UNIVERSIDADE ESTADUAL DE CAMPINAS

FACULDADE DE ENGENHARIA ELÉTRICA

DEPARTAMENTO DE COMUNICAÇÕES

SUBCÓDIGOS MULTINÍVEIS DE BLOCO DEFINIDOS A PARTIR DE CÓDIGOS CÍCLICOS SOBRE CAMPOS Z_q

ZELMANN STROBEL PENZE

ORIENTADOR: **PROF.Dr. RENATO BALDINI FILHO**

FEEC
Faculdade de Engenharia Elétrica e de Computação
UNICAMP

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação - FEEC, da Universidade Estadual de Campinas – Unicamp, como parte dos requisitos exigidos para obtenção do título de MESTRE EM ENGENHARIA ELÉTRICA.

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

P389s

Penze, Zelmann Strobel
Subcódigos multiníveis de bloco definidos a partir de códigos cíclicos sobre campos Z_q / Zelmann Strobel Penze.--Campinas, SP: [s.n.], 1999.

Orientador: Renato Baldini Filho
Dissertação (mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Teoria da codificação. 2. Anéis (Álgebra). 3. Teoria dos Grupos. 4. Modulação digital. 5. Comunicações digitais. 6. Códigos de controle de erros. I. Baldini Filho, Renato. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Para

Meus Pais Thomaz Aquino e Nelia

Meus Irmãos Helmann e Rivael

Minha Noiva Sandra

AGRADECIMENTOS

- Ao Professor Doutor Renato Baldini Filho, pela sua orientação eficiente e segura, fator importante na realização deste trabalho.
- Aos Professores da Banca Examinadora : Prof.Dr. Lee Luan Ling (FEEC-UNICAMP) e Prof.Dr. Bartolomeu Ferreira Uchoa Filho (FAPESP/ PÓS- DOUTORADO).
- A CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pelo suporte financeiro através de bolsa de estudo.
- Aos colegas de graduação que contribuíram muito na realização deste trabalho, de modo particular, aos amigos Saulo Roberto Sodré dos Reis, José Carlos da Silva, Jeferson Luiz Benitez e Leandro Paccola Danelon.
- Aos colegas do Departamento de Comunicações, que estiveram sempre presentes, contribuindo com amizade e companheirismo.
- Aos meus pais Thomaz Aquino Penze e Nelia Strobel Penze e meus irmãos Helmann Strobel Penze e Rivael Strobel Penze, a quem dedico todo esse trabalho.
- A José Adilson de Barros e Terezinha Maria de Melo Barros, pessoas a quem tenho muito respeito e admiração.
- A minha noiva Sandra Regina de Melo Barros, pelo amor, carinho e por estar sempre presente dividindo as alegrias e os problemas da vida, mas crescendo e aprendendo juntos.
- Aos meus familiares e amigos que confiaram em mim, na realização deste trabalho.
- Agradeço principalmente a Deus por mais esta caminhada que estou concluindo com sucesso em minha vida.

RESUMO

Nesta tese apresentamos uma técnica de obtenção de subcódigos de bloco multiníveis, sendo neste caso obtidos a partir de uma matriz geradora de códigos cíclicos definidos sobre campo Z_q . No processo de codificação m bits $b=(b_1,b_2,\cdots,b_m)$ de informação originados de uma fonte binária são mapeados em 2^m símbolos de uma modulação q-PSK, onde q é um número primo maior que 2^m. Para esquemas de modulações codificadas 5-PSK, 7-PSK, 11-PSK e 13-PSK apresentaremos algumas tabelas de subcódigos de bloco sobre campos Z_q obtidos a partir de códigos cíclicos. É proposto também um algoritmo de decodificação que se utiliza das características cíclicas dos subcódigos, sendo aqui apresentado um exemplo.

ABSTRACT

This work presents a class of multilevel block subcodes derived from a cyclic code over the field over Z_q. In The encoding process, m information bits $\mathbf{b} = (b_1, b_2, \cdots, b_m)$ originated from a binary source are mapped into one of 2^m symbols of a q-PSK modulation where q is a prime number greater than 2^m. A decoding algorithm which makes use of the cyclic features of the subcodes is also presented.

CONTEÚDO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

a	seqüência de informação
a, a_i	símbolo de informação ou bit de informação
b, b_i	seqüência de bits de fonte binária
C	código cíclico linear
D_E^2	distância Euclidiana quadrática
$D_{E_{\min}}^2$	distância Euclidiana quadrática mínima
$D_{E_{\min}{}^c}^2$	distância Euclidiana quadrática mínima de um esquema codificado
$D_{E_{\min}{}^u}^2$	distância Euclidiana quadrática mínima de um esquema não-codificado
d(.,.)	distância entre dois elementos
e	elemento identidade de um grupo
E_b	energia média de bit de informação
$\frac{E_b}{N_0}$	relação energia média de bit por ruído
F_q	corpo de q elementos
g	ganho de codificação
g_∞	ganho assintótico de codificação
$g(x)$	polinômio gerador
G	matriz geradora

$GF(q)$	corpo de Galois de ordem q
$\mathbf{H}$	matriz de verificação de paridade
$\mathbf{I}_k$	matriz identidade de ordem k
j	unidade imaginária dos números complexos
k	dimensão de um código
LD	linearmente dependente
LI	linearmente independente
m_c	cardinalidade de um sistema codificado
m_u	cardinalidade de um sistema não-codificado
$\mathrm{M}(\cdot)$	mapeamento
M^{T}	transposta de uma matriz M
$n(t)$	vetor ruído
n	comprimento de um código
$\mathbf{P}$	matriz paridade de um código
q	tamanho do alfabeto de modulação
r	seqüência recebida
R, R_n	anel
R_c	taxa de codificação
$R_x(y)$	resto da divisão do polinômio y pelo polinômio x
$s(t)$	seqüência de sinais
t	tempo
$v(x)$	palavra código
$w(a)$	peso do elemento a

$W_E(a)$	peso Euclidiano de a
$\mathbf{x}$	seqüência codificada
Z_q	anel de inteiros módulo-q
Z_q^k, Z_q^n	módulo sobre um anel Z_q
$\oplus$	adição módulo-q
Θ	subtração módulo-q
(n,k)	código de bloco linear de comprimento n e dimensão k
$\langle G,* \rangle$	conjunto G munido de uma operação binária *
$\langle S \rangle$	subespaço vetorial ou submódulo gerado por S
$\partial s(x)$	grau de uma seqüência $s(x)$
AWGN	ruído Gaussiano branco aditivo
BER	taxa de erro de bit
MLD	decodificador por máxima verossimilhança
PSK	Phase Shift Keying (chaveamento por mudança de fase)
SNR	relação sinal ruído

CAPITULO 1

INTRODUÇÃO

1.1-INTRODUÇÃO

Em 1974 Massey mostrou que ganhos significativos no desempenho de sistemas de comunicação digitais poderiam ser obtidos com a realização simultânea das operações de modulação e codificação mas, até 1982, essas operações continuavam sendo realizadas de forma independente, como mostradas na figura 1.1. No sistema de comunicação digital da figura 1.1, o codificador recebe uma seqüência de informação **a**, que depois de codificada resulta na seqüência codificada **x**. O modulador faz o mapeamento dos símbolos da seqüência codificada, nos elementos do espaço de sinais, e associa a cada sinal mapeado uma forma de onda *s(t)*. Assim, a seqüência codificada **x** é mapeada numa seqüência de sinais *s(t)*, que é enviada através do canal. Neste trabalho assumiremos que o canal é Gaussiano com ruído branco aditivo (AWGN). Então, na saída do canal temos uma seqüência de sinais $s'(t)=s(t)+n(t)$, onde $n(t)$ é um vetor ruído introduzido pelo canal, cujas componentes são variáveis com distribuição normal de média zero e variância $\sigma^2 = \frac{N_0}{2}$. O demodulador faz a operação inversa do modulador e envia para o decodificador uma seqüência **x'**, que depois de decodificada resulta na seqüência **a'**. O uso de códigos corretores de erros tem como objetivo corrigir os possíveis erros na seqüência **x'**, causados pelo ruído, e recuperar a seqüência de informação **a**, ou seja, obter **a' = a**.

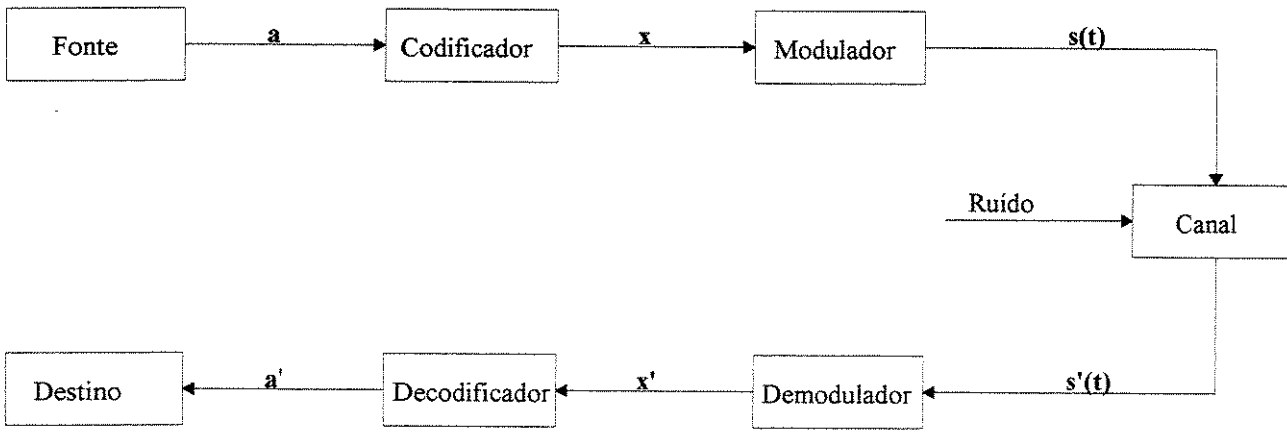

Figura 1.1- Sistema de Comunicação

Podemos melhorar o desempenho de um sistema de comunicação digital, em termos de probabilidade de erro de bits, com a introdução de mais bits de redundância, mas para manter a mesma taxa de transmissão de informação precisamos de um aumento na faixa de passagem. Então, se o sistema é limitado em faixa, podemos optar por uma modulação com número maior de pontos, de modo que os bits extras que forem adicionados possam ser acomodados nos símbolos do novo espaço de sinais. Mas, se o novo sistema tem a mesma distância Euclidiana entre os pontos da modulação, a sua energia média é maior do que a do anterior. Portanto, se o sistema é limitado em faixa e potência, essa solução não pode ser adotada. No entanto, o desempenho de tal sistema ainda pode ser otimizado, tomando uma modulação com um número maior de pontos, mantendo-se a taxa de transmissão de informação e a energia média do sistema. Isso pode ser conseguido combinando-se as operações de modulação e codificação.

Em 1977, no trabalho de Imai e Hirakawa, as operações de modulação e codificação foram feitas simultaneamente, num método de codificação multinível que utilizava vários códigos de bloco binários. Essa técnica de combinar as operações de modulação e

codificação de um sistema de comunicação digital é conhecida por **modulação codificada**. A figura 1.2 mostra um sistema de comunicação digital onde é usada a técnica de modulação codificada. Os blocos que representam a modulação e a codificação são tomados como um só, o mesmo acontecendo com os blocos que representam a demodulação e a decodificação.

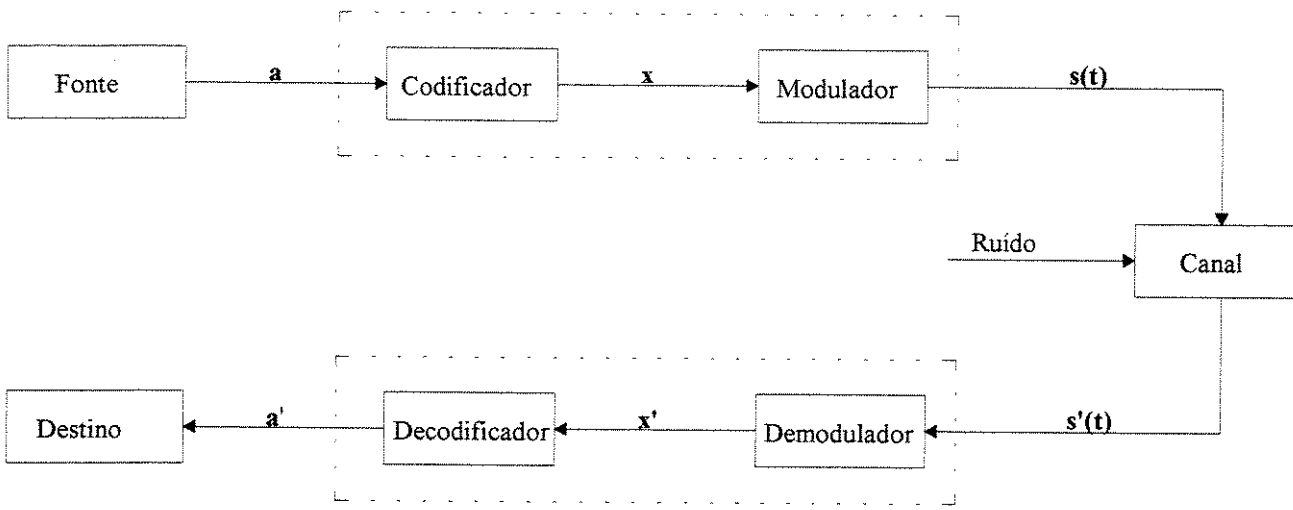

Figura 1.2- Sistema de Modulação Codificada

Foi em 1982 que a técnica de modulação codificada se consolidou, com o célebre trabalho de Ungerboeck, onde ele apresentou uma técnica, conhecida por **mapeamento por partição de conjunto**, mostrando como implementar sistemas de comunicações digitais onde as operações de modulação e codificação são realizadas simultaneamente, de modo que ganhos significativos de codificação poderiam ser obtidos, sem necessidade de diminuição de taxa de transmissão de informação nem expansão da faixa de passagem. O método de particionamento consiste em dividir sucessivamente o conjunto de pontos do

espaço de sinais em subconjuntos com uma distância Euclidiana mínima progressivamente crescente. O trabalho de Ungerboeck despertou o interesse de muitos pesquisadores e contribuiu para o surgimento de vários trabalhos nessa área.

