UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE SÃO JOÃO DA BOA VISTA

JULIA DANIELLI DUARTE

Códigos de Bloco Espaço-Tempo para Canais MIMO 2×2 via Álgebras Cíclicas de Divisão

São João da Boa Vista
2021

JULIA DANIELLI DUARTE

Códigos de Bloco Espaço-Tempo para Canais MIMO 2×2 via Álgebras Cíclicas de Divisão

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Engenharia Eletrônica e de Telecomunicações do Campus de São João da Boa Vista, Universidade Estatual Paulista "Júlio de Mesquita Filho", como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Eletrônica e de Telecomunicações .

Orientador: Profa. Dra. Cintya Wink de Oliveira Benedito

São João da Boa Vista
2021

D812c

Duarte, Julia Danielli
Códigos de bloco espaço-tempo para canais mimo 2 x 2 via álgebras cíclicas de divisão / Julia Danielli Duarte. -- São João da Boa Vista, 2021
64 f. : il., tabs.

Trabalho de conclusão de curso (Bacharelado - Engenharia de Telecomunicações) - Universidade Estadual Paulista (Unesp), Câmpus Experimental de São João da Boa Vista, São João da Boa Vista
Orientadora: Cintya Wink de Oliveira Benedito

1. Codificação. 2. Sistemas MIMO. 3. Quaternios. 4. Telecomunicações. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Câmpus Experimental de São João da Boa Vista. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CÂMPUS EXPERIMENTAL DE SÃO JOÃO DA BOA VISTA
GRADUAÇÃO EM ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

CÓDIGOS DE BLOCO ESPAÇO-TEMPO PARA CANAIS MIMO 2 X 2 VIA CORPOS DE NÚMEROS

Aluna: Julia Danielli Duarte
Orientadora: Profª. Drª. Cintya Wink de Oliveira Benedito

Banca Examinadora:

- Cintya Wink de Oliveira Benedito (Orientadora)
- Edgar Eduardo Benitez Olivo (Examinador)
- Nelson Gomes Brasil Junior (Examinador)

A ata da defesa com as respectivas assinaturas dos membros encontra-se no prontuário do aluno (Expediente nº 011/2020)

São João da Boa Vista, 04 de maio de 2021

Aos meus pais Aparecida Duarte e José Carlos Duarte,
dedico.

AGRADECIMENTOS

Aos meus pais e à minha família, por todo apoio, amor e confiança, em todos os momentos da minha vida.

Ao Thiago, pela compreensão, amor e companheirismo.

Á Amanda, Ana Letícia, Bia, Gabi, Letícia e Leonardo, amigos que fiz durante essa jornada e que foram essenciais para que para eu chegasse até aqui.

À minha orientadora Profa Dra Cintya Wink de Oliveira Benedito, pela paciência, conhecimento e dedicação com nosso trabalho.

À Letícia, Karina, Thais e Vitor Hugo que se fizeram presentes em todos os momentos, sempre me apoiando e incentivando com amor e carinho.

Aos professores e funcionários da UNESP - São João da Boa Vista, pela dedicação e conhecimento transmitido.

Aos membros da banca examinadora.

À todos que direta ou indiretamente contribuíram para a realização deste trabalho.

RESUMO

Este trabalho tem o objetivo de apresentar a construção do código de Ouro, que é um código de bloco espaço tempo (*Space-Time Block Code* - STBC) 2×2 perfeito construído a partir de uma álgebra cíclica de divisão. Este código é dito perfeito pois é de taxa e diversidade máximas, tem determinante diferente de zero, o que permite obter um limitante inferior para o determinante mínimo, e tem constelação em formato de *shaping* cúbico. Além disso, iremos definir STBC de uma forma geral, e mostrar que o código de Alamouti, precursor dos STBCs, pode ser construído via uma álgebra cíclica de divisão especial, a álgebra dos quatérnios de Hamilton. Após as construções, vamos apresentar análises desses códigos em sistemas de comunicação sem fio com múltiplas antenas no transmissor e receptor (*Multiple-Input Multiple-Output* - MIMO) 2×1 e 2×2 no caso do Alamouti e 2×2 no caso do código de Ouro, considerando que o receptor seja coerente, isto é, tenha informação do estado de canal (*Channel State Information* - CSI) perfeito e que estamos em um canal de desvanecimento Rayleigh quase-estático e plano de ruído AWGN. Utilizamos modulações de diferentes ordens M-QAM (M-*ary Quadrature Amplitude Modulation*) e um decodificador de máxima verossimilhança (*Maximum Likelihood* - ML) específico para cada codificação. As análises de desempenho dos códigos foram realizadas através de simulações computacionais, nas quais foram empregadas o método de Monte Carlo. Nessas simulações, são avaliadas as curvas da taxa de erro de símbolo (*Symbol Error Rate* - SER) pela relação sinal-ruído (*Signal-to-Noise Ratio* - SNR). Com os resultados obtidos, foi possível mostrar que o código de Ouro possui um desempenho superior em comparação ao código de Alamouti. Para a mesma ordem de modulação, o código de Ouro consegue ter o dobro da eficiência espectral com apenas $\frac{1}{4}$ da energia média, em comparação ao código de Alamouti. E para o caso que ambos tenham a mesma eficiência espectral, o código de Ouro também tem performance superior, pois necessita de menos energia para transmissão.

PALAVRAS-CHAVE: STBC. Código de Alamouti. Código de Ouro. Álgebra Cíclica de Divisão. MIMO. SER.

ABSTRACT

This work aims to present the construction of the Golden code, which is a perfect 2×2 space-time block code (STBC) built from a cyclic division algebra. This code is said to be perfect because it is of full rate and full diversity, has non-zero determinant, which allows a lower bound for the minimum determinant, and has cubic shaping constellation. Furthermore, we will define STBC in general, and show that Alamouti's code, the precursor to STBCs, can be constructed via a special division cyclic algebra, the algebra of Hamilton's quaternions. After the constructions, we will present analyses of these codes in wireless communication systems with multiple antennas at the transmitter and receiver (Multiple-Input Multiple-Output - MIMO) 2×1 and 2×2 in the case of Alamouti and 2×2 in the case of the Golden code, considering that the receiver is coherent, that is, has perfect Channel State Infomartion (CSI) and that we are in a quasi-static Rayleigh fading flat frequency channel with AWGN noise. We use modulations of different orders M-QAM (M-ary Quadrature Amplitude Modulation) and a maximum likelihood decoder (Maximum Likelihood - ML) specific to each encoding. The performance analyses of the codes were done through computer simulations, in which the Monte Carlo method was employed. In these simulations, the symbol error rate (SER) curves are evaluated by the signal-to-noise ratio (SNR). With the results obtained, it was possible to show that the Golden code has a superior performance compared to the Alamouti code. For the same modulation order, the Golden code can have twice the spectral efficiency with only $\frac{1}{4}$ of the average energy, compared to the Alamouti code. And for the case that both have the same spectral efficiency, the Golden code is also superior, since it requires less energy for transmission.

KEYWORDS: STBC. Alamouti Code. Golden Code. Cyclic Division Algebras. MIMO. SER

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

5G	Quinta geração das comunicações móveis
AWGN	Additive White Gaussian Noise
bpcu	bits por uso de canal
CSI	Channel State Information
IoT	Internet of Things
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
NVD	Non-Vanishing Determitant
SISO	Single-Input Single-Output
ML	Maximum Likelihood
M-QAM	M-ary Quadrature Amplitude Modulation
RF	Radiofrequência
SER	Symbol Error Rate
SNR	Signal-to-Noise Ratio
spcu	símbolos por uso de canal
STBC	Space-Time Block Code
STC	Space-Time Code
STTC	Space-Time Trellis Code

LISTA DE SÍMBOLOS

n_t	Número de antenas transmissoras
n_r	Número de antenas receptoras
$\mathbf{Y}$	Matriz do sinal recebido
$\mathbf{X}$	Matriz do sinal transmitido
$\mathbf{H}$	Matriz do canal de desvanecimento Rayleigh quase-estático e plano
$\mathbf{Z}$	Matriz do ruído AWGN
T	Período de símbolo
C	Capacidade de canal
$\mathbf{I}_{n_r}$	Matriz identidade de ordem n_r
μ	Módulo do ganho de canal
$\tilde{\boldsymbol{x}}$	Sinal recebido após passar pelo combinador
$\hat{\boldsymbol{x}}$	Sinal recebido após passar pelo detector ML
$\min$	Menor elemento
$\det(\cdot)$	Determinante de uma matriz
$\log(\cdot)$	Logaritmo
$\|\| \cdot \|\|$	Norma de Frobenius
$(\cdot)^t$	Matriz transposta
$\bar{q}$	Complexo conjugado
$(\cdot)^\dagger$	Conjugado transposto de uma matriz
$P(e)$	Probabilidade de erro
$P(\mathbf{X} \rightarrow \hat{\mathbf{X}})$	Probabilidade de erro aos pares
$\|x\|$	Módulo de x
Δ	Determinante do código
r	Posto da matriz de diferença da palavra-código
$\mathbf{A}$	Matriz de distância da palavra-código

λ_j	autovalores não-nulos da matriz $\mathbf{A}$
div	Ganho de diversidade
N_0	Densidade espectral de potência de ruído
$\Delta_{\min}$	Determinante mínimo do código
$\mathcal{C}$	Código
M	Ordem de modulação M-QAM
k	Número de símbolos de informação codificados
η_s	Eficiência espectral (spcu)
η	Eficiência espectral (bpcu)
G	Grupo
A, B	Anel
$\mathcal{I}$	Ideal
$\langle x \rangle$	Ideal principal
$\mathbb{K}, \mathbb{L}$	Corpos
$\mathbb{L}/\mathbb{K}$	Extensão de corpos
$\mathbb{C}$	Conjunto dos números complexos
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{H}$	Álgebra dos quatérnios de Hamilton
$[\mathbb{L} : \mathbb{K}]$	Grau da extensão $\mathbb{L}/\mathbb{K}$
φ	Homomorfismo de anel
n	Grau de um corpo de números
σ	Monomorfismo
$\langle \sigma \rangle$	Grupo cíclico de Galois
θ	Elemento primitivo
$Gal(\mathbb{L}/\mathbb{K})$	Grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$

$\mathcal{O}$	Anel de inteiros
$\mathbb{Z}[i]$	Conjunto dos inteiros Gaussiano
$\{\omega_i\}_{i=1}^{n}$	Base integral
$N_{\mathbb{L}/\mathbb{K}}(x)$	Norma de $x \in \mathbb{L}$
$Tr_{\mathbb{L}/\mathbb{K}}(x)$	Traço de $x \in \mathbb{L}$
$Nrd(q)$	Norma reduzida de q
$Trd(q)$	Traço reduzido de q
d_K	Discriminante
$\mathcal{A}$	Álgebra
$\mathbb{H}$	Quatérnios de Hamilton
q	Elemento de uma álgebra dos quatérnios
Λ	Reticulado
Λ^c	Reticulado complexo
Λ'	Reticulado algébrico
$\mathbf{M}$	Matriz geradora do reticulado
$\mathbf{v}$	Vetor dos símbolos de informação
$\mathbf{G}$	Matriz de Gram
x_0, x_1, x_2, x_3	Símbolos de informação QAM
N	Número de símbolos simulados
$\mathfrak{a}, \mathfrak{b} \sim \mathcal{N}(0,1)$	Variáveis aleatórias independente normalmente distribuída de média zero e variância unitária
E_{M-QAM}	Energia média da constelação M-QAM
d_{min}	Distância Euclidiana mínima
$Re(a)$	Parte real de a
$Im(a)$	Parte imaginária de a
$\mathbf{F}$	Matriz das partes real e imaginária dos símbolos modulados do código de Ouro

SUMÁRIO

1 INTRODUÇÃO

A comunicação sem fio é o setor das telecomunicações que se desenvolveu mais rapidamente nos últimos anos, surgindo sempre novos produtos e serviços e fazendo cada vez mais parte do nosso dia a dia. Desde o uso de sinal de fumaça até os dias atuais, com o uso de ondas eletromagnéticas, os sistemas de comunicação sem fio passaram por uma grande evolução e se tornaram essenciais em nossa vida. Em 2019, o número de assinantes de telefonia móvel em todo o mundo passou de 8 bilhões [ITU 2020], por exemplo. A demanda de usuários vem ficando cada vez maior, assim como o surgimento crescente de aplicações, dispositivos sem fio e novas tecnologias. Como exemplos do avanço desta tecnologia temos as redes móveis 5G (Quinta Geração), redes de sensores sem fio, rodovias e fábricas automatizadas, Internet das Coisas (*Internet of Things* - IoT), casas e aparelhos inteligentes e telemedicina remota. Dessa forma, é necessário projetar sistemas de comunicação que atinjam altas taxas de dados, alta eficiência espectral e de energia, transmissão confiável e sejam capazes de mitigar os efeitos de desvanecimento de multi-percurso, ruído e interferência. Para alcançar esses objetivos, podemos explorar a diversidade no tempo, na frequência ou no espaço [Falou 2013].

Uma forma de atender esse aumento de tráfego nos sistemas de comunicação sem fio, sem prejudicar a largura de banda ou potência do sinal, é utilizar a tecnologia de múltiplas entradas e múltiplas saídas (*Multiple-Input Multiple-Output* - MIMO). O MIMO aumenta a capacidade do canal, assim como a taxa de dados e eficiência espectral, pois explora a diversidade espacial pelo uso de múltiplas antenas no transmissor e no receptor. Seu ponto chave é a capacidade de transformar a propagação de multi-percurso, até então um efeito degradante do canal sem fio, em uma vantagem na comunicação [GESBERT et al. 2003].

A tecnologia MIMO foi ganhando espaço desde seus primeiros estudos [Chiurtu, Rimoldi e Telatar 2001, Foschini e Gans 1998] que mostraram os ganhos de capacidade dos sistemas MIMO em relação ao sistemas convencionais, conhecidos também como SISO (*Single-Input Single-Output*). Foi nesse período que os códigos de espaço-tempo (*Space-Time Codes* - STC) surgiram, esse termo é mais comumente usado para se referir a um tipo particular de esquema de transmissão MIMO cujo objetivo é maximizar o ganho de diversidade. Em 1998, Tarokh formalizou o conceito de um código de espaço-tempo, e introduziu códigos de treliça de espaço-tempo (*Space-Time Trellis Code* - STTC) [Tarokh, Seshadri e Calderbank 1998], um ponto negativo desse código é que para atingir a diversidade máxima é necessário aumentar o número de antenas, fazendo com que a treliça contenha exponencialmente mais estados, como a complexidade da decodificação é proporcional ao número de estados, isso tende a se tornar excessivamente caro em termos computacionais [Sibille, Oestges e Zanella 2011].

Na mesma época, Alamouti desenvolveu um esquema de transmissão simples e atrativo que alcança a diversidade máxima em sistemas MIMO $2 \times n_r$, em que n_r denota o número de antenas transmissoras [Alamouti 1998]. Esse esquema foi generalizado para um número arbitrário de antenas de transmissão, dando origem aos códigos de bloco espaço-tempo (*Space-Time Block Code* - STBC), teoria que foi formalizada em [Tarokh, Jafarkhani e Calderbank 1999], que mostrou que as propriedades desejáveis do esquema de Alamouti surgiram porque a matriz da palavra-código é uma matriz ortogonal.

