(j-1)})/2 \quad (3.20)$$

substituindo (3.20) na equação (II) obtemos,

$$\lambda_2^{(j-1)} D_{j-1} = (S_1^{(j-1)} - S_2^{(j-1)} - \lambda_3^{(j-1)})/2 \quad (3.21)$$

A equação (3.19) nos dá o valor de $\lambda_3^{(j-1)}$ e com ele podemos tornar conhecidos os lados direitos das equações (3.20) e (3.21) que serão denominados de síndromes inferiores dos seguintes ramos:

Ramo 1: Seja a nova síndrome $S^{(j-1)} = \lambda_1^{(j-1)} D_{j-1}$. Então de (3.20) temos,

$$S^{(j-1)} = (S_1^{(j-1)} + S_2^{(j-1)} - \lambda_3^{(j-1)})/2$$

particionando $S^{(j-1)}$ em duas $2^{(j-2)}$ - uplas, como em (3.15) temos,

$$S^{(j-1)} = (S_1^{(j-2)}, S_2^{(j-2)})$$

e seja,

$$\lambda_1^{(j-1)} = (\lambda_1^{(j-2)}, \lambda_2^{(j-2)}, \lambda_3^{(j-2)}) = \lambda^{(j-1)}$$

cujos comprimentos são T_{j-2} , T_{j-2} e 2^{j-2} , respectivamente, onde $T_{j-2} = j \cdot 2^{j-3}$. Então (3.20) torna-se,

$$\lambda_{j-1} D_{j-1} = S^{(j-1)}$$

que é igual a (3.16) substituindo j por $j - 1$.

Ramo 2: Analogamente, seja a nova síndrome $S^{(j-1)} = \lambda_2^{(j-1)} D_{j-1}$. Da equação (3.21) vemos que,

$$S^{(j-1)} = (S_1^{(j-1)} - S_2^{(j-1)} - \lambda_3^{(j-1)})/2$$

procedendo como no ramo 1 obtemos uma equação idêntica a (3.16) com j substituído por $j - 1$.

Continuando com este processo $j -$ vezes, no nível j , $\lambda_3^{(0)}$ tem uma única componente que pode ser obtida através da equação (3.19) e $\lambda_1^{(0)}$, $\lambda_2^{(0)}$ podem ser obtidos através das seguintes equações,

$$\begin{aligned} \lambda_1^{(0)} &= (S_1^{(0)} + S_2^{(0)} - \lambda_3^{(0)})/2 \\ \lambda_2^{(0)} &= (S_1^{(0)} - S_2^{(0)} - \lambda_3^{(0)})/2 \end{aligned} \quad (3.22)$$

Conhecidos $\lambda_1^{(0)}$ e $\lambda_2^{(0)}$, podemos determinar todos os λ_1 e λ_2 dos níveis superiores e concluir o processo de decodificação.

Exemplo 3.8 : Considere o código 3 - usuários do exemplo 3.1 e seja $Z = X_1 + Y_2 + X_3 = (2, 2)$ a palavra recebida. Temos que $Y = Y_1 + Y_2 + Y_3 = (0, 1)$ e a síndrome $S = Z - Y = (2, 1)$. Desejamos encontrar a solução da equação $S^{(1)} = \lambda^{(1)} D_1$. Particionando $S^{(1)}$ em duas novas síndromes $S^{(1)} = (S_1^{(0)}, S_2^{(0)})$ de comprimento $2^0 = 1$, isto é, $S_1^{(0)} = 2$ e $S_2^{(0)} = 1$. Da equação (3.19) temos,

$$\lambda_3 \equiv S_1^{(0)} + S_2^{(0)} \pmod{2} = 2 + 1 \pmod{2} = 1$$

Conhecido λ_3 podemos determinar λ_1 e λ_2 através das equações,

$$\begin{aligned} \lambda_1 &= (S_1^{(0)} + S_2^{(0)} - \lambda_3)/2 = (2 + 1 - 1)/2 = 1 \\ \lambda_2 &= (S_1^{(0)} - S_2^{(0)} - \lambda_3)/2 = (2 - 1 - 1)/2 = 0 \end{aligned}$$

e desta forma temos que o vetor binário $\lambda = (\lambda_1, \lambda_2, \lambda_3) = (1, 0, 1)$ e os vetores dos códigos constituintes, de acordo com a equação (3.12), são: $Z_1 = X_1$, $Z_2 = Y_2$, $Z_3 = X_3$.

Exemplo 3.9 : Para $j = 2$ a matriz diferença D_2 ,

$$D_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

gera o código 8 - usuários de comprimento $N = 2^2 = 4$ univocamente decodificável, cujos códigos constituintes são:

$$C_1 = \{ X_1 = (1, 1, 1, 1); Y_1 = (0, 0, 0, 0) \}$$

$$C_2 = \{ X_2 = (1, 0, 1, 0); Y_2 = (0, 1, 0, 1) \}$$

$$C_3 = \{ X_3 = (1, 0, 1, 0); Y_3 = (0, 0, 0, 0) \}$$

$$C_4 = \{ X_4 = (1, 1, 0, 0); Y_4 = (0, 0, 1, 1) \}$$

$$C_5 = \{ X_5 = (1, 0, 0, 1); Y_5 = (0, 1, 1, 0) \}$$

$$C_6 = \{ X_6 = (1, 0, 0, 0); Y_6 = (0, 0, 1, 0) \}$$

$$C_7 = \{ X_7 = (1, 0, 0, 0); Y_7 = (0, 0, 0, 0) \}$$

$$C_8 = \{ X_8 = (0, 1, 0, 0); Y_8 = (0, 0, 0, 0) \}$$

Suponha que a palavra recebida seja $Z = X_1 + X_2 + Y_3 + Y_4 + X_5 + X_6 + Y_7 + Y_8 = (4, 1, 3, 3)$. O problema de determinar os vetores constituintes a partir da palavra recebida Z se resume em determinar o vetor binário $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8)$ que satisfaça a equação (3.13). Primeiro a síndrome $S = Z - Y$ é calculada, onde $Y = Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7 + Y_8 = (0, 2, 3, 2)$. Então $S = (4, -1, 0, 1)$ é particionada em duas novas síndromes de comprimento 2, isto é, $S_1^{(1)} = (4, -1)$ e $S_2^{(1)} = (0, 1)$. Particionemos o vetor $\lambda^{(2)}$ da equação (3.16) em tres partes, $\lambda^{(2)} = (\lambda_1^{(i)}, \lambda_2^{(i)}, \lambda_3^{(i)})$ de comprimentos $T_1 = (2+1) \cdot 2^0 = 3$, $T_2 = 3$ e 2^1 , respectivamente. Da equação (3.19) temos:

$$\lambda_3^{(1)} = S_1^{(1)} + S_2^{(1)} \pmod{2} = (0, 0)$$

e desta forma podemos tornar conhecidos os lados direitos das equações (3.20) e (3.21), isto é,

$$\lambda_1^{(1)} D_1 = (S_1^{(1)} + S_2^{(1)} - \lambda_3^{(1)})/2 = (2, 0)$$

$$\lambda_2^{(1)} D_1 = (S_1^{(1)} - S_2^{(1)} - \lambda_3^{(1)})/2 = (2, -1)$$

que serão denominadas síndromes inferiores dos seguintes ramos:

Ramo 1: Seja a nova síndrome $S^{(1)} = \lambda_1^{(1)} D_1 = (2, 0)$. Particionemos $S^{(1)}$ em duas novas síndromes de comprimento $2^{(j-2)} = 1$, isto é,

$$S^{(1)} = (S_1^{(0)}, S_2^{(0)}) = (2, 0)$$

e seja $\lambda_1^{(1)} = (\lambda_1^{(0)}, \lambda_2^{(0)}, \lambda_3^{(0)}) = \lambda^{(1)}$. Então de acordo com a equação (3.19) temos,

$$\lambda_3^{(0)} \equiv S_1^{(0)} + S_2^{(0)} \pmod{2} = 0$$

e desde que neste nível $\lambda_3^{(0)}$ tem uma única componente, $\lambda_1^{(0)}$ e $\lambda_2^{(0)}$ podem ser obtidos das equações (3.22), isto é,

$$\lambda_1^{(0)} = (S_1^{(0)} + S_2^{(0)} - \lambda_3^{(0)})/2 = (2 + 0 - 0)/2 = 1$$

$$\lambda_2^{(0)} = (S_1^{(0)} - S_2^{(0)} - \lambda_3^{(0)})/2 = (2 - 0 - 0)/2 = 1$$

Ramo 2: Analogamente, seja a nova síndrome $S^{(1)} = \lambda_2^{(1)} D_1 = (2, -1)$. Particionemos $S^{(1)}$ em duas novas síndromes de comprimento $2^0 = 1$, isto é,

$$S^{(1)} = (S_1^{(0)}, S_2^{(0)}) = (2, -1)$$

e seja $\lambda_2^{(1)} = (\lambda_1^{(0)}, \lambda_2^{(0)}, \lambda_3^{(0)})$ então de acordo com a equação (3.19) temos,

$$\lambda_3^{(0)} \equiv S_1^{(0)} + S_2^{(0)} \pmod{2} = 1$$

e novamente, das equações (3.22) temos,

$$\lambda_1^{(0)} = (S_1^{(0)} + S_2^{(0)} - \lambda_3^{(0)})/2 = (2 - 1 - 1)/2 = 0$$

$$\lambda_2^{(0)} = (S_1^{(0)} - S_2^{(0)} - \lambda_3^{(0)})/2 = (2 + 1 - 1)/2 = 1$$

Neste nível o vetor λ é completamente determinado reconstituindo-se todos os níveis do processo de decodificação, isto é, $\lambda = \lambda^{(2)} = (\lambda_1^{(1)}, \lambda_2^{(1)}, \lambda_3^{(1)}) = (1, 1, 0, 0, 1, 1, 0, 0)$ e de acordo com (3.12) os vetores constituintes são: $Z_1 = X_1$, $Z_2 = X_2$, $Z_3 = Y_3$, $Z_4 = Y_4$, $Z_5 = X_5$, $Z_6 = X_6$, $Z_7 = Y_7$, $Z_8 = Y_8$.

3.5.2. Algoritmo de decodificação de Wilson

Nesta seção ilustraremos, através de um exemplo, o algoritmo de decodificação apresentado por Wilson, [3].

Exemplo 3.10 : Considere o código 12 - usuários dado no exemplo 3.7 e seja $Z = X_1 + X_2 + X_3 + X_4 + Y_5 + Y_6 + Y_7 + Y_8 + X_9 + X_{10} + X_{11} + X_{12} = (8, 5, 6, 3, 6, 5, 10, 3)$ o vetor transmitido. Assuma que o vetor recebido seja $U = (7, 6, 6, 3, 6, 5, 10, 3)$. Então vemos que o vetor recebido difere do vetor transmitido nas posições 1 e 2, em um erro de magnitude 1 por bit. Como em [3], primeiro a síndrome $S = U - Y$ é calculada, onde $Y = Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7 + Y_8 + Y_9 + Y_{10} + Y_{11} + Y_{12} = (0, 4, 6, 4, 6, 4, 6, 4)$. Então $S = (7, 2, 0, -1, 0, 1, 4, -1)$ é particionada em $q = 4$ segmentos de comprimento $N = 2$, onde q é a ordem da matriz de Hadamard e N é o comprimento do código univocamente decodificável gerado pela matriz D_1 . Estes segmentos são arranjados em uma matriz 4×2 que tem estes quatros segmentos como linhas, isto é,

$$M = \begin{bmatrix} 7 & 2 \\ 0 & -1 \\ 0 & 1 \\ 4 & -1 \end{bmatrix}$$

Multiplicando à esquerda pela matriz de Hadamard H_4 temos,

$$H_4 \cdot M = \begin{bmatrix} 11 & 1 \\ 3 & 5 \\ 3 & 1 \\ 11 & 1 \end{bmatrix}$$

e desde que as entradas desta matriz não são múltiplas de $q = 4$, isto deve-se aos erros ocorridos nas posições 1 e 2, a correção mais provável é obtida trocando-se as entradas da matriz pelo múltiplo de $q = 4$ mais próximo, isto é,

$$H_4 \cdot M_{SZ} = \begin{bmatrix} 12 & 0 \\ 4 & 4 \\ 4 & 0 \\ 12 & 0 \end{bmatrix} = 4 \cdot \begin{bmatrix} 3 & 0 \\ 1 & 1 \\ 1 & 0 \\ 3 & 0 \end{bmatrix}$$

dividindo as entradas desta nova matriz por $q = 4$ obtemos as síndromes no nível D_1 e neste ponto utilizamos o algoritmo de decodificação de Chang e Weldon para determinarmos quais as palavras códigos dos códigos constituintes C_i , $i = 1, 2, \dots, T = 12$ foram adicionadas para formar a palavra transmitida Z . Para isto considere o seguinte sistema matricial de equações,

$$\begin{bmatrix} \lambda_{z1} D_1 \\ \lambda_{z2} D_1 \\ \lambda_{z3} D_1 \\ \lambda_{z4} D_1 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 1 & 1 \\ 1 & 0 \\ 3 & 0 \end{bmatrix}^t \quad (3.23)$$

onde λ_{z1} , $i = 1, 2, 3$ são os vetores binários de comprimento 3 no nível D_1 da equação 3.13 e $[]^t$ denota a matriz transposta. Seja $\lambda_{z1} = (\lambda_{11}, \lambda_{12}, \lambda_{13})$, $i = 1, 2, 3, 4$ e desenvolvendo o lado esquerdo de (3.23) obtemos os seguintes sistemas de equações:

$$(I) \quad \begin{cases} \lambda_{11} + \lambda_{12} + \lambda_{13} = 3 \\ \lambda_{11} - \lambda_{12} = 0 \end{cases}$$

$$(II) \quad \begin{cases} \lambda_{21} + \lambda_{22} + \lambda_{23} = 1 \\ \lambda_{21} - \lambda_{22} = 1 \end{cases}$$

$$(III) \quad \begin{cases} \lambda_{31} + \lambda_{32} + \lambda_{33} = 1 \\ \lambda_{31} - \lambda_{32} = 0 \end{cases}$$

$$(IV) \quad \begin{cases} \lambda_{41} + \lambda_{42} + \lambda_{43} = 3 \\ \lambda_{41} - \lambda_{42} = 0 \end{cases}$$

e as soluções para estes sistemas são obtidas como na seção 3.5.1. Por exemplo, a solução de (I) é encontrada da seguinte forma: seja $S^{(1)} = (S_1^{(0)}, S_2^{(0)}) = (3, 0)$, onde o par $(3, 0)$ é formada pelos elementos do lado direito de (I). Então, de acordo com a equação 3.19

$$\lambda_{13} \equiv S_1^{(0)} + S_2^{(0)} \pmod{2} = 1$$

e das equações (3.22),

$$\lambda_{11} = (S_1^{(0)} + S_2^{(0)} - \lambda_{13})/2 = 1$$

$$\lambda_{12} = (S_1^{(0)} - S_2^{(0)} - \lambda_{13})/2 = 1$$

e, portanto, $\lambda_{z1} = (\lambda_{11}, \lambda_{12}, \lambda_{13}) = (1, 1, 1)$. Analogamente, λ_{z2} pode ser determinado do sistema (II) tomando-se $S^{(1)} = (S_1^{(0)}, S_2^{(0)}) = (1, 1)$ e desta forma obtemos,

$$\lambda_{23} \equiv S_1^{(0)} + S_2^{(0)} \pmod{2} = 0$$

$$\lambda_{21} = (S_1^{(0)} + S_2^{(0)} - \lambda_{23})/2 = 1$$

$$\lambda_{22} = (S_1^{(0)} - S_2^{(0)} - \lambda_{23})/2 = 0$$

e, portanto, $\lambda_{z2} = (\lambda_{21}, \lambda_{22}, \lambda_{23}) = (1, 0, 0)$. Novamente, do sistema (III) faça $S^{(1)} = (S_1^{(0)}, S_2^{(0)}) = (1, 0)$, então,

$$\lambda_{33} \equiv S_1^{(0)} + S_2^{(0)} \pmod{2} = 1$$

$$\lambda_{31} = (S_1^{(0)} + S_2^{(0)} - \lambda_{33})/2 = 0$$

$$\lambda_{32} = (S_1^{(0)} - S_2^{(0)} - \lambda_{33})/2 = 0$$

e desta forma $\lambda_{z3} = (\lambda_{31}, \lambda_{32}, \lambda_{33}) = (0, 0, 1)$. Finalmente, seja $S^{(1)} = (S_1^{(0)}, S_2^{(0)}) = (3, 0)$, então,

$$\lambda_{43} \equiv S_1^{(0)} + S_2^{(0)} \pmod{2} = 1$$

$$\lambda_{41} = (S_1^{(0)} + S_2^{(0)} - \lambda_{43})/2 = 1$$

$$\lambda_{42} = (S_1^{(0)} - S_2^{(0)} - \lambda_{43})/2 = 1$$

e, portanto, $\lambda_{24} = (\lambda_{41}, \lambda_{42}, \lambda_{43}) = (1, 1, 1)$. Com isto conseguimos determinar completamente o vetor binário $\lambda = (\lambda_{z_1}, \lambda_{z_2}, \lambda_{z_3}, \lambda_{z_4}) = (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$. Agora, de acordo com a equação (3.12) as palavras códigos dos códigos constituintes são: $Z_1 = X_1$, $Z_2 = X_2$, $Z_3 = X_3$, $Z_4 = X_4$, $Z_5 = Y_5$, $Z_6 = Y_6$, $Z_7 = Y_7$, $Z_8 = Y_8$, $Z_9 = X_9$, $Z_{10} = X_{10}$, $Z_{11} = X_{11}$ e $Z_{12} = X_{12}$. Desta maneira concluímos o processo de decodificação.

Este algoritmo de decodificação corrige até $t = \lfloor (q-1)/2 \rfloor$ erros por bit em um "burst" de erros consecutivos de comprimento não maior do que o comprimento do código univocamente decodificável definido por D_1 . Neste exemplo $t = \lfloor (4-1)/2 \rfloor = 1$ e, como vimos, o algoritmo foi capaz de corrigir 1 erro por bit em um "burst" de comprimento 2, que é o comprimento do código definido por D_1 .

3.6 Conclusão

Neste capítulo fizemos uma apresentação das classes de códigos univocamente decodificáveis para o canal T - Usuários propostas por Chang e Weldon [1, 11]. Também mostramos a generalização dada por Ferguson [2] para os códigos univocamente decodificáveis de Chang e Weldon. Dando continuidade as pesquisas na busca de códigos para o canal T - Usuários, apresentamos uma classe de códigos corretores de erros obtida por Wilson [3].

Técnicas de decodificações para os esquemas de codificações propostos por Chang e Weldon [1] e Wilson [3] também foram apresentadas.

Capítulo IV

Uma Classe de Códigos Corretores de Erro para o Canal Aditivo T - Usuários

4.1 Introdução

Neste capítulo apresentamos uma classe de códigos para o Canal Aditivo T - Usuários, [28, 29]. Esta classe de códigos é obtida a partir de uma aplicação do teorema de Wilson (Capítulo 3, Teorema 3.7) para a classes de códigos 2 - usuários δ - decodificáveis.

Também é dada uma generalização desta classe de códigos via a noção de classes de equivalência, segundo Ferguson, [2].

4.2 A Classe de Códigos

O corolário abaixo é uma aplicação do teorema 3.7 para matrizes diferença que definam códigos dois usuários δ - decodificáveis, $\delta \geq 2$ e nos permite obter uma classe de códigos corretores de erros para o Canal T - Usuários:

Corolário 4.1 : Seja B uma matriz de ordem q sobre $\{0, 1, -1\}$ para a qual existe uma matriz A sobre $\{0, 1, -1\}$ tal que $A.B = d_0.I$, onde d_0 é um inteiro positivo e I é a matriz identidade. Seja D_0 a matriz diferença de um código 2 - usuários δ - decodificável de comprimento N. Então o produto de Kronecker $B \otimes D_0$ é a matriz diferença para um código $2q$ - usuários de comprimento $q.N$ com L - distância mínima igual a $\delta.d_0$.