1.2 -ORGANIZAÇÃO DA TESE.

Neste trabalho apresentaremos uma classe de subcódigos de bloco definidos a partir de códigos cíclicos sobre campos de inteiros módulo-q, onde q é um número primo. O conteúdo desta tese está distribuído da seguinte maneira:

No capítulo 2, apresentaremos uma técnica de modulação codificada, onde esquemas de modulações q-PSK são codificados com códigos multiníveis sobre anéis de inteiros Z_q . No processo de codificação, em vez de se usar mapeamento por particionamento de conjuntos, os bits de informação são mapeados diretamente nos símbolos de Z_q e esses símbolos são então codificados. Isso se deve à semelhança da distribuição espacial dos sinais de uma constelação q-PSK com a representação geométrica e as propriedades de um anel Z_q.

Devido às modulações codificadas baseadas em anéis de inteiros módulo-q não possuírem um esquema de decodificação suave simples, pois a entidade algébrica definida como anel não possui inverso multiplicativo e isto não permite definir a operação divisão que é importante ferramenta para o processo de decodificação. Assim, no capítulo 3 apresentaremos um processo de obtenção de subcódigos de bloco multiníveis sobre Z_q, onde q é um número primo, condição necessária para que Z_q possa ser definido como campo.

Apresentamos também a nossa principal contribuição para esta tese, que consiste em demonstrar uma nova classe de subcódigos de bloco multiníveis. Esses subcódigos são obtidos a partir de uma matriz de códigos cíclicos definidos sobre campo Z_q. Tabelas de subcódigos de bloco multiníveis obtidos a partir de códigos cíclicos para taxas 1/2 e 2/3 com suas distâncias Euclidianas mínimas quadráticas e ganhos assintóticos de codificação também são apresentados. Finalizando, um algoritmo sub-ótimo de decodificação que explora as características cíclicas do código multinível, mais rápido e menos complexo em termos de implementação prática que os métodos de decodificação suave por máxima verossimilhança também é mostrado.

CAPITULO 2

MODULAÇÃO CODIFICADA SOBRE ANÉIS DE INTEIROS

2.1- CÓDIGOS DE BLOCO SOBRE ANÉIS DE INTEIROS MÓDULO- q

[Baldini,1992].

2.1.1- INTRODUÇÃO

A idéia principal de esquemas que utilizam modulação codificada é transmitir m bits de informação por símbolo de canal usando um modulador com $q > 2^m$ formas de onda (geralmente $q = 2^{m+1}$) e assim explorar a redundância produzida pelo uso de um conjunto de símbolos de canal conveniente. Este esquema deve estabelecer uma correspondência um para um entre m-uplas binárias e símbolos de um alfabeto q-ário.

Ungerboeck demonstrou em 1982 que é possível relacionar monotonicamente a distância de Hamming originada de uma codificação convolucional binária com a distância Euclidiana entre símbolos de canal, sendo esta relação conhecida como "mapeamento por partição em conjunto", desde então a maioria dos esquemas desenvolvidos foram baseados nesta nova técnica.

Neste capítulo apresentamos um método alternativo de codificação, baseado em anéis de inteiros módulo-q (onde q é um número inteiro não primo) o qual vem a ser conveniente para esquemas de modulação codificada.

2.1.2- CONCEITOS BÁSICOS.

Os códigos multiníveis convenientes para modulação codificada que serão apresentados estão definidos sobre uma entidade algébrica conhecida como "anel". Antes de apresentar o processo de codificação, introduziremos algumas definições algébricas básicas.

✓ **Definição 1** *Um grupo* $\langle G,* \rangle$ *é um conjunto* **G**, *junto com uma operação binária a qual satisfaça as seguintes propriedades:*

1. *O grupo G é fechado sob a operação *.*
2. *A operação binária é associativa.*
3. *Existe um elemento "e" em* **G** *tal que* $(e * x = x * e = x)$, *para todo* $x \in \mathbf{G}$ *(o elemento "e" é um elemento identidade para * sobre* **G** *).*
4. *Para cada a em* **G**, *existe um elemento a' em* **G** *com a propriedade de a' * a = a * a' = e (o elemento a' é um inverso de à com respeito a operação *).*

✓ **Definição 2** *Um grupo* **G** *é abeliano se a sua operação binária for comutativa.*

Em um grupo abeliano, a operação * é comumente substituída por +, não necessariamente indicando a soma ordinária. Neste caso, o inverso de um dado elemento a é denotado por $-a$.

✓ **Definição 3** *Um anel* $\langle R,+,\bullet \rangle$ *é um conjunto* **R** *junto com duas operações binárias + e*

- *(adição e multiplicação) tal que as seguintes propriedades são satisfeitas:*

1- $\langle R,+ \rangle$ *é um grupo abeliano.*

2- *R é fechado sob a operação multiplicação*

3- *A multiplicação é associativa.*

4- *Para todos* $a,b,c \in R$, *valem a lei distributiva à esquerda,* $a(b+c)=(ab)+(ac)$ *e a distributiva à direita* $(a+b)c=(ac)+(bc)$.

Um anel, é chamado comutativo se este é comutativo sob a operação multiplicativa, isto é:

$$\forall x_1, x_2 \in R \Rightarrow x_1 \bullet x_2 = x_2 \bullet x_1$$

Exemplo 2.1- Um anel Z_4 de inteiros módulo- 4 é dado pelo conjunto $\{0,1,2,3\}$, onde as operações adição e multiplicação entre dois elementos deste conjunto são definidas pelas seguintes tabelas:

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

•	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Figura 2.1-Tabela Verdade para o Anel Z_4

É importante notar no exemplo anterior que o anel de inteiros módulo-4 é comutativo. Se um anel de inteiros módulo–q é construído por um número primo de elementos , isto é, q é primo, então este anel é conhecido como campo ou corpo.

✓ **Definição 4** *Um campo é um anel comutativo com o elemento unidade multiplicativo definido e onde todo elemento não nulo é inversível.*

Seja $(M,+)$ um grupo abeliano e seja R um anel. Suponhamos que esteja definida uma operação, que chamaremos de **multiplicação por escalar**, entre os elementos de R e os elementos M tal que a cada par ordenado $(\lambda, v) \in M \times R$ esteja associado um elemento de M, que denotaremos por λv. Em outras palavras, estamos supondo que esteja definida uma função do tipo

$$R \times M \to M$$
$$(\lambda, v) \to \lambda v$$

✓ **Definição 5** *Sob às condições acima, dizemos que M é um módulo sobre R, ou um R-módulo se as propriedades seguintes são satisfeitas para quaisquer $\lambda, \mu \in R$ e $u, v \in M$:*

1. $\lambda(u+v) = \lambda u + \lambda v$
2. $(\lambda + \mu)v = \lambda v + \mu v$
3. $(\lambda\mu)v = \lambda(\mu v)$
4. $1v = v$, *onde* 1 *é o elemento identidade de* R.

✓ **Definição 6** *Um módulo é dito finitamente gerado se ele pode ser gerado por um conjunto finito.*

Se um espaço vetorial pode ser gerado por um conjunto finito, isto é, se o espaço tem dimensões finitas então todo subespaço também tem. Esta propriedade não é válida, em geral, para módulos pois um módulo pode ser finitamente gerado e ter um submódulo que não é.

Em um espaço vetorial, qualquer conjunto formado por um único elemento não nulo é LI. No caso de módulos isso nem sempre é verdade. Por exemplo, consideremos Z_q como um Z-módulo. Neste caso, para qualquer $a \in Z_q$ temos que $q \cdot a = 0$. Logo, $\{a\}$ é LD. Daí concluímos que Z_q, como um Z-módulo, não possui subconjunto LI e, consequentemente, não possui base.

✓ **Definição 7** *Um módulo é dito* ***livre*** *se ele possui uma base.*

Em um espaço vetorial, qualquer duas bases possuem o mesmo número de elementos. Em um módulo livre, se o anel não é comutativo, pode haver bases com cardinalidades diferentes. Mas se R é um anel comutativo com identidade então qualquer duas bases de um R-módulo livre tem mesma cardinalidade. Isto nos permite definir um conceito análogo ao de dimensão de um espaço vetorial.

✓ **Definição 8** *Seja M um R-módulo livre, onde R é comutativo. Definimos o* ***posto*** *de M como sendo a cardinalidade de qualquer base de M.*

Exemplo 2.2- Sejam q e n inteiros positivos e

$$Z_q^n = \{(x_1,\cdots,x_n) \mid x_i \in Z_q, i = 1,\cdots,n\}$$

É fácil notar que Z_q^n é um Z_q-módulo livre de posto de n, pois o conjunto de n-uplas

$$B = \{(1,0,\cdots,0),(0,1,\cdots,0),\cdots,(0,\cdots,0,1)\}$$

é uma base de Z_q^n. De fato,

i. $\mathrm{v} = (x_1,x_2,\cdots,x_n) \in Z_q^n$ então

$$\mathrm{v} = x_1(1,0,\cdots,0) + x_2(0,1,\cdots,0) + \cdots + x_n(0,\cdots,0,1).$$

Logo, B gera Z_q^n.

ii. Se $x_1(1,0,\cdots,0) + x_2(0,1,\cdots,0) + \cdots + x_n(0,\cdots,0,1) = 0$ então $(x_1,x_2,\cdots,x_n) = 0$, ou seja, $x_1 = x_2 = \cdots = x_n = 0$. Então B é LI.

Portanto B é uma base para o Z_q-módulo Z_q^n.

2.1.3 – PROCESSO DE CODIFICAÇÃO.

O esquema de modulação codificada baseado na teoria de Ungerboeck[1982] utiliza basicamente um codificador binário com taxa $m/(m+1)$, onde $(m+1)$ bits de saídas são mapeados em elementos do conjunto de sinais do canal expandido. O esquema proposto, primeiro faz primeiramente um mapeamento das seqüências binárias de informação de comprimento $(m+1)$ no conjunto expandido de 2^{m+1} sinais do canal. Então os símbolos de canal são codificados. Este esquema alternativo de codificação é demonstrado na figura 2.2.

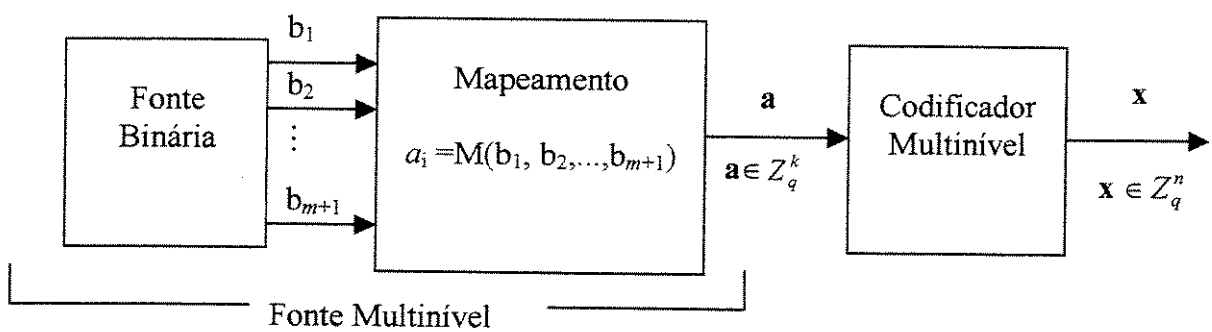

Figura 2.2- Estrutura do Codificador

Os $m+1$ bits de informação paralelos $(b_1,b_2,...,b_{m+1})$, originados da fonte binária, são mapeados (mapeamento de Gray) para um dos $q=2^{m+1}$ símbolos de canais a_i pertencentes ao conjunto Z_q de sinais de uma modulação expandida. O conjunto $Z_q = \{0,1,2,\cdots,q-1\}$ é definido como um anel de inteiros módulo–q porque, em geral, o número de pontos da modulação do conjunto de sinais é igual a uma potência de 2. Na figura 2.2 podemos considerar os dois primeiros blocos como uma única entidade chamada fonte multinível. A entrada do codificador multinível é uma seqüência de informações $\mathbf{a} = (a_1, a_2, \cdots, a_k)$ cujos os elementos pertencem ao anel Z_q. O codificador multinível então envia no canal a seqüência codificada $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ com elementos pertencentes ao

mesmo anel Z_q. É importante notar que o comprimento da seqüência **x** é maior que o comprimento da seqüência de informação, isto é, $n \geq k$.

As constelações de modulação mais adequadas para a codificação multinível de seqüências com elemento pertencentes a um anel de inteiros módulo-q são as que possui seus símbolos distribuídos sobre uma circunferência, isto é, são as modulações denominadas q-PSK.

Os símbolos de uma dada modulação q-PSK são tomados como elementos pertencentes a um anel de inteiros módulo-q porque o anel garante uma distribuição uniforme em termos de distância Euclidiana das n-uplas não pertencentes ao código em torno das palavras-código , em outras palavras, o anel de inteiros módulo–q garante que na construção do arranjo padrão para um dado código (n,k) multinível as distâncias Euclidianas entre duas n-uplas quaisquer pertencentes a um mesmo coset e as correspondentes palavras-código do topo do arranjo padrão possuem exatamente o mesmo valor numérico. Isto não se verifica quando se utiliza um corpo de extensão GF(q), onde $q = 2^{m+1}$, ao invés de um anel de inteiros módulo–q.

A principal vantagem da utilização desse esquema proposto em relação ao proposto por Ungerboeck é a possibilidade de se transmitir frações de bits de informação por intervalo de modulação, sem a necessidade de utilizar uma constelação multidimensional.

