Desempenho de um Sistema Multiportadora de Baixa Complexidade para Comunicação Digital em Ambientes Fechados

Izabel Cristina Oliveira Dionísio

Dissertação de Mestrado submetida à Coordenação dos Cursos de Pós-Graduação em Engenharia Elétrica da Universidade Federal da Paraíba - Campus II como parte dos requisitos necessários para obtenção do grau de Mestre no domínio da Engenharia Elétrica .

Área de Concentração: Processamento da Informação

Francisco Marcos de Assis, Dr.
Orientador

Campina Grande, Paraíba, Brasil

D588d Dionísio, Izabel Cristina Oliveira
Desempenho de um sistema multiportadora de baixa complexidade para comunicação digital em ambientes fechados / Izabel Cristina Oliveira Dionísio. - Campina Grande - PB: UFPB, 2000.
60 p.:
Dissertação (Mestrado) UFPB/CCT
Inclui Bibliografia

1. Multiportadora
2. Ambientes Fechados
3. Sistemas para Comunicação Digital

CDU: 621.395.34

DESEMPENHO DE UM SISTEMA MULTIPORTADORA DE BAIXA COMPLEXIDADE PARA COMUNICAÇÃO DIGITAL EM AMBIENTES FECHADOS

IZABEL CRISTINA OLIVEIRA DIONÍSIO

Dissertação Aprovada em 11.08.2000

PROF. FRANCISCO MARCOS DE ASSIS, Dr., UFPB
Orientador

PROF. BENEDITO GUIMARÃES AGUIAR NETO, Dr.-Ing., UFPB
Componente da Banca

PROF. JOÃO MARQUES DE CARVALHO, Ph.D., UFPB
Componente da Banca

JOSÉ EWERTON POMBO DE FARIAS, Dr., UFPB
Componente da Banca

CAMPINA GRANDE - PB
Julho - 2000

Dedicatória

Dedico este trabalho a minha mãe, Maria do Carmo e ao meu esposo, Diomário.

Agradecimentos

- A Deus, por minha vida;
- Aos meus pais, e principalmente a minha mãe que sempre me incentivou;
- A meu esposo Diomário, pelo apoio e incentivo;
- Ao professor Francisco Marcos, por toda dedicação e paciência, sem os quais não seria possível a realização deste trabalho.
- A CAPES, pelo apoio financeiro;
- Aos meus amigos de pós-graduação Suzete e Wamberto, pela amizade e incentivo. E os demais colegas que contribuíram direta ou indiretamente na realização deste trabalho;
- A todos os professores do DEE-UFPB;
- A todos os funcionários, em especial a Rinaldo, Eleonora e Ângela.

Resumo

A diversidade em frequência obtida através do uso de múltiplas portadoras tem sido bastante estudada em aplicações envolvendo canais em ambientes fechados. Nestes ambientes, as taxas de transmissão são elevadas, o efeito *Doppler* pode ser desprezado e o desvanecimento é lento e seletivo em frequência. Assim, torna-se viável a utilização de múltiplas portadoras em subcanais mais estreitos.

Neste trabalho, são apresentados resultados da simulação de um sistema multiportadora de baixa complexidade para comunicação digital em ambientes fechados. Esse sistema utiliza um código binário não-linear para mapear cada símbolo da informação em um conjunto de portadoras. A modulação OOK(*On-Off Keying*) e a demodulação não coerente são também utilizadas. A codificação para controle de erros é apresentada para a melhoria de desempenho do sistema multiportadora.

Foram feitas simulações com outras métricas além das métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, porém não foi encontrada nenhuma métrica que proporcionasse melhoria ao sistema. Portanto, outras alternativas além de outras métricas podem ser encontradas para aumentar ainda mais o desempenho do sistema proposto.

Abstract

Frequency diversity obtained with multiple carrier frequencies has been widely studied for indoor channels applications. Indoor channels have high channel rate, the Doppler frequency can be discarted and the fading is slow and selective frequency. So, the multiples carrier frequencies is often used in the slow bandwidth channels.

This work presents simulation results of the slow complexity multicarrier digital communication systems for indoor channels. This system uses a binary nonlinear code to specify multitone signal constellations. The OOK modulation and the noncoherent demodulation are also employed. Error control coding is presented to improve the multicarrier system performance.

Simulations with others metrics were been done. However, a new metric, to improve the performance system, is not found. So, others alternatives must been found.

Lista de Símbolos e Abreviaturas

ML – Máxima verossimilhança

SNR – Razão sinal-ruído

N_0 – Densidade espectral de potência de ruído

$AWGN$ – Ruído aditivo gaussiano branco

R – Taxa de codificação

E_b – Energia de bit

E_s – Energia de símbolo

E_t – Energia de tom

T – Duração do tom

T_s – Tempo de símbolo

T_d – Espalhamento de atraso

T_m – Máximo excesso de atraso

W – Largura de faixa do canal

f_0 – Largura de faixa de coerência

f_d – Freqüência *Doppler*

LCM – Mínimo múltiplo comum (*Least Common Multiple*)

J_0 – Função de Bessel modificada de ordem zero

fdp – Função Densidade de Probabilidade

ISI – Interferência entre símbolo (*Intersymbol Interference*)

d_{min} – Distância mínina

d – Distância de *Hamming*

$\Lambda(x)$ – Polinômio localizador de erros

$g(X)$ – Polinômio gerador

$S(X)$ – Síndrome Polinomial

$\Omega(X)$ – Magnitude polinomial do erro

B – Largura de faixa do ruído

$R(\ .\ )$ – Autocorrelação do ruído

σ^2 – Variância do ruído

N_{ca} – Número médio de canais transmitindo sinal para os quais $s_i(t) \neq 0$

N – Número de subcanais

N_a – Número de amostras do sinal

Lista de Figuras

2.1 Diagrama em blocos do sistema multiportadora para comunicação digital. 3
2.2 Representação da informação em palavras código. 4
2.3 Relações entre as funções de correlação do canal e as funções de densidade de potência. 11
2.4 Relações entre a função de transferência do canal e um sinal com largura de faixa W. 12
2.5 Modelo do receptor para a demodulação não coerente. 13

3.1 Circuito Multiplicador de Polinômios. 24
3.2 Codificador Sistemático. 25
3.3 Algoritmo de decodificação. 28
3.4 Algoritmo de *Berlekamp-Massey*. 29
3.5 Sistema com modulação BPSK com codificador RS(N,K) e canal AWGN. 32
3.6 Curvas de Probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para um sistema com modulação BPSK e canal AWGN. A curva *BPSK* é a curva obtida para o sistema sem codificação e as curvas *RS(7,3)* e *RS(31,16)* são as curvas obtidas para o sistema que utiliza os códigos RS(7,3) e RS(31,16), respectivamente. 32

4.1 Modelo equivalente passa-baixas de um subcanal em ambiente fechado. 37
4.2 Algoritmo do sistema multiportadora proposto 41

4.3 Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora com canal AWGN e o código binário BCH(15,5) linear. As curvas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente. 43

4.4 Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora com canal AWGN e o código binário BCH(15,5) não-linear. As curvas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente. 44

4.5 Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora para ambientes fechados utilizando o código binário BCH(15,5) não-linear. As curvas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente. 45

4.6 Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora para ambientes fechados utilizando o código binário BCH(21,5) não-linear. As curvas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente. 46

4.7 Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora para ambientes fechados utilizando o código binário BCH(15,5) não-linear. As curvas $d^{(j)}$, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas $d^{(j)}$, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente. 47

4.8 Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora para ambientes fechados utilizando o código binário BCH(15,5) não-linear e o código RS(31,16). As curvas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente. 48

Lista de Tabelas

2.1 Código BCH(15,5) linear e não-linear obtido pela combinação de inversão de bits. 7
2.2 Código BCH(21,5) linear e não-linear obtido pela combinação de inversão de bits. 8

3.1 Execução do algoritmo de *Berlekamp-Massey* e *Forney* 30

A.1 Adição em *GF(3)*. 53
A.2 Multiplicação em *GF(3)*. 53
A.3 Representação exponencial e polinomial. 55
A.4 Logaritmo de *Zech* em *GF(8)* 57

Índice

1 Introdução 1

2 Modelo do Sistema Multiportadora 3
- 2.1 Codificador de Multiportadora . . . 5
- 2.2 Modelo do Canal para Ambiente Interior . . . 9
- 2.3 Demodulação não coerente . . . 13
- 2.4 Dispositivo de Decisão para Detecção de Envoltória . . . 15

3 Códigos para Controle de Erros 21
- 3.1 Códigos BCH . . . 22
- 3.2 Códigos *Reed Solomon* . . . 24
- 3.3 Decodificador . . . 26
  - 3.3.1 Algoritmo de *Berlekamp-Massey* . . . 27
  - 3.3.2 Algoritmo de *Forney* . . . 27
  - 3.3.3 Exemplo . . . 28
- 3.4 Simulações Realizadas . . . 31

4 Procedimento de Simulação e Análise dos Resultados 34
- 4.1 Modelo Equivalente Passa-baixas do Sistema Multiportadora . . . 34
  - 4.1.1 Fonte de Informação . . . 35
  - 4.1.2 Codificador de Multiportadora . . . 35
  - 4.1.3 Modulador . . . 35
  - 4.1.4 Canal . . . 36

4.1.5 Demodulador 37
4.1.6 Razão Sinal/Ruído 38
4.1.7 Codificador/Decodificador *Reed Solomon* 40
4.1.8 Probabilidade de Erro de Símbolo 40
4.2 Procedimento de Simulação 41
4.3 Resultados das Simulações 42

5 Conclusão **49**

A Noções de Álgebra Abstrata **51**
A.1 Grupos, Anéis, Corpos e Espaços Vetoriais 51
A.2 Propriedades Elementares de Corpos Finitos 54
A.3 Logaritmo de *Zech* 56

Capítulo 1

Introdução

O rápido crescimento das comunicações pessoais sem fio impulsionou o surgimento de inovações tecnológicas que deverão ser capazes de permitir aos usuários o compartilhamento eficiente dos recursos comuns, não importando se isso envolve o espectro de freqüência, facilidades computacionais ou bases de dados. Ao contrário das comunicações fixas, as Redes de Comunicações Pessoais futuras permitirão aos usuários a conexão com inúmeros recursos, associando a tudo isso a liberdade de mobilidade.

As atuais pesquisas no desenvolvimento de soluções enumeram a existência de muitos obstáculos e questões que necessitam ser analisadas. A questão da portabilidade coloca restrições no tamanho da bateria e no consumo de potência nos terminais móveis. Além disso, transmissões em ambientes fechados enfrentam as severas degradações de multipercurso. Dessa forma, torna-se necessário um estudo aprofundado de técnicas que minimizem os efeitos do desvanecimento. Por essa razão, é importante desenvolver novos e eficientes sistemas que mantenham as exigências de alta capacidade em co-existência com alta concentração de usuários em ambientes fechados.

Pesquisas recentes [1], [2], [3] e [4] têm enfocado a implementação da diversidade em freqüência com o uso de multiportadora que oferece muitas vantagens em sistemas para comunicação digital que utilizam modelos de canais para ambientes fechados. Esses canais possuem banda larga, efeito *Doppler* pequeno, podendo ser desprezado, e desvanecimento lento e seletivo em freqüência. A técnica de multiportadora utiliza diversas portadoras para transportar paralelamente um determinado número de bits,

assim a taxa de transmissão em cada portadora é reduzida e a taxa total tem possibilidade de superar aquela atingível com uma única portadora. Porém, existe um compromisso a ser atendido entre a eficiência espectral de um tipo de modulação e a sua eficiência de potência. Um valor elevado para essa potência faz com que as baterias dos terminais portáteis tenham vida reduzida e tamanho elevado, além de tornar complexos os estágios de amplificação do transmissores, elevando os custos de aquisição e operação do sistema.

Este trabalho tem como objetivo simular um sistema multiportadora de baixa complexidade para comunicação digital em ambientes fechados e testar algumas variantes desse sistema proposto por Baum. Este sistema utiliza um código binário não-linear para mapear cada símbolo da informação em um conjunto de portadoras. A modulação OOK(*On-Off Keying*) é usada nos subcanais, a demodulação é não coerente utilizando detectores de envoltória e o modelo do canal é considerado dividido em subcanais mais estreitos com desvanecimento lento e não seletivo em freqüência. O desempenho do sistema é avaliado quando é utilizado um codificador para controle de erro. Foram feitas outras tentativas de melhoria para o sistema, porém os resultados obtidos, via simulação, mostraram que melhorias espetaculares não podem ser obtidas para o modelo de sistema estudado.

Este texto está organizado da seguinte maneira: O Capítulo 2 descreve o modelo do sistema simulado, dando ênfase ao modelo de canal em ambientes fechados, bem como o demodulador não coerente e o dispositivo de decisão.

Os códigos corretores de erros, BCH e *Reed Solomon*, são definidos e caracterizados no Capítulo 3. Também são apresentados os algoritmos para decodificação utilizados na simulação do sistema multiportadora.

No Capítulo 4 está descrito o procedimento de simulação do sistema. Os resultados obtidos são apresentados e avaliados.

Finalmente no Capítulo 5 são apresentadas as conclusões e sugestões para trabalhos futuros.

Capítulo 2

Modelo do Sistema Multiportadora

Neste capítulo será descrito o modelo do sistema [1] cujo diagrama em blocos está ilustrado na Figura 2.1.

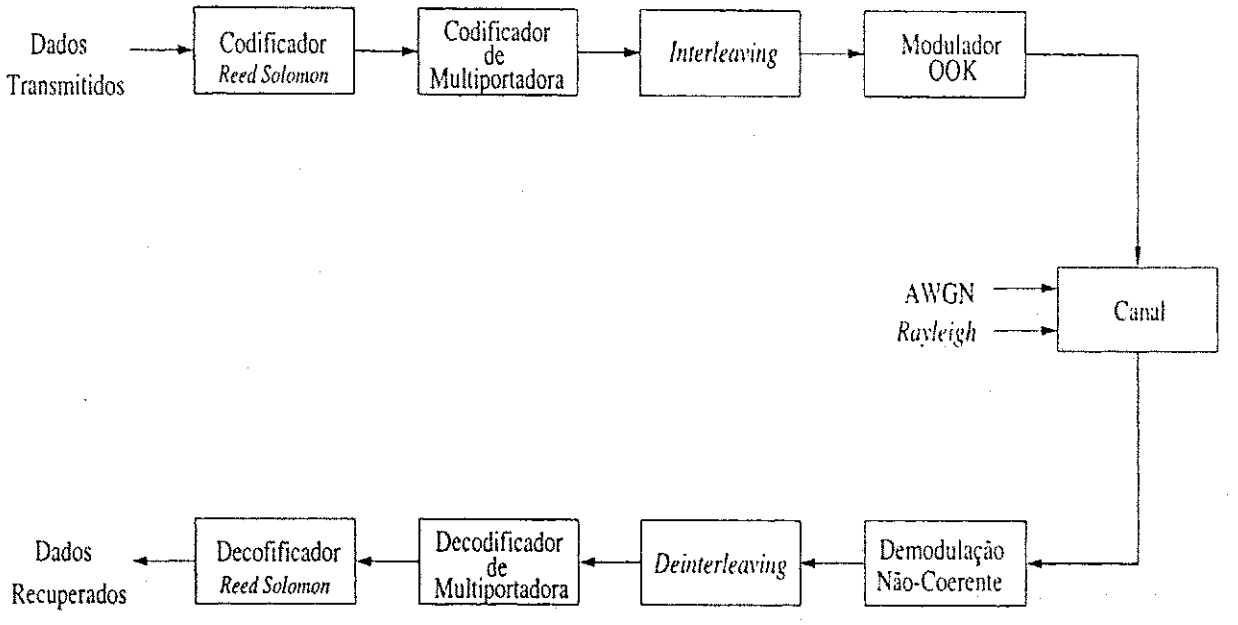


Figura 2.1: Diagrama em blocos do sistema multiportadora para comunicação digital.