Lema 4.1 : Um código T - usuários C tem distância mínima $d_{\min} = d_0$, se e somente se para quaisquer duas palavras códigos $Z \neq Z'$ as suas síndromes $S_Z, S_{Z'}$ distam de pelo menos d_0 , isto é,

$$\|S_Z - S_{Z'}\| \geq d_0.$$

Demonstração : Suponha que C tenha distância mínima $d_{\min} = d_0$, então para quaisquer duas palavras códigos Z e Z' de C, com $Z \neq Z'$ temos,

$$\|S_Z - S_{Z'}\| = \|(Z - Y) - (Z' - Y)\| = \|Z - Z'\| \geq d_0.$$

Análise do Corolário 4.1.

É claro que $B \otimes D_0$ é uma matriz $q.T \times q.N$ sobre $\{0, 1, -1\}$ e portanto define um código $q.T$ - usuários "C" de comprimento $q.N$. Para mostrarmos que C tem distância mínima $\delta.d_0$ mostraremos que dadas duas palavras códigos distintas de C suas síndromes distam de pelo menos $\delta.d_0$, lema 4.1.

Sejam Z e Z' duas palavras códigos de C, com $Z \neq Z'$. Seja Y a soma das Y_i palavras códigos dos i-ésimos códigos constituintes C_i . As síndromes de Z e Z' são, respectivamente, $S_Z = Z - Y$ e $S_{Z'} = Z' - Y$. É possível expressar as síndromes em termos da matriz diferença $B \otimes D_0$ da seguinte maneira: $S_Z = \lambda_Z (B \otimes D_0)$ e $S_{Z'} = \lambda_{Z'} (B \otimes D_0)$, onde λ_Z e $\lambda_{Z'}$ são vetores binários.

Particionemos S_Z e $S_{Z'}$ em q segmentos iguais de comprimento N e λ_Z , $\lambda_{Z'}$ em q segmentos de comprimento T. Desta forma $S_Z = (S_{Z1}, S_{Z2}, \dots, S_{Zq})$, $S_{Z'} = (S_{Z'1}, S_{Z'2}, \dots, S_{Z'q})$, $\lambda_Z = (\lambda_{Z1}, \lambda_{Z2}, \dots, \lambda_{Zq})$ e $\lambda_{Z'} = (\lambda_{Z'1}, \lambda_{Z'2}, \dots, \lambda_{Z'q})$ onde S_{Zi} e $S_{Z'i}$ tem ambos comprimento igual a N e λ_{Zi} , $\lambda_{Z'i}$ tem ambos comprimento igual a T. Seja M a matriz que tem como linhas os segmentos $S_{Zi} - S_{Z'i}$. É possível escrever a equação $S_Z - S_{Z'} = (\lambda_Z - \lambda_{Z'}) (B \otimes D_0)$ na seguinte forma matricial,

$$B^T \cdot \begin{bmatrix} (\lambda_{Z1} - \lambda_{Z'1}) \cdot D_0 \\ \vdots \\ (\lambda_{Zq} - \lambda_{Z'q}) \cdot D_0 \end{bmatrix} = M$$

onde B^T é a matriz transposta de B.

Multiplicando-se ambos os termos à esquerda por A^T e usando a hipótese do teorema temos,

$$d. \begin{bmatrix} (\lambda_{Z1} - \lambda_{Z'1}) \cdot D_0 \\ \vdots \\ (\lambda_{Zq} - \lambda_{Z'q}) \cdot D_0 \end{bmatrix} = A^T \cdot M$$

Desde que $Z \neq Z'$ é verdade que para algum i, $(\lambda_{Zi} - \lambda_{Z'i})$ não é o

vetor nulo. Para este i a linha $(\lambda_{z_1} - \lambda_{z'_1}) \cdot D_0$ tem peso $\geq \delta$, desde que é a síndrome para palavras códigos do código δ -decodificável definido pela matriz D_0 . Desta forma, pelo menos uma linha da matriz $A^T \cdot M$ tem peso $\geq \delta \cdot d_0$.

Por outro lado as entradas da matriz A^{tr} pertencem ao conjunto $\{0, 1, -1\}$ e desta forma a seguinte desigualdade é verdadeira,

$$\begin{aligned} \|S_z - S_{z'}\| &\geq \sum_{j=1}^q \sum_{k=1}^q |m_{jk}| \\ &\geq \sum_{j=1}^q \sum_{k=1}^q |a_{ik} m_{kj}| \geq d_0 \delta, \end{aligned}$$

onde a_{ik} e m_{kj} são as entradas das matrizes A^T e M , respectivamente. ■

A classe de códigos introduzida pelo corolário 4.1 pode ser obtida da seguinte maneira:

Seja H a matriz de Hadamard de ordem q sabemos de [4] que $H \cdot H^T = q \cdot I$, onde H^T denota a matriz transposta de H e I é a matriz identidade de ordem q .

Seja D_0 uma matriz diferença de ordem $2 \times N_0$ que defina um código 2-usuários δ -decodificável de comprimento N_0 . Então de acordo com o corolário 4.1. o produto de Kronecker $H \otimes D_0$ é uma matriz diferença de ordem $2 \cdot q \times N_0 \cdot q$ e, portanto, define um código 2- q -usuários de comprimento $q \cdot N_0$ e distância mínima $q \cdot \delta$.

O seguinte exemplo ilustra este fato.

Exemplo 4.1 : Seja (C_1, C_2) o código dois usuários 4-decodificável de comprimento $N_0 = 4$ dado por $C_1 = \{0000, 1111\}$, $C_2 = \{0011, 1100\}$ e seja D_0 a matriz 2×4 que tem como linha o vetor diferença $d_i = X_i - Y_i$, $i = 1, 2$ onde $C_i = \{X_i, Y_i\}$. Então,

$$D_0 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$$

Seja H_2 a matriz de Hadamard de ordem 2 dada por,

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

então o produto de Kronecker $H_2 \otimes D_0$ é uma matriz diferença de ordem 4×8 dada por,

$$H_2 \otimes D_0 = \begin{bmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \end{bmatrix}$$

e, segundo o corolário 4.1 define um código T - usuários, com $T = 4$ de comprimento $N = 8$ e distância mínima, $d_{\min} = 4.2 = 8$.

Os códigos constituintes do código 4 - usuários, segundo as regras definidas no capítulo 3, são:

$$C_1 = \{X_1 = (0, 0, 0, 0, 0, 0, 0, 0), Y_1 = (1, 1, 1, 1, 1, 1, 1, 1)\}$$

$$C_2 = \{X_2 = (0, 0, 1, 1, 0, 0, 1, 1), Y_2 = (1, 1, 0, 0, 1, 1, 0, 0)\}$$

$$C_3 = \{X_3 = (0, 0, 0, 0, 1, 1, 1, 1), Y_3 = (1, 1, 1, 1, 0, 0, 0, 0)\}$$

$$C_4 = \{X_4 = (0, 0, 1, 1, 1, 1, 0, 0), Y_4 = (1, 1, 0, 0, 0, 0, 1, 1)\}$$

A matriz diferença do código 2 - usuários é definida da seguinte maneira:

Escolha D_0 como sendo uma matriz $2 \times N_0$, $N_0 \geq 2$ que tem como primeira linha o vetor composto por -1 ; Se N_0 é um número par, então a segunda linha de D_0 tem os primeiros $N_0/2$ elementos iguais a -1 e os últimos $N_0/2$ elementos iguais a 1 ; Se N_0 é ímpar, então a segunda linha de D_0 tem os primeiros $(N_0 - 1)/2$ elementos iguais a -1 e os últimos $(N_0 - 1)/2 + 1$ elementos iguais a 1 . Esta escolha é feita para garantir que a matriz D_0 tenha $\text{rank} = 2$.

Exemplo 4.2 : Para $N_0 = 2$ e $N_0 = 3$ as matrizes diferenças são, respectivamente,

$$D_0 = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}$$

e,

$$D_0 = \begin{bmatrix} -1 & -1 & -1 \\ -1 & 1 & 1 \end{bmatrix}$$

e definem códigos 2 - usuários 2 - decodificáveis de comprimento 2 e 3, respectivamente.

Lema 4.2 : O código dois usuários de comprimento N_0 definido pela matriz D_0 acima tem as seguintes propriedades:

- i) Se N_0 é par então o código dois usuários é N_0 -decodificável;
- ii) Se N_0 é ímpar então o código dois usuários é $(N_0 - 1)$ -decodificável.

Demonstração : i) Seja (C_1, C_2) o código dois usuários definido pela matriz D_0 e seja $C_1 + C_2 = \{c_1 + c_2; c_1 \in C_1, c_2 \in C_2\}$. Este conjunto tem quatro vetores que são: um vetor cujas primeiras $N_0/2$ coordenadas são iguais a zero e as últimas $N_0/2$ coordenadas iguais a 1; um vetor cujas primeiras $N_0/2$ coordenadas são iguais a 1 e as últimas $N_0/2$ coordenadas iguais a zero; um vetor cujas primeiras $N_0/2$ coordenadas são iguais a 1 e as últimas $N_0/2$ coordenadas iguais a 2 e um vetor cujas primeiras $N_0/2$ primeiras coordenadas são iguais a 2 e as últimas $N_0/2$ coordenadas são iguais a 1. O valor absoluto da diferença de cada coordenada do primeiro vetor descrito acima para o segundo e terceiro é igual 1 e, portanto, a distância entre estes vetores é igual a N_0 . O valor absoluto da diferença de cada uma das primeiras $N_0/2$ coordenadas do primeiro vetor para o quarto é igual a 2 e das últimas $N_0/2$ coordenadas é igual a zero, logo a distância entre estes vetores é $2 \cdot (N_0/2) = N_0$. Continuando com este raciocínio podemos ver que a distância entre o segundo vetor para os demais é igual a N_0 , a distância do terceiro vetor para os demais também é igual a N_0 . Desta forma temos que se N_0 é par a distância mínima do código definido pela matriz D_0 é igual a N_0 .

ii) Se N_0 é ímpar, $C_1 + C_2$ tem os seguintes vetores: um vetor cujas primeiras $(N_0 - 1)/2$ coordenadas são iguais a zero e as últimas $(N_0 + 1)/2$ coordenadas iguais a 1; um vetor cujas primeiras $(N_0 - 1)/2$ coordenadas são iguais a 1 e as últimas $(N_0 + 1)/2$ coordenadas iguais a zero;

um vetor cujas primeiras $(N_0 - 1)/2$ coordenadas são iguais a 1 e as últimas $(N_0 + 1)/2$ coordenadas iguais a 2 e um vetor cujas primeiras $(N_0 - 1)/2$ coordenadas são iguais a 2 e as últimas $(N_0 + 1)/2$ coordenadas iguais a 1.

A distância do primeiro vetor para o segundo e terceiro é igual a N_0 e para o quarto é igual a $N_0 - 1$; a distância do segundo vetor para o terceiro é igual a $N_0 + 1$ e para o quarto é igual a N_0 ; a distância do terceiro vetor para o quarto é igual a N_0 . Portanto, a distância mínima do código (C_1, C_2) é igual a $N_0 - 1$.

A tabela 4.1 lista alguns códigos dois usuários δ - decodificáveis no nível D_0 , para vários valores de δ .

Tabela 4.1

Códigos dois usuários	Comprimento	δ
$C_1 = \{ 00, 11 \}$ $C_2 = \{ 01, 10 \}$	2	2
$C_1 = \{ 000, 111 \}$ $C_2 = \{ 011, 100 \}$	3	2
$C_1 = \{ 0000, 1111 \}$ $C_2 = \{ 0011, 1100 \}$	4	4
$C_1 = \{ 00000, 11111 \}$ $C_2 = \{ 00111, 11000 \}$	5	4
$C_1 = \{ 000000, 111111 \}$ $C_2 = \{ 000111, 111000 \}$	6	6
$C_1 = \{ 0000000, 1111111 \}$ $C_2 = \{ 0001111, 1110000 \}$	7	6
$C_1 = \{ 00000000, 11111111 \}$ $C_2 = \{ 00001111, 11110000 \}$	8	8

A tabela 4.2 mostra os parâmetros de uma lista, não exaustivos, de códigos T - usuários segundo o corolário 4.1.

Tabela 4.2

Código no nível D_0			Códigos Extendidos		
Número de usuários T_0	Comprimento N_0	δ	Número de Usuários T	Comprimento N	d_{\min}
2	2	2	4	4	4
2	2	2	8	8	8
2	2	2	16	16	16
2	2	2	24	24	24
2	3	2	4	6	4
2	3	2	8	12	8
2	3	2	16	24	16
2	3	2	24	36	24
2	4	4	4	8	8
2	4	4	8	16	16
2	4	4	16	32	32
2	4	4	24	48	48
2	5	4	4	10	8
2	5	4	8	20	16
2	5	4	16	40	32
2	5	4	24	60	48

A taxa do i -ésimo código constituinte é $R_i = (\log_2 |C_i|) / q \cdot N_0 = 1/q \cdot N_0$ e, desta forma, a taxa do código T - usuários, $R(T)$ é igual a:

$$R(T) = R_1 + R_2 + \dots + R_T = 2 \cdot q / N_0 \cdot q = 2 / N_0$$

A seguir mostraremos como podemos generalizar esta classe de códigos via a noção de classes de equivalência, segundo Ferguson [2].

4.3 Generalização da Classe de Códigos do Corolário 4.1 via a Noção de Classes de Equivalência

Seja D_0 a matriz diferença de um código dois usuários δ - decodificável de comprimento N_0 e sejam P e Q matrizes de permutações generalizadas de ordem 2×2 e $N_0 \times N_0$, respectivamente. Então $D^1 = P \cdot D_0 \cdot Q$ é uma matriz diferença de ordem $2 \times N_0$ e desta forma define um código dois usuários de comprimento N_0 .

O seguinte teorema é uma generalização do teorema 3.6 de Ferguson [2].

Teorema 4.1 : Seja D uma matriz diferença $T \times N$ de um código T - usuários e distância mínima igual a δ . Sejam P e Q matrizes de permutações generalizadas de ordens T e N respectivamente. Então $D^1 = P.D.Q$ é uma matriz diferença de um código T - usuários e distância mínima maior ou igual δ .

Demonstração : Sejam C e C' os códigos definidos pelas matrizes D e D^1 , respectivamente. Então, sabemos de [1] que,

$$d_{\min}(C) = \min_m || m.D ||$$

e

$$d_{\min}(C') = \min_{m'} || m'.D^1 ||$$

onde m e m' são T - uplas sobre $\{ 0, 1, -1 \}$.

Agora, seja $m^* \in \{ 0, 1, -1 \}^T$ tal que,

$$\begin{aligned} d_{\min}(C') &= || m^*.PDQ || = || m''.D.Q ||, \quad m'' = m^*P \\ &= || v || \end{aligned}$$

onde $v = m''.DQ$

$\implies v.Q^{-1} = m''.D$. Por outro lado, temos que,

$$d_{\min}(C) \leq || m''.D || = || v.Q^{-1} ||$$

e desde que Q^{-1} é uma matriz de permutação generalizada, lema 3.4, pp. 35, temos que,

$$|| v.Q^{-1} || = || v || = d_{\min}(C')$$

e, desta forma temos que,

$$d_{\min}(C) \leq d_{\min}(C')$$

■

Exemplo 4.3 : Seja D a matriz diferença dada por

$$D = \begin{bmatrix} -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$$

Esta matriz define um código 2 - usuários 4 - decodificável, conforme pode-se ver na tabela abaixo.

Tabela 4.3

C_1	0 1 0 1	1 0 1 0
C_2		
0 1 1 0	0 2 1 1	1 1 2 0
1 0 0 1	1 1 0 2	2 0 1 1

Sejam P e Q as matrizes de permutações generalizadas de ordem 2 e 4, respectivamente dadas por,

$$P = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \quad e \quad Q = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

então P.D.Q é a matriz diferença dada por,

$$D^1 = P.D.Q = \begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$$

que define o código 2 - usuários 4 - decodificável do exemplo 4.1. Fazendo o produto de Kronecker pela matriz de Hadamard de ordem q, isto é, $H \otimes D^1$ obtém-se um código 2.q-usuários de comprimento 4.q e distância mínima $d_{\min} = 4.q$. Por exemplo, se H é a matriz de Hadamard de ordem 2 obtemos o código 4-usuários de comprimento 2.4 = 8 e distância mínima $d_{\min} = 4.2 = 8$ do exemplo 4.2. Isto pode ser sintetizado da seguinte maneira.

Seja D uma matriz diferença de um código 2 - usuários δ - decodificável de comprimento N_0 para a qual existam matrizes de permutações generalizadas P e Q de ordem 2 x 2 e $N_0 \times N_0$ tais que a matriz $D^1 = P.D.Q$ seja da forma:

1)
 1) A primeira linha de D^1 é o vetor composto por -1;

ii) Se N_0 é um número par, então a segunda linha de D^1 tem os primeiros $N_0/2$ elementos iguais a -1 e os últimos $N_0/2$ elementos iguais a 1; Se N_0 é ímpar, então a segunda linha de D^1 tem os primeiros $(N_0 - 1)/2$ elementos iguais a -1 e os últimos $(N_0 - 1)/2 + 1$ elementos iguais a 1.

Seja H a matriz de Hadamard de ordem $q \times q$, então o produto de Kronecker $H \otimes D$ é a matriz diferença de ordem $2.q \times N_0.q$ e, desta forma define um código 2.q-usuários de comprimento $N_0.q$ e distância mínima $d_{\min} = q.\delta$.

Um outro caminho para generalizarmos a classe de códigos do corolário 4.1 via a noção de classes de equivalências é o seguinte.

Seja D_0 uma matriz diferença da forma acima descrita (itens (i) e (ii)) que defina um código 2-usuários δ -decodificável de comprimento N_0 e seja H a matriz de Hadamard de ordem q , então $H \otimes D_0$ é uma matriz diferença que define um código 2.q-usuários de comprimento $N_0.q$ e distância mínima $d_{\min} = \delta.q$. Sejam P e Q matrizes de permutações generalizadas de ordem $2.q \times 2.q$ e $N_0.q \times N_0.q$, respectivamente. Então $D^1 = P.(H.D_0).Q$ é a matriz diferença de ordem $2.q \times N_0.q$ e, portanto define um código 2.q-usuários de comprimento $N_0.q$. As matrizes D e D^1 são chamadas de matrizes equivalentes e os códigos por elas definidas códigos equivalentes. O exemplo abaixo ilustra esta generalização.

Exemplo 4.4 : Seja D_0 a matriz diferença do exemplo 4.2 e H a matriz de Hadamard de ordem 2, então,

$$H_2 \otimes D_0 = \begin{bmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \end{bmatrix}$$

Sejam P e Q matrizes de permutações generalizadas de ordem 4 e 8, respectivamente dadas por,

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

e

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

então,

$$P. (H_2 \otimes D_0). Q = \begin{bmatrix} -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{bmatrix}$$

define um código 4-usuários de comprimento 8 cujos códigos constituintes são:

$$C_1 = \{ X_1 = (0 0 1 0 1 0 1 1), Y_1 = (1 1 0 1 0 1 0 0) \}$$

$$C_2 = \{ X_2 = (0 1 1 0 0 1 1 0), Y_2 = (1 0 0 1 1 0 0 1) \}$$

$$C_3 = \{ X_3 = (1 0 1 0 0 1 0 1), Y_3 = (0 1 0 1 1 0 1 0) \}$$

$$C_4 = \{ X_4 = (1 1 1 0 1 0 0 0), Y_4 = (0 0 0 1 0 1 1 1) \}$$

4.4 Conclusão

Neste capítulo apresentamos, segundo o corolário 4.1, uma classe de códigos corretores de erros para o canal T - Usuários e generalizamos tais códigos via a noção de classe de equivalência, segundo Ferguson [2].

No capítulo seguinte apresentamos algumas propostas de algoritmos de decodificação que podem ser usadas tanto para os códigos apresentados neste capítulo como para os códigos de Chang e Weldon [1] e os códigos de Wilson [3]. Também apresentamos comparações dos algoritmos de decodificação propostos com o algoritmo de Wilson. As simulações foram realizadas para o canal Discreto sem Memória e para o canal AWGN T - usuários.