2.1.4 – DISTÂNCIA EUCLIDIANA ENTRE SINAIS q-PSK [Massey,1989]

A distância Euclidiana entre dois sinais de uma dada modulação q-PSK é diretamente proporcional ao símbolo correspondente de um anel de inteiros módulo–q, associado a esses sinais de modulação. Na figura 2.3 é demonstrado o esquema geral para a modulação q-PSK. Os sinais de modulação são representados por:

$$S i = \exp(j \frac{2\pi i}{q}),\ i = 0, 1, ..., q\text{-}1 \tag{2.1}$$

onde o elemento correspondente do anel é dado pelo índice de $S i$.

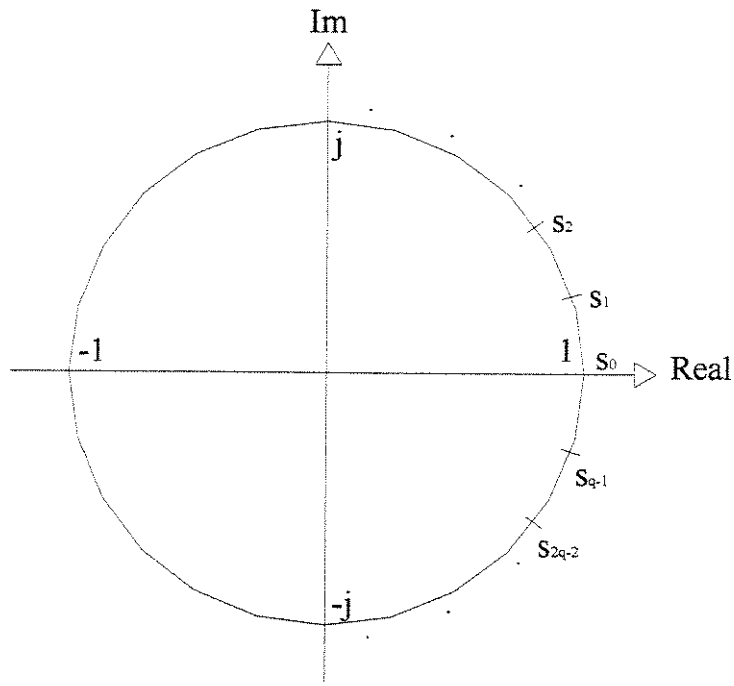

Figura 2.3-Esquema de Modulação q-PSK

A distância Euclidiana quadrática entre dois sinais de modulação S_i e S_r pode ser calculada por:

$$\begin{aligned} D_E^2(s_i, s_r) &= |s_i - s_r|^2 \\ &= \left|\exp\left(\frac{j2\pi i}{q}\right) - \exp\left(\frac{j2\pi r}{q}\right)\right|^2 \\ &= \left|\exp\left(\frac{j2\pi(i-r)}{q}\right) - 1\right|^2 \\ &= \left|\exp\left(\frac{j2\pi(i\Theta r)}{q}\right) - 1\right|^2 \end{aligned} \tag{2.2}$$

onde Θ denota subtração módulo-q.

Pode-se agora definir a distância Euclidiana quadrática entre dois pontos no espaço de sinal pela seguinte expressão:

$$D_E^2(i,r) \triangleq \left|\exp\left(\frac{j2\pi(i\Theta r)}{q}\right)-1\right|^2 \tag{2.3}$$

E o peso Euclidiano quadrático é dado por:

$$W^2(i) \triangleq D_E^2(i,0)=\left|\exp\left(\frac{j2\pi i}{q}\right)-1\right|^2 \tag{2.4}$$

É fácil verificar que a distância Euclidiana quadrática entre dois pontos no espaço de sinais é igual ao peso Euclidiano quadrático no resultado da subtração entre esses dois pontos.

$$D_E^2(i,r)=W_E^2(i\Theta r) \tag{2.5}$$

Para generalizar, a distância Euclidiana quadrática entre n-uplas **x** e **y**, com componentes pertencentes ao anel de inteiros módulo-q, pode ser definida como sendo:

$$D_E^2(x,y) \triangleq \sum_{i=1}^{n}\left|\exp\left(\frac{j2\pi(x_i\Theta y_i)}{q}\right)-1\right|^2 \tag{2.6}$$

2.2 - CÓDIGOS MULTINÍVEIS SOBRE Z_q

Nesta seção apresentaremos um método alternativo de codificação dos sinais de modulação baseado em anéis de inteiros módulo-q (Z_q). Os códigos multiníveis definidos sobre Z_q são lineares e apresentam algumas propriedades importantes que serão aqui discutidas.

2.2.1 – PROCESSO DE CODIFICAÇÃO

O processo alternativo descrito nesta seção realiza primeiro o mapeamento da seqüência binária de informação no conjunto expandido de sinais de canal e em seguida codifica os símbolos de canal para introduzir redundância aumentando-se assim a distância Euclidiana mínima. A figura 2.4 mostra este processo de modulação codificada.

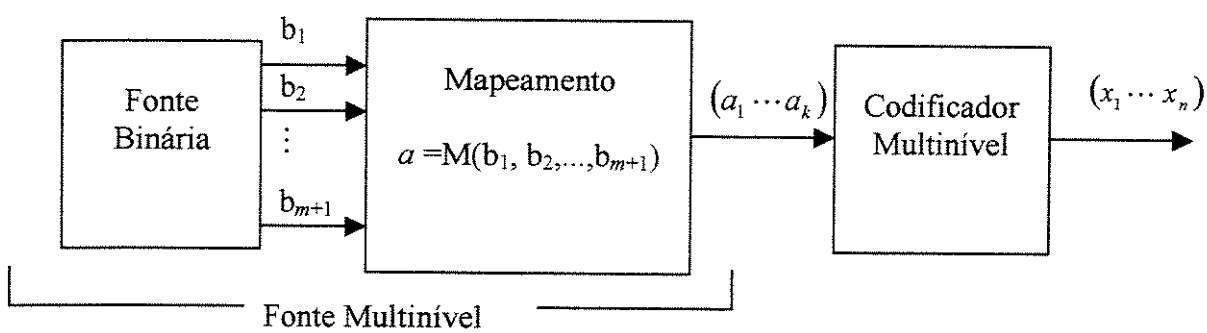

Figura 2.4 -Estrutura do Codificador

A saída paralela da fonte binária é composta por $m+1$ bits de informação $(b_1,\cdots,b_{m+1})$ que são mapeados em um dos $q=2^{m+1}$ símbolos a_i pertencentes ao conjunto Z_q dos sinais de modulação. O conjunto $Z_q=\{0,1,2,\cdots,q-1\}$ é definido como um anel de inteiros módulo-q. A entrada do codificador multinível é composta de uma seqüência $\mathbf{a}=(a_1,\cdots,a_k)$ de k elementos pertencentes ao conjunto Z_q. Esta seqüência **a** é então codificada em uma nova seqüência $\mathbf{x}=(x_1,\cdots,x_n)$ de n elementos também pertencentes a Z_q.

As constelações de modulação mais adequadas é a codificação multinível de seqüências de elementos pertencentes a um anel de inteiros módulo-q são as que possuem seus símbolos distribuídos sobre uma circunferência, isto é, são as modulações denominadas q-PSK.

Os símbolos de uma dada modulação q-PSK são tomados como elementos pertencentes a um anel de inteiros módulo-q porque o anel garante uma distribuição uniforme em termos de distância Euclidiana das n-uplas não pertencentes ao código em torno das palavras-código. Em outras palavras, o anel de inteiros módulo-q garante que na construção do arranjo padrão para um dado código (n,k) multinível as distância Euclidiana entre duas n-uplas quaisquer pertencentes ao mesmo coset e as correspondentes palavras-código do topo do arranjo padrão possui exatamente o mesmo valor numérico.

2.2.2 – GANHO DE CODIFICAÇÃO

O ganho de codificação g é obtido fazendo-se a diferença entre o valor da razão E_b/N_0 (energia de bit por densidade espectral de ruído) em dB do sistema de modulação não-codificada básica e o valor da razão E_b/N_0 de um dado sistema de modulação codificado utilizado para alcançar a mesma taxa de erro de bit (BER), isto é,

$$g = \left.\frac{E_b}{N_0}\right|_{não-codificado} - \left.\frac{E_b}{N_0}\right|_{codificado} \quad [\text{dB}] \qquad (2.7)$$

O ganho de codificação assintótico g_∞ entre sistemas codificados e não-codificados pode ser obtidos pela seguinte expressão:

$$g_\infty = g(E_b/N_0 \longrightarrow \infty) = 10\log_{10}\left\{\frac{\log m_c}{\log m_u} \cdot R_c \cdot \frac{D^2_{E_{\min}c}}{D^2_{E_{\min}u}}\right\} \quad [\text{dB}] \qquad (2.8)$$

onde:

- ✓ m_c e m_u são as cardinalidades dos alfabetos de modulação codificada e não-codificada, respectivamente.
- ✓ $D_{E_{\min}c}$ e $D_{E_{\min}u}$ são as distâncias Euclidianas mínimas para a modulação codificada e não-codificada, respectivamente.
- ✓ R_c é a taxa de codificação para a modulação codificada.

2.2.3 – REPRESENTAÇÃO MATRICIAL DOS CÓDIGOS MULTINÍVEIS

Os códigos multiníveis são códigos de bloco (n,k) definidos a partir de uma matriz geradora **G** de dimensões $k \times n$ com elementos pertencentes ao anel de inteiros módulo-q. O processo de codificação se resume então na seguinte relação:

$$\mathbf{x} = \mathbf{a}.\mathbf{G} \tag{2.9}$$

onde o vetor de saída **x** (palavra-código) e o vetor de entrada **a** (informação) possuem dimensões n e k, respectivamente.

Exemplo 2.2 – Um código com aplicação em modulação codificada utilizando o espaço de sinais da modulação 4-PSK e tendo como referência a modulação 2-PSK não-codificada é dado pela matriz geradora **G** a seguir:

$$\mathbf{G} = \begin{bmatrix} 1 & 3 & 0 & 2 & 3 & 0 & 0 & 0 \\ 0 & 1 & 3 & 0 & 2 & 3 & 0 & 0 \\ 0 & 0 & 1 & 3 & 0 & 2 & 3 & 0 \\ 0 & 0 & 0 & 1 & 3 & 0 & 2 & 3 \end{bmatrix} \tag{2.10}$$

O código definido pela matriz (2.10) é o código (8,4) de taxa de codificação R_c igual 1/2 , de distância Euclidiana mínima ao quadrado igual a 10 e ganho assintótico sobre a modulação não-codificada 2-PSK igual a 3.98 [dB]. A energia média de sinal para a modulação 4-PSK e para a 2-PSK são assumidas idênticas e de valor igual a unidade, isto é, os raios das circunferências onde os sinais das modulações 4-PSK e 2-PSK descansam possuem o valor numérico unitário.

2.2.4–PROPRIEDADES DOS CÓDIGOS SOBRE ANÉIS DE INTEIROS Z_q

Os códigos multiníveis definidos sobre anéis de inteiros módulo-q apresentam algumas propriedades interessantes. Abaixo relacionaremos estas propriedades que podem não só auxiliar na busca de novos códigos mas também ajudar a definir o processo de decodificação.

1) É possível obter a matriz de verificação de paridade **H** a partir da matriz geradora **G**. Tomando o código sobre Z_4 dado no exemplo 2.2, a matriz **G** pode ser transformada para a forma sistemática **G'**, ou seja:

$$\mathbf{G}' = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 2 & 1 & 3 \\ 0 & 0 & 0 & 1 & 3 & 0 & 2 & 3 \end{bmatrix} = [\mathrm{I} \vdots \mathrm{P}] \qquad (2.11)$$

A matriz de verificação de paridade **H** obtida de **G'** fica:

$$\mathbf{H} = \begin{bmatrix} 2 & 3 & 1 & 1 & 1 & 0 & 0 & 0 \\ 3 & 3 & 2 & 0 & 0 & 1 & 0 & 0 \\ 3 & 3 & 3 & 2 & 0 & 0 & 1 & 0 \\ 3 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = [-\mathrm{P}^{\mathrm{T}} \vdots \mathrm{I}] \qquad (2.12)$$

2) O arranjo padrão obtido para um dado código definido sobre anéis de inteiros módulo-q é uniforme em termos das distâncias Euclidianas envolvidas. Em outras palavras, os códigos sobre anéis de inteiros módulo-q possuem as regiões de decisão em torno das palavras-código congruentes.

3) Os códigos sobre anéis de inteiros módulo-q são códigos invariantes em distâncias, isto é, a distribuição de distância Euclidiana de todas as palavras-código em torno de uma dada palavra-código é a mesma qualquer que seja esta palavra-código. Para o código definido pela equação (2.10) a distribuição das palavras-código segundo a distância Euclidiana para qualquer palavra-código de **G** é dada na tabela 2.1.

D_E^2	Número de Palavras-código
10	24
12	44
14	40
16	45
18	40
20	28
22	24
24	10

Tabela 2.1 – Distribuição das palavras-código segundo a distância Euclidiana para qualquer palavra-codigo de **G**.

4) Para códigos sobre anéis de inteiros módulo-q, a seguinte condição é sempre satisfeita:

$$x_i - x_j = x_k - x_l \Rightarrow D_E^2(x_i, x_j) = D_E^2(x_k, x_l) \qquad (2.13)$$

2.3-CONCLUSÃO.

O esquema de codificação de bloco multiníveis sobre anéis de inteiros módulo-q, apesar de apresentar bom ganho de codificação e de ser altamente eficiente em termos de taxa de codificação, apresenta um processo de decodificação complexo. Isto se deve ao fato deste esquema ter como base uma estrutura algébrica que não permite definir a operação divisão, muito útil no processo de decodificação.