O STBC é capaz de atingir a ordem de diversidade máxima para um determinado número de antenas de transmissão e recepção e manter a propriedade de ter um algoritmo de decodificação de máxima verossimilhança (*Maximum Likelihood* - ML) muito simples, baseado no processamento linear no receptor. Porém, *desings* ortogonais complexos fornecem taxa máxima apenas para duas antenas.

A fim de obter códigos que fossem capazes de suprir as necessidades dos sistemas de comunicação sem fio com múltiplas antenas no transmissor e receptor (MIMO), os critérios de *desing* vão ficando cada vez mais rigorosos. Códigos com taxa e diversidade máximas, alta eficiência espectral e energética são requeridos, e isso demanda novas ferramentas e assim, as álgebras de divisão rapidamente se tornaram relevantes.

O conceito de usar álgebras de divisão foi primeiramente iniciado em [Sethuraman e Rajan 2002] onde as álgebras de Brauer foram apresentadas, e em [Sethuraman e Rajan 2002], onde foi apresentado que o código de Alamouti pode ser construído a partir dos quatérnios de Hamilton. Em [Sethuraman, Rajan e Shashidhar 2003], foram construídos códigos baseados em extensão de corpos e álgebras cíclicas. Posteriormente, os STBCs perfeitos foram introduzidos em [Oggier et al. 2006, Elia, Sethuraman e Kumar 2005, BELFIORE J.-C.; Rekaya e Viterbo 2005]. Conforme os estudos sobre códigos baseados em álgebras de divisão evoluíram, foi mostrado que para se atingir o *trade-off* de ganho de diversidade-multiplexação de Zheng e Tse [LIZHONG ZHENG e Tse 2003] de um código 2×2, é necessário ter um determinante diferente de zero [HUAN YAO e GREGORY W. WORNELL 2003] e que a estrutura algébrica de álgebras de divisão cíclica foi a solução para tal [BELFIORE J.-C.; Rekaya e Viterbo 2005]. Em [Elia et al. 2006] foi mostrado de forma mais geral, que códigos que utilizam álgebras de divisão são uma classe de códigos que conseguem atingir o *trade-off* ganho de diversidade-multiplexação devido a propriedade de determinante diferente de zero.

Um código que é construído a partir de álgebras cíclicas de divisão e chama atenção pelas suas propriedades é o código de Ouro 2×2 [BELFIORE J.-C.; Rekaya e Viterbo 2005], considerado o melhor STBC para sistemas MIMO com duas antenas transmissoras [OUERTANI et al. 2006]. Este código possui todas as características definidas por [Oggier et al. 2006] para ser um código perfeito, ou seja, é um código de taxa e diversidade máximas, tem determinante diferente de zero (*non-vanishing determinant* - NVD) e é energeticamente eficiente (*cubic shaping*).

Neste trabalho iremos apresentar a construção do código de Ouro via álgebras cíclicas de divisão, e também a construção do código de Alamouti via a álgebra dos quatérnios de Hamilton. Depois de apresentar as construções, iremos comparar o desempenho desses códigos em um canal MIMO 2×2 de desvanecimento Rayleigh quase-estático e plano com ruído AWGN. A performance dos códigos será analisada através da relação da taxa de erro de símbolo (*Symbol Error Rate - SER*) pela relação sinal-ruído (*Signal-to-Noise Ratio* - SNR) para diferentes ordens de modulação M-QAM. Para tal proposta, este trabalho foi estruturado da seguinte forma.

No Capítulo 2, abordamos conceitos algébricos importantes que serão utilizados nas construções dos códigos, como estruturas algébricas, a teoria algébrica dos números, álgebra cíclica de divisão e reticulados.

No Capítulo 3, apresentamos o sistema MIMO e suas características, o esquema de Alamouti, que deu origem aos códigos de bloco espaço-tempo STBC e então apresentamos os critérios de análise de

código necessários que um STBC deve possuir.

No Capítulo 4, iremos apresentar a construção do código de Alamouti via álgebras dos quatérnios de Hamilton e também de um STBC 2×2 geral a partir de álgebras cíclicas de divisão. Em seguida, apresentamos os códigos de bloco espaço-tempo perfeitos e a construção do código de Ouro, que é um STBC perfeito, via uma álgebra cíclica de divisão específica.

O Capítulo 5, tem o objetivo de apresentar os resultados obtidos das simulações e as análises do desempenho do código de Alamouti e do código de Ouro, realizadas a partir desses resultados.

Por último, o Capítulo 6 apresentada as conclusões obtidas pelo presente trabalho.

2 CONCEITOS ALGÉBRICOS

Este capítulo será dedicado em abordar alguns conceitos algébricos que serão de grande utilidade neste trabalho. Iremos apresentar definições, exemplos e alguns resultados importantes sobre estruturas algébricas, teoria algébrica dos números, álgebra cíclica e reticulados. Estes tópicos são muito amplos e para serem apresentados por completo seria necessário um estudo muito aprofundado que não é foco deste trabalho. Desta forma, iremos focar apenas nos conceitos essenciais para o desenvolvimento do mesmo. As principais referências utilizadas neste capítulo foram [Oggier, Belfiore e Viterbo 2007, Gonçalves 1999, Samuel 1970, Stewart e Tall 1987, Marcus 1977, Ferrari 2008, Benedito 2010, Benedito 2014].

2.1 ESTRUTURAS ALGÉBRICAS

Nesta seção iremos apresentar as definições de algumas estruturas algébricas importantes como grupos, anéis, ideais e corpos.

Definição 2.1.1 *Um conjunto não vazio G com uma operação $\cdot$ sobre G é chamado **grupo** se essa operação satisfaz as seguintes propriedades:*

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*, para todo* $a, b, c \in G$ *(associativa).*
2. *Existe* $e \in G$ *tal que* $a \cdot e = e \cdot a$*, para todo* $a \in G$ *(existência de um elemento neutro).*
3. *Para todo* $a \in G$ *existe um elemento* $a' \in G$ *tal que* $a \cdot a' = a' \cdot a = e$ *(existência do elemento simétrico).*

Se além disso a operação $\cdot$ for comutativa, isto é, $a \cdot b = b \cdot a$, para todo $a, b \in G$, o grupo é chamado **abeliano** ou **comutativo**.

Exemplo 2.1.1 *O conjunto* $G = \{-1, 1\}$ *um grupo com a operação multiplicação usual.*

Definição 2.1.2 *Um **grupo cíclico** G, denotado por $G = \langle g \rangle$, é um grupo gerado por um elemento, ou seja, todos os elementos do grupo são obtidos como potências de um elemento do grupo. Se G tem n elementos, tem-se que $G = \{1, g, g^2, \ldots, g^{n-1}\}$.*

Definição 2.1.3 *Um **anel** é um conjunto não vazio A composto por por duas operações $+$ (adição) e $\cdot$ (multiplicação), tal que A é um grupo abeliano em relação à operação $+$ e se a multiplicação satisfaz:*

1. *A operação $\cdot$ é associativa, ou seja, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo $a, b, c \in A$.*
2. *A operação $\cdot$ é distributiva em relação a $+$, ou seja, $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(a+b) \cdot c = a \cdot c + b \cdot c$ para todo $a, b, c \in A$.*

Definição 2.1.4 *Nas condições da Definição 2.1.3 ainda temos que:*

1. *Se $a \cdot b = b \cdot a$ para todo $a, b \in A$, é dito que A é um **anel comutativo**.*

2. *A multiplicação pode admitir em elemento neutro, isto é, existe $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$, para todo $a \in A$. Neste caso, dizemos que A é um **anel com unidade**.*

3. *Um anel cuja multiplicação é comutativa e possui unidade é chamado de **anel comutativo com unidade**.*

Exemplo 2.1.2 *O conjunto dos números inteiros $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ é um anel comutativo com unidade, sendo o número 1 a unidade em $\mathbb{Z}$.*

Definição 2.1.5 *Sejam A e B são anéis. Um **homomorfismo de anel** é uma função $\varphi : A \to B$ que satisfaz, para todo $a, b \in A$,*

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$;

2. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$;

3. $\varphi(1) = 1$.

Definição 2.1.6 *Um homomorfismo injetor de anéis é chamado de **monomorfismo** e um homomorfismo bijetor é chamado de **isomorfismo**. O isomorfismo de um anel A sobre si mesmo é chamado **automorfismo**.*

Definição 2.1.7 *Um **ideal** $\mathcal{I}$ é um subconjunto de um anel que satisfaz as seguintes condições*

1. $x + y \in \mathcal{I},\ para\ todo\ x, y \in \mathcal{I}$;

2. $a\mathcal{I} \subseteq \mathcal{I},\ para\ todo\ a \in A$.

Definição 2.1.8 *Um **ideal principal** é um ideal gerado por apenas um elemento, isto é, $\mathcal{I} = \langle x \rangle = \{xy \mid\ y \in A, x \in \mathcal{I}\}$.*

Exemplo 2.1.3 *Temos que $n\mathbb{Z} = \langle n \rangle$ é um ideal principal de $\mathbb{Z}$ para todo n.*

Definição 2.1.9 *Um **corpo** $\mathbb{K}$ é um anel comutativo onde todo elemento não nulo possui um inverso multiplicativo, ou seja, para todo $a \in A^* = A \backslash \{0\}$ existe $b \in A$ tal que $ab = 1$*

Exemplo 2.1.4 *O conjunto dos números racionais $\mathbb{Q} = \left\{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\right\}$, dos números reais $\mathbb{R}$ e dos números complexos $\mathbb{C}$, com as operações usuais de adição e de multiplicação, são exemplos de corpos.*

2.2 TEORIA ALGÉBRICA DOS NÚMEROS

Nesta seção vamos apresentar conceitos e alguns exemplos de extensão de corpos, corpos de números, anel dos inteiros, grupo de Galois, norma, traço e discriminante. Iremos apresentar também um exemplo muito importante de corpo de números, os corpos quadráticos, que são de interesse deste trabalho.

Definição 2.2.1 *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos. Se $\mathbb{K} \subseteq \mathbb{L}$, é dito que $\mathbb{L}$ é uma **extensão de corpos** de $\mathbb{K}$ e denotamos por $\mathbb{L}/\mathbb{K}$.*

Definição 2.2.2 *Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos. O **grau** da extensão de $\mathbb{L}$ sobre $\mathbb{K}$ é a dimensão de $\mathbb{L}$ como visto como espaço vetorial sobre $\mathbb{K}$, isto é, o número de elementos da base de $\mathbb{L}$ sobre $\mathbb{K}$, e denotamos por $[\mathbb{L} : \mathbb{K}]$. Se $[\mathbb{L} : \mathbb{K}]$ é finito, então $\mathbb{L}$ é uma **extensão finita** de $\mathbb{K}$, caso contrário, $\mathbb{L}$ é uma **extensão infinita** de $\mathbb{K}$.*

Definição 2.2.3 *Uma extensão de corpos finita de $\mathbb{Q}$ é chamado de um **corpo de números**.*

Neste trabalho estamos interessados em corpos de números de grau dois, conhecido como corpos quadráticos.

Definição 2.2.4 *Um corpo de números de grau dois sobre $\mathbb{Q}$ é chamado de um **corpo quadrático**.*

Proposição 2.2.1 *Um corpo quadrático tem a forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.*

Exemplo 2.2.1 *O corpo $\mathbb{K} = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ é um corpo quadrático pois é uma extensão de grau dois de $\mathbb{Q}$, já que i é solução da equação de grau dois $x^2 + 1 = 0$*

$$\begin{array}{c} \mathbb{Q}(i) \\ 2| \\ \mathbb{Q} \end{array} .$$

Exemplo 2.2.2 *O corpo $\mathbb{L} = \mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ é um corpo quadrático pois é uma extensão de grau dois de $\mathbb{Q}$, já que $\sqrt{5}$ é solução da equação de grau dois $x^2 - 5 = 0$*

$$\begin{array}{c} \mathbb{Q}(\sqrt{5}) \\ 2| \\ \mathbb{Q} \end{array} .$$

Definição 2.2.5 *Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos e $\theta \in \mathbb{L}$. Se existe um polinômio mônico (com coeficiente de maior grau igual a 1), irredutível e não nulo $p \in \mathbb{K}[X]$ tal que $p(\theta) = 0$, então é dito que θ é **algébrico** sobre $\mathbb{K}$. Este polinômio é conhecido como **polinômio minimal**.*

Exemplo 2.2.3 *O polinômio $p(X) = X^2 + 1$ é o polinômio minimal de i sobre $\mathbb{Q}$. Assim como $q(X) = X^2 - 5$ é o polinômio minimal de $\sqrt{5}$ sobre $\mathbb{K} = \mathbb{Q}(i)$.*

Definição 2.2.6 *Se todos os elementos de $\mathbb{L}$ são algébricos sobre $\mathbb{K}$, então é dito que $\mathbb{L}$ é uma **extensão algébrica** de $\mathbb{K}$.*

Teorema 2.2.1 *Se $\mathbb{K}$ é um corpo de números, então existe um número algébrico $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$.*

O número algébrico $\theta \in \mathbb{K}$ é chamado de **elemento primitivo** de $\mathbb{K}$. Além disso, pelo Teorema 2.2.1, tem-se que o corpo de números $\mathbb{K}$ é um $\mathbb{Q}$-espaço vetorial gerado pelas potências de θ e se, $\mathbb{K}$ tem grau n sobre $\mathbb{Q}$, então a base de $\mathbb{K}$ é $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$. Ou seja, $x \in \mathbb{K}$ pode ser escrito como $x = \sum_{i=0}^{n-1} x_i\theta^i, x_i \in \mathbb{Q}$, onde n é grau do polinômio minimal de θ.

Definição 2.2.7 *Sejam $\mathbb{K}/\mathbb{Q}$ e $\mathbb{L}/\mathbb{Q}$ duas extensões de corpos de $\mathbb{Q}$. Se φ é um homomorfismo de anel que satisfaz $\varphi(a) = a$ para todo $a \in \mathbb{Q}$, então a aplicação $\varphi : \mathbb{K} \to \mathbb{L}$ é chamada de **homomorfismo** sobre $\mathbb{Q}$.*

Teorema 2.2.2 *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n sobre $\mathbb{Q}$. Existem n monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$, $\sigma_i : \mathbb{K} \to \mathbb{C}$, tais que $\sigma_i(\theta) = \theta_i$, $i = 1, \ldots, n$, onde θ_i são os zeros distintos em $\mathbb{C}$ do polinômio minimal de θ sobre $\mathbb{Q}$.*

Definição 2.2.8 *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os n-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$. Temos que:*

1. *Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ dizemos que σ_i é um **monomorfismo real**. Caso contrário dizemos que σ_i é um **monomorfismo imaginário**.*
2. *Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$, para todo $i = 1, \ldots, n$, dizemos que $\mathbb{K}$ é um **corpo totalmente real**. Caso contrário, dizemos que $\mathbb{K}$ é um **corpo totalmente imaginário**.*

Exemplo 2.2.4 *Seja $\mathbb{K} = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. Uma vez que $X^2 + 1 = (X + i)(X - i)$, então existem dois monomorfismos dados por*

$$\begin{array}{rccc} \sigma_1 : & \mathbb{Q}(i) & \to & \mathbb{C} \\ & a + bi & \mapsto & a + bi \end{array}$$

e

$$\begin{array}{rccc} \sigma_2 : & \mathbb{Q}(i) & \to & \mathbb{C} \\ & a + bi & \mapsto & a - bi \end{array}.$$

Como σ_1 e σ_2 são imaginários, dizemos que $\mathbb{K} = \mathbb{Q}(i)$ é um corpo totalmente imaginário.