Capítulo V

Algoritmos de Decodificação e Resultados de Simulações

5.1 Introdução

Neste capítulo apresentamos algumas propostas de algoritmos de decodificações para o Canal Aditivo T - usuários baseadas na técnica do table look-up, numa adaptação do algoritmo de decodificação de Wilson apresentado no capítulo 3 e numa combinação destes dois algoritmos com o propósito de unir a simplicidade do algoritmo de Wilson com o maior poder de correção de erro do algoritmo baseado no Table Look-up. Também ilustramos, através de exemplos, que o algoritmo de decodificação proposto por Wilson não é apropriado para a classe de códigos apresentada no capítulo 4.

Resultados de simulações para os códigos apresentados nos capítulos 3 e 4 são mostrados para o Canal Discreto sem Memória T - Usuários e para o Canal AWGN T - Usuários.

5. 2. Algoritmos de Decodificação

5.2.1. Técnica de Decodificação baseada no Table Look-up

A técnica de decodificação baseada no Table Look-up pode ser enunciada da seguinte maneira: para um dado vetor transmitido do código T - usuários $C = \{ Z' \} = \{ Z_1 + Z_2 + \dots + Z_T, Z_i \in C_i \}$, seja U o vetor recebido. O vetor decodificado Z é aquele pertencente ao código C para o qual a L - distância é mínima, isto é, $d_L(Z', U)$ é mínima.

Agora para determinar os vetores códigos constituintes a partir de Z calcule, como em [3], a síndrome $S_2 = Z - Y$ e particione esta síndrome em q segmentos de comprimentos N_0 , onde q é a ordem da matriz de Hadamard e N_0 é o comprimento do código no nível D_0 . Estes segmentos são então arranjados em uma matriz $q \times N_0$ que tem estes segmentos como linhas, que denotaremos por M_{sz} . Multiplicando à esquerda esta matriz pela matriz de Hadamard de ordem q obtemos a matriz $H_q \cdot M_{sz}$ cujas

entradas são múltiplas de q . As entradas desta matriz são então divididas por q e as linhas resultantes são as síndromes corretas do código no nível D_0 . Cada uma destas síndromes são decompostas em um sistema matricial de equação cuja solução é o vetor binário $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_T)$ e os códigos constituintes são então obtidos de acordo com (3.12) da seção 3.5.1.

O seguinte exemplo ilustra este algoritmo.

Exemplo 5.1 : Seja C o código T - usuários, com $T = 4$ de comprimento $N = 2.4 = 8$ e distância mínima $d_{\min} = 2.4 = 8$ do exemplo 4.1 e seja $Z = X_1 + X_2 + Y_3 + Y_4 = (2, 2, 2, 2, 0, 0, 2, 2)$ o vetor transmitida. Suponha que o vetor recebido seja $U = (2, 5, 2, 2, 0, 0, 2, 2)$. Vemos que o vetor recebido difere do vetor transmitido na segunda coordenada por um erro de magnitude 3. A tabela de decodificação deste código é constituída pelos seguintes vetores:

```

0 0 2 2 2 2 2 2
1 1 1 1 1 1 3 3
1 1 3 3 1 1 1 1
2 2 2 2 0 0 2 2
1 1 1 1 3 3 1 1
2 2 0 0 2 2 2 2
2 2 2 2 2 2 0 0
3 3 1 1 1 1 1 1
1 1 3 3 3 3 3 3
2 2 2 2 2 2 4 4
2 2 4 4 2 2 2 2
3 3 3 3 1 1 3 3
2 2 2 2 4 4 2 2
3 3 1 1 3 3 3 3
3 3 3 3 3 3 1 1
4 4 2 2 2 2 2 2

```

Usando esta tabela vemos que o vetor mais próximo do vetor U é exatamente o vetor transmitido Z .

Agora seja a síndrome $S_Z = Z - Y = (-2 \ -2 \ 0 \ 0 \ -2 \ -2 \ 0 \ 0)$ onde $Y = Y_1 + Y_2 + Y_3 + Y_4 = (4 \ 4 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2)$, $Y_i \in C_i$. O vetor síndrome S_Z é particionado em $q = 2$ segmentos de comprimento $N_0 = 4$ e arranjado em uma

matriz 2 x 4 que tem estes dois segmentos como linhas, isto é,

$$M_{SZ} = \begin{bmatrix} -2 & -2 & 0 & 0 \\ -2 & -2 & 0 & 0 \end{bmatrix}$$

Multiplicando esta matriz à esquerda pela matriz de Hadamard de ordem 2, obtemos a seguinte matriz,

$$H_2 \cdot M_{SZ} = \begin{bmatrix} -4 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

As entradas desta matriz são então divididas por $q = 2$ e as linhas resultantes são as síndromes corretas do código no nível D_0 . Cada uma destas síndromes são decompostas no seguinte sistema de equações matricial,

$$\begin{bmatrix} \lambda_{z1} & D \\ z1 & 0 \end{bmatrix} = \begin{bmatrix} -2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

onde λ_{z1} , $i = 1, 2$ é um vetor linha de comprimento 2. A solução deste sistema de equação matricial é obtida resolvendo-se os seguintes sistemas de equações lineares,

$$I) \quad \begin{cases} -\lambda_1 - \lambda_2 = -2 \\ -\lambda_1 + \lambda_2 = 0 \end{cases}$$

$$II) \quad \begin{cases} -\lambda_3 - \lambda_4 = 0 \\ -\lambda_3 + \lambda_4 = 0 \end{cases}$$

As soluções deste sistemas podem ser escritas como um vetor $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (1, 1, 0, 0)$ e os vetores códigos transmitidas por cada usuários são: $Z_1 = X_1$, $Z_2 = X_2$, $Z_3 = Y_3$ e $Z_4 = Y_4$, de acordo com a equação (3.12).

Para este exemplo e todos os casos em que a magnitude do erro seja

menor ou igual a $\lfloor (d_{\min} - 1)/2 \rfloor$ sempre é possível identificarmos o vetor transmitido e por consequência determinarmos os vetores constituintes.

O exemplo seguinte nos mostra que quando a magnitude do erro for maior do que $\lfloor (d_{\min} - 1)/2 \rfloor$ não é possível fazer a decodificação corretamente.

Exemplo 5.2: Sejam C , ($d_{\min} = 8$) e $Z = (2, 2, 2, 2, 0, 0, 2, 2)$ como no exemplo 5.1 e suponha que o vetor recebido seja $U = (1, 1, 1, 1, 1, 0, 2, 2)$. Vemos que o vetor recebido difere do transmitido na 1ª, 2ª, 3ª, 4ª e 5ª coordenadas e que a magnitude do erro é igual a 5 que é maior do que a capacidade de correção de erro do código.

Fazendo a decodificação pelo table look-up vemos que o vetor mais próximo de U é $Z' = (1, 1, 1, 1, 1, 1, 3, 3)$ e, portanto, este é o vetor escolhido como sendo o transmitido. Agora seja a síndrome $S_{Z'} = Z' - Y = (-3, -3, -1, -1, -1, -1, 1, 1)$ e,

$$M_{S_{Z'}} = \begin{bmatrix} -3 & -3 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$$

Multiplicando esta matriz à esquerda pela matriz de Hadamard de ordem 2 temos,

$$H_2 \cdot M_{S_{Z'}} = \begin{bmatrix} -4 & -4 & 0 & 0 \\ -2 & -2 & -2 & -2 \end{bmatrix}$$

Dividindo as entradas desta matriz por $q = 2$ obtemos as síndromes no nível D_0 , isto é,

$$\begin{bmatrix} \lambda_{z1} D_0 \\ \lambda_{z2} D_0 \end{bmatrix} = \begin{bmatrix} -2 & -2 & 0 & 0 \\ -1 & -1 & -1 & -1 \end{bmatrix}$$

A solução deste sistema é obtida resolvendo-se os seguintes sistemas de equações lineares:

$$\text{III) } \begin{cases} -\lambda_1 - \lambda_2 = -2 \\ -\lambda_1 + \lambda_2 = 0 \end{cases}$$

$$\text{IV) } \begin{cases} -\lambda_3 - \lambda_4 = -1 \\ -\lambda_3 + \lambda_4 = -1 \end{cases}$$

e é o vetor binário $\lambda = (1, 1, 1, 0)$. Neste caso os vetores códigos constituintes decodificadas são: $Z_1 = X_1$, $Z_2 = X_2$, $Z_3 = X_3$ e $Z_4 = Y_4$. Como podemos ver estes não são os vetores escolhidos para formar o vetor transmitido Z (Ex. 5.1) e, portanto, a decodificação falharia. Isto deve-se ao fato de não termos escolhido corretamente o vetor recebido Z' como sendo o transmitido, em função de que o ruído, por hipótese, produziu um erro de magnitude maior do que a capacidade de correção do table look-up.

5.2.2 Algoritmo de Wilson Adaptado para os Novos Códigos

Através dos exemplos apresentados a seguir mostraremos como adaptar o algoritmo de decodificação proposto por Wilson [3] para os códigos introduzidos pelo corolário 4.1 e ilustraremos porque este algoritmo não é apropriado para estes códigos.

Exemplo 5.3 Seja (C_1, C_2) o código 2-usuários 4-decodificável de comprimento $N_0 = 4$ definido pela matriz diferença

$$D_0 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$$

e seja H_4 a matriz de Hadamard de ordem 4 dada por,

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

então o produto de Kronecker $H_4 \otimes D_0$ é a matriz diferença de um código 8-usuários de comprimento $N = 16$ e distância mínima $d_{\min} = 4 \cdot 4 = 16$, dada por,

$$H_4 \otimes D_0 = \begin{bmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \end{bmatrix}$$

e cujos códigos constituintes são:

$$\begin{aligned} C_1 &= \{ X_1 = 0000000000000000 ; Y_1 = 1111111111111111 \} \\ C_2 &= \{ X_2 = 0011001100110011 ; Y_2 = 1100110011001100 \} \\ C_3 &= \{ X_3 = 0000111100001111 ; Y_3 = 1111000011110000 \} \\ C_4 &= \{ X_4 = 0011110000111100 ; Y_4 = 1100001111000011 \} \\ C_5 &= \{ X_5 = 0000000011111111 ; Y_5 = 1111111100000000 \} \\ C_6 &= \{ X_6 = 0011001111001100 ; Y_6 = 1100110000110011 \} \\ C_7 &= \{ X_7 = 0000111111110000 ; Y_7 = 1111000000001111 \} \\ C_8 &= \{ X_8 = 0011110011000011 ; Y_8 = 1100001100111100 \} \end{aligned}$$

Seja $Z = X_1 + X_2 + Y_3 + Y_4 + X_5 + X_6 + Y_7 + Y_8$, onde $X_i \in C_i$ e $Y_j \in C_j$, $i \neq j$, a 16 - upla transmitida. O vetor Z é (4 4 4 4 0 0 4 4 4 4 4 4 4 4 4 4). Suponha que o vetor recebido seja $U = (3 5 3 5 0 0 4 4 4 4 4 4 4 4 4 4)$. Vemos então que o vetor U é o resultado da adição do vetor erro $E = (-1 1 -1 1 0 0 0 0 0 0 0 0 0 0 0 0)$ com o vetor transmitido Z . O trabalho do decodificador é retirar o erro e determinar que vetores códigos constituintes foram adicionadas para formar o vetor transmitido Z .

De acordo com [3] primeiro a síndrome $U - Y = Z - Y + E = S_2 + E$ é calculada, onde $Y = Y_1 + Y_2 + Y_3 + Y_4 + Y_5 + Y_6 + Y_7 + Y_8$ é o vetor (8 8 4 4 4 4 4 4 4 4 4 4 4 4 4 4). O vetor $S_2 + E = (-5 -3 -1 1 -4 -4 0 0 0 0 0 0 0 0 0 0)$ é então particionado em $q = 4$ segmentos de comprimento $N_0 = 4$, onde q é a ordem da matriz de Hadamard e N_0 é o comprimento do código no

nível D_0 . Estes segmentos são então arranjados em uma matriz $4 \times 4 M_{SZ+E}$ que tem estes segmentos como linhas, i.é.,

$$M_{SZ+E} = \begin{bmatrix} -5 & -3 & -1 & 1 \\ -4 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

A matriz M_{SZ+E} é então multiplicada à esquerda pela matriz de Hadamard H_4 e o resultado desta multiplicação é a matriz,

$$H_4 \cdot M_{SZ+E} = \begin{bmatrix} -9 & -7 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ -9 & -7 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix}$$

Desde que as entradas desta matriz não são múltiplas de $q = 4$, então alguns erros são indicados e a correção mais provável, [3], é obtida trocando-se cada entrada desta matriz pelo múltiplo de 4 mais próximo, desta maneira obtemos a seguinte matriz,

$$H_4 \cdot M_{SZ} = \begin{bmatrix} -8 & -8 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -8 & -8 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

A matriz corrigida é então dividida por $q = 4$ e as linhas resultantes são as síndromes corretas no nível D_0 . Cada uma destas quatro síndromes são decompostas na seguinte equação matricial,

$$\begin{bmatrix} \lambda_{z1} D_0 \\ \lambda_{z2} D_0 \\ \lambda_{z3} D_0 \\ \lambda_{z4} D_0 \end{bmatrix} = \begin{bmatrix} -2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (5.1)$$

onde λ_{zi} , $i = 1, 2, 3, 4$, é um vetor linha de comprimento 2. De uma forma diferente que a apresentada por Wilson [3], a solução desta equação matricial é obtida resolvendo os seguintes sistemas de equações lineares:

$$V) \begin{cases} -\lambda_1 - \lambda_2 = -2 \\ -\lambda_1 + \lambda_2 = 0 \end{cases}$$

$$VI) \begin{cases} -\lambda_3 - \lambda_4 = 0 \\ -\lambda_3 + \lambda_4 = 0 \end{cases}$$

$$VII) \begin{cases} -\lambda_5 - \lambda_6 = -2 \\ -\lambda_5 + \lambda_6 = 0 \end{cases}$$

$$VIII) \begin{cases} -\lambda_7 - \lambda_8 = 0 \\ -\lambda_7 + \lambda_8 = 0 \end{cases}$$

O vetor solução destes sistemas é o vetor binário $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8) = (1, 1, 0, 0, 1, 1, 0, 0)$ que de acordo com a equação (3.12) determina que vetores códigos dos códigos constituintes foram somadas para formar o vetor transmitido Z , isto é, $Z_1 = X_1$, $Z_2 = X_2$, $Z_3 = Y_3$, $Z_4 = Y_4$, $Z_5 = X_5$, $Z_6 = X_6$, $Z_7 = Y_7$ e $Z_8 = Y_8$.

Esta forma de fazer a decodificação no nível D_0 diferentemente de Wilson se faz necessária em função do algoritmo de Wilson utilizar-se neste nível do algoritmo de decodificação de Chang e Weldon o qual se utiliza da estrutura iterativa dos seus códigos para fazer a decodificação, o que não é o caso dos códigos apresentados no capítulo 4.

Neste exemplo foi possível corrigir o vetor erro porque nas posições 1, 2, 3 e 4 o vetor recebido U difere do vetor transmitido Z somente de um erro de magnitude 1. Neste e em todos os casos em que a magnitude do erro por dígito for menor ou igual a $\lfloor (q-1)/2 \rfloor$ em um burst consecutivo não maior do que o comprimento do código no nível D_0 o algoritmo é capaz de corrigir todos os erros, [3].

Por outro lado, para um erro de magnitude maior, por exemplo, $E = (-1, 2, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ o algoritmo não decodificaria corretamente como mostra o seguinte exemplo.

Exemplo 5.4 : Sejam $E = (-1, 2, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ e Z o vetor transmitido, como no exemplo anterior. Então o vetor recebido é $U = (3, 6, 5, 5, 0, 0, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$. Observe que a mag-

nitidade do erro é igual a 5 e que na 2ª coordenada do vetor erro a magnitude do erro é igual a 2 que é maior do que $\lfloor (4 - 1)/2 \rfloor = 1$.

Calculando a síndrome obtemos o seguinte vetor $U - Y = (-5, -2, 1, 1, 1, -4, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$. Particionando este vetor em 4 segmentos de comprimento 4 obtemos a seguinte matriz cujas linhas são formadas por estes segmentos,

$$M_{SZ} + E = \begin{bmatrix} -5 & -2 & 1 & 1 \\ -4 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Multiplicando à esquerda pela matriz de Hadamard de ordem quatro, H_4 , obtemos a seguinte matriz,

$$H_4 \cdot M_{SZ} + E = \begin{bmatrix} -9 & -6 & 1 & 1 \\ -1 & 2 & 1 & 1 \\ -9 & -6 & 1 & 1 \\ -1 & 2 & 1 & 1 \end{bmatrix}$$

Neste ponto temos que trocar as entradas desta matriz pelo múltiplo de quatro mais próximo. Porém para os elementos -6 e 2 não temos como tomar uma decisão correta. Suponha que decidamos por -4 e 4, respectivamente, desta forma a matriz corrigida é,

$$H_4 \cdot M_{SZ} = \begin{bmatrix} -8 & -4 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ -8 & -4 & 0 & 0 \\ 0 & 4 & 0 & 0 \end{bmatrix}$$

Dividindo as entradas desta matriz por 4 obtemos o seguinte sistema matricial,

$$\begin{bmatrix} \lambda_{z1} D_0 \\ \lambda_{z2} D_0 \\ \lambda_{z3} D_0 \\ \lambda_{z4} D_0 \end{bmatrix} = \begin{bmatrix} -2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

que são as síndromes do código no nível D_0 . A solução deste sistema de equação matricial é obtida resolvendo-se os seguintes sistemas de equações lineares,

$$I) \begin{cases} -\lambda_1 - \lambda_2 = -2 \\ -\lambda_1 - \lambda_2 = -1 \\ -\lambda_1 + \lambda_2 = 0 \end{cases}$$

$$II) \begin{cases} -\lambda_3 - \lambda_4 = 0 \\ -\lambda_3 - \lambda_4 = 1 \\ -\lambda_3 + \lambda_4 = 0 \end{cases}$$

$$III) \begin{cases} -\lambda_5 - \lambda_6 = -2 \\ -\lambda_5 - \lambda_6 = -1 \\ -\lambda_5 + \lambda_6 = 0 \end{cases}$$

$$IV) \begin{cases} -\lambda_7 - \lambda_8 = 0 \\ -\lambda_7 - \lambda_8 = 1 \\ -\lambda_7 + \lambda_8 = 0 \end{cases}$$

e desde que nenhum destes sistemas possui solução, não é possível concluir o processo de decodificação.

Como vimos, em geral o algoritmo proposto por Wilson [3] somente é capaz de corrigir $t = \lfloor (q - 1)/2 \rfloor$ erros por dígitos em um "burst" de dígitos consecutivos de comprimento não maior do que N_0 , onde q é a ordem da matriz de Hadamard e N_0 é o comprimento do código δ -decodificável definido pela matriz diferença D_0 . Esta restrição deve-se ao fato de que o algoritmo apresentado por Wilson supõe que no nível D_0 o código seja unívocamente decodificável e se utiliza de um algoritmo de decodificação para esta classe de códigos, como é o caso dos códigos de Chang e Weldon [1]. Desde que a distância mínima do código é de fato $d_{\min} = q \cdot \delta$, um algoritmo de decodificação apropriado deveria corrigir um erro de magnitude pelo menos igual a $t = \lfloor (q \cdot \delta - 1)/2 \rfloor$ como é o caso do algoritmo baseado no table look-up mas de complexidade maior.

Em vista disso, na próxima seção fazemos uma proposta de um algoritmo de decodificação para os códigos T - Usuários baseada numa combinação do algoritmo de Wilson e na técnica do table look-up.

5.2.3 Técnica de Decodificação Combinada

A proposta apresentada nesta seção pode ser sintetizada da seguinte forma: sempre que o sistema matricial (5.1) não tiver solução ou a solução não for binária a técnica de decodificação baseada no table look-up é utilizada para concluir o processo de decodificação.

Esta proposta de decodificação tem a vantagem de requerer uma quantidade menor de cálculos computacionais para concluir o processo de decodificação e apresenta um desempenho de decodificação muito próximo da técnica baseada no table look-up, conforme mostra os resultados das simulações que serão apresentados na próxima seção.