No transmissor os dados de informação são definidos em blocos de K bits que são mapeados em blocos de N bits pelo codificador de multiportadora. Para um dado bloco de bits de informação a j-ésima palavra código produzida pelo codificador de

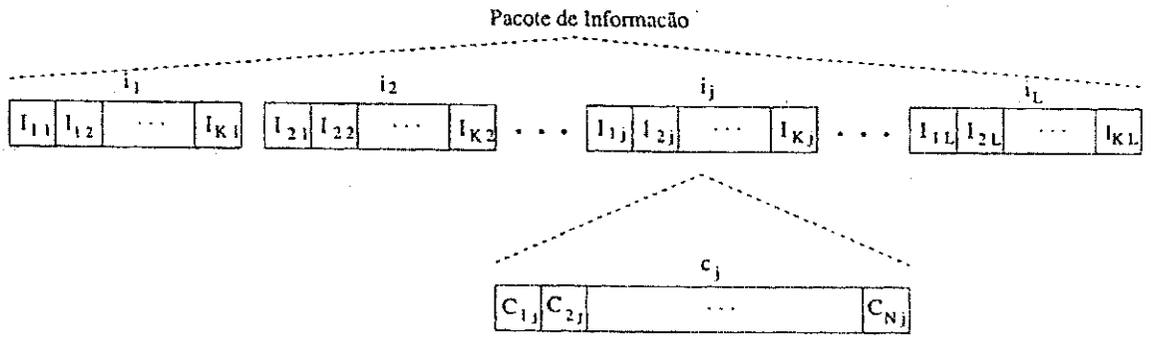


Figura 2.2: Representação da informação em palavras código.

multiportadora é representado por:

$$c_j = (C_{1j}, C_{2j}, ..., C_{Nj}). \tag{2.1}$$

As palavras código c_j são convertidas em um sinal modulado $s(t)$ dado por:

$$s_j(t) = \sqrt{\frac{2\ E_t}{T}} \sum_{i=1}^{N} C_{ij}\ cos(2\pi f_i t), \tag{2.2}$$

em que:

E_t é a energia por portadora(tom),

f_i é a freqüência do i-ésimo subcanal.

T é a duração do tom,

C_{ij} representa o i-ésimo bit da j-ésima palavra código. Considerando $C_{ij} = 1$ se $bit = 1$ e caso contrário $bit = 0$.

A modulação utilizada nos subcanais é a modulação OOK(*On-Off Keying*) [5], na qual se $C_{ij} = 1$, uma determinada quantidade de energia será transmitida caso contrário nenhuma energia será transmitida.

No canal o sinal modulado é afetado pelo desvanecimento e pelo ruído gaussiano. Dessa maneira, o sinal recebido do canal será expresso por [1]:

$$r_j(t) = \sum_{i=1}^{N} \sqrt{\frac{2\ E_t}{T}}\ C_{ij}\ \alpha_i\ cos(2\pi f_i i + \theta_i) + n(t), \tag{2.3}$$

em que:

α_i é uma v.a. com distribuição de *Rayleigh* [6] que representa a amplitude do desvanecimento no subcanal i;

θ_i é uma v.a. uniformemente distribuída no intervalo $(0, 2\pi)$;

$n(t)$ é uma v.a. gaussiana que representa o ruído térmico.

O demodulador consiste de N detetores de envoltória [6], cuja saída é definida pelo vetor:

$$\mathbf{Y} = (y_1, y_2, ..., y_N), \tag{2.4}$$

em que,

$$y_i = \sqrt{\left[\int_T r(t)\ cos(2\pi f_i t)\ dt\right]^2 + \left[\int_T r(t)\ sen(2\pi f_i t)\ dt\right]^2} \tag{2.5}$$

e

$$i = 1, 2, ..., N.$$

A saída $\mathbf{Y}$ é utilizada pelo dispositivo de decisão para estimar o símbolo enviado. O codificador de *Reed Solomon*(RS) [7] [8] é utilizado em conjunto com o entrelaçador de símbolos (*interleaving*) que embaralha os símbolos evitando a ocorrência de erros em rajada e permitindo que o codificador corrija um número maior de erros. Nas próximas seções será descrito detalhadamente o codificador de multiportadora, o modelo do canal para ambiente fechado, o demodulador não coerente e o dispositivo de decisão para detecção de envoltória utilizados no sistema multiportadora simulado.

2.1 Codificador de Multiportadora

O codificador de multiportadora tem o objetivo de associar cada símbolo transmitido pela fonte a um conjunto de portadoras, utilizando para isso, um código binário. Em conjunto com o codificador de multiportadora, o sistema proposto utiliza a demodulação não coerente que demodula o sinal através da energia do sinal recebido do canal. Assim, é considerado que a potência por bit, $C_{ij} = 1$ com $i = 1, 2, ..., N$ e $j = 1, 2, ..., L$,

da palavra codificada é constante e a potência por símbolo transmitido será proporcional ao número de $C_{ij} = 1$ da palavra código j. Dessa forma, é necessário que o conjunto de palavras código possíveis, geradas pelo codificador de multiportadora, tenha o número de ocorrências de $C_{ij} = 1$ aproximadamente constante, de forma a não prejudicar a detecção de nenhuma palavra código que possua menor número daquelas ocorrências. Com base nesse fato, pode-se-ia imaginar que o melhor código seria um código do tipo peso constante, porém isso não é verdade, pois as propriedades de distância de *Hamming* destes códigos não são boas [9].

Para melhorar o desempenho do sistema multiportadora, é sugerido [1] um código não-linear obtido através de uma combinação de inversão de bits de um código linear com boas propriedades de distância de *Hamming*. A inversão de bits é feita pela adição módulo 2 do valor do bit. O objetivo é obter um código que possua a mínima variância dos pesos das palavras código e mantenha, ou melhore, as propriedades de distância de *Hamming*. Para um código linear(N,K) existem 2^N diferentes combinações possíveis de inversão de bits. Dentro desse conjunto de combinações é selecionado, através de técnicas numéricas de busca, como por exemplo, algoritmos de busca do tipo genético, subconjuntos que tenham o maior peso mínimo e o menor peso máximo. Embora vários códigos gerados dessa maneira tenham propriedades de distância idênticas, o desempenho desses códigos no sistema multiportadora, pode variar muito. Isso ocorre por duas razões: a) Os códigos com menor peso de *Hamming* utilizam a energia do sinal mais eficientemente do que os códigos de maior peso de *Hamming*, já que a energia por portadora é constante; b) O uso da demodulação de baixa complexidade resulta em um desempenho melhor do que outros códigos não-lineares.

Para o código BCH(15,5) com distância mínima igual a 7, polinômio gerador:

$$g(X) = 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}$$

e combinação de inversão de bits:

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

obtêm-se um código não-linear (15,5) que está mostrado na Tabela 2.1 [1]. Nota-se que todas as palavras código desse código não-linear tem peso de *Hamming* entre 5 e 10.

Símbolo	Código BHC(15,5)	Peso	Código BCH(15,5) não-linear	Peso
0	000000000000000	0	000001011111111	9
1	111011001010000	7	111010010101111	10
2	011101100101000	7	011100111010111	10
3	100110101111000	8	100111110000111	9
4	001110110010100	7	001111101101011	10
5	110101111000100	8	110100100111011	9
6	010011010111100	8	010010001000011	5
7	101000011101100	7	101001000010011	6
8	000111011001010	7	000110000110101	6
9	111100010011010	8	111101001100101	9
10	011010111100010	8	011011100011101	9
11	100001110110010	7	100000101001101	6
12	001001101011110	8	001000110100001	5
13	110010100001110	7	110011111110001	10
14	010100001110110	7	010101010001001	6
15	101111000100110	8	101110011011001	9
16	000011101100101	7	000010110011010	6
17	111000100110101	8	111001111001010	9
18	011110001001101	8	011111010110010	9
19	100101000011101	7	100100011100010	6
20	001101011110001	8	001100000001110	5
21	110110010100001	7	110111001011110	10
22	010000111011001	7	010001100100110	6
23	101011110001001	8	101010101110110	9
24	000100110101111	8	000101101010000	5
25	111111111111111	15	111110100000000	6
26	011001010000111	7	011000001111000	6
27	100010011010111	8	100011000101000	5
28	001010000111011	7	001011011000100	6
29	110001001101011	8	110000010010100	5
30	010111100010011	8	010110111101100	9
31	101100101000011	7	101101110111100	10

Tabela 2.1: Código BCH(15,5) linear e não-linear obtido pela combinação de inversão de bits.

A Tabela 2.2 mostra outro código não-linear obtido através do código BCH(21,5) com distância mínima igual a 10 e polinômio gerador:

$$g(X) = 1 + X^4 + X^5 + X^8 + X^{10} + X^{12} + X^{13} + X^{14} + X^{15} + X^{16}$$

e com a combinação de inversão de bits:

$$B = \{1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0\}.$$

Observa-se que o peso de *Hamming* para esse código não-linear varia de 8 a 16.

Resultados obtidos mostrados no Capítulo 5 indicando que o código não-linear BCH(15,5) possui desempenho superior ao código linear BCH(15,5) e que o desempenho do sistema está relacionado com a escolha desse código.

Símbolo	Código BHC(21,5)	Peso	Código BCH(21,5) não-linear	Peso
0	000000000000000000000	0	111110110010000000000	8
1	100011001010111110000	10	011101111000111110000	12
2	010001100101011111000	10	101111010111011111000	14
3	110010101111100001000	10	001100011101100001000	8
4	001000110010101111100	10	110110000000101111100	10
5	101011111000010001100	10	010101001010010001100	8
6	011001010111110000100	10	100111100101110000100	10
7	111010011101001110100	12	000100101111001110100	10
8	000100011001010111110	10	111010101011010111110	14
9	100111010011101001110	12	011001100001101001110	10
10	010101111100001000110	10	101011001110001000110	10
11	110110110110110110110	14	001000000100110110110	8
12	001100101011111000010	10	1100100'1001111000010	10
13	101111100001000110010	10	010001010011000110010	8
14	011101001110100111010	12	100011111100100111010	12
15	111110000100011001010	10	000000110110011001010	8
16	000010001100101011111	10	111100111110101011111	16
17	100001000110010101111	10	011111101000101011111	14
18	010011101001110100111	12	101101011011110100111	14
19	110000100011001010111	10	001110010001001010111	10
20	001010111110000100011	10	110100001100000100011	8
21	101001110100111010011	12	010111000110111010011	12
22	011011011011011011011	14	100101101001011011011	12
23	111000010001100101011	10	000110100011100101011	10
24	000110010101111100001	10	111000100111111100001	12
25	100101011111000010001	10	011011101101000010001	10
26	010111110000100011001	10	010010000101000011001	8
27	110100111010011101001	12	001010001000011101001	8
28	001110100111010011101	12	110000010101010011101	10
29	101101101101101101101	14	010011011111101101101	14
30	011111000010001100101	10	100001110000001100101	8
31	111100001000110010101	10	000010111010110010101	10

Tabela 2.2: Código BCH(21,5) linear e não-linear obtido pela combinação de inversão de bits.

2.2 Modelo do Canal para Ambiente Interior

A caracterização do canal no projeto de sistemas para comunicações digitais é de fundamental importância para que o transmissor e o receptor sejam projetados de maneira a compensar os efeitos destrutivos presentes nos canais.

O canal de comunicações móvel tem como principal característica a propagação por multipercursos que provoca o desvanecimento no sinal transmitido. Este desvanecimento pode ser classificado em dois tipos: desvanecimento de longo termo e desvanecimento de curto termo [10]. O desvanecimento de longo termo representa a atenuação média da potência do sinal ou a perda de percurso devido ao movimento em grandes áreas, tais como montanhas, florestas, edifícios, que estão situados entre o transmissor e o receptor. As estatísticas do desvanecimento de longo termo provêem um meio de cálculo estimado da perda de percurso como função da distância.

O desvanecimento de curto termo, característico do canal em ambiente fechado [11], está relacionado com mudanças drásticas na amplitude e na fase do sinal que pode ser causadas por pequenas mudanças na separação espacial entre o receptor e o transmissor. O desvanecimento se manifesta através de dois mecanismos: o espalhamento do sinal no tempo (dispersão do sinal) e a variação do comportamento do canal no tempo. O desvanecimento de curto termo é chamado de desvanecimento *Rayleigh* Se há múltiplos percursos refletidos e não existe componente principal do sinal, o envelope do sinal recebido é estatisticamente descrito pela função densidade de probabilidade (fdp) de *Rayleigh*, que é dada por:

$$p_X(x) = \frac{x}{\sigma^2}\, e^{-\frac{x^2}{2\sigma^2}}\, u(x), \tag{2.6}$$

com média $E[X] = \sigma\,\sqrt{\frac{\pi}{2}}$ e variância $V[X] = \left(2 - \frac{\pi}{2}\right)\,\sigma^2$.

Quando há uma forte componente principal, a envoltória do sinal pode ser descrita pela fdp de *Rice*, dada por:

$$p_X(x) = \frac{x}{\sigma^2}\, e^{-\frac{x^2+A^2}{2\sigma^2}}\, I_0\left(\frac{x\ A}{\sigma^2}\right)\, u(x), \tag{2.7}$$

em que,

I_0 é a função de Bessel modificada de ordem zero;

A é a amplitude do sinal.

Dois parâmetros são frequentemente usados na caracterização dos canais com multipercurso: o espalhamento do atraso, T_d, e a largura de faixa de coerência [1] , f_0. O espalhamento do atraso é uma medida do comprimento da resposta ao impulso do canal. Esses atrasos, que são funções do tempo de bit, provocam a interferência intersimbólica (ISI) que degrada o desempenho do sistema e torna complicado o projeto do receptor. Enquanto que a largura de faixa de coerência é uma medida da correlação do desvanecimento entre as freqüências e está diretamente relacionada com o espalhamento de atraso. A Figura 2.3 ilustra as relações entre estes parâmetros.

Em um canal com desvanecimento, a relação entre o máximo excesso de atraso [2] , T_m, e o tempo de símbolo, T_s, pode ser visto em duas diferentes categorias de degradação: desvanecimento seletivo em freqüência e desvanecimento não seletivo em freqüência ou plano.

No domínio do tempo, um canal é dito seletivo em freqüência quando $T_m > T_s$. Este tipo de distorção é o mesmo tipo provocada pela ISI. Enquanto que o desvanecimento não seletivo em freqüência ou plano ocorre quando $T_m < T_s$. Neste caso, não existe a distorção ISI, pois o tempo de espalhamento do sinal não resulta em sobreposição de símbolos vizinhos que chegam no receptor. Neste tipo de canal há uma perda na SNR (Razão Sinal/Ruído) que podem ser atenuados utilizando técnicas de diversidade e codificação para controle de erros.

No domínio da freqüência, o desvanecimento seletivo em freqüência ocorre sempre que as componentes espectrais do sinal não são efetadas igualmente pela distorção, ou seja, as componentes espectrais do sinal que estiverem dentro da faixa de coerência do sinal serão afetadas diferentemente (independentemente) quando comparadas àquelas que estiverem fora desta faixa, ou seja, $f_0 < W$. Entretanto, o desvanecimento não

[1] Largura de faixa de coerência é uma medida estatística da faixa de freqüências na qual o canal transporta todas as componentes espectrais com ganho igual e fase linear, aproximadamente.

[2] O máximo excesso de atraso é o tempo decorrido entre a primeira e a última componente do sinal que chega no receptor.

