Universidade Estadual de Campinas

Faculdade de Engenharia Elétrica e de Computação

Departamento de Telemática

Métodos para a Construção de Códigos Espaço-temporais sobre Grupos, Corpos e Anéis para Canais com Desvanecimento Quasi-estático e Plano

Tese apresentada na Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, como parte dos requisitos exigidos para a obtenção do título de Mestre em Engenharia Elétrica.

Raquel Dutra Valença

Engenheira Eletricista/Eletrônica — UFPE

em 20 de agosto de 2001 sob a orientação do:

Prof. Dr. Reginaldo Palazzo Jr.

perante a banca examinadora:

Prof. Dr. Reginaldo Palazzo Jr.	**FEEC/UNICAMP**
Prof. Dr. Carlos Eduardo Camara	**USF**
Prof. Dr. Celso de Almeida	**FEEC/UNICAMP**

Agradecimentos [1]

Em primeiro lugar, agradeço a Deus por ter me permitido concluir mais uma etapa desta longa jornada.

Em especial, gostaria de agradecer ao meu orientador, Prof. Dr. Reginaldo Palazzo Jr., pela excelente orientação e pelas valiosas contribuições realizadas ao longo desses dois anos de trabalho em conjunto, que me permitiram adquirir novos conhecimentos.

Também, agradeço a meus pais, Ana Lúcia e Severino, e a toda a minha família por seu carinho e apoio constantes.

Sinceramente, gostaria de expressar meus agradecimentos a minha irmã, Virgínia, e a Yusef Cáceres por sua ajuda, confiança e incentivo nas horas difíceis.

De modo geral, agradeço a todos meus amigos e colegas que, direta ou indiretamente, contribuíram para a realização deste trabalho.

[1] Este trabalho foi financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

Resumo

Esta dissertação trata de métodos sistemáticos para a construção de códigos espaço-temporais (códigos de grupo, sobre corpos e sobre anéis) quando submetidos a canais com desvanecimento quasi-estático e plano. A motivação principal para esta pesquisa foi o fato de que esses códigos foram construídos heuristicamente através de uma busca exaustiva por códigos de treliça, cujos pares de palavras satisfizessem a dois critérios de projeto: o do posto e o do determinante. Neste trabalho, tais códigos são construídos da seguinte maneira. No caso de códigos espaço-temporais sobre grupo, emprega-se a técnica de recobrimento espacial baseado em reticulados para determinar rótulos apropriados para os ramos das treliça desses códigos. No caso de códigos espaço-temporais sobre corpos e sobre anéis, determina-se um polinômio gerador, que não contenha fator binário, de um código de bloco cíclico e utiliza-o para gerar um código convolucional M-ário.

Abstract

This work deals with systematic construction methods of space-time codes (codes over groups, fields and rings) for quasistatic and flat fading channels. We were motivated by the fact that these codes had been constructed by hand through an exhaustive search for trellis codes whose pairs of codewords satisfied two design criteria: the rank and the determinant ones. In this work, such codes are constructed in the following way. To construct space-time codes over groups, we use the space covering technique based on lattices to determine appropriate labels for the trellis branches codewords. To construct space-time codes over fields and rings, we determine a cyclic block code polynomial generator with no binary factor and use it as a M-ary convolutional code generator.

Conteúdo

Capítulo 1

Introdução

1.1 Histórico

O desafio de construir códigos corretores de erro para serem empregados em sistemas multiantenas de alta capacidade levou ao desenvolvimento dos códigos espaço-temporais, isto é, da codificação através das dimensões espacial e temporal. A codificação espaço-temporal, proposta por Tarokh *et al.* [18], consite num método eficiente, em termos de potência e largura de faixa, de comunicação móvel, através de canais com desvanecimento do tipo Rayleigh ou Rice. A seqüência de informação é codificada por um codificador de canal e, em seguida, essa informação codificada é convertida em n_T seqüências, as quais são simultaneamente transmitidas através de n_T antenas transmissoras. O sinal recebido, em cada uma das n_R antenas receptoras, corresponde a uma superposição dos n_T sinais transmitidos, corrompidos pelo desvanecimento imposto pelo canal.

Por permitir explorar completamente a diversidade na transmissão e na recepção, conseguem-se transmissões confiáveis de dados a altas taxas, através desses canais ruidosos. Mais precisamente, as propriedades espaciais dos códigos espaço-temporais possibilitam assegurar diversidade na transmissão e torná-la opcional na recepção. Já as suas propriedades temporais garantem que o ganho de diversidade seja alcançado, sem que a taxa de transmissão seja sacrificada.

Os códigos espaço-temporais apresentam uma estrutura de treliça bem definida e, conseqüentemente, utilizam-se técnicas conhecidas na sua decodificação. Teoricamente,

os códigos espaço-temporais provêem a melhor relação entre ganho de diversidade, taxa de transmissão, tamanho da constelação, dimensão do espaço de sinais e complexidade da treliça. Além disso, quando da contrução desses códigos, consegue-se a maior taxa de transmissão possível para um dado ganho de diversidade.

Em [18], estabeleceram-se dois critérios a serem satisfeitos na construção dos códigos espaço-temporais e demonstrou-se que o desempenho desses códigos é determinado por matrizes construídas a partir de pares de palavras-códigos distintas. O valor mínimo do posto dessas matrizes quantifica o ganho de diversidade (critério do posto) enquanto que o valor mínimo do determinante dessas matrizes quantifica o ganho de codificação (critério do determinante).

Em [19], demonstrou-se que códigos espaço-temporais, construídos para prover uma determinada ordem de diversidade quando se dispõe completamente da informação a respeito dos canais com desvanecimento quasi-estático e plano do tipo Rayleigh, provêem a mesma ordem de diversidade quando submetidos a diferentes tipos de canais com multipercursos e desvanecimento plano, sob várias condições de mobilidade. Além disso, mostrou-se que essa ordem de diversidade é preservada quando o receptor dispõe apenas de estimativas imperfeitas a respeito do estado do canal.

1.2 Apresentação do Problema

Como mencionado na seção anterior, a construção de códigos espaço-temporais [18], [19] é feita com base em dois critérios de projeto, os quais foram estabelecidos considerando o tipo de desvanecimento apresentado pelo canal em questão. Deste modo, determinar códigos espaço-temporais reduz-se a buscar exaustivamente códigos de treliça, cujas palavras, aos pares, satisfaçam os critérios do posto e do determinante. Obviamente, esse é um trabalho bastante árduo!

O objetivo desta dissertação é propor métodos sistemáticos para a construção de códigos espaço-temporais (códigos sobre grupos, sobre corpos e sobre anéis) quando submetidos a canais com desvanecimento quasi-estático e plano. De maneira geral, para cada uma das estruturas algébricas típicas, determina-se um código de bloco cíclico, como passo intermediário para a construção de tais códigos.

1.3 Descrição do Trabalho

Esta dissertação encontra-se dividida em cinco capítulos. Os próximos quatro capítulos estão organizados da seguinte forma:

Capítulo 2: Alguns fundamentos básicos da teoria de codificação e da álgebra abstrata, utilizados no desenvolvimento deste trabalho, são apresentados.

Capítulo 3: Introduzem-se os códigos espaço-temporais bem como o sistema de comunicações considerado e analisa-se o desempenho de tais códigos nesse cenário.

Capítulo 4: Estabelecem-se métodos sistemáticos para a construção de códigos espaço-temporais (códigos sobre grupos, sobre corpos e sobre anéis) quando submetidos a canais com desvanecimento quasi-estático e plano.

Capítulo 5: As contribuições deste trabalho são apresentadas e propõem-se alguns tópicos para serem abordados em pesquisas futuras.

Capítulo 2

Conceitos Básicos

O objetivo principal deste capítulo é apresentar alguns fundamentos básicos da teoria de codificação e da álgebra abstrata, utilizados no desenvolvimento desta dissertação.

Inicialmente, na Seção 2.1, usando algumas ferramentas importantes, determina-se um limitante superior para a probabilidade de erro de um código com duas palavras. Na Seção 2.2, expõe-se a teoria de recobrimento espacial baseado em reticulados e, em seguida, apresenta-se o conceito de diversidade de modulação (Seção 2.3). É importante destacar que essas ferramentas juntas formam a base do método sistemático para a construção de códigos espaço-temporais (códigos sobre grupos), assunto abordado no Capítulo 4 deste trabalho. Na seção final deste capítulo (Seção 2.4), os códigos convolucionais M-ários são apresentados e, em seguida, definidos como resultantes de máquinas de estado finito.

2.1 Receptor Ótimo para Canais Ruidosos

Considere o sistema de comunicações representado vetorialmente na Figura 2.1.

O transmissor é definido pela correspondência

$$m = m_i \Leftrightarrow \mathbf{x} = \mathbf{x}_i, \quad i = 1, 2, \ldots, M.$$

Ou seja, regido pelas probabilidades a priori $\{P(m_i)\}$, o transmissor seleciona alea-

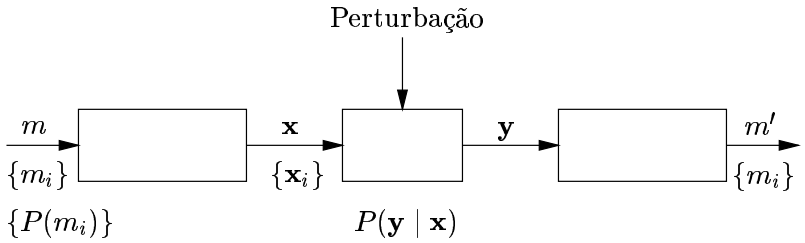

Figura 2.1: Representação vetorial de um sistema de comunicações.

toriamente um sinal dentre um conjunto de M sinais $\{\mathbf{x}_i\}$, onde

$$\mathbf{x}_i = (x_{i1}, x_{i2}, \ldots, x_{iN}).$$

O sinal recebido

$$\mathbf{y} = (y_1, y_2, \ldots, y_N),$$

devido às perturbações impostas pelo canal, consiste numa versão ruidosa daquele enviado.

Neste contexto, a regra de decodificação a ser utilizada é a da mínima probabilidade de erro. Desta forma, a probabilidade de erro de decodificação é minimizada para um dado conjunto de palavras-código (ou seja, um código) e um dado canal.

Seja $P(\mathbf{y} \mid \mathbf{x}_i)$ a probabilidade de receber a seqüência $\mathbf{y}$ (saída do canal) dado que a mensagem ou palavra-código $\mathbf{x}_i$ foi transmitida. Então,

$$P(m_i \mid \mathbf{y}) = \frac{P(\mathbf{y} \mid \mathbf{x}_i)}{P(\mathbf{y})},$$

onde

$$P(\mathbf{y}) = \sum_i P(m_i) P(\mathbf{y} \mid \mathbf{x}_i).$$

Assim, se, no receptor, o decodificador decodifica $\mathbf{y}$ como sendo a mensagem m_i, então $1 - P(m_i \mid \mathbf{y})$ é a probabilidade de decodificação errônea. Conseqüentemente, o decodificador selecionará m_i tal que $P(m_i \mid \mathbf{y})$ é máxima e, portanto, $1 - P(m_i \mid \mathbf{y})$ é

mínimo. Logo, esse processo de decodificação com mínima probabilidade de erro pode ser enunciado da seguinte maneira:

Decodifique a seqüência recebida $\mathbf{y}$ em uma mensagem m' para a qual

$$P(m' \mid \mathbf{y}) \geq P(m_i \mid \mathbf{y}), \quad \forall m_i \neq m'.$$

Ou seja,

$$\frac{P(\mathbf{y} \mid m')P(m')}{P(\mathbf{y})} \geq \frac{P(\mathbf{y} \mid m_i)P(m_i)}{P(\mathbf{y})}.$$

Como $P(\mathbf{y}) > 0$ e independe do índice i, então a decodificação com mínima probabilidade de erro implica nos dois critérios , a saber:

1. Decodificação por máxima probabilidade a posteriori (MAP):
   Se pelo menos uma $P(m_i) \neq \frac{1}{M}$ para $1 \leq i \leq M$. Então,

$$P(\mathbf{y} \mid m')P(m') \geq P(\mathbf{y} \mid m_i)P(m_i), \quad \forall m_i \neq m'.$$

2. Decodificação por máxima verossimilhança (ML):
   Se $P(m_i) = \frac{1}{M}$ para $1 \leq i \leq M$. Então,

$$P(\mathbf{y} \mid m') \geq P(\mathbf{y} \mid m_i), \quad \forall m_i \neq m'.$$

2.1.1 Probabilidade de Erro de um Código com Duas Palavras

Sejam $\mathbf{x}_1$ e $\mathbf{x}_2$ palavras-código de comprimento N. Assuma que a regra de decodifição é a de máxima verossimilhança e, sem perda de generalidade, que a mensagem transmitida foi $\mathbf{x}_1$.

Nestas circunstâncias, um erro será cometido se, quando a regra de decisão for aplicada, concluir-se que

$$P(\mathbf{y} \mid \mathbf{x}_2) \geq P(\mathbf{y} \mid \mathbf{x}_1).$$

Definindo $m(\mathbf{y})$ como sendo

$$m(\mathbf{y}) = \ln\left[\frac{P(\mathbf{y} \mid \mathbf{x}_2)}{P(\mathbf{y} \mid \mathbf{x}_1)}\right] \geq 0,$$

a probabilidade de erro dado que a palavra-código $\mathbf{x}_1$ foi enviada é expressa por

$$P(\mathbf{x}_1 \to \mathbf{x}_2 \mid \mathbf{x}_1) = P[m(\mathbf{y}) \geq 0 \mid \mathbf{x}_1]. \tag{2.1}$$

Teorema 2.1.1. [15] $P(t \geq \delta) \leq \frac{\overline{t}}{\delta}$ para $\delta > 0$, com $\overline{t} = E(t)$.

Se $t = \exp(\lambda m(y))$, então

$$P[\exp(\lambda m(y)) \geq \delta] \leq \frac{\overline{\exp(\lambda m(y))}}{\delta}. \quad \text{(Limitante de Chernoff)}$$

Desta maneira, aplicando o limitante de Chernoff à equação (2.1), obtém-se

$$\begin{aligned} P(\mathbf{x}_1 \to \mathbf{x}_2 \mid \mathbf{x}_1) &\leq E\left\{e^{\lambda m(\mathbf{y})} \mid \mathbf{x}_1\right\} \\ &\leq E\left\{e^{\lambda \ln\left[\frac{P(\mathbf{y}|\mathbf{x}_2)}{P(\mathbf{y}|\mathbf{x}_1)}\right]} \mid \mathbf{x}_1\right\} \\ &\leq E\left\{\left[\frac{P(\mathbf{y} \mid \mathbf{x}_2)}{P(\mathbf{y} \mid \mathbf{x}_1)}\right]^{\lambda} \mid \mathbf{x}_1\right\} \\ &\leq \int \left[\frac{P(\mathbf{y} \mid \mathbf{x}_2)}{P(\mathbf{y} \mid \mathbf{x}_1)}\right]^{\lambda} P(\mathbf{y} \mid \mathbf{x}_1) d\mathbf{y}. \end{aligned}$$

Ou seja,

$$P(\mathbf{x}_1 \to \mathbf{x}_2 \mid \mathbf{x}_1) \leq \int [P(\mathbf{y} \mid \mathbf{x}_2)]^{\lambda} [P(\mathbf{y} \mid \mathbf{x}_1)]^{1-\lambda} d\mathbf{y}.$$

O mínimo do termo à direita da desigualdade acima ocorre quando $\lambda = \frac{1}{2}$. Portanto, um limitante superior para a probabilidade de erro dado que a palavra-código $\mathbf{x}_1$ foi transmitida é

$$P(\mathbf{x}_1 \to \mathbf{x}_2 \mid \mathbf{x}_1) \leq \int [P(\mathbf{y} \mid \mathbf{x}_2)]^{\frac{1}{2}} [P(\mathbf{y} \mid \mathbf{x}_1)]^{\frac{1}{2}} d\mathbf{y}. \tag{2.2}$$

Um possível modelo de canal, que engloba alguns aspectos importantes dos sistemas de comunicações atuais, é aquele apenas com desvanecimento. Nele, o sinal recebido é representado vetorialmente por

$$\mathbf{y} = \alpha \mathbf{x}_i + \mathbf{n}, \quad i = 1, 2, \ldots, M,$$

sendo α uma variável aleatória com densidade de probabilidade p_α e estatisticamente independente do sinal transmitido $\mathbf{x}$ e do ruído aditivo Gaussiano branco $\mathbf{n}$.

Assim, tem-se que

$$p_y(\mathbf{y} \mid \mathbf{x}_i) = \int p_y(\mathbf{y} \mid \mathbf{x}_i, \alpha) p_\alpha d\alpha.$$

Mas

$$p_y(\mathbf{y} \mid \mathbf{x}_i, \alpha) = p_n(\mathbf{y} - \alpha \mathbf{x}_i)$$

e

$$\begin{aligned} p_n(\mathbf{y} - \alpha \mathbf{x}_i) &= \prod_{j=1}^{N} p_{n_j}(y_j - \alpha x_{ij}) \\ &= \prod_{j=1}^{N} \frac{1}{(2\pi\sigma^2)^{\frac{1}{2}}} \exp\left[-\frac{(y_j - \alpha x_{ij})^2}{2\sigma^2}\right] \\ &= \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}} \exp\left(-\frac{\|\mathbf{y} - \alpha \mathbf{x}_i\|^2}{2\sigma^2}\right), \end{aligned}$$

onde $\sigma^2 = \frac{N_0}{2}$ e $\|\mathbf{y} - \alpha \mathbf{x}_i\|$ corresponde à distância Euclidiana entre os vetores $\mathbf{y}$ e $\alpha \mathbf{x}_i$.

