UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de Ilha Solteira

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

"Construção de Códigos Espaço-temporais de Treliça via Partição de Reticulado".

DIJIANI LUDOVINO GUANAIS

.

Ilha Solteira

2013

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

"Construção de Códigos Espaço-temporais de Treliça via Partição de Reticulado".

DIJIANI LUDOVINO GUANAIS

Orientador: Prof. Dr. Jozué Vieira Filho

Co-orientador: Prof. Dr. Edson Donizete de Carvalho

Dissertação apresentada à Faculdade de Engenharia – UNESP – Campus de Ilha Solteira, como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica.
Área de Conhecimento: Automação.

Ilha Solteira

2013

FICHA CATALOGRÁFICA
Desenvolvido pelo Serviço Técnico de Biblioteca e Documentação

G913c

Guanais, Dijiani Ludovino.
Construção de códigos espaço-temporais de treliças via partição de reticulados / Dijiani Ludovino Guanais. -- Ilha Solteira: [s.n.], 2013
77 f. : il.

Dissertação (mestrado) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de conhecimento: Telecomunicação, 2013

Orientador: Jozué Vieira Filho
Co-orientador: Edson Donizete de Carvalho
Inclui bibliografia

1. Códigos espaço-temporais de treliça. 2. Sistema mimo. 3. Partição de reticulados. 4. Diversidade de modulação.

unesp **UNIVERSIDADE ESTADUAL PAULISTA**

CAMPUS DE ILHA SOLTEIRA

FACULDADE DE ENGENHARIA DE ILHA SOLTEIRA

CERTIFICADO DE APROVAÇÃO

TÍTULO: Construção de Códigos Espaço-temporais de Treliça via Partição de Reticulado

AUTORA: DIJIANI LUDOVINO GUANAIS

ORIENTADOR: Prof. Dr. JOZUE VIEIRA FILHO

CO-ORIENTADOR: Prof. Dr. EDSON DONIZETE DE CARVALHO

Aprovada como parte das exigências para obtenção do Título de Mestre em Engenharia Elétrica, Área: AUTOMAÇÃO, pela Comissão Examinadora:

Edson D. Carvalho

Prof. Dr. EDSON DONIZETE DE CARVALHO
Departamento de Matemática / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. FRANCISCO VILLARREAL ALVARADO
Departamento de Matemática / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. ANTONIO APARECIDO DE ANDRADE
Departamento de Matemática / Instituto de Biociências, Letras e Ciências Exatas de São José do Rio Preto

Data da realização: 28 de março de 2013.

DEDICATÓRIA

À Deus.

Aos meus pais, Gilson Guanais e Maria Neuzi Ludovino Guanais (in memorian) .

À minha mãe do coração Neuza da Silva Guanais pela oportunidade.

Aos meus irmãos Dianehey Ludovino Guanais e Gilson Guanais Junior pela força.

Ao meu marido Rudgen Rodrigues Caldas pela dedicação.

AGRADECIMENTO

À DEUS, que me proporcionou tudo de melhor na minha vida.

À Faculdade de Engenharia de Ilha Solteira, por fornecer meios para esta conquista;

Ao professor Dr. Edson Donizete de Carvalho pela valiosa orientação dedicada nos últimos anos que trabalhamos juntos, que me revelou autêntica demonstração de profissionalismo, competência, humildade, confiança e companheirismo, à minha pessoa, a quem considero não só como um amigo, mas como um exemplo de vida.

Ao professor Dr. Jozué Vieira Filho pela amizade, auxílio e trabalhos prestados.

Aos professores do curso, pelos ensinamentos, colaborações, incentivos e companheirismo.

Aos funcionários da Biblioteca, pela dedicação e apoio à realização das pesquisas.

Aos meus amigos Naiara, Eliane, Robson Piacente, Heidi, Larissa e Rosimeire, pelo apoio, amizade e momentos felizes de descontração. Enfim, agradeço a todos que me ajudaram a ser hoje uma pessoa melhor em todos os aspectos e àqueles que até neste momento não foram lembrados, porém jamais esquecidos.

RESUMO

Neste trabalho, abordaremos um método sistemático para a construção de códigos espaço-temporal de treliça em sistema de comunicação sem fio que emprega a tecnologia MIMO quando submetidos em canais com desvanecimento do tipo quase-estático. O método é baseado na teoria de reticulados e explora conceitos de constelações rotacionais obtidas via partições de reticulados. Esta metodologia assegura a maior diversidade possível no processo de modulação utilizado.

Palavras-chave: Código espaço-temporal de treliça. Sistema MIMO. Desvanecimento. Diversidade de modulação. Reticulado. Constelações de sinais.

ABSTRACT

This paper proposes a systematic method for building Space-Time Trellis Codes in wireless communication system that employs MIMO when submitted in fading channels. The method is based on the theory of lattices that will combine concepts of rotated constellations and partition lattices. This methodology ensures the greatest possible diversity in the process of modulation used.

Keywords: Space-time trellis codes. MIMO system. Fading. Diversity modulation. Cross linked signal constellations.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

PAM	Pulse amplitude modulation
FSK	Frequency shift-keying
PSK	Phase-shift keying
QAM	Quadrature amplitude modulation
AWGN	Additive White Gaussian Noise
MLD	Maximum likebihood decoding
MIMO	Multiple Input Multiple Output
TCM	Trellis Coded Modulation
CETT	Código Espaço Temporal de Treliça

LISTA DE SÍMBOLOS

u_j	sequência de palavras código fonte
v_j	sequência de palavras código do canal
E_s	energia média da constelação de sinal
$d(v_0, v_i)$	distância euclidiana entre os sinais v_ie v_0
C	capacidade do canal
$p(x_i, y_i)$	probabilidade de enviar o símbolo x_i e receber o símbolo y_j no canal
$p(y_j \mid x_i)$	probabilidade de se receber y_j dado que x_i foi enviado
$H(S)$	entropia de uma fonte discreta sem memória
P_e	probabilidade de erro de um canal
$M = 2^k$	possibilidades de palavras código distintas
R	taxa em bits/uso do canal
N	comprimento do código
x_m	mensagem ou palavra-código transmitida
$n(t)$	ruído do canal
$\frac{N_0}{2}$	densidade espectral
α	coeficiente de desvanecimento do sinal
G	grupo
$GF(5)$	corpo de Galois de cardinalidade 5
$GF(7)$	corpo de Galois de cardinalidade 7
$\alpha(K)$	conjunto de entradas dos códigos
$\beta(k)$	conjunto de saídas dos códigos
w	peso de Hamming
d_{free}	distância livre
$\mathbb{Z}[i]$	anel de inteiros de Gauss
$\mathbb{Z}[\omega]$	anel de inteiro de Eisenstein-Jacobi

p	inteiro primo
S	constelação de sinais
S'	constelação de sinais de S
$\mathbb{Z}^2$	reticulado associado a modulação QAM
$\mathbb{A}_2$	reticulado associado a modulação HEX
U	constelação de cardinalidade p^n
Λ	reticulado
Λ'	subreticulado
T	Transformação ortogonal
l	rótulo da constelação de sinais
Λ_α	reticulado gerado pela base α
T_α	toro planar
$\frac{E_s}{4N_0}$	relação sinal ruído
μ	função de rotulamento

Sumário

1 Introdução

1.1 Introdução

O constante aumento na transmissão de informação, tem levado as grandes corporações do setor das telecomunicações demanda pelos serviços de comunicação sem fio aliada a busca de uma alta e confiável a uma permanente busca no aperfeiçoamento de tecnologia presente em sistema deste porte. Porém, as restrições físicas inerentes aos canais de comunicações sem fio representam uma barreira tecnológica para que consiga tal objetivo. Limitações na largura de banda, perdas de propagação, variação no tempo, ruído, interferência e desvanecimento multipercurso fazem com que a transmissão de dados a altas taxas não seja uma tarefa fácil.

Dentre as novas técnicas surgidas nestas últimas décadas, destacamos a técnica denominada de MIMO (do inglês: Multiple Input Multiple Output) que significa um sistema com múltiplas antenas na transmissão e na recepção. Com a aplicação desta técnica, consegue-se obter sistemas com altas taxas de transmissão sem precisar sacrificar a potência e a largura de faixa.

Dentro deste contexto, Foshini e Gans (1998) mostraram que a capacidade de transmissão de informação aumenta linearmente com o número de antenas transmissoras desde que o número de antenas receptoras seja maior ou igual que o número de antenas transmissoras ao se levar em consideração o desvanecimento quase-estático, isto é, quando o desvanecimento é constante em um intervalo de tempo relativamente longo e com variações estatisticamente independentes entre esses intervalos.

Para combater o desvanecimento quase-estático, Tarokh et al. (1998), propuseram os códigos espaço-temporais de treliça (do inglês Space-Time Trellis Codes). A eficiência de tais códigos está baseado no ganho de diversidade que é definido como expoente da relação sinal ruído $SNR\left(\frac{E_s}{4N_0}\right)$.

Estes códigos operam sobre um símbolo de constelação de modulação utilizada a cada instante de tempo, produzindo um vetor formado por combinações lineares desses símbolos, cujo comprimento é equivalente ao número de antenas utilizadas na transmissão.

Valença (2001) propôs uma construção de códigos espaço temporal de treliças a partir de rotulamento de estados de uma treliça via constelação de uma modulação baseada na técnica de quadrados latinos. A técnica dos quadrados latinos, fundamentalmente, baseia-se

em obter um grupo cíclico aditivo de cardinalidade p que os autores denominaram de códigos de grupo.

Os códigos de grupos de cardinalidade prima p, obtidos são dados $p = 2$ e $p \equiv 1\ (mod\ 4)$ caso o quadrado latino fosse proveniente do reticulado $\mathbb{Z}^2$. Caso o quadrado latino fosse proveniente do reticulado $\mathbb{A}_2$, os códigos de grupos de cardinalidade prima p são obtidos para $p = 3$ e $p \equiv 1\ mod\ 6$.

Neste trabalho, veremos que a construção dos códigos de grupos (códigos cíclicos) proposto em Valença (2001) é uma conseqüência direta de resultados já conhecidos na literatura como a construção de grupos cíclicos obtidos pelo grupo quociente no toro planar em Costa et al.(2004), e de resultados de constelações de sinais rotacionadas.

Baseados nestes resultados e de constelações de sinais casadas a grupos aditivos cuja cardinalidade é uma potência de primo p a partir dos reticulados $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, veremos que a proposta de Valença (2001), é estendida para os casos de potências de primos, ou seja, obtém códigos de grupo (grupos aditivos cíclicos) de ordem p^n, onde $p = 2$ e $p \equiv 1\ (mod\ 4)$, sendo proveniente do reticulado $\mathbb{Z}^2$.

Da mesma forma, obtém códigos de grupos (grupos aditivos cíclicos) de ordem p^n, onde $p = 3$ e $p \equiv 1\ (mod\ 6)$, sendo proveniente do reticulado $\mathbb{A}_2$.

Por fim, mostraremos algebricamente que a construção de Valência (2001) e a construção proposto neste trabalho, estes códigos cíclicos de ordem p, são obtidos a partir de partição de uma cadeia de subreticulados obtidos a partir de $\mathbb{Z}^2$ ou $\mathbb{A}_2$. Como conseqüência, desta caracterização algébrica, simplificaremos o algoritmo de codificação proposto por Valença (2001).

1.2 Objetivo

O principal objetivo deste trabalho é apresentar um método simples e preciso para a construção de códigos espaço temporais de treliças sobre grupos, com diversidade de modulação máxima obtida a partir de uma generalização de técnica de geração de quadrados latinos quando submetidos a canais com desvanecimento quase-estático e plano. Porém, deve-se destacar que existem na literatura outros métodos para a construção de tais códigos, como demonstram os trabalhos de (TAROKH; SESHADRI, 1998; TAROKH; NAGUIB; SESHADRI, 1999). O diferencial, neste trabalho, é a metodologia usada para gerar tais códigos.

1.3 Estrutura do trabalho

Após esta breve introdução, o presente texto é desenvolvido com a seguinte estrutura:

Capítulo 2: Apresenta tópicos sobre teoria da informação e conceitos básicos da álgebra linear com o objetivo de fornecer a base teórica para o desenvolvimento do trabalho.

Capítulo 3: Apresenta o conceito dos códigos convolucionais a partir de máquinas de Estado Finito, desde a sua decodificação até as propriedades de distância desses códigos.

Capítulo 4: Apresenta-se um modelo de sistema de comunicação sem fio (MIMO) bem como a introdução e análise do desempenho dos códigos espaço temporais de treliças quando submetidos a canais com desvanecimento quase-estático empregado no modelo do sistema em questão.

Capítulo 5: São apresentadas a teoria de reticulados e a construção de constelações de sinais provenientes de reticulados casados a grupos e o esquema de modulação utilizada para se obter a diversidade máxima.

Capítulo 6: São apresentadas estratégias de codificação para se determinar códigos espaço temporal de treliça via partição de reticulados, obtidas a partir de uma generalização da técnica de geração de quadrados latinos e considerando-se canais com desvanecimento quase-estático.

Capítulo 7: São apresentadas as conclusões, destacando-se a importância deste trabalho, assim como tópicos que podem ser abordados em pesquisas futuras.

2 Teoria da informação e conceitos básicos da álgebra

2.1 Sistema de comunicação

Os sistemas de comunicação sem fio, particularmente as comunicações móveis pessoais, apresentaram nestas últimas décadas grandes avanços no seu desenvolvimento. Em especial, os sistemas de comunicação digital evoluíram a partir de uma demanda por transmissão e armazenamento confiáveis de dados com altas taxas. Esta evolução está relacionada à tecnologia computacional e viabiliza, atualmente, o controle de erros em comunicações, envolvendo canais submetidos aos mais variados tipos de interferências.

Definição 2.1.1 Entende-se como sistema de comunicação um conjunto de equipamentos e meios físicos que tem como objetivo transportar uma determinada informação de uma fonte a um determinado destinatário através de um meio físico.

O canal de comunicação pode ser um par de fios, um cabo, uma fibra ótica ou o espaço livre. A transmissão através desses canais é realizada de forma analógica ou digital. Na transmissão de forma analógica a informação original é transmitida por meio de sinais elétricos, magnéticos ou eletromagnéticos que variam continuamente em amplitude, freqüência e/ou fase e tempo. Já na transmissão digital, a informação é discretizada e transmitida em sequência por meios de sinais elétricos, magnéticos, eletromagnéticos ou luminosos (via fibra ótica) podendo variar em amplitude, fase e/ou freqüência em intervalos fixos de tempo.

Na figura 1 tem-se um exemplo, em diagramas de blocos, de um sistema de comunicação digital.

Figura 1- Sistema de comunicação digital

Fonte: Guanais (2012)

A fonte gera a informação que deve ser transmitida, que pode ser um sinal de voz, áudio, vídeo, etc. A informação original é discretizada e forma uma sequência discreta, que é codificada para gerar as sequências $(u_j) = (u_1, \dots, u_k)$ de palavras códigos fonte. Nesta etapa, deve-se utilizar o menor número possível de dígitos por unidade de tempo para armazenar a informação proveniente da saída da fonte. Assim, o codificador transforma cada palavra código fonte u_j em outra sequência $(v_j) = (v_1, \dots, v_n)$, denominada palavra código de canal, cujo objetivo é introduzir redundância na sequência (u_j) para reduzir a interferência de ruídos presentes no canal de comunicação. O modulador converte a sequência de entrada em uma sequência de formas de ondas apropriadas para a transmissão através do canal. Por fim, num processo inverso, o demodulador, decodificador de canal e decodificador de fonte recuperam a informação transmitida.

2.2 Modulação

A natureza do ruído em um canal de comunicação é decisiva na escolha dos esquemas de modulação e de codificação, já que o objetivo é minimizar a ação do ruído presente no canal. As modulações digitais básicas e que originam outros tipos de modulação digital são:

. PAM (pulse amplitude modulation): alteração de amplitude

. FSK (frequency shift-keying): alteração de frequência

. PSK (phase shift-keying): alteração de fase

. QAM (quadrature amplitude modulation): alteração de amplitude e fase.

Independente do tipo de modulação a ser usado, o modulador digital transforma símbolos discretos da saída do codificador de canal em um sinal contínuo (analógico) com duração de T segundos por símbolo.

2.3 Constelação de sinais

A informação a ser transmitida através de um sistema de comunicação sempre estará sujeita a interferências causadas pelo meio, normalmente denominadas de ruído. Assim, do ponto de vista matemático, um processo de modulação projeta constelações em espaços Euclidianos, de modo que o ruído seja reduzido.

Definição 2.3.1 Entende-se como constelação de sinais o conjunto de palavras-códigos e sinais representados por meio de esquemas compostos por pontos e vértices de grafos no espaço euclidiano $\mathbb{R}^n$.

Dentre todos os possíveis conjuntos de sinais com cardinalidade finita m, aquele que apresenta a menor energia média é a constelação de sinais associada aos m pontos de sinais. A energia média mínima, E_s, de uma constelação de sinais $\{v_0, v, \dots, v_{m-1}\}$ é dada por:

$$E_s = \sum_{i=1}^{m-1} \frac{d^2(v_0, v_i)}{m}, \qquad (2.1)$$

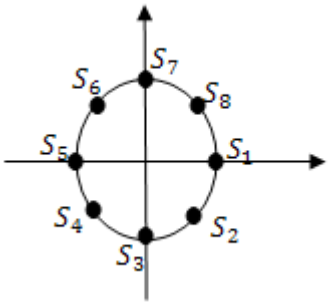
onde $d(v_0, v_i)$ denota a distância euclidiana entre os sinais v_i e v_0.

Na verdade, existe uma relação geométrica entre a constelação de sinais e o tipo de modulação. Por exemplo, do ponto de vista geométrico os sinais de uma modulação PSK são caracterizados no espaço euclidiano sobre um ponto R do círculo unitário. Do ponto de vista algébrico, os n sinais são raízes da unicidade, ou seja, $\xi^n = 1$, com $\xi = cos\frac{\pi}{n} + isen\frac{\pi}{n}$ e os sinais sendo representados por $1, \xi, \xi^2, \dots, \xi^{n-1}$.

Como mencionado anteriormente, dependendo do tipo de modulação, o ruído pode afetar mais ou menos a transmissão. Para o tipo de codificação estudada neste trabalho, a opção é pelo uso das modulações QAM.

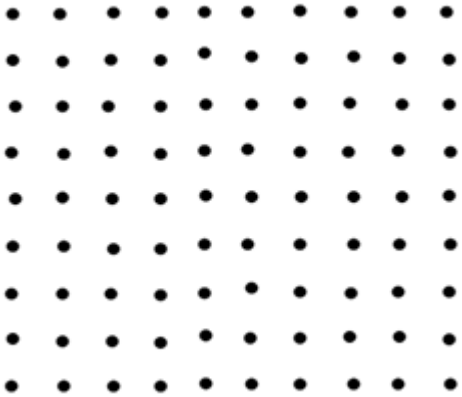
Assim, para um melhor entendimento, serão consideradas as constelações de sinais do tipo PSK e QAM como apresentadas nas figuras 2 e 3. Estas constelações serão fundamentais para a geração dos códigos espaço-temporal de treliça propostos neste trabalho.

Figura 2- Constelação 8-PSK em $\mathbb{R}^2$.



Fonte: Guanais (2012)

Figura 3- Constelação QAM em $\mathbb{R}^2$.



Fonte: Guanais (2012)

2.4 Probabilidade de erros e codificação de fonte e canal.

A capacidade de um sistema de comunicação digital sem fio em resistir às interferências em um determinado canal é quantificada através da probabilidade de erro de transmissão. Assim, a busca por um sistema de comunicação robusto significa a redução da probabilidade de erro. Uma das maneiras mais diretas de se fazer isso é acrescentar mais redundância a dígitos de informação associado à mensagem, ou seja, aumentar o comprimento da palavra-código. Porém, este procedimento não deve ser feito de forma aleatório, pois, ao aumentar-se o comprimento da palavra código, tem-se como conseqüência uma redução na capacidade de transmissão do sistema, representada através de uma taxa de bits.

Shannon em 1948 demonstrou, através do Teorema de Codificação de Canal, que é possível reduzir a probabilidade de erro sem sacrificar a taxa de transmissão.

2.4.1 Teorema de codificação da fonte e canal

Entende-se como capacidade C de canal discreto a quantidade máxima de informação que pode ser processada pelo canal definida por:

$$C = max\left\{\sum_{j=0}^{q-1}\sum_{i=0}^{m-1} p(x_i, y_i) log_a \frac{p(y_j|x_i)}{p(y_j)}\right\}$$

sendo que $p(x_i, y_i)$ é a probabilidade de enviar o símbolo x_i e receber o símbolo y_j no canal, $p(y_j|x_i)$ é a probabilidade de se receber y_j dado que x_i foi enviado, $p(y_j)$ é a probabilidade de se receber y_j, m a cardinalidade do alfabeto das palavras-códigos na entrada do modulador e q a cardinalidade do alfabeto das palavras-códigos na saída do demodulador.