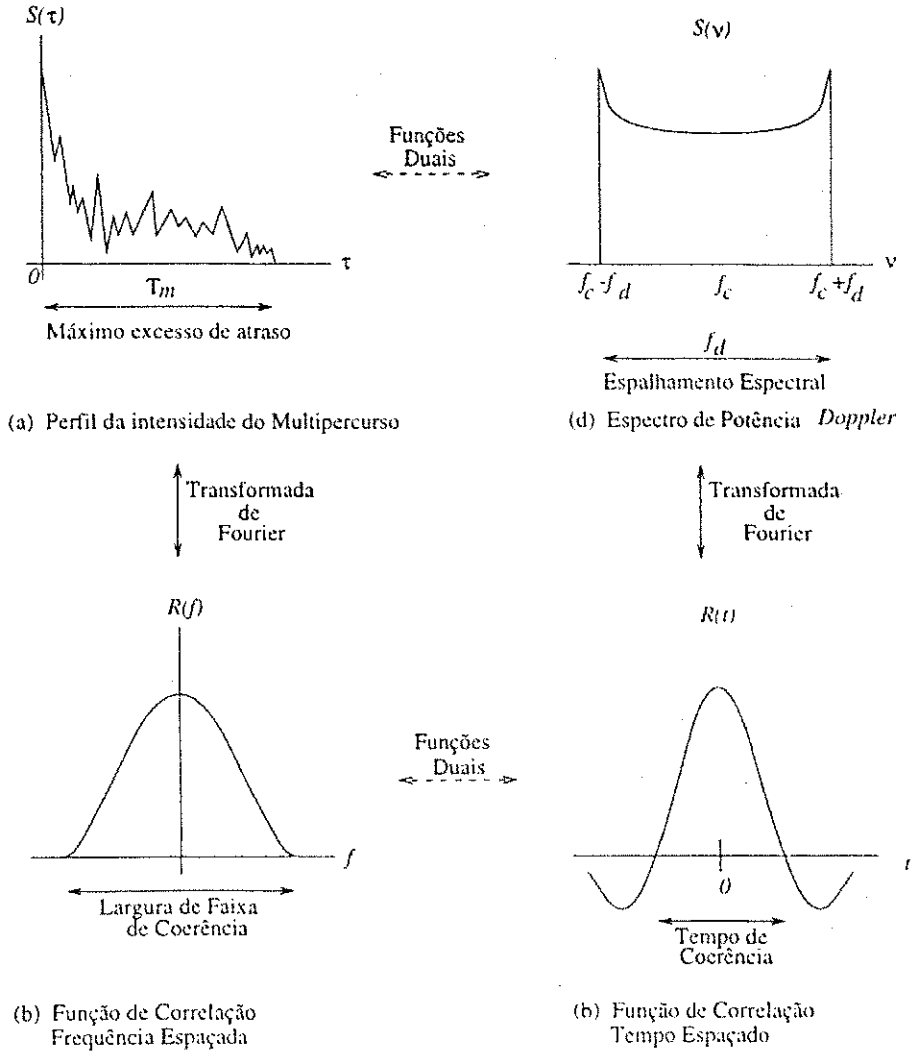
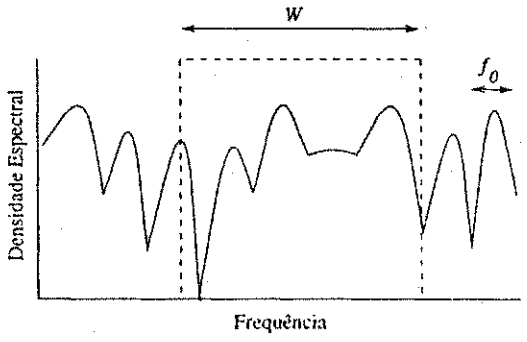
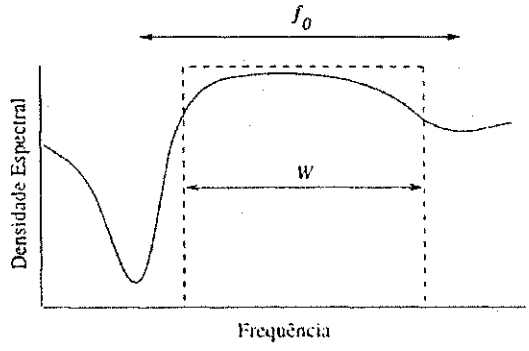


Figura 2.3: Relações entre as funções de correlação do canal e as funções de densidade de potência.

seletivo em freqüência ou plano ocorre sempre que $f_0 > W$. Todas as componentes espectrais do sinal serão afetadas igualmente pelo canal, ou seja, serão desvanecidas ou não. A Figura 2.4 mostra as relações entre a função de transferência do canal e um sinal com largura de faixa W.



(a) Típico Devanecimento Seletivo em Frequência
Caso: $f_0 < W$



(b) Típico Desvanecimento não Seletivo em Frequência (Plano)
Caso: $f_0 > W$

Figura 2.4: Relações entre a função de transferência do canal e um sinal com largura de faixa W.

Outra característica é o espalhamento *Doppler* que pode ser interpretado como uma medida da variação da portadora, ou seja, é uma medida da taxa em que ocorre mudanças no canal. Pesquisas indicam que o efeito *Doppler* é relativamente pequeno com valores na faixa de 0.3 a 6.1Hz [12] em ambientes fechados. E o espalhamento de atraso *rms*(*root mean square*) é em geral pequeno com valores típicos na faixa de 10 a

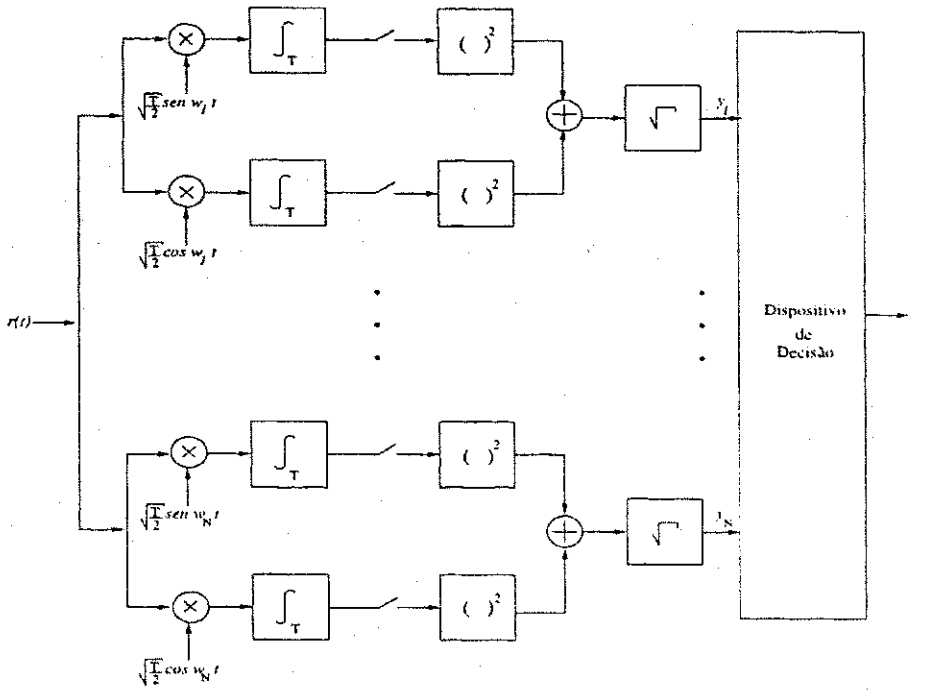


Figura 2.5: Modelo do receptor para a demodulação não coerente.

50 ns na freqüência de 810 MHz [13].

Neste trabalho será considerado que a largura de faixa do sinal é pequena comparada com a largura de faixa de coerência do canal, de modo que podemos considerar que o desvanecimento afeta todos os subcanais igualmente, ou seja, o desvanecimento é não seletivo em freqüência ou plano. Esta comparação possibilita uma simulação simples de um canal em ambiente fechado no qual suas caracteríticas muda lentamente com o tempo e o efeito *Doppler* pode ser desprezado.

2.3 Demodulação não coerente

A demodulação não coerente é aplicada em sistemas que não necessitam manter o sincronismo da portadora, possibilitando a redução da complexidade do sistema.

A Figura 2.5 ilustra um demodulador não coerente que consiste de $2N$ ramos. Como existe a possibilidade de haver uma diferença de fase entre os sinais recebidas e os sinais

gerados localmente, o sinal recebido estará parcialmente correlacionado com $cos\ w_i t$ e também com $sen\ w_i t$ para um dado subcanal i. Nesse tipo de demodulação, o sinal transmitido é estimado a partir da energia do sinal recebido, justificando-se o uso da soma dos quadrados na saída dos ramos superior e inferior de cada subcanal.

Por causa do ruído e da distorção presentes no canal, o envelope do sinal recebido é geralmente complexo, assim a operação de deteção do envelope do sinal simplesmente envolve a aquisição do valor absoluto do envelope complexo.

O sinal recebido do i-ésimo subcanal é expresso por:

$$r_i(t) = \sqrt{\frac{2\ E_t}{T}}\ C_{ij}\ \alpha_i\ cos(2\pi f_i t + \theta_i) + n(t), \tag{2.8}$$

$$i = 1, 2, ..., N,$$

em que:

θ_i é uma v.a. com distribuição Uniforme com valores de 0 a 2π e
α_i é uma v.a. com ditribuição de Rayleigh com média unitária.

A demodulação do sinal real $r_i(t)$ será obtida utilizando dois correlatores com funções de base dadas por:

$$\psi_F^{(i)} = \sqrt{\frac{2}{T}}\ cos(2\pi f_i t) \tag{2.9}$$

e

$$\psi_Q^{(i)} = \sqrt{\frac{2}{T}}\ sen(2\pi f_i t), \tag{2.10}$$

com $i = 1, 2, ..., N$.

As saídas dos correlatores serão determinadas por:

$$I_F^{(i)} = \int_T r_i(t)\ \sqrt{\frac{2}{T}}\ cos(2\pi f_i t)\ dt \tag{2.11}$$

e

$$I_Q^{(i)} = \int_T r_i(t) \sqrt{\frac{2}{T}} \, sen(2\pi f_i t) \, dt, \tag{2.12}$$

em que:

$I_F^{(i)}$ e $I_Q^{(i)}$ representam as correlações em fase e quadratura do sinal recebido no i-ésimo subcanal , respectivamente;

$\int_T$ representa a integral em um intervalo de tom com duração T.

Substituindo $r_i(t)$ na Equação 2.11, têm-se:

$$I_F^{(i)} = \sqrt{E_t} \, C_{ij} \, \alpha_i \, cos(\theta_i) + n_F^{(i)}. \tag{2.13}$$

Similarmente, obtêm-se:

$$I_Q^{(i)} = \sqrt{E_t} \, C_{ij} \, \alpha_i \, sen(\theta_i) + n_Q^{(i)}. \tag{2.14}$$

Reescrevendo a Equação 2.5 em função de $I_F^{(i)}$ e $I_Q^{(i)}$, então:

$$y_i = \sqrt{(I_F^{(i)})^2 + (I_Q^{(i)})^2}. \tag{2.15}$$

Substituindo os valores calculados, têm-se:

$$y_i = \sqrt{E_T \, C_{ij}^2 \, \alpha_i^2 \; + 2 \sqrt{E_t} \, C_{ij} \, \alpha_i \, \left[n_f^{(i)} \, cos(\alpha_i) + n_Q^{(i)} \, sen(\theta_i) \right] + \left(n_F^{(i)} \right)^2 + \left(n_Q^{(i)} \right)^2}. \tag{2.16}$$

O resultado acima mostra que o sinal recebido é corrompido tanto pelo ruído gaussiano, como também, pelo desvanecimento com distribuição de *Rayleigh*.

2.4 Dispositivo de Decisão para Detecção de Envoltória

Nesta seção será descrito o dispositivo de decisão [14] da Figura 2.5, na suposição de que os símbolos na entrada do canal sejam equiprováveis.

Considerando que o sistema possue N subcanais distintos, a representação dos N sinais modulados será: $s_1(t)$, $s_2(t)$, ... , $s_N(t)$.

Em geral, o sinal recebido em um subcanal é considerado estatisticamente independente dos demais, é representado por:

$$r_i(t) = \alpha_i \; s_i(t) + n_i(t),$$

em que:

$n_i(t)$ representa o ruído térmico definido pelo processo gaussiano com densidade espectral de potência igual a $\frac{N_0}{2}$;

α_i é uma v.a. com distribuição de *Rayleigh* que representa a amplitude do desvanecimento no subcanal i.

As hipóteses para cada subcanal será:

$$\begin{cases} H1 : r_i(t) = \alpha_i \; s_i(t) + n_i(t) & se \quad C_{ij} = 1 \\ H2 : r_i(t) = n_i(t) & se \quad C_{ij} = 0 \end{cases}$$

em que: $i = 1, 2, ..., N$.

A razão de verossimilhança é definida por:

$$\lambda(\mathbf{r}) = \frac{p_1(r_1, r_2, ..., r_N)}{p_0(r_1, r_2, ..., r_N)}. \tag{2.17}$$

em que: $p_i(r_1, r_2, ..., r_N)$ representam as funções densidade de probabilidades das r_1, $r_2, ..., r_N$ condicionadas na hipótese H_i, $i = 1, 2$..

Neste caso, a função de verossimilhança do canal pode ser escrita como:

$$\lambda(\mathbf{r}) = \frac{p_1(r_1) \; p_1(r_2) \; \cdots \; p_1(r_N)}{p_0(r_1) \; p_0(r_2) \; \cdots \; p_0(r_N)}. \tag{2.18}$$

$$\lambda(\mathbf{r}) = \prod_{i=1}^{N} \frac{p_1(r_i)}{p_0(r_i)} = \prod_{i=1}^{N} \lambda_i(r_i), \tag{2.19}$$

em que: $\lambda_i(r_i)$ representa a razão de verossimilhança do i-ésimo subcanal.

A Equação 2.19 mostra que a razão de verossimilhança de n subcanais estatisticamente independentes é o produto das N razões individuais.

A razão de verossimilhança do canal é dada por [14]:

$$\lambda(\mathbf{r}) = \prod_{i=1}^{N} e^{-\frac{1}{N_0}\int_T s_i^2(t)\ dt}\ e^{\frac{2}{N_0}\int_T r_i(t)\ s_i(t)\ dt}. \tag{2.20}$$

Pela regra de máxima verossimilhança escolhe-se o símbolo que corresponde à palavra código c_m se:

$$p(y/c_m) = \max_j\{p(y/cj)\}, \tag{2.21}$$

em que: $j = 1, 2, ..., 2^K$

Denominando $I_a = \int_T\ s_i(t)\ dt$ na Equação 2.20 e substituindo $s_i(t)$, têm-se:

$$I_a = \int_0^T \left(\sqrt{\frac{2\ E_t}{T}}\ C_{ij}\ cos(2\pi f_i t)\right)^2\ dt. \tag{2.22}$$

$$I_a = E_t\ C_{ij}^2. \tag{2.23}$$

Denominando $I_b = \int_T\ r_i(t)\ s_i(t)\ dt$ da Equação 2.20 e reescrevendo $r_i(t)$ descrito pela Equação 2.8, têm-se:

$$r_i(t) = \sqrt{\frac{2\ E_t}{T}}\ C_{ij}\ \alpha_i\ cos(2\pi f_i t)\ cos(\theta_i) - \sqrt{\frac{2\ E_t}{T}}\ C_{ij}\ \alpha_i sen(2\pi f_i t)\ sen(\theta_i) + n(t). \tag{2.24}$$

Substituindo $s_i(t)$ e a Equação 2.24 em I_b, têm-se:

$$\begin{aligned} I_b \ = \ & \left[\int_0^T \sqrt{\tfrac{2\ E_t}{T}}\ C_{ij}\ cos(2\pi f_i t)\ .\ \sqrt{\tfrac{2\ E_t}{T}}\ C_{ij}\ \alpha_i\ cos(2\pi f_i t)\ dt\right]\ .\ cos(\theta_i)\ + \\ & \left[\int_0^T \sqrt{\tfrac{2\ E_t}{T}}\ C_{ij}\ cos(2\pi f_i t)\ .\ \sqrt{\tfrac{2\ E_t}{T}}\ C_{ij}\ \alpha_i\ sen(2\pi f_i t)\ dt\right]\ .\ sen(\theta_i)\ + \\ & \int_0^T \sqrt{\tfrac{2\ E_t}{T}}\ C_{ij}\ cos(2\pi f_i t)\ n(t)\ dt. \end{aligned}$$

Portanto, I_b será escrita como:

$$I_b = \sqrt{E_t}\, C_{ij}\, I_F^{(i)}\, cos(\theta_i) - \sqrt{E_t}\, C_{ij}\, I_Q^{(i)}\, sen(\theta_i). \tag{2.25}$$

Simplificando a Equação 2.25:

$$I_b = \sqrt{E_t}\, C_{ij}\, \left[I_F\, cos(\theta_i) - I_Q\, sen(\theta_i)\right], \tag{2.26}$$

$$I_b = \sqrt{E_t}\, C_{ij} \sqrt{\left(I_F^{(i)}\right)^2 + \left(I_Q^{(i)}\right)^2}\, cos\left[\theta_i + tan^{-1}\left(\frac{I_Q^{(i)}}{I_F^{(i)}}\right)\right], \tag{2.27}$$

$$I_b = \varepsilon_i\, cos(\beta_i), \tag{2.28}$$

em que:

$$\varepsilon_i = \sqrt{E_t}\, C_{ij} \sqrt{\left(I_F^{(i)}\right)^2 + \left(I_Q^{(i)}\right)^2}$$

e

$$\beta_i = \theta_i + tan\left(\frac{I_Q^{(i)}}{I_F^{(i)}}\right).$$

Portanto, escolhe-se o símbolo que correspondente à palavra código c_m se:

$$c_m \leftarrow \max_j \left\{ \prod_{i=1}^{N} e^{-\frac{E_t\, C_{ij}^2}{N_0}}\, \frac{1}{2\pi} \int_0^{2\pi} e^{\frac{2}{N_0}\, \varepsilon_i\, cos(\beta_i)}\, d\theta \right\}. \tag{2.29}$$

Por definição, a função de Bessel de ordem zero é dada por:

$$J_0(x) \triangleq \frac{1}{2\pi} \int_0^{2\pi} e^{x\, cos(\gamma)}\, d\gamma. \tag{2.30}$$

Então, a Equação 2.29 pode ser reduzida para:

$$c_m \leftarrow \max_j \left\{ \prod_{i=1}^{N} \left[e^{-\frac{\varepsilon_i\, C_{ij}^2}{N_0}}\, J_0\left(\frac{2\, \sqrt{E_t}\, C_{ij}\, y_i}{N_0}\right)\right]\right\}. \tag{2.31}$$

em que: J_0 é a função de Bessel modificada de ordem zero.