Portanto,

$$p_y(\mathbf{y} \mid \mathbf{x}_i) = \int \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}} \exp\left(-\frac{\|\mathbf{y} - \alpha \mathbf{x}_i\|^2}{2\sigma^2}\right) p_\alpha d\alpha.$$

Dependendo do conjunto de sinais $\{\mathbf{x}_i\}$ e da densidade de probabilidade p_α, o valor de $p_y(\mathbf{y} \mid \mathbf{x}_i)$ pode ou não ser calculado (e interpretado fisicamente). Com o intuito de contornar este problema, é comum avaliar o desempenho do sistema baseando-se no

valor de $p_y(\mathbf{y} \mid \mathbf{x}_i, \alpha)$ ao invés de $p_y(\mathbf{y} \mid \mathbf{x}_i)$. Desta forma, pode-se "reescrever" (2.2) como

$$P(\mathbf{x}_1 \to \mathbf{x}_2 \mid \mathbf{x}_1) \leq \int [P(\mathbf{y} \mid \mathbf{x}_2, \alpha)]^{\frac{1}{2}} [P(\mathbf{y} \mid \mathbf{x}_1, \alpha)]^{\frac{1}{2}} d\mathbf{y}.$$

Logo,

$$\begin{aligned}
P(\mathbf{x}_1 \to \mathbf{x}_2 \mid \mathbf{x}_1) &\leq \int_{-\infty}^{+\infty} \left\{ \frac{1}{(2\pi\sigma^2)^N} \exp\left[-\frac{\|\mathbf{y} - \alpha\mathbf{x}_2\|^2}{2\sigma^2} \right] \exp\left[-\frac{\|\mathbf{y} - \alpha\mathbf{x}_1\|^2}{2\sigma^2} \right] \right\}^{\frac{1}{2}} d\mathbf{y} \\
&\leq \int_{-\infty}^{+\infty} \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}} \exp\left[-\frac{2}{4\sigma^2} \left(\|\mathbf{y}\|^2 - \alpha \mathbf{y} \bullet (\mathbf{x}_2 + \mathbf{x}_1) + \right. \right. \\
&\quad \left. \left. + |\alpha|^2 \frac{\|\mathbf{x}_2\|^2 + \|\mathbf{x}_1\|^2}{2} \right) \right] d\mathbf{y} \\
&\leq \int_{-\infty}^{+\infty} \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}} \exp\left[-\frac{1}{2\sigma^2} \left\| \mathbf{y} - \alpha \frac{\mathbf{x}_2 + \mathbf{x}_1}{2} \right\|^2 \right] \cdot \\
&\quad \exp\left[-\frac{1}{2\sigma^2} \left(-|\alpha|^2 \frac{\|\mathbf{x}_2 + \mathbf{x}_1\|^2}{4} + |\alpha|^2 \frac{\|\mathbf{x}_2\|^2 + \|\mathbf{x}_1\|^2}{2} \right) \right] d\mathbf{y}.
\end{aligned}$$

Mas

$$\int_{-\infty}^{+\infty} \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}} \exp\left[-\frac{1}{2\sigma^2} \left\| \mathbf{y} - \alpha \frac{\mathbf{x}_2 + \mathbf{x}_1}{2} \right\|^2 \right] d\mathbf{y} = 1$$

e conseqüentemente

$$\begin{aligned}
P(\mathbf{x}_1 \to \mathbf{x}_2 \mid \mathbf{x}_1) &\leq \exp\left[-\frac{1}{2\sigma^2} \left(-|\alpha|^2 \frac{\|\mathbf{x}_2 + \mathbf{x}_1\|^2}{4} + |\alpha|^2 \frac{\|\mathbf{x}_2\|^2 + \|\mathbf{x}_1\|^2}{2} \right) \right] \\
&\leq \exp\left(-\frac{\|\alpha(\mathbf{x}_2 - \mathbf{x}_1)\|^2}{8\sigma^2} \right) \\
&\leq \exp\left[-\frac{d^2(\mathbf{x}_1, \mathbf{x}_2)}{8\sigma^2} \right],
\end{aligned}$$

onde

$$d^2(\mathbf{x}_1, \mathbf{x}_2) = \|\alpha\,(\mathbf{x}_2 - \mathbf{x}_1)\|^2$$

corresponde ao quadrado da distância Euclidiana entre os vetores $\alpha\mathbf{x}_1$ e $\alpha\mathbf{x}_2$.

2.2 Recobrimento Espacial

O problema de recobrimento espacial consiste em recobrir o espaço Euclidiano n-dimensional fazendo uso de esferas idênticas, que não se sobrepõem. A solução para esse problema pode ser conseguida arrumando essas esferas de modo que os seus centros formem um reticulado, isto é, um arranjo de infinitos pontos (ou vetores), que algebricamente formam um grupo sob a adição vetorial. Como os reticulados são descritos por formas quadráticas[1], o problema inicial reduz-se a resolver a equação

$$f(x_1, x_2, \ldots, x_n) = Q, \tag{2.3}$$

onde $f(x_1, x_2, \ldots, x_n)$ denota a forma quadrática associada ao reticulado n-dimensional em consideração e Q é a ordem do corpo. A equação polinomial (2.3), por apresentar coeficientes inteiros e soluções também inteiras, é conhecida como **equação de Diofanto**.

O vetor $(x_1, x_2, \ldots, x_n)$, solução da equação (2.3), dita o movimento ao longo do reticulado, fornecendo as palavras de um código sobre grupos (cíclico), associado aos Q sinais da modulação empregada. Tal código, resultante desse procedimento, apresenta uma importante característica: a distância mínima entre as suas palavras é máxima.

Alguns exemplos de formas quadráticas associadas a reticulados são:

1. $f(x, y) = x^2 + y^2$, associada ao reticulado $\mathbb{Z}^2$;
2. $f(x, y) = x^2 + xy + y^2$, associada ao reticulado A_2 ou hexagonal;
3. $f(x, y, z) = x^2 + y^2 + z^2$, associada ao reticulado $\mathbb{Z}^3$.

[1]Seja $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ um vetor-linha e M uma matriz simétrica n-dimensional. A expressão $f(\mathbf{x}) = \mathbf{x}M\mathbf{x}^T$ é denominda **forma quadrática** n**-ária** com matriz M [5].

Nesta dissertação, o interesse volta-se principalmente para os dois tipos de reticulados bidimensionais acima exemplificados, usados em modulações PSK.

2.2.1 Reticulado $\mathbb{Z}^2$

Neste caso, o problema de recobrir o espaço Euclidiano bidimensional empregando esferas idênticas, cujos centros formam o arranjo $\mathbb{Z}^2$, é reduzido a resolver a equação de Diofanto

$$x^2 + y^2 = Q. \tag{2.4}$$

A existência de soluções para a equação (2.4) é garantida pelos seguintes teoremas:

Teorema 2.2.1. [6] A equação $x^2 + y^2 = Q$ pode ser resolvida para x e y inteiros e com Q primo se, e somente se, $Q \equiv 1 mod(4)$ ou $Q = 2$.

Teorema 2.2.2. [6] Seja $f(x, y) = x^2 + y^2 = Q$. Então,

$$f(x, y)f(x', y') = f(xx' - yy', xy' + x'y).$$

Assim, dado um número inteiro qualquer Q, primeiramente deve-se fatorá-lo em números primos que obedeçam ao Teorema 2.2.1. Em seguida, aplica-se a equação (2.4) a cada fator primo e utiliza-se o Teorema 2.2.2 para se obter as suas soluções.

A determinação das palavras do código sobre grupos associado é uma conseqüência de se encontrar uma transformação T, cujas colunas são vetores linearmente independentes e cujo determinante é igual a Q. É desejável que pelo menos uma das colunas de T seja uma das soluções inteiras da equação (2.4). Todavia, nem sempre é possível satisfazer tal condição uma vez que a imposição de gerar um código cíclico via a transformação T pode estar fora do espaço das soluções de Diofanto. Em [6], encontram-se tabeladas soluções da equação (2.4) para $2 \leq Q \leq 38$.

Com o propósito de elucidar a técnica descrita, considere o exemplo a seguir.

Exemplo 2.2.1. Seja o reticulado $\mathbb{Z}_4^2$. A equação de Diofanto associada é dada por

$$x^2 + y^2 = 4.$$

Claramente, as suas soluções são: $\{(2,0);(-2,0);(0,2);(0,-2)\}$. Caso se utilize as soluções $(2,0)$ e $(0,2)$ como vetores-coluna da matriz T, o correspondente código sobre grupos será: $\{00,02,20,22\}$, que não é cíclico. A fim de se obter um código cíclico, um dos vetores-coluna deverá ser o par $(2,1)$ (ou $(1,2)$), com o outro vetor-coluna sendo uma das soluções da equação de Diofanto, tal que o determinante de T seja igual a 4. Portanto, uma matriz transformação T possível é

$$T = \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix}.$$

Aplicando essa transformação a um dado ponto inicial, obtém-se o código sobre grupos $\{00,12,20,32\}$, ilustrado na Figura 2.2.

	0	1	2	3
0	00			
1			12	
2	20			
3			32	

Figura 2.2: Arranjo $\mathbb{Z}_4^2$ com seus respetivos pares ordenados.

Neste caso, percebe-se que a distribuição das palavras-código sobre a região $\mathbb{Z}_4^2$ apresenta as seguintes características:

- cada uma das linhas do reticulado $\mathbb{Z}_4^2$ contém uma única palavra-código;
- duas das colunas do arranjo $\mathbb{Z}_4^2$ possuem duas palavras-código (isto é, no código, há palavras com componentes iguais); e
- duas das colunas da região $\mathbb{Z}_4^2$ não têm palavras-código.

Com base nessas observações, define-se um conceito de grande importância na teoria de recobrimento espacial:

Definição 2.2.1. [6] Um **quadrado latino** de ordem Q é um arranjo de pontos composto por Q linhas e Q colunas, no caso de um reticulado bidimensional, onde um certo símbolo ocorre Q vezes, mas não duas vezes na mesma linha ou coluna.

2.2.2 Reticulado A_2

No caso do recobrimento do espaço Euclidiano bidimensional empregando esferas idênticas, cujos centros formam o arranjo A_2, deve-se resolver a equação de Diofanto

$$x^2 + xy + y^2 = Q. \tag{2.5}$$

Assegura-se a existência de soluções para a equação (2.5) através dos seguintes teoremas:

Teorema 2.2.3. [6] A equação $x^2 + xy + y^2 = Q$ pode ser resolvida para x e y inteiros e com Q primo se, e somente se, $Q \equiv 1 mod(6)$ ou $Q = 3$.

Teorema 2.2.4. [6] Seja $f(x, y) = x^2 + xy + y^2 = Q$. Então,

$$f(x, y)f(x', y') = A(xx' - yy', xy' + x'y + yy').$$

Ao contrário do que acontece no caso do reticulado $\mathbb{Z}^2$, o par (x, y), solução da equação (2.5), sempre fornecerá o movimento ao longo do reticulado de modo a maximizar a distância mínima entre as palavras do código sobre grupos associado. Também em [6], encontram-se tabeladas soluções da equação (2.5) para valores de $Q \leq 41$.

Com o objetivo de esclarecer o método descrito, apresenta-se o seguinte exemplo.

Exemplo 2.2.2. Considere o reticulado A_2 com $Q^2 = 49$ elementos. A equação de Diofanto associada é dada por

$$x^2 + xy + y^2 = 7.$$

É fácil verificar que o par $(x, y) = (2, 1)$ é solução da equação anterior e, portanto, provê a melhor maneira de se percorrer o reticulado. A matriz transformação T correspondente é

$$T = \begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix},$$

a qual, aplicada a um dado ponto inicial, fornece o código sobre grupos $\{00, 12, 24, 36, 41, 53, 65\}$, ilustrado na Figura 2.3.

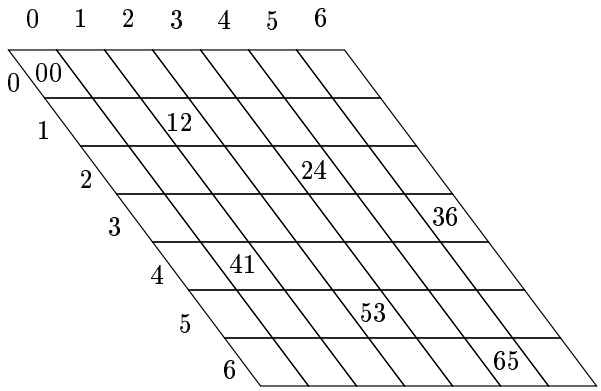

Figura 2.3: Reticulado A_2 com 49 elementos e seus respetivos pares ordenados.

Neste caso, observa-se que cada uma das linhas e colunas do reticulado A_2, mostrado na Figura 2.3, contém uma única palavra-código, o que caracteriza-o como um quadrado latino.

É importante ressaltar que, caso se obtenha um quadrado latino após a aplicação da técnica de recobrimento espacial baseado em reticulados, o código sobre grupos assim gerado apresentará uma peculiaridade muito importante: duas palavras quaisquer sempre terão componentes diferentes, ou seja, uma determinada componente das palavras-código nunca assumirá o mesmo valor em palavras distintas.

Como resultado do procedimento descrito nesta seção, obtém-se uma diversidade de modulação (diversidade espacial de sinais), abordada a seguir.

2.3 Diversidade de Modulação

Em decorrência da rápida expansão dos sistemas de comunicações móveis, cresce a necessidade de se melhorar a capacidade e o desempenho dos sistemas de transmissão. Isso pode ser obtido através do uso das técnicas de diversidade espacial e de combinação ótima. Os códigos espaço-temporais, a serem abordados nos dois próximos capítulos,

combinam diversidades espacial e temporal e, desta maneira, apresentam um bom desempenho quando submetidos a canais com desvanecimento.

Entretanto, a diversidade do sistema também pode ser aumentada através da introdução de redundância oriunda da rotação e do embaralhamento (feitos de maneira combinada) dos símbolos da constelação, antes de modulá-los. Esta técnica é denominada de **diversidade de modulação**. Neste caso, a ordem da diversidade de um conjunto de sinais multidimensionais é definida como o número mínimo de componentes distintas entre dois pontos quaisquer da constelação, isto é, como a distância de Hamming mínima entre dois vetores da constelação de pontos. Com base nessa última interpretação, conclui-se que, para uma constelação n-dimensional, a ordem da diversidade do sistema associado é sempre menor ou igual a n.

A essência da diversidade de modulação é aplicar uma determinada rotação a uma constelação de sinais clássica, de modo que o número de componentes distintas entre dois pontos quaisquer seja máximo. Empregando um componente embaralhador/desembaralhador, assume-se que as componentes em fase e em quadratura do símbolo recebido sofrem desvanecimentos independentes.

A Figura 2.4 ilustra esse procedimento para uma constelação 4-PSK.

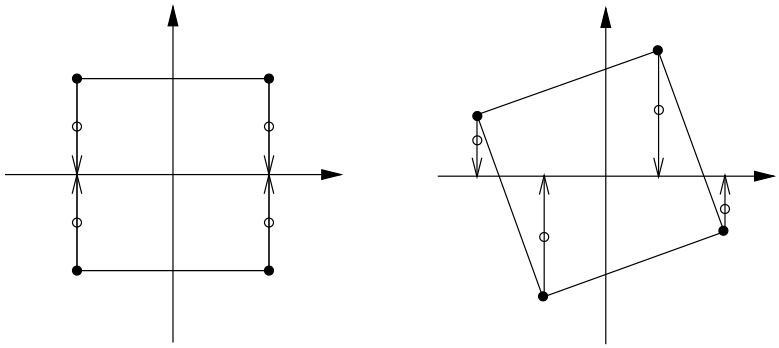

Figura 2.4: Diversidade de modulação para a constelação 4-PSK.

Caso se suponha que o desvanecimento só atinge uma única componente do vetor associado ao sinal transmitido, pode-se concluir que a constelação "desvanecida" da Figura 2.4(b) (círculos vazios) oferece mais proteção contra os efeitos do ruído, uma vez que dois pontos quaisquer nunca coincidirão, como acontece na Figura 2.4(a).

Observa-se que, quando submetido a um canal apenas com ruído aditivo Gaussiano branco, o conjunto de sinais rotacionados apresenta um desempenho igual ao de um conjunto de sinais não-rotacionados. Quando submetida a um canal com desvanecimento do tipo Rice, a constelação rotacionada apresenta um desempenho intermediário entre aqueles apresentados quando submetida a canais puramente Gaussiano e com desvanecimento do tipo Rayleigh.

2.4 Códigos Convolucionais M-ários

Nesta seção, os códigos convolucionais são definidos de maneira que, para cada bit de informação que entra no codificador, gera-se um símbolo M-ário na sua saída. Esses códigos convolucionais de "taxa" 1 são análogos aos códigos convolucionais binários de taxa $\frac{1}{\log_2 M}$. De fato, o aspecto desses dois codificadores são idênticos.

Inicialmente, os códigos convolucionais M-ários serão definidos como resultantes de máquinas de estado finito. Esse tratamento torna mais conveniente a introdução das propriedades e dos parâmetros desses códigos. No Capítulo 4, redefinem-se tais códigos, usando uma abordagem algébrica, o que permite a construção de códigos convolucionais M-ários bons a partir de códigos de bloco conhecidos.

2.4.1 Códigos Convolucionais M-ários: Códigos obtidos a partir de Máquinas de Estado Finito

O codificador mostrado na Figura 2.5 é uma máquina de estado finito composta por um registrador deslocamento com K estágios e por $\log_2 M$ somadores módulo 2, os quais estão conectados às células do registrador deslocamento de alguma maneira fixa.

A informação binária, que chega ao codificador, é deslocada ao longo do registrador, a uma taxa de 1 bit por unidade de tempo. Após cada deslocamento, o conteúdo das células do registrador são combinados de maneira determinada pelas conexões, fornecendo uma $(\log_2 M)$-upla binária ou, analogamente, um símbolo M-ário. Como um símbolo do código é produzido a cada bit de entrada, o código resultante apresenta uma taxa $r = 1$ bit/símbolo.