Exemplo 2.2.5 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5}) = \{a+b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. Uma vez que $X^2-5 = (X+\sqrt{5})(X-\sqrt{5})$, então existem dois monomorfismos dados por*

$$\begin{array}{rccc} \sigma_1 : & \mathbb{Q}(\sqrt{5}) & \to & \mathbb{R} \\ & a + b\sqrt{5} & \mapsto & a + b\sqrt{5} \end{array}$$

e

$$\begin{array}{rccc} \sigma_2: & \mathbb{Q}(\sqrt{5}) & \to & \mathbb{R} \\ & a+b\sqrt{5} & \mapsto & a-b\sqrt{5} \end{array}.$$

Como σ_1 e σ_2 são reais, dizemos que $\mathbb{K}=\mathbb{Q}(\sqrt{5})$ é um corpo totalmente real.

Observação 2.2.1 *Quando σ_i são definidos de $\mathbb{K}$ para $\mathbb{K}$, para todo $i=1,\ldots,n$, eles são chamados de $\mathbb{Q}$-automorfismo de $\mathbb{K}$.*

Exemplo 2.2.6 *No Exemplo 2.2.4 observe que ambos os monomorfismos definidos podem ser também mapeamentos de $\mathbb{Q}(i)$ para ele mesmo, ou seja, ambas as raízes do polinômio minimal X^2+1 pertencem a $\mathbb{Q}(i)$.*

Definição 2.2.9 *Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos de grau n. Os n $\mathbb{K}$-homomorfismos de $\mathbb{L}$ em $\mathbb{C}$ são chamados de **monomorfismos relativos**.*

Exemplo 2.2.7 *Se adicionarmos o elemento $\sqrt{5}$ ao corpo $\mathbb{Q}(i)$, obtemos um corpo de números $\mathbb{Q}(i,\sqrt{5})$ de grau 4 sobre $\mathbb{Q}$. Considere a extensão de corpos relativa $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i)$. O polinômio $p(x)=x^2-5$ é um polinômio minimal sobre $\mathbb{Q}(i)$ de grau dois*

$$\begin{array}{c} \mathbb{Q}(i,\sqrt{5}) \\ 2| \\ \mathbb{Q}(i) \end{array}.$$

Como

$$x^2-5=\left(x-\sqrt{5}\right)\left(x+\sqrt{5}\right),$$

então $\pm\sqrt{5}\in\mathbb{Q}(i,\sqrt{5})$. Logo, os monomorfismos relativos de $\mathbb{Q}(i,\sqrt{5})$ sobre $\mathbb{Q}(i)$ são

$$\begin{array}{rccc} \sigma_1: & \mathbb{Q}(i,\sqrt{5}) & \to & \mathbb{C} \\ & a+b\sqrt{5} & \mapsto & a+b\sqrt{5} \end{array}$$

e

$$\begin{array}{rccc} \sigma_2: & \mathbb{Q}(i,\sqrt{5}) & \to & \mathbb{C} \\ & a+b\sqrt{5} & \mapsto & a-b\sqrt{5} \end{array},$$

para $a,b\in\mathbb{Q}(i)$.

Definição 2.2.10 *Seja $\mathbb{K}$ um corpo de números. Dizemos que $\theta\in\mathbb{K}$ é um número **inteiro algébrico** se θ for uma raiz do polinômio mônico com coeficientes em $\mathbb{Z}$. O conjunto de inteiros algébricos de $\mathbb{K}$ é um anel chamado de **anel de inteiros** de $\mathbb{K}$, denotado por $\mathcal{O}_{\mathbb{K}}$.*

Teorema 2.2.3 *Seja $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ um corpo quadrático, então o seu anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é dado por:*

1. *Se $d\equiv 2$ ou $d\equiv 3 \pmod 4$, então $\mathcal{O}_{\mathbb{K}}=\mathbb{Z}[\sqrt{d}]$ e sua $\mathbb{Z}$-base é dada por $\{1,\sqrt{d}\}$.*
2. *Se $d\equiv 1 \pmod 4$, então $\mathcal{O}_{\mathbb{K}}=\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ e sua $\mathbb{Z}$-base é dada por $\{1,\frac{1+\sqrt{d}}{2}\}$.*

Exemplo 2.2.8 *Considere o corpo de números* $\mathbb{K} = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. *Quando* a *e* b *são restritos a* $\mathbb{Z}$, *obtém-se pelo Teorema 2.2.3 que o anel dos inteiros de* $\mathbb{K}$ *dado por* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ *chamado de* ***anel dos inteiros Gaussiano****. Observa-se que a constelação obtida a partir de uma modulação QAM pode ser rotulada a partir de* $\mathbb{Z}[i] + (1 + i)/2$.

Exemplo 2.2.9 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *um corpo quadrático, pelo Teorema 2.2.3, temos que seu anel de inteiros é dado por* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \left\{a + b\left(\frac{1+\sqrt{5}}{2}\right) \mid a, b \in \mathbb{Z}\right\}$.

Definição 2.2.11 *Seja* $\mathbb{K}$ *um corpo de números. Dizemos que o conjunto* $\{\omega_1, \omega_2, \ldots, \omega_n\}$ *de* $\mathcal{O}_{\mathbb{K}}$ *é uma* ***base integral*** *de* $\mathbb{K}$, *se qualquer elemento* x *de* $\mathcal{O}_{\mathbb{K}}$ *pode ser escrito de forma única como* $x = \sum_{i=1}^{n} a_i\omega_i$, *com* $a_i \in \mathbb{Z}$, *para todo* i.

Definição 2.2.12 *Seja* $\mathbb{L}/\mathbb{K}$ *uma de extensão de corpos de grau* n, *onde* $\sigma_1, \ldots, \sigma_n$ *representa os* n *monomorfismos relativos de* $\mathbb{L}$

$$N(x) = \prod_{i=1}^{n} \sigma_i(x), \quad Tr(x) = \sum_{i=1}^{n} \sigma_i(x) \tag{2.1}$$

são chamados, respectivamente, a ***norma*** *e o* ***traço*** *de x.*

Teorema 2.2.4 *Seja* $\mathbb{L}/\mathbb{K}$ *uma extensão de corpos. Para qualquer* $x \in \mathbb{L}$, *temos* $N_{\mathbb{L}/\mathbb{K}}(x)$ *e* $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) \in \mathbb{K}$. *Se* $x \in \mathcal{O}_{\mathbb{L}}$, *temos* $N_{\mathbb{L}/\mathbb{K}}(x)$ *e* $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) \in \mathcal{O}_{\mathbb{K}}$.

Definição 2.2.13 *Seja* $\mathcal{I} = \langle x \rangle = x\mathcal{O}_{\mathbb{L}}$ *um ideal principal de* $\mathcal{O}_{\mathbb{L}}$ *e* $x \neq 0$. *A norma de* $\mathcal{I}$ *é definida por* $N(\mathcal{I}) = |N(x)|$.

Definição 2.2.14 *Seja* $\{\omega_1, \omega_2, \ldots, \omega_n\}$ *uma base integral de* $\mathbb{K}$. *O* ***discriminante*** *de* $\mathbb{K}$ *é definido como* $d_{\mathbb{K}} = \det[\sigma_j(\omega_i)]^2$.

Exemplo 2.2.10 *Vamos calcular o discriminante* $d_{\mathbb{K}}$ *do corpo* $\mathbb{Q}(\sqrt{5})$. *Pelo Exemplo 2.2.5, aplicando os monomorfismos na base integral* $\{\omega_1, \omega_2\} = \{1, \frac{1+\sqrt{5}}{2}\}$, *temos*

$$d_{\mathbb{K}} = \det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}^2 = \det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1+\sqrt{5}}{2} \end{pmatrix}^2 = 5. \tag{2.2}$$

No caso de corpos quadráticos existe um resultado que fornece o discriminante.

Proposição 2.2.2 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *é um corpo quadrático, então o discriminante de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por:*

1. $d_{\mathbb{K}} = d$, *se* $d \equiv 1 \pmod 4$.
2. $d_{\mathbb{K}} = 4d$, *se* $d \equiv 2$ *ou* $3 \pmod 4$.

Exemplo 2.2.11 *No caso do corpo* $\mathbb{Q}(i)$, *temos que* $\sqrt{-1} = i$, *logo* $d = -1$. *Então, seu discriminante, pela Proposição 2.2.2, é* $d_{\mathbb{K}} = -4$. *Uma vez que* $-1 \equiv 3 \pmod 4$.

Definição 2.2.15 *Uma extensão de corpos de números $\mathbb{L}/\mathbb{K}$ é uma **extensão de Galois** se todas as raízes de cada polinômio irredutível sobre $\mathbb{K}$ estão em $\mathbb{L}$. O **grupo de Galois** da extensão $\mathbb{L}/\mathbb{K}$ é o grupo de todos automorfismos de $\mathbb{K}$ sobre $\mathbb{L}$ e denotamos por Gal($\mathbb{L}/\mathbb{K}$).*

Observação 2.2.2 *Um grupo cíclico de Galois é representado por $\langle\sigma\rangle$, onde σ é o elemento gerador do grupo.*

2.3 ÁLGEBRA CÍCLICA

Nesta seção vamos apresentar conceitos de álgebra, álgebra de divisão e álgebra cíclica. Em especial, estamos interessados em álgebras cíclicas de divisão para construir STBC para 2×2 antenas, dessa forma, a álgebra dos quatérnios será considerada.

Definição 2.3.1 *Uma **álgebra** $\mathcal{A}$ é um conjunto sobre o corpo $\mathbb{K}$ com operações de adição, multiplicação e multiplicação por elementos de $\mathbb{K}$ que satisfaz:*

1. *$\mathcal{A}$ é um **espaço vetorial** com respeito à adição e multiplicação pelos elementos do corpo.*
2. *$\mathcal{A}$ é um anel em relação à adição e multiplicação.*
3. *$(\lambda a)b = a(\lambda b) = \lambda(ab)$ para qualquer $\lambda \in \mathbb{K}, a, b \in \mathcal{A}$.*

Exemplo 2.3.1 *O conjunto $\mathcal{M}_n(\mathbb{R})$ de matrizes $n \times n$ com entradas em $\mathbb{R}$ é uma álgebra sobre $\mathbb{R}$. É um espaço vetorial de dimensão n^2 sobre $\mathbb{R}$ e é um anel não-comutativo em relação a adição e multiplicação usual de matrizes.*

Definição 2.3.2 *Se em uma álgebra $\mathcal{A}$ todo elemento não nulo tem um inverso multiplicativo, então $\mathcal{A}$ é uma **álgebra de divisão**.*

Definição 2.3.3 *Seja $\mathbb{L}/\mathbb{K}$ uma extensão de Galois de grau n, tal que seu grupo de Galois $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ é cíclico com gerador σ. Dado um elemento $\gamma \in \mathbb{K}$ diferente de zero, pode-se definir uma **álgebra cíclica**, denotada por $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$, como segue*

$$\mathcal{A} = \mathbb{L} \oplus e\mathbb{L} \oplus \cdots \oplus e^{n-1}\mathbb{L}, \tag{2.3}$$

em que e satisfaz

$$e^n = \gamma \quad \text{e} \quad \lambda e = e\sigma(\lambda),$$

para $\lambda \in \mathbb{L}$ e $\oplus$ representa a soma direta.

Definição 2.3.4 *Chamamos de **álgebra cíclica de divisão**, uma álgebra que seja cíclica e também de divisão.*

Teorema 2.3.1 *Seja $\mathbb{L}/\mathbb{K}$ uma extensão cíclica de grau n com Gal$(\mathbb{L}/\mathbb{K}) = \langle\sigma\rangle$. Se $\gamma \in \mathbb{K}$ diferente de zero não é uma norma de algum elemento de $\mathbb{L}$, então $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$ é uma álgebra de divisão cíclica.*

Sejam $\mathcal{A}$ uma álgebra cíclica e $x \in \mathcal{A}$ escrito na base $\{1, e, e^2, \ldots, e^{n-1}\}$, ou seja,

$$x = x_0 + ex_1 + x_2e^2 + \ldots + x_{n-1}e^{n-1}. \tag{2.4}$$

A matriz de multiplicação à esquerda por *x* é dada por

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}. \tag{2.5}$$

Para o caso de $n = 2$, sejam $x = x_0 + ex_1, y = y_0 + ey_1 \in \mathcal{A}$ na base $\{1, e\}$, tem-se que

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0y_0 + x_0ey_1 + ex_1y_0 + ex_1ey_1 \\ &= x_0y_0 + e\sigma(x_0)y_1 + ex_1y_0 + e^2\sigma(x_1)y_1 \\ &= x_0y_0 + e\sigma(x_0)y_1 + ex_1y_0 + \gamma\sigma(x_1)y_1 \\ &= (x_0y_0 + \gamma\sigma(x_1)y_1) + e(\sigma(x_0)y_1 + x_1y_0), \end{aligned} \tag{2.6}$$

uma vez que $\gamma = e^2$. Na forma matricial, tem-se

$$xy = \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}. \tag{2.7}$$

Além disso, temos que

$$\det \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} = x_0\sigma(x_0) - \gamma x_1\sigma(x_1) = N_{\mathbb{L}/\mathbb{K}}(x_0) - \gamma N_{\mathbb{L}/\mathbb{K}}(x_1). \tag{2.8}$$

Então

$$\det \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} = 0 \iff \gamma = N_{\mathbb{L}/\mathbb{K}}\left(\frac{x_0}{x_1}\right). \tag{2.9}$$

Assim, pelo Teorema 2.3.1, é preciso verificar se γ é uma norma de algum elemento de $\mathbb{L}$ para garantir que $\mathcal{A}$ é uma álgebra cíclica de divisão.

O caso de interesse neste trabalho são álgebras cíclicas de divisão para $n = 2$. Para isso, iremos definir um caso particular dessas álgebras, a álgebra do quatérnios.

Definição 2.3.5 *Uma **álgebra dos quatérnios** $\mathcal{A} = (a, b)_{\mathbb{K}}$ sobre um corpo de números $\mathbb{K}$ é uma álgebra de dimensão 4 sobre $\mathbb{K}$ com base $\{1, i, j, k\}$ que satisfaz a condição $i^2 = a$, $j^2 = b$, $k^2 = -ab$ e $k = ij = -ji$, onde $a, b \in \mathbb{K}\backslash\{0\}$.*

Um exemplo especial de álgebra dos quatérnios, que na verdade foi a percursora dessas álgebras, é

a hoje conhecida como álgebra dos quatérnios de Hamilton que definiremos a seguir.