Aplicando o logaritmo, têm-se:

$$c_m \leftarrow \max_j \left\{ \sum_{i=1}^{N} ln \left[J_0 \left(\frac{2\sqrt{E_t}\, C_{ij}\, y_i}{N_0} \right) \right] - \frac{E_t\, C_{ij}^2}{N_0} \right\}.$$

Portanto, o critério de máxima verossimilhança (ML) escolherá o símbolo correspondente a palavra código c_j que maximize a métrica $d^{(j)}$, dada por:

$$d_o^{(j)} = \sum_{i=1}^{N} \left\{ ln \left[J_0 \left(\frac{2\sqrt{E_t}\, C_{ij}\, y_i}{N_0} \right) \right] - \frac{E_t\, C_{ij}^2}{N_0} \right\}. \tag{2.32}$$

Para um canal sujeito a desvanecimento, o critério ML é mais complexo. Considerando um caso especial, no qual a largura de faixa de freqüência de correlação do canal é muito maior do que a largura de coerência do canal. Neste caso, os portadoras são consideradas igualmente desvanecidas. Então, a densidade conjunta $p(y/c_j)$ dos N subcanais pode ser obtida primeiramente condicionando no valor da variável de desvanecimento e depois integrando com relação a densidade de desvanecimento que é *Rayleigh*. O critério ML, neste caso, escolhe o símbolo que corresponde a palavra código c_j que maximiza a métrica definida por [1]:

$$d^{(j)} = ln \left[\int_0^{\infty} \frac{a}{\tau^2} e^{-\frac{a^2}{2\tau^2}} \prod_{i=1}^{N} e^{-\frac{C_{ij} a^2}{2\sigma^2}} J_0 \left(\frac{C_{ij}\, y_i\, a}{\sigma^2} \right) \right]. \tag{2.33}$$

em que: τ^2 e σ^2 são as variâncias de *Rayleigh* e do ruído gaussiano branco, respectivamente; e $\frac{\tau^2}{\sigma^2} = \frac{E_t}{N_0}$.

O cálculo desta métrica, para sistemas reais, se torna impraticável. Para solucionar este problema, foi sugerido em [1] três métricas que fornecem o símbolo estimado a partir de simples cálculos e sem necessitar do conhecimento dos valores das potências do sinal nem do ruído. Estas métricas são:

$$d_1^{(m)} = \frac{\mathbf{z} \cdot \mathbf{c}_m}{\|c_m\|}. \tag{2.34}$$

$$d_2^{(m)} = \frac{\mathbf{z} \cdot (\mathbf{c}_m - \bar{\mathbf{c}}_m)}{\|c_m\|}, \tag{2.35}$$

$$d_3^{(m)} = \frac{\mathbf{z} \cdot \mathbf{c}_m}{\|c_m\|} - \frac{\mathbf{z} \cdot \bar{\mathbf{c}}_m}{\|\bar{c}_m\|}, \tag{2.36}$$

em que:

$\bar{c}_m$ é o complemento de um de c_m;
$\|.\|$ representa o peso de *Hamming*;
$\mathbf{z} = (y_1^2, y_2^2, \ldots, y_n^2)$.

Nas Equações 2.34, 2.35 e 2.36 é considerado:

$$\frac{\mathbf{z} \cdot 0}{\|0\|} = 0.$$

Com o propósito de melhorar o desempenho do sistema multiportadora foram estudados os códigos para controle de erros: BCH e *Reed Solomon*. No próximo capítulo será descrito de forma sucinta esses códigos.

Capítulo 3

Códigos para Controle de Erros

Em sistemas para comunicação digital a informação sofre alterações proveniente do ruído e do desvanecimento presentes no canal, ocasionando erros na recepção do sinal original. A codificação, portanto, introduz redundância (bits extras) na informação de modo a permitir a detecção e correção de erros que possam ocorrer.

Basicamente os códigos corretores de erros são divididos em duas classes: Códigos de Bloco e Códigos Convolucionais. Os códigos de bloco foram desenvolvidos usando conceitos de álgebra abstrata, enquanto que a classe dos códigos convolucionais foi desenvolvida por via empírica, através de pesquisas via computador [15].

Nos códigos de bloco k bits da informação são codificados em n bits formando uma palavra código. Apenas 2^k dos 2^n possíveis palavras são usadas para formar o código. Fazendo n suficientemente grande, para um dado k, pode-se fazer com que cada palavra código seja diferente das demais palavras código em pelo menos $2t+1$ possíveis posições de bits. Em tais casos, t ou menos erros na palavra código pode ser detectada e corrigida pela simples comparação da palavra código recebida com cada uma das 2^k palavras códigos que poderia ter sido transmitida.

O número de posições em que duas palavras código diferem é chamada de distância de *Hamming* d, e o menor valor de d de todos os pares de palavras código é chamado de distância mínima do código d_{min}. A relação entre t e d_{min} é dada por:

$$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor \tag{3.1}$$

em que,

t é o número de erros possíveis de serem corrigidos;

$\lfloor \cdot \rfloor$ representa o maior número inteiro menor que " $\cdot$ ".

O fator de expansão da largura de faixa é $\frac{n}{k}$ e a taxa ou eficiência do código é definida como $R = \frac{k}{n}$. Enquanto que a distância mínima d_{min} determina a capacidade de correção do código, a taxa do código define a eficiência do código. Como o codificador mapeia k bits em n bits, e $n > k$, a taxa de bit da saída do codificador será maior do que a taxa de bit da entrada do codificador. Isto é, o sistema codificado tem maior taxa de bit e requer maior largura de faixa de transmissão.

O objetivo do projetista é maximizar R e d_{min}. Portanto, a complexidade do codificador e do decodificador aumenta com n e, assim, é desejável no projeto de códigos baixos valores de n.

A mais importante subclasse dos códigos de bloco lineares é a classe dos códigos cíclicos. Esses códigos tem, geralmente, bom desempenho e tem estrutura particular que permite bom desempenho e implementação de algoritmos de decodificação eficientes. Os códigos BCH são os melhores tipos de códigos de bloco cíclicos binários. Uma importante subclasse dos códigos BCH são os códigos *Reed Solomon* que são extremamente usados para correção de múltipos erros ou erros em rajadas.

Este capítulo tem como objetivo definir os códigos BCH e os códigos de *Reed Solomon* (RS). Porém, para melhor entendimento deste capítulo, é necessário um conhecimento básico de álgebra e aritmética dos corpos finitos. O Apêndice A apresenta um resumo da aritmética dos corpos finitos. Maiores detalhes podem ser encontrados em [16], [7] e [8]. É também mostrado neste capítulo os resultados da simulação destes códigos em sistema para comunicações com modulação BPSK(*Binary Phase Shift Keying*).

3.1 Códigos BCH

Um código BCH binário com capacidade de correção de t erros pode ser construído com elementos do corpo finito $GF(2^m)$ com m ($m \geq 3$) e t ($t < 2^{m-1}$) e possui os

seguintes parâmetros:

Comprimento do Código: $n = 2^m - 1$

Números de bits de paridade: $n - k \leq m\ t$

Distância mínima: $d_{min} \geq 2\ t + 1$

Dado um comprimento de bloco primitivo $n = q^m - 1$ para algum m e t o número de erros a serem corrigidos. O procedimento para definir o polinômio gerador é:

a) Escolher um polinômio primo de grau m e construir o $GF(q^m)$.

b) Achar $f_j(X)$, o polinômio mínimo de α^i para $i = 1, ..., 2t$.

c) $g(X) = LCM[f_1(X), f_2(X), ..., f_{2t}(X)]$, em que:

LCM(*Least Common Multiple*) é o mínimo múltiplo comum das $f_i(X)$'s, ou seja, é o menor inteiro positivo que é divisível por todos os polinômios $f_i(X)$.

A construção e as operações aritméticas que envolvem elementos do corpo finito $GF(q^m)$ são apresentados no Apêndice A.

A palavra código polinomial $c(X)$ é obtida multiplicando o polinômio da informação pelo polinômio gerador:

$$c(X) = i(X)\ g(X). \tag{3.2}$$

em que:

$$i(X) = i_u\ X^u + i_{u-1}\ X^{u-1} + ... + i_1\ X + i_0 \tag{3.3}$$

e

$$g(X) = g_r\ X^r + g_{r-1}\ X^{r-1} + ... + g_1\ X + g_0. \tag{3.4}$$

Então:

$c(X) = i_u\ g_r\ X^{u+r} +$
$+(i_{u-1}\ g_r + i_u\ g_{r-1} + i_u\ g_{u-2})\ X^{u+r-1} + (i_{u-2}\ g_r + i_{u-1}\ g_{u-1} + i_u\ g_{u-2})\ X^{u+r-2} + ... +$
$+(i_0\ g_2 + i_1\ g_1 + i_2\ g_0)\ X^2 + (i_0\ g_1 + i_1\ g_0)\ X + i_0\ g_0.$

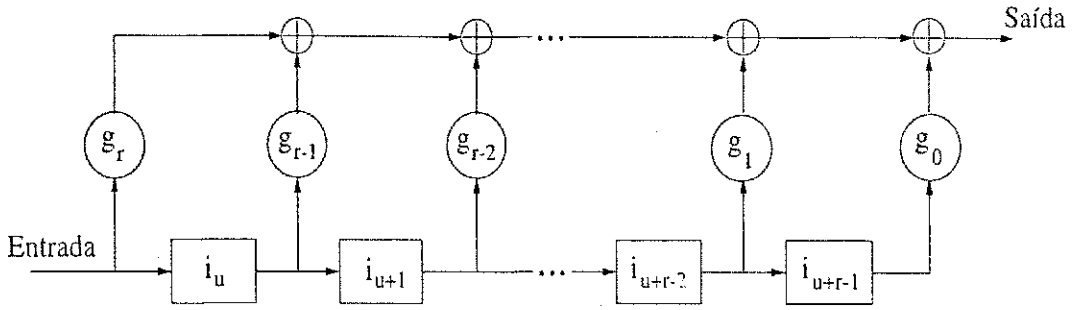


Figura 3.1: Circuito Multiplicador de Polinômios.

A Figura 3.1 ilustra o diagrama em bloco de um circuito multiplicador de polinômios [17] para a obtenção da palavra código. Os dispositivos de armazenamento contém inicialmente zero. A entrada dos coeficientes de $i(X)$, no circuito, é na ordem decrescente, ou seja, o coeficiente de maior grau entra primeiro. Depois de entrar com todos os coeficientes de $i(X)$ completa-se o processo com zeros. Na saída obtemos os coeficientes de $c(X)$ na ordem decrescente. Lembre-se que nste circuito todos os elementos dos polinômios e as operações de soma e multiplicação são efetuados no corpo finito $GF(q^m)$ descritos no Apêncice A.

3.2 Códigos *Reed Solomon*

Um código RS em $GF(q)$ é um código BCH não binário com parâmetros:

Comprimeto do Código: $N = q - 1$

Números de bits de Paridade: $N - K = 2\ t$

Distândia Mínima: $d_{min} = 2\ t + 1$

Considerando α um elemento primitivo em GF(q). O polinômino gerador do código RS(N,K) que corrige t erros é:

$$g(X) = \prod_{i=1}^{v} \left(X - \alpha^i\right) \tag{3.5}$$

em que: $v = 2t$.

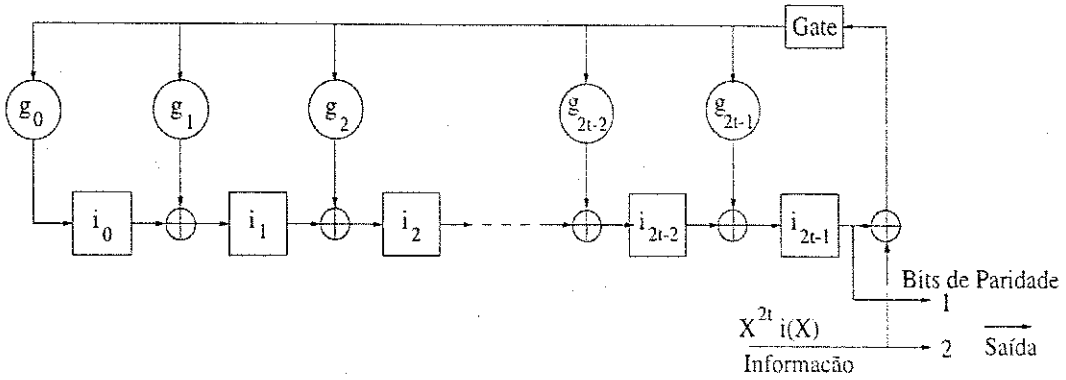


Figura 3.2: Codificador Sistemático.

Ao considerar o código RS(N,K) com polinômio gerador dado pela Equação 3.5, então a expressão da palavra código $c = c_0 c_1 \ldots c_{N-1}$ deste código é obtida por adicionar um bit c_N, que é um bit de paridade de todos os outros bits de c, ou seja:

$$c_N = -\sum_{i=0}^{N-1} c_i, \tag{3.6}$$

produzindo, assim, um código(N+1,K) que é chamado de código RS extendido.

Seguindo o mesmo procedimento feito para o código BCH, a palavra código polinomial $c(X)$ é definida pela Equação 3.2. Neste caso tem-se a codificação não sistemática.

O codificador sistemático mapeia a mensagem $i(X)$ em uma palavra código $c(X)$ de tal maneira que a mensagem pode ser encontrada sem alterações na palavra código. Na forma sistemática, os $2t$ símbolos de paridade são os coeficientes do resto $b(X) = b_0 + b_1\ X^2 + \ldots + b_{2\ t-1}\ X^{2\ t-1}$ da divisão do polinômio da mensagem vezes $X^{2\ t}$, pelo polinômio gerador $g(X)$. A implementação deste processo pode ser feita usando um circuito divisor como mostra a Figura 3.2. Inicialmente a chave está na posição 2. Ao mesmo tempo que $i(X)$ entra no canal, é também armazenado nos registradores. Depois que os símbolos de informação tenham sido enviados no canal, os $N - K$ bits restantes serão gerados pelos registradores que fazem o cálculo da paridade.

3.3 Decodificador

Supondo $c(x) = c_0 + c_1\ x + c_2\ x^2 + ... + c_{n-1}\ x^{n-1}$ o vetor transmitido e $r(x) = r_0 + r_1\ x + r_2\ x^2 + ... + r_{n-1}\ x^{n-1}$ o correspondente vetor recebido. Então:

$$e(x) = r(x) - c(x). \tag{3.7}$$

Assim, $e(x) = e_0 + e_1\ x + e_2\ x^2 + ... + e_{n-1}\ x^{n-1}$ é o vetor erro adicionado pelo canal, em que $e_i = r_i - c_i$ é um símbolo de $GF(2^m)$.