O comprimento K do registrador deslocamento é denominado de **comprimento de**

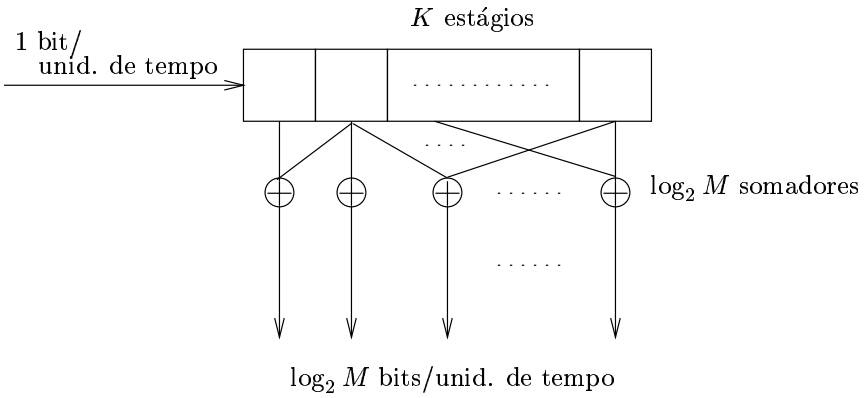

Figura 2.5: Código convolucional M-ário geral com taxa 1 e comprimento de restrição K.

restrição porque cada bit de entrada afeta, no máximo, K símbolos do código, à medida que o mesmo se desloca ao longo do registrador. Portanto, esse codificador produz um código convolucional M-ário com taxa 1 e comprimento de restrição $K = m + 1$, onde m é definido como sendo a memória do codificador.

É importante ressaltar que, como se empregam apenas operações lineares, a soma módulo 2 de duas palavras-código também é uma palavra-código. Além disso, a seqüência de entrada toda nula produz a seqüência-código toda nula. Logo, as palavras-código formam um grupo sob a operação soma módulo 2.

O codificador da Figura 2.5 pode ser visualizado como um codificador convolucional binário com taxa $r = \frac{1}{\log_2 M}$. A diferença entre essas duas abordagens reside no fato de que as conexões para o codificador convolucional M-ário são escolhidas de modo que o mesmo apresente um bom desempenho em canais M-ários. Como conseqüência, esse codificador pode não apresentar um bom desempenho em canais binários.

Como exemplo, considere o codificador convolucional 4-ário com $r = 1$ e $K = 4$, ilustrado na Figura 2.6.

Esse codificador é o melhor codificador convolucional 4-ário com $r = 1$ e $K = 4$. Entretanto, o mesmo não corresponde ao melhor codificador convolucional binário com $r = \frac{1}{2}$ e $K = 4$.

O estado de um codificador convolucional é definido como sendo o conteúdo das $(K - 1)$ células mais à direita do registrador deslocamento. Assim, o número total de

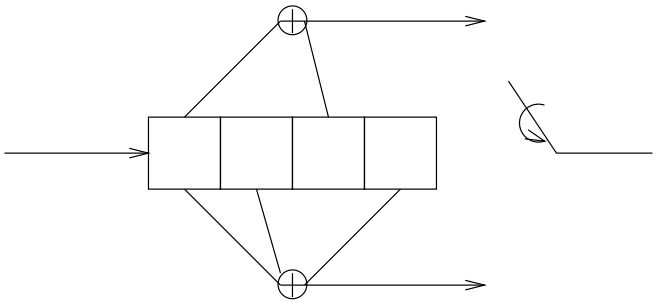

Figura 2.6: Código convolucional 4-ário com comprimento de restrição $K = 4$.

estados é igual a 2^{K-1}. Durante a codificação, o registrador transiciona de um estado a outro, a cada novo bit que entra no codificador. Com base nestas informações, um diagrama de estados, mostrando como essas transições ocorrem, pode ser desenhado para cada codificador. Na Figura 2.7, encontra-se o diagrama de estados do codificador convolucional mostrado na Figura 2.6.

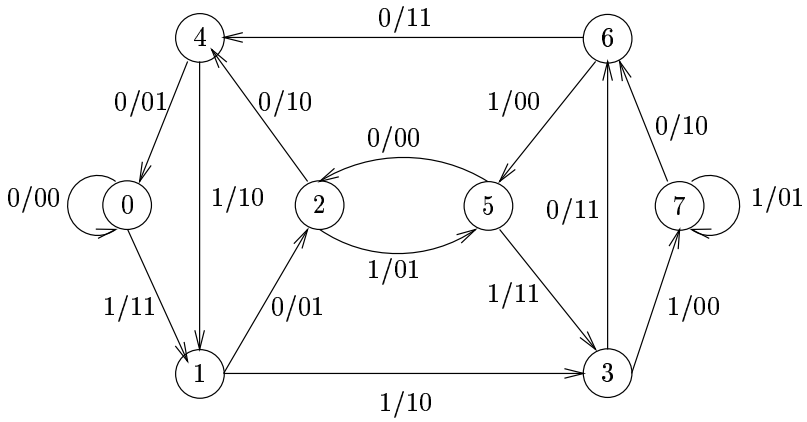

Figura 2.7: Diagrama de estados do código convolucional 4-ário da Figura 2.6.

Nesse grafo, os oito possíveis estados são representados por nós. As linhas, que conectam os nós diretamente, ilustram as possíveis transições. Além disso, cada linha é rotulada pelo bit de entrada, que causa a transição, e pelo símbolo produzido na saída do codificador.

Uma outra maneira muito útil de representar um codificador convolucional é através do diagrama de treliça. Para o codificador convolucional mostrado na Figura 2.6, a sua treliça encontra-se ilustrada na Figura 2.8.

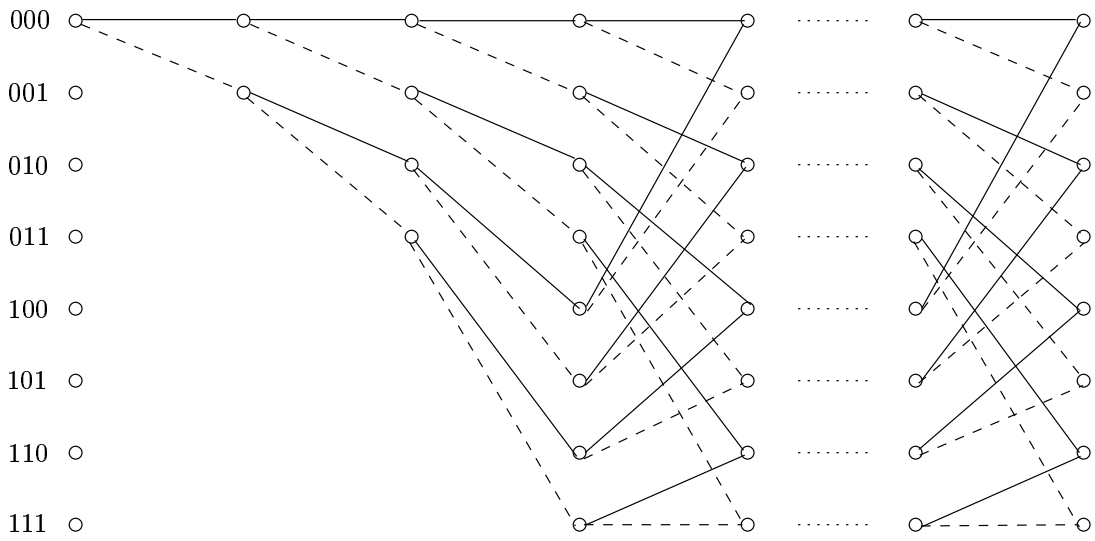

Figura 2.8: Treliça associada ao código convolucional 4-ário da Figura 2.6.

Cada coluna de nós representa os oito possíveis estados do codificador e a profundidade na treliça, a partir da coluna de nós mais à esquerda, corresponde ao número de bits que entraram no codificador. As transições resultantes da entrada de um bit 0 no codificador convolucional são representadas por linhas cheias enquanto que aquelas ocasionadas pela entrada de um bit 1 são representadas por linhas tracejadas. Note que, a partir do quarto bit de entrada, todos os caminhos-código chegam aos pares em cada um dos estados. Isto acontece porque há apenas dezesseis transições entre os oito estados. Conseqüentemente, dois caminhos quaisquer, que entram num determinado estado, produzirão os mesmos símbolos-código ao deixá-lo. Este fato será de extrema importância durante a decodificação.

Um conceito muito importante em codificação é o de distância entre palavras-código. A distância entre duas palavras de um código é definida como o número de posições em que os seus símbolos M-ários diferem. Neste contexto, a palavra 4-ária 01 10 00 01 dista 2 da palavra 01 10 01 11. Devido ao fato de as palavras-código formarem um grupo, a

soma módulo 2 de duas palavras é igual ao número de símbolos não-nulos da palavra resultante dessa operação, o que, por sua vez, é definido como o seu peso.

Agora, considere todos os pares de caminhos-código que partem do estado nulo e voltam a esse estado, pela primeira vez, após algumas transições. O valor mínimo das distâncias entre todos esses pares é denominado de distância livre do código, d_{free}. Note que d_{free} também corresponde ao mínimo dos pesos de todas as palavras não-nulas que partem do estado nulo e passam a coincidir com a palavra-código toda nula após algumas transições. Quanto maior o valor de d_{free}, menor é o desempenho mínimo e, portanto, melhor é o código. Assim, se dois códigos convolucionais apresentam o mesmo valor para d_{free}, aquele que tiver o menor número de palavras com peso d_{free} apresentará o melhor desempenho. Além disso, se ambos possuírem o mesmo número de palavras-código com peso d_{free}, aquele com o menor número de palavras com peso $d_{free}+1$ apresentará o melhor desempenho e assim sucessivamente.

A seguir, enuncia-se um teorema de grande importância na teoria de códigos convolucionais M-ários.

Teorema 2.4.1. [15] Para qualquer valor de K e para M infinitamente grande, existe um código convolucional M-ário com taxa $r = 1$, comprimento de restrição igual a K e $d_{free} = K$.

No Capítulo 4, serão apresentadas técnicas algébricas que permitem a construção de códigos convolucionais M-ários com uma determinada distância livre, pré-estabelecida. Além disso, apresentam-se exemplos de tais códigos com a maior distância livre possível ($d_{free} = K$).

Capítulo 3

Códigos Espaço-temporais para Comunicação Móvel

Neste capítulo, são introduzidos os códigos espaço-temporais bem como o sistema de comunicações considerado. Além disso, analisa-se o desempenho de tais códigos no cenário descrito.

Na Seção 3.1, expõe-se o problema enfrentado pelas comunicações móveis e propõe-se o uso de códigos espaço-temporais com o objetivo de solucioná-lo. Em seguida (Seção 3.2), define-se o modelo do sistema de comunicações móveis a ser empregado. Na Seção final deste capítulo (Seção 3.3), analisa-se o desempenho de códigos espaço-temporais em alguns tipos de canais ruidosos e reproduzem-se os critérios a serem satisfeitos no projeto desses códigos.

3.1 Introdução

Para que seja de boa qualidade, a transmissão de dados a altas taxas, através de canais de comunicações móveis, deve ser feita levando em consideração o desvanecimento causado por multipercursos. A técnica da diversidade tem se mostrado como sendo a estratégia mais eficiente para combater esse tipo de perda. Além das diversidades temporal e em freqüência, também emprega-se a diversidade espacial quando se utilizam múltiplas antenas, principalmente na estação base.

Para que se consiga diversidade na transmissão, deve-se adicionalmente introduzir

uma codificação no transmissor e, assim, evitar que sinais transmitidos simultaneamente por antenas distintas sofram interferências destrutivas. Os códigos espaço-temporais, propostos por Tarokh *et al.* [18], permitem que esse objetivo seja atingido em sistemas com múltiplas antenas, sem que haja a necessidade do transmissor conhecer instantaneamente o canal.

Os códigos espaço-temporais empregam múltiplas antenas transmissoras e receptoras para alcançar ganhos de diversidade e de codificação na comunicação através de canais com desvanecimento. Uma alta eficiência, proporcionada pela largura de faixa, com desempenho próximo à capacidade *outage*[1] teórica, é conseguida. Como conseqüência, permitem-se transmissões confiáveis de dados a altas taxas através de canais com desvanecimento. Desde a sua introdução, os códigos espaço-temporais têm recebido especial atenção, uma vez que provêem uma maneira efetiva de explorar completamente a diversidade na transmissão e na recepção. Entretanto, para um número fixo de antenas transmissoras, a complexidade de decodificação dos códigos espaço-temporais , medida pelo número de estados da treliça presentes no decodificador, cresce exponencialmente com a taxa de transmissão.

No *CDMA2000 Radio Transmission Technology*, proposta para os sistemas de terceira geração, tanto os códigos espaço-temporais como os códigos turbo foram adotados.

3.2 Modelo do Sistema

Supondo que o desvanecimento do canal é quasi-estático e plano[2], considera-se um sistema de comunicações móveis no qual a estação base é composta por n_T antenas transmissoras enquanto que o móvel possui n_R antenas receptoras. Primeiramente, a seqüência de informação é codificada por um codificador de canal e convertida em n_T seqüências paralelas. Em seguida, essas seqüências passam por um formatador de pulso e são moduladas.

[1] A capacidade *outage* [9] corresponde à máxima taxa de informação que pode ser atingida em qualquer condição de desvanecimento, considerando-se que não há interrupção na transmissão.

[2] Um canal apresenta desvanecimento quasi-estático e plano [23] quando sua largura de faixa coerente é maior que a largura de faixa do sinal modulado transmitido. Nesta situação, todas as componentes de freqüência do sinal enviado sofrem desvanecimento de maneira igual. Por largura de faixa coerente do canal entende-se a máxima separação em freqüência para a qual essas componentes ainda são consideradas correlacionadas ao chegarem (com diferentes tempos de atraso) no receptor.

O sinal transmitido pela i-ésima antena num dado instante de tempo t é denotado por $\sqrt{E_S}x_t^i$, para $1 \leq i \leq n_T$, onde x_t^i apresenta uma amplitude normalizada de modo que a energia média da constelação seja 1, sendo E_S a energia de cada sinal transmitido. Os n_T sinais $\sqrt{E_S}x_t^i$ têm mesmo período T e, num dado instante de tempo t, todos são simultaneamente transmitidos. O diagrama de blocos do transmissor associado ao sistema de comunicações considerado é mostrado na Figura 3.1.

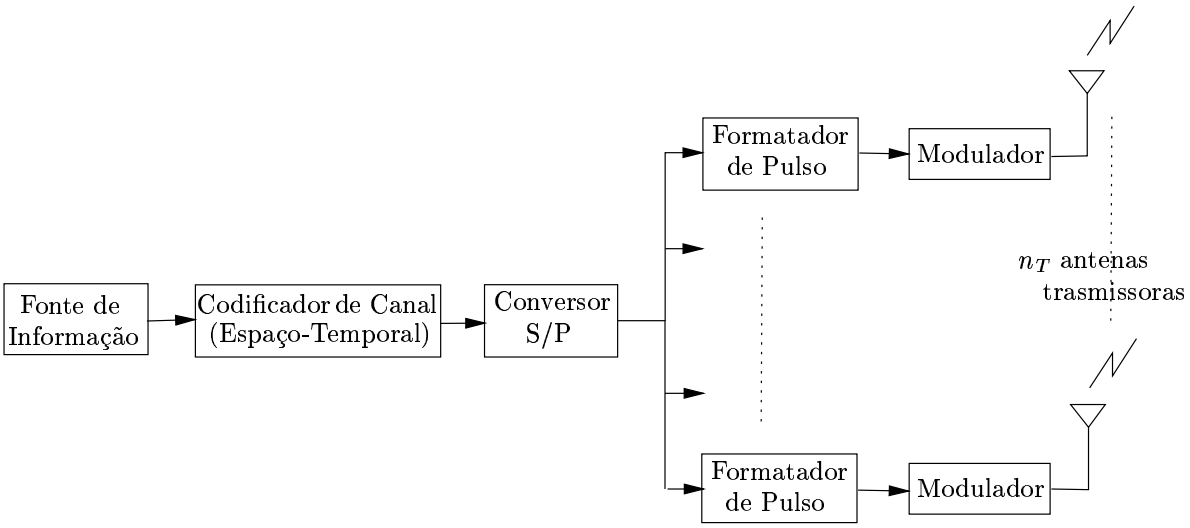

Figura 3.1: Diagrama de blocos do transmissor.

O sinal recebido em cada uma das n_R antenas corresponde a uma superposição dos n_T sinais transmitidos, corrompidos pelo desvanecimento imposto pelo canal. Portanto, denotando por y_t^j o sinal recebido na j-ésima antena num certo instante de tempo t, tem-se

$$y_t^j = \sum_{i=1}^{n_T} \alpha_{ij} x_t^i \sqrt{E_S} + n_t^j, \quad 1 \leq j \leq n_{R,}$$

onde o ruído n_t^j, num determinado instante de tempo t, é modelado como amostras independentes de uma variável aleatória complexa Gaussiana de média nula e variância $\frac{N_0}{2}$ por dimensão e α_{ij} é o ganho de percurso que atua no sinal transmitido pela i-ésima antena e recebido na j-ésima antena. Os coeficientes α_{ij} são modelados como amostras independentes da envoltória de uma variável aleatória complexa Gaussiana

com média $E[\alpha_{ij}]$ (que pode ser não-nula) e variância $0,5$ por dimensão. Assume-se que esses ganhos de percurso são constantes ao longo de um quadro de transmissão de comprimento l e que seus valores mudam independentemente de um quadro para outro (desvanecimento quasi-estático e plano).

Supondo que as antenas estão suficientemente separadas, considera-se que os sinais dos $n_T n_R$ caminhos entre as antenas transmissoras e receptoras sofrem desvanecimentos independentes. Em decorrência dessa suposição, é possível atingir significativos ganhos de diversidade na transmissão e na recepção para canais móveis com desvanecimento.