5.2.4 Técnicas de Decodificação por Decisão Suave e Abrupta

• Decisão Suave

A técnica de decodificação por decisão suave (S/D) é baseada na quantização do vetor recebido que denotaremos por Y_{AWGN} , isto é,

$$Y_{AWGN} = (y_1, y_2, \dots, y_j, \dots, y_N)$$

O número de níveis de quantização ou níveis threshold é igual a 2^{NBSOFT} , conforme Borelli [35], onde NBSOFT é o número de bits de decisão ou bits de confiança. Os níveis de quantização são igualmente espaçados com distância entre dois níveis consecutivos de quantização igual a $1/2^{NBSOFT}$, desta forma estes níveis de quantização assumem valores no conjunto $\{0, 1/2^{NBSOFT}, 2/2^{NBSOFT}, \dots, (2^{NBSOFT} - 1)/2^{NBSOFT}, 1\}$.

No esquema de decodificação por decisão suave, $NBSOFT \neq 0$, as coordenadas do vetor quantizado, que denotaremos por Y_0 , isto é,

$$Y_0 = (y_{q_1}, y_{q_2}, \dots, y_{q_j}, \dots, y_{q_N})$$

são obtidas da seguinte forma: tome a j -ésima coordenada do vetor recebido, y_j , e calcule o valor de $y_j - \text{int}(y_j)$, onde $\text{int}(y_j)$ denota a parte inteira de y_j . Verifique no conjunto acima que nível de quantização está mais próximo de $y_j - \text{int}(y_j)$. Suponhamos que este nível seja $k/2^{NBSOFT}$, onde $1 \leq k \leq 2^{NBSOFT}$ e então faça a j -ésima coordenada do vetor quantizado, y_{q_j} igual a $\text{int}(y_j) + k/2^{NBSOFT}$.

Por exemplo, suponhamos que o número de bits de confiança seja

NBSOFT = 2, então o número de níveis de quantização é igual a 4 e assumem valores no conjunto $\{0, 1/4, 2/4, 3/4, 1\}$. Agora, suponhamos mais uma vez que a j -ésima coordenada do vetor recebido seja $y_j = 1.3421$, então $y_j - \text{int}(y_j) = .3421$ e, é fácil ver que este número está mais próximo de $1/4$ e, portanto, a j -ésima coordenada do vetor quantizado y_{q_j} é igual a $\text{int}(y_j) + .25 = 1.25$. O vetor quantizado é então decodificado através de um algoritmo de decodificação apropriado.

• Decisão Abrupta

Por outro lado, no esquema de decodificação por decisão abrupta (H/D) o número de bits de confiança NBSOFT = 0 e, neste caso, a j -ésima coordenada do vetor quantizado é obtido da seguinte maneira: se $y_j - \text{int}(y_j) \leq .5$ então $y_{q_j} = \text{int}(y_j)$, caso contrário $y_{q_j} = 1 + \text{int}(y_j)$.

Por exemplo, suponha que $y_j = 1.3421$, então $y_j - \text{int}(y_j) = .3421 < .5$ e, neste caso, $y_{q_j} = 1$.

5.3. Desempenho dos Novos Códigos

5.3.1 Simulação para o Canal Discreto sem Memória (DMC)

Alguns resultados de simulações para o Canal Discreto sem Memória T - Usuários foram apresentados em [29] da seguinte forma: seja $U = (u_1, u_2, \dots, u_N)$ o vetor na saída do canal. Este vetor é o resultado da soma do vetor transmitido Z com um vetor erro $E = (e_1, e_2, \dots, e_N)$, isto é, $U = Z + E$, onde as coordenadas do vetor erro são da forma $e_i = K_i \cdot B/N$, onde K_i é um número aleatório gerado com distribuição uniforme entre zero e +1 ou -1 e B é um número real positivo relacionado com a potência do ruído, isto é, quanto maior o valor de B menor a relação sinal/ruído. O método utilizado para as realizações das simulações é o método de Monte Carlo.

Os códigos usados nas simulações foram os códigos da tabela 4.2 de parâmetros d_{\min} e N conforme os seguintes vetores $d_{\min} = (4, 4, 8, 8)$ e $N = (4, 6, 8, 10)$ denominados códigos 1, 2, 3 e 4, respectivamente e o algoritmo de decodificação utilizado é o table look-up.

As figuras 5.1a à 5.1d apresentam graficamente os resultados (Pe versus B) destas simulações, onde Pe é a probabilidade de erro de palavras códigos do código T - usuários.

As figuras 5.1a e 5.1b mostram os comportamentos dos códigos 1 e 2 e dos códigos 3 e 4 para uma variação ampla do parâmetro B, enquanto que as figuras 5.1c e 5.1d apresentam os comportamentos destes mesmos códigos somente para probabilidades de erros menores do que 10^{-1} .

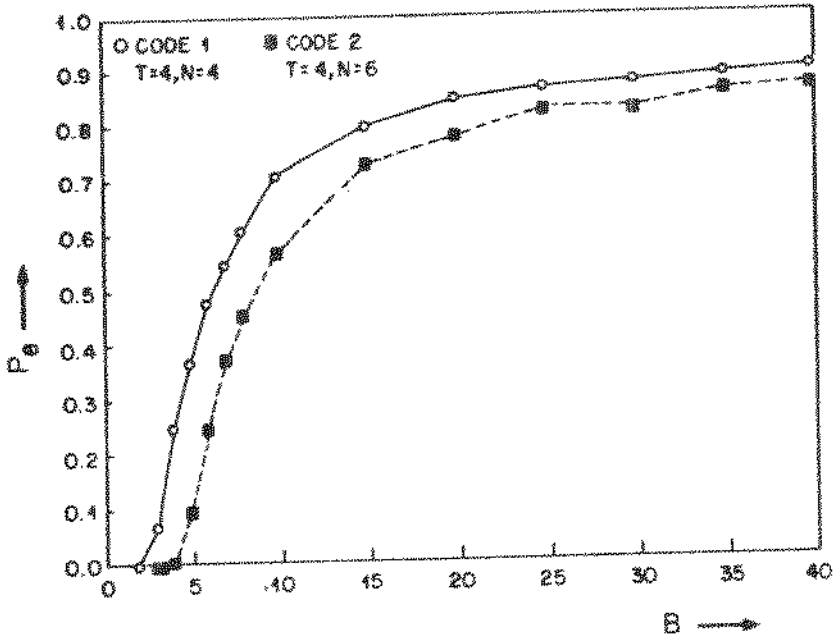


Fig 5.1a - Canal Discreto sem Memória;
Códigos $d_{\min} = 4$; Tabela 4.2; $0 \leq B \leq 40$

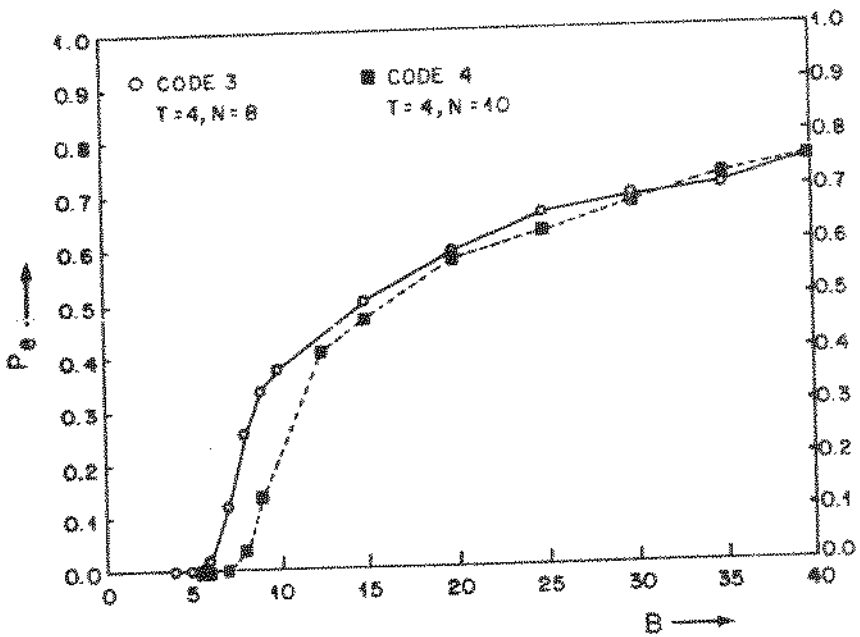


Fig. 5.1b - Canal Discreto sem Memória;
Códigos $d_{\min} = 8$; Tabela 4.2; $0 \leq B \leq 40$

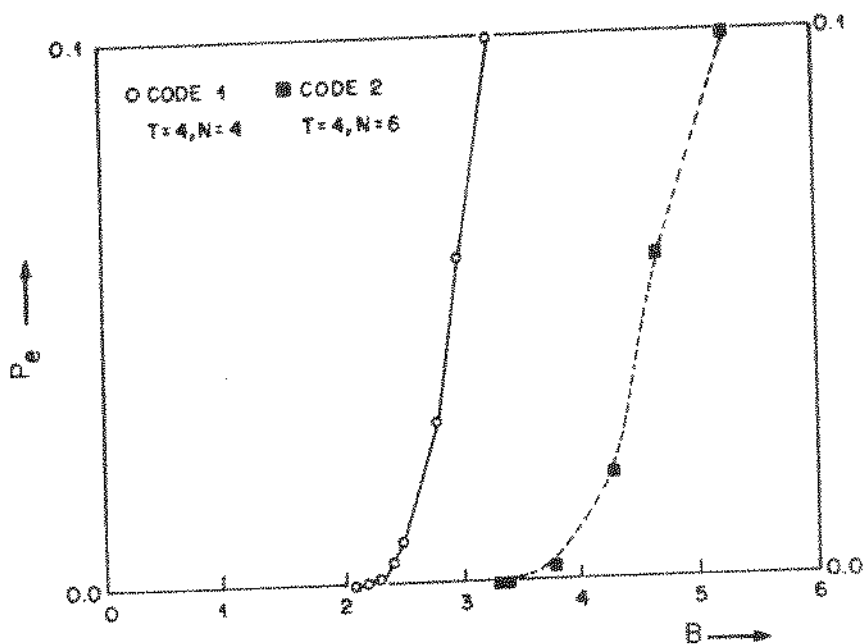


Fig. 5.1c - Canal Discreto sem Memória;
 Códigos $d_{\min} = 4$; Tabela 4.2; $0 \leq B \leq 6$

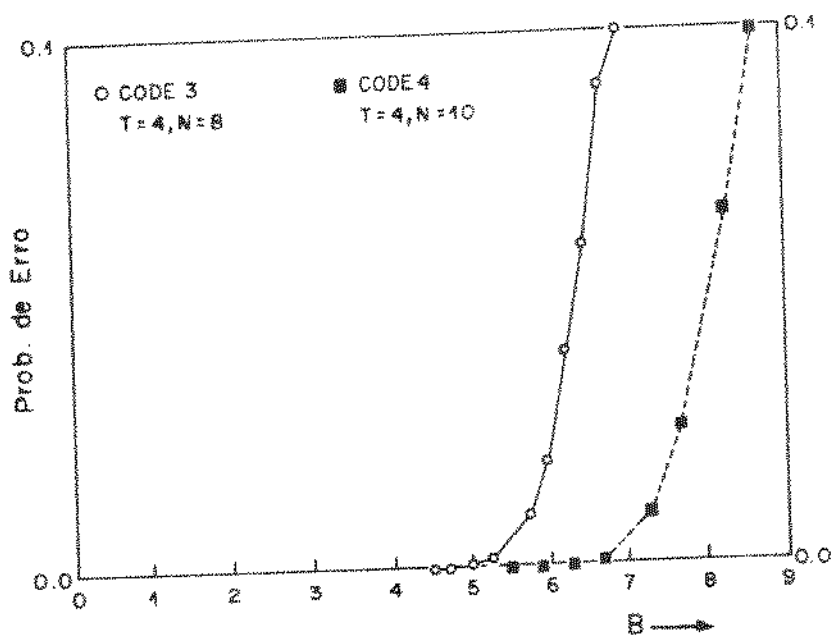


Fig. 5.1d - Canal Discreto sem Memória;
 Códigos $d_{\min} = 8$; Tabela 4.2; $0 \leq B \leq 9$

Conforme podemos ver em ambos os casos para os códigos com a mesma distância mínima (a menos da taxa do código T - usuários $R(T)$) o que apresenta um melhor desempenho é aquele que tem maior comprimento, isto é, o código 2, que tem a mesma distância mínima do código 1, $d_{\min} = 4$, porém possui comprimento maior, $N = 6$, apresenta um desempenho melhor do que o código 1. O código 4 que tem distância mínima igual ao código 3, $d_{\min} = 8$, mas de comprimento maior, $N = 10$, apresenta um desempenho melhor do que o código 3.

O código 3 apresenta um desempenho melhor do que os códigos 1 e 2 por possuir distância mínima maior, $d_{\min} = 8$ e, portanto, de todos estes códigos o que apresenta um desempenho melhor é o código 4. Por exemplo, para $B = 7$ os códigos 1 e 2 apresentam uma probabilidade de erro, $P_e > 10^{-1}$, enquanto que o código 3 tem $P_e \approx 10^{-1}$ e o código 4 apresenta uma probabilidade de erro $P_e \approx 3 \times 10^{-3}$.

5.3.2 Simulação para o Canal AWGN T - Usuários

Os resultados das simulações para o Canal AWGN T - Usuários são apresentados nas figuras 5.2a à 5.2d.

Dois sistemas são considerados, conforme [24] :

1. Sistema banda base antipodal, onde os sinais dos T - usuários são superpostos por amplitude e podem ser escritos na forma,

$$W_1 = (2I - T)\sqrt{E}$$

onde $E = A^2$ é a energia média por usuários. Por exemplo, para $T = 2$, $W_1 \in \{-2A, 0, 2A\}$, como mostrado na tabela abaixo

X_1	X_2	X'_1	X'_2	W_1
0	0	-A	-A	-2A
1	0	A	-A	0
0	1	-A	A	0
1	1	A	A	2A

2) Sistema banda base on - off onde os sinais dos T - usuários são superpostos por potência e podem ser escritos na forma,

$$W_1 = \sqrt{(2I)E}$$

onde $E = A^2$.

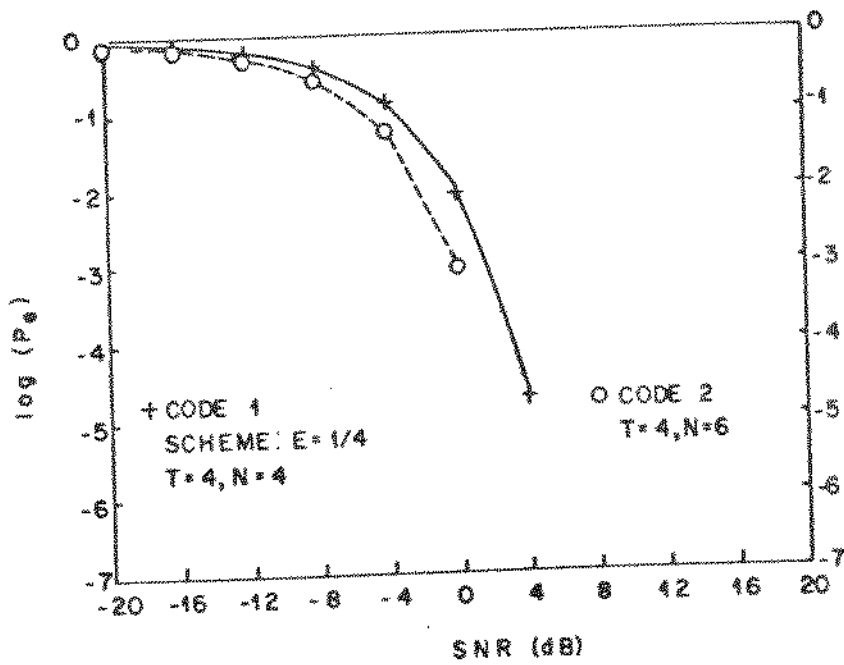


Fig. 5.2c - Sistema Banda Base On - Off ($E = 1/4$);
 Códigos $d_{\min} = 4$; Tabela 4.2;

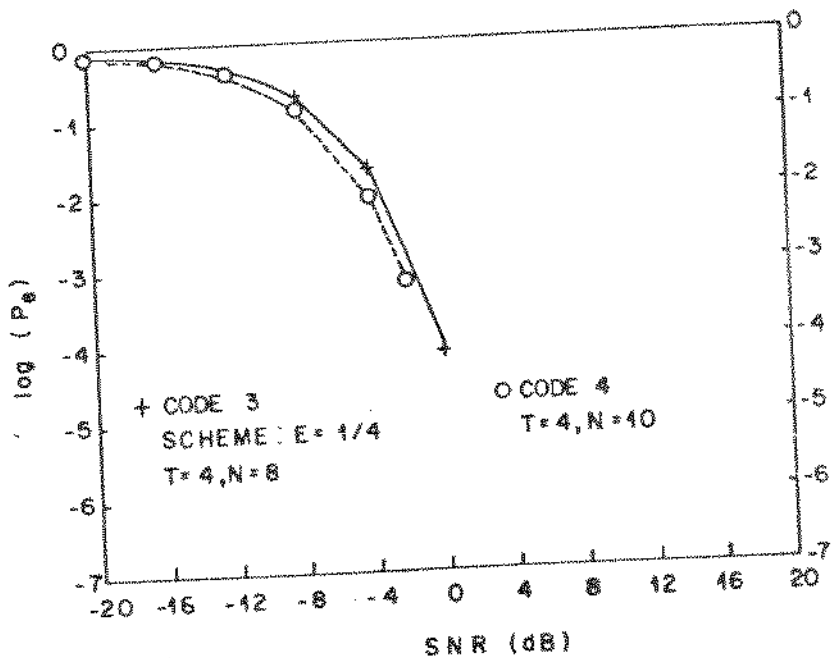


Fig. 5.2d - Sistema Banda Base On - Off ($E = 1/4$);
 Códigos $d_{\min} = 8$; Tabela 4.2

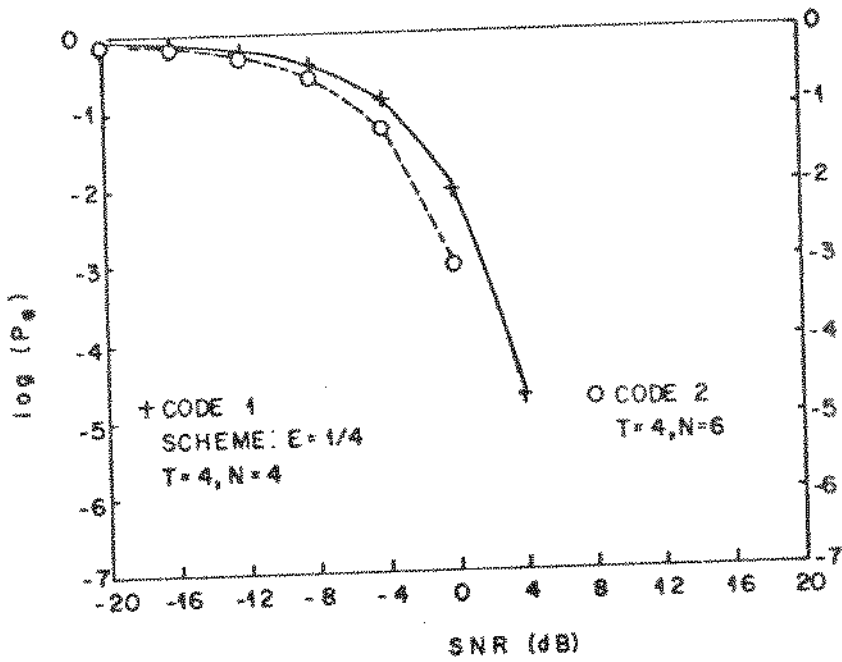


Fig. 5.2c - Sistema Banda Base On - Off ($E = 1/4$);
 Códigos $d_{\min} = 4$; Tabela 4.2;

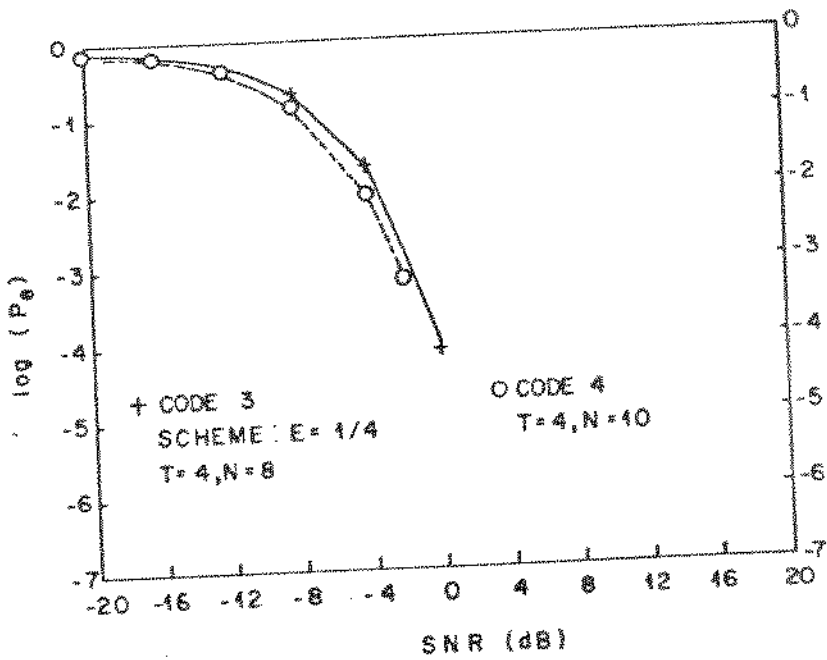


Fig. 5.2d - Sistema Banda Base On - Off ($E = 1/4$);
 Códigos $d_{\min} = 8$; Tabela 4.2

5.4 Comparação entre Esquemas de Decodificações

Nesta seção fazemos comparações dos esquemas de decodificações apresentandos nas seções 3.5 (Algoritmo de Wilson) e 5.2. Os códigos utilizados são os de Chang e Weldon (Capítulo 3, tabela 3.2) e os novos códigos (Capítulo 4, tabela 4.2).