O teorema de codificação de canal proposto por Shannon é fundamentado nos conceitos de entropia de uma fonte e da capacidade de um canal.

Definição 2.4.1 A entropia de uma fonte discreta sem memória com símbolos $S = \{s_1, \dots, s_n\}$ e cuja distribuição de probabilidade é $P = \{p_1, \dots, p_m\}$, é definido por

$$H(S) = \sum_{i=1}^{m} p_i \log_a \frac{1}{p_i},$$

sendo o bit $(a = 2)$ a unidade de medida da entropia por símbolo da fonte e $P_i = p(S_i), \forall\, i = 1, \dots, n$.

Note que se a probabilidade p_i da fonte de emitir s_i for alta, então a quantidade de informação obtida é baixa. Por outro lado, caso a probabilidade p_i da fonte de emitir s_i seja baixa, então a quantidade de informação obtida é alta. Em outras palavras, a entropia nada mais é do que a quantidade do conteúdo de informação por símbolo emitido pela fonte.

Teorema 2.4.1 Se a entropia da fonte, H, é maior do que a capacidade do canal, C, isto é, $H > C$, então a probabilidade de erro, P_e, é necessariamente maior do que zero.

Teorema 2.4.2 Se $H < C$, então $P_e \to 0$.

Neste caso, quantas restrições forem necessárias serão impostas, então iremos assumir que o codificador de canal é do tipo codificador de bloco, que por definição são códigos de mesmo comprimento N sem memória, podendo este ser linear ou não. Assim, no caso binário, existe $M = 2^k$ possibilidades de palavras código distintas.

Dizemos que um código é unicamente decodificável, se existe uma aplicação bijetiva entre o conjunto de sequências na saída do codificador de fonte e o conjunto de palavras-código na saída do codificador de canal, definida da seguinte maneira:

$$\begin{array}{ccc} Fonte & & Palavras - código \\ 1 & \leftrightarrow & x_1 = (x_{11}, x_{12}, \dots, x_{1N}) \\ 2 & \leftrightarrow & x_2 = (x_{21}, x_{22}, \dots, x_{2N}) \\ 3 & \leftrightarrow & x_3 = (x_{31}, x_{32}, \dots, x_{3N}) \\ & & \vdots \\ & & \vdots \\ M & \leftrightarrow & x_M = (x_{M1}, x_{M2}, \dots, x_{MN}). \end{array}$$

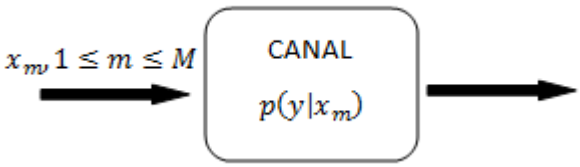
Definindo R como a taxa em bits/uso do canal, tem-se que

$$R = \frac{logM}{N} = \frac{log2^K}{N} = \frac{Klog2}{N}.$$

É importante ressaltar que se o logaritmo estiver na base 2, então a unidade de medida será bits/uso do canal; já se o logaritmo estiver na base e, então a unidade de R será nats/uso de canal.

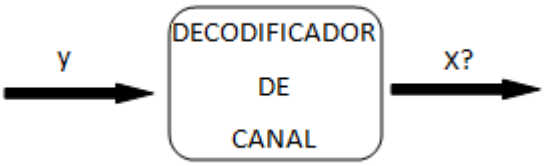
Pelo fato de o mapeamento ser biunívoco, segue que o canal e o decodificador podem ser representados de acordo com as Figuras 4 e 5, respectivamente.

Figura 4 - Bloco do canal



Fonte: Palazzo (1998)

Figura 5 - Bloco associado ao decodificador do canal



Fonte: Palazzo (1998)

No decodificador, o objetivo é determinar qual x_m, para $1 \leq m \leq M$, foi transmitido. Assim, se $x = x_m$ é o dado que foi transmitido, então a decodificação foi correta, caso contrário tem-se um erro de decodificação.

Em se tratando dos parâmetros N e R, segue que os possíveis erros do processo de decodificação podem ser avaliados através da probabilidade de erro P_e.

Em geral, observando-se o comportamento dos parâmetros em questão, pode-se concluir que uma diminuição na taxa R que entra no codificador, mantendo-se o comprimento N fixo, leva a uma redução de P_e, já que $R = \frac{K}{N}$. No caso, tem-se uma redução de K e, por conseqüência, um aumento na diferença $N - K$. Assim, mais bits de informação poderão ser usados para a correção de erro.

2.5 Regra de decodificação

A regra de decodificação tem como objetivo minimizar a probabilidade de erro para um dado conjunto de palavras-código.

Neste contexto, seja x_m a mensagem ou palavra-código transmitida e y a sequência da saída do canal. Denotando por $p(y|x_m)$ a probabilidade de receber y em um canal discreto e sem memória, tem-se que

$$p(y|x_m) = \prod_{i=1}^{N} p(y_i|x_{mi}).$$

Assumindo $p(m)$ como sendo a probabilidade de ocorrência da mensagem m, tem-se

$$p(m|y) = \frac{p(m)p(y|x_m)}{P(y)}.$$

sendo,

$$p(y) = \sum_{m} p(m)p(y|x_m).$$

Dessa forma, pode-se concluir que se o decodificador decodifica y como m, então o complemento $1 - p(m|y)$ é a probabilidade de decodificação errônea, sendo que o decodificador selecionará m para que $p(m|y)$ seja máximo e consequentemente, $1 - p(m|y)$ será mínimo.

Contudo, podemos descrever este processo de tal forma que P_e seja mínima, decodificando a sequência recebida y para um m' de modo que

$$p(m'|y) \geq p(m|y), \forall\, m \neq m'.$$

Como $p(y) > 0$ e independe de m, segue que a decodificação com a finalidade de ser mínima para P_e implica em dois critérios de decodificação, dados por:

I) **Decodificação por máxima verossimilhança:** Se $p(m) = \frac{1}{M}$, $1 \leq m \leq M$, então

$$p(y|m') \geq p(y|m), \forall\, m \neq m'.$$

II) **Decodificação por máxima probabilidade a posteriori:** Se pelo menos alguma $p(m) \neq \frac{1}{M}$, para $1 \leq m \leq M$, então

$$p(y|m^{'})p(m^{'}) \geq p(y|m)p(m), \forall\, m \neq m'.$$

Neste trabalho supõe-se que todas as palavras-código são equiprováveis, em relação a aplicação da decodificação por Máxima Verossimilhança. Para ilustrar o que significa minimizar a probabilidade de transmitir uma informação errônea através da decodificação por máxima verossimilhança, tomemos x_1e x_2 palavras códigos de comprimento N. Sem perda de generalidade, se a mensagem transmitida foi x_1, então um erro será cometido se a regra de decisão concluir que

$$p(y|x_2) \geq p(y|x_1).$$

Definindo $m(y)$ como sendo

$$m(y) = ln\left[\frac{p(y|x_2)}{p(y|x_1)}\right] \geq 0,$$

segue que a probabilidade de que a palavra-código $x_1$tenha sido enviada é expressa por

$$p(x_1 \rightarrow x_2|x_1) = p[m(y) \geq 0\ |x_1]. \qquad (1.4)$$

2.5.1 Teorema (Limitante de Chernoff): (PALLAZZO et al., 1999) Seja $p(t \geq \delta) \leq \frac{\bar{t}}{\delta}$, para $\delta > 0$, com $\bar{t} = E(t)$. Se $t = \exp(\lambda m(y))$,então

$$p\left[\exp(\lambda m(y)) \geq \delta\right] \leq \frac{\overline{\exp(\lambda m(y))}}{\delta}.$$

Desta maneira, aplicando o limitante de Chernoff à Equação (1.4), obtém-se que

$$p(x_1 \rightarrow x_2|\, x_1) \leq E\{e^{\lambda m(y)}|x_1\},$$

ou seja,

$$p(x_1 \rightarrow x_2|\, x_1) \leq \int \left[\frac{p(y|x_2)}{p(y|x_1)}\right]^{\lambda} p(y|x_1)dy\,.$$

Assim,

$$p(x_1 \to x_2|x_1) \leq \int [p(y|x_2]^{\lambda}[p(y|x_1)]^{1-\lambda} dy. \quad (1.5)$$

O mínimo do termo à direita da desigualdade (1.5) ocorre quando $\lambda = \frac{1}{2}$. Portanto, um limitante superior para a probabilidade de erro, dado que a palavra-código x_1 foi transmitida, é dado por

$$p(x_1 \to x_2|x_1) \leq \int [p(y|x_2)]^{\frac{1}{2}} [p(y|x_1)]^{\frac{1}{2}} dy. \quad (1.6)$$

2.6 Canais de Comunicação

Os canais de comunicação móvel são agrupados em dois tipos: Canal Gaussiano e Canal com Desvanecimento do tipo Rayleigh.

2.6.1 Canal Gaussiano

Introduzido por Shannom em 1948, é um modelo de canal de comunicação no qual mensagens usadas na transmissão são representadas por vetores de $\mathbb{R}^n$. Neste tipo de canal predominam fortes atenuações e muitas vezes atrasos de propagação do sinal.

Quando um vetor x é transmitido o sinal recebido é representado por um outro vetor na forma $y(t) = x(t) + n(t),\ 0 \leq t \leq T$, que consiste do vetor original x mais um vetor $n = (n_1, \dots, n_n)$, denominado de ruído e independente do sinal x.

Com base no teorema da Capacidade de Canal AWGN (Additive White Gaussian Noise), Shannon mostrou a possibilidade de se alcançar uma taxa de transmissão menor que C (capacidade do canal) com probabilidade de erro P_e arbitrariamente pequena, mas não estabeleceu uma maneira ou técnica de fazê-lo.

Teorema 2.6.1 (Teorema da Capacidade de Canal AWGN). Se o ruído em um canal de transmissão é do tipo AWGN com densidade espectral de potência $\frac{N_0}{2}$, sendo $\sigma^2 = N_0 a$, então a capacidade de canal C com largura de faixa de freqüência limitada a a hertz para uma dada potência de sinal P watts é dada por

$$C = a\ log_2\left(1 + \frac{P}{N_0 a}\right)\ bits/segundo.$$

Para se ter um código que consiga atingir uma probabilidade de erro tão pequena quanto se queira, deve-se ter um decodificador que seja de máxima verossimilhança (MLD: maximum likelihood decoding), ou seja, que existem códigos de bloco de comprimento N tal que

$$P_e \leq 2^{-NE_a(R)},$$

onde $E_b(R)$ é uma função positiva para $R < C$ que é determinada pela característica do canal.

Neste contexto, existem na literatura diversas técnicas de decodificação e/ou modulação que permitem obter valores de P_e próximos do limite estabelecido por Shanom.

2.6.2 Canal com desvanecimento do tipo Rayleigh

Em um ambiente sem fio e móvel, obstáculos físicos como construções, árvores e casas, agem como refletores de ondas eletromagnéticas. Devido a estas reflexões, as ondas eletromagnéticas percorrem caminhos diferentes, com diferentes distâncias, gerando sinais com diferentes amplitudes e fases, dando origem a uma propagação por múltiplos percursos. A atenuação do sinal devido à distância e por obstruções entre o transmissor e o receptor é que se denomina na literatura de desvanecimento.

A soma vetorial dos vários sinais dos múltiplos percursos pode resultar em uma interferência construtiva ou destrutiva do sinal recebido, ou seja, as estruturas em torno do receptor vão se modificando com o movimento e, consequentemente, interferências passam constantemente de uma situação construtiva para uma destrutiva, fazendo com que a intensidade do sinal recebido varie ao longo tempo, ou seja, causando o desvanecimento por múltiplos percursos.

Definição 2.6.1 Um canal apresenta desvanecimento quase-estático plano quando sua largura de faixa coerente é maior que a largura de faixa do sinal modulado transmitido. Nesta situação, todas as componentes de frequências do sinal enviado sofrem desvanecimentos de maneira igual.

Por largura de faixa coerente do canal entende-se a máxima componente do sinal ainda não considerada correlacionada aos que chegarem (com diferentes tempos de atrasos) no receptor. Este tipo de desvanecimento é conhecido como desvanecimento de Rayleigh ou plano.

Suponha $y = (y_1, \dots, y_2)$ como sendo o vetor recebido e $\alpha = (\propto_1, \dots, \propto_n)$ como sendo os coeficientes de desvanecimento. Se o sinal $x \equiv x(t)$ é transmitido através de um canal com desvanecimento do tipo Rayleigh, então o sinal recebido no intervalo de tempo $0 < t < T$ é dado por

$$y(t) = \propto * x(t) + n(t),$$

onde $n = (n_1, \dots, n_n)$ é o ruído Gaussiano, $\alpha = (\propto_1, \dots, \propto_n)$ é coeficiente de desvanecimento e $*$ representa o produto interno.

2.7 Diversidade de um canal de comunicação

Uma alternativa mais simples para aumentar a capacidade do canal com desvanecimento é utilizar técnicas de diversidade, que permitem combater o desvanecimento do sinal.

Diversidade é uma técnica que fornece, ao receptor, réplicas da informação transmitida que experimentam desvanecimentos descorrelacionados. Neste caso, se uma componente do sinal estiver sobre um desvanecimento profundo, algumas das outras componentes terão uma grande probabilidade de sofrer uma atenuação mais leve. Em sistemas de comunicações móveis as técnicas de diversidade podem ser do tipo temporal, freqüência e espacial.

• **Diversidade temporal:** É utilizada uma combinação de codificação de canal e entrelaçamento fazendo com que réplicas do sinal transmitido estejam presentes no receptor na forma de redundância no domínio do tempo.

• **Diversidade em freqüência:** Réplicas do sinal são enviadas ao receptor através de faixas de freqüências diferentes, explorando-se o fato de que sinais transmitidos através de portadoras distintas sofrem desvanecimentos diferentes.

• **Diversidade espacial:** Réplicas do sinal são transmitidas desde locais diferentes de forma tal que haja uma descorrelação entre os caminhos percorridos pelo sinal. Na implementação desta técnica são utilizadas múltiplas antenas no transmissor e/ou no receptor, separadas adequadamente ou diferentemente polarizadas para garantir a descorrelação entre os caminhos percorridos pelo sinal.

Quando possível, os sistemas de comunicações móveis (em particular os sistemas de telefonia celular) podem ser projetados para utilizar todas as formas de diversidade.

Como será visto nos próximos capítulos, uma das vantagens de sistemas com múltiplas antenas (MIMO) é que estes fornecem uma melhor confiabilidade nas transmissões,

usando-se técnicas de diversidade, sem aumentar a potência transmitida ou sacrificar a largura de faixa.

2.7.1 Diversidade de Modulação

O desvanecimento provocado pelos múltiplos percursos de propagação dos sinais transmitidos em canais de comunicações móveis pode degradar significativamente o desempenho de sistemas de comunicações digitais. Em decorrência disto, cresce a necessidade de se melhorar a capacidade e o desempenho desses tipos de sistemas de transmissão. Com o uso das técnicas de diversidade espacial e de combinação ótima consegue-se, de fato, essa melhoria no desempenho.

Os códigos espaço-temporais de treliças, assunto a ser abordado nos próximos capítulos, combinam diversidade espacial e temporal e garantem que um ganho de diversidade seja alcançado sem sacrificar a taxa de transmissão.

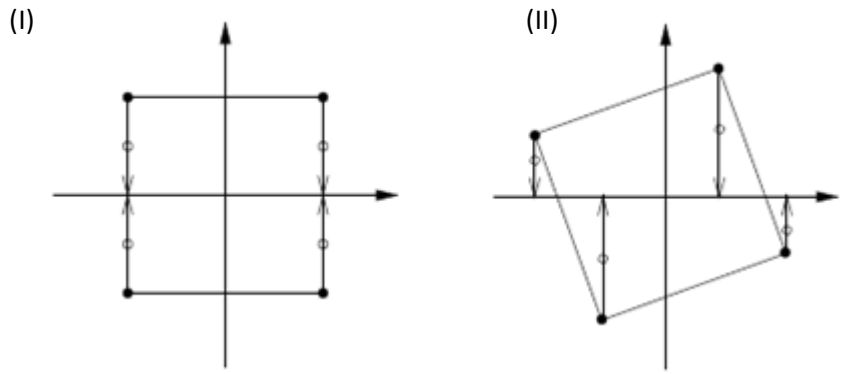
No entanto, Boutros e Viterbo (1998) mostraram outra forma de melhorar a diversidade, que é baseada na rotação e no embaralhamento dos símbolos da constelação, antes da etapa de modulação, denominada de diversidade de modulação.

Em decorrência disto, a ordem de diversidade de um conjunto de sinais multidimensional é definida como o número mínimo de componentes distintas entre dois pontos quaisquer da constelação, ou seja, é a distância mínima de Hamming[1] entre dois vetores da constelação, fato importante que conclui que para uma constelação $n-$ dimensional, a ordem de diversidade é sempre menor ou igual a n.

Essa técnica de diversidade de modulação é de suma importância para a construção de códigos sobre grupo que será explorado nos próximos capítulos. Dessa forma, para um melhor entendimento, considera a constelação 4 – PSK ilustrada na Figura 6.

[1]A **distância de Hamming** entre duas palavras-código de mesmo comprimento é o número de posições nas quais elas diferem entre si.

Figura 6 - Diversidade de modulação para a constelação 4 - PSK



Fonte: Boutros e Viterbo (1998)

Caso o desvanecimento atinja somente uma única componente do vetor associado ao sinal transmitido, conclui-se que a constelação que sofre desvanecimento na Figura 6 (II) oferece mais proteção contra os efeitos do ruído, pois observa-se que os pontos jamais se coincidem, como no caso da Figura 6 (I).

2.8 Revisão de álgebra abstrata

Nesta seção apresentamos conceitos de álgebra abstrata, tais como: grupo, ideais, anéis, corpos e grupo quociente, que são fundamentais para desenvolvimento dos capítulos subseqüentes.

O conceito de grupo é a parte central da teoria de códigos, desempenha um papel fundamental na geração, decodificação e análise de desempenho de códigos corretores de erros.

Neste sentido, seja G um conjunto não vazio. Definimos uma operação entre pares de elementos (x, y) de G, denotada por:

$$* : G \times G \to G$$

$$(\mathrm{x}, \mathrm{y}) \rightsquigarrow \mathrm{x} * \mathrm{y}$$

Dizemos que G possui uma estrutura de grupo via a operação $*$ se as seguintes propriedades descritas a seguir forem satisfeitas.

i) Associativa, isto é, $a * (b * c) = (a * b) * c, \ \forall a, b, c \in G$.

ii) Identidade de G, ou seja, existe um elemento e em G tal que $e * g = g * e = g, \forall g \in G$.

iii) Inverso de g, que denotamos por g^{-1}, ou seja, para $\forall g \in G$, existe um único elemento g^{-1} em G com a propriedade de que $g^{-1} * g = g * g^{-1} = e$.

Exemplo 2.8.1 O conjunto dos inteiros $\mathbb{Z}$ sob a operação de adição satifaz a propriedade associativa, tomando $e = 0$, satisfaz a propriedade (ii) e para todo $a \in \mathbb{Z}$ não nulo tomando $a^{-1} = -a$, facilmente mostra-se a propriedade (iii), ou seja, $\mathbb{Z}$ é um grupo aditivo.

Dado um elemento a em um grupo G, caso todos os elementos de G sejam gerados pelo elemento a, denotamos $G = \{a^n | n \in \mathbb{Z}\}$. A notação $G = \{a^n | n \in \mathbb{Z}\}$ significa que estamos tomando $a^n = a * ... * a$ (n-vezes), caso a operação em G seja satisfeita, então $G = \langle a \rangle$ é um grupo cíclico gerado por a.

Exemplo 2.8.2 Os inteiros $\mathbb{Z}$ sob adição ordinária formam um grupo cíclico gerado por 1, ou seja, $\mathbb{Z} = \langle 1 \rangle$.

Definição 2.8.1 Sejam G um grupo e G' um subconjunto não vazio de G. Dizemos que G' é um subgrupo de G se G' for ele próprio um grupo sob a operação herdada do grupo G.

Dessa forma, para que G' seja um subgrupo são necessários satisfazer as condições abaixo, mas essas condições não são suficientes para que G′ seja um subgrupo.

i) $e \in G'$.

ii) $a, b \in G'$ então $ab \in G'$.

A próxima Proposição estabelece condições necessárias e suficientes para que G' seja um sugrupo de G. Se G' for um subgrupo de G, denotaremos $G' \leq G$.