Os códigos de bloco multiníveis definidos sobre anel de inteiros módulo-q são uma alternativa ao esquema de codificação proposto por Ungerboeck[1982].

CAPITULO 3

MODULAÇÃO CODIFICADA SOBRE CAMPOS Z_q

3.1-SUBCÓDIGOS DE BLOCO SOBRE CAMPOS Z_q [Baldini,1994]

Esquemas de modulação codificada sobre anéis de inteiros módulo-q apresentam alta flexibilidade de taxa de codificação e também têm como uma característica importante poder ser invariante à rotação de fase.

Os códigos de anéis de inteiros módulo-q, apresentados anteriormente, não possuem um esquema simples de decodificação suave com desempenho próximo daquela obtida com decodificação de máxima verossimilhança. Isso se deve ao fato desses códigos terem por base uma estrutura algébrica que não permite definir a operação divisão, crucial para o processo de decodificação utilizando métodos algébricos. O anel é uma estrutura onde nem todos os elementos que a ele pertencem possuem inverso multiplicativo. Este problema poderia ser facilmente resolvido se os códigos multiníveis fossem definidos sobre campos ao invés de aneis. Neste capítulo será apresentada uma análise de subcódigos de bloco multiníveis sobre Z_q, convenientes para uma modulação codificada q-PSK, onde q é um número primo, condição suficiente e necessária para um anel Z_q ser um corpo.

3.1.1-PROCESSO DE CODIFICAÇÃO

A proposta de modulação codificada q-PSK primeiro mapeia uma seqüência $\mathbf{b} = (b_1, b_2, \cdots, b_m)$ de m bits em um elemento a_i, onde $a_i \in \{0,1,2,\cdots,2^m - 1\}$, e então codifica a seqüência $\mathbf{a} = (a_1, a_2, \cdots, a_k)$ em uma seqüência $\mathbf{x} = (x_1, x_2, \cdots, x_n)$, onde os elementos pertencem ao conjunto expandido de sinais da modulação de tamanho q (q é um número primo maior que 2^m). Ou seja, o codificador de bloco multinível introduz redundância não somente aumentando o comprimento da seqüência de informação **a**, mas também aumentando o alfabeto de canal multinível. Portanto se consegue mapear seqüências m-binárias em símbolos q-PSK, sobrando para serem usados como redundâncias $(q - 2^m)$ símbolos de Z_q. Assim estas redundâncias são utilizadas para aumentar a distância mínima Euclidiana. Na figura 3.1 é mostrada a proposta do esquema de codificação.

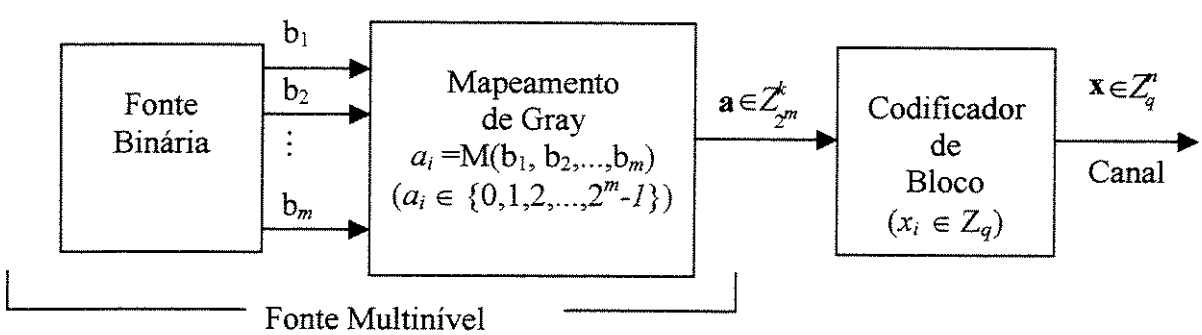

Figura.3.1 Estrutura do Codificador

Um subcódigo de bloco multinível de taxa k/n pode ser representado pela seguinte matriz geradora **G:**

$$\mathbf{G} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1r} & 0 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & g_{11} & g_{12} & \cdots & g_{1r} & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & 0 & g_{11} & g_{12} & \cdots & g_{1r} \end{bmatrix}_{kxn} \tag{3.1}$$

Apesar da estrutura cíclica das linhas da matriz geradora **G**, ela pode não gerar um código cíclico sobre o campo Z_q. Ver seção (3.2) para ocaso em que (3.1) gera um código cíclico.

A taxa do código gerado pela matriz geradora (n, k) é dada pela relação (3.2), o valor do índice r do elemento g_{1r} depende desta taxa.

$$R_C = \frac{\log(2^m)^k}{\log q^n} = \frac{k.\log 2^m}{n.\log q} \tag{3.2}$$

Um codificador multinível então realiza a seguinte operação **x** = **aG**.

O desempenho do esquema de modulação codificada pode ser avaliado através do ganho assintótico que é dado pela expressão(3.3):

$$g_\infty = 10 \cdot \log\left[\frac{\log m_c}{\log m_u} \cdot R_c \cdot \frac{D^2_{E_{\min}c}}{D^2_{E_{\min}u}}\right] \tag{3.3}$$

onde:

- ✓ $D^2_{E_{\min}c}$ e $D^2_{E_{\min}u}$ são distâncias mínimas Euclidianas quadráticas de um sistema codificado e de um não codificado, respectivamente.

✓ m_c e m_u são as cardinalidades dos alfabetos da modulação codificada e não codificada, respectivamente.

✓ R_c é a taxa de codificação.

As tabelas 3.1 e 3.2 mostram subcódigos de bloco multiníveis para a modulação 5-PSK com taxa 0.430 e 7-PSK com taxa 0.356, onde o ganho assintótico é calculado tendo como referência a modulação não codificada 2-PSK.

Tabela.3.1- Subcódigos de bloco multiníveis para modulação codificada 5-PSK($n = 2 \cdot k$)

n	*Matriz Geradora*	$D^2_{E_{\min}}$	g_∞
4	121	6.38	2.67
6	1131	7.76	3.52
8	10243	9.15	4.24
10	120334	10.53	4.85
12	1142411	11.91	5.38
14	11134111	13.29	5.86
16	113314404	14.67	6.28
18	1112414311	15.52	6.53
20	11142241101	16.91	6.90

Tabela 3.2- Subcódigos de bloco multiníveis para modulação codificada 7-PSK($n = 2 \cdot k$)

n	*Matriz Geradora*	$D^2_{E_{\min}}$	g_∞
4	113	5.31	2.70
6	1132	7.75	4.34
8	11223	9.26	5.12
10	112653	10.77	5.77
12	1132221	12.31	6.35
14	12223211	14.30	7.00
16	111245556	15.36	7.31
18	1112455556	17.68	7.92

As tabelas 3.3 e 3.4 mostram subcódigos de multiníveis de taxa 2/3 para modulação 11-PSK com taxa 0.578 e 13-PSK com taxa 0.540, onde o ganho assintótico é calculado tendo como referência a modulação não codificada 4-PSK.

Tabela 3.3- Subcódigos de bloco multiníveis para modulação codificada 11-PSK($n = \frac{3}{2} \cdot k$)

n	*Matriz Geradora*	$D^2_{E_{\min}}$	g_∞
3	12	1.49	-0.67
6	125	3.24	2.70
9	12104	3.61	3.17
12	11231	4.41	4.04

Tabela 3.4-Subcódigos de bloco multiníveis para modulação codificada 13-PSK($n = \frac{3}{2} \cdot k$)

n	*Matriz Geradora*	$D^2_{E_{\min}}$	g_∞
3	13	1.99	0.88
6	136	3.31	3.10
9	1226	4.17	4.11
12	11237	5.99	5.67

Modulação codificada utilizando subcódigos de bloco baseados em campos de inteiros módulo-q e modulação q-PSK apresentam bons ganhos assintóticos de codificação. Este esquema não convencional de modulação codificada tem uma estrutura algébrica que é melhor tratável que a modulação codificada baseada em anéis de inteiros módulo-2^m. Sua estrutura algébrica pode ajudar na implementação prática de algoritmo de decodificação suave, com menor complexidade e bom desempenho.

3.2-SUBCÓDIGOS MULTINÍVEIS DE BLOCO DEFINIDOS A PARTIR DE CÓDIGOS CÍCLICOS SOBRE CAMPOS Z_q

3.2.1-CONCEITOS BÁSICOS SOBRE CÓDIGOS CÍCLICOS.

Os códigos cíclicos formam uma ampla classe de grande importância teórica e prática. Dentre os códigos lineares, pode-se dizer que os códigos cíclicos formam a classe mais importante.

A importância teórica vem do fato de que vários resultados da álgebra abstrata, em particular dos corpos finitos, mostram-se bastante úteis para caracterizar as suas propriedades. Já a importância prática vem do fato de que os circuitos que realizam a codificação e principalmente a decodificação, serem menos complexos e custosos do que aqueles para códigos lineares em geral. Entretanto, os códigos cíclicos não apresentam, na maioria das vezes, propriedades ótimas com relação à distância Euclidiana mínima e taxa, isto é, grandes distâncias mínimas são obtidas ao custo de "baixas" taxas.

3.2.1.1-DEFINIÇÕES E PROPRIEDADES BÁSICAS.

- ✓ **Definição 1**-*Um código linear C sobre GF(q) de comprimento n é* ***cíclico*** *se quando* $\mathbf{v} = (v_0, v_1, \cdots, v_{n-2}, v_{n-1}) \in C$, *então um vetor obtido pelo deslocamento cíclico de seus elementos* $\mathbf{v}^{(1)} = (v_{n-1}, v_0, v_1, \cdots, v_{n-2})$ *também pertence a C, isto é,*

um deslocamento cíclico de uma palavra-código em C resulta em uma outra palavra-código pertencente a C.

Os códigos cíclicos são geralmente descritos na forma polinomial, isto é, a cada palavra $V = (v_0, v_1, \cdots, v_{n-2}, v_{n-1}) \in C$, corresponde um único polinômio código especificado por :

$$v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1} \tag{3.4}$$

isto é, um polinômio de grau $\leq n-1$ com coeficientes em GF(q).

Note primeiramente que a palavra $\mathbf{v}^{(1)} = (v_{n-1}, v_0, v_1, \cdots, v_{n-2}) \in C$ (que representa o deslocamento cíclico de $\mathbf{v} = (v_0, v_1, \cdots, v_{n-2}, v_{n-1})$), corresponde ao polinômio:

$$v^{(1)}(x) = v_{n-1} + v_0 x + \cdots + v_{n-2} x^{n-1} \tag{3.5}$$

que é justamente o polinômio $R_{x^n-1}(xv(x))$, isto é, o resto da divisão de $xv(x)$ por $x^n - 1$.

Note também que o conjunto de todas as palavras pertencentes a um código cíclico C formam um subconjunto do anel $R_n = F_q/(x^n - 1)$, isto é, do conjunto de todos os polinômios cujo grau é menor do que n. O teorema a seguir garante que C não é apenas um subconjunto de R_n, mais um ideal em R_n. Um ideal I de um anel R_n comutativo é o conjunto dos elementos em R_n que satisfaça as duas seguintes condições:

(i) *Se $a \in I$, então $a \cdot b \in I$, para todo $b \in R_n$.*

(ii) *Se a e $b \in I$, então $a+b$ e $a-b \in I$.*

A soma de dois polinômios em C e o produto módulo $x^n - 1$ de um polinômio em R_n por um polinômio código resulta também em um polinômio código. Estas propriedades refletem a linearidade e a "ciclicidade" de C. Temos então:

Teorema 1-*Um subconjunto* C *de* $R_n = F_q[x]/(x^n - 1)$ *é um código cíclico se, e somente se, ele satisfaz a seguintes propriedades:*

1- C *é um subgrupo de* R_n *sob adição;*

2- *Se* $v(x) \in C$ *e* $a(x) \in R_n$, *então* $R_{x^n-1}(a(x)v(x)) \in C$.

Na linguagem da álgebra abstrata, C *é um código cíclico se e somente se,* C *é um ideal em* R_n.

Prova: Primeiramente suponha que o subconjunto C satisfaça as duas propriedades. Então, C é fechado sob a operação adição e também sob multiplicação por uma constante $c \in F_q$. Mais ainda, $R_{x^n-1}(xv(x)) \in C$ sempre quando $v(x) \in C$,isto é, se $v(x) \in C$, então $v(x)^{(1)} \in C$. Estas propriedades caracterizam C como sendo código cíclico.

Agora suponha que C seja um código cíclico. Como C é linear, então a propriedade 1 está satisfeita. Se $w(x) = w_0 + w_1 x + \cdots + w_{n-1}x^{n-1} \in R_n$ e $v(x) \in C$, então $w(x)v(x) = w_0 v(x) + w_1 xv(x) + w_2 x^2 v(x) + \cdots + w_{n-1}x^{n-1}v(x)$. Portanto:

$$R_{x^n-1}(w(x)v(x)) = R_{x^n-1}(w_0 v(x)) + R_{x^n-1}(w_1 xv(x)) + \cdots + R_{x^n-1}(w_{n-1}x^{n-1}v(x))$$

$$= \sum_{i=0}^{n-1} w_i R_{x^n-1}(x^i v(x))$$

isto é, $R_{x^n-1}(w(x)v(x))$ é uma combinação linear do polinômio $v(x)$ e seus deslocamentos cíclicos e, portanto é um polinômio em C. Assim a propriedade 2 também está satisfeita.

Considere novamente que C seja um código cíclico sobre F_q. Dentre todos os polinômios código em C, considere um cujo o grau seja o mínimo possível. Se necessário multiplique o seu coeficiente líder por uma constante em F_q de tal forma a torná-lo mônico (note que esta operação ainda resulta em um polinômio que esta em C). Denote o polinômio obtido por *g(x)*. Este polinômio deve ser único. Pois se admitirmos a existência de um outro polinômio mônico *h(x)* (também de grau mínimo em C), então a diferença $d(x) = g(x) - h(x)$ seria um polinômio código de grau menor que o de *g(x)* e *h(x)*, o que contradiz a nossa hipótese. O polinômio *g(x)* é conhecido como polinômio gerador de C. Se o comprimento de C for n, então denota-se o grau de *g(x)* por $n-k$.