5.4.1 Table Look-up versus o Algoritmo de Wilson

As figuras 5.3a e 5.3b mostram as curvas de desempenho do table look-up versus o algoritmo de Wilson para os códigos de Chang e Weldon, (Cap. 3, tabela 3.2) de parâmetros ($T = 6, N = 4, d_{\min} = 2$) e ($T = 12, N = 8, d_{\min} = 4$) para o canal AWGN e o sistema antipodal, ($E = 1$).

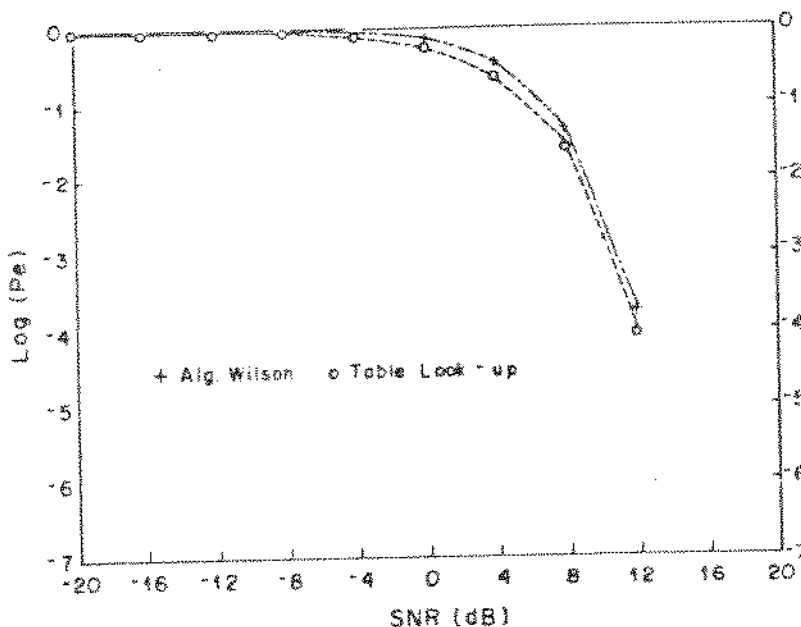


Fig. 5.3a - Código de Chang e Weldon;

$T = 6; N = 4; d_{\min} = 2$; Tabela 3.2;

Canal AWGN; Sistema Antipodal ($E = 1$);

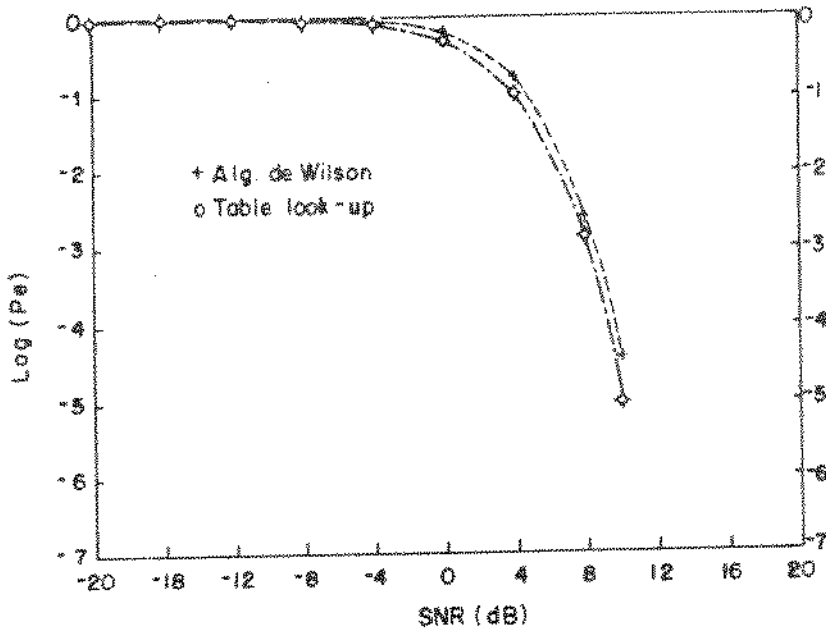


Fig. 5.3b - Código de Chang e Weldon;

$T = 12$; $N = 8$; $d_{\min} = 4$; Tabela 3.2;

Canal AWGN; Sistema Antipodal ($E = 1$);

Como podemos ver em ambas as figuras o table look-up apresenta um desempenho melhor do que o algoritmo de Wilson.

5.4.2 Table Look-up versus Algoritmo de Wilson Adaptado para os Novos Códigos.

As figuras 5.4a, 5.4b e 5.4c mostram as curvas de desempenho do table look-up versus o algoritmo de Wilson adaptado para os novos códigos e os códigos utilizados nas simulações são os códigos 1, 2 e 3, respectivamente, (Cap.4. Tabela 4.2). Aqui também verifica-se que a técnica de decodificação baseada no table look-up apresenta um melhor desempenho, em termos de ganho de decodificação versus probabilidade de erro, P_e , do que o algoritmo de Wilson. Por exemplo, o código 1, fig. 5.4a para uma relação sinal/ruído de 8 dB o algoritmo de Wilson apresenta uma probabilidade de erro, $P_e = 0.46 \times 10^{-1}$, enquanto que no table look-up, para esta mesma relação sinal/ruído, $P_e = 0.75 \times 10^{-3}$.

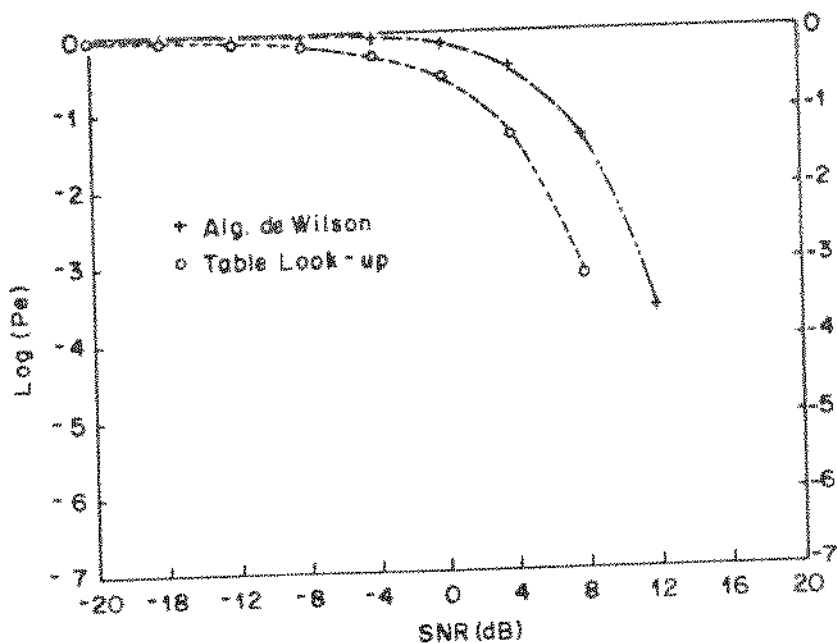


Fig. 5.4a - Código 1; $T = 4$; $N = 4$; $d_{\min} = 4$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$)

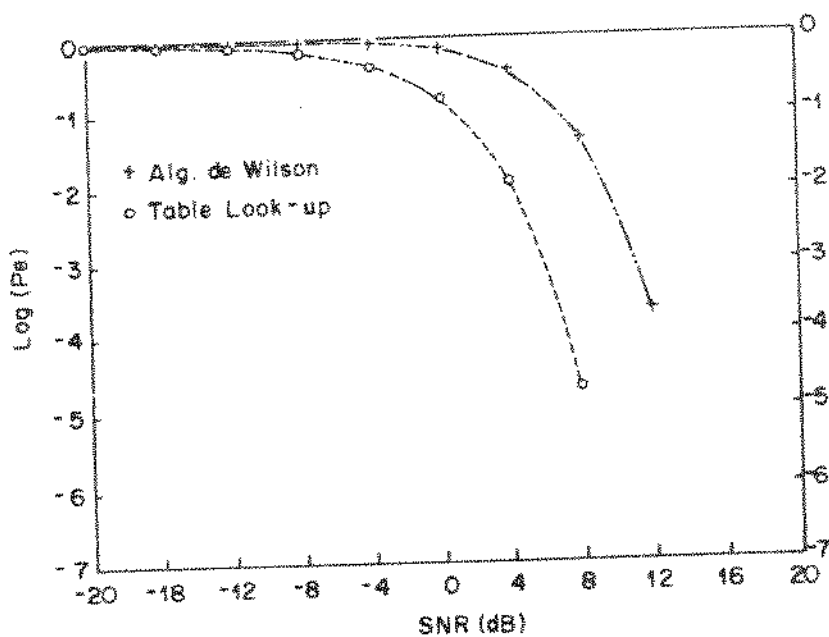


Fig. 5.4b - Código 2; $T = 4$; $N = 6$; $d_{\min} = 4$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$)

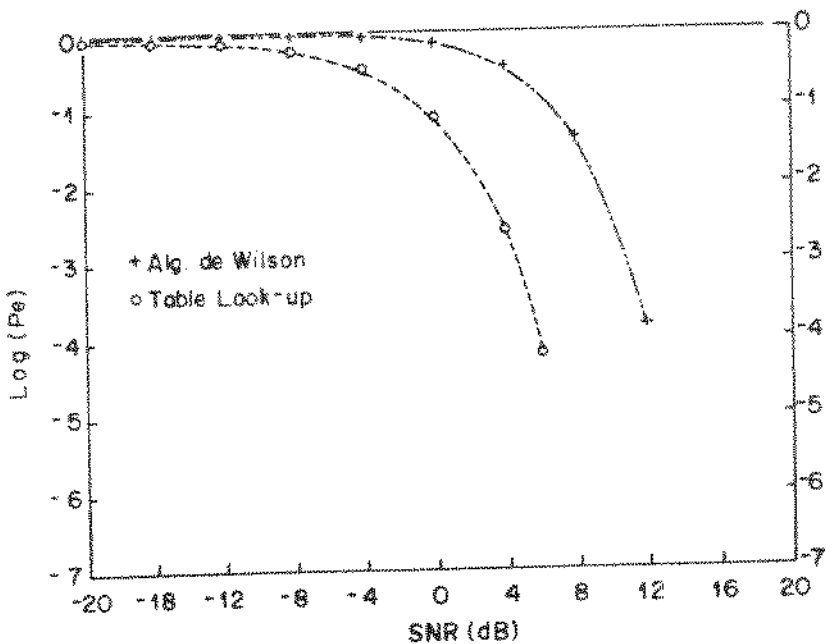


Fig. 5.4c - Código 3; $T = 4$; $N = 8$; $d_{\min} = 8$;
Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);

5.4.3 Técnica de Decodificação Combinada versus o Algoritmo de Wilson

As figuras 5.5a e 5.5b mostram as curvas de desempenho da técnica de decodificação combinada proposta na seção 5.2.3 versus o algoritmo de Wilson para os códigos de Chang e Weldon das figuras 5.3a e 5.3b,

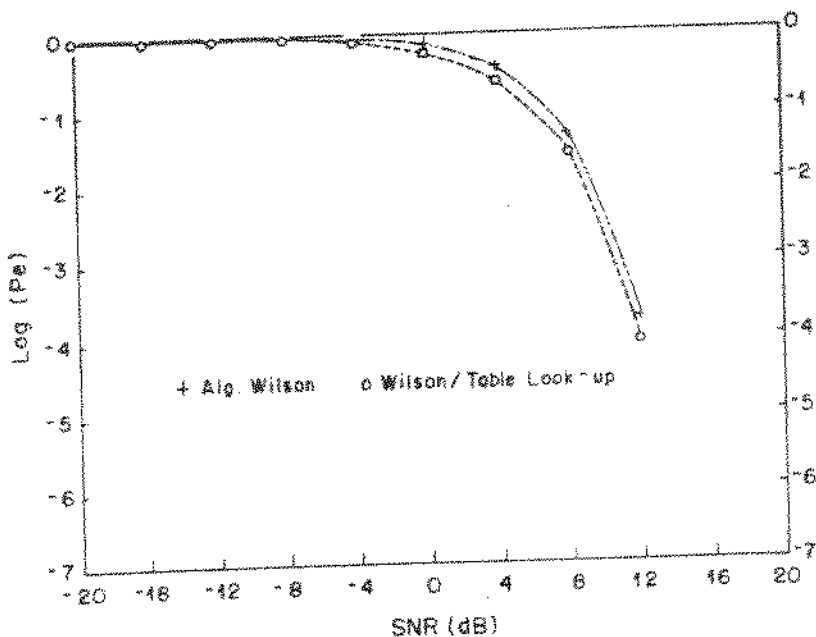


Fig. 5.5a - Código de Chang e Weldon;
 $T = 6$; $N = 4$; $d_{\min} = 2$; Tabela 3.2;
Canal AWGN; Sistema Antipodal ($E = 1$);

respectivamente. Como podemos ver em ambos os casos a técnica combinada apresenta um melhor desempenho do que o algoritmo de Wilson.

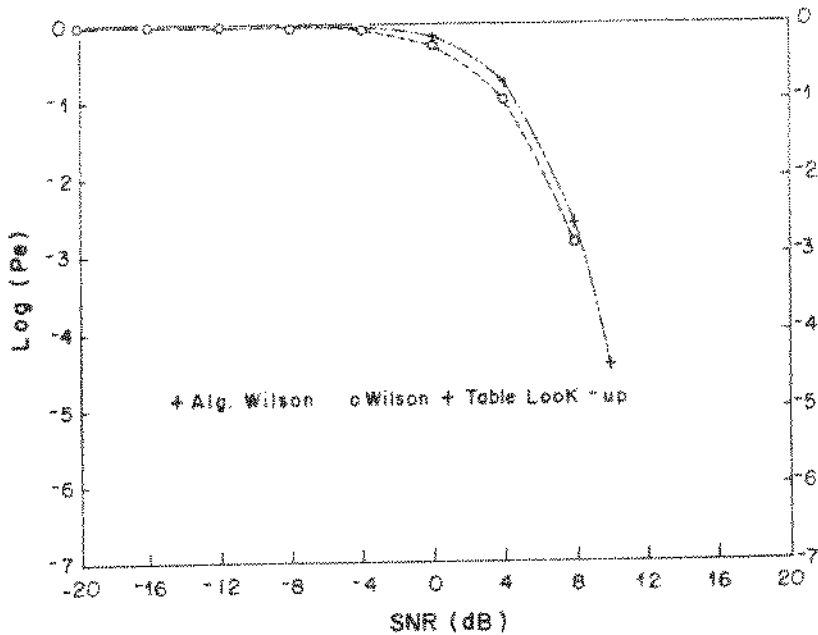


Fig. 5.5b - Código de Chang e Weldon;
 $T = 12$; $N = 8$; $d_{\min} = 4$; Tabela 3.2;
 Canal AWGN; Sistema Antipodal ($E = 1$);

5.4.4 Técnica de Decodificação Combinada versus Algoritmo de Wilson Adaptado para os Novos Códigos

As figuras 5.6a, 5.6b e 5.6c apresentam os desempenhos da técnica de decodificação combinada versus o algoritmo de Wilson adaptado para os novos códigos, para os códigos 1, 2 e 3, (Tabela 4.2), respectivamente. Como se pode ver a técnica combinada apresenta um melhor desempenho do que o algoritmo de Wilson adaptado. Por exemplo, o código 1, fig. 5.6a, para uma relação sinal/ruído de 8 dB o algoritmo de Wilson adaptado apresenta uma probabilidade de erro $P_e = 0.46 \times 10^{-1}$ enquanto que a técnica combinada $P_e = 0.75 \times 10^{-3}$.