Proposição 2.8.1 Seja G um grupo e G' um subconjunto de G. As seguintes condições são equivalentes:

i) G' é um subgrupo de G.

ii) $e \in G'$

iii) $a, b \in G'$ então $ab \in G'$

iv) $\forall g \in G'$ tem-se $g^{-1} \in G'$

v) $G' \neq \emptyset$ e $\forall a, b \in G'$ tem-se $a.b^{-1} \in G'$.

Demonstração: ver em (Gonçalves, 2003)

Exemplo 2.8.3 Dado m um inteiro positivo qualquer, o conjunto do múltiplos de m que denotaremos por $G = m\mathbb{Z} = \{t = mn | n \in \mathbb{Z}\}$ possui uma estrutura de grupo aditivo associado e sendo um subgrupo aditivo de $\mathbb{Z}$.

Definição 2.8.2 Seja G um grupo e $Q \leq G$. Dizemos que Q é normal em G se $\forall g \in G$ tivermos $gQ = Qg$.

Exemplo 2.8.4 Seja G um grupo dado por $G = \mathbb{Z}$ e $G' = m\mathbb{Z}$ um subgrupo em G. Facilmente, mostra-se que $G' = m\mathbb{Z}$ é um subgrupo normal em $G = \mathbb{Z}$.

Considere agora uma classe de equivalência $\bar{x} = \{y \in G: y \equiv x\ (mod\ S)\}$. Dessa forma, $y \in \bar{x}$ se, e somente se, $y \equiv x\ (mod\ S) \Leftrightarrow yx^{-1} = s \in S \Leftrightarrow y = sx$, para algum $s \in S$.

Definição 2.8.3 Se $Sx = \{sx: s \in S\}$, então $\bar{x}$ é chamado de classe lateral de S em G, tal que $\bar{x} = Sx$.

Para definirmos uma noção de grupo quociente, suponhamos G um grupo e Q um subgrupo normal em G denotado por $Q \prec G$.

Se $x, y \in G, x \equiv y(mod\ Q) \Leftrightarrow xy^{-1} \in Q$, esta operação define uma relação de equivalência em G e $G/Q = \{\bar{g}: g \in G\}$ é conjunto quociente de G por esta relação de equivalência, sendo $\bar{g} = Qg = \{ng: n \in Q\}$ é a classe de equivalência módulo Q tendo g como seu representante.

Como $Q \prec G$, será introduzida uma operação no conjunto das classes G/Q de tal forma que seja um grupo com esta operação e receberá o nome de grupo quociente de G por Q.

Proposição 2.8.2 Se $Q \prec G$, então $\forall x, y \in G, \bar{x}.\bar{y} = \overline{x.y}$ define uma operação no conjunto das classes de G/Q e ainda G/Q é um grupo com essa operação.

Demonstração: explanado em Gonçalves (2003).

Exemplo 2.8.5 Seja G o grupo dado por $G = \mathbb{Z}$ e G' o subgrupo dado por $G' = m\mathbb{Z}$. O grupo quociente $\mathbb{Z}/m\mathbb{Z}$ tem m elementos e $m\mathbb{Z}$ é um subgrupo normal em $\mathbb{Z}$.

Dessa forma, tem-se que $\mathbb{Z}_n$ é obtido como o quociente de $\mathbb{Z}/n\mathbb{Z}$, onde $n\mathbb{Z}$ é um subgrupo normal em $\mathbb{Z}$.

2.9 Anéis e corpos

Dizemos que um anel é um conjunto definido de duas operações $(A + \cdot)$, que será denotada por adição e multiplicação, respectivamente; possuindo as seguintes propriedades:

A_1) Associativa da adição, isto é, $a + (b + c) = (a + b) + c,\ \forall a, b, c \in A$.

A_2) Existência de um elemento neutro na adição chamado zero e denotado por 0 tal que: $a + 0 = 0 + a = a,\ \forall a \in A$.

A_3) Existência de um elemento inverso chamado simétrico $(-a)$, tal que: $a + (-a) = -a + a = 0$, para um dado $a \in A$.

M_1) Comutatividade da adição, isto é, $a + b = b + a$, $\forall a, b \in A$.

M_2) Associativa da multiplicação, isto é, $a.(b.c) = (a.b).c,\ \forall a, b, c \in A$.

M_3) Existência de um elemento neutro na multiplicação chamado unicidade e denotado por 1, tal que: $a.1 = 1.a = a,\ \forall a \in A$.

M_4) Distributividade da multiplicação com relação a adição, ou seja, $a.(b + c) = ab + ac\ \ \forall a, b, c \in A$.

Exemplo 2.9.1 Os inteiros $\mathbb{Z}$ possui uma estrutura de anel sob as operações de adição e multiplicação, satisfazendo as propriedades A_1, A_2 e A_3. Tomando a como elemento neutro, temos que M_3 é satisfeita e as demais.

Outros importantes anéis que faremos uso neste trabalho são dados pelo Exemplo 2.9.2.

Exemplo 2.9.2 Anel dos inteiros de Gauss $\mathbb{Z}[i] = \{x + yi | x, y \in \mathbb{Z}\}$, $i^2 = -1$ e o anel dos inteiros Eisenstein-Jacobi $\mathbb{Z}[\omega] = \{x + \omega y | x, y \in \mathbb{Z}\}, \omega = \frac{1+i\sqrt{3}}{2}$. Ver em Engler e Brumatti, (2001).

Definição 2.9.1 Um elemento $a \in A$ será invertível se existir um elemento $b \in A$ tal que $a.b = 1$. Nesse caso, dizemos que b é um inverso de a.

Exemplo 2.9.3 Note que em $\mathbb{Z}$, somente $a = 1$ ou $a = -1 \in \mathbb{Z}$, são elementos inversíveis em $\mathbb{Z}$.

Definição 2.9.2 Em um anel comutativo, onde todo elemento não nulo é invertível é chamado de corpo.

Definição 2.9.2 Seja $I \subset \mathbb{Z}$. Dizemos que I é um ideal de $\mathbb{Z}$ se a seguintes condições são satisfeitas:

i) $0 \in I$

ii) $x, y \in I \Rightarrow x + y \in I$

iii) $x \in I \Rightarrow -x \in I$

iv) $r \in \mathbb{Z}\ e\ x \in I \Rightarrow rx \in I$

Podemos observar que se as condições (i), (ii), (iii) e (iv) da definição 2.8.2 podem ser substituídas por:

i) $I \neq \emptyset$

ii) $x, y \in I \Rightarrow x - y \in I$.

Exemplo 2.9.4 Seja A um anel dado por $A = \mathbb{Z}$ e seja I um conjunto dado por $I = \{m.n | n \in \mathbb{Z}\}$, ou seja, o conjunto dos múltiplos inteiros de m. Facilmente, pelas propriedades da Definição 2.9.2 verifica-se que I é um ideal em $\mathbb{Z}$.

Exemplo 2.9.5 Seja A um anel dado por $A = \mathbb{Z}[i]$ e seja I um conjunto dado por $I = \{m.a | a \in \mathbb{Z}[i]\}$, onde $m = 1 + 2\text{i}$. Facilmente, pelas propriedades da Definição 2.9.2 verifica-se que I é um ideal em $\mathbb{Z}[i]$.

Exemplo 2.9.6 Seja A um anel dado por $A = \mathbb{Z}[\omega]$ e seja I um conjunto dado por $I = \{m.a | a \in \mathbb{Z}[\omega]\}$, onde $m = 1 + 2\omega$. Facilmente, pelas propriedades da Definição 2.9.2 verifica-se que I é um ideal em $\mathbb{Z}[\omega]$.

3 Códigos convolucionais

3.1 Introdução

Existem duas grandes famílias de códigos corretores de erros: os códigos de bloco e os convolucionais.

Os códigos de bloco são descritos na literatura como códigos sem memória e com as palavras-códigos com mesmo comprimento n, isto é, a codificação de bloco atribui a cada bloco de n bits de informação uma palavra código com k bits codificados. Por outro lado, existe uma bijeção entre as sequências $(\alpha_j) = (\alpha_1, .., \alpha_k)$ e cada palavra-código, sendo que é imposto $k < n$ para que existam redundâncias nas palavras $(\beta_j) = (\beta_1, .., \beta_k)$. Dessa maneira, diz-se que tal código de bloco possui taxa $R = \frac{k}{n}$. Em geral, quanto menor a taxa de um código, maior a sua capacidade de detecção e correção de erros.

A outra família de códigos são os códigos convolucionais, que podem ser vistos como uma classe particular e mais estruturada de códigos de blocos lineares, isto é, as palavras-códigos destes códigos estão estruturadas sob forma de uma treliça. Estes tipos de códigos possuem memória, isto é, os bits codificados dependem não só dos bits de informação como também da informação armazenada pela memória do código e, além disso, o comprimento das palavras-códigos é variável.

O diferencial dos códigos convolucionais em relação aos códigos de bloco é a memória, que é caracterizada da seguinte forma: um bloco de comprimento n (sequência de informação que sai do codificador do canal) resultante da codificação de um bloco de comprimento k (sequência de informação que entra no codificador de canal) depende deste último e dos m blocos de k dígitos armazenados no codificador. Como no caso anterior, impondo $k < n$, o código possui uma taxa $R = \frac{k}{n}$.

3.2 Códigos convolucionais: códigos obtidos a partir de máquina de estado finito

Um codificador pode ser representado por uma máquina de estados finito, que é o nome genérico para máquinas que têm memória dos sinais passados. O termo finito refere-se ao fato de que existe apenas um número de estados único e finito que a máquina pode gerar.

Definição 3.2.1 Uma máquina M é representada pela quíntupla $(\propto, \beta, S, f, g)$ onde $\propto$ representa o conjunto de entradas; β representa o conjunto de saídas; S representa o conjunto de estados; $f: \propto$ x $S \rightarrow S$ representa a função do próprio estado; e $g: \alpha \times S \rightarrow \beta$ representa a função da saída (PALAZZO, 1998).

Da Definição 3.2.1, pode-se descrever o estado e a saída como sendo, respectivamente:

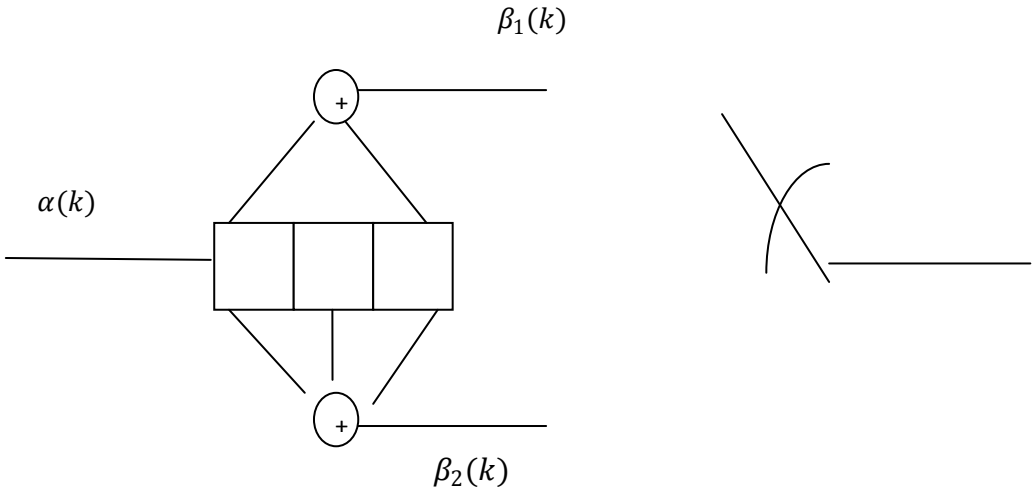
$$s_k = f(\alpha(k-1), \alpha(k-2)) \rightarrow \text{estado}$$

$$\beta(k) = g(s_k, \alpha(k)) \rightarrow \text{saída.}$$

Observa-se que a cardinalidade $|S|$ do conjunto de estado S é finita e para cada $\alpha(k)$ são associadas transições entre os estados com as correspondentes saídas $\beta(k) = (\beta_1(\text{k}), \beta_2(k))$.

Considere o exemplo de um codificador convolucional com memória $m = 2$ e taxa $R = \frac{1}{2}$. Este codificador consiste de um registrador de deslocamento contendo três células, dois somadores $mod\ 2$ e um multiplexador para se realizar a saída codificada. A figura seguinte mostra o esquema deste codificador.

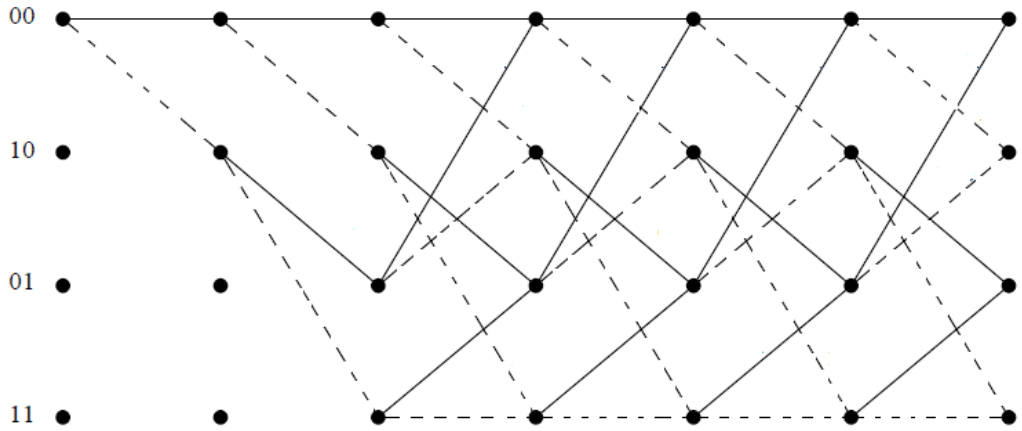
Figura 7- Codificador convolucional binário, $m = 2$ e $R = \frac{1}{2}$.



Fonte: Palazzo (1998)

Uma outra forma de se apresentar um codificador convolucional é através do diagrama de treliça. Para o codificador convolucional mostrado na Figura 7, a sua treliça encontra-se ilustrada na seguinte figura.

Figura 8- Diagrama de Treliça .



Fonte: Guanais (2012)

Cada coluna de nós representa os quatro possíveis estados do codificador e a profundidade da treliça. A partir da coluna de nós mais à esquerda, corresponde ao número de bits que entram no codificador. Assim, as transições resultantes da entrada de um bit 0 no codificador convolucional são representadas por linhas cheias e as transições resultantes da entrada de um bit 1 no codificador convolucional são representadas por linhas tracejadas.

O processo de decodificação para códigos convolucionais não é tão simples como no caso dos códigos de bloco devido ao estágio de memória introduzido no processo de codificação. O método mais conhecido e utilizado para a decodificação é o Algoritmo de Viterbi, que é equivalente a decodificação por máxima verossimilhança.

O algoritmo de Viterbi é descrito da seguinte forma:

A cada unidade de tempo:

- Somar 2^K métricas de ramo às métricas dos caminhos previamente armazenados.
- Comparar as métricas de todos os 2^K caminhos que chegam a cada estado.
- Selecionar o caminho com a maior métrica (sobrevivente).
- Armazenar o caminho sobrevivente e sua métrica.

Uma explanação detalhada de tal algoritmo pode ser conferida em Tarokh et al. (1999).

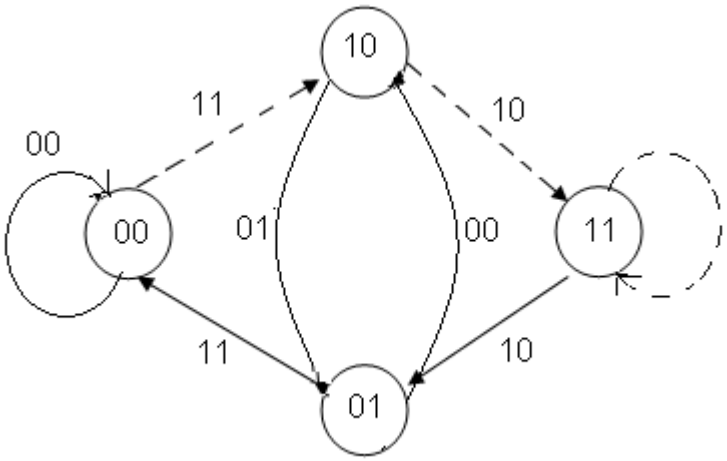
3.3 Enumeração dos pesos das palavras-códigos

As palavras-código de um código convolucional apresentam uma estrutura de grupo, pois satisfazem às propriedades de fechamento, possui elemento inverso aditivo e

elemento identidade aditivo, isto é, o código convolucional forma um código de grupo. Além disso, tal fato é só válido para códigos lineares.

Dessa forma, o diagrama de estado do código convolucional pode ser modificado de tal forma que podemos ter a descrição completa dos pesos de Hamiming w de todas as palavras códigos-códigos não nulas.

Figura 9 - Diagrama de estado do código convolucional com $m = 2$ e $R = \frac{1}{2}$.



Fonte: Palazzo (1998)

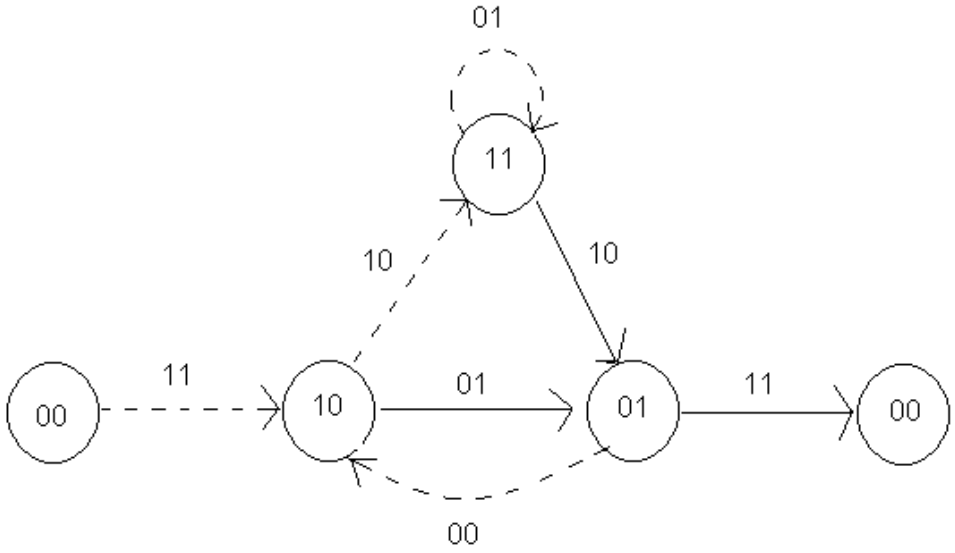
De acordo com a Figura 9, cada círculo representa um estado e cada estado e cada seta representam um transição entre estados. Uma transição parte de um estado no tempo t_i e alcança um estado no tempo $t_i + 1$, mas para que isso aconteça, é necessário que um bit entre para provocar a saída. Por exemplo, para sair do estado 00 e ir para o estado 10 é necessário que o bit de entrada seja 1, o que resulta uma saída 11.

Em geral, para qualquer sequência de informação α existe um caminho no diagrama de estado correspondente à sequência codificada; por exemplo, se $\alpha = (1,0,1,1,1)$, a correspondente sequência codificada será $\beta = (11, 10, 00, 10, 10)$. Todavia, se $\alpha = (0,0,0,0,0)$, a correspondente sequência codificada será $\beta = (00,00,00,00,00)$ e, portanto, o peso de Hamming desta sequência será zero.

No diagrama de estado, para cada transição existe uma função associada a cada transição. Neste diagrama é dentada por D^w, onde w é o peso de Hamming da correspondente transição, e D é a função de Bhattaryya. Sendo assim, todo caminho que inicia e termina no estado zero representa uma palavra código não nula de um código convolucional, o que neste caso, a função de transferência resultante para cada um desses caminhos é obtido pelo produto

das correspondentes funções de transferências das transições (PALAZZO, 1998). O diagrama de estados particionado para o codificador da Figura 7 é mostrado na figura 10.