Definição 2.3.6 *A álgebra dos quatérnios $\mathbb{H} = (-1,-1)_{\mathbb{R}}$ que satisfaz $i^2 = -1$, $j^2 = -1$, $k^2 = -1$, e $k = ij = -ji$, é chamada de **álgebra dos quatérnios de Hamilton**. Os quatérnios de Hamilton podem ser representados pelo conjunto*

$$\mathbb{H} = \{x_0 + x_1 i + x_2 j + x_3 k \mid x_0, x_1, x_2, x_3 \in \mathbb{R}\}, \tag{2.10}$$

que possuem uma estrutura de anel com adição e multiplicação bem definidas.

Definição 2.3.7 *Para um elemento $q = x_0 + x_1 i + x_2 j + x_3 k$ de uma álgebra dos quatérnios podemos definir o **conjugado** de q como*

$$\bar{q} = x_0 - x_1 i - x_2 j - x_3 k. \tag{2.11}$$

Definição 2.3.8 *Seja $\mathcal{A}$ uma $\mathbb{K}$-álgebra, definimos o **traço reduzido** e **norma reduzida** de um elemento $q \in \mathcal{A}$ por*

$$Trd(q) = q + \bar{q} \; e \; Nrd(q) = q\bar{q}, \tag{2.12}$$

respectivamente.

Exemplo 2.3.2 *Se $\mathbb{H} = (-1,-1)_{\mathbb{R}}$ é a álgebra dos quatérnios de Hamilton então*

$$Trd(q) = q + \bar{q} = 2x_0 \quad e \quad Nrd(q) = q\bar{q} = x_0^2 + x_1^2 + x_2^2 + x_3^2, \tag{2.13}$$

para todo $q = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{H}$.

Observe por (2.13) que $Nrd(q) = 0$ se, e somente se $q = 0$. Este resultado é válido em geral para toda álgebra dos quatérnios.

Teorema 2.3.2 *Seja $\mathcal{A} = (a,b)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre $\mathbb{K}$. $\mathcal{A}$ é uma álgebra de divisão se, e somente se, $Nrd(q) = 0$ apenas para $q = 0$.*

Observação 2.3.1 *Nas condições das Definições 2.3.7 e 2.3.8, segue pelo Teorema 2.3.2 que para $q = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{A}$, a não ser que $x_0 = x_1 = x_2 = x_3 = 0$, tem-se $q\bar{q} > 0$, para todo $x_0, x_1, x_2, x_3 \in \mathbb{K}$. Assim, temos que o **inverso** de q é dado da seguinte forma*

$$q^{-1} = \frac{\bar{q}}{q\bar{q}}. \tag{2.14}$$

2.4 RETICULADOS

Nesta seção iremos apresentar conceitos básicos sobre reticulados algébricos construídos a partir do conhecido como homomorfismo canônico e ideais, apresentando suas matrizes geradoras e matriz de Gram. Neste trabalho, o interesse na construção de reticulados algébricos está relacionado com a propriedade de *shaping* de uma constelação que é obtida quando utilizamos reticulados munidos de certas propriedades. A teoria de reticulados e reticulados algébricos é muito ampla e por não ser foco

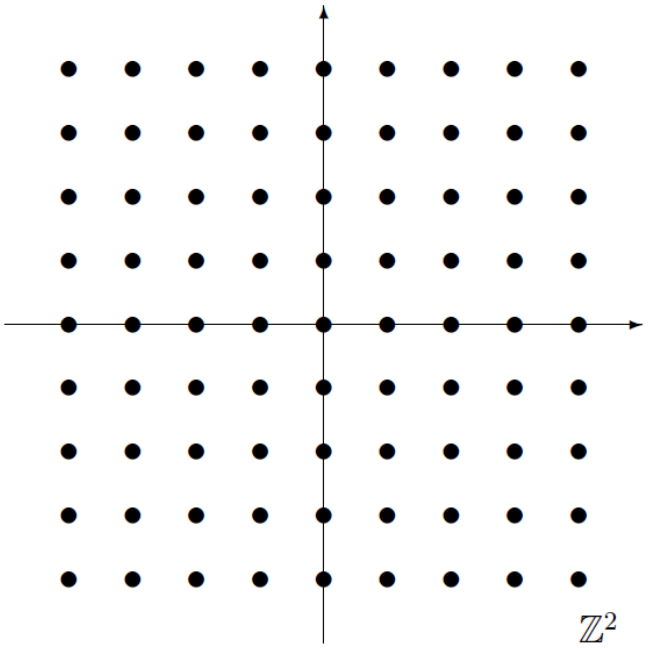
deste trabalho não serão apresentados os detalhes, para um estudo mais aprofundado ver [Benedito 2010, Ferrari 2008].

Definição 2.4.1 *Sejam $\mathcal{B} = \{\omega_1, \ldots, \omega_n\}$ um conjunto de vetores do $\mathbb{R}^n$ linearmente independentes sobre $\mathbb{R}$. Chamamos de **reticulado completo** de dimensão n e base $\mathcal{B}$ ao subconjunto do $\mathbb{R}^n$ da forma*

$$\Lambda = \left\{ x \in \mathbb{R}^n, \ tal \ que \ x = \sum_{i=1}^{n} a_i \omega_i, \ com \ a_i \in \mathbb{Z} \right\}. \tag{2.15}$$

Exemplo 2.4.1 *Seja $\mathcal{B} = \{(1,0)(0,1)\}$ a base canônica de $\mathbb{Z}^2$. Temos que $\Lambda = \mathbb{Z}^2$ é reticulado gerado por $\mathcal{B}$.*

Figura 1 – Reticulado $\mathbb{Z}^2$.



Fonte: [**?**]

Definição 2.4.2 *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado, com $\mathbb{Z}$-base $\mathcal{B} = \{\omega_1, \ldots, \omega_n\}$. A **matriz geradora** do reticulado Λ é definida como sendo a matriz*

$$\mathbf{M} = \begin{pmatrix} \omega_{11} & \omega_{12} & \cdots & \omega_{1n} \\ \omega_{21} & \omega_{22} & \cdots & \omega_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{n1} & \omega_{n2} & \cdots & \omega_{nn} \end{pmatrix}, \tag{2.16}$$

no qual $\omega_i = (\omega_{1i}, \cdots, \omega_{ni})$, para todo $i = 1, \cdots, n$.

Um reticulado Λ pode ser expresso por meio da sua matriz geradora $\mathbf{M}$

$$\Lambda = \{\mathbf{x} = \boldsymbol{\lambda}\mathbf{M} \ \in \mathbb{R}^n \mid \boldsymbol{\lambda} \in \mathbb{Z}^n\}, \tag{2.17}$$

ou ainda por sua matriz de Gram que será definida a seguir.

Definição 2.4.3 *Sejam Λ um reticulado e $\mathbf{M}$ sua matriz geradora. Definimos a **matriz de Gram** associada a matriz geradora por*

$$\mathbf{G} = \mathbf{M}^{\dagger}\mathbf{M}. \tag{2.18}$$

Definição 2.4.4 *Sejam $\sigma_1, \ldots, \sigma_n$ os n monomorfismos distintos de um corpo de números $\mathbb{K}$ de grau n. Podemos ordenar os σ_i's de forma que para todo $x \in \mathbb{K}, \sigma_i(x) \in \mathbb{R}, 1 \leq i \leq r_1$, ou seja, até o índice r_1 os monomorfismos $\sigma_1, \ldots, \sigma_{r_1}$ sejam reais e $\sigma_{j+r_2}(x)$ é o complexo conjugado de $\sigma_j(x)$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Note que $r_1 + 2r_2 = n$. Chamamos de **homomorfismo canônico** $\sigma : \mathbb{K} \to \mathbb{R}^n$ o homomorfismo definido por*

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)). \tag{2.19}$$

Exemplo 2.4.2 *Sejam o corpo quadrático $\mathbb{K} = \mathbb{Q}(i)$ e $\{\sigma_1, \sigma_2\}$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ dados no Exemplo 2.2.4, onde σ_1 é a aplicação identidade e $\sigma_2(a + bi) = a + bi$, com $a, b \in \mathbb{Q}$. Neste caso, temos que $r_1 = 0$ e $r_2 = 1$, ou seja, $\mathbb{K}$ é um corpo totalmente imaginário. Para $x = a + bi \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, temos que o homomorfismo canônico é dado por*

$$\sigma = (\Re\sigma_1(x), \Im\sigma_1(x)) = (a, b). \tag{2.20}$$

Um **reticulado algébrico** Λ é um reticulado que pode ser construído como imagem do homomorfismo canônico definido em (2.4.4) aplicado em uma base $\{\omega_1, \ldots, \omega_n\}$ de $\mathcal{O}_{\mathbb{K}}$, sendo sua matriz geradora $\mathbf{M}$ dada por

$$\mathbf{M} = \begin{pmatrix} \sigma_1(\omega_1) & \cdots & \sigma_{r_1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1), \ldots, \Im\sigma_{r_1+r_2}(\omega_1) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \cdots & \sigma_{r_1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n), \ldots, \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix}. \tag{2.21}$$

Esta construção resulta em um reticulado real.

De forma semelhante, podemos definir um homomorfismo considerando uma extensão de corpos mais geral $\mathbb{L}/\mathbb{K}$ da seguinte forma

$$\begin{array}{rccl} \sigma: & \mathbb{L} & \to & \mathbb{C}^n \\ & x & \mapsto & \sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x)), \end{array} \tag{2.22}$$

onde $\sigma_1(x), \ldots, \sigma_n(x)$ são os monomorfismos relativos de $\mathbb{L}/\mathbb{K}$.

Assim, um reticulado complexo Λ^c é dado por

$$\Lambda^c = \{\mathbf{x} = \boldsymbol{\lambda}\mathbf{M} \ \in \mathbb{C}^n \mid \boldsymbol{\lambda} \in \mathbb{Z}[i]^n \text{ ou } \mathbb{Z}[j]^n\}. \tag{2.23}$$

E sua matriz geradora é dada, usando o homomorfismo dado em (2.22), por

$$\mathbf{M} = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \cdots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \cdots & \sigma_n(\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \cdots & \sigma_n(\omega_n) \end{pmatrix}, \tag{2.24}$$

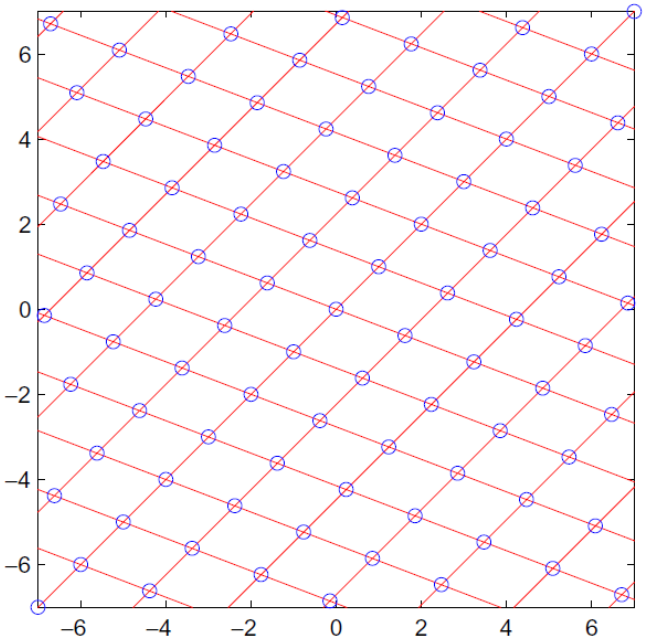
onde $\{\omega_1, \ldots, \omega_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{K}$, e $\sigma_1, \ldots, \sigma_n$ são monomorfismos relativos de $\mathbb{L}/\mathbb{K}$.

Exemplo 2.4.3 *Seja o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, com os monomorfismos $\sigma_1(\sqrt{5}) = \sqrt{5}$ e $\sigma_2(\sqrt{5}) = -\sqrt{5}$ obtidos no Exemplo 2.2.5 e seu anel de inteiros $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ no Exemplo 2.2.9. Assim, aplicando o homomorfismo canônico nos elementos da base $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$, a matriz geradora do reticulado algébrico Λ é dada por*

$$\mathbf{M} = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}. \tag{2.25}$$

E a representação deste reticulado é apresentado na Figura 2.

Figura 2 – Reticulado do corpo $\mathbb{Q}(\sqrt{5})$.



Fonte: [Oggier, Belfiore e Viterbo 2007]

Um reticulado algébrico Λ' pode ser construído a partir de um ideal $\mathcal{I} \subset \mathcal{O}_L$, sendo um subreticulado do reticulado algébrico Λ obtido a partir de $\mathcal{O}_{\mathbb{L}}$. Se $\mathcal{I} = \alpha\mathcal{O}_{\mathbb{L}}$, então a matriz geradora $\mathbf{M}$

de Λ' é dada por

$$\mathbf{M} = \begin{pmatrix} \sigma_1(\alpha\omega_1) & \sigma_2(\alpha\omega_1) & \cdots & \sigma_n(\alpha\omega_1) \\ \sigma_1(\alpha\omega_2) & \sigma_2(\alpha\omega_2) & \cdots & \sigma_n(\alpha\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\alpha\omega_n) & \sigma_2(\alpha\omega_n) & \cdots & \sigma_n(\alpha\omega_n) \end{pmatrix}, \tag{2.26}$$

onde $\{\omega_1, \ldots, \omega_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{K}$, e $\sigma_1, \ldots, \sigma_n$ são monomorfismos relativos de $\mathbb{L}/\mathbb{K}$. Observe que, a matriz dada em (2.26) é a matriz dada em (2.24) multiplicada pela matriz diagonal

$$\begin{pmatrix} \sigma_1(\alpha) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\alpha) \end{pmatrix}. \tag{2.27}$$

Conhecendo a matriz geradora do reticulado, é possível calcular o **determinante** do mesmo. Temos que

$$\begin{aligned} \det(\Lambda') &= |\det(\mathbf{M})|^2 = |\det[\sigma_j(\alpha\omega_i)]|^2 && (2.28) \\ &= |N(\alpha)|^2 |\det[\sigma_j(\omega_i)]|^2 && (2.29) \\ &= |N(\alpha)|^2 d_K = |N(\alpha)|^2 \det(\Lambda). && (2.30) \end{aligned}$$

3 CÓDIGOS DE BLOCO ESPAÇO-TEMPO

Neste capítulo, iremos apresentar um estudo sobre o sistema MIMO e suas características, em seguida o esquema de Alamouti, que deu origem aos códigos de bloco espaço-tempo STBC será apresentado, além de critérios de análise utilizados para definir um STBC eficiente. As principais referências utilizadas neste capítulo foram [Sibille, Oestges e Zanella 2011, Falou 2013, Alamouti 1998, Oggier, Belfiore e Viterbo 2007, Biglieri et al. 2007, Salz, Winters e Gitlin 1994].

3.1 SISTEMA MIMO

O sistema MIMO (*Multiple-Input Multiple-Output*) é uma tecnologia que utiliza múltiplas antenas transmissoras e receptoras, e que ganhou popularidade rapidamente na última década devido aos seus eficientes recursos de aprimoramento de desempenho [Biglieri et al. 2007].