3.3 Desempenho de Códigos Espaço-temporais em Canais com Desvanecimento Quasi-estático e Plano e Critérios para seu Projeto

Com o intuito de avaliar o desempenho de códigos espaço-temporais no cenário descrito na seção anterior, analisa-se a probabilidade de que um receptor de máxima verossimilhança decida erroneamente em favor de um sinal

$$\widetilde{x} = \widetilde{x}_1^1 \widetilde{x}_1^2 \cdots \widetilde{x}_1^{n_T} \widetilde{x}_2^1 \widetilde{x}_2^2 \cdots \widetilde{x}_2^{n_T} \cdots \widetilde{x}_l^1 \widetilde{x}_l^2 \cdots \widetilde{x}_l^{n_T}$$

quando

$$x = x_1^1 x_1^2 \cdots x_1^{n_T} x_2^1 x_2^2 \cdots x_2^{n_T} \cdots x_l^1 x_l^2 \cdots x_l^{n_T}$$

é transmitido, assumindo que a informação a respeito do estado do canal é completamente disponível [18]. Para tanto, seguindo um raciocínio análogo ao desenvolvido na Subseção 2.1.1 e adotando $\sigma^2 = \frac{N_0}{2}$, conclui-se que essa probabilidade de erro é limitada superiormente por

$$P(x \to \widetilde{x} | \alpha_{ij},\ 1 \leq i \leq n_T,\ 1 \leq j \leq n_R) \leq \exp\left[-\frac{d^2(x, \widetilde{x}) E_S}{4N_0}\right]$$

onde

$$d^2(x,\widetilde{x}) = \sum_{j=1}^{n_R}\sum_{t=1}^{l}\left|\sum_{i=1}^{n_T}\alpha_{ij}(x_t^i - \widetilde{x}_t^i)\right|^2. \tag{3.1}$$

Mas

$$\begin{aligned} d^2(x,\widetilde{x}) &= \sum_{j=1}^{n_R}\sum_{t=1}^{l}\left(\sum_{i=1}^{n_T}\alpha_{ij}(x_t^i - \widetilde{x}_t^i)\right)\left(\sum_{k=1}^{n_T}\overline{\alpha_{kj}}\,\overline{(x_t^k - \widetilde{x}_t^k)}\right) \\ &= \sum_{j=1}^{n_R}\sum_{k=1}^{n_T}\overline{\alpha_{kj}}\sum_{i=1}^{n_T}\alpha_{ij}\sum_{t=1}^{l}(x_t^i - \widetilde{x}_t^i)\overline{(x_t^k - \widetilde{x}_t^k)}, \end{aligned}$$

onde $\overline{(\,\cdot\,)}$ denota complexo conjugado.

Assim, definindo $\Omega_j = (\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{n_T j})$, pode-se reescrever a expressão em (3.1) como

$$d^2(x,\widetilde{x}) = \sum_{j=1}^{n_R}\Omega_j A(x,\widetilde{x})\Omega_j^*,$$

onde $*$ denota transposto conjugado e o elemento a_{pq} da matriz $A(x,\widetilde{x})$ é definido por

$$a_{pq} = \sum_{t=1}^{l}(x_t^p - \widetilde{x}_t^p)\overline{(x_t^q - \widetilde{x}_t^q)},$$

para $1 \leq p, q \leq n_T$.

Desta maneira,

$$P(x \to \widetilde{x}|\alpha_{ij},\, 1 \leq i \leq n_T,\, 1 \leq j \leq n_R) \leq \prod_{j=1}^{n_R}\exp\left[-\Omega_j A(x,\widetilde{x})\Omega_j^*\frac{E_S}{4N_0}\right].$$

Como a matriz $A(x,\widetilde{x})$ é hermitiana, isto é, $A^*(x,\widetilde{x}) = A(x,\widetilde{x})$, existem uma matriz unitária V (ou seja, $V^* = V^{-1}$) e uma matriz diagonal real D tais que $VA(x,\widetilde{x})V^* = D$. As linhas de V (denotadas por $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{n_T}\}$) formam uma base ortonormal para o espaço $\mathbb{C}^{n_T}$, a qual é composta pelos autovetores da matriz $A(x,\widetilde{x})$. Além disso, os elementos da diagonal da matriz D são os autovalores $\lambda_i, 1 \leq i \leq n_T$, da matriz $A(x,\widetilde{x})$,

levando em consideração suas multiplicidades.

Pode-se verificar que a matriz

$$B(x,\widetilde{x}) = \begin{bmatrix} \widetilde{x}_1^1 - x_1^1 & \widetilde{x}_2^1 - x_2^1 & \cdots & \cdots & \widetilde{x}_l^1 - x_l^1 \\ \widetilde{x}_1^2 - x_1^2 & \widetilde{x}_2^2 - x_2^2 & \cdots & \cdots & \widetilde{x}_l^2 - x_l^2 \\ \widetilde{x}_1^3 - x_1^3 & \widetilde{x}_2^3 - x_2^3 & \ddots & \vdots & \widetilde{x}_l^3 - x_l^3 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \widetilde{x}_1^{n_T} - x_1^{n_T} & \widetilde{x}_2^{n_T} - x_2^{n_T} & \cdots & \cdots & \widetilde{x}_l^{n_T} - x_l^{n_T} \end{bmatrix}$$

corresponde à raiz quadrada da matriz $A(x,\widetilde{x})$, isto é, $B(x,\widetilde{x})B^*(x,\widetilde{x}) = A(x,\widetilde{x})$. Portanto, os autovalores da matriz $A(x,\widetilde{x})$ são números reais não-negativos.

Definindo $(\beta_{1j}, \beta_{2j}, \ldots, \beta_{n_T j}) = \Omega_j V^*$, tem-se

$$\Omega_j A(x,\widetilde{x})\Omega_j^* = \sum_{i=1}^{n_T} \lambda_i \left|\beta_{ij}\right|^2,$$

sendo

$$\beta_{ij} = \sum_{k=1}^{n_T} \alpha_{kj}\overline{v_{ik}}.$$

Logo,

$$P(x \to \widetilde{x} \mid \alpha_{ij}, 1 \le i \le n_T, 1 \le j \le n_R) \le \prod_{j=1}^{n_R} \exp\left(-\frac{E_S}{4N_0}\sum_{i=1}^{n_T} \lambda_i \left|\beta_{ij}\right|^2\right). \qquad (3.2)$$

Como a matriz V é unitária, $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{n_T}\}$ forma uma base ortonormal para o espaço $\mathbb{C}^{n_T}$ e $\beta_{ij}, 1 \le i \le n_T, 1 \le j \le n_R$, são variáveis aleatórias Gaussianas complexas independentes, com variância

$$\begin{aligned} var\left[\beta_{ij}\right] &= var\left[\sum_{k=1}^{n_T}\alpha_{kj}\overline{v_{ik}}\right] \\ &= \sum_{k=1}^{n_T}\left\|v_{ik}\right\|^2 var\left[\alpha_{kj}\right] \\ &= var\left[\alpha_{kj}\right] \\ &= \frac{1}{2} \quad \text{por dimensão} \end{aligned}$$

e média dada por

$$\begin{aligned} E\left[\beta_{ij}\right] &= E\left[\sum_{k=1}^{n_T}\alpha_{kj}\overline{v_{ik}}\right] \\ &= \sum_{k=1}^{n_T}E\left[\alpha_{kj}\right]\overline{v_{ik}} \\ &= \mathbf{K}^j \bullet \mathbf{v}_i, \end{aligned}$$

onde

$$\mathbf{K}^j = (E[\alpha_{1j}], E[\alpha_{2j}], \ldots\ E[\alpha_{n_Tj}]).$$

Seja

$$K_{ij} = \left|E[\beta_{ij}]\right|^2 = \left|\mathbf{K}^j \bullet \mathbf{v}_i\right|^2.$$

Logo, $\left|\beta_{ij}\right|, 1 \leq i \leq n_{T,}1 \leq j \leq n_R$, são independentes e apresentam uma distribuição de Rice com função densidade de probabilidade dada por

$$p\left(\left|\beta_{ij}\right|\right) = 2\left|\beta_{ij}\right|\exp\left(-\left|\beta_{ij}\right|^2 - K_{ij}\right) I_0\left(2\left|\beta_{ij}\right|\sqrt{K_{ij}}\right), \quad \left|\beta_{ij}\right| \geq 0,$$

onde $I_0(\cdot)$ é a função de Bessel de ordem zero e do primeiro tipo modificada.

Avaliando a expressão (3.2) com respeito às distribuições de $|\beta_{ij}|$, obtém-se

$$P(x \to \widetilde{x}) \leq \prod_{j=1}^{n_R} \left(\prod_{i=1}^{n_T} \frac{1}{1 + \frac{E_S}{4N_0}\lambda_i} \exp\left(-\frac{K_{ij}\frac{E_S}{4N_0}\lambda_i}{1 + \frac{E_S}{4N_0}\lambda_i} \right) \right). \tag{3.3}$$

Para o caso no qual o canal apresenta desvanecimento do tipo Rayleigh, $E[\alpha_{ij}] = 0$ e, conseqüentemente, $K_{ij} = 0$, para $1 \leq i \leq n_T, 1 \leq j \leq n_R$. Logo, a probabilidade de se escolher $\widetilde{x}$ quando x é transmitido (expressão (3.3)) é limitada superiormente por

$$P(x \to \widetilde{x}) \leq \left(\frac{1}{\prod_{i=1}^{n_T} 1 + \frac{E_S}{4N_0}\lambda_i} \right)^{n_R} \leq \frac{1}{\left(\prod_{i=1}^{r} \lambda_i\right)^{n_R} \left(\frac{E_S}{4N_0}\right)^{n_R r}}, \tag{3.4}$$

onde $r \leq n_T$ é o posto da matriz $B(x, \widetilde{x})$ e $\lambda_1, \lambda_2, \ldots, \lambda_r$ são os autovalores não-nulos da matriz $A(x, \widetilde{x})$.

Deste modo, definindo o ganho de diversidade como sendo o expoente da relação sinal-ruído $\left(\frac{E_S}{4N_0}\right)$ no denominador do termo mais à direita da expressão (3.4), verifica-se que um ganho de diversidade igual a $n_R r$ é alcançado. Além disso, consegue-se um ganho de codificação igual a $(\lambda_1 \lambda_2 \ldots \lambda_r)^{\frac{1}{r}}$. Tal ganho de codificação corresponde a uma medida aproximada do ganho obtido em relação a um sistema não-codificado operando com o mesmo ganho de diversidade. Como o ganho de diversidade corresponde a um expoente na expressão (3.4), conclui-se que atingir o seu valor máximo é mais importante do que atingir um valor alto do ganho de codificação quando a relação sinal-ruído é baixa.

Com base na análise realizada anteriormente, estabeleceram-se os seguintes critérios a serem satisfeitos na determinação de códigos espaço-temporais sujeitos a desvanecimento do tipo Rayleigh [18]:

- **Critério do Posto:** Para que se atinja uma diversidade máxima igual a $n_R n_T$, a matriz $B(x, \widetilde{x})$ deve ter posto completo para qualquer par de palavras-código x e $\widetilde{x}$. Se essa matriz possui um posto mínimo r para um dado par de palavras-código distintas, então uma diversidade igual a $n_R r$ é obtida.

- **Critério do Determinante:** Suponha que se deseja atingir uma diversidade igual a $n_R r$. O valor mínimo das raízes r-ésimas da soma dos determinantes

de todos os cofatores principais $r \times r$ da matriz $A(x, \widetilde{x})$ (ou seja, do produto $\lambda_1 \lambda_2 \ldots \lambda_r$), calculados para todos os pares de palavras-código distintas x e $\widetilde{x}$, corresponde ao ganho de codificação. O objetivo do projeto é tornar esta soma a maior possível. Se tal objetivo for alcançar uma diversidade igual a $n_R n_T$, então o valor mínimo do determinante da matriz $A(x, \widetilde{x})$, calculado para todos os pares de palavras-código distintas, deve ser maximizado.

Para o caso no qual o canal apresenta desvanecimento do tipo Rice e a relação sinal-ruído é suficientemente alta, a probabilidade de se escolher x quando $\widetilde{x}$ é transmitido (expressão (3.3)) é limitada superiormente por

$$P(x \to \widetilde{x}) \leq \left(\frac{E_S}{4N_0}\right)^{-n_R r} \left(\prod_{i=1}^{r} \lambda_i\right)^{-n_R} \left[\prod_{j=1}^{n_R} \prod_{i=1}^{r} \exp(-K_{ij})\right].$$

Um ganho de diversidade igual a $n_R r$ e um ganho de codificação igual a

$$(\lambda_1 \lambda_2 \ldots \lambda_r)^{\frac{1}{r}} \left[\prod_{j=1}^{n_R} \prod_{i=1}^{r} \exp(-K_{ij})\right]^{\frac{1}{n_R r}}$$

são alcançados.

Os critérios a serem satisfeitos na construção de códigos espaço-temporais sujeitos a desvanecimento do tipo Rice são [18]:

- **Critério do Posto:** Para que se atinja uma diversidade máxima igual a $n_R n_T$, a matriz $B(x, \widetilde{x})$ deve ter posto completo para qualquer par de palavras-código x e $\widetilde{x}$. Se essa matriz possui um posto mínimo r para um dado par de palavras-código distintas, então uma diversidade igual a $n_R r$ é obtida.

- **Critério do Determinante:** Seja $\Lambda(x, \widetilde{x})$ a soma de todos os determinantes dos cofatores principais $r \times r$ da matriz $A(x, \widetilde{x})$. O valor mínimo do produto

$$\Lambda(x, \widetilde{x}) \left[\prod_{j=1}^{n_R} \prod_{i=1}^{r} \exp(-K_{ij})\right]^{\frac{1}{n_R r}},$$

calculado para todos os pares de palavras-código distintas, deve ser maximizado.

Capítulo 4

Construção de Códigos Espaço-temporais

O propósito deste capítulo é apresentar métodos sistemáticos para a construção de códigos espaço-temporais (códigos sobre grupos, sobre corpos e sobre anéis) quando submetidos a canais com desvanecimento quasi-estático e plano.

Primeiramente (Seção 4.1), são apresentadas as estratégias de codificação empregadas e enfatiza-se a importância da diversidade de modulação para se determinar códigos espaço-temporais (códigos sobre grupos). Na Seção 4.2, apresentam-se alguns desses códigos para canais com desvanecimento quasi-estático e plano. Em seguida (Seção 4.3), apresenta-se um método sistemático para a construção de tais códigos espaço-temporais nesse cenário. Na Seção 4.4, os códigos convolucionais M-ários, introduzidos no Capítulo 2, são redefinidos segundo uma visão algébrica. Esse tipo de abordagem constitui a base dos métodos para a construção de códigos espaço-temporais sobre corpos e sobre anéis (Seções 4.4.1 e 4.4.2, respectivamente).

4.1 Estratégias de Codificação (Códigos sobre grupos)

Como já comentado, é de fundamental importância melhorar a capacidade e o desempenho dos sistemas de transmissão empregados em comunicações móveis. Diversas

maneiras de se resolver esse problema podem ser obtidas utilizando quadrados latinos.

Uma solução seria usar um código de repetição juntamente com alguma estratégia de combinação, tal como combinação de máxima razão (*maximal ratio combining*). Neste caso, o nível de interferência atuante em cada um dos usuários seria igual, ou muito próximo, a seu valor médio. Entretanto, haveria um desperdício de faixa.

Uma outra solução consiste em empregar, de forma combinada, codificação de canal e a técnica de embaralhamento para espalhar os bits de informação. Nesta situação, consegue-se o ganho de codificação usual (isto é, para uma determinada taxa de informação, a probabilidade de erro especificada pode ser alcançada com a menor relação sinal-ruído possível) e, além disso, dado que as relações sinal-ruído, para os sucessivos símbolos que chegam ao decodificador, são descorrelacionadas, aumenta-se a ordem da diversidade do sistema. Essa diversidade, decorrente da codificação, está diretamente relacionada com a distância mínima do código e também com o modo como é feita a sua decodificação. Assim, utilizando a métrica de decodificação apropriada, o codificador de canal faz uso da técnica da diversidade para determinar a seqüência mais provável de ter sido transmitida. Logo, a técnica de quadrados latinos pode ser entendida como uma combinação daquelas de codificação e de diversidade, fornecendo os correspondentes ganhos de codificação e de diversidade. É importante ressaltar que, ao se empregar, de maneira combinada, a codificação de canal e a técnica de quadrados latinos, obtêm-se sistemas de comunicações móveis limitados em interferência.

Já é sabido que caso se chegue a um quadrado latino, após a aplicação da técnica de recobrimento espacial baseado em reticulados, as componentes das palavras do código sobre grupos resultante sempre apresentarão valores diferentes para palavras-códigos distintas. Conseqüentemente, a diversidade de modulação do sistema de transmissão associado será máxima. Com base nesse raciocínio, estabelece-se o seguinte teorema:

Teorema 4.1.1. Dado um sistema de transmissão, que emprega uma modulação bidimensional qualquer de cardinalidade Q, a ordem da sua diversidade atingirá o seu valor máximo se, e somente se, após a aplicação da técnica de recobrimento espacial baseado em reticulados, um quadrado latino for obtido. Neste caso, o código sobre grupos gerado apresentará o melhor desempenho possível, ou seja, a menor probabilidade de erro possível quando submetido a canais puramente Gaussiano ou com desvanecimento do tipo Rayleigh ou Rice.

Caso o Teorema 4.1.1 não seja satisfeito, as palavras do código de grupo obtido apresentarão componentes iguais e, portanto, a diversidade do sistema associado não será máxima.

Com o objetivo de esclarecer a abordagem feita anteriormente, serão apresentados dois exemplos, como se segue.

Exemplo 4.1.1. Considere um sistema de comunicações que utiliza a modulação 4-PSK na transmissão. Nesta situação, caso o recobrimento espacial se baseie no reticulado $\mathbb{Z}^2$, a equação de Diofanto associada é

$$x^2 + y^2 = 4.$$

Como mostrado no Exemplo 2.2.1, o código sobre grupos obtido é $\{00, 12, 20, 32\}$, o qual é apresentado na Figura 4.1.

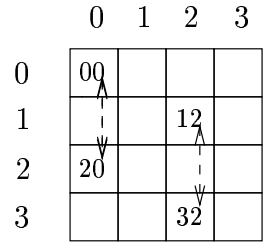

Figura 4.1: Arranjo $\mathbb{Z}_4^2$ com seus respetivos pares ordenados.