Figura 10 - Diagrama de estados particionado do codificador convolucional com $m = 2$ e $R = \frac{1}{2}$



Fonte: Palazzo (1998)

Palazzo (1998), para especificar o número de palavras-código com peso de Hamming w, utilizou um polinômio enumerador que pode ser facilmente obtido uma vez que o diagrama de estados particionados possa ser visto como um sistema linear discreto no tempo. As equações de estado e de saída associadas a este sistema linear são dadas respectivamente, por

$$E(i+1) = A(i)E(i) + B(i) \quad (3.2)$$

$$T(i) = C(i)E(i) \quad (3.3),$$

onde, $E(i)$é a matriz de estado que especifica os estados intermediário no instante de tempo $t = i$. No exemplo, esta matriz é da orden 3×1 dada por:

$$E(i) = [\varphi_{i1}\varphi_{i2}\varphi_{i3}];$$

$A(i)$é a matriz de transição que contém os elementos correspondentes às transições entre os estados intermediários. No exemplo, é uma matriz de orden 3×3 dada por:

$$A(i) = \begin{bmatrix} 0 & 1 & 0 \\ D & 0 & D \\ D & 0 & D \end{bmatrix};$$

$C(i)$ é a matriz de saída que especifica as transições entre os estados intermediários e o estado zero. No exemplo, é uma matriz de ordem 3×1 dada por:

$$C(i) = [0 \quad D^2 \quad 0];$$

$B(i)$ é a matriz condição inicial que especifica as transições entre os estados intermediários. No exemplo, é uma matriz de orden 3×1 dada por

$$B^T(i) = [D^2 \quad 0 \quad 0].$$

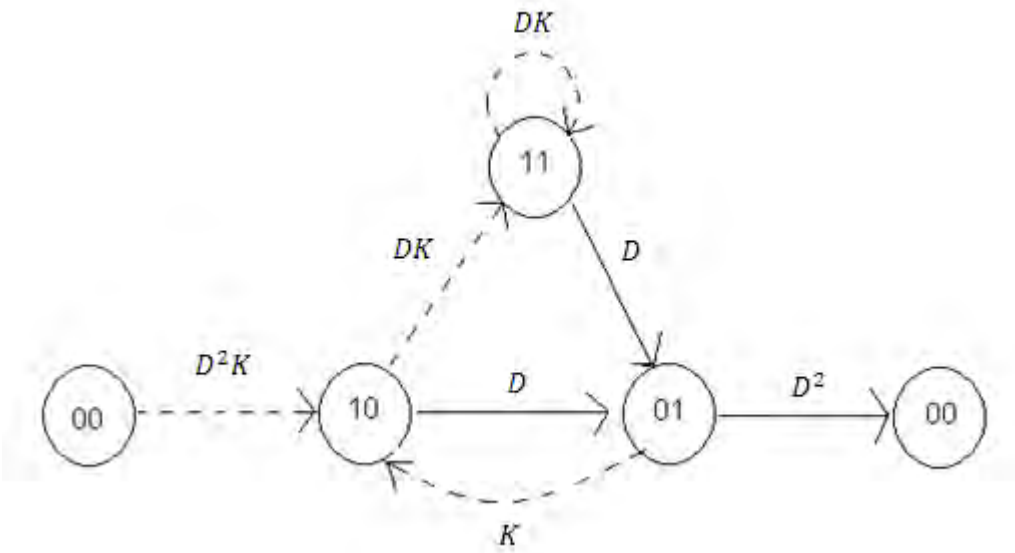
Substituindo nas equações 3.2 e 3.3, resolvendo o sistema temos

$$T(D) = \frac{D^5}{1-2D} = D^5 + 2D^6 + 4D^7 + \cdots \qquad (3.4).$$

Observando a Equação 3.4 podemos dizer que existe um caminho com peso de Hamming 5, dois caminhos com peso de Hamming 6, quatro caminhos com o peso de Hamming 7. Os pesos estão relacionados com o caminho todo nulo.

Todavia, se for necessário determinar o número de dígitos 1 contidos nas sequências, deve-se introduzir uma variável K em todas as transições no diagrama de estados particionados que tenham sido originadas pelo 1 como mostra na Figura 11 .

Figura 11 - Diagrama de estado particionado com *K* incluído.



Fonte: Palazzo (1998)

Dessa forma, as matrizes $A(i)$ e $B(i)$ serão modificadas ao introduzirmos a variável Kpara

$$A(i) = \begin{bmatrix} 0 & K & 0 \\ D & 0 & D \\ DK & 0 & DK \end{bmatrix}$$

$$B^T(i) = [D^2K \quad 0 \quad 0].$$

Do mesmo modo, substituindo nas Equações 2.2 e 2.3, tem-se

$$T(D,K) = \frac{D^5K}{1-2DK} = D^5K + 2D^6K^2 + 4D^7K^3 + \cdots \tag{3.5}$$

Observando a equação 3.5 pode-se dizer que existe um caminho com peso de Hamming 5 cuja a correspondente informação contém somente um único dígito1, dois caminhos com peso de Hamming 6 cuja a correspondente informação contém somente um único dígito1, quatro caminhos com o peso de Hamming 7 cuja a correspondente informação contém somente um único dígito1. Os pesos estão relacionados com o caminho todo nulo.

3.4 Propriedades de distância dos códigos

O desempenho de um código convolucional depende, além do algoritmo de decodificação, das propriedades da distância do código. Neste aspecto, tem-se as seguintes distâncias associadas ao código convolucional :

- distância livre denotada por d_{free} .
- distância de coluna por d_i.
- distância mínima, denotada por d_{min} .

Entre estas distâncias, daremos ênfase na distância livre, pois é a mais importante por estabelecer a capacidade de erro associada ao código convolucional.

Definição 3.4.1 É denominada distância livre d_{free} de um código convolucional como sendo a menor distância de Hamming entre quaisquer duas sequências codificadas provenientes de duas sequências de informação distintas, isto é,

$$d_{free} = \min\{d(\beta_1, \beta_2) : \alpha_1 \neq \alpha_2\},$$

ondeβ_1 e β_2 são as sequências codificadas correspondentes às sequências de informação α_1 e α_2, respectivamente.

Devido ao fato dos códigos convolucionais serem uma classe de códigos de treliça linear, valem as seguintes propriedades de linearidade:

$$d_{free} = \min\{ w(\beta_1 \oplus \beta_2): \alpha_1 \neq \alpha_2 \}, \text{ sendo } \oplus \text{ operação binária,}$$

$$d_{free} = \min\{w(\beta): \alpha \neq 0\}.$$

Portanto, o d_{free} corresponde ao peso mínimo das sequências codificadas de qualquer comprimento sob a condição de que o primeiro bloco das sequências de informação seja diferente de zero, e consequentemente, a distância livre d_{free} corresponde ao peso de Hamming mínimo entre todos os possíveis caminhos na treliça que divergem do estado zero e retornam ao estado zero após algumas transições. Este fato só se aplica em códigos de treliça lineares, como no caso dos códigos convolucionais (PALAZZO, 1998).

Para um melhor entendimento, será retomado o exemplo citado na seção 3.3 na Equação 3.4 obtida pelo polinômio enumerador, de acordo com o diagrama particionado da Figura 3.4.

$$T(D) = \frac{D^5}{1 - 2D} = D^5 + 2D^6 + 4D^7 + \cdots$$

Como já foi visto, os pesos de Haming relacionados ao caminho todo nulo são 5, 6 , 7, ... , e portanto, a distância livre d_{free} é igual a 5 neste exemplo.

4 Códigos Espaço-temporais para sistema de tecnologia MIMO

4.1 Introdução

Com a crescente demanda no mundo da comunicação sem fio móvel, desde o seu surgimento, passaram por uma evolução excepcional na sua tecnologia, desde os primeiros sistemas de comunicações AM e FM, até o desenvolvimento de sistemas de telefonia celular de última geração, que por sua vez exploram modernas técnicas de comunicação digital.

Dessa forma, as tecnologias de transmissões em sistemas de comunicações móveis têm procurado utilizar todos os recursos possíveis para seu aperfeiçoamento para aumentar a capacidade e a confiabilidade destes sistemas. Na literatura, são encontrados conjuntos de técnicas e implementações impressionantes que resultam em melhorias para estes tipos de sistemas de comunicações.

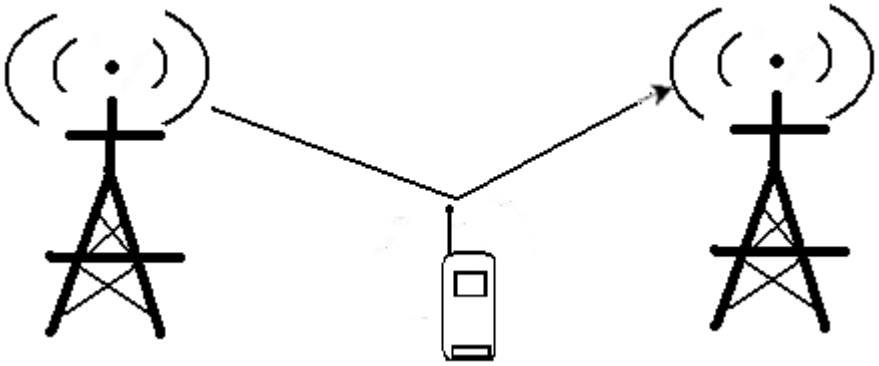
Neste cenário, os códigos espaço-temporais de treliças (CETT) têm recebido especial atenção, uma vez que provêem uma maneira efetiva de explorar completamente a diversidade na transmissão e recepção do canal com um específico tipo de desvanecimento, apresentando uma melhor eficiência no seu desempenho.

Portanto, neste trabalho veremos um método sistemático para a construção de códigos espaço-temporal de treliças (CETT) aplicados em canais com desvanecimento quase-estático e plano. Tal procedimento é baseado na teoria de reticulados, onde será fornecido uma nova estratégia de codificação que aliará de forma combinada conceitos de constelações de sinais casadas a grupos aditivos e constelações de sinais rotacionadas.

4.2 Modelo de sistema de comunicação com múltiplas antenas

Considere a seguinte situação problema na qual um sistema de comunicação no transmissor, está equipado com uma antena que deve transmitir informações para um receptor, também equipado com uma antena, através de um canal sem fio, como ilustrado na Figura 12. (BERHUY; OGGIER, 2009)

Figura 12 - Um canal com uma antena transmissora e uma antena receptora.



Fonte: Guanais (2012)

O sinal que o transmissor deve enviar pode ser representado vetorialmente por $x = (x_1, \dots, x_n) \in \mathbb{C}^n$. No tempo t, $t = 1, \dots, n$, a antena de transmissão envia x_t, que chegará a antena receptora por diferentes caminhos, incluindo algumas reflexões (ocasionado pela natureza do ambiente sem fio). Além disso, x_t será afetada pelo ruído, provenientes de interferências ocasionadas ao longo do percurso. Logo, o que o receptor recebe é um sinal modificado y_t, como descrito na Equação (4.1).

$$y_t = x_t h_t + v_t, \qquad t = 1, \dots, n, \tag{4.1}$$

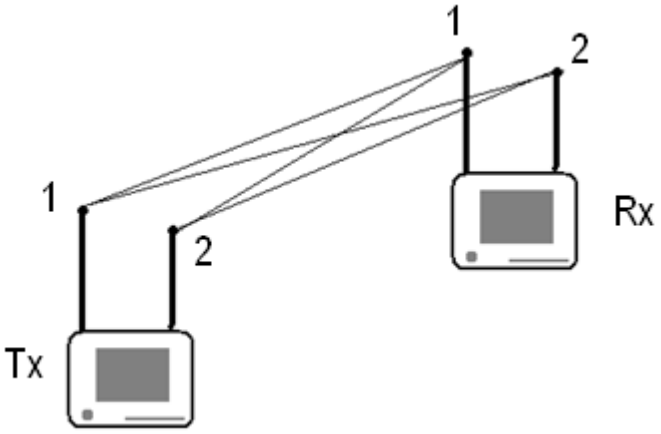
os coeficientes h_t e v_t são variáveis aleatórias complexas Gaussianas, representam respectivamente o desvanecimento (ocasionado pelos multipercursos do sinal) e ruído do canal. Ao reescrever o modelo de transmissão descrito pela equação (4.1) em uma forma matricial, obtem-se que

$$y = xH + v, \tag{4.2}$$

onde, $y = (y_1, \dots, y_n)$ representa o vetor recebido, e H é uma matriz diagonal $n \times n$ chamada matriz do canal. O vetor v contém o ruído H e v são escolhidos de tal forma que tenham coeficientes complexos.

Vejamos a situação em que o canal tenha duas antenas na transmissão e duas antenas na recepção como mostra na Figura 12 abaixo.

Figura 12 - Um canal com duas antenas transmissoras e receptoras.



Fonte: Guanais (2012)

No tempo t, as antenas transmissoras geram os sinais x_{1t} e x_{2t}. Esses sinais serão recebidos pelas duas antenas receptoras, seguindo caminhos diferentes. Os sinais y_{1t} e y_{2t} recebidos por cada uma das antenas receptoras são descritos pelo sistema a seguir:

$$\begin{cases} y_{1t} = h_{11}x_{1t} + h_{12}x_{2t} + v_{1t} \\ y_{2t} = h_{21}x_{1t} + h_{22}x_{2t} + v_{2t} \end{cases} \quad (4.3)$$

h_{ij} denota o desvanecimento ocorrido da antena transmissora i à antena receptora j, e v_{jt} denota o ruído na antena receptora j no tempo t.

O coeficiente de atenuação h_{ij} depende de *t*, como pode ser observado pelo sistema descrito na Equação 4.3. No entanto, é razoável supor que o ambiente não mude tão rápido e que exista um período *T* durante o qual o canal h_{ij} permanece constante. Este período *T* é chamado de intervalo de coerência.

Por exemplo, suponha que o canal permanece aproximadamente constante ao longo de um período de duração $T = 2$, e a transmissão tem início em $t = 1$, onde a antena 1, nos instantes $t = 1$ e $t + 1 = 2$ transmite os sinais x_{11} e x_{12}. Da mesma forma, a segunda antena transmite em t e $t + 1$ os sinais x_{21} e x_{22}. Na recepção, a antena 1 recebe, consecutivamente, um sinal que é a soma dos dois sinais transmitidos com desvanecimento e alguns ruídos, dados por:

$$\begin{cases} y_{11} = h_{11}x_{11} + h_{12}x_{21} + v_{11} \\ y_{2t} = h_{21}x_{11} + h_{22}x_{21} + v_{21} \end{cases}$$

De forma análoga, a segunda antena recebe

$$\begin{cases} y_{21} = h_{11}x_{12} + h_{12}x_{22} + v_{21} \\ y_{22} = h_{21}x_{12} + h_{22}x_{22} + v_{22}. \end{cases}$$

Reescrevendo este modelo de transmissão em forma matricial, obtemos que

$$\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} + \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}.$$

Este modelo pode ser descrito para um sistema mais geral, isto é, para $M \geq 2$ antenas transmissoras e $N \geq 2$ antenas receptoras. No instante *t*, as *M* antenas enviam cada um dos *M* sinais, que podem ser agrupados na forma $x = (x_{1t}, \dots, x_{Mt})^T$. Cada x_{it} será recebida por todas as *N* antenas receptoras. Assim, x_{it} segue *N* caminhos diferentes, cada um correspondendo a um desvanecimento denotado por h_{ji}, $j = 1, \dots, N$ para cada destino.

Para os casos em que $T \geq 2$, onde *T* é a coerência de intervalo de tempo durante o qual o canal é considerado como constante, o modelo de transmissão com múltiplas antenas ao longo de um tempo T de coerência pode ser descrito matricialmente por:

$$Y_{NxT} = H_{NxM} X_{MxT} + V_{NxT},$$

onde todas as matrizes têm coeficientes em $\mathbb{C}$, e suas dimensões são descritas pelos índices denotado dos subconjuntos. Cada coluna da matriz *X* contém o vetor x_t enviadas no tempo *t*. Os coeficientes das matrizes *H* e *V* são dados por variáveis aleatórias complexas Gaussianas.

4.3 Códigos Espaço-temporal de Treliças (CETT).

Tarokh et al. (1998) demonstraram que os sistemas de comunicações na qual a codificação espaço-temporal, provenientes de estados de uma treliça, apresentam uma melhor eficiência, tanto em termos de potência como em termos de largura de banda, em canais ruidosos. Estes códigos são conhecidos na literatura por códigos espaço-temporal de treliça (CETT) que aliam de forma simultânea a diversidade espacial e temporal. Esta técnica tem despertado cada vez mais o interesse da comunidade da teoria de informação porque permite explorar de forma completa a diversidade na transmissão e na recepção. A codificação na dimensão do tempo garante que o ganho de diversidade seja atingido sem comprometer a taxa de transmissão.

Considere um sistema de comunicação móvel com modelo de canal do tipo Rayleigh e desvanecimento plano quase-estático configurado com n_t antenas transmissoras e n_r antenas receptoras.

A cada instante de tempo t, n_t palavras-códigos complexas são transmitidas simultaneamente através de blocos de comprimento l, dados por $n_t(c_t^1, \dots, c_t^{n_t})$, para $t = 1, \dots, n_t$. O sinal recebido pela antena $\mathrm{j}, \mathrm{j} = 1,2, \dots, \mathrm{n_t}$, corrompido pelo desvanecimento do canal é descrito pela Equação 4.4:

$$r_t^j = \sum_{i=1}^{n} \propto_{i,j} c_j^i \sqrt{E_s} + \eta_t^j, \tag{4.4}$$

onde $\mathrm{E_s}$ representa a energia média do sinal transmitido; η_t^j é o ruído aditivo Gaussiano branco complexo (do inglês: Additive White Gaussian Noise-AWGN) com média zero e variância No/2 por dimensão; $\alpha_{i,j}$ denota o desvanecimento presente ao longo do caminho da i-ésima antena transmissora a j-ésima antena receptora.

Uma das vantagens de se trabalhar com os códigos do tipo CETT é que estes são definidos por estruturas de treliças, possibilitando a utilização do algoritmo de Viterbi, que é baseado na distância Euclidiana. O ganho de codificação entre a i-ésima antena transmissora e a j-ésima antena receptora permanece constante durante um quadro de transmissão, mas muda de forma independente de um quadro para o outro.

Dado um par de palavras c e e, considere $\mathrm{P(c \to e)}$ como sendo a probabilidade de um decodificador de máxima verossimilhança decidir erroneamente pela palavra código $\mathrm{e} = \mathrm{e_1^1 e_1^2 \dots e_1^n e_2^1 e_2^2 \dots . e_2^n \dots e_l^1 e_l^2 \dots e_l^n}$, dado que a palavra transmitida tenha sido $\mathrm{c} = \mathrm{c_1^1 c_1^2 \dots c_1^n c_2^1 c_2^2 \dots . c_2^n \dots c_l^1 c_l^2 \dots c_l^n}$.

Assumindo que os parâmetros associados ao desvanecimento $\alpha_{i,j}$ sejam conhecidos, então pode-se mostrar que o limite superior da probabilidade $\mathrm{P\left(c \to e \middle| \alpha_{i,j}, i = 1,2, \dots, n, j = 1,2, \dots, m\right)}$ é exponencial e igual a:

$$\frac{1}{2}\exp\left(-\frac{\mathrm{d^2(c,e)E_s}}{4\mathrm{N_0}}\right), \tag{4.5}$$

onde $\mathrm{d^2(c,e)}$ é dado por:

$$\mathrm{d^2(c,e)} = \sum_{j=1}^{m} \sum_{t=1}^{l} \left| \sum_{j=1}^{n} \alpha_{i,j} \left(c_t^i - e_t^i\right) \right|^2. \tag{4.6}$$

A partir do limitante superior obtido na Equação (4.5), Tarokh et al., (1998), define o ganho de diversidade como o expoente da relação sinal/ruído (SNR)$\left(\frac{Es}{4N_0}\right)$. Por consequência, a diversidade máxima atingida ocorre quando $d^2(c,e)$ for máxima, onde d denota distância Euclidiana.

Por outro lado, desenvolvendo a Equação (4.6) obtém-se uma nova maneira de escrever $\mathrm{d}^2(\mathrm{c},\mathrm{e})$ na forma:

$$\mathrm{d}^2(\mathrm{c},\mathrm{e}) = \sum_{\mathrm{j}=1}^{\mathrm{m}} \sum_{\mathrm{i}=1}^{\mathrm{n}} \sum_{\mathrm{k}=1}^{\mathrm{n}} \alpha_{\mathrm{i,j}}\, \overline{\alpha_{\mathrm{i,j}}} \left(\mathrm{c}_{\mathrm{t}}^{\mathrm{i}} - \mathrm{e}_{\mathrm{t}}^{\mathrm{i}}\right) \overline{\left(\mathrm{c}_{\mathrm{t}}^{\mathrm{k}} - \mathrm{e}_{\mathrm{t}}^{\mathrm{k}}\right)}, \tag{4.7}$$

onde a notação $\bar{\mathrm{a}}$, representa o complexo conjugado do elemento a.

A Equação (4.7) pode ser reescrita matricialmente por:

$$\mathrm{d}^2(\mathrm{c},\mathrm{e}) = \sum_{\mathrm{j}=1}^{\mathrm{m}} \Omega_{\mathrm{j}}\, \mathrm{A}\overline{\Omega_{\mathrm{j}}}, \tag{4.8}$$

onde $\Omega = \left(\alpha_{1,\mathrm{j}}, \alpha_{2,\mathrm{j}}, \ldots, \alpha_{\mathrm{n,j}}\right)$ e $\overline{\Omega} = \left(\overline{\alpha_{1,\mathrm{j}}}\ , \overline{\alpha_{2,\mathrm{j}}}\ \ \ldots, \overline{\alpha_{\mathrm{n,j}}}\right)$.