Em um sistema de comunicação sem fio, os canais sofrem os efeitos degradantes do desvanecimento de multi-percurso. O multi-percurso consiste na chegada do sinal transmitido com ângulos, atrasos de tempo e mudanças de frequência (Efeito Doppler) diferentes. As causas desse fenômeno incluem difração de sinal, refração e reflexão, espalhamento e pela presença de obstruções, como edifícios, montanhas, etc., além da questão da mobilidade do transmissor ou receptor. Esses efeitos afetam gravemente a qualidade e a confiabilidade da comunicação sem fio. Ainda, temos as restrições impostas pela largura de banda de frequência escassa e potência limitada, que tornam ainda mais desafiador o trabalho de projetar sistemas de comunicação sem fio de alta confiabilidade e alta taxa de dados.

A fim de mitigar os efeitos do desvanecimento, utilizamos algumas técnicas que estão relacionadas com o conceito de diversidade. A diversidade explora a natureza aleatória da propagação de rádio, transmitindo réplicas do mesmo dado com objetivo que elas sejam atenuadas independentemente das outras, assim, o receptor recebe múltiplas versões do mesmo sinal. Isso faz com que a probabilidade de todas as réplicas desvanecerem simultaneamente diminua à medida que o número de réplicas aumenta.

A seguir, vamos apresentar dois tipos de esquema de diversidade em um sistema de comunicação sem fio.

- Diversidade de tempo: consiste em transmitir o mesmo sinal em intervalos de tempo diferentes. Esses períodos devem ser espaçados de modo que os coeficientes de desvanecimento do canal mudem e diferentes ganhos de canal sejam obtidos.

- Diversidade de espaço: consiste na transmissão do sinal por várias antenas de transmissão e recebido através de diferentes antenas de recepção. Isso é aplicável nos casos em que o espaçamento da antena é de pelo menos meio comprimento de onda da frequência da portadora, garantindo que o desvanecimento em cada caminho será independente (ou descorrelacionado) [Salz, Winters e Gitlin 1994]. Os códigos de espaço-tempo, como o nome já diz, exploram a diversidade no espaço e no tempo.

Além disso, temos duas formas diferentes de diversidade de espaço.

- Diversidade de recepção: em canais do tipo SIMO (*Single-Input Multiple-Output*), é transmitido apenas uma versão do sinal, as réplicas do sinal transmitido são obtidas no receptor e, então, é feita a combinação dessas réplicas. No entanto, em telefones celulares torna-se caro e complicado sua implantação, por isso a diversidade de transmissão se tornou popular.

- Diversidade de transmissão: em canais do tipo MISO (*Multiple-Input Single-Output*), são transmitidas várias réplicas do sinal para apenas um antena de recepção. Para isso, é necessário o uso de técnicas de processamento de sinais, como os códigos espaço-tempo.

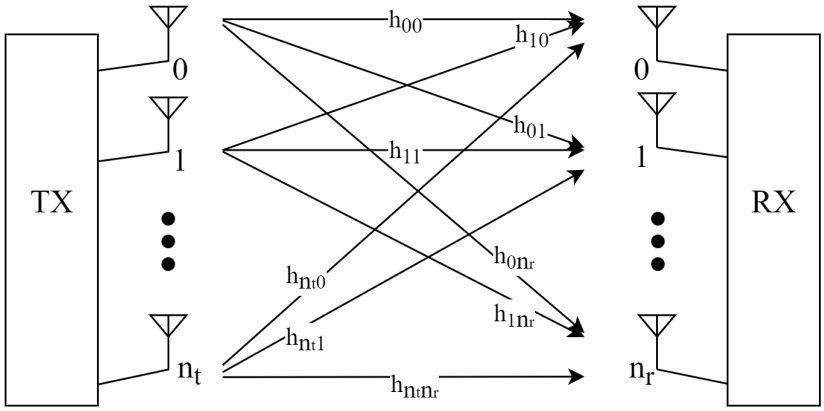
Por o canal MIMO ser de múltiplas antenas no transmissor e no receptor, é obtido ambas diversidade de espaço: a de transmissão e a de recepção. E esses canais que utilizam STBCs conseguem obter também a diversidade de tempo.

Neste trabalho iremos considerar um canal com desvanecimento Rayleigh quase-estático e plano, em que desvanecimento quase-estático significa que o canal permanece constante dentro de cada período de transmissão de uma palavra-código, variando independentemente de um período para o próximo, e plano significa que a largura de banda de coerência do canal é maior do que a largura de banda do sinal, por isso todas as componentes de frequência do sinal sofrem um desvanecimento de magnitude igual. Considere um sistema MIMO com n_t antenas no transmissor e n_r antenas no receptor, conforme Figura 3, a matriz $\mathbf{Y}$ do sinal recebido é dada por

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t} \mathbf{X}_{n_t \times T} + \mathbf{Z}_{n_r \times T}, \tag{3.1}$$

em que $\mathbf{X}$ é a matriz de símbolos transmitidos, $\mathbf{H}$ é a matriz do canal e seus elementos são modelados como uma variável aleatória complexa de média zero e variância unitária, e $\mathbf{Z}$ é a matriz do ruído Gaussiano branco aditivo. Isso para um único bloco de duração T, em que o canal permanece invariante no tempo e vamos assumir que T seja igual ao intervalo de tempo em que os coeficientes de canal são constantes.

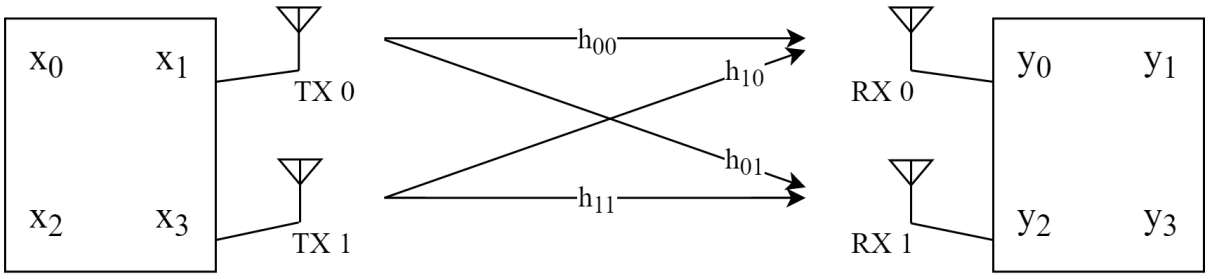
Figura 3 – Esquema sistema MIMO $n_t \times n_r$.



Fonte: Próprio autor.

Considere o exemplo de um caso interessante, em que se tem duas antenas de transmissão e duas de recepção, conforme Figura 4.

Figura 4 – Esquema sistema MIMO 2×2.



Fonte: Próprio autor.

Neste caso, a primeira antena transmite os símbolos x_0 e x_1 e a segunda antena transmite os símbolos x_2 e x_3. Os símbolos x_0 e x_2 são os primeiros a serem enviados, as duas antenas receptoras recebem os símbolos y_0 e y_2 que são uma combinação dos símbolos enviados pelo transmissor que sofreram os efeitos do canal. O mesmo acontece para os símbolos x_1 e x_3, produzindo então y_1 e y_3.

A decodificação é feita pelo método de máxima verossimilhança (ML), onde o receptor escolhe a palavra-código $\mathbf{X}$ que minimiza:

$$\min_{\mathbf{X} \in \mathcal{C}} \|\mathbf{Y} - \mathbf{HX}\|^2. \tag{3.2}$$

Para canais MIMO, como o modelado anteriormente, supondo que o receptor seja coerente, isto é, que ele tenha o conhecimento exato sobre o estado do canal ou um CSI (*Channel State Information*) perfeito. A sua capacidade pode ser expressa como [Gesbert et al. 2003]

$$C(\text{SNR}) = \log_2 \left[\det \left(\mathbf{I}_{n_r} + \frac{\text{SNR}}{n_t} \mathbf{H}\mathbf{H}^\dagger \right) \right], \tag{3.3}$$

em que $\mathbf{I}_{n_r}$ é a matriz identidade de tamanho n_r e $(\cdot)^\dagger$ representa o conjugado transposto de uma matriz. Para atingir essa capacidade é necessário transmitir sinais gaussianos complexo de média zero e potência igual, codificados de forma que sejam independentes no espaço e no tempo.

No caso de canais MIMO com SNRs mais altas, a capacidade de canal é dada por [Oggier, Belfiore e Viterbo 2007]

$$C(n_t, n_r, \text{SNR}) \sim \min(n_t, n_r) \log_2(\text{SNR}). \tag{3.4}$$

Pela Equação 3.4 vemos a efetividade do sistema MIMO, pois proporciona aproximadamente $\min(n_t, n_r)$ canais espaciais independentes, obtendo uma ordem de diversidade espacial de $n_t n_r$, possibilitando o aumento da taxa de dados.

3.2 CÓDIGOS DE BLOCO ESPAÇO-TEMPO

Como apresentado na Seção 3.1, o sistema MIMO pode ser usado como técnica de diversidade, fazendo uso de múltiplas antenas de transmissão e de recepção. E, para realizar a transmissão de múltiplas cópias, os códigos de bloco espaço-tempo (STBCs) são utilizados para codificar os símbolos antes de serem transmitidos. Esse tipo de codificação permite que o receptor obtenha o máximo de informação possível dos símbolos recebidos.

Os STBCs têm essa nomenclatura pois, para códigos de sistemas MIMO, o espaço e o tempo são realmente codificados, já que várias antenas (devidamente espaçadas) são utilizadas, e os dados são transmitidos em intervalos de tempo diferentes. Em 1998, Siavash M. Alamouti publicava seu artigo "*A Simple Transmit Diversity Technique for Wireless Communications*" [Alamouti 1998], dando origem aos Códigos de Bloco Espaço-Tempo. Os STBCs são uma generalização do esquema de Alamouti para uma quantidade arbitrária de antenas e podem atingir a diversidade máxima para um determinado número de antenas de transmissão e recepção. Neste trabalho estamos interessados em construções algébricas de STBCs que serão apresentadas no Capítulo 4, porém a seguir apresentamos estes códigos de modo geral.

3.2.1 Código de Alamouti

O código de Alamouti é o mais simples e famoso código de bloco espaço-tempo. Este esquema proporciona diversidade máxima de transmissão para sistemas de duas antenas transmissoras e uma receptora, sem a necessidade de obter informação do estado de canal (ou seja, não é necessário saber os coeficientes de canal) no transmissor. O esquema proposto por Alamouti proporciona um aumento na capacidade de sistemas de comunicação sem fio, pois diminui o efeito do desvanecimento causado pelos múltiplos percursos fazendo uso de múltiplas antenas no lado do transmissor. Além disso, o código de Alamouti possui baixa complexidade computacional.

Na Figura 5 é apresentado o esquema para duas antenas transmissoras e uma receptora. É possível observar a codificação e transmissão dos símbolos de informação modulados, o esquema de combinação no receptor e a detecção por máxima verossimilhança.

No processo de codificação e transmissão, os símbolos

$$\mathbf{X} = \begin{bmatrix} \boldsymbol{x}_0 & \boldsymbol{x}_1 \\ -\bar{\boldsymbol{x}}_1 & \bar{\boldsymbol{x}}_0 \end{bmatrix}, \tag{3.5}$$

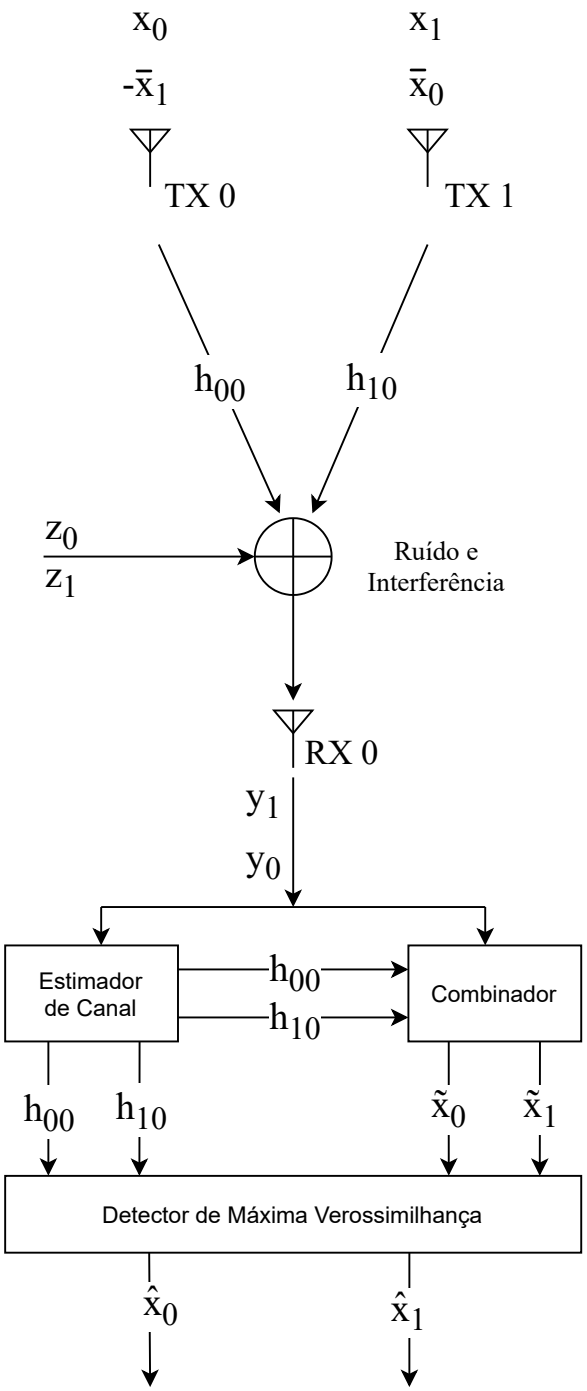
são enviados. Em um determinado instante (t), $\boldsymbol{x_0}$ é transmitido pela antena TX 0 e $\boldsymbol{x_1}$ pela antena TX 1, simultaneamente. No instante seguinte ($t + T$), a antena TX 0 transmite o símbolo $-\bar{\boldsymbol{x}}_1$ e a antena TX 1 transmite o símbolo $\bar{\boldsymbol{x}}_0$, também de forma simultânea.

A Tabela 1 exemplifica o processo de codificação e transmissão do esquema.

Tabela 1 – Sequência de codificação e transmissão do esquema de Alamouti para 2 antenas de transmissão.

	Antena TX 0	Antena TX 1
Tempo t	$\boldsymbol{x_0}$	$\boldsymbol{x_1}$
Tempo $t + T$	$-\bar{\boldsymbol{x}}_1$	$\bar{\boldsymbol{x}}_0$

Figura 5 – Esquema de Alamouti para sistema com uma antena receptora.



Fonte: Próprio autor.

Como apresentado na Seção 3.1, esses sinais passam pelo canal de desvanecimento do tipo Rayleigh, com coeficientes de canal $\mathbf{H} = \begin{bmatrix} \boldsymbol{h_{00}} \\ \boldsymbol{h_{10}} \end{bmatrix}$, sendo $\boldsymbol{h_{00}}$ e $\boldsymbol{h_{10}}$ modelados como uma variável aleatória complexa de média zero e variância unitária. Assumindo que o canal é constante dentro de cada

período de transmissão, os coeficientes podem ser escritos como

$$\begin{aligned} \boldsymbol{h_{00}}(t) &= \boldsymbol{h_{00}}(t+T) = \boldsymbol{h_{00}} = \mu_0 e^{j\theta_0} \\ \boldsymbol{h_{10}}(t) &= \boldsymbol{h_{10}}(t+T) = \boldsymbol{h_{10}} = \mu_1 e^{j\theta_1}, \end{aligned} \tag{3.6}$$

em que $\boldsymbol{h_{00}}$ e $\boldsymbol{h_{10}}$ podem ser modelados por uma distorção multiplicativa complexa composta por μ_0 e μ_1, que são as amplitudes e, θ_0 e θ_1 que são as fases dos canais.