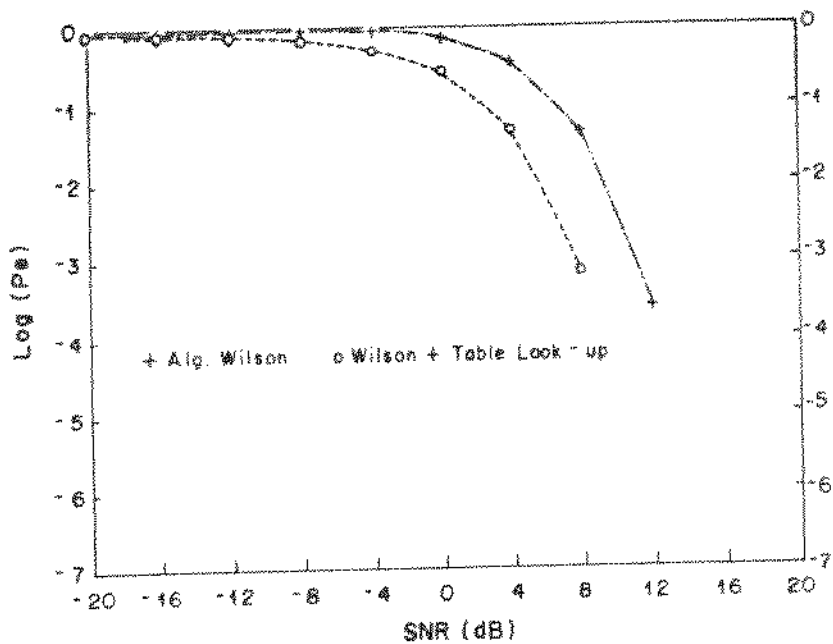


Fig. 5.6a - Código 1; $T = 4$; $N = 4$; $d_{\min} = 4$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);

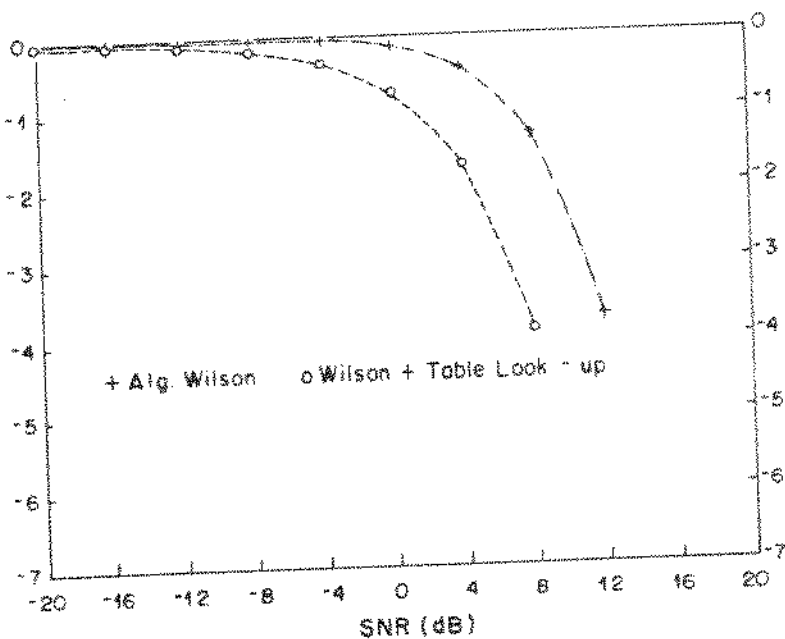


Fig. 5.6b - Código 2; $T = 4$; $N = 6$; $d_{\min} = 4$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);

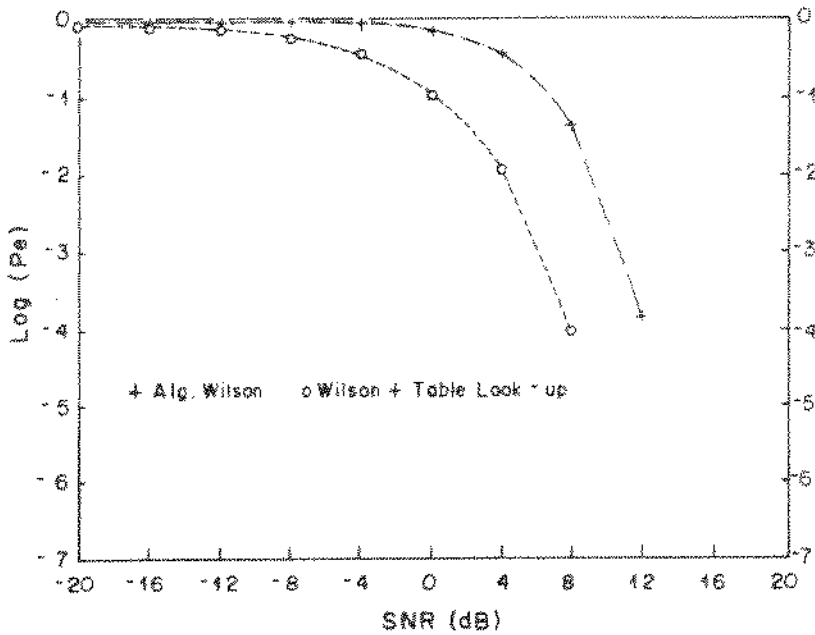


Fig. 5.6c - Código 3; $T = 4$; $N = 8$; $d_{\min} = 8$;
Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);

5.4.5 Table Look-up versus Técnica de Decodificação Combinada

As curvas de desempenho do table look-up versus a técnica de decodificação combinada são mostrados nas figuras 5.7a e 5.7b para os códigos de Chang e Weldon das figuras 5.3a e 5.3b, respectivamente e nas figuras 5.8a, 5.8b e 5.8c para os códigos 1, 2 e 3, respectivamente, da tabela 4.2. Como podemos ver, nas figuras 5.7a, 5.7b e 5.8a os desempenhos dos dois esquemas de decodificação são iguais, enquanto que nas figuras 5.8b e 5.8c o esquema baseado na técnica do table look-up é melhor do que a técnica combinada. Isto deve-se ao fato de que na técnica de decodificação combinada seja possível que a equação (5.1) tenha solução binária, porém o vetor decodificado Z' não seja o vetor transmitido Z , erro este que é detectado pelo table look-up, o que faz com que este último algoritmo de decodificação apresente um desempenho melhor do que a técnica combinada.

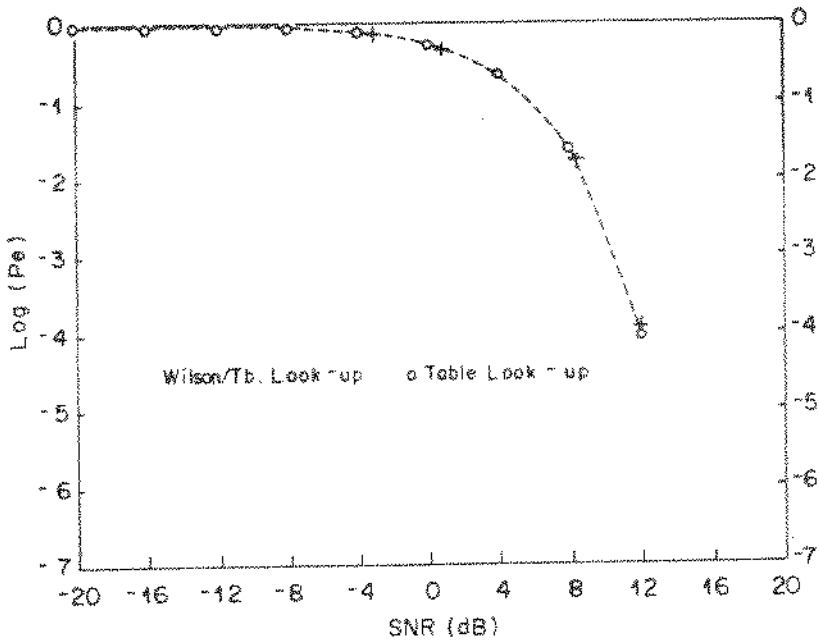


Fig. 5.7a - Código de Chang e Weldon;
 $T = 6$; $N = 4$; $d_{\min} = 2$; Tabela 3.2;
 Canal AWGN; Sistema Antipodal ($E = 1$);

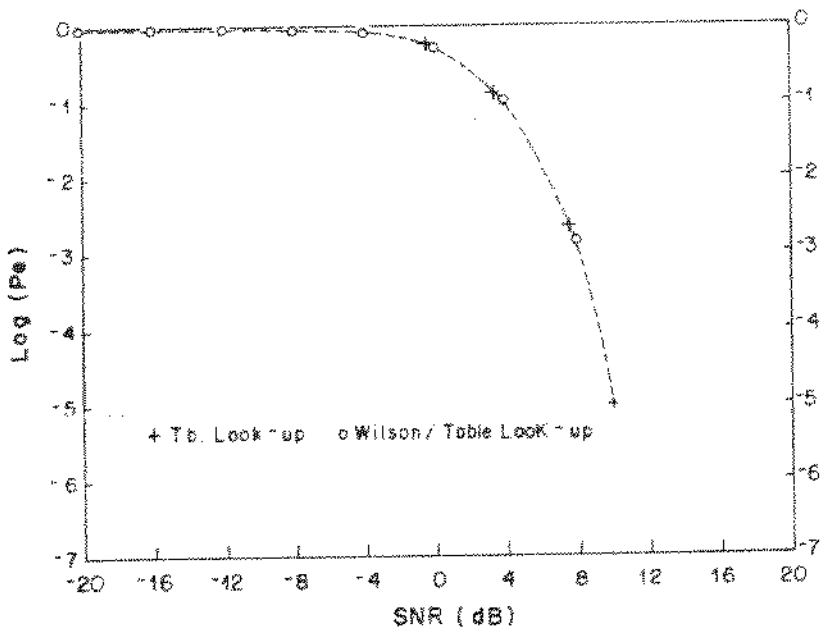


Fig. 5.7b - Código de Chang e Weldon;
 $T = 12$; $N = 8$; $d_{\min} = 4$; Tabela 3.2;
 Canal AWGN; Sistema Antipodal ($E = 1$);

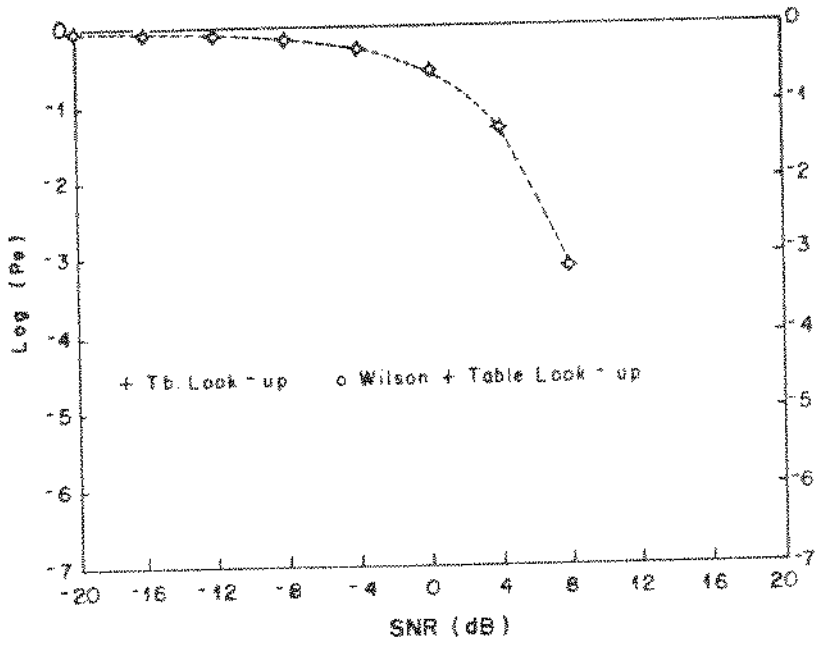


Fig. 5.8a - Código 1; $T = 4$; $N = 4$; $d_{\min} = 4$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);

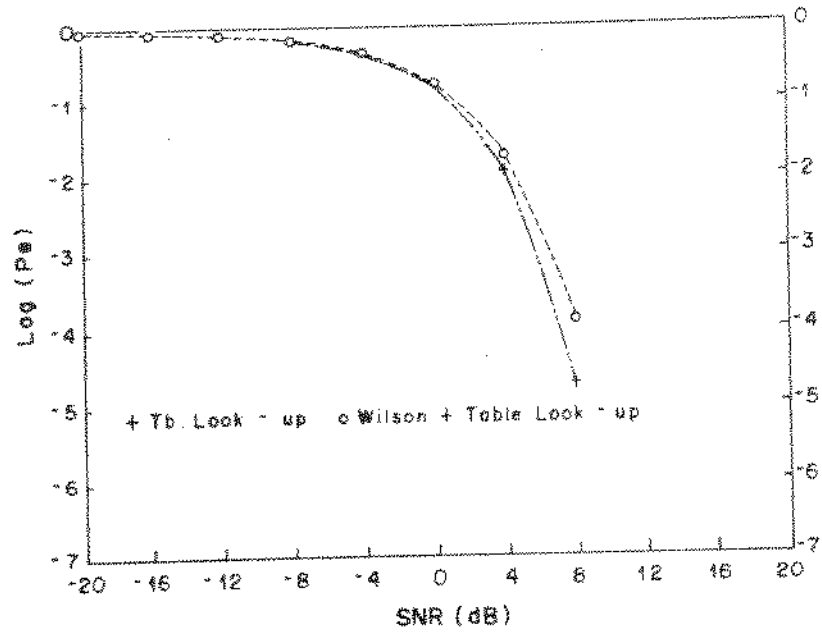


Fig. 5.8b - Código 2; $T = 4$; $N = 6$; $d_{\min} = 4$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);

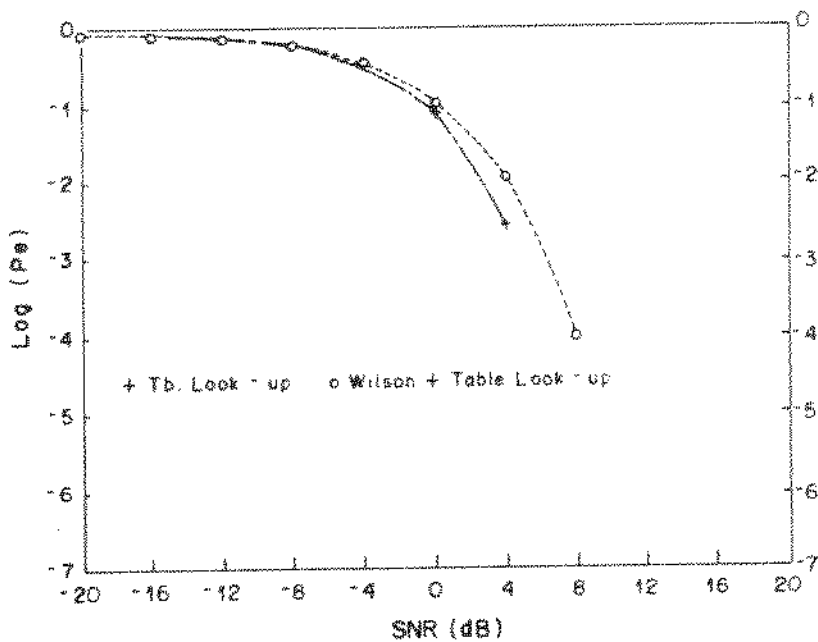


Fig. 5.8c - Código 3; $T = 4$; $N = 8$; $d_{\min} = 8$;
Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);

5.4.6 Comparações entre os Esquemas de Decodificação por Decisão Suave e por Decisão Abrupta

As figuras 5.9a e 5.9b apresentam o desempenho da decodificação por decisão suave (S/D) com 1 bit de confiança versus a decodificação por decisão abrupta (H/D) para os códigos 1 e 3, respectivamente, da tabela 4.2. O algoritmo de decodificação utilizado no processo de decodificação é o table look-up. Como era de se esperar, o esquema (S/D) é superior ao esquema (H/D). Isto deve-se ao fato de que na decodificação por decisão suave, em média, o vetor quantizado Y_Q estar mais próximo do vetor recebido Y_{AWGN} , do que no caso de decisão abrupta.

As figuras 5.10a e 5.10b apresentam as curvas de desempenho do esquema (S/D) com 1 e 2 bits de confiança, para os códigos 1 e 3, respectivamente. Conforme podemos ver, a decodificação suave com 2 bits de confiança apresenta um melhor desempenho do que a decodificação suave com 1 bit de confiança. Isto deve-se ao fato de que quanto maior for o número de bits de confiança no processo de quantização mais próximo do vetor recebido se encontra o vetor quantizado. Aqui também, o algoritmo de decodificação utilizado foi o table look-up.

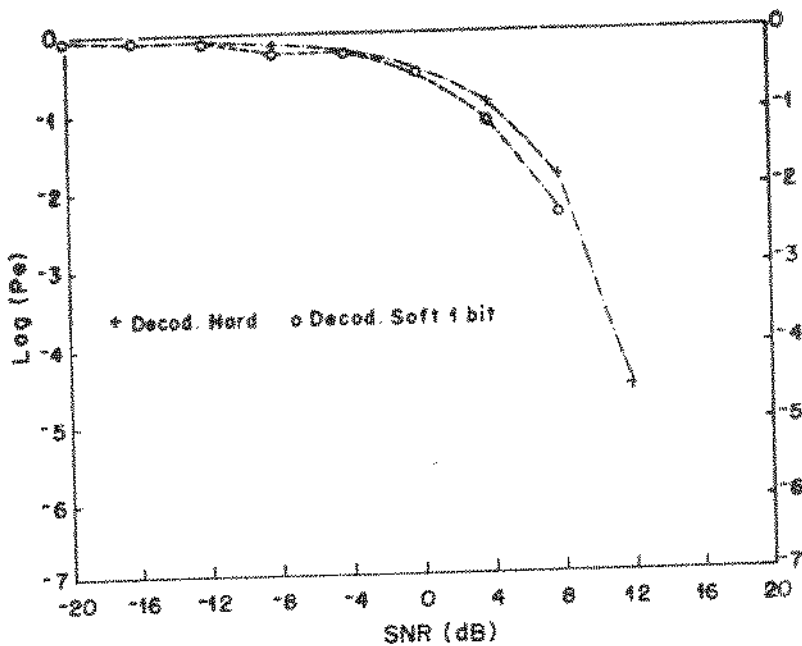
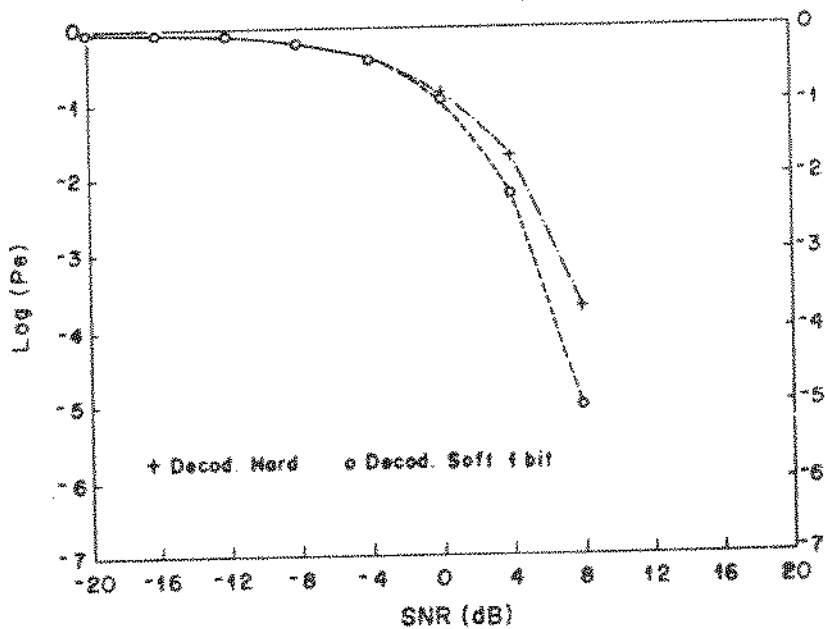


Fig. 5.9a - Código 1; $T = 4$; $N = 4$; $d_{\min} = 4$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);
 Table Look-up



5.9b - Código 3; $T = 4$; $N = 8$; $d_{\min} = 8$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);
 Table Look-up

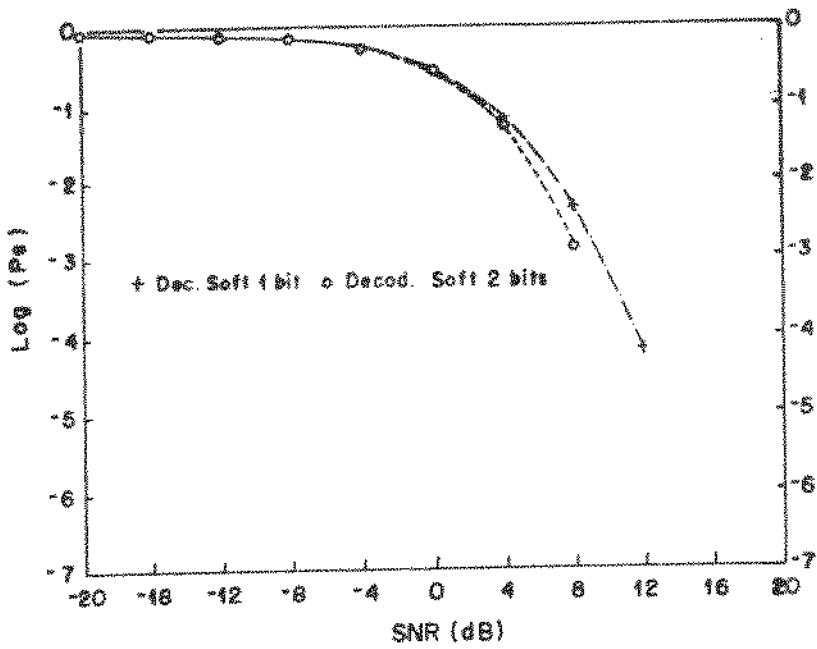


Fig. 5.10a - Código 1; $T = 4$; $N = 4$; $d_{\min} = 4$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);
 Table Look-up

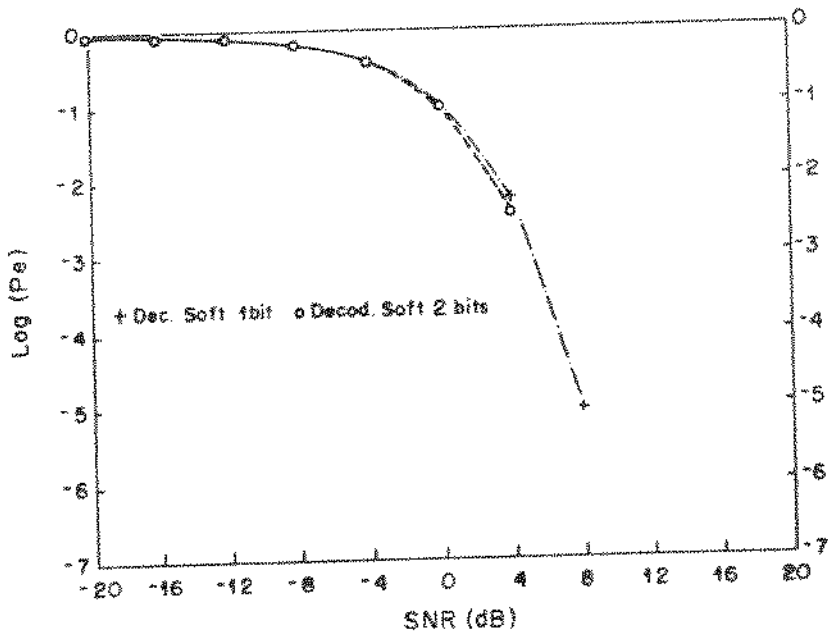


Fig. 5.10b - Código 3; $T = 4$; $N = 8$; $d_{\min} = 8$;
 Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);
 Table Look-up

As figuras 5.11a e 5.11b apresentam as curvas de desempenho do esquema (S/D) com 2 e 3 bits de confiança para os códigos 1 e 3, respectivamente. Também nestes casos vemos que a decodificação suave com 3 bits de confiança apresenta um melhor desempenho do que a decodificação com dois bits de confiança.