As entradas $\mathrm{A}_{\mathrm{p,q}}$ da matriz A são obtidas pelos produtos internos $\mathrm{A}_{\mathrm{p,q}} = \sum_{\mathrm{t}=1}^{\mathrm{l}} \left(\mathrm{c}_{\mathrm{t}}^{\mathrm{p}} - \mathrm{e}_{\mathrm{t}}^{\mathrm{p}}\right) \left(\overline{\mathrm{c}_{\mathrm{t}}^{\mathrm{q}} - \mathrm{e}_{\mathrm{t}}^{\mathrm{q}}}\right)$, para $1 \leq p,q \leq n$. Ao substituir $\mathrm{d}^2(\mathrm{c},\mathrm{e})$ na Equação (4.5), verifica-se que a probabilidade de erro com relação ao par $\mathrm{P}\left(\mathrm{c} \to \mathrm{e} \middle| \alpha_{\mathrm{i,j}}, \mathrm{i} = 1,2,\ldots,\mathrm{n}, \mathrm{j} = 1,2,\ldots,\mathrm{m}\right) \leq \prod_{\mathrm{j}=1}^{\mathrm{m}} \exp\left(-\Omega_{\mathrm{j}} \mathrm{A}(\mathrm{c},\mathrm{e}) \overline{\Omega}_{\mathrm{j}} \mathrm{E}_{\mathrm{s}} \middle| 4\mathrm{N}_0\right)$.

Nos Capítulos 5 e 6 será visto uma nova técnica para se obter $\mathrm{d}^2(\mathrm{c},\mathrm{e})$ máxima definida na Equação (4.5). Tal procedimento é baseado na teoria de reticulados onde é fornecida uma nova estratégia de codificação que aliará de forma combinada conceitos de constelações de sinais rotacionadas e partições de reticulados.

Ao fazer uso dos resultados conhecidos da álgebra linear, Tarokh et al. (1998), determinaram dois critérios de análise de desempenho de códigos espaço-temporais quando sujeito a desvanecimento do tipo Rayleigh, como será visto no final deste capítulo.

Para isto, usa-se o fato que se a matriz $A(c,e)$ for hermitiana, então existe uma matriz unitária V ($V^* = V^{-1}$) e uma matriz diagonal D tal que $VA(c,e)V^* = D$.

Assim, as linhas de $V = \{v_1, v_2, \ldots, v_{n_T}\}$ formam uma base ortonormal no espaço $\mathbb{C}^{n_T}$, sendo composta pelos autovetores da matriz $A(c,e)$. Em relação a matriz D, os elementos da diagonal são os autovalores $\lambda_i, 1 \leq i \leq n_T$, da matriz $A(c,e)$, levando em consideração suas multiplicidades.

Dessa maneira,

$$B(c,e) = \begin{bmatrix} (e_1^1 - c_1^1) & (e_2^1 - c_2^1) \ldots & (e_l^1 - c_l^1) \\ (e_1^2 - c_1^2) & (e_2^2 - c_2^2) \quad \ldots & (e_l^2 - c_l^2) \\ \vdots & \vdots & \vdots \\ (e_1^{n_T} - c_1^{n_T}) & (e_2^{n_T} - c_2^{n_T}) \quad \ldots & (e_l^{n_T} - c_l^{n_T}) \end{bmatrix}$$

é a raiz quadrada da matriz $A(c,e)$, sendo que $B(c,e)B^*(c,e) = A(c,e)$, então conclui-se que os autovalores da matriz $A(c,e)$ são números reais não negativos.

Chamando de $\omega_j V^* = (\beta_{1j}, \beta_{2j}, \ldots, \beta_{n_T j})$, tem-se que

$$\omega_j A(c,e)\omega_j^* = \sum_{i=1}^{n_T} \lambda_i \left|\beta_{ij}\right|^2,$$

onde

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

Portanto,

$$p\left(c \to e \middle| \alpha_{ij}, 1 \le i \le n_T, 1 \le j \le n_R\right) \le \prod_{j=1}^{n_R} exp\left(-\frac{Es}{4N_0} \sum_{i=1}^{n_T} \lambda_i \left|\beta_{ij}\right|^2\right). \tag{4.9}$$

Como a matriz $V = \{v_1, v_2, \ldots, v_{n_T}\}$ é unitária e forma uma base ortogonal para o espaço $\mathbb{C}^{n_T}$ e β_{ij}, $1 \le i \le n_T, 1 \le j \le n_R$, são variáveis aleatórias Gaussianas complexas independentes com variância

$$\sigma^2[\beta_{ij}] = var\left[\sum_{k=1}^{n_T} \alpha_{kj}\, \overline{v_{ik}}\right]$$

$$\sigma^2[\beta_{ij}] = \sum_{k=1}^{n_T} \|v_{ik}\|^2\, var\left[\alpha_{kj}\right]$$

$$\sigma^2[\beta_{ij}] = var\left[\alpha_{kj}\right]$$

$\sigma^2[\beta_{ij}] = \frac{1}{2}$ por dimensão e média dada por

$$E\left[\propto_{ij}\right] = E\left[\sum_{k=1}^{n_T} \alpha_{kj}\, \overline{v_{ik}}\right]$$

$$E\left[\propto_{ij}\right] = \sum_{k=1}^{n_T} E\left[\alpha_{ij}\right] \overline{v_{ik}}$$

$$E[\propto_{ij}] = K^j . v_i$$

onde

$$K^j = (E[\alpha_{1j}], E[\alpha_{2j}], \dots, E[\alpha_{n_T j}]).$$

Para o canal que apresenta desvanecimento do tipo Rayleigh, tem-se $E[\alpha_{ij}] = 0$ e, consequentemente, $k_{ij} = 0$, para $1 \leq i \leq n_T, 1 \leq j \leq n_R$, e portanto a probabilidade de se escolher e quando c é transmitido é limitada superiormente por

$$p(c \to e) \leq \left(\frac{1}{\prod_{i=1}^{n_T} 1 + \frac{Es}{4N_0}\lambda_i} \right)^{n_R} \leq \frac{1}{(\prod_{i=1}^{r} \lambda_i)^{n_R} \left(\frac{Es}{4N_0}\right)^{n_R r}}, \quad (4.10)$$

sendo $r \leq n_T$ o posto da matriz $B(c,e)$ e $\lambda_1, \lambda_2, \dots, \lambda_r$ os autovalores não-nulos da matriz $A(c,e)$.

Da relação obtida no denominador do termo mais a direita da desigualdade dada pela Equação 4.10, conclui-se que um ganho de diversidade igual a $n_R r$ é alcançado. Portanto, o ganho de codificação é igual a $(\lambda_1, \lambda_2, \dots, \lambda_r)^{\frac{1}{r}}$ que corresponde a uma medida aproximada do ganho obtido em relação a um sistema não codificado operando com o mesmo ganho de diversidade (TAROKH et al.1998).

Como consequência, obtém os seguintes critérios na análise de desempenho de códigos espaços-temporais quando submetidos ao desvanecimento do tipo Rayleigh, dado por:

- **Critério do Posto:** Para que se consiga a diversidade máxima igual a $n_R n_T$, a matriz $B(c,e)$ deve ter posto completo para qualquer par de palavra-código c e e . No entanto, se essa matriz possui um posto mínimo r para um dado par de palavra-código distintas, então uma diversidade igual a $n_R r$ é obtida.
- **Critério do Determinante:** Para se obter a diversidade máxima igual a $n_R n_T$, suponha-se que uma diversidade igual a $n_R r$é alcançada. Como o ganho de codificação corresponde ao produto $(\lambda_1 \lambda_2 \dots \lambda_r)$ que é o valor mínimo das raízes r-ésimas da soma dos determinantes de todos os cofatores principais $r \times r$ da matriz $A(c,e)$ calculados para todos os pares de palavras-códigos distintas c e e. Sendo assim, o valor mínio do determinante da matriz $A(c,e)$, calculado para todos os pares de palavras-códigos distintas, deve ser maximizado.

5 Reticulados e constelações de sinais

5.1 Introdução

Um reticulado Λ é um conjunto infinito de pontos em $\mathbb{R}^n$ que herda uma estrutura de grupo aditivo, representa uma importante ferramenta algébrica-geométrico no estudo da teoria de informação, principalmente em problemas relacionados à teoria de códigos. Diz-se que Λ é um reticulado de dimensão n completo em $\mathbb{R}^n$, se existe um conjunto de vetores dado por $\beta = \{v_1, \dots, v_n\}$ linearmente independente em $\mathbb{R}^n$, tal que, Λ seja gerado por β, isto é, $\Lambda = \{x = \sum_{i=1}^{m} \lambda_i \, v_i, \lambda_i \in \mathbb{Z}^n\}$. (5.1)

O conjunto β é chamado de base do reticulado. Neste trabalho, faremos uso apenas dos reticulados completos.

Exemplo 5.11 Se tomarmos $n = 1$ a partir da Equação 5.1, obtemos o reticulado $\Lambda = \mathbb{Z}$, isto é, o conjunto dos números inteiros que possui uma estrutura de grupo aditivo associado. A base mais natural é dado por $\beta = \{1\}$. Assim, $\forall\, n \in \mathbb{Z}$, obtemos $\Lambda = \mathbb{Z} = \{n = n.1 | n \in \mathbb{Z}\}$.

Associado uma base β de cardinalidade n, então existe uma matriz geradora M de ordem n, onde as n colunas são formadas pelos n vetores da base β e as n linhas são obtidas a partir das n coordenadas dos vetores da base β. Cada vetor $x = (x_1, \dots, x_n) \in \Lambda$ pode ser escrito na forma $\mathrm{x} = \xi_1 \mathrm{v}_1 + \cdots + \xi_\mathrm{n} \mathrm{v}_\mathrm{n} = \xi \mathrm{M}$, onde os elementos ξ_i são inteiros e $\xi = (\xi_1, \dots, \xi_n)$. Define-se a norma N de um vetor $x \in \Lambda$ da seguinte forma:

$N(x) = N(\xi_1 v_1 + \cdots + \xi_n v_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} \xi_i \, \xi_j \, v_i v_j = \xi . G . \xi^{tr} = f(\xi)$, (5.1)

onde $G = M . \bar{M}^{tr}$ e $\bar{M}^{tr}$ representa a matriz transposta conjugada de M. A função $f(\xi)$ das n variáveis $\xi_1, \dots, \xi_n$ é chamada de forma quadrática associada ao reticulado Λ.

Note que a partir da Equação 5.1, se tomarmos $n = 2$ e a base mais natural em $\mathbb{R}^2$, isto é, a base canônica $\beta = \{v_1, v_2\}$, onde $v_1 = (1,0)$ e $v_2 = (0,1)$, então obtemos o reticulado $\Lambda = \mathbb{Z}^2$ descrito no próximo exemplo.

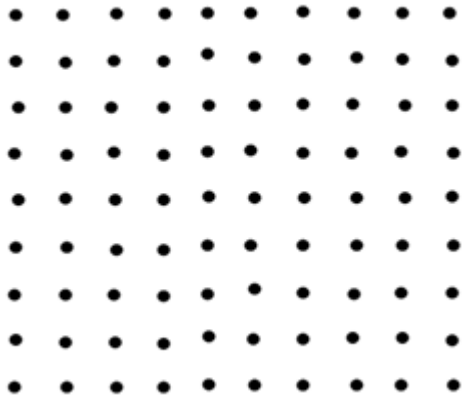
Exemplo 5.1.2 O reticulado $\Lambda = \mathbb{Z}^2$ é gerado pela base $\beta = \{v_1, v_2\}$, onde $v_1 = (1,0)$ e $v_2 = (0,1)$, tem como matriz geradora

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

A forma quadrática associada a cada elemento $\xi \in \mathbb{Z}^2$ é dada por $f(\xi) = \xi_1^2 + \xi_2^2$. O reticulado $\mathbb{Z}^2$ é identificado de forma natural com o anel dos inteiros de Gauss $\mathbb{Z}[i] =$

$\{x + iy | x, y \in \mathbb{Z}\}$, onde $i^2 = -1$. Cada elemento $(x, y) \in \mathbb{Z}^2$ corresponde de forma biunívoca a um único elemento $x + iy \in \mathbb{Z}[i]$.

Figura 14- Reticulado $\mathbb{Z}^2$



Fonte: Guanais (2012)

Note que se considerarmos em $\mathbb{R}^2$ outra base β' diferente da base β do Exemplo 5.1.2, dada por $\beta' = \{v_1, v_2\}$ onde $v_1 = (1,0)$ e $v_2 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, então obtemos um outro reticulado de dimensão 2, como descrito no próximo Exemplo.

Exemplo 5.1.3 O reticulado $\Lambda = \mathbb{A}_2$ (também, conhecido por reticulado hexagonal) é gerado pela base $\beta = \{v_1, v_2\}$, onde $v_1 = (1,0)$ e $v_2 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, e tem como matriz geradora

$$M = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

A forma quadrática associada a cada elemento $\xi \in \mathbb{A}_2$ é dada por $f(\xi) = \xi_1^2 + \xi_1\xi_2 + \xi_2^2$. O reticulado $\mathbb{A}_2$ é identificado de forma natural com o anel dos inteiros de Eisenstein-Jacobi $\mathbb{Z}[\omega] = \{x + \omega y | x, y \in \mathbb{Z}\}$, que possui uma estrutura de grupo aditivo associado, onde $\omega = \frac{1+i\sqrt{3}}{2}$. Cada elemento $(x, y) \in \mathbb{A}_2$ corresponde de forma biunívoca a um único elemento $x + \omega y \in \mathbb{Z}[\omega]$.

Figura 15- Reticulado $\mathbb{A}_2$

Fonte: Guanais (2012)

A seguir apresentaremos algumas propriedades de reticulados que faremos uso no final deste capítulo.

2.5.1 Propriedades de reticulados

Seja Λ um reticulado de dimensão n. A partir de Λ podemos obter novos reticulados através das seguintes operações:

i) Seja $r \in \mathbb{R}$, então $r\Lambda$ é um reticulado que consiste de todos os múltiplos $r\Lambda$ de todos vetores $v \in \Lambda$ por um escalar r.

ii) Se T é uma dada transformação ortogonal de um espaço de dimensão n, então $T\Lambda$ é um reticulado que consiste de todas transformação Tv de todos vetores $v \in \Lambda$ via transformação T. Dizemos que $T\Lambda$ é uma versão rotacionada do reticulado Λ.

Observação 5.1 Se um reticulado Λ_2 é obtido a partir de um reticulado do Λ_1 via qualquer umas das operações (i) ou (ii), então dizemos que Λ_1 e Λ_2 são reticulados equivalentes, e mais, se M_1 e M_2 então $M_1 = UM_2U^T$, onde U^T é uma matriz transposta de $T\ e\ \det(U) = 1$.

Exemplo 5.1.4 Seja a transformação ortogonal dada pela rotação T, onde

$T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Note que $T\mathbb{Z}^2$ é uma versão de $\mathbb{Z}^2$ obtida pela rotação de $\mathbb{Z}^2$ por $\frac{\pi}{4}$ rad. Logo pela Observação 5.1 segue que $T\mathbb{Z}^2$ é um reticulado equivalente ao reticulado $\mathbb{Z}^2$.

2.5.2 Subreticulados e cadeias de partições de reticulados.

Sejam Λ um reticulado dado e Λ' um subconjunto de Λ. Dizemos que um subconjunto Λ' é um subreticulado de Λ, se Λ' possui uma estrutura de grupo aditivo associado. Em outras palavras, Λ' é um subgrupo aditivo do grupo aditivo Λ.

Exemplo 5.1.5 Seja m um inteiro positivo qualquer, e o conjunto dos inteiros múltiplos de m que denota por $\Lambda' = m\mathbb{Z}$. Assim, $m\mathbb{Z}$ possui uma estrutura de grupo aditiva associada e é um subgrupo aditivo do grupo aditivo $\mathbb{Z}$, ou melhor, os inteiros múltiplos de m é um subreticulado de $\mathbb{Z}$, isto é, podemos escrever Λ' na forma,

$$\Lambda' = m\mathbb{Z} = \{t = m.n | n \in \mathbb{Z}\}.$$

Seja Λ' um reticulado de Λ, logo Λ' é um subgrupo aditivo do grupo aditivo Λ.

Então, faz sentido considerar o grupo quociente do reticulado Λ por um subreticulado Λ'. Uma vez que a operação de grupo aditivo Λ/Λ' está bem definido.

Logo, Λ' induz uma partição no reticulado Λ via classes de equivalência módulo Λ'.

Exemplo 5.1.6 Seja m um inteiro positivo. O subgrupo $m\mathbb{Z}$ dos múltiplos inteiros de m é um subreticulado de $\mathbb{Z}$. O grupo quociente $\mathbb{Z}/m\mathbb{Z}$ geometricamente representa uma partição do conjunto dos inteiro em m classe de equivalência módulo m. Como $|\mathbb{Z}/m\mathbb{Z}| = m$, então os representantes das classes laterais desta partição são dados por $\{0,1,\dots,m-1\}$.

Note que $\forall\, x \in \mathbb{Z}$, temos pelo algoritmo da divisão de Euclides que $x = am + b$, onde $b \in \{0,1,\dots,m-1\}$ e $am \in m\mathbb{Z}$ (múltiplos de m). Os elementos $b \in \{0,1,\dots,m-1\}$ representa as classes de restos módulo m, ou seja, os elementos do anel $\mathbb{Z}_m$. Ou melhor, temos que $\mathbb{Z}_m \simeq \mathbb{Z}/m\mathbb{Z}$.

Uma cadeia de partição de reticulados $\Lambda/\Lambda'/\Lambda''$ é uma sequência de reticulados, onde cada novo reticulado da sequência é um subreticulado do seu antecessor. Em outras palavras, tem-se que $\Lambda \supseteq \Lambda' \supseteq \Lambda'' \supseteq \cdots$

Exemplos 5.1.6: A partição de reticulados dada por $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}$ ...

Observe que temos $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots$.

5.2 Esquemas de modulação a partir dos reticulados $\mathbb{A}_2$ e $\mathbb{Z}^2$.

Um fato bem conhecido na literatura é que as modulações QAM e HEX estão associados aos reticulados $\mathbb{Z}^2$ e $\mathbb{A}_2$, respectivamente. Como visto nos Exemplos 5.1.2 e 5.1.3 as formas quadráticas $f(x,y) = x^2 + y^2$ e $g(x,y) = x^2 + xy + y^2$ estão associados

respectivamente aos anéis de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$. Por outro lado, os anéis $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$, por sua vez estão associados a $\mathbb{Z}^2$ e $\mathbb{A}_2$, respectivamente.

Como conseqüência destas identificações, baseando nas formas quadráticas e em propriedades algébricas da teoria de números, vários trabalhos, Huber (1994), Nóbrega et al. (2001) e Carvalho et al. (2008), proporam procedimentos de construções de constelações de sinais via partições de reticulados por subreticulados.

Huber (1994) e Nóbrega et al. (2001), propuseram uma estratégia de codificação sobre um grupo aditivo associado aos p sinais de modulação empregada, isto é, como as constelações são descritos por formas quadráticas, e assim as soluções dessas equações fornecem simultaneamente um procedimento algébrico e geométrico para a classe dos códigos sobre corpos de Galois, associados aos p sinais das modulações.

5.3 Constelações de sinais provenientes de reticulados casadas a grupos aditivos.

Huber (1994) e Nóbrega et al. (2001) propuseram procedimentos algébricos para se obter constelações de sinais casadas a grupos aditivos provenientes da estrutura aditiva dos corpos de Galois $GF(p)$. Tais grupos aditivos são isomorfos a reticulados (dados por um anel de inteiros de Gauss ou anel de inteiros de Eisenstein-Jacobi) por subreticulados (ideais destes anéis). Esses procedimentos foram baseados em resultados clássicos da teoria dos números. Assim, se um inteiro primo p é escrito como soma de quadrados de inteiros, isto é, se $p = a^2 + b^2$, com $a, b \in \mathbb{Z}$, ou se p é escrito da forma $p = a^2 + ab + b^2$, com $a, b \in \mathbb{Z}$, então, dado um inteiro primo p, existe uma constelação de sinais U de cardinalidade p proveniente do reticulado $\mathbb{Z}[i]$ casada ao grupo aditivo G do corpo de Galois $GF(p)$ se $p = 2$ *ou* $p \equiv 1\ (mod\ 4)$ (HUBER, 1994;NÓBREGA et al. 2001).