Novamente, ressalta-se que há palavras do código com componentes idênticas e, conseqüentemente, a distância de Hamming mínima entre duas palavras-códigos quaisquer (que, devido ao fato das mesmas terem duas componentes, poderia atingir um valor máximo igual a 2) é igual a 1. Logo, a ordem da diversidade desse sistema é reduzida a 1.

Exemplo 4.1.2. Admita que um dado sistema de transmisão emprega a modulação 5-PSK. Desta maneira, utilizando o reticulado $\mathbb{Z}^2$ como base no recobrimento espacial, a equação de Diofanto a ser resolvida é

$$x^2 + y^2 = 5.$$

Adotando a solução $(x, y) = (2, 1)$, obtém-se o código sobre grupos $\{00, 12, 24, 31, 43\}$, ilustrado na Figura 4.2.

	0	1	2	3	4
0	00				
1			12		
2					24
3		31			
4				43	

Figura 4.2: Arranjo $\mathbb{Z}_5^2$ com seus respetivos pares ordenados.

Neste caso, observa-se que todas as palavras-códigos apresentam componentes distintas. Portanto, a ordem da diversidade do sistema associado atinge o máximo valor permitido para quando se utiliza uma constelação bidimensional: 2.

4.2 Códigos Espaço-temporais para Canais com Desvanecimento Quasi-estático e Plano

A construção de códigos de treliça para sistemas de comunicações móveis, com modelos descritos na Seção 3.2, baseia-se nos critérios de projeto reproduzidos na Seção 3.3. Adicionalmente, deve-se considerar o fato de que, tanto no começo quanto no fim de cada quadro de transmissão, o codificador deve estar no estado zero (codificador convolucional).

Em cada instante de transmissão t, dependendo dos bits de entrada e do estado ocupado pelo codificador, uma transição específica ocorre. Cada transição é rotulada por uma seqüência de n_T sinais da constelação, denotada por $q_t^1 q_t^2 \cdots q_t^{n_T}$. Mais uma vez, enfatiza-se que a transmissão desses sinais é simultânea, sendo o sinal $q_t^i, 1 \leq i \leq n_T$, transmitido pela i-ésima antena no instante de tempo t.

No processo de decodificação, emprega-se o algoritmo de Viterbi para se determinar o caminho que possui a menor métrica acumulada. O valor da métrica para uma transição rotulada por $q_t^1 q_t^2 \cdots q_t^{n_T}$, quando o sinal y_t^j é recebido na j-ésima antena no

instante de tempo t, é expressa como

$$\sum_{j=1}^{n_R} \left| y_t^j - \sum_{i=1}^{n_T} \alpha_{ij} q_t^i \right|^2 .$$

Para tanto, assume-se que a informação a respeito do estado do canal é completamente disponível e, portanto, os ganhos de percurso $\alpha_{ij}, 1 \leq i \leq n_T, 1 \leq j \leq n_R$, são conhecidos pelo decodificador.

Sob essas condições, alguns códigos espaço-temporais foram construídos de maneira heurística [18]. Fixando valores para a taxa, o ganho de diversidade, o tamanho da constelação e a complexidade da decodificação de treliça, determinaram-se, em [18] e [19], códigos que maximizam o ganho de codificação, dado pelo critério do determinante. Resultados de simulações, apresentados em [18] e [20], comprovam o bom desempenho de tais códigos em canais com desvanecimento quasi-estatático e plano.

Entretanto, fazendo uso de um método sistemático simples, baseado na teoria de recobrimento espacial baseado em reticulados (Seção 2.2), foi possível obter esses mesmos códigos sobre grupos, quando se consideraram modulações do tipo M-PSK, com código de treliça associado apresentando M estados. Esse procedimento será inicialmente ilustrado através de alguns exemplos e, em seguida, abordado formalmente.

Exemplo 4.2.1. Como no Exemplo 4.1.1, suponha um sistema de comunicações utilizando a constelação de sinais 4-PSK para a transmissão da seqüência de dígitos na saída da fonte. Assuma que os sinais dessa constelação sejam rotulados como mostrado na Figura 4.3.

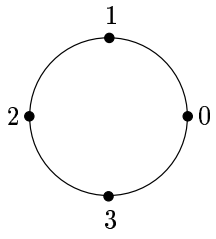

Figura 4.3: Constelação 4-PSK.

Será empregado o conceito de recobrimento espacial baseado em reticulados para se

determinar rótulos apropriados para as transições da treliça do código espaço-temporal, associado ao código de bloco resultante desse procedimento. Como o código de bloco assim obtido apresenta a maior diversidade de modulação possível, o código de treliça correspondente também possuirá essa importante característica.

Novamente, utilizando os resultados obtidos no Exemplo 2.2.1, tem-se

$$x^2 + y^2 = 4,$$

cuja solução conveniente é o par $(x, y) = (2, 1)$.

Na Figura 4.4, ilustra-se o código de bloco obtido. Como discutido no Exemplo 4.1.1, observa-se que apenas a **primeira componente** de suas palavras apresenta valores diferentes para palavras-código distintas. Conseqüentemente, a mesma será tomada como referência no rotulamento dos ramos da treliça do código espaço-temporal associado.

	0	1	2	3
0	00			
1			12	
2	20			
3			32	

Figura 4.4: Arranjo $\mathbb{Z}_4^2$ com seus respectivos pares ordenados.

Deste modo, as transições partindo do i-ésimo estado terão a primeira componente igual a i, isto é, igual à **primeira componente** da palavra-código situada na i-ésima linha do reticulado $\mathbb{Z}_4^2$. Sua segunda componente será rotulada sucessivamente com os elementos de $\mathbb{Z}_4$. Na Figura 4.5, apresenta-se a seção de treliça do código espaço-temporal correspondente.

Como os rótulos das transições desse código de treliça apresentam duas componentes, conclui-se que o sistema de comunicações considerado possui duas antenas de transmissão, onde cada uma delas é usada para transmitir uma componente dos mesmos.

Enfatiza-se o fato de que, quando um código espaço-temporal é submetido a um

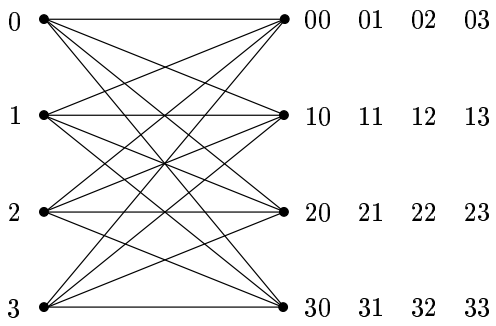

Figura 4.5: Seção de treliça do código espaço-temporal, com maior diversidade de modulação possível, associado à constelação 4-PSK.

canal apenas com ruído aditivo Gaussiano branco, emprega-se a distância de Lee como métrica e, quando o mesmo é submetido a canais com desvanecimento do tipo Rayleigh ou Rice, utiliza-se a métrica obtida em (3.1). Nestas condições, esse código espaço-temporal (trivial) apresenta um $d^2_{free} = 2$ no primeiro caso e um $d^2_{free} = 2$ na segunda situação.

Pode-se verificar que o código de treliça anteriormente obtido é linear e coincide com o apresentado em [18] e [19], onde se encontram simulações que comprovam o seu bom desempenho em canais com desvanecimento quasi-estatático e plano.

Exemplo 4.2.2. Considere um sistema de transmissão que emprega a constelação de sinais 5-PSK, como no Exemplo 4.1.2. Os elementos dessa constelação estão rotulados como ilustrado na Figura 4.6.

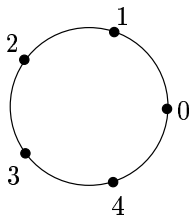

Figura 4.6: Constelação 5-PSK.

Mais uma vez, para se determinar os rótulos apropriados para as transições da treliça do código espaço-temporal associado ao código de bloco, será empregado o conceito de

recobrimento espacial baseado em reticulados. Logo, fazendo uso dos resultados obtidos no Exemplo 4.1.2, tem-se

$$x^2 + y^2 = 5 \quad \Rightarrow \quad (x, y) = (2, 1),$$

resultando no código de bloco mostrado na Figura 4.7. É importante destacar que a realização geométrica deste reliculado corresponde a um simplex, contido numa esfera em quatro dimensões.

	0	1	2	3	4
0	00				
1			12		
2					24
3		31			
4				43	

Figura 4.7: Arranjo $\mathbb{Z}_5^2$ com seus respectivos pares ordenados.

Neste caso, nota-se que todas as palavras do código apresentam componentes distintas, como já havia sido ressaltado no Exemplo 4.1.2. Portanto, a título de comparação, o rotulamento dos ramos da treliça do código espaço-temporal associado a esse código de bloco será feito de duas maneiras, como se segue.

1. Primeiramente, a primeira componente das transições partindo do i-ésimo estado assumirá um valor igual ao da **primeira componente** da palavra-código situada na i-ésima linha do arranjo $\mathbb{Z}_5^2$. A segunda componente das mesmas será rotulada sucessivamente com os elementos de $\mathbb{Z}_5$. A seção de treliça do código espaço-temporal associado é apresentada na Figura 4.8. apresenta um $d_{free}^2 = 2$ quando submetido a um canal com ruído puramente aditivo Gaussiano e um $d_{free}^2 = 2$ quando submetido a canais com desvanecimento do tipo Rayleigh ou Rice.

2. Agora, o rótulo dos ramos que partem do i-ésimo estado terão a primeira componente igual à **segunda componente** da palavra-código situada na i-ésima linha

do reticulado $\mathbb{Z}_5^2$. Mais uma vez, a sua segunda componente será rotulada sucessivamente com os elementos de $\mathbb{Z}_5$. Na Figura 4.9, ilustra-se a seção de treliça do código espaço-temporal correspondente. Neste caso, quando submetido a um canal com ruído puramente aditivo Gaussiano, esse código espaço-temporal apresenta um $d^2_{free} = 3$ e, quando submetido a canais com desvanecimento do tipo Rayleigh ou Rice, o mesmo apresenta um $d^2_{free} = 5$. Logo, o seu desempenho é superior ao do código trivial obtido no item 1.

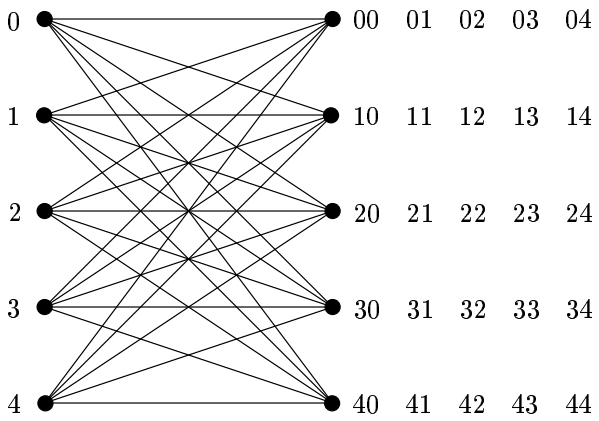

Figura 4.8: Seção de treliça de um código espaço-temporal, com maior diversidade de modulação possível, associado à constelação 5-PSK (item 1).

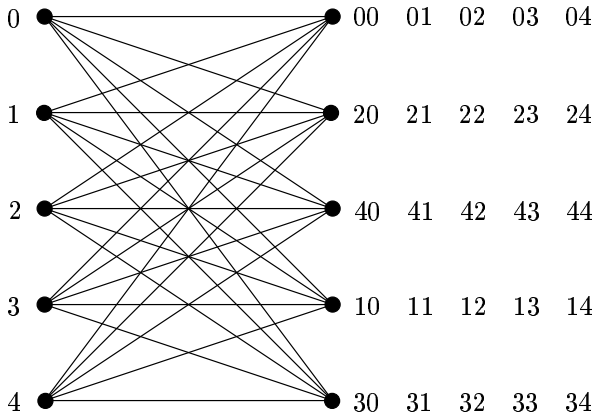

Figura 4.9: Seção de treliça de um código espaço-temporal, com maior diversidade de modulação possível, associado à constelação 5-PSK (item 2).

Novamente, como os rótulos das transições desses códigos de treliça apresentam duas componentes, conclui-se que o sistema de comunicações considerado possui duas antenas de transmissão.

A seguir, com base no Teorema 4.1.1 e nas observações feitas nos exemplos anteriores, enuncia-se um método para se obter códigos espaço-temporais (códigos sobre grupos) quando sujeitos a canais com desvanecimento quasi-estático e plano.

4.3 Método Sistemático para a construção de Códigos Espaço-temporais (Códigos de Grupo) para Canais com Desvanecimento Quasi-estático e Plano

Considerando um sistema de transmissão, que emprega uma modulação bidimensional qualquer de cardinalidade Q, o seguinte procedimento determina um código de treliça espaço-temporal ótimo (códigos sobre grupos) a ele associado:

Passo 1: Aplicar a técnica de recobrimento espacial baseado em reticulados e, assim, obter o código de bloco com maior ordem de diversidade possível. Caso, como resultado desse procedimento, se obtenha um quadrado latino, ir para o Passo 3; caso contrário, ir para o Passo 2.

Passo 2: Rotular as transições da treliça do código espaço-temporal da seguinte maneira: aquelas partindo do i-ésimo estado terão a primeira componente igual a i, isto é, igual à **primeira componente** da palavra-código situada na i-ésima linha do reticulado correspondente; a sua segunda componente será rotulada sucessivamente com os elementos de $\mathbb{Z}_Q$. O código assim construído sempre resultará no trivial, o qual apresenta um $d^2_{free} = 2$ quando submetido a um canal com ruído puramente aditivo Gaussiano e um $d^2_{free} = 2$ quando submetido a canais com desvanecimento do tipo Rayleigh ou Rice.

Passo 3: Os ramos da treliça do código espaço-temporal serão rotulados do seguinte modo: os que partem do i-ésimo estado terão a primeira componente igual

à **segunda componente** da palavra-código situada na i-ésima linha do reticulado associado; a sua segunda componente será rotulada sucessivamente com os elementos de $\mathbb{Z}_Q$. Nesta situação, o código obtido difere do trivial. Quando submetido a um canal com ruído puramente aditivo Gaussiano, tal código apresenta um $d^2_{free} > 2$ e, quando submetido a canais com desvanecimento do tipo Rayleigh ou Rice, o mesmo apresenta um $d^2_{free} > 2$. Ou seja, o código resultante sempre apresentará um desempenho superior ao do seu correpondente trivial.

O método aqui apresentado para a construção de códigos espaço-temporais (códigos sobre grupos) faz uso da teoria de recobrimento espacial baseado em reticulados bidimensionais. Entretanto, seguindo um raciocínio análogo, é possível construir tais códigos empregando a teoria de recobrimento espacial baseado em reticulados de dimensão superior a dois.

Para elucidar o método acima de obtenção de códigos espaço-temporais (códigos sobre grupos), considere os seguintes exemplos.

Exemplo 4.3.1. Suponha que certo sistema de comunicações utiliza a constelação 8-PSK na sua transmissão. Considere que o rotulamento dos sinais dessa constelação é feito de acordo com a Figura 4.10.

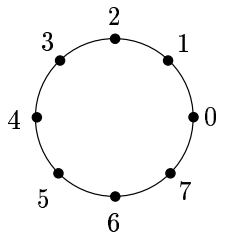

Figura 4.10: Constelação 8-PSK.

Seguindo o procedimento anteriormente apresentado e baseando o recobrimento espacial no reticulado $\mathbb{Z}^2$, deve-se resolver a equação

$$x^2 + y^2 = 8$$

e, assim, determinar o código de bloco com maior ordem de diversidade possível.

A solução conveniente da equação acima é o par $(x, y) = (3, 1)$, a qual fornece o código de bloco mostrado na Figura 4.11.

	0	1	2	3	4	5	6	7
0	00							
1				13				
2							26	
3		31						
4					44			
5								57
6			62					
7						75		

Figura 4.11: Arranjo $\mathbb{Z}_8^2$ com seus respectivos pares ordenados.

Uma vez que se obteve um quadrado latino, o Passo 3 desse procedimento deve ser realizado. Portanto, a **segunda componente** das palavras $\{00, 13, 26, 31, 44, 57, 62, 75\}$ será usada como referência no rotulamento dos ramos da treliça do código espaço-temporal associado. Na Figura 4.12, apresenta-se a seção de treliça de tal código.

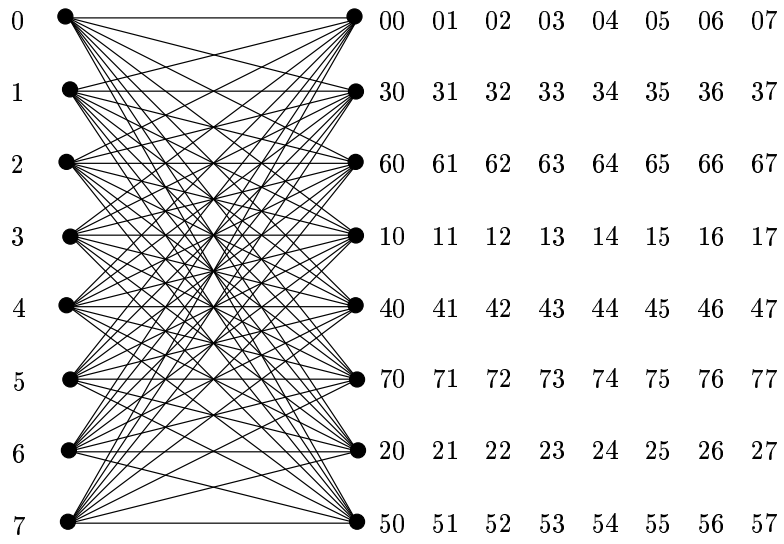

Figura 4.12: Seção de treliça do código espaço-temporal, com maior diversidade de modulação possível, associado à constelação 8-PSK.

Esse código espaço-temporal, quando submetido a um canal com ruído puramente aditivo Gaussiano, apresenta um $d^2_{free} = 4$ e, quando submetido a canais com desvanecimento do tipo Rayleigh ou Rice, o mesmo apresenta um $d^2_{free} = 10$.

Pode-se verificar que essa seção de treliça coincide com aquelas apresentadas em [18] e [19].