Assumindo que o vetor recebido têm v erros nas posições $i_1, i_2, ...i_v$. Então:

$$e(x) = e_{i_1}\ x^{i_1} + e_{i_2}\ x^{i_2} + ... + e_{i_v}\ x^{i_v}. \tag{3.8}$$

Definindo $\{X_l\} = \alpha^{i_l}$, $l = 1, 2, ..., v$, os números das localizações dos erros. Então as $2t$ síndromes são calculadas da seguinte forma:

$$S_j = r(\alpha^j) = e_{i_1}\ (\alpha^j)^{i_1} + e_{i_2}\ (\alpha^j)^{i_2} + ... + e_{i_v}\ (\alpha^j)^{i_v} \tag{3.9}$$

$$S_j = e_j\ (\alpha^{i_1})^j + e_j\ (\alpha^{i_2})^j + ... + e_j\ (\alpha^{i_v})^j \tag{3.10}$$

$$S_j = e_{i_1}\ X_1^j + e_{i_2}\ X_2^j + ... + e_{i_v}\ X_v^j \tag{3.11}$$

Fazendo a expansão da equação anterior:

$$\begin{array}{rcccccccc} S_1 & = & e_{i_1}\ X_1 & + & E_{i_2}\ X_2 & + & ... & + & e_{i_v}\ X_v \\ S_2 & = & e_{i_1}\ X_1^2 & + & E_{i_2}\ X_2^2 & + & ... & + & e_{i_v}\ X_v^2 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ S_{2t} & = & e_{i_1}\ X_1^2 t & + & E_{i_2}\ X_2^2 t & + & ... & + & e_{i_v}\ X_v^2 t \end{array}$$

As equações das síndromes podem ser transladadas em séries de equações lineares, definindo o polinômio localizador de erros, $\Lambda(x)$, na qual as raízes são as raízes inversas das localizações dos erros $\{X_i\}$:

$$\Lambda(x) = \prod_{l=1}^{v} (1 - X_l\ x).$$

$$\Lambda(x) = \Lambda_v\, x^v + \Lambda_{v-1}\, x^{v-1} + ... + \Lambda_1\, x + 1. \tag{3.12}$$

Assumindo que $v = t$ erros tenha ocorrido, em que t é a capacidade de correção de erro do código. Então, obtemos a seguinte equação:

$$\begin{bmatrix} S_1 & S_2 & S_3 & \dots & S_t \\ S_2 & S_3 & S_4 & \dots & S_{t+1} \\ S_3 & S_4 & S_5 & \dots & S_{t+2} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ S_t & S_{t+1} & S_{t+2} & \dots & S_{2t-1} \end{bmatrix} \begin{bmatrix} \Lambda_t \\ \Lambda_{t-1} \\ \Lambda_{t-2} \\ \vdots \\ \Lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ -S_{t+3} \\ \vdots \\ -S_{2t} \end{bmatrix} \tag{3.13}$$

A Figura 3.3 ilustra o algoritmo de decodificação. Primeiramente é feito o cálculo das síndromes. Em seguida, é calculado o polinômio localizador de erros utilizando o algoritmo de *Berlekamp-Massey* [7]. Na etapa seguinte, acha-se as localizações dos erros, ou seja, calculam-se as raízes do polinômio localizador de erros. Por fim, utiliza-se o algoritmo de *Forney* [7] para achar as magnitudes dos erros.

3.3.1 Algoritmo de *Berlekamp-Massey*

O algoritmo de *Berlekamp-Massey* é um algoritmo utilizado para calcular os coeficientes do polinômio localizador de erros $\Lambda(X)$. Este algoritmo oferece uma alternativa mais eficiente e menos complexa para correções de um número maior de erros.A Figura 3.4 mostra, na forma de organograma, todas as etapas deste algoritmo.

3.3.2 Algoritmo de *Forney*

Inicialmente define-se uma síndrome polinomial de grau infinito:

$$S(X) = S_1\, X + S_2\, X^2 + ... + S_{2t}\, X^{2t} + S_{2t+1}\, X^{2t+1} + ... \tag{3.14}$$

Então, calcula-se a magnitude polinomial do erro:

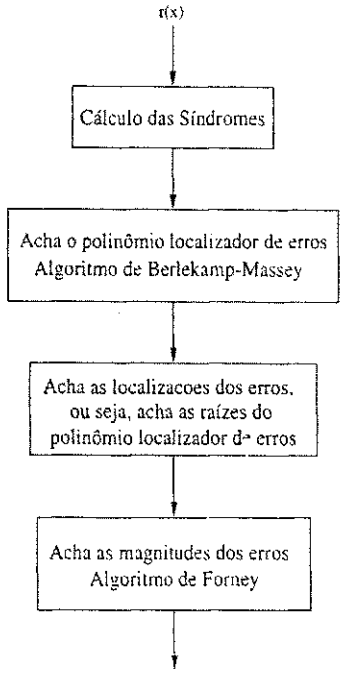


Figura 3.3: Algoritmo de decodificação.

$$\Omega(X) = [1 + S(X)]\ \Lambda(X). \tag{3.15}$$

Dado que é conhecido apenas os primeiros $2t$ coeficientes de $S(X)$, o problema de decodificação se reduz a achar um polinômio $\Lambda(X)$ de grau menor ou igual que t que satisfaz:

$$\Lambda(X)\ [1 + S(X)] \equiv \Omega(X)\ mod(X^{2t+1}). \tag{3.16}$$

As magnitudes dos erros são calculadas usando a equação:

$$e_{iK} = \frac{-X_K\ \Omega(X_K^{-1})}{\Lambda'(X_k^{-1})}. \tag{3.17}$$

3.3.3 Exemplo

Para exemplificar a decodificação do código RS será considerado o código RS$(7, 3)$ que corrige dois erros:

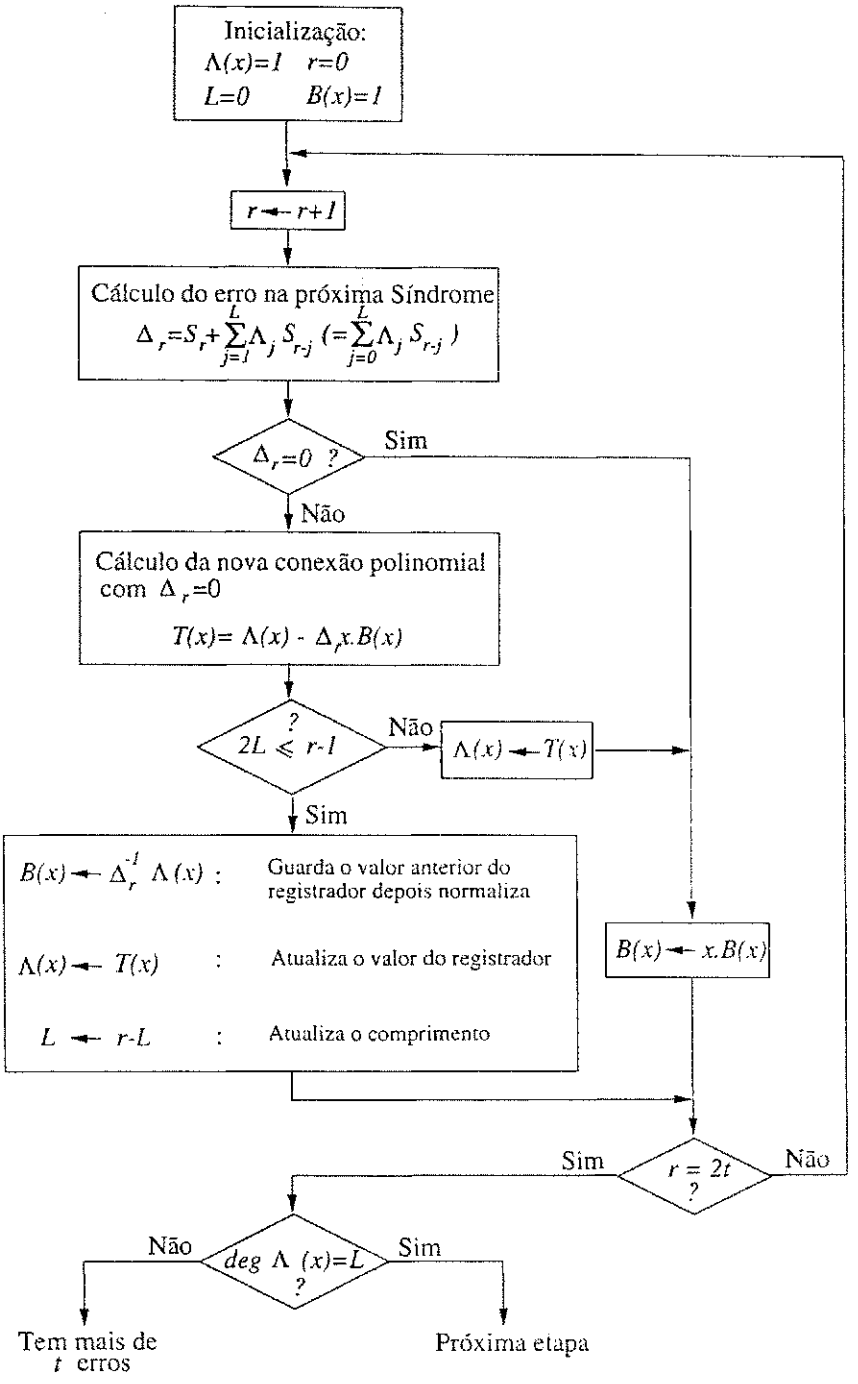


Figura 3.4: Algoritmo de *Berlekamp-Massey*.

k	S_k	$\Lambda(k)(x)$	$\Delta(k)$	L	$T(x)$
0	-	1	-	0	x
1	α^6	$1+\alpha^6\ x$	$S_1 - 0 = \alpha^6$	1	$\alpha\ x$
2	α^3	$1+\alpha^4\ x$	$S_2 - \alpha^5 = \alpha^2$	1	$\alpha\ x^2$
3	α^4	$1+\alpha^2\ x+\alpha\ x^2$	$S_3 - 1 = \alpha^5$	2	$\alpha^2\ x+\alpha^6\ x^2$
4	α^3	$1+\alpha^2\ x+\alpha\ x^2$	$S_4 - \alpha^4 = \alpha^6$	-	-

Tabela 3.1: Execução do algoritmo de *Berlekamp-Massey* e *Forney*

Neste caso o corpo finito $GF(2^3)$ é usado nas operações envolvidas.
Por definição o polinômio gerador é dado por:

$$g(x) = (x+\alpha)\ (x+\alpha^2)\ (x+\alpha^3)\ (x+\alpha^4) \tag{3.18}$$

$$g(x) = x^4 + \alpha^3\ x^3 + x^2 + \alpha\ x + \alpha^3 \tag{3.19}$$

Supondo que o polinômio recebido seja:

$$r(x) = \alpha^2\ x^6 + \alpha^2\ x^4 + x^3 + \alpha^5\ x^2.$$

Calculando os valores das síndromes utilizando a Equação 4.8, obtemos os seguintes valores:

$$S_1 = \alpha^6,$$
$$S_2 = \alpha^3,$$
$$S_3 = \alpha^4,$$
$$S_4 = \alpha^3.$$

Aplicando o algoritmo de *Berlekamp-Massey*,obtem-se:

$$\Lambda(x) = 1 + \alpha^2\ x + \alpha\ x^2.$$

Calculando o pilonômio da magnitude do erro:

$$\Omega(x) = \Lambda(x)[1 + S(x)] \; mod \; x^{2t+1}, \tag{3.20}$$

$$\Omega(x) = (1 + \alpha^2 \; x + \alpha \; x^2) \; (1 + \alpha^6 \; x + \alpha^3 \; x^2 + \alpha^4 \; x^3 + \alpha^3 \; x^4) \; mod \; x^5,$$

$$\Omega(x) = (1 + x + \alpha^3 \; x^2) \; mod \; x^5.$$

As localizações dos erros são: $X_1 = \alpha^3$ e $X_2 = \alpha^5$. E as magnitudes dos erros são:

$$e_{i_k} = \frac{-X_k \; \Omega(X_k^{-1})}{\Delta`(X_k^{-1})} \tag{3.21}$$

$$e_{i_k} = \alpha^5 \; X_k + \alpha^5 + \alpha \; X_k^{-1} \tag{3.22}$$

$$e_3 = \alpha^5 \; \alpha^3 + \alpha^5 + \alpha \; \alpha^4 = \alpha \tag{3.23}$$

$$e_5 = \alpha^5 \; \alpha^5 + \alpha^5 + \alpha \; \alpha^2 = \alpha^5 \tag{3.24}$$

3.4 Simulações Realizadas

Para se verificar a eficiência dos códigos RS, foi feita uma simulação de um sistema com modulação BPSK (*Binary Phase Shift Keying*), cuja expressão do sinal modulado é:

$$s_i(t) = \sqrt{\tfrac{2 \; E}{T}} \; cos \; (2\pi f_0 t + \pi i), \quad 0 \leq t \leq T, \quad i = 1, 2;$$

em que:

E é a energia por símbolo;

T é a duração do símbolo;

f_0 é a freqüência da portadora.

A Figura 3.5 ilustra o diagrama em blocos do sistema considerando um canal AWGN(*Aditive White Gaussian Noise*) com densidade espectral de potência $\frac{N_0}{2}$. Inicialmente esse sistema foi simulado sem o codificador RS e em seguida foram utilizados os códigos RS(7,3) e RS(31,16).

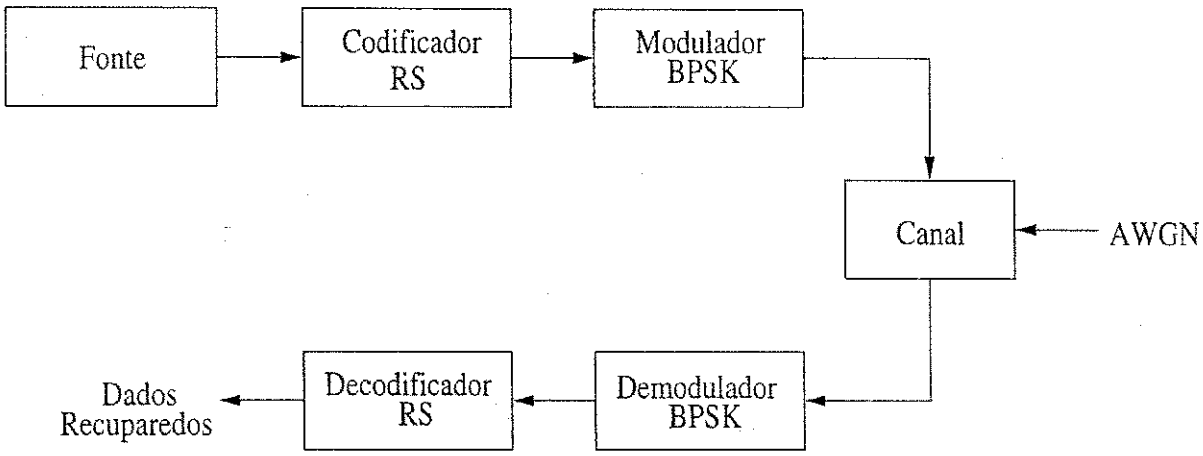


Figura 3.5: Sistema com modulação BPSK com codificador RS(N,K) e canal AWGN.