C.Q.D.

Teorema 2-*Um código cíclico C de comprimento n e cujo o polinômio gerador g(x) tem grau* $\partial g = n-k$, *consiste de todos os múltiplos de g(x) por polinômios de grau* $k-1$ *ou menos.*

Prova: Pelo teorema 1, se multiplicarmos *g(x)* (que pertence a C) por qualquer polinômio de grau $k-1$ ou menos, obteremos também um polinômio em C. Por outro lado, suponha que *v(x)* seja um polinômio código em C. Então, dividindo *v(x)* por *g(x)*, obtemos:

$$v(x) = Q(x)g(x) + s(x) \tag{3.6}$$

com $\partial s < \partial g$. Assim,

$$s(x) = v(x) - Q(x)g(x) \tag{3.7}$$

é um polinômio em C de grau menor que o grau de *g(x)* . Isto é uma contradição (já que o grau de *g(x)* foi suposto ser mínimo) , a menos que $s(x) \equiv 0$. Assim, $v(x) = Q(x)g(x)$ e como $\partial Q \leq k-1$, o teorema está provado.

C.Q.D.

Teorema 3 *Se C for um código cíclico de comprimento n e com polinômio gerador g(x), então g(x) divide* $x^n - 1$. *Por outro lado, se um polinômio g(x), tal que* $\partial g \leq n-1$, *divide* $x^n - 1$, *então g(x) é o polinômio gerador de um código cíclico de comprimento n.*

Prova: Suponha que C seja um código cíclico de comprimento *n* e que *g(x)* seja o seu polinômio gerador . Então, dividindo $x^n - 1$ por *g(x)*, obtemos:

$$x^n - 1 = Q(x)g(x) + s(x) \tag{3.8}$$

onde $\partial s < \partial g$. Disso segue que:

$$0 = R_{x^n-1}(x^n - 1) = R_{x^n-1}(Q(x)g(x)) + R_{x^n-1}(s(x)) \tag{3.9}$$

Temos então:

$$s(x) = -R_{x^n-1}(Q(x)g(x)) \tag{3.10}$$

e, assim , *s(x)* é também um polinômio código. Como $\partial s < \partial g$, isto só é possível se $s(x) \equiv 0$ e a conclusão é então que *g(x) divide* $x^n - 1$.

Por outro lado, suponha que um polinômio $g(x) \in F_q/(x^n-1)$ divida x^n-1. Devemos provar que *g(x)* tem grau mínimo em $\langle g(x) \rangle$, isto é, ele é o gerador de um código cíclico . Suponha por absurdo que exista um polinômio $b(x) \in \langle g(x) \rangle$ tal que $\partial b < \partial g$.

Então:

$$a(x)g(x) = d(x)(x^n-1)+b(x) \tag{3.11}$$

para algum $a(x), d(x) \in F_{q_i}[x]$. Isto é, *b(x)* deve ser o resto da divisão de um múltiplo de *g(x)* por x^n-1. Agora em $F_q[x]$, como *g(x)* divide $(d(x)(x^n-1)+b(x))$ e *g(x)* divide x^n-1, então *g(x)* divide $b(x)$, o que é contradição, já que $\partial b < \partial g$. Portanto, em $\langle g(x) \rangle$, *g(x)* é o polinômio de menor grau e é o gerador de um código cíclico.

C.Q.D

O teorema 3 de fato nos fornece um método de construção de códigos cíclicos. Mais ainda, ele implica na determinação de todos os códigos cíclicos de comprimento *n*. Portanto o método sistemático de se procurar todos os códigos cíclicos de comprimento *n* sobre F_q é através da fatoração de x^n-1 (sobre F_q).

✓ **Definição 2**-*Um comprimento de bloco n da forma* $n = q^m - 1$, *onde q é uma potência de primo é denominado* ***comprimento de bloco primitivo*** *para um código sobre* F_q . *Um código cíclico sobre* F_q *de comprimento de bloco primitivo é denominado um* ***código cíclico primitivo.***

Portanto, códigos cíclicos primitivos sobre *GF(q)* podem ser encontrados através da fatoração de $x^{q^m-1}-1$ sobre *GF(q)*. Sabemos que :

$$x^{q^m-1}-1=(x-\beta)(x-\beta^2)\cdots(x-\beta^{q^m-1}) \qquad (3.12)$$

onde β é um elemento primitivo de $GF(q^m)$.

3.2.1.2-DESCRIÇÃO MATRICIAL DE CÓDIGOS CÍCLICOS

Nesta seção abordaremos a questão da determinação das matrizes geradora e verificação de paridade dos códigos cíclicos. Simultaneamente, estaremos apresentando também a matriz geradora do código dual. Iremos provar um teorema auxiliar antes de construirmos essas matrizes.

Teorema 4-*Seja C um código cíclico sobre GF(q) gerado por g(x) tal que* $\partial g = n-k$. *Então os polinômios código* $g(x), xg(x), x^2g(x), \cdots x^{k-1}g(x)$ *são linearmente independentes e geram C.*

Prova: Se tais vetores não fossem LI, então existiriam elementos $a_i \in GF(q)$, $1 \le i \le k-1$, não todos nulos, tais que:

$$a_0g(x)+a_1xg(x)+\cdots+a_{k-1}x^{k-1}g(x)=(a_0+a_1x+\cdots+a_kx^{k-1})g(x)=0 \qquad (3.13)$$

Como o grau deste produto é menor do que n, esta ultima igualdade só se verifica se $a_0=a_1=\cdots a_{k-1}=0$.

Agora do teorema 2, sabemos que $\forall v(x) \in C, v(x)=c(x)g(x)$, onde $\partial c \le k-1$. Assim,

$$c(x)g(x)=(c_0+c_1x+\cdots+c_kx^{k-1})g(x)=c_0g(x)+c_1xg(x)+\cdots+c_{k-1}x^{k-1}g(x) \qquad (3.14)$$

isto é, qualquer polinômio código é uma combinação linear daqueles polinômios.

C.Q.D

Deste teorema, podemos concluir que se C for um código cíclico gerado por $g(x)$, onde $\partial g = n-k$, então C tem dimensão k e uma matriz geradora para C é:

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & 1 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{n-k-2} & g_{n-k-1} & 1 & \cdots & 0 \\ & & & \cdots & & & & & \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & g_2 & & 1 \end{bmatrix} \tag{3.15}$$

Trataremos agora da questão da determinação da matriz verificação de paridade. Sabemos que o polinômio gerador $g(x)$ de um código cíclico divide $x^n - 1$, isto é,

$$x^n - 1 = g(x)h(x), \tag{3.16}$$

onde $\partial h = k$ e $h(x)$ tem a forma:

$$h(x) = h_0 + h_1 x + \cdots + h_k x^k \tag{3.17}$$

com $h_k = 1$ e $h_0 \neq 0$. Iremos então mostrar que uma matriz verificação de paridade para C pode ser obtida a partir de $h(x)$. Seja $v(x)$ um polinômio código em C. Então $v(x) = a(x)g(x)$. Multiplicando $v(x)$ por $h(x)$, obtemos:

$$v(x)h(x) = a(x)g(x)h(x) = a(x)(x^n - 1) = x^n a(x) - a(x) \tag{3.18}$$

Como $\partial a \leq k-1$, então as potências $x^k, x^{k+1}, \cdots, x^{n-1}$ não aparece em $a(x)x^n - a(x)$. Portanto, na expansão de $v(x)h(x)$, os coeficientes de $x^k, x^{k+1}, \cdots, x^{n-1}$ devem ser iguais a zero. A partir disso, obtemos as seguintes n-k equações:

$$\sum_{i=0}^{k} h_i v_{n-i-j} = 0 \tag{3.19}$$

para $1 \le j \le n-k$. Agora, considerando o polinômio recíproco de *h(x)*, isto é, $h^*(x) = x^k h(x^{-1}) = h_k + h_{k-1}x + \cdots + h_0 x^k$, não é difícil verificar que $h^*(x)$ é também um fator de $x^n - 1$ e, portanto, gera um código cíclico $(n, n-k)$, o qual possui a seguinte matriz geradora:

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_2 & h_1 & h_0 & \cdots & 0 \\ & & & \cdots & & & & & 0 \\ 0 & 0 & 0 & \cdots & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \end{bmatrix} \qquad (3.20)$$

Qualquer palavra $\mathbf{v} \in C$ é ortogonal a toda linha de *H*. Portanto, *H* é uma matriz de verificação de paridade para o código cíclico *C* e o espaço linha de *H* é o código dual de *C*.

3.2.2-PROCESSO DE CODIFICAÇÃO

No processo de codificação para esquemas de modulação codificada sobre campo Z_q de inteiros módulo-*q*, os *m* bits $\mathbf{b} = (b_1, b_2, \cdots, b_m)$ originados da fonte binária são mapeados em 2^m símbolos de uma modulação *q*-PSK, onde *q* é um número primo maior que 2^m. Em seguida, uma seqüência de símbolos $\mathbf{a} = (a_1, a_2, \cdots, a_k)$ entra num codificador de bloco cíclico multinível produzindo uma seqüência $\mathbf{x} = (x_1, x_2, \cdots, x_n)$, onde x_i é um símbolo da modulação *q*-PSK escolhida e $n > k$. Note que $x_i \in Z_q$ enquanto que $a_i \in \{0,1,2,3,\cdots,2^m - 1\}$, portanto se consegue mapear seqüências de *m* bits em símbolos *q*-PSK , sobrando para serem usados como redundâncias $(q - 2^m)$ símbolos de Z_q.

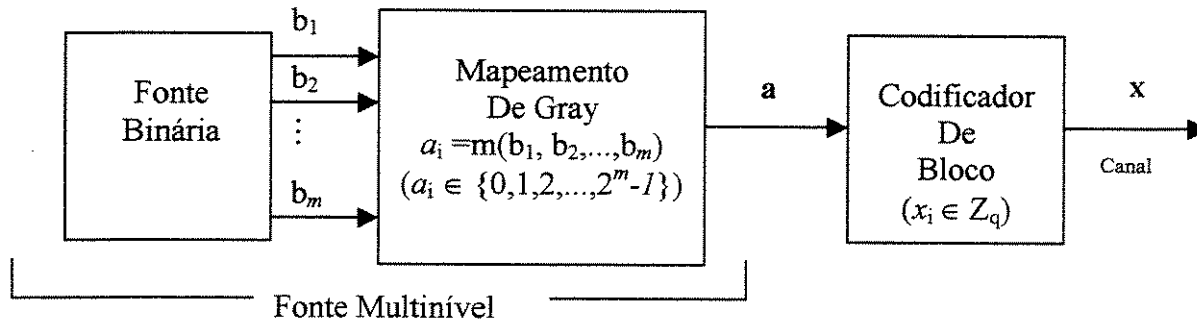

Figura 3.2-Estrutura do Codificador

Como exemplo apresentamos na figura 3.3 a modulação 5-PSK, mostrando também o mapeamento de Gray dos dibits para os símbolos de Z_5 .

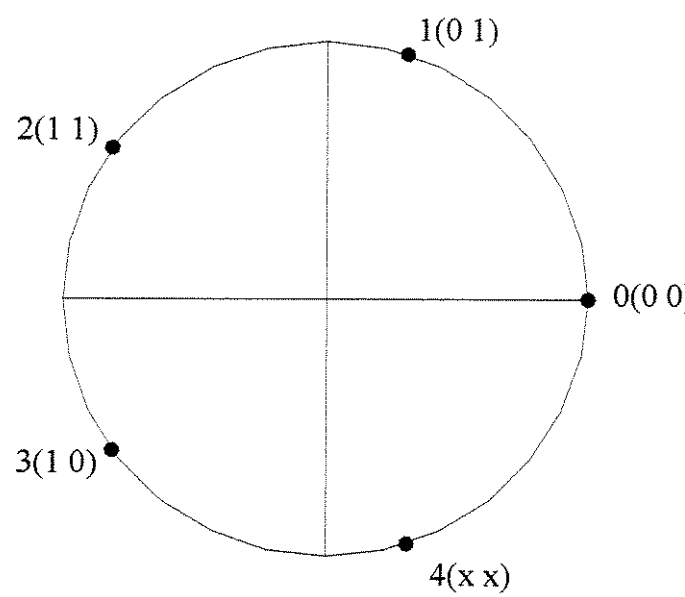

Figura 3.3-Modulação 5-PSK

É importante notar que ao símbolo 4 não é associado nenhum bit, sendo este utilizado apenas para redundância. Podemos verificar também que a fonte multinível,

representada pela fonte binária e pelo mapeador de Gray na figura 3.2, gera símbolos de um conjunto pertencente a Z_4, enquanto que a saída do codificador é um conjunto de símbolos pertencentes a Z_5.

Apresentamos na figura 3.4 abaixo os esquemas de modulações 5-PSK, 7-PSK, 11-PSK e 13-PSK com os seus respectivos mapeamentos de Gray dos símbolos.