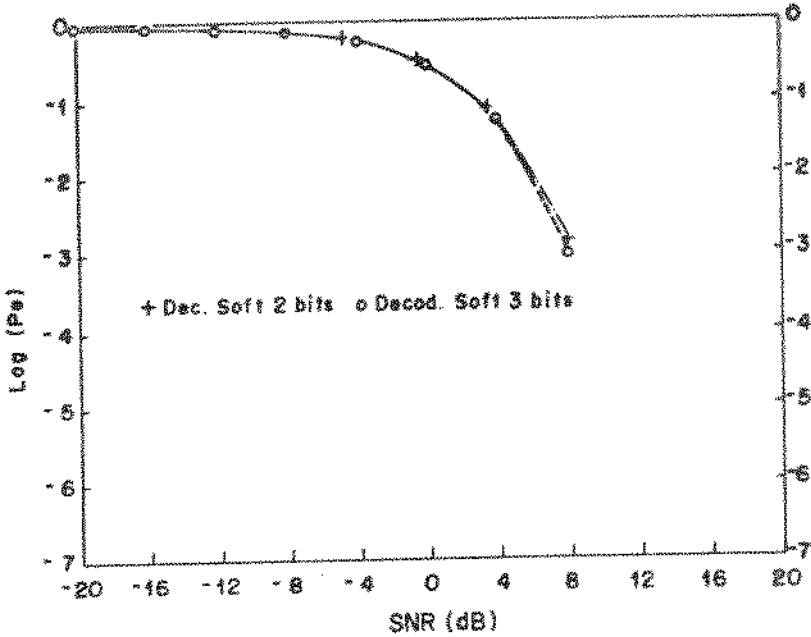


Fig. 5.11a - Código 1; $T = 4$; $N = 4$; $d_{\min} = 4$;
Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);
Table Look-up

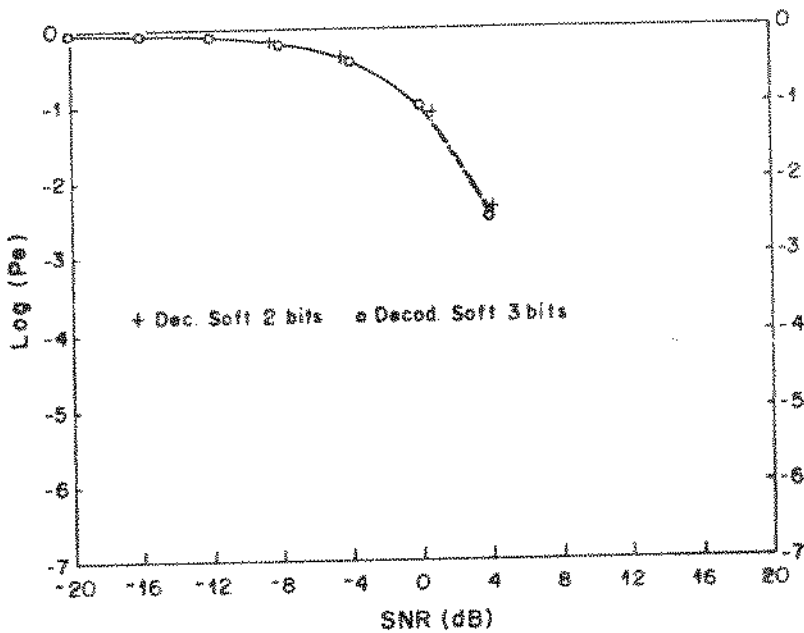


Fig. 5.11b - Código 3; $T = 4$; $N = 8$; $d_{\min} = 8$;
Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);
Table Look-up

As figuras 5.12a e 5.12b apresentam os desempenhos das decodificações por decisão abrupta (H/D) e decisões suaves (S/D) com 1, 2 e 3 bits de confiança para os códigos 1 e 3, respectivamente. Estas figuras mostram o comportamento do incremento de ganho de decodificação quando se passa do esquema (H/D) para o esquema (S/D) de 1 bit de confiança, deste para o esquema (S/D) com 2 bits e do esquema com dois bits para o esquema com 3 bits de confiança. Este incremento é menor quanto maior for o valor do número NBSOFT de bits de confiança. Um esquema com NBSOFT = 4 bits para estes códigos traria ganho desprezível em relação as curvas com NBSOFT = 3, indicando que, como em outras aplicações [35] o esquema (S/D) com 3 bits de confiança pode ser o mais apropriado em termos do binômio complexidade e ganho de decodificação.

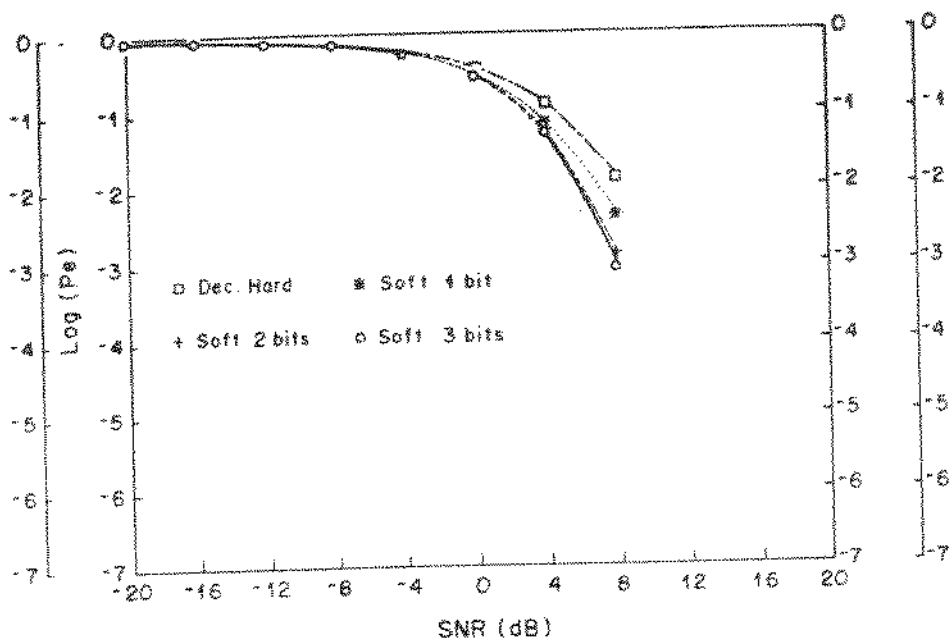


Fig. 5.12a - Código 1; $T = 4$; $N = 4$; $d_{\min} = 4$;
Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);
Table Look-up

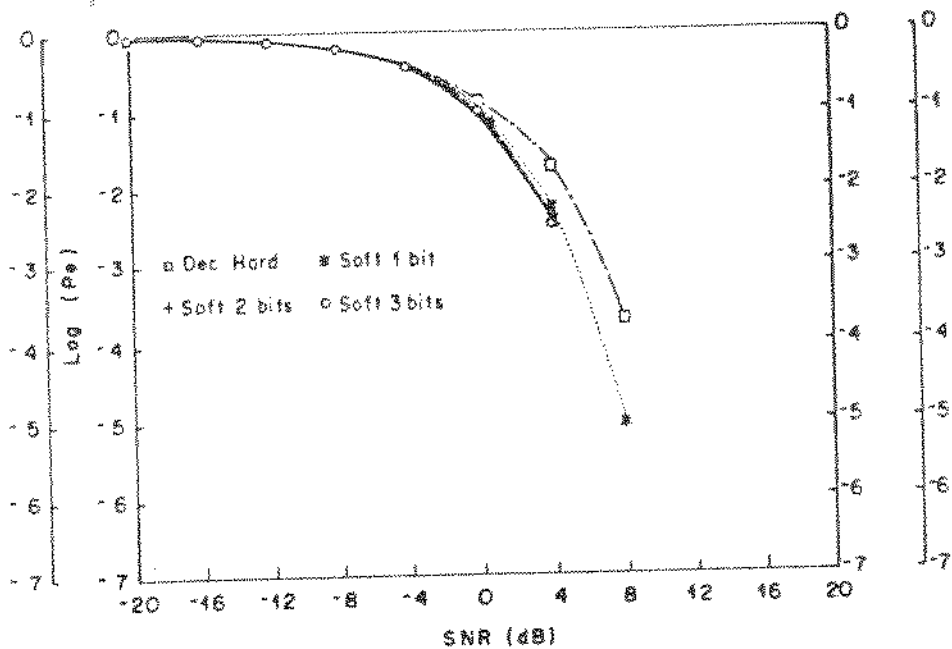


Fig. 12b - Código 3; $T = 4$; $N = 8$; $d_{\min} = 8$;
Tabela 4.2; Canal AWGN; Sistema Antipodal ($E = 1$);
Table Look-up

5.5 Conclusão

Neste capítulo apresentamos propostas de algoritmos de decodificação para os códigos de Chang e Weldon [1], John H. Wilson [3] e para os códigos introduzidos pelo corolário 4.1 (cap. 4). As técnicas são baseadas no table look-up, numa adaptação do algoritmo de Wilson para os códigos apresentados no capítulo 4 e numa combinação destas duas técnicas de decodificações. Também apresentamos as técnicas de decodificação por decisão suave (S/D) e por decisão abrupta (H/D).

Através de simulações para o canal DMC e para o canal AWGN T - usuários foram apresentadas curvas de desempenho de probabilidade de erro para diversos códigos de Chang e Weldon (caso particular dos códigos de Wilson) e para os códigos do capítulo 4, usando as várias técnicas de decodificações.

Capítulo VI

Conclusões Finais

Neste trabalho apresentamos uma classe de códigos corretores de erros para o canal AWGN T - usuários, corolário 4.1, e propomos novas técnicas de decodificação para o sistema de comunicação T - usuários.

No capítulo 2 apresentamos o sistema de comunicação objeto deste trabalho e enfocamos os esquemas de codificações existentes na literatura para os sistemas de comunicações dois usuários com e sem ruído. Na seção 2.4.1 tratamos da capacidade do canal Aditivo T - Usuários sem ruído e julgamos necessário ressaltar que a demonstração dada para a obtenção da expressão algébrica que determina a capacidade deste canal é de autoria do autor deste trabalho, uma vez que não nos foi possível obtê-la na literatura.

No capítulo 3 mostramos a classe de códigos unívocamente decodificáveis e a classe de códigos com distância mínima, $d_{\min} = 2^i$, $i \geq 1$ propostas por Chang e Weldon [1]. Também mostramos como Chang [11] obteve, a partir dos códigos unívocamente decodificáveis de [1], uma outra classe de códigos unívocamente decodificáveis para o canal T - usuários. Na seção 3.3 é mostrada as generalizações feitas por Thomas J. Ferguson [2] dos códigos de Chang e Weldon. A seção 3.4 mostra como John H. Wilson [3] generalizou os códigos de Chang e Weldon e obteve uma classe de códigos corretores de erros para o canal T - usuários. Na seção 3.5 mostramos o algoritmo de decodificação proposto por Chang e Weldon para os códigos unívocamente decodificáveis apresentados na seção 3.2, bem como o algoritmo de decodificação proposto por Wilson para a classe de códigos corretores de erros apresentados na seção 3.4.

No capítulo 4, seção 4.2, apresentamos uma classe de códigos corretores de erros, corolário 4.1, para o canal T - usuários. Esta classe de códigos é obtida a partir de uma aplicação do teorema de Wilson, (teor. 3.7), para matrizes diferença que definam no nível D_0 códigos dois usuários δ - decodificáveis.

Na seção 4.3 damos uma generalização, via a noção de classes de equivalência, conforme Ferguson [2], para os códigos introduzidos pelo corolário 4.1. Esta generalização é feita via dois caminhos:

- o primeiro é considerar a matriz diferença D_0 que define os códigos dois usuários δ -decodificáveis da tabela 4.1, multiplicá-la por matrizes de permutações generalizadas, conforme Ferguson e aplicar o corolário 4.1 para esta nova matriz, isto é, fazer o produto de Kronecker desta matriz por uma matriz diferença que satisfaça as hipóteses do corolário 4.1, por exemplo, as matrizes de Hadamard de ordem q e, desta forma obter uma matriz diferença que define um código 2. q -usuários de comprimento $q.N$ e distância mínima $d_{\min} = q.\delta$, onde N é o comprimento do código definido pela matriz D_0 ;
- o segundo caminho é considerar as matrizes diferença dos códigos dois usuários da tabela 4.1, fazer o produto de Kronecker por uma matriz diferença que satisfaça as hipóteses do corolário 4.1, por exemplo, as matrizes de Hadamard e multiplicar esta nova matriz por matrizes de permutações generalizadas, segundo Ferguson.

No capítulo 5 apresentamos novas propostas de algoritmos de decodificação para os códigos de Chang e Weldon, códigos de Wilson e para os códigos introduzidos pelo corolário 4.1 do capítulo 4. Estas propostas são: a técnica de decodificação baseada no table look-up, o algoritmo de Wilson adaptado para os códigos apresentados no capítulo 4, uma combinação destas duas técnicas de decodificação, seção 5.2.3 e as técnicas de decodificação por decisão suave, seção 5.2.3, que incorporadas às anteriores melhora o desempenho final do sistema T - usuários.

Na seção 5.3 apresentamos resultados de simulações para o canal discreto sem memória e para o canal AWGN T - usuários, utilizando a técnica de decodificação baseada no table look-up e os códigos do capítulo 4, tabela 4.2, de parâmetros $(T = 4, N = 4, d_{\min} = 4)$, $(T = 4, N = 6, d_{\min} = 4)$, $(T = 4, N = 8, d_{\min} = 8)$ e $(T = 4, N = 10, d_{\min} = 8)$, denominados códigos 1, 2, 3 e 4, respectivamente. Para o canal AWGN T - usuários os sistemas considerados foram o sistema banda base antipodal e o sistema banda base on - off, conforme seção 5.3.2. Comparações entre os diversos esquemas de decodificação para o canal AWGN são mostrados na seção 5.4. Os códigos utilizados nas simulações foram os códigos de

Chang e Weldon, capítulo 3, tabela 3.2, de parâmetros ($T = 6$, $N = 4$, $d_{\min} = 2$), ($T = 12$, $N = 8$, $d_{\min} = 4$) e os códigos denominados de códigos 1, 2 e 3. Nas diversas comparações feitas, verificamos que o esquema de decodificação que apresenta melhor desempenho é a técnica de decodificação baseada no table look-up, porém com complexidade computacional (memória e número de computações) que cresce exponencialmente com o número de usuários - T .

Por outro lado a técnica de decodificação apresentada na seção 5.2.3 combina a simplicidade computacional do algoritmo de Wilson com o maior poder de correção do table look-up e pode contribuir no sentido de diminuir o número de computações necessário no esquema combinado aliado ao fato de apresentar um ganho de decodificação igual (figs. 5.7a, 5.7b e 5.8a) ou um pouco menor (figs. 5.8b e 5.8c) quando comparado com o esquema de decodificação baseado na técnica do table look-up.

Nas comparações feitas entre os esquemas de decodificação por decisão suave e por decisão abrupta verificamos que o primeiro apresenta um desempenho melhor do que o segundo e que dentre os esquemas de decodificação por decisão suave aquele que apresenta um melhor desempenho em termos do binômio ganho de decodificação versus complexidade é aquele em que o número de bits de confiança, NBSOFT é igual a 3, isto é, o esquema com 8 níveis de quantização.

Como sugestão para futuros trabalhos apresentamos os seguintes temas:

- verificar se as duas formas de generalizar os códigos apresentados no capítulo 4 via a noção de classes de equivalência determinam classes de códigos equivalentes por permutações de linhas e colunas das matrizes diferença ou, segundo Ferguson: dada uma das formas será que existem matrizes de permutações generalizadas tais que uma forma é equivalente a outra ?
- aplicar o corolário 4.1 para matrizes diferença que também satisfaçam as suas hipóteses, como por exemplo as matrizes conferência;
- pesquisar sequências de sincronismos [10, 14] para os codificadores que permitam ao decodificador, após a recepção de cada uma delas, estabelecer sincronismo de bloco com o codificador que a enviou;

- procurar esquemas mais complexos de correção de erro que apresentem estruturas de códigos lineares de bloco ou estruturas de códigos convolucionais [8] a fim de utilizar-se dos esquemas de decodificação clássicos que permitam um maior ganho de codificação comparados aos esquemas apresentados neste trabalho;
- construir novos códigos com distâncias mínimas maiores ou iguais às da classe de códigos apresentada neste trabalho, porém com taxa $R(T) > 1$, como sugerido em [1, 36].

APÉNDICE

Vamos mostrar que,

$$\left(\begin{array}{c} T \\ \left[\frac{T}{2} \right] \end{array} \right) < \frac{2^T}{\sqrt{\pi(T/2)}} \quad (\text{A.1})$$

ou, equivalentemente,

$$\frac{2^T}{\left(\begin{array}{c} T \\ \left[\frac{T}{2} \right] \end{array} \right)} > \sqrt{\pi(T/2)} \quad (\text{A.2})$$

A demonstração desta desigualdade é dividida em dois casos:

1º Caso : Suponha T par, isto é, $T = 2N$. Sabemos de [13, pp. 466] que,

$$\left(\begin{array}{c} N \\ \lambda N \end{array} \right) \leq \frac{\lambda^{-\lambda N} \cdot \mu^{-\mu N}}{\sqrt{2\pi N \lambda \mu}} \quad (\text{A.3})$$

onde $\mu = 1 - \lambda$.

Fazendo em (A.1) $T = 2N$,

$$\lambda = \frac{\left[\frac{2N}{2} \right]}{2N} = 1/2$$

e $\mu = 1 - \lambda = 1/2$, então de (A.3) temos,

$$\begin{aligned} \begin{pmatrix} T \\ \left[\frac{T}{2} \right] \end{pmatrix} &= \begin{pmatrix} T \\ \lambda T \end{pmatrix} \approx \frac{(1/2)^{(-1/2)T} \cdot (1/2)^{(-1/2)T}}{\sqrt{2\pi T(1/4)}} \\ &= \frac{(1/2)^{-T}}{\sqrt{\pi(T/2)}} = \frac{2^T}{\sqrt{\pi(T/2)}} \end{aligned}$$

e, portanto, a desigualdade é verdadeira para T par.