Exemplo 4.3.2. Considere um sistema de transmissão empregando a constelação 9-PSK, cujos elementos estão rotulados como ilustrado na Figura 4.13.

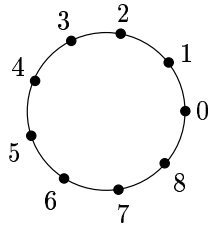

Figura 4.13: Constelação 9-PSK.

Novamente, fazendo uso do procedimento apresentado anteriormente e considerando que o recobrimento espacial baseia-se no reticulado $\mathbb{Z}^2$, a equação de Diofanto

$$x^2 + y^2 = 9$$

deve ser resolvida para se determinar o código de bloco com maior ordem de diversidade possível.

A solução conveniente dessa equação é o par $(x, y) = (3, 1)$, resultando no código de bloco mostrado na Figura 4.14.

Neste caso, não se obteve um quadrado latino e, portanto, o próximo passo desse procedimento a ser realizado é o Passo 2. Logo, no rotulamento das transições da treliça do código espaço-temporal associado, a **primeira componente** das palavras $\{00, 13, 26, 30, 43, 56, 60, 73, 86\}$ será utilizada como referência . Na Figura 4.15, ilustra-se a seção de treliça de tal código.

Como já era esperado, esse código espaço-temporal obtido é o trivial. Deste modo, o mesmo apresenta um $d^2_{free} = 2$ quando submetido a um canal com ruído puramente

	0	1	2	3	4	5	6	7	8
0	00								
1				13					
2							26		
3	30								
4				43					
5							56		
6	60								
7				73					
8							86		

Figura 4.14: Arranjo $\mathbb{Z}_9^2$ com seus respectivos pares ordenados.

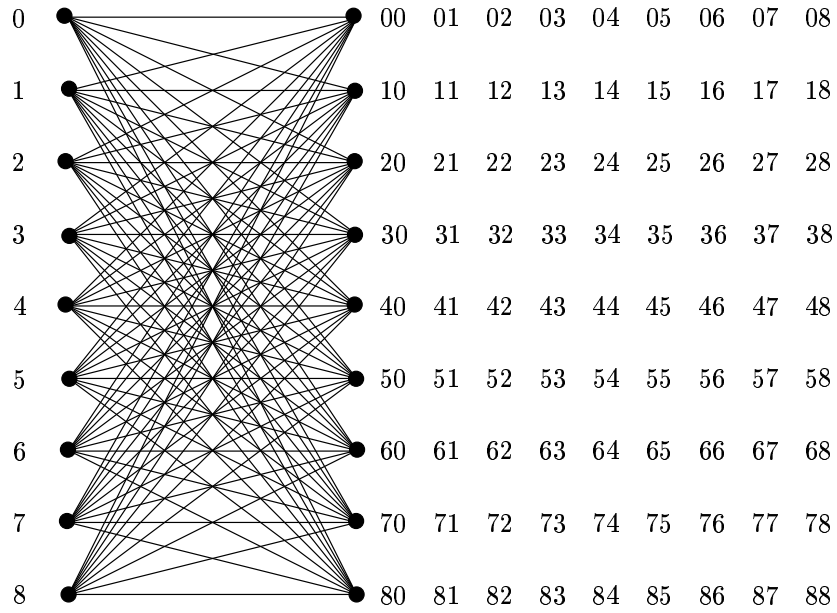

Figura 4.15: Seção de treliça do código espaço-temporal, com maior diversidade de modulação possível, associado à constelação 9-PSK.

aditivo Gaussiano e um $d_{free}^2 = 2$ quando submetido a canais com desvanecimento do tipo Rayleigh ou Rice.

Em todos os exemplos apresentados sobre a construção de códigos espaço-temporais, o recobrimento espacial baseou-se no reticulado $\mathbb{Z}^2$. Logo, faz-se oportuno exemplificar a obtenção desses códigos utilizando o recobrimento espacial baseado em reticulados distintos do $\mathbb{Z}^2$. Neste contexto, considere os seguintes exemplos.

Exemplo 4.3.3. Admita um sistema de comunicações que emprega, na sua transmissão, a constelação 7-PSK, sendo os seus sinais rotulados como mostrado na Figura 4.16.

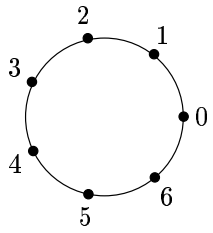

Figura 4.16: Constelação 7-PSK.

A técnica de recobrimento espacial será baseada no reticulado A_2. Logo, utilizando os resultados obtidos no Exemplo 2.2.2, tem-se

$$x^2 + xy + y^2 = 7 \quad \Rightarrow \quad (x, y) = (2, 1).$$

Aplicando essa solução a um dado ponto inicial, obtém-se o código de bloco ilustrado na Figura 4.17.

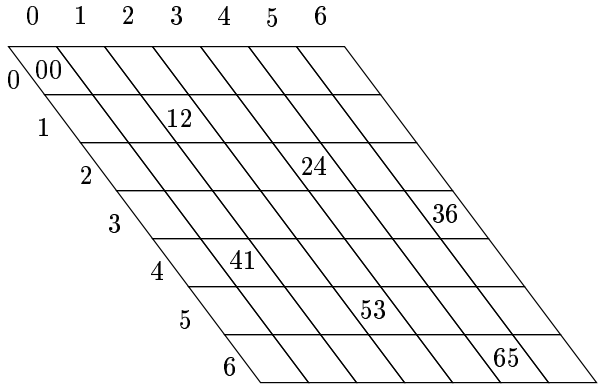

Figura 4.17: Reticulado A_2 com 49 elementos e seus respetivos pares ordenados.

Como já comentado no Exemplo 2.2.2, esse reticulado A_2 é caracterizado por um quadrado latino. Portanto, seguindo o procedimento apresentado anteriormente, a **segunda componente** das palavras $\{00, 12, 24, 36, 41, 53, 65\}$ será utilizada como referência no rotulamento das transições da treliça do código espaço-temporal associado. Na Figura 4.18, apresenta-se a seção de treliça de tal código.

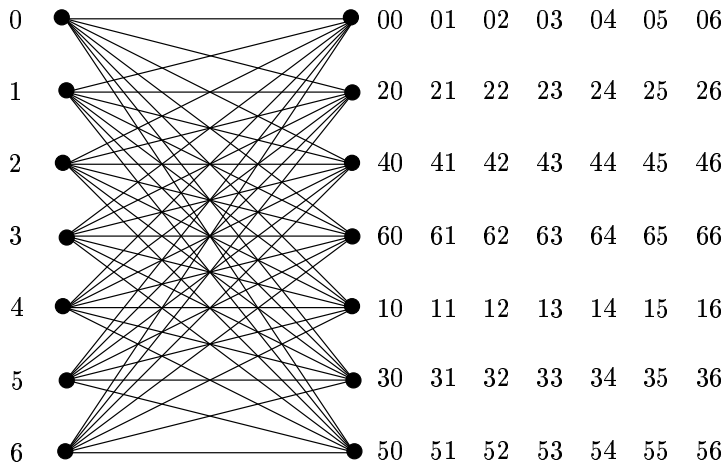

Figura 4.18: Seção de treliça do código espaço-temporal, com maior diversidade de modulação possível, associado à constelação 7-PSK.

Quando submetido a um canal com ruído puramente aditivo Gaussiano, esse código espaço-temporal apresenta um $d^2_{free} = 3$ e, quando submetido a canais com desvanecimento do tipo Rayleigh ou Rice, o mesmo apresenta um $d^2_{free} = 5$.

Exemplo 4.3.4. Similarmente ao Exemplo 4.2.2, suponha um sistema de trasmissão que emprega a constelação de sinais 5-PSK, cujos elementos estão rotulados como ilustrado na Figura 4.19.

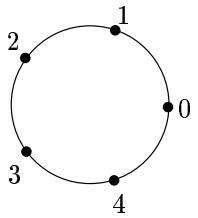

Figura 4.19: Constelação 5-PSK.

Entretanto, neste caso, o recobrimento espacial será baseado no reticulado $\mathbb{Z}^3$. Assim, a equação de Diofanto

$$x^2 + y^2 + z^2 = 5$$

deve ser resolvida para se determinar o código de bloco com maior ordem de diversidade possível.

A solução conveniente para essa equação é a tripla $(x, y, z) = (2, 1, 1)$, a qual fornece o código de bloco $\{000, 121, 242, 313, 434\}$. Este arranjo corresponde a cinco planos $\mathbb{Z}_5^2$ paralelos, cada um deles contendo uma única palavra do código de bloco obtido no Exemplo 4.2.2. Deste modo, este reticulado é caracterizado como um quadrado latino e, portanto, a ordem de diversidade do sistema em consideração é igual a 3.

Neste caso, o rotulamento dos ramos da treliça do código espaço-temporal correspondente será feito baseado na **segunda componente** das palavras do código de bloco. Na Figura 4.20, apresenta-se a seção de treliça de tal código espaço-temporal.

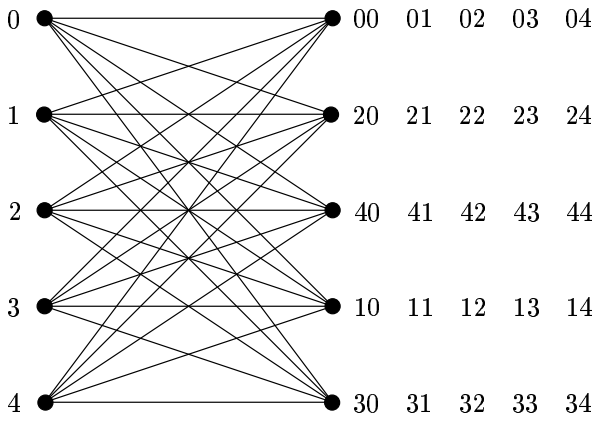

Figura 4.20: Seção de treliça do código espaço-temporal, com maior diversidade de modulação possível, associado à constelação 5-PSK.

Esse código apresenta um $d^2_{free} = 3$ quando submetido a um canal com ruído puramente aditivo Gaussiano e um $d^2_{free} = 5$ quando submetido a canais com desvanecimento do tipo Rayleigh ou Rice.

Um problema crucial na teoria de códigos convolucionais tem sido encontrar um método para caracterizar, de maneira eficaz, a distância livre de um dado código convolucional. Estreitamente relacionado a esse problema, há a tarefa de projetar, uma vez estabelecidas a taxa e a complexidade, códigos bons que apresentem uma distância livre boa. Atualmente, talvez a técnica mais eficaz de se fazer isso seja buscar exaustivamente uma classe de códigos determinados a partir do pré-estabelecimento das taxa e complexidade desejadas e, então, calcular a distância livre dos codificadores pertencentes a essa classe, até que se encontre um código cuja distância livre atinja o valor máximo permitido ou esteja próxima a esse valor. Obviamente, essa técnica tem as suas limitações.

Têm-se pesquisado vários métodos para se construir códigos convolucionais. Talvez, a técnica mais popular seja relacionar os geradores de um código convolucional àqueles de algum código cíclico (ou quase cíclico) e, posteriormente, mostrar que a distância desse código cíclico consiste num limitante inferior para a distância livre do código convolucional. Pode-se também restringir-se à classe de códigos convolucionais sobre o corpo de Galois $GF(q)$ com taxa $r = \frac{1}{n}$ e, então, desenvolver técnicas eficazes para a construção de tais códigos.

Neste sentido, os códigos convolucionais M-ários, introduzidos na Seção 2.4, serão reapresentados a seguir, segundo uma abordagem algébrica. De fato, duas linhas convergentes de pesquisa provocaram o interesse pelo tratamento algébrico dos códigos convolucionais. Primeiramente, o sucesso obtido na geração de códigos de bloco bons, empregando métodos algébricos, indicavam que métodos construtivos de geração de códigos convolucionais bons, baseados em estruturas algébricas, deveriam ser desenvolvidos. Além disso, a utilidade de abordar os códigos convolucionais como circuitos seqüênciais lineares tornou-se evidente. Na observação de Omura e de outros pesquisadores, por exemplo, o algoritmo de decodificação por máxima verossimilhança de Viterbi é, na verdade, uma solução de programação dinâmica para um determinado problema de controle e, na observação de Massey, certas questões relativas à propagação de erro estão relacionadas a questões relativas à inversibilidade de sistemas lineares [8]. Como a teoria de sistemas lineares de dimensões finitas é essencialmente algébrica, tem-se outro motivo para examinar os códigos convolucionais num contexto algébrico.

4.4 Códigos Convolucionais M-ários: Uma Visão Algébrica

Na Subseção 2.4.1, os códigos convolucionais M-ários foram definidos segundo uma abordagem essencialmente binária. De fato, o aspecto do codificador mostrado na Figura 2.5 é idêntico ao do binário com taxa $r = \frac{1}{\log_2 M}$. Nesta subseção, redefinem-se tais códigos num contexto algébrico, fazendo uso de polinômios com coeficientes M-ários. Ressalta-se que, a partir deste ponto desta dissertação, por questão de uniformidade de notação, o parâmetro M será substituído por q.

Um codificador convolucional q-ário geral com taxa $r = 1$ e comprimento de restrição $K = m + 1$ é redesenhado na Figura 4.21.

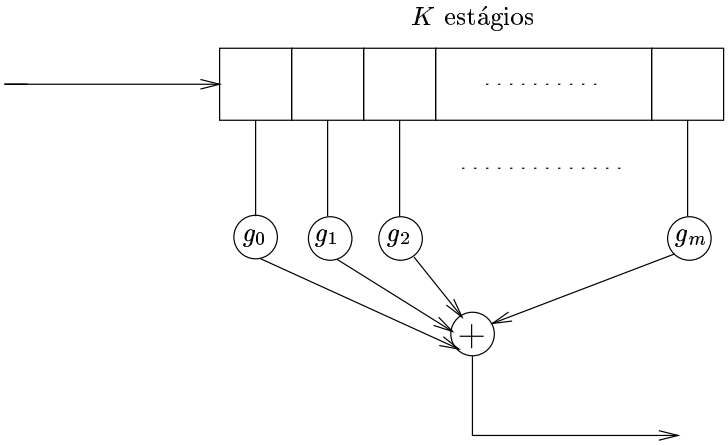

Figura 4.21: Codificador convolucional algébrico.

Os símbolos de entrada são binários e a operação realizada por esse codificador coincide com aquela efetuada pelo codificador da Figura 2.5. Os coeficientes $g_0, g_1, \ldots, g_m$ estão no corpo de Galois $GF(q)$, onde q é uma potência de 2.

Seja $u_0, u_1, u_2, \ldots$ a seqüência de entrada e defina o polinômio de entrada

$$U(x) = u_0 + u_1 x + u_2 x^2 + \ldots .$$

Para cada entrada binária, gera-se um símbolo-código q-ário na saída do codificador

convolucional. Seja $v_0, v_1, v_2, \ldots$ a seqüência de saída e defina o polinômio-código

$$V(x) = v_0 + v_1 x + v_2 x^2 + \ldots .$$

Com base na Figura 4.21, os símbolos-código são dados por

$$\begin{aligned} v_0 &= u_0 g_0, \\ v_1 &= u_0 g_1 + u_1 g_0, \\ &\vdots \\ v_k &= u_{k-m} g_m + u_{k-m+1} g_{m-1} + \ldots + u_k g_0, \end{aligned}$$

ou, de uma maneira mais geral,

$$V(x) = U(x)G(x),$$

onde $G(x)$, o polinômio gerador do código convolucional q-ário, é definido como

$$G(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_m x^m.$$

Para se conseguir códigos convolucionais q-ários bons, o polinômio gerador $G(x)$ não pode ser escolhido arbitrariamente. Isto porque certas escolhas geram códigos que apresentam propagação catastrófica de erros. Neste caso, um número finito de erros na transmissão faz com que o decodificador cometa um número infinito de erros. Em termos dos polinômios definidos anteriormente, isto significa que um polinômio de entrada infinito produz um polinômio-código finito. Conseqüentemente, para que um código convolucional q-ário não seja catastrófico, o seu polinômio gerador não deve conter fator binário. Por exemplo, suponha $G(x) = B(x)Q(x)$, onde $B(x)$ é binário e $Q(x)$ é q-ário. Assim, o polinômio binário de entrada infinito $U(x) = A(x)/B(x)$, onde $A(x)$ é um polinômio binário finito qualquer, gera o polinômio código $V(x) = Q(x)A(x)$, que é finito.

A utilidade da definição desses polinômios reside na construção do código convolucional q-ário. Note que se $G(x)$ divide $x^n - 1$, então $V(x)$ reduzido módulo $(x^n - 1)$ define uma palavra-código de um código de bloco cíclico q-ário com parâmetros $(n, n-m)$.

Esse fato pode ser utilizado para provar a relação existente entre códigos de bloco cíclicos com uma dada distância mínima e códigos convolucionais com taxa 1 e com uma determinada distância livre.

No contexto desta seção, a distância livre de um código é definida como

$$d_{free} = \min_{\substack{V(x)=U(x)G(x) \\ u_0=1}} \{W[V(x)]\},$$

onde $W[\cdot]$ denota o número de coeficientes não-nulos (ou peso) do polinômio argumento.

Teorema 4.4.1. [15] Suponha que $g(x)$ gere um código de bloco cíclico q-ário com parâmetros $(n, n-m, d)$. Se $g(x)$ não contém fator binário, então $G(x) = g(x)$ gera um código convolucional q-ário não-catastrófico com taxa $r = 1$, comprimento de restrição $K = m + 1$ e distância livre $d_{free} = d$.

Corolário 4.4.1. [15] Para códigos convolucionais com taxa $r = 1$, construídos a partir de códigos de bloco cíclicos com parâmetros $(n, n-m)$, pelo menos uma palavra-código com peso d_{free} é produzida por uma seqüência de entrada com comprimento menor ou igual a $n - m$.