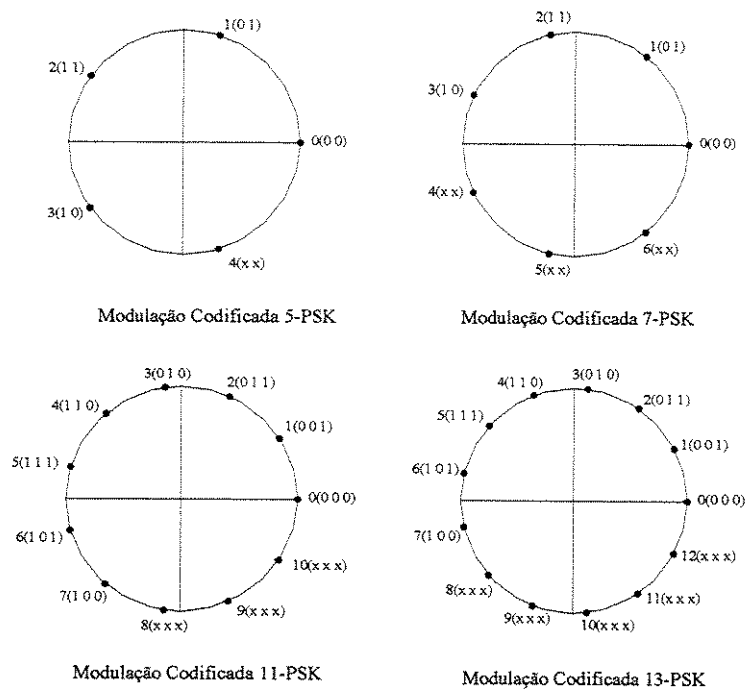

Figura 3.4-Esquemas de Modulações

Para obtermos a matriz geradora do código cíclico (n,k) sobre Z_q temos que fatorar o polinômio $x^n - 1$ sobre Z_q. Um método sistemático de se procurar todos os códigos cíclicos de comprimento n sobre Z_q é através da fatoração de $x^n - 1$ (sobre Z_q) que nos fornece:

$$x^n - 1 = f_1(x) f_2(x) \cdots f_s(x) \tag{3.21}$$

onde $f_i(x)$ são polinômios minimais de cada elemento α de Z_q, os quais serão combinados de acordo com a taxa do código. A matriz geradora do código cíclico sobre Z_q é obtida através de produtos destes polinômios. A estrutura da matriz geradora de um código cíclico sobre Z_q é dada por:

$$\mathbf{G} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1r} & 0 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & g_{11} & g_{12} & \cdots & g_{1r} & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & 0 & g_{11} & g_{12} & \cdots & g_{1r} \end{bmatrix} \tag{3.22}$$

A taxa do código cíclico (n,k) é dada pela relação k/n (número de linhas / número de colunas da matriz geradora). O valor do índice r do elemento g_{1r} depende desta taxa. Porém a taxa do subcódigo obtido a partir do código cíclico sobre Z_q é dada pela expressão (3.2). Um codificador multinível então realiza a operação $\mathbf{x} = \mathbf{aG}$.

Enquanto a codificação tradicional tenta maximizar a distância de Hamming entre seqüências binárias, o processo de codificação utilizando modulação codificada tenta maximizar a distância entre as seqüências de canal, por isso é interessante utilizar uma métrica baseada em distância Euclidiana ao invés de distância de Hamming.

O desempenho do esquema de modulação codificada pode ser avaliado através do ganho assintótico que é dado pela expressão (3.3).

As tabelas 3.5 e 3.6 mostram subcódigos de bloco obtidos a partir de códigos de bloco cíclicos multiníveis de taxa 1/2 para as modulações 5-PSK e 7-PSK. Note que a taxa do subcódigo utilizado na modulação 5-PSK é igual $\frac{1}{2} \cdot \frac{\log 4}{\log 5} = 0.430$, enquanto que para a

modulação 7-PSK é igual a $\frac{1}{2}\cdot\frac{\log 4}{\log 7} = 0.356$. O ganho assintótico é calculado sobre a modulação 2-PSK não codificada.

Tabela 3.5- Subcódigos de bloco multiníveis para modulação codificada 5-PSK a partir de códigos cíclicos.

n	*Matriz Geradora*	$D^2_{E_{min}}$	$g\infty$
4	143	5.527864	2.053161
6	1324	5.527864	2.053161
8	13414	7.763932	3.528404
10	113311	10.000000	4.627587
12	1133143	11.381965	5.389760
14	13232324	5.527864	2.053161
16	134124232	10.000000	4.627587
18	1220330221	8.291796	3.814073
20	14101032031	13.291795	5.863423

Tabela 3.6- Subcódigos de bloco multiníveis para modulação codificada 7-PSK a partir de códigos cíclicos.

n	*Matriz Geradora*	$D^2_{E_{min}}$	$g\infty$
4	143	3.951083	1.419234
6	1456	6.396125	3.512426
8	11411	6.814019	3.786107
10	122221	8.655186	4.824837
12	1113431	10.579121	5.696569
14	14152636	10.161226	5.521535
16	125624406	12.420287	6.393389
18	1251340524	13.359288	6.709906
20	12222055556	13.628038	6.796407

As tabelas 3.7 e 3.8 mostram subcódigos de bloco obtidos a partir de códigos de bloco cíclicos multiníveis de taxa 2/3 para modulação 11-PSK e 13-PSK. Os subcódigos utilizados na modulação 11-PSK possuem taxa igual a $\frac{2}{3}\cdot\frac{\log 8}{\log 11}=0.578$, enquanto que para a modulação 13-PSK igual a $\frac{2}{3}\cdot\frac{\log 8}{\log 13}=0.540$, onde o ganho assintótico é calculado tendo como referência a modulação não codificada 4-PSK.

Tabela 3.7- Subcódigos de bloco multiníveis para modulação codificada 11-PSK a partir de códigos cíclicos.

n	*Matriz Geradora*	$D^2_{E_{min}}$	$g\infty$
3	110	0.634986	-4.363824
6	111	0.952479	-2.602912
9	18310	1.904958	0.4073879
12	11511	3.608312	3.1815759

Tabela 3.8-Subcódigos de bloco multiníveis para modulação codificada 13-PSK a partir de códigos cíclicos.

n	*Matriz Geradora*	$D^2_{E_{min}}$	$g\infty$
3	140	1.956829	0.8165497
6	1210	2.185917	1.2973577
9	14112	2.238398	1.4003937
12	124118	3.049788	2.7437167

3.2.3 - PROCESSO DE DECODIFICAÇÃO

O receptor ótimo (de Máxima Verossimilhança (MLD)) realiza um processo de decodificação suave que, a partir da seqüência recebida, produz a melhor estimação para a seqüência de informação transmitida. Embora seja altamente eficiente, este receptor consome muito tempo e possui alta complexidade de implementação prática, quando o comprimento e/ou alfabeto do código de bloco é aumentado. Devido às características cíclicas do código multinível, o algoritmo de decodificação aqui proposto é mais rápido e menos complexo em termos de implementação prática que o decodificador MLD.

3.2.3.1 – PROPOSTA DE DECODIFICAÇÃO POR DECISÃO SUAVE

O algoritmo proposto para efetuar a decodificação da seqüência recebida é dividido em duas partes. Na primeira parte é feita uma decisão abrupta nos símbolos da seqüência recebida $r = (r_1, r_2, \cdots, r_n)$, produzindo assim a seqüência $\mathbf{S} = (S_1, S_2, \cdots, S_n)$. Através da divisão desta seqüência **S** pelo polinômio gerador do código ***g(x)*** , verifica-se se **S** é uma palavra-código. Se o resto da divisão for igual a zero, **S** é uma palavra-código e o algoritmo passa a decodificar a próxima seqüência recebida. Se o resto for diferente de zero, a segunda parte do algoritmo é então utilizada.

Na segunda parte do algoritmo tenta-se encontrar a palavra-código que está mais próxima da seqüência recebida . O processo pelo qual a decisão suave é feita pode ser descrito pelas seguintes etapas:

1. Quando a decisão abrupta falha na determinação da palavra-código correta, o algoritmo calcula a distância Euclidiana entre cada símbolo recebido e cada ponto do conjunto de modulação, produzindo assim a matriz $\mathbf{D_E}$ de distância Euclidiana:

$$\mathbf{D_E} = \begin{bmatrix} d_{0,1} & d_{0,2} & \cdots & d_{0,n} \\ d_{1,1} & d_{1,2} & \cdots & d_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{q-1,1} & d_{q-1,2} & \cdots & d_{q-1,n} \end{bmatrix} \tag{3.23}$$

O índice i dos elementos $d_{i,j}$ representa o ponto no conjunto de modulação, tomado para calcular a distância Euclidiana, e j a posição do símbolo recebido na seqüência r.

2. Após obter as distâncias Euclidianas mínimas $d_{\min j}(j = 1,2,\cdots,n)$ de cada coluna da matriz $\mathbf{D_E}$, o algoritmo subtrai de cada elemento da coluna j a distância mínima Euclidiana $d_{\min j}$, produzindo assim a matriz **DIF** das diferenças:

$$\mathbf{DIF} = \begin{bmatrix} d_{0,1} - d_{\min 1} & d_{0,2} - d_{\min 2} & \cdots & d_{0,n} - d_{\min n} \\ d_{1,1} - d_{\min 1} & d_{1,2} - d_{\min 2} & \cdots & d_{1,n} - d_{\min n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{q-1,1} - d_{\min 1} & d_{q-1,2} - d_{\min 2} & \cdots & d_{q-1,n} - d_{\min n} \end{bmatrix}$$

$$= \begin{bmatrix} dif_{0,1} & dif_{0,2} & \cdots & dif_{0,n} \\ dif_{1,1} & dif_{1,2} & \cdots & dif_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ dif_{q-1,1} & dif_{q-1,2} & \cdots & dif_{q-1,n} \end{bmatrix} \tag{3.24}$$

Note que cada coluna da matriz **DIF** possui um elemento $dif_{i,j}$ igual a zero. O índice i dessas n entidades $dif_{i,j}$ iguais a zero da matriz **DIF**, produz a seqüência **S**, obtida pela decisão abrupta.

3. Os elementos $dif_{i,j}$, exceto os elementos $dif_{i,j}$ iguais a zero da matriz DIF , são ordenados da mínima para a máxima distância obtida. O símbolo S_j da decisão abrupta é considerado o menos confiável se o valor mínimo encontrado é $dif_{i,j}$, para algum $i \in \{0,1,\cdots,q-1\}$.

4. Então o símbolo S_j, considerado o menos confiável, é mudado para o valor dado pelo índice i da mínima dif_{ij}. A nova seqüência $\overline{\mathbf{S}}$ é testada através da utilização do polinômio gerador do código ***g(x)***. Se $\overline{\mathbf{S}}$ é uma palavra-código é então decodificada e o algoritmo passa para a próxima seqüência recebida. Senão, a seqüência **S** é então restaurada e o segundo símbolo menos confiável é modificado para o índice i da segunda dif_{ij} mínima. Obtida a nova seqüência $\overline{\mathbf{S}}$, esta é novamente testada utilizando o polinômio gerador do código ***g(x)***, sendo decodificada se for palavra-código e senão, **S** é novamente restaurada. A próxima mudança na seqüência **S** pode ser feita no terceiro símbolo menos confiável ou na combinação dos dois primeiros símbolos menos confiáveis. A escolha que irá mudar **S** é a que produz uma distância cumulativa mínima. O processo de decodificação descrito acima então se repete. Este processo prosseguirá, sempre tomando a combinação que fornece a distância cumulativa mínima. Quando a palavra-código é encontrada ele é então enviada para a saída e o processo toma uma nova seqüência codificada .

Exemplo 3.1- Suponha um esquema que utiliza uma modulação 5-PSK e um subcódigo de bloco multinível com taxa 2/4 obtido a partir do código cíclico dado pelo polinômio gerador :

$$g(x) = x^2 + 4x + 3 . \tag{3.25}$$

Sua matriz geradora na forma sistemática é dada por:

$$\begin{bmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 4 & 3 \end{bmatrix}, \tag{3.26}$$

onde os elementos pertencem ao campo Z_5. Supor ainda que a seqüência r recebida é dada pelos seguintes pares (x,y) de coordenadas cartesianas.

$$r = \big((1.00;0.39),(1.50;-0.94),(1.10;-0.02),(0.92;1.50)\big) \tag{3.27}$$

A seqüência **S** obtida por decisão abrupta, calculada a partir da seqüência r é :

$$\mathbf{S} = (0,0,0,1) \tag{3.28}$$

A seqüência **S** não é palavra-código pois o resto da divisão $S(x)/g(x) = 1 \neq 0$. Pode-se testar, antes de ir para a segunda parte do algoritmo, se existem símbolos de informação em **S**, quando da decisão abrupta, iguais a 4. Se existir muda-se diretamente estes símbolos. Portanto, como neste exemplo os símbolos de informação estão representados pelos dois primeiros símbolos da palavra recebida, se estes são diferentes de

4, então a segunda parte do algoritmo de decodificação já pode ser aplicada. A matriz D_E pode ser construída pelo cálculo das distâncias Euclidianas entre os pontos da seqüência r e o conjunto de modulação.

$$D_E = \begin{bmatrix} d_{0,1} & d_{0,2} & \cdots & d_{0,n} \\ d_{1,1} & d_{1,2} & \cdots & d_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{q-1,1} & d_{q-1,2} & \cdots & d_{q-1,n} \end{bmatrix}$$

$$= \begin{bmatrix} 0.158 & 1.148 & 0.012 & 2.260 \\ 0.783 & 5.026 & 1.595 & 0.680 \\ 3.308 & 7.708 & 4.048 & 3.835 \\ 4.244 & 5.488 & 3.982 & 7.365 \\ 2.297 & 1.433 & 1.487 & 6.392 \end{bmatrix} \tag{3.29}$$

De acordo com a matriz D_E obtida, podemos determinar a distância mínima de cada coluna :

$$d_{\min 1} = 0.158,\ d_{\min 2} = 1.148,\ d_{\min 3} = 0.012 \text{ e } d_{\min 4} = 0.680$$

Essas distâncias mínimas serão subtraídas de cada elemento da coluna correspondente, formando assim a matriz diferença **DIF**:

$$\mathbf{DIF} = \begin{bmatrix} dif_{0,1} & dif_{0,2} & dif_{0,3} & dif_{0,4} \\ dif_{1,1} & dif_{1,2} & dif_{1,3} & dif_{1,4} \\ dif_{2,1} & dif_{2,2} & dif_{2,3} & dif_{2,4} \\ dif_{3,1} & dif_{3,2} & dif_{3,3} & dif_{3,4} \\ dif_{4,1} & dif_{4,2} & dif_{4,3} & dif_{4,4} \end{bmatrix}$$

$$= \begin{bmatrix} 0.000 & 0.000 & 0.000 & 1.579 \\ 0.625 & 3.878 & 1.582 & 0.000 \\ 3.150 & 6.560 & 4.036 & 3.155 \\ 4.085 & 4.340 & 3.970 & 6.685 \\ 2.138 & 0.285 & 1.475 & 5.711 \end{bmatrix} \quad (3.30)$$

Baseado nas novas distâncias podemos ordenar os elementos da matriz **DIF** da menor para maior distância:

$dif_{4,2} < dif_{1,1} < dif_{4,3} < dif_{0,4} < dif_{1,3} < dif_{4,1} < dif_{2,1} < dif_{2,4} < dif_{1,2} < dif_{3,3} < dif_{2,3} < dif_{3,1}$.