Os sinais transmitidos sofrem os efeitos do ruído gaussiano branco aditivo (AWGN) $\mathbf{Z} = \begin{bmatrix} \boldsymbol{z_0} \\ \boldsymbol{z_1} \end{bmatrix}$, e assim, como na Equação 3.1 que modela o canal MIMO, os sinais recebidos, na forma matricial, é dado por

$$\mathbf{Y} = \begin{bmatrix} \boldsymbol{y_0} \\ \boldsymbol{y_1} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}_0 & \boldsymbol{x}_1 \\ -\bar{\boldsymbol{x}}_1 & \bar{\boldsymbol{x}}_0 \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{h_{00}} \\ \boldsymbol{h_{10}} \end{bmatrix} + \begin{bmatrix} \boldsymbol{z_0} \\ \boldsymbol{z_1} \end{bmatrix}. \tag{3.7}$$

Os símbolos, $\boldsymbol{y_0}$ é recebido no tempo t e $\boldsymbol{y_1}$ no tempo $t+T$, podem ser dados também por

$$\begin{aligned} \boldsymbol{y_0}(t) = \boldsymbol{y}(t) &= \boldsymbol{h_{00}}\boldsymbol{x_0} + \boldsymbol{h_{10}}\boldsymbol{x_1} + \boldsymbol{z_0} \\ \boldsymbol{y_1}(t) = \boldsymbol{y}(t+T) &= -\boldsymbol{h_{00}}\bar{\boldsymbol{x}}_1 + \boldsymbol{h_{10}}\bar{\boldsymbol{x}}_0 + \boldsymbol{z_1}, \end{aligned} \tag{3.8}$$

em que T é o período de símbolo. Após isso, os sinais recebidos alimentam o estimador de canal e o combinador, obtendo-se

$$\begin{aligned} \tilde{\boldsymbol{x_0}} &= \bar{\boldsymbol{h}}_{\boldsymbol{00}}\boldsymbol{y_0} + \boldsymbol{h_{10}}\bar{\boldsymbol{y}}_1 \\ \tilde{\boldsymbol{x_1}} &= \bar{\boldsymbol{h}}_{\boldsymbol{10}}\boldsymbol{y_0} - \boldsymbol{h_{00}}\bar{\boldsymbol{y}}_1. \end{aligned} \tag{3.9}$$

Substituindo as Equações 3.6 e 3.8 em 3.9, temos

$$\begin{aligned} \tilde{\boldsymbol{x_0}} &= \mu_0 e^{-j\theta_0}(\mu_0 e^{j\theta_0}\boldsymbol{x}_0 + \mu_1 e^{j\theta_1}\boldsymbol{x}_1 + \boldsymbol{z_0}) + \mu_1 e^{j\theta_1}(-\mu_0 e^{-j\theta_0}\boldsymbol{x}_1 + \mu_1 e^{-j\theta_1}\boldsymbol{x}_0 + \bar{\boldsymbol{z}}_1) \\ \tilde{\boldsymbol{x_1}} &= \mu_1 e^{-j\theta_1}(\mu_0 e^{j\theta_0}\boldsymbol{x}_0 + \mu_1 e^{j\theta_1}\boldsymbol{x}_1 + \boldsymbol{z}_0) - \mu_0 e^{j\theta_0}(-\mu_0 e^{-j\theta_0}\boldsymbol{x}_1 + \mu_1 e^{-j\theta_1}\boldsymbol{x}_0 + \bar{\boldsymbol{z}}_1) \end{aligned}, \tag{3.10}$$

multiplicando, temos

$$\begin{aligned} \tilde{\boldsymbol{x_0}} &= \mu_0^2\boldsymbol{x}_0 + \mu_0 e^{-j\theta_0}\mu_1 e^{j\theta_1}\boldsymbol{x}_1 + \mu_0 e^{-j\theta_0}\boldsymbol{z_0} - \mu_0 e^{-j\theta_0}\mu_1 e^{j\theta_1}\boldsymbol{x}_1 + \mu_1^2\boldsymbol{x}_0 + \mu_1 e^{j\theta_1}\bar{\boldsymbol{z}}_1 \\ \tilde{\boldsymbol{x_1}} &= \mu_0 e^{j\theta_0}\mu_1 e^{-j\theta_1}\boldsymbol{x}_0 + \mu_1^2\boldsymbol{x}_1 + \mu_1 e^{-j\theta_1}\boldsymbol{z_0} + \mu_0^2\boldsymbol{x}_1 - \mu_0 e^{j\theta_0}\mu_1 e^{-j\theta_1}\boldsymbol{x}_0 - \mu_0 e^{j\theta_0}\bar{\boldsymbol{z}}_1 \end{aligned}. \tag{3.11}$$

Dessa forma, obtemos

$$\begin{aligned} \tilde{\boldsymbol{x_0}} &= (\mu_0^2 + \mu_1^2)\boldsymbol{x}_0 + \bar{\boldsymbol{h}}_{\boldsymbol{00}}\boldsymbol{z_0} + \boldsymbol{h_{10}}\bar{\boldsymbol{z}}_1 \\ \tilde{\boldsymbol{x_1}} &= (\mu_0^2 + \mu_1^2)\boldsymbol{x}_1 - \boldsymbol{h_{00}}\bar{\boldsymbol{z}}_1 + \bar{\boldsymbol{h}}_{\boldsymbol{10}}\boldsymbol{z}_0 \end{aligned}, \tag{3.12}$$

e os sinais $\tilde{\boldsymbol{x_0}}$ e $\tilde{\boldsymbol{x_1}}$ são enviados para um detector de máxima verossimilhança.

Na Equação 3.12, é possível observar como os símbolos $\boldsymbol{x}_0$ e $\boldsymbol{x}_1$ são multiplicados por $(\mu_0^2 + \mu_1^2)$, que são os módulos dos ganhos dos canais, sendo μ_0 e μ_1 números reais e positivos. Isso mostra que o esquema proposto por Alamouti explora os efeitos de multi-percussos, obtendo ganhos, por meio da técnica de diversidade. Vemos também que o símbolo $\boldsymbol{x}_1$ não faz parte do sinal $\tilde{\boldsymbol{x_0}}$ assim como $\boldsymbol{x}_0$

não faz parte de $\tilde{x_1}$, ou seja, não há interferência entre antenas. Isso significa que os sinais podem ser decodificados de forma independente.

Para o caso de duas antenas de transmissão e n_r de recepção, o esquema de Alamouti proporciona uma ordem de diversidade de $2n_r$. Esquemas $2 \times n_r$ são utilizados em sistemas onde múltiplas antenas receptoras são praticáveis pois assim proporcionam uma ordem de diversidade mais alta. Vamos abordar o caso do esquema de duas antenas transmissoras e duas antenas receptoras que possui ordem de diversidade 4, que é o foco do estudo desse trabalho.

A Figura 6 mostra o esquema de Alamouti de duas antenas de transmissão e duas antenas de recepção. As etapas de codificação e de transmissão dos símbolos de informação são iguais às do esquema 2×1 apresentado anteriormente na Figura 5 e exemplificado na Tabela 1.

Neste esquema, temos quatro coeficientes de canais diferentes $\mathbf{H} = \begin{bmatrix} \boldsymbol{h_{00}} & \boldsymbol{h_{01}} \\ \boldsymbol{h_{10}} & \boldsymbol{h_{11}} \end{bmatrix}$, ou seja, quatro caminhos diferentes para a transmissão dos sinais de informação. A Tabela 2 define tais coeficientes entre as antenas transmissoras e receptoras.

Tabela 2 – Coeficientes de canais entre as antenas transmissoras e receptoras do esquema de Alamouti 2×2.

	Antena RX 0	Antena RX 1
Antena TX 0	$\boldsymbol{h_{00}}$	$\boldsymbol{h_{01}}$
Antena TX 1	$\boldsymbol{h_{10}}$	$\boldsymbol{h_{11}}$

Os sinais recebidos em cada antena são organizados conforme Tabela 3.

Tabela 3 – Coeficientes de canais entre as antenas transmissoras e receptoras do esquema de Alamouti 2×2.

	Antena RX 0	Antena RX 1
Tempo t	$\boldsymbol{y_0}$	$\boldsymbol{y_2}$
Tempo $t + T$	$\boldsymbol{y_1}$	$\boldsymbol{y_3}$

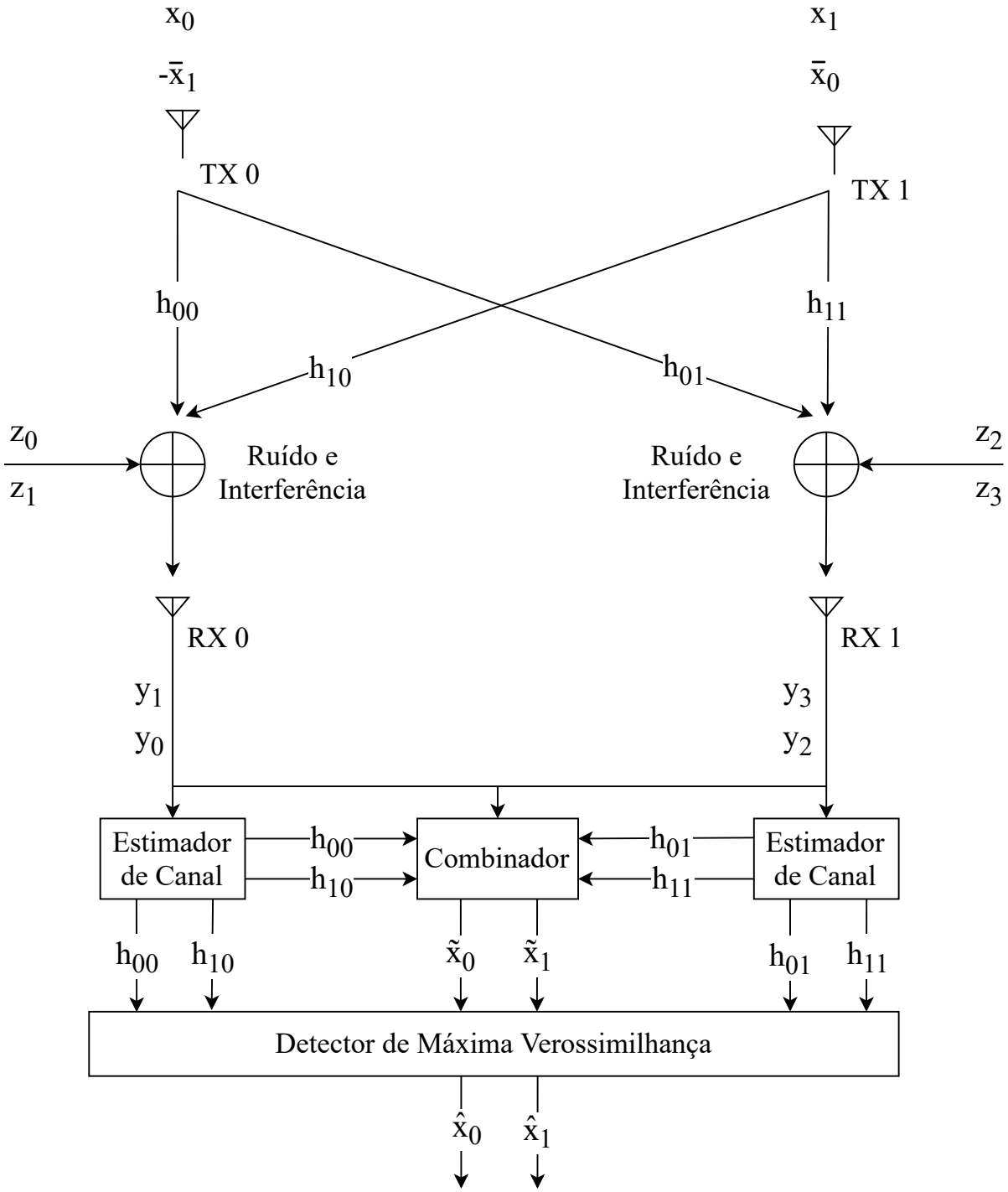
Similarmente ao caso anterior, os sinais transmitidos sofrem os efeitos do ruído gaussiano branco aditivo $\mathbf{Z} = \begin{bmatrix} \boldsymbol{z_0} & \boldsymbol{z_2} \\ \boldsymbol{z_1} & \boldsymbol{z_3} \end{bmatrix}$. Assim, os sinais recebidos podem ser expressados por

$$\mathbf{Y} = \begin{bmatrix} \boldsymbol{y_0} & \boldsymbol{y_2} \\ \boldsymbol{y_1} & \boldsymbol{y_3} \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}_0 & \boldsymbol{x}_1 \\ -\bar{\boldsymbol{x}}_1 & \bar{\boldsymbol{x}}_0 \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{h_{00}} & \boldsymbol{h_{01}} \\ \boldsymbol{h_{10}} & \boldsymbol{h_{11}} \end{bmatrix} + \begin{bmatrix} \boldsymbol{z_0} & \boldsymbol{z_2} \\ \boldsymbol{z_1} & \boldsymbol{z_3} \end{bmatrix}. \tag{3.13}$$

Realizando os cálculos das matrizes, obtemos

$$\begin{aligned} \boldsymbol{y_0} &= \boldsymbol{h_{00}}\boldsymbol{x_0} + \boldsymbol{h_{10}}\boldsymbol{x_1} + \boldsymbol{z_0} \\ \boldsymbol{y_1} &= -\boldsymbol{h_{00}}\bar{\boldsymbol{x}}_1 + \boldsymbol{h_{10}}\bar{\boldsymbol{x}}_0 + \boldsymbol{z_1} \\ \boldsymbol{y_2} &= \boldsymbol{h_{01}}\boldsymbol{x_0} + \boldsymbol{h_{11}}\boldsymbol{x_1} + \boldsymbol{z_2} \\ \boldsymbol{y_3} &= -\boldsymbol{h_{01}}\bar{\boldsymbol{x}}_1 + \boldsymbol{h_{11}}\bar{\boldsymbol{x}}_0 + \boldsymbol{z_3}. \end{aligned} \tag{3.14}$$

Figura 6 – Esquema de Alamouti para sistema com duas antenas receptoras.



Fonte: Próprio autor.