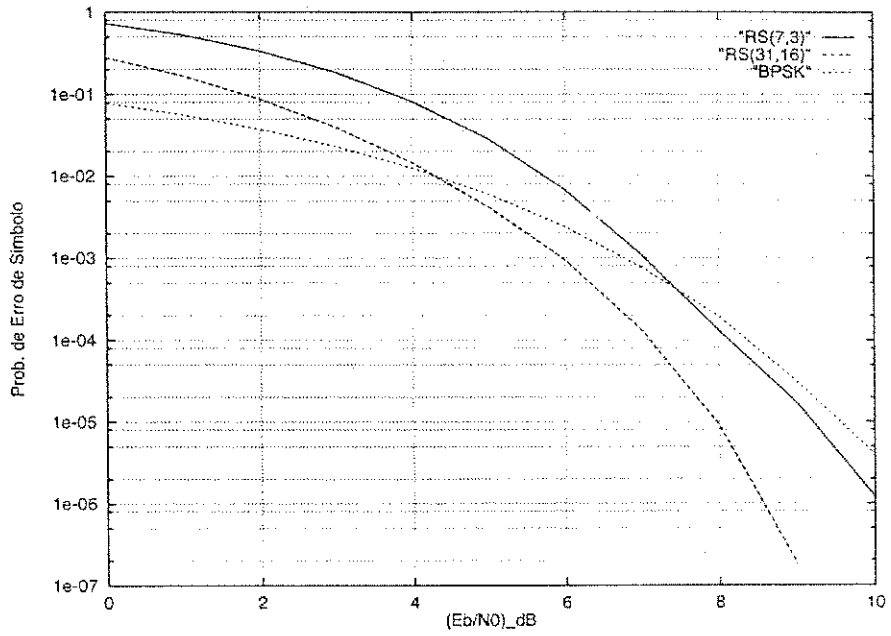


Figura 3.6: Curvas de Probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para um sistema com modulação BPSK e canal AWGN. A curva *BPSK* é a curva obtida para o sistema sem codificação e as curvas *RS(7,3)* e *RS(31,16)* são as curvas obtidas para o sistema que utiliza os códigos RS(7,3) e RS(31,16), respectivamente.

As curvas da Figura 3.6 mostram que o desempenho do sistema com codificação para controle de erro. É observado que o código RS(31,16) é cerca de 0.8 dB melhor que o código RS(7,3). Isso mostra que quanto menor o número de bits extras da palavra código, pior será o desempenho do código.

Capítulo 4

Procedimento de Simulação e Análise dos Resultados

Nos capítulos anteriores foi apresentado o sistema multiportadora incluindo o modelo do canal em ambientes fechados considerado neste trabalho, a modulação utilizada nos subcanais, a demodulação, o codificador de multiportadora e por fim, o codificador para controle de erros.

Neste capítulo apresenta os detalhes da simulação do sistema proposto, a descrição do modelo equivalente passa-baixas e os resultados das simulações serão mostrados e avaliados.

4.1 Modelo Equivalente Passa-baixas do Sistema Multiportadora

Em simulação, trabalha-se com o equivalente passa-baixas do sinal que corresponde de maneira similar ao sinal real e tem a vantagem de não conter componentes da portadora do sinal.

4.1.1 Fonte de Informação

A fonte de informação consiste de um gerador de números aleatórios que produz, a cada iteração, símbolos do corpo finito $GF(2^K)$ e de um conversor decimal/binário que transforma os símbolos em um vetor de tamanho K.

4.1.2 Codificador de Multiportadora

Os K bits fornecidos pela fonte são transformados na palavra código c_j de tamanho N de acordo com o código binário (N,K) utilizado para mapear as portadoras. Neste trabalho, utiliza-se os códigos binários BCH(15,5) linear e não-linear, como também, o código BCH(21,5) não-linear conforme descrito no Capítulo 2.

4.1.3 Modulador

Cada um dos bits C_{ij} da palavra código c_j serão modulados e enviados por um subcanal. Um sinal em um subcanal com modulação OOK é descrita da seguinte forma:

$$s_i(t) = \begin{cases} A\ cos(2\pi f_i t + \theta_i) & ,\ se\ \ C_{ij} = 1 \\ 0 & ,\ se\ \ C_{ij} = 0 \end{cases}$$

em que:

$A = \sqrt{\frac{2\ E_t}{T}}$ é a amplitude do sinal modulado;

$i = 1, 2, ..., N$ representa o tamanho de cada palavra código;

$j = 1, 2, ..., L$ representa os L símbolos fornecidos pela fonte.

A relação entre um sinal $s_i(t)$ e seu equivalente passa baixa $\hat{s}_i(t)$ é:

$$s_i(t) = Re\left[\hat{s}_i(t)\ e^{j2\pi f_i t}\right]. \tag{4.1}$$

O equivalente passa baixa de $s_i(t)$, neste caso, é:

$$\hat{s}_i(t) = \begin{cases} A & ,\ se\ \ C_{ij} = 1 \\ 0 & ,\ se\ \ C_{ij} = 0 \end{cases}$$

4.1.4 Canal

Como em uma simulação trabalha-se com seqüências discretas no tempo, deve-se realizar a amostragem do sinal e também do ruído. Cada intervalo de sinalização, T, será dividido em N_a intervalos de amostragem de duração T_a, ou seja:

$$T = N_a \, T_a$$

As seqüências de amostras do ruído gaussiano adicionado às amostras do sinal enviado através de um subcanal são constituídas por duas seqüências de variáveis aleatórias gaussianas $\{\hat{n}_{Fl}\}$ e $\{\hat{n}_{Ql}\}$, correspondentes às amostras das componentes em fase e quadratura do equivalente em banda básica. Essas seqüências são independentes, identicamente distribuídas e possuem média nula e variância (σ^2) que é ajustada de modo a obter-se o valor desejado de $\frac{E_b}{N_0}$ na entrada de receptor.

Considerando $\{\hat{r}_{Fl}\}$ e $\{\hat{r}_{Ql}\}$ como as seqüências de amostras em fase e quadratura do sinal recebido em um subcanal, respectivamente. Com a modulação OOK o sinal transmitido, $s_i(t)$, é real e igual a A ou 0. Para o caso em que $s_i(t) = A$, tem-se que as respectivas seqüências em fase e quadratura do sinal recebido é:

$$\hat{r}_{Fl} = \hat{s}_{Fl} + \hat{n}_{Fl} \tag{4.2}$$

$$\hat{r}_{Ql} = \hat{n}_{Ql} \tag{4.3}$$

em que: $l = 1, 2, ..., N_a$. é o número de amostras do sinal.

No canal em ambiente fechado foi considerado que o desvanecimento *Rayleigh* lento em cada subcanal. Desta forma, as amplitudes do desvanecimento α_i dos subcanais são variáveis aleatórias independentes e identicamente distribuídas com densidade de probabilidade *Rayleigh* dada pela seguinte expressão:

$$p(\alpha) = \frac{2 \, \alpha}{\sigma^2} \, e^{-\frac{\alpha^2}{\sigma^2}}, \qquad \alpha \geq 0. \tag{4.4}$$

A consideração de independência do desvanecimento é válida se cada um dos N subcanais forem independentes. As componentes em fase e quadratura do sinal recebido, são:

$$\hat{r}_{Fl} = \hat{s}_{Fl} \,.\hat{\alpha}_{Fl} \; + \; \hat{n}_{Fl} \tag{4.5}$$

$$\hat{r}_{Ql} = \hat{s}_{Ql} \,.\hat{\alpha}_{Ql} \; + \; \hat{n}_{Ql} \tag{4.6}$$

em que: $l = 1, 2, ..., N_a$. é o número de amostras do sinal.

A detecção do sinal recebido é obtida pela envoltória complexa deste sinal. Portanto, teremos que o canal em ambiente fechado será afetado pelo desvanecimento e pelo ruído AWGN. A Figura 4.1 ilustra este subcanal.

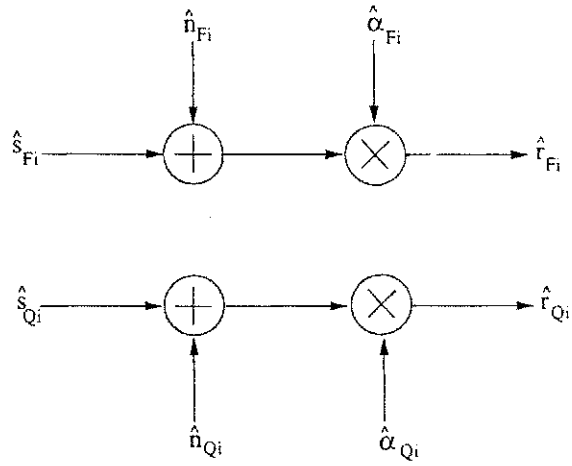


Figura 4.1: Modelo equivalente passa-baixas de um subcanal em ambiente fechado.

4.1.5 Demodulador

Neste sistema é utilizado a demodulação não coerente com N detectores de envoltória. A saída de cada detector será dada pelo valor médio dos amostras em fase e quadratura do sinal recebido:

$$y_i = \sqrt{\left(\frac{\sum_{i=1}^{N_a} \hat{r}_{Fi}}{N_a}\right)^2 + \left(\frac{\sum_{i=1}^{N_a} \hat{r}_{Qi}}{N_a}\right)^2} \tag{4.7}$$

O vetor $\mathbf{Y} = (y_1, y_2, ..., y_N)$ será usado para o cálculo das métricas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, descritas no Capítulo 2, que estimarão o símbolo enviado.

4.1.6 Razão Sinal/Ruído

A razão sinal/ruído, $\frac{E_b}{N_0}$, relaciona o sinal e o ruído gaussiano branco e é o parâmetro fundamental do qual depende a probabilidade de erro.

A energia do sinal em um período de sinalização em um subcanal é calculada pela seguinte expressão:

$$\varepsilon = \frac{1}{2} \int_T |\hat{s}(t)|^2 \, dt. \tag{4.8}$$

Como estamos utilizando um sinal OOK em que cada intervalo de sinalização é enviado um tom, temos que a energia por tom em um canal AWGN, é:

$$E_t = \frac{A^2 \, T}{2}. \tag{4.9}$$

Para um canal AWGN, a largura de faixa do ruído será considerada igual a B e com distribuição de potência:

$$S(f) = \tfrac{N_0}{2}, \quad para \quad |f| < B.$$

A autocorrelação do ruído é:

$$R(\tau) = \int_{-\infty}^{\infty} \frac{N_0}{2} \, e^{j2\pi f \tau} \, df = N_0 \, B \, \frac{sen(2\pi B\tau)}{2\pi B\tau}.$$

O ruído será descorrelacionado caso $R(\tau) = 0$, ou seja, quando $\tau = \frac{1}{2B}$. E a variância do ruído é: $\tau^2 = R(0) = N_0 \, B$.

Entretanto para um subcanal, temos que sua largura de faixa é $\frac{B}{N}$, em que N é o número de subcanais determinado pelo tamanho da palavra código de multiportadora. Em um subcanal, isto ocorre quando $\tau = \frac{N}{2B}$. Desta forma, o tempo de amostragem a ser utilizado na simulação deve ser $T_a = \frac{N}{2B}$.

Para se definir a razão $\frac{E_b}{N_0}$, é necessário definir a relação entre a energia de tom e a energia de bit. Um intervalo de sinalização T é equivalente a K T_b e a relação de E_t com E_b é:

$$E_t = \frac{K\ E_b}{N_{ca}}, \tag{4.10}$$

em que:

K é o número de bits da informação a ser codificados pelo codificador de multiportadora,

N_{ca} é o número médio de canais transmitindo sinal para os quais $s_i(t) \neq 0$, ou seja, é o somatório de $C_{ij} = 1$ de cada palavra código dividido pelo número de palavras códigos possíveis do código.

Substituindo $T = N_a\ T_a$ e $T_a = \frac{N}{2B}$ na Equação 4.8, tem-se:

$$E_t = \frac{A^2\ N_a\ N}{4\ B}. \tag{4.11}$$

Dividindo E_t por N_0 e substituimos E_t por E_b, tem-se:

$$\frac{E_b}{N_0} = \frac{A^2\ N_a\ N\ N_{ca}}{4\ N_0\ B\ K}.$$

Como $\sigma^2 = N_0\ B$, então:

$$\frac{E_b}{N_0} = \frac{A^2\ N_{ca}\ N_a\ N}{4\ K\ \sigma^2}. \tag{4.12}$$

Entretanto:

$$\left(\frac{E_b}{N_0}\right)_{dB} = 10\ log\left(\frac{E_b}{N_0}\right),$$

$$\frac{E_b}{N_0} = 10^{0.1\ \left(\frac{E_b}{N_0}\right)_{dB}}.$$

Assim:

$$\sigma^2 = \frac{A^2\ N_a\ N\ N_{ca}}{4\ K}\ 10^{-0.1\ \left(\frac{E_b}{N_0}\right)_{dB}} \tag{4.13}$$

A Equação 4.13 relaciona todos os parâmetros envolvidos na simulação. É considerado fixo o número de amostras N_a em 16, a amplitude do sinal A é unitária, N_{ca} para o caso do código binário BCH(15,5) não-linear é $N_{ca} = \frac{320}{32} = 7.5$.

Para o canal sujeito ao desvanecimento, que é o caso do canal em ambiente fechado, o sinal recebido é multiplicado por um fator α que representa a amplitude do desvanecimento. Neste caso, a energia por tom será dada por:

$$E_t = \frac{\mathcal{E}[\alpha^2]\ A^2\ T}{2} \tag{4.14}$$

Considerando que o desvanecimento *Rayleigh* é obtido através de duas v.a. gaussianas com parâmetro $\frac{1}{2}$, o valor esperado, $\mathcal{E}[\alpha^2]$, será igual a um. Com esta consideração, os cálculos da relação sinal/ruído para o canal AWGN, descritas anteriormente, são também válidas para o canal com desvanecimento.

4.1.7 Codificador/Decodificador *Reed Solomon*

Ao adicionar o codificador RS(31,16) e o entrelaçamento(*interleaving*) ao sistema multiportadora foi considerado que a fonte de informação deveria gerar uma palavra código de 16 símbolos que seriam codificados para 31 símbolos em $GF(32)$. O entrelaçamento foi obtido considerando que os desvanecimentos fossem independentes entre os símbolos da palavra código RS. Cada um desses símbolos foi convertido para binário para posteriormente foram codificados pelo codificador de multiportadora e enviados através dos subcanais.

4.1.8 Probabilidade de Erro de Símbolo

Para um determinado número de iterações, símbolos são gerados pela fonte e é feita a contagem dos erros ocorridos comparando o símbolo enviado com o sómbolo recebido. A razão entre o número de erros e o número total de símbolos gerados determina a probabilidade de erro de símbolo.

4.2 Procedimento de Simulação

Utilizando a liguagem de programação "C", cada um dos blocos da Figura 2.1 representados por seu equivalente passa-baixas correspondeu a uma função do programa principal.

Na simulação foi utilizado o método de Monte Carlo [23]. Nesse método, conta-se o número de "sucessos", que nesse caso são os erros de símbolos, e divide-se pelo número de tentativas que geralmente é da ordem de 10.000. A Figura 4.2 ilustra o algoritmo implementado do sistema multiportadora proposto.

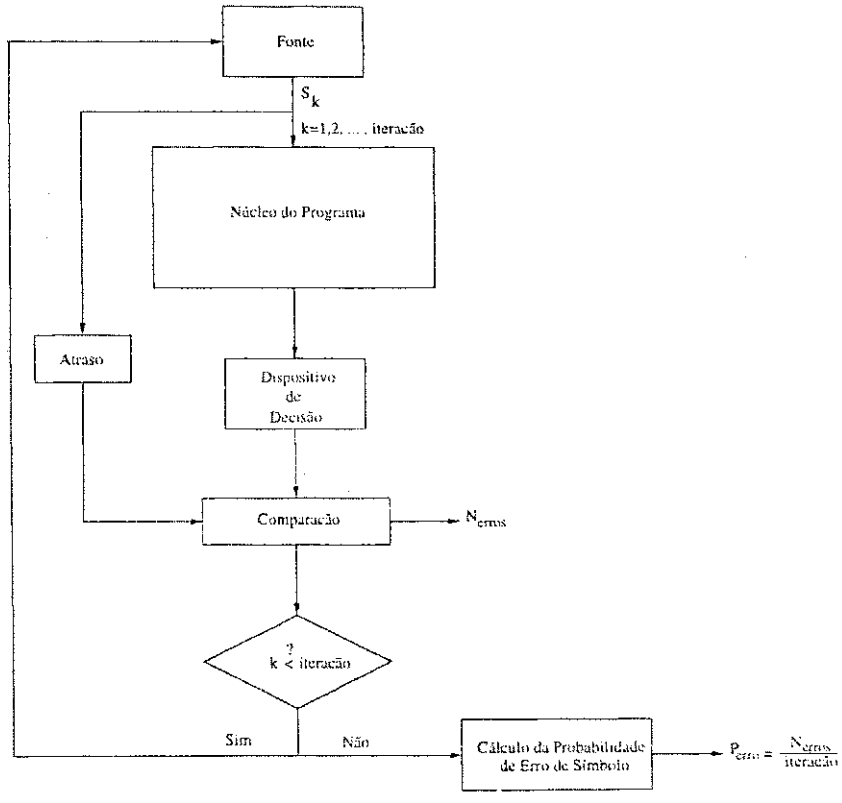


Figura 4.2: Algoritmo do sistema multiportadora proposto

4.3 Resultados das Simulações

As simulações do sistema proposto foram feitas em três etapas. A primeira etapa teve o objetivo de avaliar o desempenho das métricas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ sistema multiportadora com canal AWGN utilizando os códigos binários BCH(15.5) linear e não-linear. A segunda etapa, o sistema multiportadora, considerando o canal em ambiente fechado, utilizando os códigos binários BCH(15,5) linear e não-linear foi avaliado através das métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$. Nesta etapa, foi também simulado o sistema multiportadora através da métrica descrita pela Equação 2.32. Na última etapa o sistema multiportadora utilizando o código binário não-linear (15,5) e o canal em ambiente fechado, foi avaliado em conjunção com o codificador para controle de erros, RS(31.16), e o entrelaçamento. A seguir será mostrados os resultados obtidos nestas três etapas.