Então a primeira mudança a ser feita de acordo com os índices i e j do elemento de menor valor numérico da matriz **DIF**, isto é, $dif_{4,2}$, é substituir o segundo símbolo da seqüência **S** (dado pelo índice j), que inicialmente **0**, pelo símbolo **4** (dado pelo índice **i**), produzindo assim a nova seqüência $\overline{\mathbf{S}} = (0,4,0,1)$. Verifica-se então se $\overline{\mathbf{S}}$ é palavra-código através da divisão $\overline{\mathbf{S}}(\mathbf{x}) / \mathbf{g}(\mathbf{x})$, resultando como resto dessa divisão módulo-5 o polinômio $4x + 4 \neq 0$, que demonstra que $\overline{\mathbf{S}}$ não é palavra-código. O próximo passo do processo de decodificação é restaurar a seqüência **S** e realizar a segunda mudança de acordo com os índices i e j do segundo menor elemento da matriz DIF, sendo neste exemplo o elemento $dif_{1,1}$. A mudança é realizada na primeira posição da seqüência **S**, de acordo com o índice j, onde inicialmente era representado pelo símbolo **0**, passa agora a ser representado pelo símbolo **1**, de acordo com o índice i, produzindo assim a nova seqüência $\overline{\mathbf{S}} = (1,0,0,1)$. Esta é novamente testada utilizando o polinômio gerador ***g(x)***, cujo o resto da divisão desta nova seqüência $\overline{\mathbf{S}}(x)$ por ***g(x)*** é o polinômio $3x + 3 \neq 0$, demonstrando que $\overline{\mathbf{S}}$ não é palavra-código. O terceiro passo no processo de decodificação é recuperar novamente a seqüência **S** e realizar a terceira mudança que pode ser feita através de duas possíveis

combinações de distâncias $dif_{i,j}$, isto é, a mudança poderá ser feita utilizando os índices de $dif_{4,3}$ somente, ou pela combinações dos índices de $dif_{4,2}$ e $dif_{1,1}$ juntos. A escolha sempre deverá ser feita por aquela que apresentar menor distância cumulativa. Como neste caso $dif_{4,3} = 1.475$ é maior que $dif_{4,2} + dif_{1,1} = 0.910$, a mudança na seqüência **S** deverá ser feita no primeiro e no segundo símbolos, onde eram inicialmente representados pelos símbolos **0** e **0**, passam agora a ser representados pelos símbolos **1** e **4**, respectivamente. A nova seqüência $\overline{\mathbf{S}} = (1,4,0,1)$ é novamente testada utilizando o polinômio gerador ***g(x)***, e o resto da sua divisão por ***g(x)*** é o polinômio $2x+1 \neq 0$, demonstrando que a seqüência $\overline{\mathbf{S}}$ não é palavra-código.

As etapas seguintes do processo de decodificação são mostradas na tabela 3.9, onde para este exemplo o algoritmo utilizado no processo de decodificação é finalizado quando a seqüência $\overline{\mathbf{S}} = (0,0,0,0)$ é encontrada, sendo agora $\overline{\mathbf{S}}$ uma palavra-código, produzida pela mudança na seqüência **S** de acordo com os índices de dif_{04}. A seqüência decodificada é $(0,0)$, dado pelos dois primeiros símbolos de $\overline{\mathbf{S}}$, isto devido ao fato do código de bloco utilizado neste exemplo ser sistemático.

Distâncias Cumulativas	Valor	$\overline{\mathbf{S}}$	$\overline{\mathbf{S}}$ / g(x)
$dif_{4,2}$	0.285	0 4 0 1	4x+4
$dif_{1,1}$	0.625	1 0 0 1	3x+3
$dif_{4,2}+dif_{1,1}$	0.910	1 4 0 1	2x+1
$dif_{4,3}$	1.475	1 0 4 1	2x+3
$dif_{0,4}$	1.579	0 0 0 0	0

Tabela3.9- Tabela de decodificação para a seqüência recebida

Na figura 3.5 demonstraremos o desempenho, em um canal com ruído gaussiano branco aditivo, de subcódigos de bloco multiníveis, obtidos através de códigos cíclicos de comprimento *n* igual a 6, aplicados às modulações 5-PSK e 7-PSK. O ganho assintótico de codificação sobre o sistema não codificado 2-PSK é igual a 2.053 no caso da modulação 5-PSK e igual a 3.5124 para a modulação 7-PSK. Comparando ainda com um sistema codificado 4-PSK que se utiliza de uma decodificação por decisão suave. O eixo vertical do gráfico da figura 3.5 representa a taxa de erro de bit (BER), enquanto que o eixo horizontal representa a relação entre a energia do sinal e a densidade espectral de ruído (SNR).

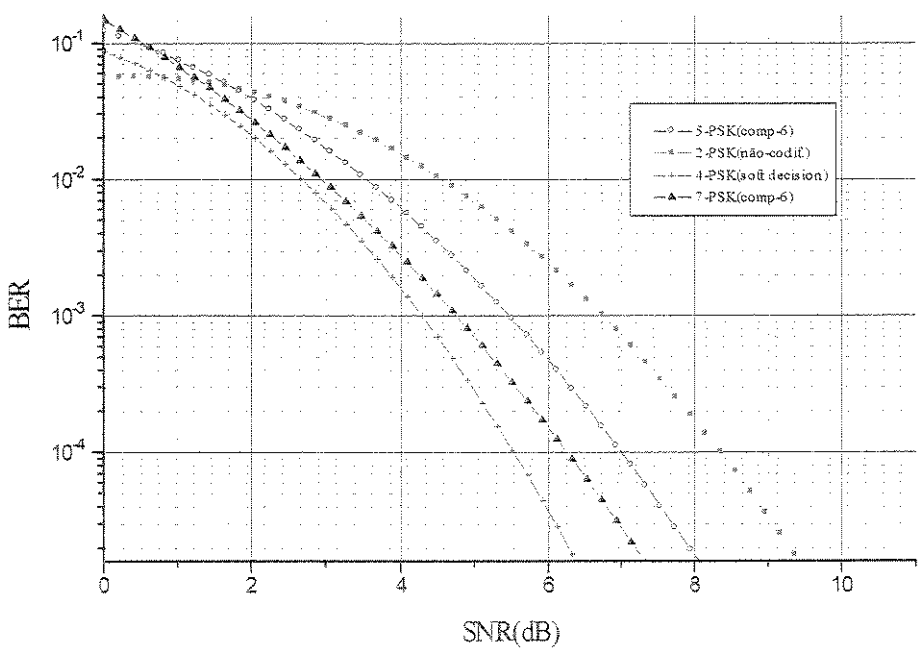

Figura 3.5-Desempenho de Esquemas Multiníveis Obtidos a partir de Códigos Cíclicos de taxa 1/2 em Canal AWGN.

3.2.4- CONCLUSÃO

Subcódigos multiníveis de blocos definidos sobre campos Z_q, conveniente para um esquema de modulação q-PSK, podem ser obtidos a partir de códigos cíclicos. Esse esquema de modulação codificada não tradicional também apresenta um bom ganho assintótico de codificação e tem uma grande vantagem em relação a esquemas de modulação codificada baseados em anéis de inteiros, é que sua estrutura algébrica ajuda na obtenção de algoritmos de decodificação suave com menor complexidade e bom desempenho.

CAPITULO 4

TRABALHOS FUTUROS E CONCLUSÃO

4.1-SUGESTÕES PARA TRABALHOS FUTUROS.

Como todo trabalho de pesquisa, os resultados não completam e finalizam as investigações. Existe sempre a possibilidade de aprimoramento do trabalho apresentado e de sua extensão. Fazendo uma análise de todo o assunto abordado pela tese podemos apresentar as seguintes sugestões para trabalhos futuros:

- ✓ Estudar mais a fundo as propriedades algébricas dos subcódigos de bloco sobre campos Z_q.
- ✓ A implementação de decodificadores de decisão suave eficientes para estes subcódigos que explorem suas propriedades algébricas.
- ✓ A obtenção de subcódigos multiníveis adequados para canais com desvanecimentos.
- ✓ Análise de desempenho destes códigos em canais com desvanecimentos.

4.2 CONCLUSÃO.

Neste trabalho apresentamos uma classe de subcódigos de bloco multiníveis, obtidos a partir de uma matriz geradora de códigos cíclicos definidos sobre o campo Z_q

Apresentamos a seguir algumas tabelas, onde fazemos uma comparação em termos de distância Euclidiana mínima quadrática dos subcódigos de bloco multiníveis obtidos a partir de códigos cíclicos e dos subcódigos de bloco multiníveis não cíclicos.

Para essas tabelas será feita uma análise individual com relação à taxa de codificação dos subcódigos de bloco multiníveis, do ganho assintótico de codificação e ainda a verificação dos valores de distâncias Euclidianas mínimas quadráticas para os subcódigos de bloco multiníveis obtidos a partir de códigos cíclicos quanto ao seu crescimento não uniforme de acordo com o aumento de n. Essa não uniformidade de crescimento ocorre devido à matriz geradora do código cíclico (n,k) ser obtida através da combinação, de acordo com a taxa do código, dos polinômios minimais $f_i(x)$, originados pela fatoração do polinômio $x^n - 1$ sobre Z_q , onde para determinados valores de n o número de combinações desses polinômios é menor em relação aos demais, ou seja, apenas um número menor de combinações de polinômios poderão ser testadas.

	Subcódigos de bloco a partir de códigos cíclicos	Subcódigos de bloco não cíclicos
n	$D^2_{E_{\min}}$	$D^2_{E_{\min}}$
4	5.5278	6.38
6	5.5278	7.76
8	7.7639	9.15
10	10.0000	10.53
12	11.3819	11.91
14	5.5278	13.29
16	10.0000	14.67
18	8.2917	15.52
20	13.2917	16.91

Tabela 4.1-Distâncias Euclidianas mínimas quadráticas para modulação 5-PSK

Para a modulação 5-PSK, apesar da taxa do código cíclico ser igual a 1/2, dada pela relação k/n, a taxa dos subcódigos de bloco multiníveis de acordo com a equação (3.2) é dada pela relação $\frac{1}{2}\cdot\frac{\log 4}{\log 5}$, ou seja , a taxa é igual a 0.430.

As distâncias Euclidianas mínimas quadráticas e por conseqüência os ganhos assintóticos de codificação, para o esquema de modulação 5-PSK, de subcódigos de bloco multiníveis obtidos a partir de códigos cíclicos são numericamente inferiores aos valores para subcódigos de bloco multiníveis não cíclicos.

Os subcódigos de bloco obtidos a partir de códigos cíclicos apresentam um crescimento não-uniforme de valores de distâncias Euclidianas mínimas quadráticas, onde

podemos observar, por exemplo, que para n igual a 12 o valor de distância Euclidiana mínima quadrática é maior em comparação ao valor para n igual a 14.

	Subcódigos de bloco a partir de códigos cíclicos	Subcódigos de bloco não cíclicos
n	$D^2_{E_{\min}}$	$D^2_{E_{\min}}$
4	3.9510	5.31
6	6.3961	7.75
8	6.8140	9.26
10	8.6551	10.77
12	10.5791	12.31
14	10.1612	14.30
16	12.4202	15.36
18	13.3592	17.68
20	13.6280	-

Tabela 4.2-Distâncias Euclidianas mínimas quadráticas para modulação 7-PSK

Para a modulação 7-PSK, a taxa dos subcódigos de bloco multiníveis de acordo com a equação (3.2) é dada pela relação $\frac{1}{2}\cdot\frac{\log 4}{\log 7}$, ou seja , a taxa é igual a 0.356, apesar da taxa do código cíclico, assim como para a modulação 5-PSK, ser igual a 1/2, dada pela relação k/n.

As distâncias Euclidianas mínimas quadráticas e por conseqüência os ganhos assintóticos de codificação, para o esquema de modulação 7-PSK, de subcódigos de bloco multiníveis obtidos a partir de códigos cíclicos são numericamente inferiores aos valores para subcódigos de bloco multiníveis não cíclicos.

Mas os valores de distâncias Euclidianas mínimas quadráticas, para a modulação 7-PSK, possuem um crescimento mais uniformes em comparação com os valores apresentados para a modulação 5-PSK.

	Subcódigos de bloco a partir de códigos cíclicos	Subcódigos de bloco não cíclicos
n	$D^2_{E_{\min}}$	$D^2_{E_{\min}}$
3	0.6349	1.49
6	0.9524	3.24
9	1.9049	3.61
12	3.6083	4.41

Tabela 4.3-Distâncias Euclidianas mínimas quadráticas para modulação 11-PSK

Para a modulação 11-PSK, a taxa dos subcódigos de bloco multiníveis de acordo com a equação (3.2) é dada pela relação $\frac{2}{3}\cdot\frac{\log 8}{\log 11}$, ou seja , a taxa é igual a 0.578, sendo a taxa do código cíclico neste caso igual a 2/3, dada pela relação k/n.