Para o caso do reticulado $\mathbb{Z}[\omega]$, dado um inteiro primo p, existe uma constelação de sinais U de cardinalidade p proveniente do reticulado $\mathbb{Z}[\omega]$ casada ao grupo aditivo de $GF(p)$ se $p = 3$ *ou* $p \equiv 1\ (mod\ 6)$ (HUBER, 1994;NÓBREGA et al. 2001).

Convém, observar que encontrar pares de inteiros (a, b) e (c, d) tais que $a^2 + b^2 = p$ e $c^2 + cd + d^2 = p$, significa que a e b são soluções inteiras da forma quadrática $f(x, y) = x^2 + y^2 = p$ e que c e d são soluções inteiras da forma quadrática $g(x, y) = x^2 + xy + y^2 = p$.

Carvalho et al. (2008) estendeu os resultados apresentados em Huber (1994) e Nóbrega et al. (2001) mostrando que dado um inteiro primo p, existe uma constelação de sinais U de cardinalidade p^n $(n \geq 1)$ casada a um grupo aditivo G de cardinalidade p^n, se

$p = 2\ e\ p \equiv 1\ (mod\ 4)$ *ou se* $p = 3\ e\ p \equiv 1(\ mod\ 6)$ a partir dos reticulados $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente.

O procedimento proposto em Carvalho et al.(2008) para se estabelecer um método de construção de uma constelação de sinais U de cardinalidade p^n, casada a um grupo aditivo G de cardinalidade p^n, equivale do ponto de vista algébrico, determinar ideais I em $\mathbb{Z}[\theta]$(para $\theta = i$ ou ω) de norma relativa p^n, que satisfaçam à condição de que $G \simeq \mathbb{Z}[\theta]/I$.

Assim, os elementos de G podem ser vistos como classes de equivalências de $\mathbb{Z}[\theta]$, cujos representantes são dados por $0, \dots , p^{n-1} - 1$. Desde que $\theta \in \mathbb{Z}[\theta]$, segue-se então que θ pertence a alguma classe lateral $\bar{s} \in \mathbb{Z}[\theta]/I$, com $0 \leq s \leq p^n - 1$, onde a norma relativa de θ é s. Ao tomar-se um dado elemento $x + y\theta$ que pertence a alguma classe lateral $\bar{l} \in \mathbb{Z}[\theta]$/I, com norma relativa l, onde $0 \leq s \leq p^n - 1$, obtem-se, $\overline{x + y\theta} = \bar{x} + \overline{ys} = \overline{x + ys} = \bar{l}$. Assim,

$$x + y\theta \equiv l(mod I) \Leftrightarrow x + ys \equiv l(mod l). \tag{5.2}$$

Um elemento $l \in G$ é um rótulo de um ponto $x + y\theta \in \mathbb{Z}[\theta]$, se a equação $x + yr \equiv l(mod p^n)$ for satisfeita. Para isso, é suficiente encontrar uma única solução $r \in \mathbb{Z}$ para a equação $x + ys \equiv 0(mod p^n)$, onde $0 \leq s \leq p^n - 1$ (CARVALHO et al. 2008).

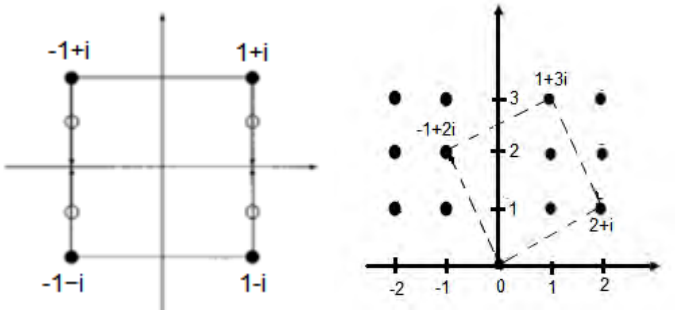
Exemplo 5.3.1 Considere $p = 5$. Note que existe um par de inteiros $(2,1)$ tal que $2^2 + 1^2 = 5$. Logo, existe um ideal $I = \langle 2 + i \rangle \in \mathbb{Z}[i]$ e uma constelação de sinais S de cardinalidade 5 proveniente do reticulado $\mathbb{Z}[i]$, casada ao grupo aditivo do corpo de Galois $GF(5)$ isormofo ao grupo quociente $\mathbb{Z}[i]/I$. Agora se $r = 3$ é uma solução inteira de $2 + s = 5,$ então o rótulo de qualquer elemento $x + yi$ em $\mathbb{Z}[i]$ é obtido através da equação $x + 3y \equiv l\ (mod\ 5)$.

Exemplo 5.3.2 De forma análoga, considerando $p = 7$, encontra-se um par de inteiros $(1,2)$ tal que $1^2 + 1.2 + 2^2 = 7$. Para este caso, obtém-se uma constelação de sinais S de cardinalidade 7 a partir do reticulado $\mathbb{Z}[\omega]$, porém, casada ao grupo aditivo proveniente do corpo de Galois $GF(7)$ isomorfo ao grupo quociente $\mathbb{Z}[\omega]/I$, onde $I = \langle 1 + 2\omega \rangle$. Agora se $r = 3$ é uma solução inteira de $1 + 2s = 7,$ então o rótulo do elemento $x + y\omega$ em $\mathbb{Z}[\omega]$ é obtido a partir da equação $x + 3y \equiv l\ (mod\ 7)$.

5.4 Diversidade de Modulação máxima Provenientes de Reticulados.

A diversidade de um sistema de comunicação pode ser maximizada desde que se utilize específicas constelações de sinais, ou seja, aplicando a técnica denominada de diversidade de modulação (BOUTROS;VITERBO, 1998). Do ponto de vista geométrico, como visto na Seção 2.7.1, a diversidade de modulação é caracterizada pela ação de uma rotação na constelação S, de modo que o número de componentes distintas seja máximo. A figura 16 ilustra este procedimento para constelação bidimensional com 4 sinais.

Figura 16- constelação bidimensional com 4 sinais.



(I) (II)

Fonte: Guanais (2012)

Note que ao considerarmos os sinais da primeira constelação S da Figura 5.3 como vértice de um quadrado, tem-se que S é dado por $S = \{-1-i, -1+i, 1+i, 1-i\}$. Transladando e rotacionando a constelação S de forma conveniente, obtemos uma nova constelação $S' = \{0+0i, -1+2i, 1+3i, 2+i\}$.

Observação 5.2 Observe que a constelação S' apresenta diversidade máxima em cada componente real e complexa, ou seja, qualquer elemento de S' difere dos demais elementos de S' e a distância de Hamming entre quaisquer dois elementos é 2 (máxima possível). O que não acontece com a constelação S.

As constelações de sinais obtidas via uma rotação, como ilustrada na Figura 16 são conhecidas por constelações de sinais rotacionadas. Em espaços Euclidianos n-dimensionais, as constelações podem ser caracterizadas como um reticulado na forma cúbica do tipo $\mathbb{Z}^n$. Um ponto x da constelação rotacionada é obtido pela ação de uma matriz M em u, ou seja, é o conjunto dos pontos $\{x = uM, u \in \mathbb{Z}^n\}$. No caso, bidimensional o reticulado é dado por $\mathbb{Z}^2$e a sua matriz de rotação tem a seguinte forma:

$M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, com $a, b \in \mathbb{Z}^2$, satisfazendo a condição de que $a^2 + b^2 = 1$.

Exemplo 5.4.1 Os sinais da constelação S' da Observação 5.2 são escritos via inteiros de Gauss que de forma natural são identificados por elementos de $\mathbb{Z}^2$, como visto, no Exemplo 5.1.1. Assim, os sinais de S' é descritos na forma $S' = \{(0,0), (1,-2), (1,3), (2,1)\}$.

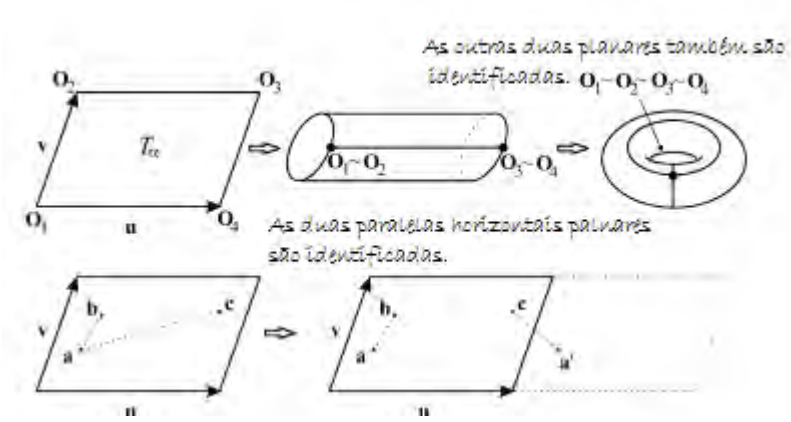
Tomando $(\mathrm{a}, \mathrm{b}) = (1,0)$ tem-se que para todo $(\mathrm{c}, \mathrm{d}) \in S'$ é obtido via o produto $(c,d) = uM$, onde $u = (c,d) \in \mathbb{Z}^2$ e $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

Outra versão das constelações de sinais rotacionadas existentes em espaços Euclidianos, mas apenas para os casos que sejam da forma $2n$-dimensionais, são as constelações caracterizadas como um reticulado da forma $\mathbb{A}_2{}^n$. Um dado ponto x da constelação rotacionada é obtido pela ação de uma matriz M' em u, ou seja, é o conjunto dos pontos $\{x = uM, u \in \mathbb{A}_2{}^n\}$.

5.5 Constelações de sinais identificados a grupos cíclicos $\mathbb{Z}_n$e toros planares.

Dada uma base $\propto = \{u, v\}$ de $\mathbb{R}^2$, um toro planar é algebricamente definido pelo espaço quociente $T_\alpha = \mathbb{R}^2/\Lambda_\alpha$, onde Λ_α é o reticulado gerado pela base α. Maiores detalhes ver Costa et al. (2004). A figura 17 ilustra essa situação.

Figura 17- Toro Planar



Fonte: Costa et al (2004)

A distância medida no toro planar T_α entre as classes laterais $\bar{a}$ e $\bar{b}$ de a e b com $a, b \in \mathbb{R}^2$ é dado por $d_\alpha(\bar{a}, \bar{b}) = min\{d(z,y) = \|z - y\|; z \in \bar{a}, y \in \bar{b}\}$, onde $\|x\| = \sqrt{\sum_{i=1}^{2} x_i^2}$ a norma de um vetor em $\mathbb{R}^2$. A figura 17 mostra que no toro planar as distâncias $d_\alpha(\bar{a}, \bar{b})$, onde $\bar{a}$,$\bar{b}$ e $\bar{c}$ são classes laterais na sequência de a, b e $c \in T_\propto$.

Assim, Costa et al. (2004) estabeleceram quais são as condições necessárias para se obter uma tesselação em $\mathbb{R}^2$ a partir de uma tesselação no toro planar $T_{\propto}$. Em particular ao considerar $\propto = \{u, v\}$, onde $u = (1,0)$ e $v = (0,1)$, Λ_α gera uma tesselação em $\mathbb{R}^2$ dada por quadrados, todos congruentes.

Tomando uma nova base no plano dado por $\propto = \{w_1, w_2\}$, com $w_1 = (1,0)$ e $w_2 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, tem-se que Λ_α gera um tesselação hexagonal no plano, onde todos os hexagonos são congruentes.

A Proposição 5.5.1 estabelece condições para se obter uma constelação de sinais casadas a um grupo cíclico $\mathbb{Z}_n$ proveniente do reticulado $\mathbb{Z}^2$, ou seja, quando os sinais são identificados por elementos do grupo cíclico $\mathbb{Z}_n$.

Proposição 5.5.1 Sejam $u = (a, b)$ e $v = (c, d)$ e $D = |ad - bc|$. Se $mdc(a, c) = 1$ então grupo $\mathbb{Z}^2/\Lambda_\alpha$ é isomorfo ao grupo cíclico $\mathbb{Z}_n$ (COSTA et al.2004).

Observação 5.3 No reticulado Λ_α de $\mathbb{Z}^2$ ao tomarmos como matriz geradora $\mathrm{M} = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ -\mathrm{b} & \mathrm{a} \end{pmatrix}$, desde que $mdc\,(a, b) = 1$, segue que o grupo $\mathbb{Z}^2/\Lambda_\alpha$ é isomorfo a $\mathbb{Z}_n$ e ao considerarmos uma base $\beta = \{\mathrm{u}', \mathrm{v}'\}$, onde $\mathrm{u}' = (1,0)$ e $\mathrm{v}' = (0,1)$, segue que Λ_α gera uma tesselação em Λ_α dados por quadrados congruentes.

A proposta de codificação que será apresentada no próximo capítulo se baseará em grupos cíclico, o que de fato é de suma importância para esta caracterização.

5.6 Representação geométrica em forma de paralelogramo para constelações de sinais casadas a grupos aditivos.

No capítulo 6, apresentaremos um procedimento algébrico e geométrico para codificação baseadas nas propostas de Tarokh et al. (1998) e Valença (2001). A proposta de Valença (2001) faz uso dos quadrados latinos, no sentido de fundamentar um procedimento algébrico e geométrico desta proposta, estendê-la a uma situação mais geral é o que apresentamos estas específicas constelações de sinais descritas a seguir.

Considere as particulares constelações de sinais de cardinalidade m^2 (com m sendo uma potência de um inteiro primo) proveniente do reticulado $\mathbb{Z}[i]$ ou $\mathbb{Z}[w]$. Porém, de tal forma que seus pontos sejam rotulados por elementos de grupos quocientes aditivos G de cardinalidade p^n, como proposto em Carvalho et al. (2008). Em outras palavras, assume-se $S = \{j + k\theta \in \mathbb{Z}[\theta],\ j \in \{0, \dots, p^n - 1\};\ k \in \{0, \dots, p^n - 1\}\}$, onde $\theta = i$ ou $\theta = \omega$.

A representação geométrica de S pode ser vista como um paralelogramo com p^n linhas e p^n colunas, onde os elementos da t-ésima linha são escritos na forma $j + t\theta$ com $j \in \{0, \dots, p^n - 1\}$, e os elementos da t-ésima coluna são escritos na forma $t + k\theta$ com $k \in \{0, \dots, p^n - 1\}$.

Proposição 5.6.1 Se S é uma constelação de sinais em que os sinais sejam rotulados por elementos do grupo aditivo de G de cardinalidade p^n(com $n \geq 1$), onde p é um inteiro primo da forma $p = 2, p \equiv 1\ (mod\ 4)$ ou $p = 3, p \equiv 1\ (mod\ 6)$ provenientes dos reticulados $\mathbb{Z}$[i] e $\mathbb{Z}[\omega]$, respectivamente, então:

1) $mdc(p^n, r) = 1$, onde r é o inteiro obtido como solução da Equação 5.2, através do qual rotula-se um elemento $x + y\theta \in S$ no grupo G através da equação $x + yr \equiv l(mod\ p^n)$.

2) todos os p^n elementos distintos de uma linha qualquer de S recebem rótulos distintos no grupo G,

3) todos os p^n elementos distintos de uma coluna qualquer de S recebem rótulos distintos no grupo G.

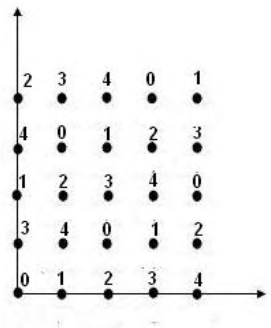
Demonstração: Inicialmente, tome $p = 2$ ou $p \equiv 1\ (mod\ 4)$. De acordo com Carvalho et al. (2008), existe um conjunto de sinais de cardinalidade p^n casado ao grupo aditivo G isomorfo ao grupo quociente $\mathbb{Z}[i]/I$. O ideal I é gerado por $I = \langle u + iv \rangle = \langle (a + bi)^n \rangle$, onde o par de inteiros (a, b) é uma solução da forma quadrática $x^2 + y^2 = p$ e o par de inteiros (u, v) é solução da forma quadrática $x^2 + y^2 = p^n$. Um elemento $l \in G$ (de ordem p^n) é um rótulo de um elemento $x + yi \in \mathbb{Z}[i]$ se $x + yr \equiv l\ mod\ p^n$, onde $r \in \mathbb{Z}$, é a única solução em s da equação $x + ys \equiv 0\ (mod\ p^n)$, onde $0 \leq s \leq p^n - 1$. Supondo a relação r/p^n, deve existir algum $t \in \mathbb{Z}$ tal que $r = p^t$. Assim, se r satisfaz à desigualdade $0 < r < p^n$ e, também, é solução da equação: $u + p^t v \equiv 0\ (mod\ p^t)$,então, conclui-se *que* $u + p^t v \equiv 0\ (mod\ p^t)$, ou seja, $u \equiv 0\ mod p^t$.

Mas, $p^t v \equiv 0 mod p^t$. Dessa forma, obtém-se $u + p^t v \equiv 0\ (mod\ p^t)$. Por outro lado, $p^n \equiv 0\ (mod\ p^t)$. Por meio da Equação 5.2, conclui-se que $r = p^r$ é de forma simultânea solução inteira das equações $u + vr = p^t$ e $u + vr = p^n$. Porém, isto ocorre se, e somente se, $p^t = p^n$, ou melhor, se $t =$ n. Voltando na equação $u + p^n v = p^n$, obtêm-se como par de soluções inteiras de forma quadrática $f(x, y) = x^2 + y^2 = p^n$. Isso leva a uma contradição do tipo $0^1 + 1^2 = p^n$. Conclui-se, assim, que r não divide p^n. Como $0 \leq r \leq p^n - 1$, segue-se então que $mdc(p^n, r) = 1$. No caso de $p \equiv 1\ (mod 6)$, por meio de uma argumentação análoga ao caso de $p \equiv 1\ (mod 4)$, determina-se uma constelação de sinais S e

mostra-se que $mdc(p^n, r) = 1$. Porém, neste caso o reticulado é $\mathbb{Z}[\omega]$. Pela equação 5.2, o rótulo de um elemento $x + y\theta \in \mathbb{Z}[\theta]$ por um elemento $l \in G$ é realizado através da equação $x + yr \equiv 0 mod p^n$, onde $0 < r \leq p^n - 1$. Nota-se que os p^n elementos de uma linha qualquer de S são escritos na forma $j + t\theta$, para um certo índice j fixo, que pode assumir valores entre $j \in \{0, \dots, p^n - 1\}$. Suponha que dois elementos quaisquer de uma linha de S, $e + t\theta$ e $d + t\theta$, recebem o mesmo rótulo $l$em G, onde e, $d \in \{0, \dots, p^n - 1\}$. Então $e + tr \equiv d + tr \equiv l\ (mod\ p^n)$. Isso implica $\mathrm{p^n}|(\mathrm{e} - \mathrm{d})$. Desde que $0 \leq e,\ d \leq p^n - 1$, segue-se então que $d = e$. Logo, conclui-se que dois elementos quaisquer distintos de uma linha de S recebem rótulos distintos em G, o que prova o item (2). Suponha que dois elementos quaisquer de uma coluna de $S, t\ + e\theta$ e $t + d\theta$ recebam o mesmo rótulo l em G, onde $e, d \in \{0, \dots, p^n - 1\}$. Então, tem-se $t + er \equiv t + dr \equiv l\ (mod\ p^n)$. Segue-se, então que $p^n | r(e - d)$. Portanto, $p^n | r$ ou $p^n | (e - d)$. Mas, sabe-se que o $mdc(p^n, r) = 1$, já que p é um inteiro primo e que $r \in \{0, \dots, p^n - 1\}$. Assim, conclui-se que $p^n | (e - d)$. Por outro lado, $0 \leq e, d \leq p^n - 1$, então $e = d$. Logo, a conclusão é que dois elementos quaisquer distintos de uma linha de S recebem rótulos distintos em G.

Exemplo 5.6.1 A Figura 18 ilustra o rotulamento dos sinais de uma constelação $S \subset \mathbb{Z}[i]$ de cardinalidade 25 (como definida na Proposição 5.6.1) por elementos do grupo aditivo G de cardinalidade 5 proveniente do corpo de Galois $GF(5)$, através da função de rotulamento $x + 3y \equiv l\ (mod\ 5)$ avaliada nos pontos $(x + iy) \in S$.

Figura 18- Constelação S de cardinalidade 25 rotulado por elemento de $GF(5)$.



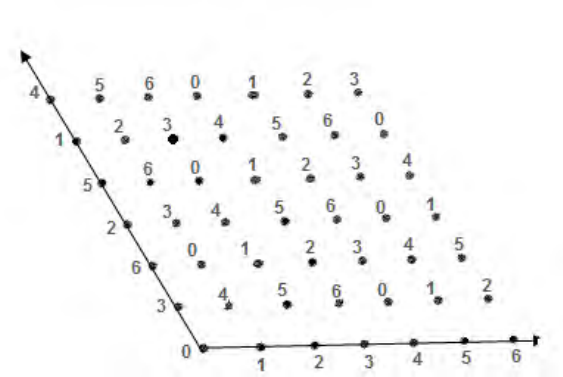
Fonte: Guanais (2012)

Como pode ser observada pela Figura 18, S pode ser visto como paralelograma de 5 linhas por 5 colunas.