Estes sinais passam pelo estimador de canal e pelo combinador para que então possam ser enviados para o detector de ML, obtendo-se

$$\begin{aligned} \tilde{\boldsymbol{x}_0} &= \bar{\boldsymbol{h}}_{\boldsymbol{00}}\boldsymbol{y_0} + \boldsymbol{h_{10}}\bar{\boldsymbol{y}}_1 + \bar{\boldsymbol{h}}_{\boldsymbol{01}}\boldsymbol{y_2} + \boldsymbol{h_{11}}\bar{\boldsymbol{y}}_3 \\ \tilde{\boldsymbol{x}_1} &= \bar{\boldsymbol{h}}_{\boldsymbol{10}}\boldsymbol{y_0} - \boldsymbol{h_{00}}\bar{\boldsymbol{y}}_1 + \bar{\boldsymbol{h}}_{\boldsymbol{11}}\boldsymbol{y_2} - \boldsymbol{h_{01}}\bar{\boldsymbol{y}}_3. \end{aligned} \tag{3.15}$$

Substituindo os coeficientes de canais da Tabela 2 e as Equações 3.14 em (3.15), temos

$$\begin{array}{c}\tilde{\boldsymbol{x}_0} = \mu_0 e^{-j\theta_0}(\mu_0 e^{j\theta_0}\boldsymbol{x}_0 + \mu_1 e^{j\theta_1}\boldsymbol{x}_1 + \boldsymbol{z}_0) + \mu_1 e^{j\theta_1}(-\mu_0 e^{-j\theta_0}\boldsymbol{x}_1 + \mu_1 e^{-j\theta_1}\boldsymbol{x}_0 + \bar{\boldsymbol{z}}_1) + \\ \mu_2 e^{-j\theta_2}(\mu_2 e^{j\theta_2}\boldsymbol{x}_0 + \mu_3 e^{j\theta_3}\boldsymbol{x}_1 + \boldsymbol{z}_2) + \mu_3 e^{j\theta_3}(-\mu_2 e^{-j\theta_2}\boldsymbol{x}_1 + \mu_3 e^{-j\theta_3}\boldsymbol{x}_0 + \bar{\boldsymbol{z}}_3) \\ \tilde{\boldsymbol{x}_1} = \mu_1 e^{-j\theta_1}(\mu_0 e^{j\theta_0}\boldsymbol{x}_0 + \mu_1 e^{j\theta_1}\boldsymbol{x}_1 + \boldsymbol{z}_0) - \mu_0 e^{j\theta_0}(-\mu_0 e^{-j\theta_0}\boldsymbol{x}_1 + \mu_1 e^{-j\theta_1}\boldsymbol{x}_0 + \bar{\boldsymbol{z}}_1) + \\ \mu_3 e^{-j\theta_3}(\mu_2 e^{j\theta_2}\boldsymbol{x}_0 + \mu_3 e^{j\theta_3}\boldsymbol{x}_1 + \boldsymbol{z}_2) - \mu_2 e^{j\theta_2}(-\mu_2 e^{-j\theta_2}\boldsymbol{x}_1 + \mu_3 e^{-j\theta_3}\boldsymbol{x}_0 + \bar{\boldsymbol{z}}_3)\end{array}, \tag{3.16}$$

multiplicando, temos

$$\begin{array}{c}\tilde{\boldsymbol{x}_0} = \mu_0^2\boldsymbol{x}_0 + \mu_0 e^{-j\theta_0}\mu_1 e^{j\theta_1}\boldsymbol{x}_1 + \mu_0 e^{-j\theta_0}\boldsymbol{z}_0 - \mu_0 e^{-j\theta_0}\mu_1 e^{j\theta_1}\boldsymbol{x}_1 + \mu_1^2\boldsymbol{x}_0 + \mu_1 e^{j\theta_1}\bar{\boldsymbol{z}}_1 + \mu_2^2\boldsymbol{x}_0 + \\ \mu_2 e^{-j\theta_2}\mu_3 e^{j\theta_3}\boldsymbol{x}_1 + \mu_2 e^{-j\theta_2}\boldsymbol{z}_2 - \mu_2 e^{-j\theta_2}\mu_3 e^{j\theta_3}\boldsymbol{x}_1 + \mu_3^2\boldsymbol{x}_0 + \mu_3 e^{j\theta_3}\bar{\boldsymbol{z}}_3 \\ \tilde{\boldsymbol{x}_1} = \mu_0 e^{j\theta_0}\mu_1 e^{-j\theta_1}\boldsymbol{x}_0 + \mu_1^2\boldsymbol{x}_1 + \mu_1 e^{-j\theta_1}\boldsymbol{z}_0 + \mu_0^2\boldsymbol{x}_1 - \mu_0 e^{j\theta_0}\mu_1 e^{-j\theta_1}\boldsymbol{x}_0 - \mu_0 e^{j\theta_0}\bar{\boldsymbol{z}}_1 + \mu_3^2\boldsymbol{x}_1 + \\ \mu_2 e^{j\theta_2}\mu_3 e^{-j\theta_3}\boldsymbol{x}_0 + \mu_3 e^{-j\theta_3}\boldsymbol{z}_2 + \mu_2^2\boldsymbol{x}_1 - \mu_2 e^{j\theta_2}\mu_3 e^{-j\theta_3}\boldsymbol{x}_0 - \mu_2 e^{j\theta_2}\bar{\boldsymbol{z}}_3\end{array}. \tag{3.17}$$

Dessa forma, obtemos

$$\begin{array}{c}\tilde{\boldsymbol{x}_0} = (\mu_0^2 + \mu_1^2 + \mu_2^2 + \mu_3^2)\boldsymbol{x}_0 + \bar{\boldsymbol{h}}_{\mathbf{00}}\boldsymbol{z}_{\mathbf{0}} + \boldsymbol{h}_{\mathbf{10}}\bar{\boldsymbol{z}}_1 + \bar{\boldsymbol{h}}_{\mathbf{01}}\boldsymbol{z}_{\mathbf{2}} + \boldsymbol{h}_{\mathbf{11}}\bar{\boldsymbol{z}}_3 \\ \tilde{\boldsymbol{x}_1} = (\mu_0^2 + \mu_1^2 + \mu_2^2 + \mu_3^2)\boldsymbol{x}_1 - \boldsymbol{h}_{\mathbf{00}}\bar{\boldsymbol{z}}_1 + \bar{\boldsymbol{h}}_{\mathbf{10}}\boldsymbol{z}_0 - \boldsymbol{h}_{\mathbf{01}}\bar{\boldsymbol{z}}_3 + \bar{\boldsymbol{h}}_{\mathbf{11}}\boldsymbol{z}_2.\end{array} \tag{3.18}$$

Observando as construções matemáticas das equações acima, vemos que os sinais combinados de duas antenas receptoras ($\tilde{\boldsymbol{x}_0}$ e $\tilde{\boldsymbol{x}_1}$) são a soma dos sinais combinados de cada antena de recepção ($\boldsymbol{y_0}$, $\boldsymbol{y_1}$, $\boldsymbol{y_2}$ e $\boldsymbol{y_3}$), o que acontece também no caso de apenas uma antena receptora. Isso mostra que o esquema de combinação utilizado em ambos os casos, de uma antena receptora e de duas antenas receptoras, é igual.

Como já dito anteriormente, os STBCs são uma generalização do esquema de Alamouti. Em [Tarokh, Jafarkhani e Calderbank 1999], foi introduzido o termo STBC construídos a partir de *designs* ortogonais.

Definição 3.2.1 *Um STBC é um conjunto finito $\mathcal{C}$ de matrizes complexas $\mathbf{X}$ de tamanho $n_t \times T$. Em que cada linha representa a quantidade de antenas transmissoras e cada coluna representa um intervalo de tempo.*

3.3 CRITÉRIOS DE ANÁLISE

Nesta seção iremos apresentar os critérios de análise de um STBC, assumindo um canal de desvanecimento Rayleigh quase-estático e plano, isto é, o canal permanece constante dentro de cada período de transmissão, variando independentemente de um período para o próximo. E assumindo que o receptor seja coerente, isto é, que o mesmo tenha o conhecimento exato sobre o estado do canal ou um CSI (*Channel State Information*) perfeito.

A probabilidade de erro $P(e)$ pode ser estimada utilizando a união limitada, que mostra que a probabilidade de $P(e)$ ocorrer é menor que a soma das probabilidades de erros aos pares

$$P(e) \leq \frac{1}{|\mathcal{C}|}\sum_{\mathbf{X}\in\mathcal{C}}\sum_{\hat{\mathbf{X}}\neq\mathbf{X}} P(\mathbf{X} \to \hat{\mathbf{X}}), \tag{3.19}$$

no qual $P(\mathbf{X} \rightarrow \hat{\mathbf{X}})$ é a probabilidade de erro aos pares, ou seja, a probabilidade do receptor ML decidir erroneamente por uma palavra-código $\hat{\mathbf{X}}$, quando na verdade foi transmitido $\mathbf{X}$.

Após algumas manipulações algébricas, que podem ser encontradas em [Oggier, Belfiore e Viterbo 2007], é possível obter a seguinte expressão para SNRs altas

$$P(\mathbf{X} \rightarrow \hat{\mathbf{X}}) \leq \Delta^{-n_r} \left(\frac{1}{4N_0} \right)^{-rn_r}, \tag{3.20}$$

no qual $\Delta = \prod_{j=1}^{r} \lambda_j$, r denota o posto da matriz de diferença da palavra-código e λ_j são os autovalores não-nulos da matriz de distância da palavra-código

$$\mathbf{A} = (\mathbf{X} - \hat{\mathbf{X}})(\mathbf{X} - \hat{\mathbf{X}})^{\dagger}. \tag{3.21}$$

Chamamos um código de **posto máximo**, se $r = n_t$. E, para este tipo de código temos que

$$\Delta = \prod_{j=1}^{n_t} \lambda_j = \det(\mathbf{A}) \neq 0 \text{ , para todo } \mathbf{A}, \tag{3.22}$$

o que nos permite dizer que este código tem diversidade máxima, possibilitando explorar a independência dos $n_t n_r$ canais do sistema MIMO.

Definição 3.3.1 *O **ganho de diversidade** de um código é dado por*

$$div = \min\{rn_r\}. \tag{3.23}$$

Definição 3.3.2 *Para códigos de diversidade máxima, podemos definir o **determinante mínimo** do código como,*

$$\Delta_{\min} = \min_{\boldsymbol{X} \neq \hat{\boldsymbol{X}}} \det(\boldsymbol{A}). \tag{3.24}$$

*Em que $(\Delta_{\min})^{1/n_t}$ é chamado de **ganho de codificação**.*

Definição 3.3.3 *Um STBC linear é definido como STBC $\mathcal{C}$ que, para todo **X** e **X'** pertencente ao código $\mathcal{C}$, **X** $\pm$ **X'** pertence a $\mathcal{C}$, ou seja, a soma ou diferença de qualquer par de palavras-código é uma palavra-código.*

Por conta da definição de código linear, a expressão do limite de união pode ser reduzido para

$$P(e) \leq \frac{1}{|\mathcal{C}|} \sum_{\hat{\mathbf{X}} \neq \mathbf{0}} P(\mathbf{0} \rightarrow \mathbf{X}), \tag{3.25}$$

e assim temos

$$\Delta_{\min} = \min_{\mathbf{X} \neq 0_{n_t \times T}} \det(\mathbf{X}\mathbf{X}^{\dagger}). \tag{3.26}$$

A fim de aumentar a confiabilidade, o objetivo é obter códigos lineares de diversidade máxima com determinante mínimo grande.

Para o esquema de modulação M-QAM, em que $M = 2^m$ para um número inteiro positivo m. Vamos considerar que os m bits de informação são mapeados utilizando o código de Gray. Seja k o número de símbolos de informação QAM codificados, a eficiência espectral do sistema MIMO é $\eta_s = k/T$ símbolos por uso de canal (spcu) ou $\eta = km/T$ bits por uso de canal (bpcu).

Definição 3.3.4 *Chamamos um código de* ***taxa máxima****, se* $k = n_r T$.

Para códigos de taxa máxima, temos que a eficiência espectral é $\eta_s = n$ spcu ou $\eta = nm$ bpcu, sendo $n = n_t = n_r = T$.

As palavras-código são pontos que formam a constelação. A performance de uma constelação está relacionada com sua região delimitadora, assim, as palavras-código devem ser empacotadas de forma eficiente. Para otimizar a eficiência energética dos códigos, introduzimos uma restrição de modelagem, *shaping*, na constelação de sinais. Para realizar um *shaping* no formato da constelação, é necessário que uma matriz M unitária seja aplicada em um vetor de valores discretos contendo símbolos de informação QAM, gerando assim uma rotação na constelação. De modo a otimizar a eficiência energética, esta matriz M pode ser interpretada como pontos geradores de um reticulado, como definido em (2.4.2). Sendo que para símbolos QAM, obtemos o reticulado $\mathbb{Z}^n$ cúbico e portanto, o formato da constelação é chamado de *shaping* cúbico. Na Seção 4.3 iremos mostrar como obter o formato de *shaping* cúbico utilizando álgebras cíclicas de divisão.

Outra característica importante requerida é a de que $\Delta_{\min} \neq 0$, ou seja, a propriedade de determinante diferente de zero (*Non-Vanishing Determinant* - NVD). Dessa forma o aumento no tamanho constelação não diminui $\Delta_{\min}$, pois quando o determinante mínimo é igual a zero, o ganho geral é reduzido extremamente. Para atingir o *trade-off* de diversidade-multiplexação, é necessário que a propriedade de NVD seja satisfeita.

Resumindo, os critérios de *design* para STBCs que estamos procurando são:

- Código de bloco espaço-tempo linear com $n_t = n_r = T$.
- Diversidade máxima e determinante mínimo grande, para aumentar a confiabilidade.
- Taxa máxima, para maximar a eficiência espectral.
- Constelação cúbica, para economizar energia média transmitida.
- E determinante diferente de zero, para atingir um *trade-off* de diversidade-multiplexação.

Nesse trabalho estamos interessados em códigos STBC com duas antenas transmissoras e duas antenas receptoras, ou seja, $n_t = n_r = T = 2$. Vamos considerar construções via álgebras cíclicas de divisão que garantem códigos com diversidade máxima, taxa máxima e determinante diferente de zero. Além disso, sob certas condições temos também a propriedade de constelação cúbica e um limitante inferior diferente de zero para o determinante mínimo.

4 STBC PARA MIMO 2×2 VIA ÁLGEBRAS CÍCLICAS DE DIVISÃO

Neste capítulo, iremos apresentar na Seção 4.1 a construção do código de Alamouti 2×2 via a álgebra dos quatérnios de Hamilton $\mathbb{H}$ e depois, como uma generalização deste caso, apresentamos a construção mais geral de um STBC 2×2 a partir de álgebra de divisão cíclica sobre corpos de números. Na Seção 4.3, as condições para que códigos de bloco espaço-tempo sejam considerados perfeitos são apresentadas, para então na Subseção 4.3.1 apresentarmos a construção e propriedades do código de Ouro que é um exemplo de STBC 2×2 perfeito e foco deste trabalho. As principais referências utilizadas neste capítulo foram [Alamouti 1998, BELFIORE J.-C.; Rekaya e Viterbo 2005, Oggier, Belfiore e Viterbo 2007, Tarokh, Jafarkhani e Calderbank 1999, Oggier et al. 2006].