As distâncias Euclidianas mínimas quadráticas e por conseqüência os ganhos assintóticos de codificação, para o esquema de modulação 11-PSK, de subcódigos de bloco multiníveis obtidos a partir de códigos cíclicos são ainda numericamente inferiores aos valores para subcódigos de bloco multiníveis não cíclicos.

E os valores de distâncias Euclidianas mínimas quadráticas possuem um crescimento uniforme, de acordo com o aumento de n.

	Subcódigos de bloco a partir de códigos cíclicos	Subcódigos de bloco não cíclicos
n	$D^2_{E_{\min}}$	$D^2_{E_{\min}}$
3	1.9568	1.99
6	2.1859	3.31
9	2.2383	4.17
12	3.0497	5.99

Tabela 4.4-Distâncias Euclidianas mínimas quadráticas para modulação 13-PSK

Para a modulação 13-PSK, a taxa dos subcódigos de bloco multiníveis de acordo com a equação (3.2) é dada pela relação $\frac{2}{3}\cdot\frac{\log 8}{\log 13}$, ou seja , a taxa é igual a 0.540, sendo a taxa do código cíclico neste caso também igual a 2/3, dada pela relação k/n.

As distâncias Euclidianas mínimas quadráticas e por conseqüência os ganhos assintóticos de codificação, para o esquema de modulação 13-PSK, de subcódigos de bloco multiníveis obtidos a partir de códigos cíclicos são ainda numericamente inferiores aos valores para subcódigos de bloco multiníveis não cíclicos.

E os valores de distâncias Euclidianas mínimas quadráticas também possuem um crescimento uniforme, de acordo com o aumento de n.

A principal vantagem desse esquema de modulação codificada não tradicional, em relação a esquemas de modulação codificada baseados em anéis de inteiros módulo-2^q e ainda em relação a subcódigos de bloco multiníveis não cíclicos é que, devido a sua estrutura algébrica e as suas características cíclicas, existe algoritmos de decodificação suave mais rápidos que o decodificador MLD, embora com um pouco de perda no

desempenho. O algoritmo sub-ótimo de decodificação que é apresentado neste trabalho é apenas uma das alternativas que podem ser utilizadas para o processo de decodificação de subcódigos de bloco multiníveis obtidos a partir de códigos cíclicos.

APÊNDICE A

Tabela A_1 -Fatoração de x^n-*1* módulo-5

n	Polinômios Mínimais
2	$(x+4)(x+1)$
3	$(x+4)(x^2+x+1)$
4	$(x+4)(x+1)(x+3)(x+2)$
5	$(x+4)^5$
6	$(x+4)(x+1)(x^2+4x+1)(x^2+x+1)$
7	$(x+4)(x^6+x^5+x^4+x^3+x^2+x+4)$
8	$(x+4)(x+1)(x+3)(x^2+3)(x+2)(x^2+2)$
9	$(x+4)(x^2+x+1)(x^6+x^3+1)$
10	$(x+4)^5(x+1)^5$
11	$(x+4)(x^5+4x^4+4x^3+x^2+3x+4)(x^5+2x^4+4x^3+x^2+x+4)$
12	$(x+4)(x+3)(x+1)(x+2)(x^2+3x+4)(x^2+4x+1)(x^2+2x+4)(x^2+x+1)$
13	$(x+4)(x^4+2x^3+x^2+2x+1)(2x^4+3x^3+3x+1)(x^4+x^3+4x^2+x+1)$
14	$(x+4)(x+1)(x^6+4x^5+x^4+4x^3+x^2+4x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$
15	$(x+4)^5(x^2+x+1)^5$
16	$(x+4)(x+1)(x+2)(x+3)(x^2+2)(x^2+3)(x^4+2)(x^4+3)$
17	$(x+4)(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
18	$(x+4)(x+1)(x^2+x+1)(x^2+4x+1)(x^6+x^3+1)(x^6+4x^3+1)$
19	$(x+4)(x^9+x^8+3x^7+x^6+3x^5+3x^4+3x^3+2x^2+4)(x^9+3x^7+2x^6+2x^5+2x^4+4x^3+2x^2+4x+4)$
20	$(x+4)^5+(x+1)^5+(x+2)^5+(x+3)^5$

Tabela A_2 -Fatoração de x^n-*1* módulo-7

n	Polinômios Mínimais
2	$(x+6)(x+1)$
3	$(x+6)(x+5)(x+3)$
4	$(x+6)(x+1)(x^2+1)$
5	$(x+6)(x^4+x^3+x^2+x+1)$
6	$(x+6)(x+1)(x+2)(x+3)(x+4)(x+5)$
7	$(x+6)^7$
8	$(x+6)(x+1)(x^2+1)(x^2+4x+1)(x^2+3x+1)$
9	$(x+6)(x+3)(x+5)(x^3+3)(x^3+5)$
10	$(x+6)(x+1)(x^4+x^3+x^2+x+1)(x^4+6x^3+x^2+6x+1)$
11	$(x+6)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
12	$(x+6)(x+1)(x+2)(x+3)(x+4)(x+5)(x^2+1)(x^2+2)(x^2+4)$
13	$(x+6)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
14	$(x+6)^7(x+1)^7$
15	$(x+6)(x+3)(x+5)(x^4+x^3+x^2+x+1)(x^4+2x^3+4x^2+x+2)(x^4+4x^3+2x^2+x+4)$
16	$(x+6)(x+1)(x^2+1)(x^2+x+6)(x^2+3x+1)(x^2+4x+6)(x^2+4x+1)(x^2+6x+6)(x^2+3x+6)$
17	$(x+6)(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
18	$(x+6)(x+1)(x+2)(x+3)(x+4)(x+5)(x^3+2)(x^3+3)(x^3+4)(x^3+5)$
19	$(x+6)(x^3+2x+1)(x^3+4x^2+4x+6)(x^3+6x^2+3x+6)(x^3+4x^2+x+6)(x^3+3x^2+3x+6)$ (x^3+5x^2+6)
20	$(x+6)(x+1)(x^2+1)(x^4+x^3+x^2+x+1)(x^4+6x^3+x^2+6x+1)(x^4+3x^3+4x^2+4x+1)$ $(x^4+4x^3+4x^2+3x+1)$

Tabela A_3-Fatoração de x^n-*1* módulo-11

n	Polinômios Mínimais
3	$(x+10)(x^2+x+1)$
6	$(x+10)(x+1)(x^2+x+1)(x^2+10x+1)$
9	$(x+10)(x^2+x+1)(x^6+x^3+1)$
12	$(x+10)(x+1)(x^2+1)(x^2+x+1)(x^2+6x+1)(x^2+10x+1)(x^2+5x+1)$
15	$(x+10)(x+2)(x+6)(x+7)(x+8)(x^2+3x+9)(x^2+5x+3)(x^2+4x+5)(x^2+x+1)(x^2+9x+4)$
18	$(x+10)(x+1)(x^6+10x^3+1)(x^6+x^3+1)(x^2+x+1)(x^2+10x+1)$
21	$(x+10)(x^2+x+1)(x^3+5x^2+4x+10)(x^3+7x^2+6x+10)(x^6+4x^5+10x^4+10x^2+6x+1)$ $(x^6+6x^5+10x^4+10x^2+4x+1)$
24	$(x+10)(x+1)(x^2+1)(x^2+6x+1)(x^2+3x+10)(x^2+5x+1)(x^2+5x+10)(x^2+8x+10)$ $(x^2+2x+10)(x^2+9x+10)(x^2+x+1)(x^2+10x+1)(x^2+6x+10)$
27	$(x+10)(x^{18}+x^9+1)(x^6+x^3+1)(x^2+x+1)$
30	$(x+10)(x+1)(x+2)(x+3)(x+4)(x+5)(x+6)(x+7)(x+8)(x+9)(x^2+3x+9)(x^2+2x+4)$ $(x^2+6x+3)(x^2+5x+3)(x^2+4x+5)(x^2+7x+5)(x^2+x+1)(x^2+10x+1)(x^2+9x+4)$ (x^2+8x+9)

Tabela A_4-Fatoração de x^n-*1* módulo-13

n	Polinômios Mínimais
3	$(x+12)(x+4)(x+10)$
6	$(x+12)(x+1)(x+3)(x+4)(x+9)(x+10)$
9	$(x+12)(x+4)(x+10)(x^3+4)(x^3+10)$
12	$(x+12)(x+1)(x+2)(x+3)(x+4)(x+5)(x+6)(x+7)(x+8)(x+9)(x+10)(x+11)$
15	$(x+12)(x+4)(x+10)(x^4+9x^3+3x^2+x+9)(x^4+3x^3+9x^2+x+3)(x^4+x^3+x^2+x+1)$
18	$(x+12)(x+1)(x+3)(x+4)(x+9)(x+10)(x^3+3)(x^3+4)(x^3+9)(x^3+10)$
21	$(x+12)(x+4)(x+10)(x^2+6x+1)(x^2+2x+9)(x^2+5x+1)(x^2+6x+3)(x^2+5x+9)(x^2+3x+1)$ $(x^2+2x+3)(x^2+x+3)(x^2+9x+9)$
24	$(x+12)(x+1)(x+2)(x+3)(x+4)(x+5)(x+6)(x+7)(x+8)(x+9)(x+10)(x+11)(x^2+2)$ $(x^2+5)(x^2+6)\ (x^2+7)(x^2+8)(x^2+11)$
27	$(x+12)(x+4)(x+10)(x^3+4)(x^3+10)(x^9+4)(x^9+10)$
30	$(x+12)(x+1)(x+3)(x+4)(x+9)(x+10)(x^4+10x^3+9x^2+12x+3)(x^4+9x^3+3x^2+x+9)$ $(x^4+x^3+x^2+x+1)\ (x^4+3x^3+9x^2+x+3)(x^4+12x^3+x^2+12x+1)(x^4+4x^3+3x^2+12x+9)$

REFERÊNCIAS

Baldini Filho, R., *"Coded Modulation Based on Rings of Integers"*, PhD Thesis, University of Manchester, 1992.

Baldini Filho, R., **Farrell**, P.G., *"Coded Modulation Based on Rings of Integers Modulo-q. Part 1 : Block Codes"*, IEE Proc.-Commun., Vol.141, No. 3, June 1994.

Baldini Filho, R., **Farrell**, P.G., *"Coded Modulation Based on Rings of Integers Modulo-q. Part 2 : Convolutional Codes"*, IEE Proc.-Commun., Vol.141, No. 3, June 1994.

Baldini Filho., R., **Farrell**, P.G., *"Coded modulation with convolutional codes over rings"*, EUROCOD 90, udini, Italy, 5 - 9 November 1990.

Baldini Filho., R., **Farrell**, P.G.: *"Multilevel Block Subcodes for Coded Phase Modulation"* IEE Eletronics Letters , vol. 30, 1994, pp. 927-929.

Baldini Filho., R., **Pessoa**, A.C.F., **Arantes**, D.S.: "*Systematic Linear Codes over a Rings for Encoded Phase Modulation*".Int.Symp. on Infomation and Coding theory (ISICT'87), 27-1 July-August 1987, Campinas, SP, Brazil.

Benedetto, B., **Marsan**, M.A., **Albertengo**, G., **Giachin**, E., *"Combined Coding and Modulation: Theory and Applications"*, IEEE Trans. on Information Theory, pp. 223-236, Mar. 1988

Clark, Jr.G.C., **Cain**, J.B., *"Error-Corretion Coding for Digital Communications"* Plenum-Press, 1988.

Fraleigh, J.B., *"A First Course in Abstract Algebra"* Adison-Wesley Publishing Company, 1973.

Imai, H., **Hirakawa**, S., *"A New Coding Method Using Error-Correcting Codes"*, IEEE Trans. on Information Theory, Vol. IT-23, No. 3, 1977.

Lin, S., **Costello**, Jr.D.J., *" Error Control Coding: Fundamentals and Aplications"*, Prentince-Hall, 1983.

MacWilliams, F.J., **Sloane**, N.J.A, *"The Theory of Error-Correcting Codes"*, North-Holland, 1988.

Massey, J.L., *" Coding and Modulation in Digital Communications"*, Proc.1974 Int. Zurich Seminar on Digital Communication, Zurich Switzerland, March 1974.

Massey, J.L., **Mittelholzer**, T., *" Codes over Rings – A Pratical Necessity"*, AAECC7 International Conference, Université P. Sabatier, Toulouse, France, June 1989.

Massey, J.L., **Mittelholzer**, T., *" Convolutional Codes over Rings"*, Proceedings of Fourth Joint Swedish-Soviet International Workshop on Information Theory, Gotland, Sweden, August 1989.

Olcayto, E., **Lesz**, T., *"Class of Linear Cyclic Block Codes for Brust Errors Occurring in One-, Two- and Three-Dimensional Channels"*, *"*, IEE Procedings Vol. 130, Part F, No.5, August 1983.

Olcayto, E., **Lesz**, T., *"Simple Cyclic Codes for Brust Errors"*, IEE Procedings Vol. 131, Part F, No.2, April 1984.

Olcayto, E., **Birse**, A.R., *"Split-Syndrome Burst Error Correcting Codes for One-Dimensional Channels"*, IEE Procedings Vol. 134, Part F, No.4, July 1987.

Peterson, W.W., **Weldon**, Jr.E.J., *"Error Correting Codes"*, The MIT Press, 1984.

Pless,V., *"Introduction to the Theory of Error-Correting Codes"*, A Wiley-Interscince Publication, Sec. Edition,1990.

Sayegh, S., *"A Class of Optimum Block Codes in Signal Space"*, IEEE Trans. on Communication, Vol. COM-34, No. 10, Oct.1986.

Ungerboeck, G., *"Channel Coding with Multilivel / Phase Signal"*, IEEE Trans. on Information Theory, Vol. IT-28, No.2, Jan.1982.

Ungerboeck, G., *"Trellis-coded modulation with redundant signal sets: Part II: State of the art"*, IEEE Commun. Mag. , 1987, 25, (2),pg.12-21.