Exemplo 5.6.2 A Figura 19 ilustra o rotulamento dos sinais de uma constelação $S \subset \mathbb{Z}[w]$ de cardinalidade 49 (como definido na Proposição 5.6.1) por elemento do grupo

aditivo G de cardinalidade 7 proveniente do corpo de Galois $GF(7)$, através da função de rotulamento $x + 3y \equiv l\ (mod\ 7)$.

Figura 19-Rotulamento do sinais de uma constelação S de cardinalidade 49.



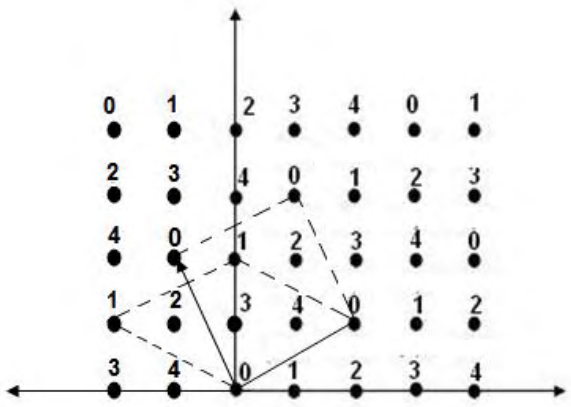
Fonte: Guanais (2012)

Mostraremos adiante que o procedimento proposto por Carvalho et al. (2008), assim como o nosso descrito na Proposição 5.6.1 e o procedimento de se obter um grupo cíclico $\mathbb{Z}_n$ a partir de toros planares estão intimamente ligados.

No sentido de se obter uma melhor compreensão no que será visto mais adiante neste trabalho é que consideraremos uma outra situação.

Exemplo 5.6.3 Seja S' uma constelação dada por $S' = \{j + ki | j \in \{-2, -1,0,1, \dots ,4\}\}$ e $k \in \{0,1,2,3,4\}$ onde $S' \supset S$e S é dada pelo Exemplo 5.6.1. Avaliando a função de rotulamento $x + 3y \equiv l(mod5)$ nos pontos $(x + iy) \in S'$, obtemos a Figura 20.

Figura 20- Rotulamento de uma constelação dada por S'



Fonte: Guanais (2012)

Note que se tomarmos um subconjunto $U = \{2 + i, 1 + 3i, 3 + 4i, 4 + 2i\} \subset S$, então U é uma constelação de sinais rotacionada. Usando a função de rotulamento $x + 3y \equiv$

$l\ (mod\ 5)$ como proposto por Carvalho et al. (2008), observamos que todos elementos de U são rotulados no elemento $l = 0$ no grupo aditivo de $GF(5)$, conforme a tabela 1.

Tabela 1- Função Rotulamento

$\mathbb{Z}[i]$	Função rotulamento	$GF(5)$
0	$x + 3y \equiv l \ \ mod\ 5$	l
0	$0 + 3.0 = 0$	0
1	$1 + 3.0 = 1$	1
2	$2 + 3.0 = 2$	2
3	$3 + 3.0 = 3$	3
4	$4 + 3.0 = 4$	4
i	$0 + 3.1 = 3$	3
$1 + i$	$1 + 3.1 = 4$	4
$2 + i$	$2 + 3.1 = 5$	5
$3 + i$	$3 + 3.1 = 6 \equiv 1$	1
$4 + i$	$4 + 3.1 = 7 \equiv 2$	2

Fonte: Guanais (2012)

Observe que, tomando $u = (2,1)$ e $v = (-1,2)$, tem-se que $5 = |2.2 - (-1).1|$. Como $mdc(2,-1) = 1$ segue pela proposição 5.5.1, que $\mathbb{Z}^2/\Lambda_\alpha$ é isomorfo ao grupo cíclico $\mathbb{Z}_5$. Como pode ser visto na Figura 19, todos os elementos de $\mathbb{Z}_5$ tem representantes no paralelogramo determinado por $\|u\|$ e $\|v\|$, apenas como uma redundância na fronteira do paralelogramo, o que está de acordo com a proposta de Costa et al. (2004) quando consideramos tal procedimento no toro planar, onde $\mathbb{Z}_5$ é o grupo aditivo do corpo de Galois de $GF(5)$ e Λ_α é o reticulado gerado pela base $\alpha = \{u, v\}$. Por outro lado, quando levamos em consideração apenas a constelação S, cada rótulo de $\mathbb{Z}_5$, não se repete em nenhuma linha e em nenhuma coluna.

Observação 5.4 Pelo Exemplo 5.6.3, vemos que a partir da constelação S', obtem-se a constelação $S'' = \{0, 2 + i, -1 + 2i, 1 + 3i\}$, ou melhor, uma constelação rotacionada. Observe que $1 + 3i = (2 + i) + (-1 + 2i)$, o que se verifica conforme as propriedades (ii) de reticulados na seção 5.1.2. Ou seja, a ação da transformação T em $\mathbb{Z}^2$ gera um subreticulado rotacionado em $\mathbb{Z}^2$. Como pode ser visto S'' é uma partição do reticulado rotacionado $T\mathbb{Z}^2$. Logo, como $(2 + i)$ e $(-1 + 2i) \in T\mathbb{Z}^2$ segue que $1 + 3i = (2 + i) + (-1 + 2i) \in T\mathbb{Z}^2$. Por outro lado, observe que todos os elementos de S'' recebem rótulos 0 em $\mathbb{Z}_5$. Assim, esta associação pode ser estendida a uma situação muito mais geral, se lavarmos em consideração a Proposição 5.5.1 e a função de rotulamento da Equação 5.2.

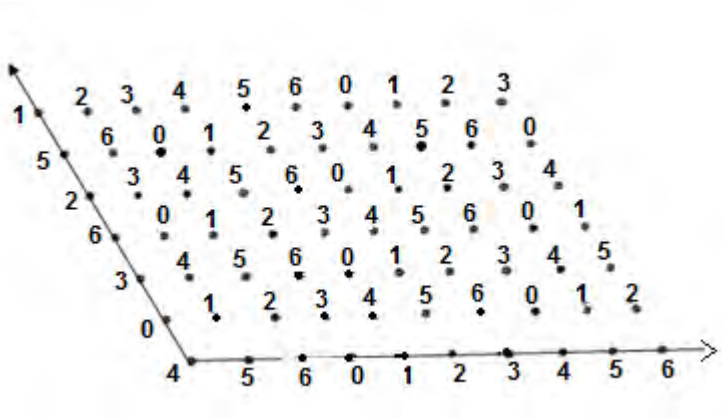
Observação 5.5 Observe que no procedimento proposto por Carvalho et. al (2008), se existe (a, b) inteiros tal que $a^2 + b^2 = p$, então existe uma constelação de sinais S

casado ao grupo aditivo G do corpo de Galois $GF(p)$. O par de inteiros (a, b) determina o ideal $I = \langle a + ib \rangle$ e $G \simeq \mathbb{Z}[i]/I$. Aplicando a função de rotulamento dada pela Equação 5.2 em $a + bi$, temos que este elemento recebe o rótulo 0. Caso tomemos $u = (a, b)$ e $v = (-b, a) \in \mathbb{Z}^2$, obtemos o reticulado Λ_α gerado por u e v que por sua vez é um subreticulado de $\mathbb{Z}^2$ e mais o grupo quociente $\mathbb{Z}^2/\Lambda_\alpha$ tem cardinalidade m dado por $m = |a^2 + b^2|$ que coincide com a forma quadrática $a^2 + b^2 = p$. Ou seja, $\mathbb{Z}^2/\Lambda_\alpha \simeq \mathbb{Z}^2/I \simeq GF(p)$ que é um grupo cíclico aditivo. Por outro lado, se avaliarmos a função de rotulamento da Equação 5.2 em todos pontos do reticulado Λ_α, então estes elementos recebem rótulos zero. A matriz T associada ao reticulado Λ_α é dada por $T = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, ou seja, $T\mathbb{Z}^2$ é um subreticulado de $\mathbb{Z}^2$, cujo grupo quociente é cíclico de índices p.

Observação 5.6 Note que o reticulado Λ_α visto na Observação 5.5 representa um reticulado Λ_α que é uma versão rotacionada do reticulado $\mathbb{Z}^2$. De acordo com Boutro e Viterbo (1998), as constelações de sinais rotacionadas obtidas como partição destes reticulados obtidas como partição destes reticulados rotacionados a apresentam diversidade máxima.

Exemplo 5.6.4 No Exemplo 5.6.2, tomando uma nova constelação onde $S' = \{j + kw | j \in \{-3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}\}$ e $k \in \{0, 1, 2, 3, 4, 5, 6\}$ ao avaliarmos a função de rotulamento $x + 3y \equiv l(mod\ 7)$ nos pontos $(x + iy) \in S'$, obtemos:

Figura 21-Rotulamento de uma nova constelação S'



Fonte: Guanais (2012)

Nota-se, que tomando $u = (1,2)$ e $v = (-3,1)$ e considerando a função de rotulamento $x + 3y \equiv l(mod 7)$, conclui-se que $\mathbb{A}_2/\Lambda_\alpha$ é isomorfo ao grupo cíclico $\mathbb{Z}_7$, como pode ser visto na Figura 21, todos os elementos de $\mathbb{Z}_7$ tem representantes no paralelogramo determinado por $\|u\|$ e $\|v\|$, apenas com redundância na fronteira do paralelogramo se

levarmos em consideração apenas a constelação S, onde cada rótulo de $\mathbb{Z}_7$ não se repete em nenhuma linha e nenhuma coluna.

Será apresentado no próximo capítulo que as mesmas conclusões obtidas nas observações 5.4, 5.5 e 5.6 também se verificam para o reticulado $\mathbb{A}_2$.

6 Construção dos códigos espaço temporal de treliças (CETT) provenientes de reticulados

No Capítulo 4, Tarokh et al. (1998) definiu o ganho de diversidade como sendo o expoente da relação sinal ruído (SNR) $\left(\frac{E_s}{4N_0}\right)$ e que a diversidade máxima é atingida quando $d^2(c,e)$ for máxima, onde c: palavra-código transmitida e é a palavra-código recebida erroneamente e d é a distância Euclidiana. As palavras-códigos c são dadas por sinais do tipo $c_1^1, c_1^2, \ldots, c_1^n$ provenientes de uma constelação de sinais.

Como consequência de resultados da álgebra linear foram determinados dois critérios de desempenho para os códigos temporais como sendo critério do Posto e o critério do Determinante.

Por fim, estabelecidos tais critérios, Tarokh et al. (1998) propuseram um procedimento de codificação dos códigos de treliças, por meio de um rotulamento dos estados de uma treliça por sequências de sinais proveniente de uma constelação bidimensional S. Na decodificação, foi utilizado o algoritmo de Viterbi para se calcular o caminho que gera a menor métrica acumulada. Neste sentido, tem-se que

$$\sum_{j=1}^{n_R} \left| y_t^j - \sum_{i=1}^{n_T} \propto_{ij} q_t^i \right|^2. \tag{6.1}$$

Quando o sinal y_t^j é recebido na j-ésima antena de instante de tempo t, tem-se a sequência de rótulos $q_t^1 q_t^2 \ldots q_t^{n_T}$, onde é assumido que a informação a respeito do canal é conhecida, ou seja, que os ganhos de percursos são conhecidos pelo decodificador.

Em geral, como os rótulos das transições desses códigos de treliças apresentam duas componentes, o sistema de comunicação possui duas antenas de transmissão, sendo que cada uma delas é usada para transmitir uma componente.

6.1 Construção de códigos espaço temporal de treliças via técnica dos quadrados latinos.

Baseado na proposta de rotulamento dos estados de uma treliça via uma sequência de sinais provenientes de uma constelação de sinais, Valença (2001) propôs a utilização da técnica dos quadrados latinos.

Por um quadrado latino de ordem p entende-se como um arranjo de pontos compostos por p linhas e p colunas, no caso de um reticulado bidimensional, onde um certo símbolo ocorre p vezes, mas não duas vezes na mesma linha ou coluna.

Fundamentalmente, a técnica dos quadrados latinos propostos por Valença (2001) tinha como meta gerar um grupo cíclico aditivo de cardinalidade prima p, para casos em que $p = 2$ e $p \equiv 1\ (mod\ 4)$ ou $p = 3$ e $p \equiv 1\ (mod\ 6)$ provenientes dos reticulados $\mathbb{Z}^2$ e $\mathbb{A}_2$, respectivamente.

Para estes grupos a diversidade máxima era atingida se $p \equiv 1\ mod\ 4$, se (a, b) é solução da forma quadrática $x^2 + y^2 = p$, então Valença (2001) observou que existia um código de grupo aditivo cíclico H de cardinalidade prima p. Agora se $p \equiv 1\ mod\ 6$ e se (a, b) é solução da forma quadrática $x^2 + xy + y^2 = p$, então existe um grupo aditivo cíclico H de cardinalidade prima p.

Exemplo 6.1.1 Seja $p = 5$, então $5 \equiv 1 mod\ 4$, e $(2,1)$ é um par de soluções inteiras da forma quadrática dada por $x^2 + y^2 = 5$.

Por uma simples inspeção, obtem-se um grupo cíclico aditivo de cardinalidade 5, onde a notação $\bar{a}$ denota o menor inteiro representante de uma classe de restos módulo 5, verifica-se que H é dado por $H = \{\bar{0}\bar{0}, \bar{2}\bar{1}, \bar{4}\bar{2}, \bar{1}\bar{3}, \bar{3}\bar{4}\}$, por uma simples questão de comodidade, denotaremos H por $H = \{00,21,42,13,34\}$.

A Figura 22, mostra-se que os elementos de H, podem serem representados como elementos de um quadrado latino, através do rearranjo geométrico de $\mathbb{Z}_5^2$.

Figura 22- Arranjo $\mathbb{Z}_5^2$ com os seus pares ordenados

	0	1	2	3	4
0	00				
1				13	
2		21			
3					34
4			42		

Fonte: Valença (2001)

Exemplo 6.1.2 Seja $p = 7$, então $7 \equiv 1\ (mod\ 6)$ e $(2,1)$ é um par de solução inteira da forma quadrática $x^2 + xy + y^2 = 7$. A partir do par de elementos $(\bar{2}, \bar{1})$, obtem-se um grupo cíclico aditivo de cardinalidade 7. Por uma simples inspeção, verifica-se que H é dado por $H = \{(0,0), (2,1), (4,2), (6,3), (1,4), (3,5), (5,6)\}$.

Por uma questão de comodidade, denotaremos simplesmente por $H = \{00,21,42,63,14,35,56\}$.

A Figura 23 mostra que os elementos de H podem ser representados como elementos de um quadrado latino. Ou melhor, como um subconjunto do rearranjo geométrico de $\mathbb{Z}_7^2$.

Figura 23- Arranjo $\mathbb{Z}_7^2$ com os seus pares ordenados

	0	1	2	3	4	5	6
0	00						
1					14		
2		21					
3						35	
4			42				
5							56
6				63			

Fonte: Valença (2001)

Por meio dessa técnica, a diversidade obtida é sempre máxima e igual a 2.

Desta forma Valença (2001) propôs um rotulamento dos estados da treliça na forma $q_t^1 q_t^2 \ldots q_t^{n_T}$ onde os rótulos q_i fossem tomados a partir do grupo aditivo H de cardinalidade p. A diversidade máxima atingida para estes códigos de grupo é 2.

Se levarmos em consideração a Figura 20, vemos que os elementos do grupo cíclico aditivo são identificados nos elementos que recebem rótulos zero, como visto e proposto na representação geométrica das constelações de sinais na forma de um paralelogramo da seção 5.5.

De um modo geral, esta associação vai muito além, uma vez que existe uma relação entre um quadrado latino de ordem p, como será visto mais adiante na Proposição 5.6.1.

Tal fato será de extra importância para a construção dos códigos espaço temporal de treliças (CETT) ao se empregar uma modulação na constelação casada a um grupo aditivo.

Uma contribuição deste trabalho é de mostrar que este grupo cíclico H é isomorfo a um grupo quociente Λ'/Λ'', onde Λ'' é um subreticulado de Λ', já Λ' é um subreticulado de Λ, onde $\Lambda = \mathbb{Z}^2$ ou $\Lambda = \mathbb{A}$. Adicionalmente, mostraremos que a ordem deste grupo quociente H pode ser estendida a potências de um primo p, esta construção será obtida para os casos em que $p \equiv 1\ (mod\ 4)$ em $\mathbb{Z}^2$ e $p \equiv 1\ (mod\ 6)$ em $\mathbb{A}_2$.

6.2 Construção de código espacial temporal de treliça a partir de quadrados latinos.

No sentido de se estabelecer a conexão da técnica de constelação de sinais rotacionadas e grupos cíclicos aditivos, ilustraremos alguns exemplos já apresentados até o momento neste trabalho.

Note que os elementos de $\mathbb{Z}_5^2$ da figura 22 podem ser caracterizados como elementos do tipo $(a, b) \in \mathbb{Z}^2$, onde $a, b \in \{0,1,2,3,4\}$. Por outro lado, já vimos que os elementos de $\mathbb{Z}^2$ são identificados por elementos do anel de inteiros de Gauss na forma $(a + bi)$, onde $a, b \in \{0,1,2,3,4\}$. O que significa que podemos utilizar a função de rotulamento definida pela equação 5.2. Portanto, os elementos de $\mathbb{Z}_5^2$ recebem rótulos em $GF(5)$, como pode ser observada pela Figura 18.

Assim, baseando-se na proposta de codificação de Tarokh et al. (1998) em Palazzo e Valença (2002) estabeleceu um procedimento para se obter a maior d_{free} (distância livre na treliça obtida pela sequência de rótulos) e, consequentemente, obter a maior diversidade de modulação para os CETT a partir das constelações de sinais de cardinalidade p, onde e $p \equiv 1\ mod\ 4$ ou e $p \equiv 1\ mod\ 6$.

O algorítmo de construção dado por Palazzo e Valença (2002) é estabelecido da seguinte forma.

Passo1) Deve-se aplicar a técnica de recobrimento espacial baseado em reticulados e, assim, obter um código de grupo com a maior diversidade possível, isto é, será obtido um quadrado latino. Caso contrário ir para o passo 3.

Passo 2) A segunda componente da palavra-código é usada como referência no rotulamento dos ramos da treliça com os elementos do código de grupo H do código espaço-temporal associado. Nesta situação, quando submetido a canais com desvanecimento do tipo Rayleigh a $\mathrm{d_{free}} > 2$, o código apresentará um melhor desempenho comparado com o caso trivial em que um quadrado latino não é obtido.

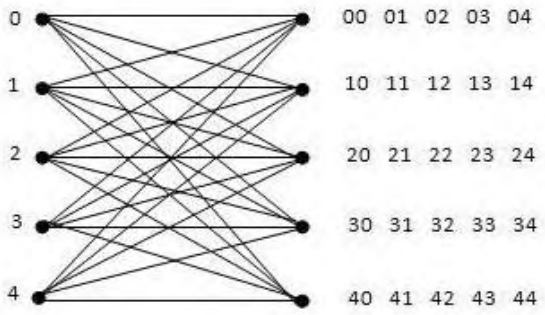
Passo 3) As transições da treliça que partem do i-ésimo estado terão a primeira componente igual a i e a segunda componente será rotulada sucessivamente com os elementos de H. Neste caso, quando submetidos a canais com desvanecimento do tipo Rayleigh a $d_{free} = 2$, não se obtém quadrado latino e a solução será sempre trivial.

Dessa forma, nota-se que o quadrado latino pode ser visto como uma constelação de sinais K de $\mathbb{Z}[\theta]$, onde K é um subconjunto de uma constelação S como definida na

Proposição 6.2.1, onde cada elemento do quadrado latino da forma (a, b)é identificado pelo elemento da forma $a + b\theta$ do reticulado $\mathbb{Z}[\theta]$.

Exemplo 6.2.2 Para o caso *p=5*, após a aplicação da técnicados quadrados latinos, obtém-se o diagrama apresentado na Figura 24, quando as transições da treliça que partem do i-ésimo estado terão a primeira componente igual a i e a segunda componente será rotulada sucessivamente com os elementos de $\mathbb{Z}_5$.