2º Caso : $T = 2N + 1$. Devemos mostrar que,

$$\frac{2^{2N+1}}{\binom{2N+1}{N}} > \sqrt{\pi \cdot (2N+1)/2}$$

ou, equivalentemente,

$$\frac{2^{2N+1}}{\binom{2N+1}{N}} - \sqrt{\pi \cdot (2N+1)/2} > 0 \quad (\text{A.4})$$

Desde que a desigualdade é verdadeira para T par, temos:

$$\frac{2^{2N+2}}{\binom{2N+2}{N+1}} - \sqrt{\pi \cdot (N+1)} > 0 \quad (\text{A.5})$$

e, desta forma a demonstração fica concluída se mostrarmos que o 1º membro da inequação (A.4) é maior do que o 1º membro da inequação (A.5), isto é,

$$\frac{2^{2N+1}}{\binom{2N+1}{N}} - \sqrt{\pi \cdot (2N+1)/2} > \frac{2^{2N+2}}{\binom{2N+2}{N+1}} - \sqrt{\pi \cdot (N+1)}$$

se, e somente se,

$$\frac{2^{2N+1}}{\binom{2N+1}{N}} - \frac{2^{2N+2}}{\binom{2N+2}{N+1}} > \sqrt{\pi \cdot (2N+1)/2} - \sqrt{\pi \cdot (N+1)}$$

se, e somente se,

$$\frac{2^{2N+1} \cdot N! \cdot (N+1)!}{(2N+1)!} - \frac{2^{2N+2} \cdot (N+1)! \cdot (N+1)!}{(2N+2)!} > \sqrt{\pi} \left(\sqrt{N+1/2} - \sqrt{N+1} \right)$$

se e somente se,

$$\frac{2^{2N+1} \cdot N! \cdot (N+1)!}{(2N+1)!} \left(1 - \frac{2(N+1)}{2N+2} \right) > \sqrt{\pi} \left(\sqrt{N+1/2} - \sqrt{N+1} \right)$$

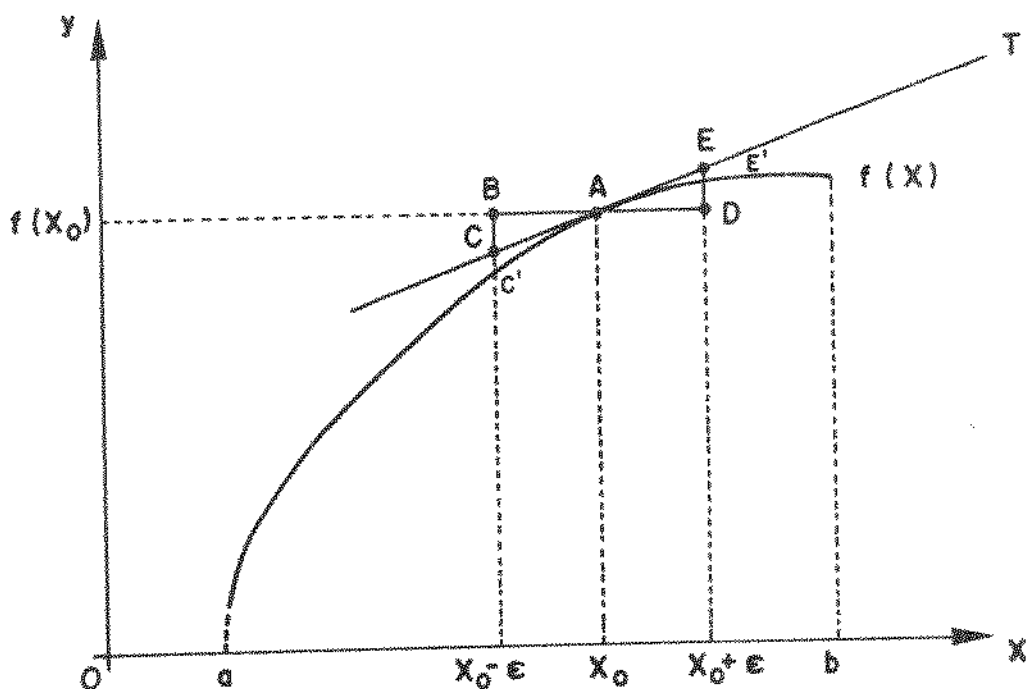
e, desde que o lado esquerdo desta desigualdade é zero e o lado direito é negativo, a desigualdade é verdadeira.

Uma demonstração mais elegante, do ponto de vista matemático, para o caso 2 é apresentada a seguir e para isto, faz-se necessário a demonstração dos teoremas A.1 e A.2.

Teorema A.1 : Seja $f : [a, b] \rightarrow \mathbb{R}_+$ uma função de classe C^2 tal que $f''(x) < 0, \forall x \in (a, b)$. Então $\forall x_0 \in (a, b)$ e $\forall \varepsilon > 0$ tal que $(x_0 - \varepsilon, x_0 + \varepsilon) \subset (a, b)$, temos,

$$f(x_0) > 1/(2\varepsilon) \int_{x_0-\varepsilon}^{x_0+\varepsilon} f(x) dx \quad (A.6)$$

Demonstração : Desde que $f''(x) < 0$ segue que $\forall x_0 \in (a, b)$ a reta tangente no ponto x_0 ao gráfico de f se encontra sobre o gráfico de f , conforme figura abaixo.



Agora os triângulos ABC e ADE são semelhantes, pois têm todos os ângulos congruentes.

Sejam A_1 = a área limitada pelos segmentos de retas $\overline{C'B}$, \overline{BA} e pelo gráfico de f no intervalo $(x_0 - \epsilon, x_0)$;

A_2 = a área limitada pelos segmentos de retas \overline{AD} , $\overline{DE'}$ e pelo gráfico de f no intervalo $(x_0, x_0 + \epsilon)$;

A_{t_1} = a área do triângulo ABC;

A_{t_2} = a área do triângulo ADE;

Temos que,

$$A_1 > A_{t_1} = A_{t_2} > A_2$$

Por outro lado,

$$\begin{aligned} \int_{x_0 - \epsilon}^{x_0 + \epsilon} f(x) dx &= \epsilon \cdot f(x_0) - A_1 + \epsilon \cdot f(x_0) + A_2 \\ &= 2\epsilon \cdot f(x_0) - A_1 + A_2 \end{aligned}$$

e desde que $-A_1 + A_2 < 0$, temos,

$$\int_{x_0 - \epsilon}^{x_0 + \epsilon} f(x) dx < 2\epsilon \cdot f(x_0)$$

portanto,

$$f(x_0) > (1/2\epsilon) \int_{x_0 - \epsilon}^{x_0 + \epsilon} f(x) dx$$

Teorema A.2 : Sejam $f, g : [a, b] \rightarrow \mathbb{R}$ funções de classe C^1 tais que:

i) $\exists x_0 \in [a, b]$ tal que $f(x_0) > g(x_0)$;

ii) $f'(x) > g'(x), \forall x \in [x_0, b]$;

Então,

$$f(x) > g(x), \forall x \in [x_0, b]$$

Demonstração : Seja $h(x) = f(x) - g(x)$. Então de (i) temos,

$$h(x_0) > 0$$

de (ii) $h'(x) > 0, \forall x \in [x_0, b]$, portanto $h(x)$ é uma função estritamente crescente no intervalo $[x_0, b]$. Desta forma temos que,

$$h(x) > h(x_0) > 0, \forall x \in (x_0, b]$$

logo,

$$f(x) > g(x), \forall x \in (x_0, b]$$

Agora vamos demonstrar a desigualdade (A.2) para $T = 2n$, isto é,

$$\frac{2^{2n}}{\binom{2n}{n}} > \sqrt{\pi n}$$

\iff

$$4^n > \frac{(2n!) \cdot \sqrt{\pi n}}{n! n!}$$

↔

$$4^n > \prod_{i=1}^n \frac{(n+1)}{i} \sqrt{\pi n}$$

↔

$$\log 4^n > \log \sqrt{\pi n} + \sum_{i=1}^n (\log(n+1) - \log(i))$$

Agora a função logarítmica goza das seguintes propriedades,

$$\log(i) > \int_{i-1/2}^{i+1/2} \log x \, dx, \quad i \geq 2 \quad (\text{A.7})$$

$$\log(i) < \int_1^{i+1} \log x \, dx, \quad i \geq 1 \quad (\text{A.8})$$

A desigualdade (A.8) é trivial e (A.7) é um corolário do teorema A.1 tomando $\varepsilon = 1/2$.

Agora, de (A.7) temos,

$$- \int_{i-1/2}^{i+1/2} \log x \, dx > - \log(i), \quad i \geq 2$$

então,

$$- \sum_{i=2}^n \int_{i-1/2}^{i+1/2} \log x \, dx > - \sum_{i=2}^n \log(i)$$

→

$$- \int_{3/2}^{n+1/2} \log x \, dx > - \sum_{i=2}^n \log(i) \quad (\text{A.9})$$

De (A.8) temos,

$$\int_1^{i+1} \log x \, dx > \log(i), \quad i \geq 1$$

e, portanto,

$$\sum_{i=1}^n \int_{n+i}^{n+i+1} \log x \, dx > \sum_{i=1}^n \log(n+1)$$

→

$$\int_{n+1}^{2n+1} \log x \, dx > \sum_{i=1}^n \log(n+1) \quad (\text{A.10})$$

Somando (A.9) com (A.10), obtemos a seguinte desigualdade,

$$\int_{n+1}^{2n+1} \log x \, dx - \int_{3/2}^{n+1/2} \log x \, dx > \sum_{i=1}^n (\log(n+1) - \log(i)) \quad (\text{A.11})$$

Por outro lado,

$$\int \log x \, dx = x(\log x - 1)$$

e, portanto,

$$\begin{aligned} \int_{n+1}^{2n+1} \log x \, dx - \int_{3/2}^{n+1/2} \log x \, dx &= x(\log x - 1) \Big|_{n+1}^{2n+1} - x(\log x - 1) \Big|_{3/2}^{n+1/2} \\ &= (2n+1)\{\log(2n+1) - 1\} - (n+1)\{\log(n+1) - 1\} - \\ &\quad - (n+1/2)\{\log(n+1/2) - 1\} + (3/2)\{\log(3/2) - 1\} \\ &= (2n+1)\log(2n+1) - 2n - 1 - (n+1)\log(n+1) + n + 1 - \\ &\quad - (n+1/2)\log(n+1/2) + n + 1/2 + (3/2)\log(3/2) - 3/2 \\ &= (2n+1)\log(2n+1) - (n+1)\log(n+1) - \\ &\quad - (n+1/2)\log(n+1/2) + (3/2)\log(3/2) - 1 \\ &= \log \left(\frac{(2n+1)^{2n+1}}{(n+1)^{n+1} (n+1/2)^{n+1/2}} \right) + (3/2)\log(3/2) - 1 \end{aligned}$$

e, de (A.11)

$$\begin{aligned} & \log \left(\frac{(2n+1)^{2n+1}}{(n+1)^{n+1} (n+1/2)^{n+1/2}} \right) + (3/2)\log(3/2) - 1 \\ & > \sum_{i=1}^n (\log(n+1) - \log(1)) \end{aligned} \quad (\text{A.12})$$

Agora, para concluirmos a demonstração vamos mostrar que,

$$\begin{aligned} n \log 4 > \log \sqrt{\pi n} + \log \left(\frac{(2n+1)^{2n+1}}{(n+1)^{n+1} (n+1/2)^{n+1/2}} \right) + \\ & + (3/2)\log(3/2) - 1 \end{aligned} \quad (\text{A.13})$$

Para esta demonstração vamos aplicar o teorema A.2 à desigualdade (A.13). É fácil verificar que para $n_0 = 12$ (A.13) é verdadeira. Derivando (A.13) obtemos,

$$\begin{aligned} \log 4 > 1/(2n) + 2 \log(2n+1) + 2 - \log(n+1) - \\ & - 1 - \log(n+1/2) - 1 \\ & = 1/(2n) + 2\log(2n+1) - \log(n+1) - \log(n+1/2) \end{aligned} \quad (\text{A.14})$$

Agora para mostrarmos que (A.14) é verdadeira vamos aplicar, novamente, o teorema A.2. Para $n'_0 = 23$ a desigualdade (A.14) é verdadeira. Derivando (A.14) temos,

$$0 > -1/(2n^2) + 4/(2n+1) - 1/(n+1) - 1/(n+1/2) \quad (\text{A.15})$$

Agora,

$$-1/(2n^2) + 4/(2n + 1) - 1/(n + 1) - 1/(n+1/2)$$

$$= \frac{-4n^4 - 6n^3 - 2n^2 - (11/2)n - 1/2}{2n^2(2n + 1)(n + 1)(n + 1/2)} \quad (\text{A. 16})$$

e desde que para todo $n \geq 1$ o numerador de (A.16) é menor do que zero e o denominador é maior do que zero, então (A.16) é negativo e, portanto (A.15) é verdadeira para todo $n \geq 23$, desta forma, pelo teorema A.2 (A.14) também é verdadeira para todo $n \geq 23$ e desde que (A.12) é verdadeira para $n = 12$, novamente, pelo teorema A.2 (A.13) é verdadeira para todo $n \geq \max \{12, 23\} = 23$.

Referências

- [1] S.C. Chang and E.J. Weldon, Jr., "Coding for T - User Multiple - Access Channels," *IEEE Trans. Inform. Theory*, Vol. IT - 25, Nº 6, pp. 684 - 691, November 1979.
- [2] T.J. Ferguson, "Generalized T - User Codes for Multiple - Access Channels," *IEEE Trans. Inform. Theory*, Vol. IT - 28, Nº 5, pp. 775 - 778, September 1982.
- [3] J.H. Wilson, "Error-Correcting Codes for a T - User Binary Adder Channel," *IEEE Trans. Inform. Theory*, Vol. IT - 34, Nº 5, pp. 888 - 890, July 1988.
- [4] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error - Correcting Codes," New York: North-Holland, 1977.
- [5] P.G. Farrel "Survey of Channel Coding for Multi User Systems" in "New Concept in Multi User Communication" J.K. Skwirzynski, Ed., Sijthoff and Noordhof, 1981.
- [6] S.C. Chang and J.K. Wolf, "On the T-User M-Frequency Noiseless Multiple-Access Channel with and without Intensity Information", *IEEE Trans. Inform. Theory*, Vol. IT-27, Nº 1, pp. 41 - 47, January 1981.
- [7] T. Kasami and S. Lin "Coding for a Multiple-Access Channel", *IEEE Trans. Inform. Theory*, Vol. IT-22, Nº 2, pp. 129 - 137, March 1976.
- [8] R. Peterson and D.J. Costello, Jr., "Binary Convolutional Codes for a Multiple-Access Channel", *IEEE Trans. Inform. Theory*, Vol. IT - 25, Nº 1, pp. 101 - 109, January 1979.
- [9] S.L. and V.K. Wei, "Nonhomogeneous Trellis Codes for the Quasi-Synchronous Multiple-Access Binary Adder Channel with Two Users", *IEEE Trans. Inform. Theory*, Vol. IT - 32, Nº 6, pp. 787 - 796, November 1986.

- [10] M.A. Deaett and J.K. Wolf, "Some very Simply Codes for the Nonsynchronized Two-User Multiple-Access Channel with Binary Inputs", *IEEE Trans. Inform. Theory*, Vol. IT-24, N° 5, September 1978.
- [11] S.C. Chang, "Further Results on Coding for T-User Multiple-Access Channels", *IEEE Trans. Inform. Theory*, Vol. IT-30, N° 2, March 1984.
- [12] P.R. Chevillat, "N - User Trellis Coding for a Class of Multiple Access Channels", *IEEE Trans. Inform. Theory*, Vol. IT-27, N° 1, pp. 114 - 120, January 1981.
- [13] W.W. Peterson and E.J. Weldon Jr., "Error Correcting Codes", 2nd Ed. Cambridge, MA: MIT Press, 1972.
- [14] T. Kasami, S. Lin, V.K. Wei and S. Yamamura, "Graph Theoretic Approaches to the Code Construction for Two - User Multiple - Access Binary Adder Channel", *IEEE Trans. Information Theory*, Vol. IT - 29, N° 1, pp. 114 - 130, January 1983.
- [15] E.J. Weldon, Jr., "Coding for a Multiple Access Channel", *Information and Control*, N° 36, pp. 256 - 274, 1978.
- [16] H.C.A. Van Tilborg, "An Upper Bound for Codes in a Two - Access Binary Erasure Channel", *IEEE Trans. on Information Theory*, Vol. IT - 24, N° 1, pp. 112 - 116, January 1978.
- [17] H.C.A. Van Tilborg, "An Upper Bound for Codes for the Noisy Two - Access Binary Adder Channel", *IEEE Trans. on Information Theory*, Vol. 32, N° 32, pp. 436 - 443, May 1986.
- [18] T. Kasami, "Decoding of Linear δ - Decodable Codes for a Multiple Access Channel", *IEEE Transactions on Information Theory*, Vol. IT - 24, N° 5, pp. 633 - 634, September 1978.

- [19] G.H. Khachatryan, "Decoding Algorithm of Linear δ - Decodable Codes for 2 - User Adder Channel", *Fonte desconhecida*.
- [20] T. Kasami and S. Lin, "Bounds on the Achievable Rates of Block Coding for a Memoryless Multiple - Access Channel", *IEEE Trans. Inform. Theory*, Vol. IT - 24, Nº 2, pp. 187 - 197, 1978.
- [21] G.H. Khachatryan, "New Construction of Linear δ - Decodable Codes for 2 - User Adder Channel", *Problem of Control and Information Theory*, Vol. 13(4), pp. 275 - 279, 1984.
- [22] L. Györfi and I. Kerekes, "A Block Code for Noiseless Asynchronous Multiple Access or Channel", *IEEE Transactions on Information Theory*, Vol. IT - 27, Nº 6, pp. 788 - 791, November 1981.
- [23] F. Ali and B. Honary, "Low Complexity Soft Decision Decoding Technique for T - User Collaborative Coding Multiple - Access Channels", *Electronics Letters*, 20th June 1991, Vol. 27, Nº 13, pp. 1167 - 1169.
- [24] B. Honary, F. Ali and M. Darnell, "Capacity of T - User Collaborative Coding Multiple - Access Scheme Operating over Noisy Channel", *Electronics Letters*, 25th May 1989, Vol. 25, Nº 11, pp. 742 - 744.
- [25] A. Brine and P.G. Farrell, "Bandpass Adder Channel for Multiuser (Collaborative) Coding Schemes", *Electronics Letters*, 24th October 1985, Vol. 21, Nº 22, pp. 1030 - 1031.
- [26] B. Honary and F. Ali, "Information Transmission Capacity and Error Control Capability of Collaborative Coding Multiple Access System", *2º Bangor Symposium on Communications*, 23 - 24 May 1990, pp. 195 - 198.
- [27] E. Plotnik, "Code Constructions for Asynchronous Random Multiple - Access to the Adder Channel", *IEEE Transactions on Information Theory*, Vol. 39, Nº 1, January 1993, pp. 195 - 197.

- [28] J.B.B. Lacerda and W.C. Borelli, "A New Class of Error - Correcting Codes for a T - User Binary Adder Channel", *International Symposium on Signals, Systems and Electronics, ISSSE'92*, Paris September 1992, pp. 132 - 135.
- [29] J.B.B. Lacerda e W.C. Borelli, "Desempenho de uma Nova Classe de Códigos Corretores de Erros para o Canal T - Usuários", *V Simpósio Brasileiro de Microondas e X Simpósio Brasileiro de Telecomunicações, TELEM0'92*, Brasília 1992, pp. 73 - 78.
- [30] E.C. Van Der Meulen, "A Survey of Multi - Way Channels in Information Theory", *IEEE Transactions on Information Theory*, Vol. IT - 23, Nº 1, January 1977, pp. 1 - 37.
- [31] I. Csisfár and J. Körner, "Broadcast Channels with Confidential Messages", *IEEE Transactions on Information Theory*, Vol. IT - 24, Nº 3, May 1978, pp. 339 - 348.
- [32] T.M. Cover and A.A. El Gamal, "Capacity Theorems for the Relay Channel", *IEEE Transactions on Information Theory*, Vol. IT - 25, Nº 5, September 1979, pp. 572.
- [33] B.S. Tsybakov, "Survey of USSR Contributions to Random Multiple - Access Communications", *IEEE Transactions on Information Theory*, Vol. 11 - 31, Nº 2, March 1985, pp. 143 - 165.
- [34] R.G. Gallager, "A Perspective on Multiaccess Channels", *IEEE Transactions on Information Theory*, Vol. IT - 31, Nº 2, March 1985, pp. 124 - 142.
- [35] W.C. Borelli, "Convolutional Codes for Multi-Level Data Transmission", Tese de Ph.D., Univ. de Kent, Canterbury, Inglaterra, Junho de 1983.
- [36] G.H. Khachatrian and S.S. Martirosian, "Code Constructions for T-User Noiseless Adder Channel", Armenia Academy of Sciences.