Etapa 1

Utilizando o código binário BCH(15,5) linear, mostrado na Tabela 2.1, para mapear o conjunto de portadoras e considerando o canal AWGN, o desempenho do sistema multiportadora foi avaliado através das métricas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$. A Figura 4.3 apresenta os resultados da simulação deste sistema.

Verifica-se que o desempenho das métricas $d1^{(m)}$, $d2^{(m)}$ e $d3^{(m)}$ não são aceitáveis devido as probabilidades de erro possuirem valores acima de 0.01. Nesta etapa, a métrica ML é ótima para canais AWGN.

Utilizando o código binário (15,5) não-linear, mostrado na Tabela 2.1, verifica-se que o desempenho das métricas possuem valores aceitáveis. Neste caso, a diferença entre a métrica $d3^{(m)}$ e a ML é menor que 1 dB. Verifica-se, portanto, que o código não-linear e a métrica $d_3^{(m)}$ proporcionam um desempenho satisfatório na presença do ruído gaussiano branco.

Etapa 2

Nesta etapa foi simulado o sistema multiportadora para ambientes fechados utilizando os códigos binários não-lineares (15,5) e (21,5), mostrados nas Tabelas 2.1 e 2.2 respectivamente, em conjunto com as métricas $d1^{(m)}$, $d2^{(m)}$ e $d3^{(m)}$. Verifica-se, na Figura 4.4, utilizando o código (15,5), que a métrica $d3$ possue melhores resultados e

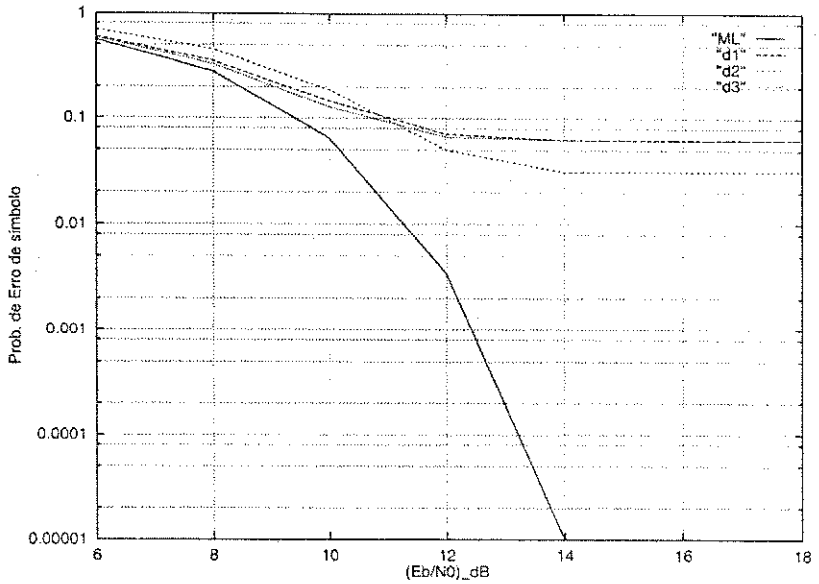


Figura 4.3: Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora com canal AWGN e o código binário BCH(15,5) linear. As curvas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente.

que a diferença entre a métrica ML e a métrica $d_3^{(m)}$ é menor que 1 dB.

A Figura 4.5 ilustra o desempenho do sistema multiportadora para ambientes fechados que utiliza o código binário não-linear (21,5). Neste caso, é observado que a métrica $d1^{(m)}$ proporciona o melhor desempenho. Através dos resultados mostrados nas Figuras 4.5 e 4.6, concluimos, através das métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, que o desempenho do sistema multiportadora está fortemente relacionado com a escolha do código de multiportadora utilizado para mapear os conjuntos de portadoras.

Também nesta etapa, foi simulado o sistema multiportadora para ambientes fechados utilizando a métrica obtida pelo critério ML, descrita pela Equação 2.33, para canais com desvanecimento. A Figura 4.7 mostra as curvas obtidas nesta simulação. Observa-se que os resultados obtidos através desta métrica não são melhores do que os resultados da métrica $d_3^{(m)}$. Portanto, o cálculo desta métrica para sistema reais é impraticável devido a sua complexidade.

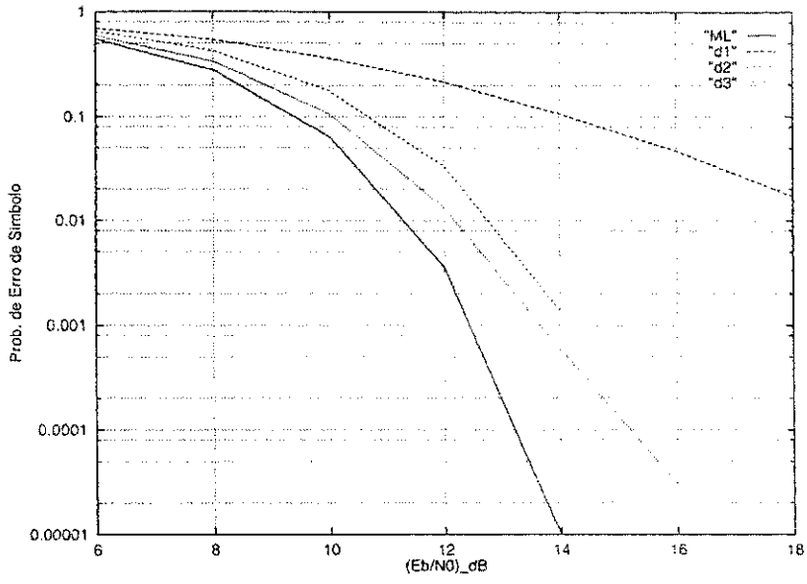


Figura 4.4: Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora com canal AWGN e o código binário BCH(15,5) não-linear. As curvas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas ML, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente.

Etapa 3

Nesta etapa, foi simulado o sistema multiportadora para ambientes fechados utilizando o código binário não-linear (15,5), o codificador RS(31,16) e o entrelaçamento. Foi considerado que a independência dos níveis de desvanecimento entre os símbolos das palavras códigos RS proporciona o entrelaçamento desejado. A Figura 4.8 apresenta os resultados desta simulação. Observa-se que as métricas, neste caso, possuem melhores desempenhos do que o sistema sem correção de erros, tendo a métrica $d3^{(m)}$ o melhor desempenho em relação as demais métricas.

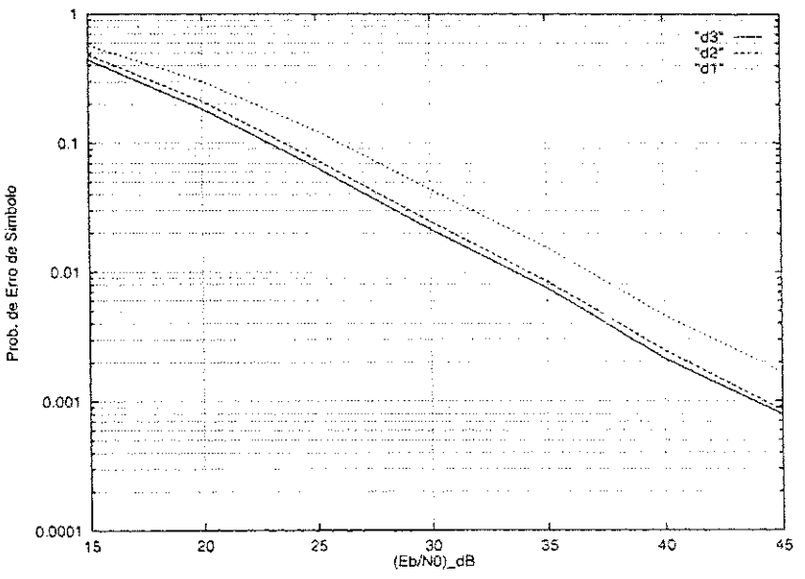


Figura 4.5: Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora para ambientes fechados utilizando o código binário BCH(15,5) não-linear. As curvas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente.

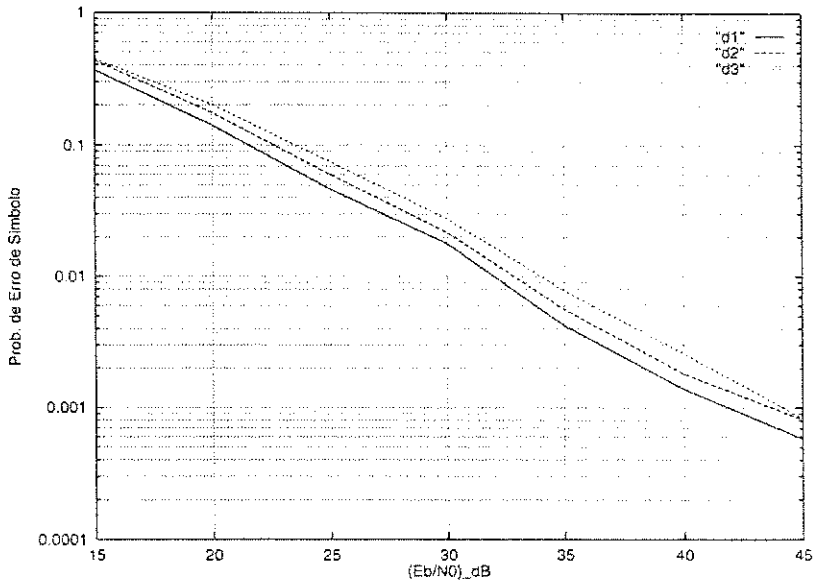


Figura 4.6: Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora para ambientes fechados utilizando o código binário BCH(21,5) não-linear. As curvas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente.

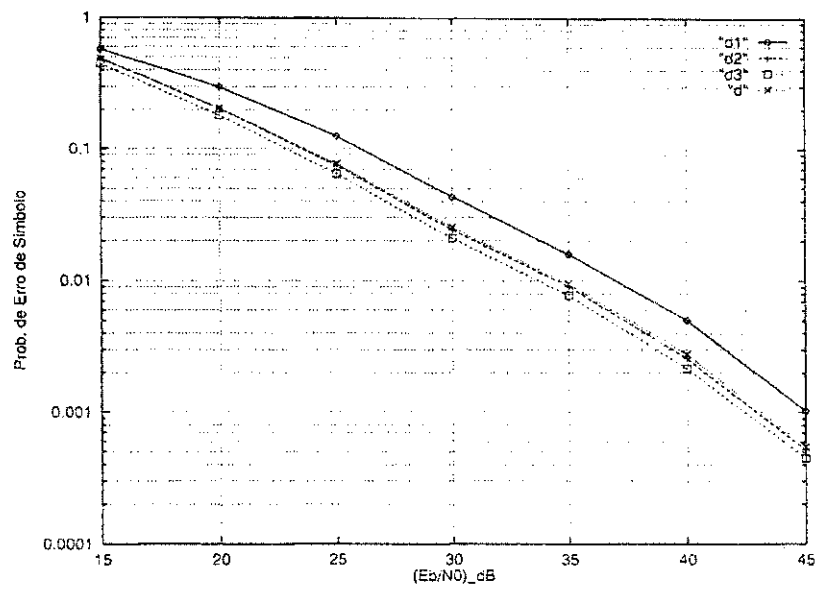


Figura 4.7: Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora para ambientes fechados utilizando o código binário BCH(15,5) não-linear. As curvas $d^{(j)}$, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas $d^{(j)}$, $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente.

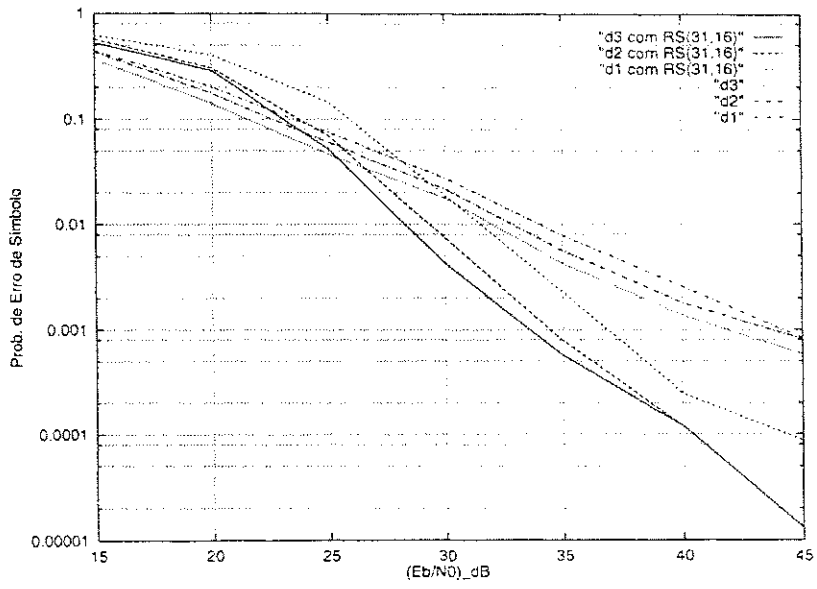


Figura 4.8: Curvas de probabilidade de erro de símbolo versus $\frac{E_b}{N_0}$ para o sistema multiportadora para ambientes fechados utilizando o código binário BCH(15,5) não-linear e o código RS(31,16). As curvas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$ são as curvas obtidas utilizando as métricas $d_1^{(m)}$, $d_2^{(m)}$ e $d_3^{(m)}$, respectivamente.

Capítulo 5

Conclusão

Neste trabalho foram feitas algumas simulações com o sistema multiportadora com o objetivo de avaliar o seu desempenho para canais em ambientes fechados utilizando um código binário não-linear para mapear os conjuntos de portadoras.

O sistema multiportadora utilizando o código binário BCH(15,5) linear não apresentou desempenho aceitável. Isso porque esse código possui palavras código de pesos que variam de 0 a 15 favorecendo a detecção incorreta de símbolos de peso superior aos demais. Ao utilizar o código BCH(15,5) não linear, que possui palavras código com pesos quase constantes, verificou-se que o desempenho do sistema foi melhor do que o sistema que utiliza o código BCH(15,5) linear. A diferença entre a métrica d_3 e a métrica ML, que é ideal para canais AWGN, foi de aproximadamente 1 dB.

Resultados mostraram que o desempenho do sistema multiportadora proposto, está relacionado com a escolha do código não-linear utilizado para mapear os conjuntos de portadoras e com a métrica utilizada para estimar o símbolo enviado. Para o código BCH(15,5) não-linear, a métrica d_3 proporcionou melhores resultados, enquanto que a métrica d_1 proporcionou melhores resultados para o código BCH(21,5) não-linear.

A simulação do sistema proposto com a métrica ML para canais com desvanecimento mostrou resultados aproximado ao resultado da métrica d_2. Tal resultado se deve ao cálculo aproximado da integral. Apesar desta métrica ser ideal para canais com desvanecimento, seu calculo é complexo para sistemas reais.

Algumas simulações com outras métricas foram realizadas com resultados pratica-

mente idênticos aos da métrica d_3. Portanto, tais resultados sugerem a utilização de outras técnicas, além da detecção de envoltória, caso se procure melhorias ainda maior no desempenho do sistema.