Figura 24- Seção de treliça do código espaço-temporal

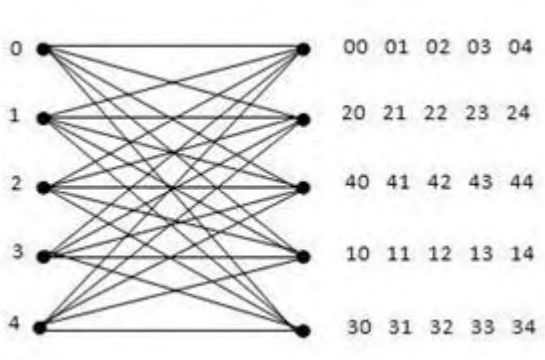


Fonte: Valença (2001)

Neste caso, $d_{free} = 2$ quando submetido a canais com desvanecimento do tipo Rayleigh.

Para o mesmo caso, quando a segunda componente da palavra-código será usada como referência no rotulamento dos ramos da treliça do código espaço-temporal associado. A Figura 25 ilustra essa seção de treliça.

Figura 25-Seção de treliça do código espaço-temporal



Fonte: Valença (2001)

Note que na proposta do Algoritmo de construção de códigos espaço temporal a partir de quadrados latinos propostas por Palazzo e Valença (2002) é baseada em três passos e que a diversidade máxima é satisfeita quando é possível aplicar a técnica de recobrimento espacial de reticulados (quadrados latinos).

Fixado um dado inteiro primo p, vimos na seção 6.1 para que possamos aplicar a técnica de recobrimento espacial de reticulados (quadrados latinos) e consequentemente obter um quadrado latino de ordem p, inicialmente procura-se determinar um par de inteiros (a, b) de tal forma que (a, b) seja soluções inteiras da forma quadrática $x^2 + y^2 = p$ ou $x^2 + xy + y^2 = p$.

Por meio da Observação 6.1, vimos que aplicar a técnica dos quadrados latinos para se obter um grupo cíclico de cardinalidade prima p está intimamente ligado aos resultados obtidos na Proposição 5.6.1, ou seja, que os elementos que determinam um quadrado latino recebem rótulos zeros no grupo aditivo G da Proposição 5.6.1.

Porém, como consequência desta relação podemos formalizar o procedimento de Dutra e determinar uma situação mais geral, como descrito na próxima observação.

Observação 6.2 Dado um inteiro primo p, obtém-se um grupo aditivo cíclico G de ordem p^n (com $n \geq 1$) com diversidade máxima igual à 2 para os casos em que $p = 2$, $p \equiv 1\ (mod\ 4)$ ou $p = 3$ e $p \equiv 1\ (mod\ 6)$ quando proveniente dos reticulados $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$, respectivamente.

6.3 Construção de código espaço-temporal de treliça a partir de partição de reticulados.

Nesta seção, será sistematizado algebricamente e geometricamente o procedimento proposto por Valença para construção de CETT.

Desta sistematização, mostraremos um procedimento de geração de subreticulados de codificação espaço-temporal de treliça a partir de grupos aditivos cíclicos de cardinalidade p^n para os casos $p \equiv 1\ mod\ 4$ ou e $p \equiv 1\ mod\ 6$ a partir dos reticulados de $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$, respectivamente.

Para isso, inicialmente construiremos uma cadeia de subreticulados $\Lambda', \Lambda'', \Lambda'''$ de Λ de tal forma que $\Lambda''' \subset \Lambda'' \subset \Lambda' \subset \Lambda$, onde $\Lambda = \mathbb{Z}[i]$ ou $\Lambda = \mathbb{Z}[w]$. Por Carvalho et al. (2008), se $p \equiv 1\ (mod\ 4)$ ou e $p \equiv 1\ (mod\ 6)$ então existe uma constelação de sinais S de cardinalidade p^n proveniente dos reticulados $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$, respectivamente. Precisamente os sinais de S são rotulados por elementos de um grupo aditivo G, onde G representa uma partição de $\mathbb{Z}[\theta]$ de cardinalidade p^n. A função de rotulamento é dado por:

$$\begin{array}{ccc} \mu: \mathbb{Z}[\theta] & \longrightarrow & G \\ x + y\theta & \longrightarrow & x + yr \end{array}$$

onde r é a solução em s da equação $x + ys = p^n$.

Seja uma constelação S de cardinalidade p^n casada a um grupo aditivo de cardinalidade p^n, nas mesmas condições propostas por Carvalho et al., (2008) acima. Considere agora um particular subconjunto Λ' formado pelos elementos $x + y\theta \in \mathbb{Z}[\theta]$,tais que $\mu(x + y\theta) = 0$ e μ é a função de rotulamento dada pela equação $x + ys = p^n$.

Proposição 6.3.1 O conjunto $\Lambda^{'}$ é um subreticulado de Λ.

Demonstração: Note $0 \in \Lambda'$, já que $0 = 0 + 0.r = 0$. A propriedade de fechamento também é observado uma vez que $a = x_1 + y_1\theta$ e $b = x_2 + y_2\theta \in \Lambda^{'}$, então $\mu(a) = 0$. Assim, $a + b = (x_1 + y_1\theta) + (x_2 + y_2\theta)$. Como $\mu(a + b) = 0$, note que $x_1 + y_1r = x_2 + y_2r = 0$, segue que $0 = (x_1 + x_2) + (y_1 + y_2)r = (x_1 + y_1r) + (x_2 + y_2)r$. Portanto $a + b\theta \in \Lambda^{'}$. Agora se $a \in \Lambda^{'}$ é um elemento qualquer elemento não nulo. Então, $a = x_1 + y_1\theta$ onde $x_1, y_1 \in \mathbb{Z}$. Logo, $\mu(x_1 + y_1\theta\ ) = 0$, o que implica que $p^n|x_1 + y_1r$, e r é a solução em s da equação $x + ys = p^n$. Finalmente, se $h = -x_1 - y_1\theta \neq 0$, mostraremos que $h = a^{-1}$ (ou seja h é o inverso aditivo de a). De fato, note que $h + a = (-x_1 - y_1\theta) + (x_1 + y_1\theta) = 0$, onde 0 é o elemento neutro aditivo em Λ'. Avaliando a função de rotulamento μ em h, obtem-se $\mu(h) = \mu(-x_1 - y_1\theta) = -x_1 - y_1r$. Por outro lado, $p^n|(x_1 + y_1r)$. Então, usando propriedade de divisibilidade em $\mathbb{Z}$, temos que de $p^n \backslash (x_1 + y_1r)$ o que implica $p^n|(-1)(x_1 + y_1r) = (-x_1 - y_1r)$. Assim, concluímos que $h = a^{-1}$, ou seja, $\forall a \in \Lambda^{'} \Rightarrow a^{-1} \in \Lambda^{'}$, com $a \neq 0$. Portanto Λ' é um subreticulado de Λ.

Continuando com este processo, agora consideremos um particular subconjunto Λ'' do reticulado $\Lambda^{'}$.

Seja $\Lambda'' = \{m(a + b\theta) | \forall m \in \mathbb{Z}\}$, onde $a, b \in \mathbb{Z}$ e são solução da forma quadrática $x^2 + y^2 = p^n$, se $p \equiv 1\ (mod\ 4)$ ou da forma quadrática $x^2 + xy + y^2 = p^n$ se $p \equiv 1\ (mod\ 6)$. A próxima proposição estabelece que Λ'' é um subreticulado de Λ'.

Proposição 6.3.2 O conjunto Λ''é um subreticulado de Λ'.

Demonstração: Note que $0 \in \Lambda''$,já que $m = 0$,então $m(a + b\theta) = 0$. Agora, $\forall m \in \mathbb{Z}$, $m(a + b\theta) \in \Lambda^{'}$, uma vez que $a + b\theta \in \Lambda'$,então existe $r \in \mathbb{Z}$ tal que $a + br \equiv 0\ (mod\ p^n)$, ou seja, $p^n|a + br$. Assim, $\mu(x + y\theta) = 0$. Logo, se $p^n|a + br \Rightarrow p^n|m(a + br), \forall m \in \mathbb{Z}$, ou seja, $m(a + br) \equiv 0\ mod\ p^n$, o que implica que $\mu\big(m(a + b\theta)\big) = 0$. Para o fechamento, $m_1(a + b\theta)$ e $m_2(a + b\theta) \in \Lambda^{''}$. Como, $p^n|(a + b\theta)$, já que $\mu(a + b\theta) = 0$ como vimos na Proposição 6.3.1, então por propriedades de divisibilidade temos que $p^n|m_1(a + b\theta)$ e $p^n|m_2(a + b\theta)$. Consequentemente, $p^n|(m_1 + m_2)(a + br)$, ou seja, $(m_1 + m_2)(a + br) \equiv 0\ mod\ p^n$. Então, $\mu\big((m_1 + m_2)(a + b\theta)\big) = 0$. Finalmente dado $x = m(a + b\theta) \neq 0 \in \Lambda^{''}$, então $h = -m(a + b\theta)$ é o inverso aditivo de x, uma vez que

$x + h = m(a + b\theta) + (-m(a + b\theta)\,) = \big(m + (-m)\big)(a + b\theta) = 0.(a + b\theta) =$ 0.Portanto, Λ'' é um subreticulado de Λ'.

Observação 6.3 Note que o grupo associado ao subreticulado Λ'' e dado pelo grupo cíclico $G = \langle(a, b)\rangle$.

Observe também que consideremos $a, b \in \mathbb{Z}$ no início da construção de tal forma que $mdc(a, b) = 1$. A próxima proposição estabelece uma importante propriedade associada ao reticulado Λ''.

Proposição 6.3.3 O subreticulado Λ'' é isomorfo ao reticulado $\mathbb{Z}$.

Demonstração: A aplicação

$$f: \Lambda'' \longrightarrow \mathbb{Z}$$
$$m(a + b\theta) \longrightarrow m$$

facilmente mostra-se que f bijetora é um homomorfismo.

Agora, consideremos um especial subconjunto de Λ''' do reticulado Λ'' dado por $\Lambda''' = \{mq(a + b\theta) | q \in \mathbb{Z}\}$, onde são os inteiros múltiplos de m.

Proposição 6.3.4 O conjunto Λ''' é um subreticulado de Λ''.

Demonstração: Note que $0 \in \Lambda'''$, uma vez que como visto na Proposição 6.3.2, o produto dos múltiplos de p^n. Para o fechamento, se $x, y \in \Lambda'''$ então $x = mq_1(a + b\theta)$ e $y = mq_2(a + b\theta)$ para algum $q_1, q_2 \in \mathbb{Z}$. Logo, $x + y = \big(m(q_1 + q_2)(a + b\theta)\big)$para algum $q_1 + q_2 \in \mathbb{Z}$. Então, $x + y \in \Lambda'''$. Fixado m e $a + b\theta$, seja $a = m(a + b\theta) \in \Lambda''$ não nulo. Consideremos $h = m(-a - b\theta)$. Avaliando a função de rotulamento μ em h, temos $\mu(m(a + b\theta))$. Assim, $h^{-1} = a^{-1}$, uma vez que $h + h^{-1} = m(a + b\theta) + m(-a - b\theta) = m(0) = 0$. Além disso, $p^n | m(a + b\theta)$, obtemos que os $p^n | (-1)(m(a + b\theta) = m(-a - b\theta)$, ou seja, $\mu(h^{-1}) = 0$. Portanto, $h^{-1} = a^{-1}$. Logo, Λ'' é um subreticulado de Λ'.

A próxima proposição estabelece que o reticulado Λ''' é isomorfo ao reticulado $m\mathbb{Z}$.

Proposição 6.3.5 O subreticulado Λ''' de Λ é isomorfo ao subgrupo aditivo $m\mathbb{Z}$ do grupo aditivo $\mathbb{Z}$.

Demonstração: Seja G'o grupo aditivo associado a $\Lambda''' = \langle m(a + b\theta)\rangle$. Considerando a aplicação f'parecida com a aplicação apresentada na demonstração da Proposição 6.3.3, dado por:

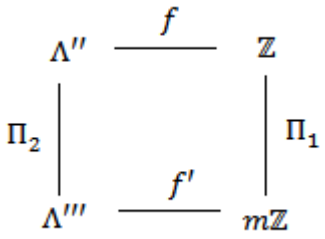
$$f': \Lambda''' \longrightarrow m\mathbb{Z}$$
$$m(a + b\theta) \longrightarrow m$$

para m fixo, a aplicação leva múltiplos de $(a + b\theta)$ e de m em múltiplos de m em $m\mathbb{Z}$.

Por outro lado, um fato muito conhecido na literatura é dado pela proposição 6.3.6.

Proposição 6.3.6 O grupo formado pelas classes de restos módulo m tal que $\mathbb{Z}_n \simeq \mathbb{Z}/m\mathbb{Z}$.

Como consequência das Proposições 6.3.3, 6.3.4, 6.3.5 e 6.3.6, temos o seguinte diagrama comutativo, sendo Π_1 e Π_2 projeções dos reticulados.



Do fato que $\mathbb{Z}_n \simeq \frac{\mathbb{Z}}{m\mathbb{Z}}$, pelo diagrama, temos que $\frac{\Lambda''}{\Lambda'''} \simeq \mathbb{Z}_n$, ou seja, a classe de restos módulo m.

Por fim, como conseqüência desta seção, concluímos que o procedimento de construção dos códigos espaço-temporais de treliça feito por Palazzo e Valença (2002), é conseqüência da geração de subreticulados de codificação espaço-temporal de treliça a partir de grupos aditivos cíclicos de cardinalidade p^n para os casos $p \equiv 1\ (mod\ 4)$ ou e $p \equiv 1\ (mod\ 6)$ a partir dos reticulados de $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$, respectivamente. Assim, sua sistematização pode ser estendida da seguinte forma:

I) Obter uma constelação de sinais U de cardinalidade p^n, casada a um grupo aditivo G de cardinalidade p^n, o que equivale do ponto de vista algébrico, determinar ideais I em $\mathbb{Z}[\theta]$ (para $\theta = i$ ou ω) de norma relativa p^n, que satisfaçam à condição de que $G \simeq \mathbb{Z}[\theta]/I$.

II) Precisamente os sinais de U são rotulados por elementos de um grupo aditivo G, onde G representa uma partição de $\mathbb{Z}[\theta]$ de cardinalidade p^n. Com todos os sinais da constelação rotulado é equivalente dizer que um quadrado latino é obtido. Nesta situação, quando submetido a canais com desvanecimento do tipo Rayleigh a $d_{free} > 2$, e o código apresentará um melhor desempenho, obtendo assim a diversidade máxima.

Dessa forma, o algoritmo sistematizado acima, faz com que o grande objetivo seja alcançado, isto é, obter a diversidade máxima de um sistema de comunicação com tecnologia

MIMO. Resumidamente, para se chegar a tal objetivo, é suficiente obter constelações de sinais rotacionadas a partir de partições de reticulados de cardinalidade p^n.

7 Conclusão e propostas futuras de trabalho

Neste trabalho sistematizamos algebricamente e geometricamente o procedimento de construção de códigos espaço-temporais de treliça via quadrados latinos proposto por Valença (2001) usados para se obter diversidade máxima de modulação.

Tal extensão do trabalho foi obtido como consequência natural do fato de termos mostrado que os códigos de grupos cíclicos da proposta de Valença (2001) poderem ser obtidos via grupos quocientes de subreticulados Λ'' de um reticulado rotacionado Λ'.

Uma interessante abordagem futura, na mesma linha deste trabalho, é propor estes grupos cíclicos *H* (códigos) de grupo via a técnica da construção *A* de reticulados e um outro tema interessante seria propor códigos cíclicos via partição de reticulados em dimensão superior a 2.

Referências

ALAMOUTI, S.M. A simple transmit diversity technique for wireless communications**, IEEE Journal on Selected Areas in Communications**, Canadá, v. 16, n. 8, p. 1451-1458, October 1998.

ALMEIDA, C. **Modulação-codificada generalizada via equação de diofanto**. 1990. 115f. (Tese Doutorado)-Faculdade de Engenharia Elétrica, Universidade Estadual de Campinas-UNICAMP, Campinas, 1990.

AlVES, C. **Reticulados e códigos.** 2003. 156f. **(**Tese Doutorado)-Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas-UNICAMP, Campinas, 2003.

AGUSTINI, E. **Constelação de sinais em espaços hiperbólicos.** 2003. 139f. **(**Tese Doutorado)-Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas-UNICAMP, Campinas, 2003.

BERHUY,G.; OGGIER, F. **Introduction to central simple algebras and their applications to wireless communication**. Grenoble: Universidade Joseph Fourier, 2008. Disponível em < www-fourier.ujf-grenoble.fr/ sim berhuy/fichiers/BOCSA.pdf>. Acesso em: 29 nov. 2012.

BOUTROS, J.; VITERBO, E. Signal space diversity: a power – andbandwidth - efficient diversity technique for the rayleigh fading channel**. IEEE Trans. Inform.Theory**, Suiça, v. IT-44, p. 1453-1467, July 1998.

CARVALHO, E.D.; PALAZZO, R.; FIRER JUNIOR, M. On the Construction of Geometrically Uniform Signal Sets in $\mathbb{R}^2$ Matched to Additive Quotient Groups. **Jornal of Applied Mathematics and Computing**, Nova York, v. 27, n. 2, p. 1-6, 2008.

COSTA, S. I. R.; MUNIZ, M.; AGUSTINI, E.; PALAZZO, R. Graphs, tessellations, and perfect codes on flat tori. **IEEE Trans. Inform. Theory**, Suiça, v. 50, n. 10, p. 2363‑2377, 2004.

ENGLER, A.J; BRUMATTI, P. Inteiros Quadráticos e o Grupo de Classes**.** In: COLÓQUIO BRASILEIRO DE MATEMÁTICA, 23., 2001, Rio de Janeiro: Associação Instituto Nacional de Matemática Aplicada-IMPA, 2001. p.1-82. Coleção Matemática e Aplicações.

FOSCHINI, G. J.; GANS, M. J. On limits of wireless communication in a fading environment when using multiples antennas. **Wireless Personal Communications**, New Jersey, v. 6, p. 311-335, 1998.

GONÇALVES, A. **Introdução à álgebra**. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2003. 194p.

HUBER, K. Codes over gaussian integers. **IEEE Trans. Theory**, Germany, v. IT-40, n.1, p. 207-216, Jan.1994.

HUBER, K. Codes over Eisenstein-Jacobi integers. **Contemporary Mathematics**, Germany, v.168, n.1, p. 165-179, 1994.

LOURÊDO, A.T.; SILVA, A. A. **Códigos de permutação para o canal gaussiano.** 2000. 82f. (Tese Doutorado)-Centro de Ciências Exatas e da Natureza, Universidade Federal da Paraíba, Paraíba, 2000.

NÓBREGA NETO, T.P.; INTERLANDO, J.C.; FAVARETO, O.M.; ELIA, M.; PALAZZO JUNIOR, R. Lattice constellations and codesfrom quadratic number fields. **IEEE Trans. Inform.Theory**, Canadá, v. T-47, n. 4, p. 1514-1527, May 2001.

PALAZZO JUNIOR, R.; INTERLANDO, J.C.; GERONIMO, J. R.; de ANDRADE, A. A.; FAVARETO, O. M.; COSTA ARAÚJO, M. da; NÓBREGA NETO, T. P.; SANTOS, G.O. dos. **Fundamentos algébricos e geométricos dos códigos corretores de erros.** Campinas: Universidade Estadual de Campinas-UNICAMP, 2003.

PALAZZO JUNIOR., R.; UCHÔA FILHO, B. F.; ARPAZI, J. P. **Fundamentos e aplicações de códigos convolucionais em sistemas de comunicações**. Campinas: DT, FEEC-Unicamp, 1999.

PALAZZO JUNIOR., R.; VALENÇA, D. R. Construction of optimum space-time trellis codes based on cyclic codes over groups and fields. **IEEE International Symposium on Information Theory**, Switzerland, v. 1, p.1-133, 2002.

TAROKH,V.; JAFARKHANI, H.; CALDERBANK, A.R. Space-time block codes from orthogonal designs. **IEEE Transactions on Information Theory**, Ireland, v. 45, n. 5, p. 1456-1467, July 1999.

TAROKH,V.; SESHADRI, N.; CALDERBANK,A.R. Space-time codes for high data rate wireless communication: performance criterion and code construction. **IEEE Transactions on Information Theory**, Ireland, v. 44, n. 2, p. 744-765, March1998.

TELATAR, I. E. Capacity of multi-antenna gaussian channels. **European Trans. On Telecommunications**, New Jersey, v. 10, n. 6, p. 585-595, Nov. 1999.

VALENÇA, R. D.;PALAZZO JUNIOR, R. **Métodos para a construção de códigos espaço-temporais sobre grupo, corpos e anéis para canais com desvanecimento quase-estático e plano.** 2001**.** 72f. (Tese Doutorado)- Faculdade de Engenharia Elétrica e Computação, Universidade Estadual de Campinas-UNICAMP, Campinas, 2001.

.