O Teorema 4.4.1 provê uma técnica bem definida para se construir códigos convolucionais q-ários com taxa 1. A seguir, será abordada a construção de tais códigos a partir de códigos cíclicos com máxima distância de separação. Esses códigos, com parâmetros $(n, n-m)$, têm a propriedade de apresentar uma distância $d = m + 1$. Os códigos convolucionais q-ários, construídos a partir desses códigos, possuirão uma distância livre com máximo valor, isto é, $d_{free} = K$. Os códigos Reed-Solomon (RS) sobre o corpo $GF(q)$, com comprimento $q - 1$, constituem uma classe bem conhecida de códigos com máxima distância de separação. Os códigos não-binários BCH sobre o corpo $GF(q)$, com comprimento $q+1$, também exibem máxima distância de separação. Os seguintes exemplos, relativos à construção de códigos convolucionais com máximo valor para a distância livre, baseiam-se em códigos RS e BCH.

Exemplo 4.4.1. Considere a construção de códigos convolucionais 4-ários sobre o corpo $GF(4)$. Logo, $q = 2^2$. Para tanto, deve-se primeiramente determinar o polinômio gerador de um código de bloco cíclico 4-ário. Ressalta-se que esse polinômio não deve conter fator binário (Teorema 4.4.1).

O corpo de Galois $GF(4)$ é formado pelas classes residuais de polinômios em $GF(2)[x]$ módulo x^2+x+1, ou seja

$$\begin{aligned} GF(4) \cong \frac{GF(2)[x]}{< x^2+x+1 >} &= \{a+bx;\ a,b \in GF(2)\} \\ &= \{0, 1, x, 1+x\} \end{aligned}$$

Seja α um elemento primitivo em $GF(4)$. Logo, α é uma raiz de x^2+x+1 ou, em outras palavras

$$\alpha^2+\alpha+1=0 \quad \Rightarrow \quad \alpha^2 = -1-\alpha = 1+\alpha,$$

onde essas operações são realizadas em $GF(2)$.

Desta maneira, $GF(4)$ apresenta os seguintes elementos:

$$\begin{aligned} &0 \\ &1 \\ &\alpha \\ &\alpha^2 = 1+\alpha \end{aligned}$$

Os polinômios minimais associados a esses elementos são:

Elementos		Polinômio minimal
1	$\longleftrightarrow$	$(x+1)$
α, α^2	$\longleftrightarrow$	$(x+\alpha)(x+\alpha^2) = x^2+x+1$

onde

$$x^3-1 = (x+1)(x+\alpha)(x+\alpha^2).$$

- **Códigos RS:**
  Neste caso, o código cíclico tem comprimento $n = q-1 = 4-1 = 3$ (exatamente igual ao número de elementos não-nulos do corpo $GF(q)$). O valor da distância d do código é definido como sendo igual ao número de fatores consecutivos de $g(x)$ (fatores com potências consecutivas do elemento primitivo) mais 1. Conseqüentemente, o polinômio gerador deve possuir o maior número de fatores consecutivos

(em termos das potências de α) dos polinômios minimais, sem contudo conter um polinômio minimal completo (fator binário). Logo, os possíveis geradores para esse código são:

1. $g(x) = (x+\alpha)$. Nesta situação, $d = 2$. O código convolucional 4-ário associado apresenta uma distância livre $d_{free} = K = 2$ e o seu codificador é mostrado na Figura 4.22.

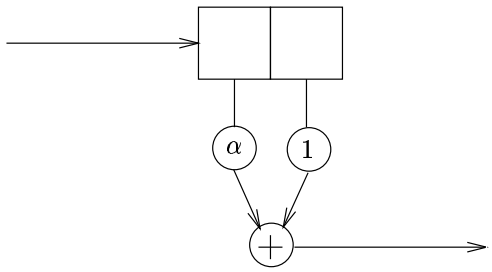

Figura 4.22: Codificador convolucional 4-ário, construído a partir de um código RS (código sobre corpo).

2. $g(x) = (x + \alpha^2)$. Neste caso, $d = 2$. Na Figura 4.23, ilustra-se o código convolucional 4-ário correspondente, cuja distância livre é $d_{free} = K = 2$.

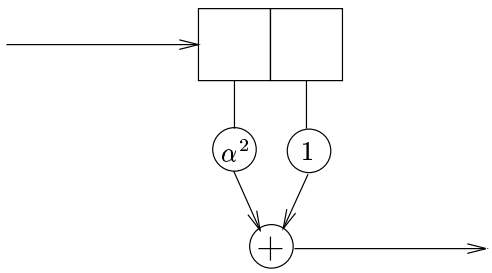

Figura 4.23: Codificador convolucional 4-ário, construído a partir de um código RS (código sobre corpo).

- **Códigos BCH:**
  Nesta situação, o código tem comprimento $n = q+1 = 4+1 = 5$. Como n é maior que o número de elementos não-nulos do corpo $GF(q)$, é necessário procurar um grupo multiplicativo de ordem n, em alguma extensão desse corpo. Assim, seja β um elemento primitivo de $GF\,(4^2 = 16)$, extensão de grau 2 de $GF(4)$. Então, $\gamma = \beta^3$ gera um subgrupo cíclico de ordem 5, como desejado. Os polinômios minimais associados a cada um dos cinco elementos deste grupo multiplicativo são (vide Observação 4.4.1, a seguir):

Elementos		Polinômio minimal
1	$\longleftrightarrow$	$(x+1)$
γ, γ^4	$\longleftrightarrow$	$(x+\gamma)(x+\gamma^4) = x^2+\alpha x+1$
γ^2, γ^3	$\longleftrightarrow$	$(x+\gamma^2)(x+\gamma^3) = x^2+\alpha^2 x+1$

  O polinômio gerador de códigos BCH é definido da seguinte maneira. Suponha que se deseja construir um código BCH com distância $d = \iota + 1$, de modo que $\gamma^{\lambda_1}, \gamma^{\lambda_2}, \ldots, \gamma^{\lambda_\iota}$ são raízes de $g(x)$. Então, esse polinômio é definido como

$$g(x) = mmc\{M_{\lambda_1}(x), M_{\lambda_2}(x), \ldots, M_{\lambda_\iota}(x)\},$$

  onde $M_i(x)$ corresponde ao polinômio minimal associado ao elemento γ^{λ_i}. Mais uma vez, enfatiza-se que esse polinômio não pode conter fator binário.

  Logo,

$$g(x) = (x+\gamma)(x+\gamma^2)(x+\gamma^3)(x+\gamma^4)$$

  gera um código BCH com distância $d = 5$. O código convolucinal 4-ário correspondente, gerado por

$$G(x) = x^4 + x^3 + \alpha^3 x^2 + x + 1,$$

  apresenta uma distância livre igual a $d_{free} = K = 5$. O seu codificador é mostrado na Figura 4.24.

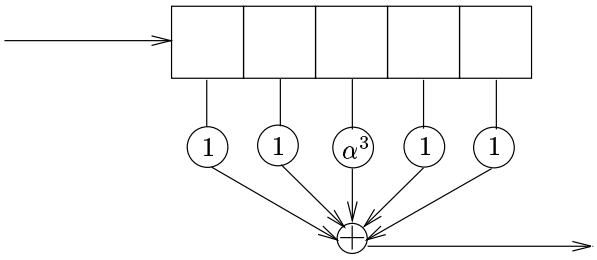

Figura 4.24: Codificador convolucional 4-ário, construído a partir de um código BCH (código sobre corpo).

Observação 4.4.1. Já é sabido que $GF(16)$ pode ser obtido a partir de uma extensão de grau 2 de $GF(4)$. Entretanto, qual a relação existente entre os elementos desses dois corpos de Galois?

O corpo $GF(16)$ também pode ser formado pelas classes residuais de polinômios em $GF(2)[x]$ módulo $x^4 + x^3 + 1$, isto é

$$GF(16) \cong \frac{GF(2)[x]}{< x^4 + x^3 + 1 >} = \{a + bx + cx^2 + dx^3;\ a, b, c, d \in GF(2)\}.$$

Novamente, seja β um elemento primitivo em $GF(16)$. Portanto, β é uma raiz de $x^4 + x^3 + 1$, ou seja

$$\beta^4 + \beta^3 + 1 = 0 \quad \Rightarrow \quad \beta^4 = -1 - \beta^3 = 1 + \beta^3,$$

onde essas operações são realizadas em $GF(2)$.

Logo, os elementos de $GF(16)$ são:

0		
1	$\beta^5 = 1 + \beta + \beta^3$	$\beta^{10} = \beta + \beta^3$
β	$\beta^6 = 1 + \beta + \beta^2 + \beta^3$	$\beta^{11} = 1 + \beta^2 + \beta^3$
β^2	$\beta^7 = 1 + \beta + \beta^2$	$\beta^{12} = 1 + \beta$
β^3	$\beta^8 = \beta + \beta^2 + \beta^3$	$\beta^{13} = \beta + \beta^2$
$\beta^4 = 1 + \beta^3$	$\beta^9 = 1 + \beta^2$	$\beta^{14} = \beta^2 + \beta^3$

Do corpo de Galois $GF(16)$, é possível extrair um grupo multiplicativo de ordem 3 e associar os seus elementos àqueles do grupo multiplicativo de $GF(4)$. Deste modo, pode-se estabelecer um mapeamento entre os elementos dos corpos $GF(4)$ e $GF(16)$:

Elemento de $GF(4)$		Elemento de $GF(16)$
0	$\longleftrightarrow$	0
1	$\longleftrightarrow$	1
α	$\longleftrightarrow$	β^5
α^2	$\longleftrightarrow$	β^{10}

Com base na representação binária dos elementos de $GF(16)$, no mapeamento acima e tendo em mente que $\gamma = \beta^3$ é o gerador de um subgrupo cíclico de $GF(16)$ de ordem 5, é possível escrever:

$$(x+\gamma)(x+\gamma^4) = x^2 + (\beta^3 + \beta^{12})x + 1 = x^2 + \alpha x + 1$$

e

$$(x+\gamma^2)(x+\gamma^3) = x^2 + (\beta^6 + \beta^9)x + 1 = x^2 + \alpha^2 x + 1.$$

Exemplo 4.4.2. Considere a construção de códigos convolucionais 8-ários sobre $GF(8)$. Logo, $q = 2^3$. Mais uma vez, deve-se determinar inicialmente o polinômio gerador de um código de bloco cíclico 8-ário. Será seguido um raciocínio análogo ao do exemplo anterior.

O corpo de Galois $GF(8)$ é formado pelas classes residuais de polinômios em $GF(2)[x]$ módulo $x^3 + x + 1$, ou seja

$$\begin{aligned} GF(8) \cong \frac{GF(2)[x]}{< x^3 + x + 1 >} &= \{a + bx + cx^2;\ a, b, c \in GF(2)\} \\ &= \{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}. \end{aligned}$$

Seja α um elemento primitivo em $GF(8)$. Assim, α é uma raiz de $x^3 + x + 1$, isto é

$$\alpha^3 + \alpha + 1 = 0 \quad \Rightarrow \quad \alpha^3 = -1 - \alpha = 1 + \alpha,$$

onde essas operações são realizadas em $GF(2)$.

Logo, $GF(8)$ apresenta os seguintes elementos:

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

Os polinômios minimais associados a esses elementos são:

Elementos		Polinômio minimal
1	$\longleftrightarrow$	$(x+1)$
$\alpha, \alpha^2, \alpha^4$	$\longleftrightarrow$	$(x+\alpha)(x+\alpha^2)(x+\alpha^4) = x^3 + x + 1$
$\alpha^3, \alpha^6, \alpha^5$	$\longleftrightarrow$	$(x+\alpha^3)(x+\alpha^6)(x+\alpha^5) = x^3 + x^2 + 1$

onde

$$x^7 - 1 = (x+1)(x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6).$$

- **Códigos RS:**
  Neste caso, o código cíclico tem comprimento $n = q - 1 = 8 - 1 = 7$. Para que esse código apresente a maior distância possível, o seu polinômio gerador será

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

  Logo, o código convolucional 8-ário associado é gerado por

  $$G(x) = x^4 + \alpha^4 x^3 + \alpha^2 x^2 + \alpha^4 x + 1,$$

  apresentando uma distância livre $d_{free} = K = 5$. Na Figura 4.25, ilustra-se o seu codificador.

- **Códigos BCH:**
  Neste caso, o código tem comprimento $n = q + 1 = 8 + 1 = 9$. Mais uma vez, deve-se procurar um grupo multiplicativo de ordem 9, numa extensão de $GF(8)$.

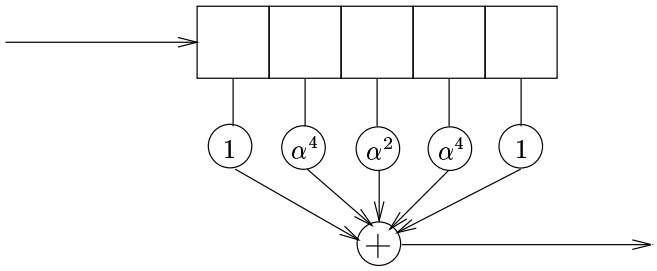

Figura 4.25: Codificador convolucional 8-ário, construído a partir de um código RS (código sobre corpo).

Desta maneira, seja β um elemento primitivo de $GF\,(8^2 = 64)$. Logo, $\gamma = \beta^7$ gera um subgrupo cíclico de ordem 9. Os polinômios minimais associados aos elementos deste grupo multiplicativo são:

Elementos		Polinômio minimal
1	$\longleftrightarrow$	$(x+1)$
γ, γ^8	$\longleftrightarrow$	$(x+\gamma)(x+\gamma^8) = x^2 + \alpha^5 x + 1$
γ^2, γ^7	$\longleftrightarrow$	$(x+\gamma^2)(x+\gamma^7) = x^2 + \alpha^3 + 1$
γ^3, γ^6	$\longleftrightarrow$	$(x+\gamma^3)(x+\gamma^6) = x^2 + x + 1$
γ^4, γ^5	$\longleftrightarrow$	$(x+\gamma^4)(x+\gamma^5) = x^2 + \alpha^6 x + 1$

Para que esse código apresente a maior distância possível, considerando que o seu polinômio gerador não pode conter fator binário, tem-se

$$g(x) = (x+\gamma^4)(x+\gamma^5).$$

Assim,

$$G(x) = x^2 + \alpha^6 x + 1$$

gera o código convolucional 8-ário associado, o qual apresenta uma distância livre $d_{free} = K = 3$. O seu codificador é mostrado na Figura 4.26.

A seguir, com base nos dois exemplos anteriores, enuncia-se um método para se

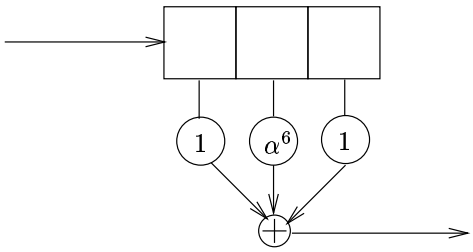

Figura 4.26: Codificador convolucional 8-ário, construído a partir de um código RS (código sobre corpo).

obter códigos espaço-temporais (códigos sobre corpos).

4.4.1 Método Sistemático para a construção de Códigos Espaço-temporais (Códigos sobre Corpos)

O seguinte procedimento permite construir códigos de treliça espaço-temporais sobre um dado corpo $GF(q)$, onde $q = 2^\kappa$:

Para se obter códigos espaço-temporais sobre $GF(q)$ (códigos convolucionais q-ários sobre $GF(q)$), deve-se inicialmente determinar o polinômio gerador de um código de bloco cíclico q-ário. Sabendo que o corpo de Galois $GF\left(2^\kappa\right)$ é formado pelas classes residuais de polinômios em $GF(2)[x]$ módulo um ideal primitivo de grau κ, também pertencente a $GF(2)[x]$, suponha que α seja um elemento primitivo no corpo em questão. Portanto, α é uma raiz do polinômio gerador desse ideal. Conseqüentemente, é possível expressar uma dada potência de α em função de outras menores, ferramenta essencial para se determinar os elementos do corpo $GF\left(2^\kappa\right)$ (ou seja: $0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^\kappa - 2}$). Ressalta-se que as operações devem ser realizadas em $GF(2)$. É importante enfatizar que o termo $x^{2^\kappa - 1} - 1$ pode ser fatorado como

$$x^{2^\kappa - 1} - 1 = (x + 1)(x + \alpha)(x + \alpha^2) \cdots (x + \alpha^{2^\kappa - 2}).$$

Determinados os polinômios minimais associados a cada um dos $2^\kappa - 1$ elementos do grupo multiplicativo de $GF\left(2^\kappa\right)$, pode-se definir o polinômio gerador do código de bloco cíclico, o qual, caso não contenha fator binário, concidirá com aquele do código

convolucional q-ário (código espaço-temporal ótimo sobre $GF(q)$).

Caso a construção do código espaço-temporal se baseie em códigos Reed-Solomon, deve-se escolher o maior número de fatores consecutivos (em termos das potências de α) dos polinômios minimais para compor o seu polinômio gerador, sem contudo selecionar um polinômio minimal completo (fator binário).

Caso a construção do código espaço-temporal se baseie em códigos BCH, deve-se procurar um grupo multiplicativo de ordem $q+1$, em alguma extensão do corpo $GF(q)$. Seja γ um elemento primitivo desse subgrupo cíclico e suponha que se deseja construir um código BCH com distância $d = \iota + 1$, de modo que $\gamma^{\lambda_1}, \gamma^{\lambda_2}, \ldots, \gamma^{\lambda_\iota}$ são raízes de $g(x)$. Então, o polinômio gerador desse código (e, conseqüentemente, do código espaço-temporal) é definido como

$$g(x) = mmc\{M_{\lambda_1}(x), M_{\lambda_2}(x), \ldots, M_{\lambda_\iota}(x)\},$$

onde $M_i(x)$ corresponde ao polinômio minimal associado ao elemento γ^{λ_i}. Mais uma vez, enfatiza-se que esse polinômio não pode conter fator binário.

O código espaço-temporal ótimo sobre $GF(q)$, assim construído, apresentará uma distância livre com máximo valor, isto é, $d_{free} = K$.