A utilização da codificação para controle de erro juntamente com o entrelaçamento de símbolos proporcionou melhorias significativas ao sistema proposto. Os resultados dessa simulação mostraram que para uma probabilidade de erro de símbolo de 10^{-2}, há que uma melhoria de desempenho de cerca de 5 dB.

Em decorrência, trabalhos futuros podem ser interessantes nos seguintes tópicos:

- Determinação de outros códigos binários não-lineares para mapear os conjuntos de portadoras, utilizando, por exemplo, algoritmos de busca tipo genético;
- Avaliação do desempenho do sistema com outras técnicas de modulação e demodulação;
- Introduzir diversidade espacial com múltiplas antenas;
- Avaliação do desempenho do sistema utilizando multiportadora com constelações rotacionadas [18].

Apêndice A

Noções de Álgebra Abstrata

Em geral, os códigos de bloco utilizam estruturas polinomiais e aritmétricas de corpos finitos em seus esquemas de codificação e decodificação. Os conceitos básicos de álgebra abstrata, a aritmétrica de corpos finitos e o logaritmo de *Zech* serão apresentados neste apêndice. Para aprofundar estes conceitos é recomendado [16], [8] e [7].

A.1 Grupos, Anéis, Corpos e Espaços Vetoriais

A álgebra de corpo finito possue três estruturas básicas: grupo, anel e corpo.

GRUPO

Um grupo G é um conjunto associado a uma operação binária sobre pares de elementos deste conjunto que satisfaz as seguintes propriedades:

- Fechamento: $c = a \star b$; $\forall$ a, b, c $\in$ G;
- Associatividade: $a \star (b \star c) = (a \star b) \star c$; $\forall$ a, b, c $\in$ G; $\forall$ a, b, c $\in$ G;
- Elemento Neutro: $a \star e = e \star a = a$, em que e é um elemento identidade ou neutro;
- Elemento inverso: $a \star b = b \star a = e$; $\forall a \in$ G, então existe $b \in$ G que é o inverso de a;

Nos grupos finitos o número de elementos é denominado ordem do grupo. Desta forma, a ordem de um elemento sempre divide a ordem do grupo.

Em todo grupo, o elemento neutro é único e a inversa de cada elemento do grupo é única.

ANEL

Um anel $\mathbf{R}$ é um conjunto com duas operações: adição "+" e multiplicação "." que satisfaz as seguintes propriedades:

- Comutatividade em relação a adição, ou seja, é um grupo abeliano;
- Fechamento: $a.b \in \mathbf{R}$; $\forall\ a, b \in \mathbf{R}$;
- Associatividade: $a.(b.c) = (a.b).c$; $\forall a, b, c \in \mathbf{R}$;
- Distributividade: $a.(b+c) = a.b + a.c$ e $(b+c).a = b.a + c.a$, $\forall a, b, c \in \mathbf{R}$;
- A operação multiplicação tem o elemento identidade definido por "1".

CORPO

Um corpo $\mathbf{F}$ é um conjunto que possue duas operações definidas sobre seus elementos, que são: a adição e a multiplicação, satisfazendo as seguintes propriedades:

- $\mathbf{F}$ é um grupo comutativo na operação adição "+";
- $\mathbf{F}$ é fechado sob a multiplicação e $\mathbf{F} - \{0\}$ é um grupo comutativo na operação multiplicação ".";
- Distributividade: $(a+b).c = a.c + b.c$, $\forall a, b, c \in \mathbf{F}$;

Considera-se:

"0" a identidade sob a adição;
"$-a$" a inversa aditiva de a;
"1" a identidade na operação multiplicação;
"a^{-1}" a inversa multiplicativa de a;

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabela A.1: Adição em *GF(3)*.

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Tabela A.2: Multiplicação em *GF(3)*.

A subtração é definida como: $(a-b) = a + (-b)$ e a divisão como: $\left(\frac{a}{b}\right) = b^{-1}.a$.

Geralmente utiliza-se a notação *GF(q)*, em que "q" é o número de elementos do corpo finito que pode ser um número primo ou uma potência de um número primo. As letras G e F referem-se a *Galois Field*, em homenagem ao matemático francês Evariste Galois, que estabeleceu as bases para a teoria dos corpos finitos [15].

Os elementos $\{0, 1, 2, ..., q-1\}$, em que q é um número primo, formando o corpo finito *GF(q)*. Exemplo: Os elementos $\{0, 1, 2\}$ formam o corpo finito *GF(3)* com adição e multiplicação módulo 3:

Espaços Vetoriais

Se **F** um corpo cujos elementos são chamados de escalares e **V** um conjunto de objetos denominados vetores. **V** é dito um espaço vetorial sobre **F** se as seguintes propriedades são satisfeitas:

- **V** é comutativo sob a adição "+";
- Fechamento: $u.v = t \in \mathbf{V}$, $\forall u \in \mathbf{F}$ e $\forall v \in \mathbf{V}$;
- Distributividade: $u.(v+t) = u.v + u.t$ e $(u+v).t = u.t + v.t$;

- Associatividade: $(u.v).t = u.(v.t), \forall u, v, t \in \mathrm{F}$;

O vetor nulo $v = 0$ é a origem do espaço vetorial V.

A.2 Propriedades Elementares de Corpos Finitos

Seja α um elemento em *GF(q)* e "1" o elemento identidade da operação multiplicação. Considerando a sequência de elementos: $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \ldots$; desde que α está em *GF(q)*, todas as sucessivas potências de α devem está também em *GF(q)* dado que a multiplicação é uma operação fechada. Como o *GF(q)* tem somente um número finito de elementos, a sequência começa a repetir valores anteriores da sequência.

A ordem de α, denota por $ord(\alpha)$ é o menor interiro positivo m tal que $3^m = 1$.

O elemento primo em *GF(q)* é o elemento com ordem $(q-1)$ em *GF(q)*.

Um polinômio $f(x)$ é dito irredutível em *GF(q)* se $f(x)$ não pode ser fatorado em um produto de polinômios de menor grau em $GF(q)[x]$. Em que $GF(q)[x]$ é a notação da coleção de todos os polinômios $a_0 + a_1x + a_2x^2 + \ldots + x^n$ de grau arbitrário com coeficientes $\{a_i\}$ em *GF(q)*.

Um irredutível polinômio $p(x) \in GF(q)[x]$ de grau m é dito primitivo se o menor número inteiro positivo n, em que $p(x)$ divide $x^n - 1$ é $n = p^m - 1$.

Seja $p(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0$ um polinômio primitivo de $GF(q)[x]$. Se α é uma raiz de $p(x)$, ou seja, $p(\alpha) = \alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0 = 0$. Assim:

$$\alpha^m = -a_0 - a_1\ x - a_2\ \alpha^2 - \ldots - a_{m-1}\ \alpha^{m-1}.$$

As potências de α de grau maior ou igual a m podem ser expressas por polinômios em α de grau menor ou igual a $(m-1)$. Desde que α tenha ordem $q^m - 1$ as potências distintas de α devem ser $q^m - 1$ distintos polinômios não zeros da forma: $b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{m-1}x^{m-1}$, em que os coeficientes b_i estejam em *GF(q)*. As raízes de um polinômio primitivo de grau m em $GF(q)[x]$ são os elementos primitivos de $GF(q^m)$.

EXEMPLO: Construção de *GF(8)*

Representação Exponencial	Representação Polinômio
α^0	1
α^1	α
α^2	α^2
α^3	$\alpha + 1$
α^4	$\alpha^2 + \alpha$
α^5	$\alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$
α^6	$\alpha^2 + 1$
0	0

Tabela A.3: Representação exponencial e polinomial.

Seja $p(x) = x^3 + x + 1$ o polinômio primitivo em $GF(2)[x]$. Seja α uma raiz de $p(x)$, isto implica que: $\alpha^3 + \alpha^2 + 1 = 0$ ou $\alpha^3 = \alpha + 1$.

A adição de $\alpha^2 + \alpha^5$ é feita substituindo α^2 e α^5 por duas representações polinômiais em α, ou seja: $\alpha^2 + \alpha^5 = (\alpha^2) + (\alpha^2 + \alpha + 1) = (\alpha + 1) = \alpha^3$.

E a operação de multiplicação destes elementos é feita da seguinte maneira:

$$\alpha^2 \, . \, \alpha^5 = \alpha^{(2 \, . \, 5) \; mod(7)} = \alpha^2.$$

Em geral, um corpo finito $GF(q^m)$ construindo usando um polinômio primitivo $p(x)$ têm elemento do corpo finito representado por polinômio na forma: $a_0 + a_1 \, \alpha + ... + a_{m-1} \, \alpha^{m-1}$, em que α é uma raiz de $p(x)$. O elemento da multiplicação pode ser expresso por:

$$(a_0 + a_1 \, \alpha + ... + a_{m-1} \, \alpha^{m-1}) \; (b_0 + b_1 \, \alpha + ... + b_{m-1} \, \alpha^{m-1}) \; \textit{modulo} \; p(x).$$

As representação polinomial e exponencial deste exemplo estão ilustradas na Tabela A.3.

A.3 Logaritmo de *Zech*

Seja α um elemento primitivo de *GF(q)* que é uma raiz do polinômio primitivo $p(x)$ de grau m. Para *GF(q)* considere $N_q = \{0, 1, ..., q-2\} \cup (-\infty)$. Então, o logaritmo de *Zech* $Z(x)$ é definido por:

$$\alpha^{Z(x)} = 1 + \alpha^x, \tag{A.1}$$

em que: Z é o mapeamento $Z : N_q \rightarrow N_q$. Um elemento β é assumido ser dado, nesta representação polar, como uma potência do elemento primitivo α : $\beta = \alpha^1$ (define-se $\alpha^{-\infty} = 0$). Então, a multiplicação é mais fácil, pois consistirá da adição de expoente $mod(q-1)$.

A operação de adição de um elemento α^a com α^b é feita da seguinte maneira:

$$\begin{cases} \alpha^a + \alpha^b = \alpha^{a+Z(b-a)}, & \text{para } a < b \\ \alpha^a + \alpha^b = \alpha^{b+Z(a-b)}, & \text{para } a > b \end{cases}$$

E a operação de multiplicação entre α^a e α^b é:

$$\alpha^a \, . \, \alpha^b = \alpha^{a+b}.$$

A seguir são descritas algumas propriedades do logaritmo de *Zech* [19]:

- $Z(q-1-x) = Z(x) - x \ (mod\ q-1),\ x \neq -\infty$;
- $Z(p\ x) = p\ Z(x) \ (mod\ q-1)$;
- $Z(0) = -\infty$;
- $Z\left(\frac{q-1}{2}\right) = -\infty$, para $p \neq 2$;
- Para todos os primos: $Z(-\infty) = 0$.

O logaritmo de *Zech* torna a implementação dos codificadores/decodificadores BCH e *Reed Solomon* mais simples de serem implementados. A Tabela A.4 ilustra um exemplo da aplicação do logaritmo de *Zech*. A primeira coluna contém os elementos

x	log(x)
α	1
α^2	2
α^3	3
α^4	4
α^5	5
α^6	6
$\alpha^7 = 1$	0
0	∞

Tabela A.4: Logaritmo de *Zech* em *GF(8)*

primitivos de *GF(8)* e a segunda coluna contém os logaritmo que corresponde ao expoente de α.

Bibliografia

[1] C. W. Baum and K. F. Conner. "A multicarrier transmission scheme for wireless local communications". *IEEE J. Selected Areas Communications*, 14:521–529, Apr. 1996.

[2] Essam A. Sourour, and Masao Nakagawa. "Performance of Orthogonal Multicarrier CDMA in a Multipath Fading Channel". *IEEE Transation Communication*, 44:356–367, Dec. 1996.

[3] Qingxim Chen, Elvino S. Souza, and Subbarayan Pasupathy. "Multicarrier CDMA with Adaptive Frequency Hopping for Mobile Radio Systems". *IEEE J. Selected Areas Communications*, 14:1852–1858, Dec. 1996.

[4] Yukitoshi Sanada, and Masao Nakagawa. "A Multiuser Interference Cancellation Technique Utilizing Convolutional Codes and Orthogonal Multicarrier Modulation for Wireless Indoor Communications". *IEEE J. Selected Areas Communications*, 14:1500–1509, Otc. 1996.

[5] Bernard Sklar. *"Digital Communications: Fundamentals and Applications"*. Prentice-Hall Internacional, Inc., 1998.

[6] J. G. Proakis. *"Digital Communicatios"*. Mc Gra-Hill, Inc., 1995.

[7] Richard E. Blahut. *"Theory and Practice of Error Control Codes"*. Addison-Wesley, Inc., 1984.

[8] Stephen B. Wicker. *"Error Control Systems for Digital Communication and Storage"*. Ms Gra-Hill, Inc., 1995.

[9] F. J. MacWilliams, and N. J. A. Sloane. *"The Theory of Error-Correcting Codes"*. North-Holland Publishing Company, 1977.

[10] Bernard Sklar. "Rayleigh fading channel in mobile digital communication systems Part I: Characterization". *IEEE Communication Magazine*, pages 90–100, July 1997.

[11] H. Hashemi. "The indoor radio propagation channel". *Proceedings of the IEEE*, 81:943–968, July 1993.

[12] S. Howard and K. Pahlavan. "Doppler spread mesuarements of the indoor radio channel". *Eletronic Letters*, 26:107–109, Jan. 1990.

[13] R. Ganesh and K. Pahlavan. "Effects of traffic and local movements on multipath characteristics of an indoor radio channel". *IEEE J. Selected Areas Communications*, 26:810–812, June 1990.

[14] Anthony D. Whalen. *"Detection of Signals in Noise"*. Academic Press, Inc., 1971.

[15] Francisco Marcos de Assis. *"Princípios de Transmissão Digital"*. UFPB/Editora Universitária, 1999.

[16] Shu Lin and Daniel J. Costello. *"Error Control Coding: Fundamentals and Applications"*. Prentice-Hall International, Inc., 1983.

[17] W. Wesley Peterson, and E. J. Weldon,Jr. *"Error-Correcting Codes"*. The Mit Press, Inc., 1971.

[18] Francisco M. de Assis and Elvino S. Souza. "Rotated Constellation MC-CDMA System". *Proceedings of the Global Telecommunications Conference - GLOBECOM 99*, pages 996–1000, Dec. 1999.

[19] Klaus Huber. "Some Comments on Zech's Logarithms". *IEEE Trans. on Information Theory*, 36:946–950, July 1990.

[20] Izabel C. O. Dionísio e Francisco M. de Assis. "Simulação de um Sistema Multiportadora para Comunicação Digital em Ambientes Interiores de Baixa Complexidade". *XVIII Simpósio Brasileiro de Telecomunicações - SBrT 2000*, Setembro 2000.

[21] Bernard Sklar. "Rayleigh fading channel in mobile digital communication systems Part II: Mitigation". *IEEE Communication Magazine*, pages 102-108, July 1997.

[22] A. C. Caswell. "Multicarrier Transmission in a mobile radio channel". *Eletronic Letters*, 32:1962-1963, Oct. 1996.

[23] Michel C. Jeruchim, Philip Balaban, and K. Sam Shanmugan. *"Simulation of Communication Systems"*. Plenum Press, Inc., 1992.

[24] J. M. Wozencraft and I. M. Jacobs. *"Principles of Communicatios Engineering"*. John Wiley Sons, Inc., 1965.

[25] R. Ganesh, and K. Pahlavan. "Effects of Traffic and Local Movements on Multipath Characteristic of an Indoor Radio Channel". *Eletronic Letters*, 26:810-812, June 1990.

[26] Victor M. DaSilva, and Elvino S. Sousa. "Multicarrier Orthogonal CDMA Signals for Quasi-Synchronous Communication Systems". *IEEE J. Selected Areas Communications*, 12:842-852, July 1990.

[27] Robert J. C. Bultitude. "Measurement Characterization and Modeling of Indoor 800/900 MHz Radio Channels for Digital Communications". *IEEE Communications Magazine*, 25:5-12, June 1987.

[28] Theodore S. Rappaport. "Indoor Radio Communications for Factories of the Future". *IEEE Communications Magazine*, pages 15-24, May 1989.

[29] Alex Grant. *"Error Control Codes - BCH Codes"*. Disponível na URL http://www.itr.unisa.edu.au/ alex/ECC, 2000.