A seguir, será abordada a construção de códigos convolucionais, cujas componentes de suas palavras-código pertencem a um dado anel $\mathbb{Z}_q$, sendo q uma potência de 2. Esses códigos baseiam-se em códigos RS e também apresentam máximo valor para a distância livre. Inicialmente, serão apresentados dois exemplos e, em seguida, será enunciado um método para a construção de tais códigos.

Exemplo 4.4.3. Considere a construção de códigos convolucionais 16-ários ($q = 2^4$), formado por duplas quaternárias. Novamente, deve-se, a princípio, determinar o polinômio gerador de um código de bloco cíclico 16-ário.

O anel de Galois $GR\left(2^2, 2\right)$ é formado pelas classes residuais de polinômios em $\mathbb{Z}_{2^2}[x]$ módulo $x^2 + x + 1$, ou seja

$$GR\left(2^2, 2\right) \cong \frac{\mathbb{Z}_{2^2}[x]}{< x^2 + x + 1 >} = \{a + bx;\ a, b \in \mathbb{Z}_4\}.$$

Similarmente à construção de tais códigos sobre corpos, deve-se determinar um grupo multiplicativo no anel $GR\left(2^2, 2\right)$. Neste sentido, seja α um elemento primitivo

em $GR(2^2, 2)$. Logo, α é uma raiz de $x^2 + x + 1$ ou, em outras palavras

$$\alpha^2 + \alpha + 1 = 0 \quad \Rightarrow \quad \alpha^2 = -1 - \alpha = 3 + 3\alpha,$$

onde essas operações são realizadas em $\mathbb{Z}_4$.

Assim, os elementos de tal grupo multiplicativo em $GR(2^2, 2)$ são:

$$1$$
$$\alpha$$
$$\alpha^2 = 3 + 3\alpha$$

Os polinômios minimais associados a esses elementos são:

Elementos		Polinômio minimal
1	$\longleftrightarrow$	$(x + 1)$
α, α^2	$\longleftrightarrow$	$(x + \alpha)(x + \alpha^2) = x^2 + x + 1$

onde

$$x^3 - 1 = (x + 1)(x + \alpha)(x + \alpha^2).$$

O código cíclico RS tem comprimento $n = q - 1 = 16 - 1 = 15$. Mais uma vez, o valor da distância d do código é definido como sendo igual ao número fatores com potências consecutivas do elemento primitivo mais 1. Como conseqüência, o polinômio gerador deve possuir o maior número de fatores consecutivos (em termos das potências de α) dos polinômios minimais, sem contudo conter um polinômio minimal completo (fator binário). Logo, os possíveis geradores para o código convolucional 16-ário sobre $\mathbb{Z}_{16}$ coincidem com aqueles apresentados nas Figuras 4.22 e 4.23.

Exemplo 4.4.4. Considere a construção de códigos convolucionais 64-ários ($q = 4^3$), formado por triplas quaternárias. Mais uma vez, deve-se determinar o polinômio gerador de um código de bloco cíclico 64-ário.

O anel de Galois $GR(2^2, 3)$ é formado pelas classes residuais de polinômios em $\mathbb{Z}_{2^2}[x]$ módulo $x^3 + x + 1$, ou seja

$$GR\left(2^2, 3\right) \cong \frac{\mathbb{Z}_{2^2}[x]}{< x^3 + x + 1 >} = \{a + bx + cx^2;\ a, b, c \in \mathbb{Z}_4\}.$$

Novamente, deve-se determinar um grupo multiplicativo em $GR(2^2, 3)$. Assim, seja α um elemento primitivo em $GR(2^2, 3)$. Logo, α é uma raiz de $x^3 + x + 1$ ou, em outras palavras

$$\alpha^3 + \alpha + 1 = 0 \quad \Rightarrow \quad \alpha^3 = -1 - \alpha = 3 + 3\alpha,$$

onde essas operações são realizadas em $\mathbb{Z}_4$.

Desta forma, o grupo multiplicativo em $GR(2^2, 3)$ é composto pelos seguintes elementos:

1	$\alpha^7 = 3 + 2\alpha^2$
α	$\alpha^8 = 2 + \alpha$
α^2	$\alpha^9 = 2\alpha + \alpha^2$
$\alpha^3 = 3 + 3\alpha$	$\alpha^{10} = 3 + 3\alpha + 2\alpha^2$
$\alpha^4 = 3\alpha + 3\alpha^2$	$\alpha^{11} = 2 + \alpha + 3\alpha^2$
$\alpha^5 = 1 + \alpha + 3\alpha^2$	$\alpha^{12} = 1 + 3\alpha + \alpha^2$
$\alpha^6 = 1 + 2\alpha + \alpha^2$	$\alpha^{13} = 3 + 3\alpha^2$

Como o número de elementos desse grupo multiplicativo é par, a fatoração do termo $x^{14} - 1$ não é única. Neste caso, deve-se buscar outro grupo multiplicativo, cuja ordem seja ímpar. Definindo $\beta = \alpha^2$, obtém-se um grupo multiplicativo com 7 elementos, como desejado. Conseqüentemente, a fatoração do termo $x^7 - 1$ é única.

Os polinômios minimais associados aos elementos desse novo grupo multiplicativo são:

Elementos		Polinômio minimal
1	$\longleftrightarrow$	$(x + 1)$
β, β^2, β^4	$\longleftrightarrow$	$(x + \beta)(x + \beta^2)(x + \beta^4)$
$\beta^3, \beta^6, \beta^5$	$\longleftrightarrow$	$(x + \beta^3)(x + \beta^6)(x + \beta^5)$

onde

$$x^7 - 1 = (x + 1)(x + \beta)(x + \beta^2)(x + \beta^3)(x + \beta^4)(x + \beta^5)(x + \beta^6).$$

O código cíclico RS tem comprimento $n = q - 1 = 64 - 1 = 63$. Para que esse código

apresente a maior distância possível, o seu polinômio gerador será

$$g(x) = (x + \beta^2)(x + \beta^3)(x + \beta^4)(x + \beta^5).$$

Logo, o código convolucional 64-ário associado é gerado por

$$G(x) = x^4 + (2 + \alpha + 2\alpha^2)x^3 + (2 + 2\alpha)x^2 + (2 + \alpha + 2\alpha^2)x + 1$$

e o seu codificador encontra-se ilustrado na Figura 4.27. Esse código apresenta uma distância livre $d_{free} = K = 5$.

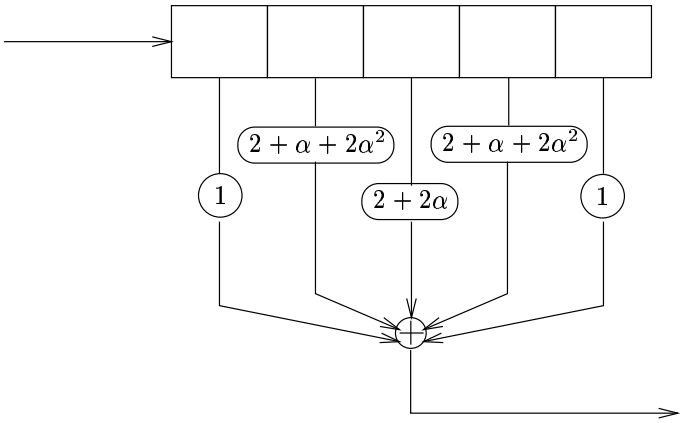

Figura 4.27: Codificador convolucional 64-ário, construído a partir de um código RS (código sobre anel).

A seguir, com base nos dois exemplos anteriores, enuncia-se um método para se obter códigos espaço-temporais (códigos sobre anéis).

4.4.2 Método Sistemático para a construção de Códigos Espaço-temporais (Códigos sobre Anéis)

O seguinte procedimento permite construir códigos de treliça espaço-temporais, cujas componentes de suas palavras-código pertencem a um dado anel $\mathbb{Z}_q$, onde $q = 2^\kappa$:

Para se obter códigos espaço-temporais, formados por τ-uplas q-árias (códigos convolucionais q^{τ}-ários formados por τ-uplas q-árias), deve-se inicialmente determinar o polinômio gerador de um código de bloco cíclico q^{τ}-ário. O anel de Galois $GR\left(2^{\kappa},\tau\right)$ é formado pelas classes residuais de polinômios em $\mathbb{Z}_{2^{\kappa}}[x]$ módulo um ideal primitivo de grau τ, também pertencente a $\mathbb{Z}_{2^{\kappa}}[x]$. Com objetivo de determinar um grupo multiplicativo dentro de $GR\left(2^{\kappa},\tau\right)$, suponha que α seja um elemento primitivo no anel em questão. Conseqüentemente, α é uma raiz desse ideal e, portanto, é possível expressar uma dada potência de α em função de outras menores, ferramenta essencial para se determinar os elementos desse grupo multiplicativo. Ressalta-se que as operações devem ser realizadas em $\mathbb{Z}_{2^{\kappa}}$. Caso a ordem δ do grupo multiplicativo seja par, o termo $x^{\delta}-1$ não pode ser fatorado de maneira única. Logo, deve-se determinar, nesse grupo multiplicativo, um elemento β (potência de α), cuja ordem θ seja uma multiplicidade ímpar da ordem de α no corpo $GF\left(2^{\tau}\right)$. Desta maneira, o termo $x^{\theta}-1$ pode ser fatorado de forma única. Determinados os polinômios minimais associados a cada um dos elementos do grupo multiplicativo gerado por β, pode-se definir o polinômio gerador do código de bloco cíclico, o qual, caso não contenha fator binário, concidirá com aquele do código convolucional q-ário (código espaço-temporal ótimo sobre $\mathbb{Z}_q$). Neste sentido, deve-se escolher o maior número de fatores consecutivos (em termos das potências de β) dos polinômios minimais para compô-lo, sem contudo selecionar um polinômio minimal completo (fator binário). O valor da distância d do código de bloco cíclico é definido como sendo igual ao número fatores com potências consecutivas do elemento primitivo mais 1. O código espaço-temporal ótimo sobre $\mathbb{Z}_q$, assim construído, apresentará uma distância livre com máximo valor, isto é, $d_{free}=K$.

Capítulo 5

Conclusões

O procedimento para a construção de códigos espaço-temporais, encontrado na literatura [18], [19], consiste basicamente em buscar exaustivamente códigos de treliça, cujos pares de palavras, satisfaçam dois critérios de projeto. Ressalta-se que esses critérios foram estabelecidos considerando o tipo de desvanecimento apresentado pelo canal em questão.

Por essa ser uma tarefa bastante árdua, havia a necessidade de se determinar um método mais simples para a construção de tais códigos. E essa foi a motivação principal desta dissertação: determinar métodos sistemáticos para a construção de códigos espaço-temporais (códigos sobre grupos, sobre corpos e sobre anéis) quando submetidos a canais com desvanecimento quasi-estático e plano.

5.1 Contribuições

No Capítulo 4 deste trabalho, encontram-se as suas contribuições. Nesse capítulo, inicialmente estabeleceu-se um método sistemático para a construção de códigos espaço-temporais (códigos sobre grupos). Tal método consiste basicamente em se determinar, através da técnica de recobrimento espacial baseado em reticulados, um código de bloco sobre grupos e associar-lhe adequadamente a um código de treliça. Enfatiza-se que, caso esse código de bloco seja oriundo de um quadrado latino, o código espaço-temporal a ele associado apresentará o melhor desempenho possível quando submetido a canais ruidosos. Esse resultado foi enunciado no Teorema 4.1.1. Além disso, é importante

ressaltar que não há qualquer restrição quanto à dimensão do reticulado, no qual a técnica de recobrimento espacial se baseia. Em seguida, os códigos sobre corpos, cuja proposta inicial era servir de ferramenta para a técnica de espalhamento espectral, foram utilizados como passo intermediário para a construção de códigos espaço-temporais (códigos convolucionais M-ários sobre corpos). Também, inovou-se ao se empregar os códigos sobre anéis como base para a construção de códigos espaço-temporais (códigos convolucionais M-ários sobre anéis).

5.2 Propostas para Trabalhos Futuros

Como temas para futuras pesquisas, propõem-se:

- Analisar, por meio de simulação, o desempenho dos códigos espaço-temporais estudados teoricamente nesta dissertação, comparando ambos os resultados e verificando a sua factibilidade (ou não).

- Determinar métodos sistemáticos para a construção de códigos espaço-temporais (códigos de treliça) quando submetidos a canais com desvanecimento do tipo Rayleigh ou Rice, sendo esses desvanecimentos rápidos, e canais com desvanecimento do tipo Nakagami, podendo esse desvanecimento ser quasi-estático e plano ou rápido. Nestes casos, por se tratar de tipos de ruídos diferentes daqueles abordados neste trabalho, deverão ser utilizadas métricas distintas daquelas aqui empregadas. Como conseqüência, a técnica de recobrimento espacial basear-se-á em reticulados diferentes daqueles tratados nesta dissertação.

- Estudar os códigos espaço-temporais (códigos sobre grupos) com maior número de estados, ou seja, com uma memória maior, analisando o seu desempenho quando submetidos a canais ruidosos típicos de comunicações móveis e determinando métodos sistemáticos para a sua construção.

Referências Bibliográficas

[1] Alouini, M.-S., e Goldsmith, A. J., "A Unified Approach for Calculating Error Rates of Linearly Modulated Signals over Genralized Fading Channels", *IEEE Trans. Commun.*, vol. 47, nº 9, Setembro 1999, pp.1324-1334 .

[2] Barbosa, P. R., "Construção de Códigos $\mathbb{Z}_{2^k}$-pseudolineares através de Aplicações Isométricas e Extensões de Galois sobre Anéis Locais", *Tese de Mestrado - Unicamp*, 2000.

[3] Bäro, S., "Performance Analysis of Space-Time Trellis Coded Modulation on Flat Fading Channels".[1]

[4] Boutros, J., e Viterbo, E., "Signal Space Diversity: A Power-and-Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel", *IEEE Trans. Inform. Theory*, vol. 44, nº 4, Julho 1998, pp. 1453-1467.

[5] Conway, J. H., e Sloane, N. J. A., *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1988.

[6] de Almeida, C., "Modulação-Codificada Generalizada via Equação de Diofanto", *Tese de Doutorado - Unicamp*, 1990.

[7] de Almeida, C., e Palazzo Jr., R., "Efficient two-dimensional interleaving technique by use of the set partioning concept", *Electronics Letters*, vol. 32, nº 6, Março 1996, pp. 538-540.

[8] Forney Jr., G. D., "Convolutional Codes I: Algebraic Structures", *IEEE Trans. Inform. Theory*, vol. IT-16, nº 6, Novembro 1970, pp. 720-738.

[1] Referência encontrada na Internet, sem maiores dados bibliográficos.

[9] Goldsmith, A., *Advanced Topics in Wireless Communications*, **URL:** http://wsl.stanford.edu/~ee360/top_lecture4.ps, 2001.

[10] Hammons Jr., A. R., e Gamal, H. E., "On the Theory of Space-Time Codes for PSK Modulation", *IEEE Trans. Inform. Theory*, vol. 46, nº 2, Março 2000, pp. 524-542.

[11] Interlando, J. C., Palazzo Jr., R., Gerônimo, J. R., Andrade, A. A., Favareto, O. M., e Nóbrega Neto, T. P., *Códigos Corretores de Erros sobre Estruturas de Corpos, Anéis e Grupos*, DT-FEEC-UNICAMP, 1998.

[12] Lin, X. e Blum, R. S., "Systematic Design of Space-Time Codes Employing Multiple Trellis Coded Modulation", *submetido a IEEE Trans. Infrom. Theory.*

[13] Loeliger, H.-A., e Mitterlholzer, T., "Convolutional Codes over Groups", *IEEE Trans. Inform. Theory*, vol. 42, nº 6, Novembro 1996, pp. 1660-1686.

[14] Lopes, W. T. A. e de Alencar, M. S., "Space-Time Coding Performance Improvement Using Rotated Constellation", *XIX Simpósio Brasileiro de Telecomunicações*, Fortaleza - CE, Setembro 2001.

[15] Palazzo Jr., R., Uchôa Filho, B. F., e Arpazi, J. P., *Fundamentos e Aplicações de Códigos Convolucionais em Sistemas de Comunicações*, DT-FEEC-UNICAMP, 1999.

[16] Pottie, G. J., e Calderbank, A. R., "Channel Coding Strategies for Cellular Radio", *IEEE Trans. Veh. Technol.*, vol. 44, nº 4, Novembro 1995, pp. 763-770.

[17] Rosental, J., Schumacher, J. M., e York, E. V., "On Behaviors and Convolutional Codes", *IEEE Trans. Inform. Theory*, vol. 42, nº 6, Novembro 1996, pp. 1881-1891.

[18] Tarokh, V., Seshadri, N., e Calderbank, A. R., "Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction", *IEEE Trans. Inform. Theory*, vol. 44, nº 2, Março 1998, pp. 744-765.

[19] Tarokh, V., Naguib, A., Seshadri, N., e Calderbank, A. R., "Space-Time Codes for High Data Rate Wireless Communication: Performance Criteria in the Presence

of Channel Estimation Errors, Mobility, and Multipaths", *IEEE Trans. Commun.*, vol. 47. n^o 2, Fevereiro 1999, pp. 199-207.

[20] Tarokh, V., Jafarkhani, H., e Calderbank, A. R., "Space-Time Block Coding for Wireless Communications: Performance Results", *IEEE J. Select. Areas Commun.*, vol. 47, n^o 3, Março 1999, pp. 451-460.

[21] Tarokh, V., Jafarkhani, H., e Calderbank, A. R., "Space-Time Block Codes from Orthogonal Designs", *IEEE Trans. Inform. Theory*, vol. 45, n^o 5, Julho 1999, pp. 1456-1467.

[22] Wozencraft, J. M., Jacobs, I. M., *Principles of Communication Engineering*, John Wiley & Sons, New York, 1965.

[23] Yacoub, M. D., *Foundations of Mobile Radio Engineering*, CRC Press, New York, 1993.

[24] Yan, Q. e Blum, R. S., "Optimum Space-Time Convolutional Codes".[2]

[25] Zhang, Y. e Blum, R. S., "Multistage Multiuser Detection for CDMA with Space-Time Coding".[2]

[2]Referência encontrada na Internet, sem maiores dados bibliográficos.