4.1 CÓDIGO DE ALAMOUTI VIA ÁLGEBRA DOS QUATÉRNIOS DE HAMILTON

Seja $\mathbb{H} = (-1,-1)_{\mathbb{R}}$ a álgebra dos quatérnios de Hamilton definida em (2.3.6) e seja $q = x_0 + x_1 i + x_2 j + x_3 k$ um elemento de $\mathbb{H}$, onde $i^2 = -1,\ j^2 = -1$ e $k = ij$. Podemos escrever q da seguinte forma

$$\begin{aligned} q &= (x_0 + x_1 i) + (x_2 j + x_3 ij) \\ &= (x_0 + x_1 i) + (x_2 j - x_3 ji) \\ &= (x_0 + x_1 i) + j(x_2 - x_3 i) \\ &= \alpha_q + j\beta_q, \end{aligned} \tag{4.1}$$

onde $\alpha_q = x_0 + x_1 i \in \mathbb{C}$ e $\beta_q = x_2 - x_3 i \in \mathbb{C}$. Portanto, $\mathcal{A}$ é um espaço vetorial à direita sobre $\mathbb{C}$, o que significa que escalares se multiplicam à direita, com base $\{1, j\}$ em $\mathbb{C}$ e $q = (\alpha_q, \beta_q)$.

O homomorfismo $\varphi : \mathbb{H} \to M_{\mathbb{C}}(2)$ relaciona um elemento q da álgebra dos quatérnios de Hamilton $\mathbb{H}$ com uma matriz 2×2 com coeficientes em $\mathbb{C}$. Considerando $M_{\mathbb{C}}(2)$ o espaço vetorial das matrizes 2×2 com coeficientes em $\mathbb{C}$ e com base

$$\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \varphi(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \varphi(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \varphi(k) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \tag{4.2}$$

temos que

$$\begin{array}{rccl} \varphi: & \mathbb{H} & \to & M_{\mathbb{C}}(2) \\ & q & \mapsto & \varphi(x_0 + x_1 i + x_2 j + x_3 k) = x_0\varphi(1) + x_1\varphi(i) + x_2\varphi(j) + x_3\varphi(k) \end{array}. \tag{4.3}$$

E assim,

$$x_0\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+x_1\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}+x_2\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}+x_3\begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix}=\begin{pmatrix}x_0+x_1i & -(x_2+x_3i)\\ x_2-x_3i & x_0-x_1i\end{pmatrix}. \quad (4.4)$$

Como $\alpha_q = x_0 + x_1$ e $\beta_q = x_2 - x_3 i$, obtemos a seguinte matriz

$$\begin{pmatrix}\alpha_q & -\bar{\beta}_q\\ \beta_q & \bar{\alpha}_q\end{pmatrix}. \quad (4.5)$$

Dessa forma, o conjunto destas matrizes forma um código STBC 2×2

$$\mathcal{C}=\left\{\mathbf{X}=\begin{pmatrix}\alpha & -\bar{\beta}\\ \beta & \bar{\alpha}\end{pmatrix} \mid \alpha,\beta\in\mathbb{C}\right\}, \quad (4.6)$$

em que estas matrizes correspondem as palavras-código do Código de Alamouti como em (3.5). A diversidade máxima do código de Alamouti derivado da álgebra dos quatérnios de Hamilton como em (4.6) também é obtida pelo fato de $\mathbb{H}$ ser uma álgebra de divisão. Ou seja, se $q = \alpha + j\beta \in \mathbb{H}$ então

$$\mathbf{X}=\begin{pmatrix}\alpha & -\bar{\beta}\\ \beta & \bar{\alpha}\end{pmatrix}\in C, \quad (4.7)$$

é uma palavra-código. Assim,

$$\det(\mathbf{X}) = |\alpha|^2 + |\beta|^2 = x_0^2 + x_1^2 + x_2^2 + x_3^2 = Nrd(q) \neq 0, \quad (4.8)$$

pois pelo Teorema 2.3.2, $Nrd(q) = 0$ se, e somente se, $q = 0$.

4.2 STBC 2×2 VIA ÁLGEBRA DE DIVISÃO SOBRE CORPOS DE NÚMEROS

Como apresentado na Seção 3.2, os códigos STBC são uma generalização dos códigos de Alamouti. Nas construções algébricas de códigos STBC, esta generalização segue de forma análoga. Assim como apresentamos na Seção 4.1 que o código de Alamouti pode ser derivado da álgebra dos quatérnios de Hamilton, nesta seção mostraremos que um código STBC geral para 2×2 antenas pode ser derivado de uma álgebra dos quatérnios sobre um corpo de números $\mathbb{K}$, ou analogamente por uma álgebra cíclica de divisão sobre uma extensão $\mathbb{L}/\mathbb{K}$ de grau 2. O foco deste trabalho são álgebras cíclicas de divisão tal que o grau da extensão $\mathbb{L}/\mathbb{K}$ é $n = 2$ porém de forma geral, códigos construídos a partir de álgebras cíclicas utilizando (2.4) são ditos de taxa máxima, pois transmitem n^2 sinais que codificam n^2 símbolos de informação.

Seja $\mathcal{A} = (a, b)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre um corpo de números $\mathbb{K}$ tal que $Nrd(q) \neq 0$ para todo $q \neq 0$, com $q \in \mathcal{A}$. Ou seja, $\mathcal{A}$ é um álgebra cíclica de divisão. Podemos construir códigos de bloco espaço-tempo 2×2 com diversidade máxima considerando um homomorfismo análogo ao apresentado em (4.3). Seja $M_{\mathbb{K}}(2)$ o espaço vetorial das matrizes 2×2 com coeficientes no corpo de números $\mathbb{K}$ e com base

$$\varphi(1)=\begin{pmatrix}1&0\\0&1\end{pmatrix},\varphi(i)=\begin{pmatrix}\sqrt{a}&0\\0&-\sqrt{a}\end{pmatrix},\varphi(j)=\begin{pmatrix}0&1\\b&0\end{pmatrix},\varphi(k)=\begin{pmatrix}0&\sqrt{a}\\b\sqrt{a}&0\end{pmatrix}, \tag{4.9}$$

tem-se que

$$\begin{array}{rccl}\varphi: & \mathcal{A} & \to & M_{\mathbb{K}}(2)\\ & q & \mapsto & \varphi(x_0+x_1i+x_2j+x_3k)=\begin{pmatrix}x_0+x_1\sqrt{a} & x_2+x_3\sqrt{a}\\ b(x_2-x_3\sqrt{a}) & x_0-x_1\sqrt{a}\end{pmatrix}.\end{array} \tag{4.10}$$

Logo, o conjunto das matrizes 2×2 com coeficientes em $\mathbb{K}$ forma um código STBC 2×2

$$\mathcal{C}=\left\{\mathbf{X}=\begin{pmatrix}x_0+x_1\sqrt{a} & x_2+x_3\sqrt{a}\\ b\,(x_2-x_3\sqrt{a}) & x_0-x_1\sqrt{a}\end{pmatrix};x_0,x_1,x_2,x_3\in\mathcal{O}_{\mathbb{K}}\right\}, \tag{4.11}$$

no qual b não é uma norma dos elementos de $\mathcal{O}_{\mathbb{K}}$ e $\det(\mathbf{X})\neq 0$, para todo $\mathbf{X}\neq 0$.

Usualmente para termos símbolos QAM, utilizamos corpos de números do tipo $\mathbb{K}=\mathbb{Q}(i)$ e então o anel dos inteiros sendo $\mathcal{O}_{\mathbb{K}}=\mathbb{Z}[i]$. Códigos de bloco espaço-tempo 2×2 conhecidos que utilizam essa estrutura são o código de Ouro que pode ser gerado pela álgebra dos quatérnios $\mathcal{A}=(5,i)_{\mathbb{Q}(i)}$ [BELFIORE J.-C.; Rekaya e Viterbo 2005], e o código de Prata que utiliza a álgebra $\mathcal{A}=(7,i)_{\mathbb{Q}(i)}$ [Hollanti et al. 2008]. Neste trabalho estamos interessados no código de Ouro, que será apresentado na Seção 4.3.

Exemplo 4.2.1 *Seja $\mathcal{A}=(-1,-1)_{\mathbb{K}}$ uma álgebra dos quatérnios sobre um corpo de números $\mathbb{K}=\mathbb{Q}(\sqrt{2})$. As palavras-código dos códigos de bloco espaço-tempo obtidos a partir de $\mathcal{A}=(-1,-1)_{\mathbb{K}}$ são*

$$\mathbf{X}=\begin{pmatrix}x_0+x_1i & x_2+x_3i\\ -(x_2-x_3i) & x_0-x_1i\end{pmatrix} \tag{4.12}$$

no qual $x_0,x_1,x_2,x_3\in\mathbb{K}=\mathbb{Q}(\sqrt{2})$. Observe que,

$$x_l=a_l+b_l\sqrt{2},\ \ l=0,1,2,3. \tag{4.13}$$

Então,

$$\begin{aligned}x_0+x_1i&=(a_0+b_0\sqrt{2})+(a_1+b_1\sqrt{2})i\\ &=(a_0+a_1i)+(b_0+b_1i)\sqrt{2}\\ &=y_0+y_1\sqrt{2},\end{aligned} \tag{4.14}$$

em que $y_0,y_1\in\mathbb{Q}(i)$. Da mesma forma,

$$x_2+x_3i=y_2+y_3\sqrt{2}, \tag{4.15}$$

onde $y_2,y_3\in\mathbb{Q}(i)$. Portanto, se tomarmos $x_l\in\mathbb{K}$ então $y_l\in\mathbb{Z}[i]$, para todo $l=0,1,2,3$. Assim,

temos um código de bloco espaço-tempo dado por

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} x_0 + x_1\sqrt{2} & x_2 + x_3\sqrt{2} \\ -\left(x_2 - x_3\sqrt{2}\right) & x_0 - x_1\sqrt{2} \end{pmatrix} ;\ x_0,\ x_1,\ x_2,\ x_3 \in \mathbb{Z}[i] \right\} \tag{4.16}$$

com diversidade máxima porque $\det(\mathbf{X}) \neq 0$*, para todo* $\mathbf{X} \neq 0$*.*

Agora considere uma álgebra cíclica de divisão $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$ sobre uma extensão $\mathbb{L}/\mathbb{K}$ qualquer de grau 2, σ um monomorfismo de $\mathbb{L}/\mathbb{K}$ e γ um elemento que não é uma norma de algum elemento de $\mathbb{L}$. Assim, por (2.7), as palavras-código de um STBC para sistemas MIMO de 2×2 antenas, construídas a partir de álgebras cíclicas de divisão tem a seguinte forma:

$$\mathcal{C} = \mathbf{X} = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}^t \mid x_0,\ x_1 \in \mathcal{O}_{\mathbb{L}} \right\}. \tag{4.17}$$

Exemplo 4.2.2 *Seja* $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$ *uma álgebra cíclica de divisão, onde* $\mathbb{L} = \mathbb{Q}(i, \sqrt{5})$*,* $\mathbb{K} = \mathbb{Q}(i)$ *e* $\sigma = a - b\sqrt{5}$ *como em (2.2.7). Então*

$$x_0 = a_0 + b_0\sqrt{5},\ \ x_1 = a_1 + b_1\sqrt{5},\ \ a_0, a_1, b_0, b_1 \in \mathbb{Q}(i). \tag{4.18}$$

Dessa forma, tem-se

$$\mathcal{C} = \left\{ \begin{pmatrix} a_0 + b_0\sqrt{5} & \gamma(a_1 - b_1\sqrt{5}) \\ a_1 + b_1\sqrt{5} & a_0 - b_0\sqrt{5} \end{pmatrix}^t \mid a_0, a_1, b_0, b_1 \in M\text{−QAM} \right\}. \tag{4.19}$$

onde γ *será escolhido a fim de otimizar o desempenho do código. Uma vez que símbolos QAM podem ser vistos como elementos de* $\mathbb{Q}(i)$*, eles pertencem a base do corpo* $\mathbb{K} = \mathbb{Q}(i)$*. Então* x_0 *e* x_1 *codificam dois símbolos de informação QAM,* a_0, b_0 *e* a_1, b_1*, respectivamente.*

4.3 CÓDIGOS DE BLOCO ESPAÇO-TEMPO PERFEITOS

Nesta seção iremos definir um código de bloco espaço-tempo perfeito, utilizando as teorias algébricas estudadas no Capítulo 2 em conjunto com os critérios de análise do Capítulo 3. E então vamos apresentar um tipo de STBC perfeito, o código de Ouro, sua construção e características.

Antes de apresentar o código de Ouro e suas propriedades, vamos definir o que é um Código de Bloco Espaço-Tempo STBC perfeito.

Definição 4.3.1 *Um STBC quadrado de* $n_t \times n_t$ *é dito* ***perfeito*** *se, e somente se:*

- *For um código linear de taxa máxima, que utiliza* n_t^2 *símbolos de informação modulados QAM.*
- *O determinante mínimo de um código infinito é diferente de zero, atendendo o critério de posto.*
- *Formato de constelação cúbica, assim há uma otimização na eficiência energética.*

- *Energia média uniforme transmitida por antena, ou seja, todos os símbolos codificados possuem a mesma energia média.*

Para mostrar que um STBC satisfaz as condições da Definição 4.3.1, vamos considerar $\mathbb{L} = \mathbb{Q}(\theta)$ uma extensão quadrática de $\mathbb{K} = \mathbb{Q}(i)$. Como apresentamos em (4.17), um STBC infinito $\mathcal{C}$ pode ser definido como o conjunto de matrizes da forma

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} x_0 + x_1\theta & x_2 + x_3\theta \\ \gamma(x_2 - x_3\overline{\theta}) & x_0 + x_1\overline{\theta} \end{pmatrix} ;\ x_0,\ x_1,\ x_2,\ x_3 \in \mathbb{Z}[i] \right\}, \tag{4.20}$$

onde γ é um elemento que não é uma norma em $\mathbb{L}$. Temos inicialmente que $\mathcal{C}$ é um código linear se $\mathbf{X}_1, \mathbf{X}_2 \in \mathcal{C}$ então $\mathbf{X}_1 + \mathbf{X}_2 \in \mathcal{C}$. O código finito $\mathcal{C}$ é obtido limitando os símbolos de informação $x_0, x_1, x_2, x_3 \in S$, onde assumimos que a constelação de sinal S sendo $M - QAM$, logo temos um código linear de taxa máxima. No Exemplo 4.2.2 apresentamos um código $\mathcal{C}$ desta forma tomando $\mathbb{L} = \mathbb{Q}(i, \sqrt{5})$ uma extensão quadrática de $\mathbb{K} = \mathbb{Q}(i)$.

A diversidade máxima é obtida se o código possuir a propriedade do determinante diferente de zero (NVD - *Non-Vanishing Determinant*). O determinante da diferença entre duas palavras-código é diferente de zero se

$$|\det(\mathbf{X}_i - \mathbf{X}_j)|^2 \neq 0, \quad \text{para} \quad \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}. \tag{4.21}$$

Pela linearidade, essa expressão é simplificada para $|\det(\mathbf{X})|^2 \neq 0$, para toda palavra-código $\mathbf{X} \in \mathcal{C}$ diferente de zero . Como uma álgebra cíclica de divisão herda um conjunto estruturado de matrizes invertíveis, a diversidade máxima do STBC $\mathcal{C}$ é alcançada.

Já o determinante mínimo de um STBC $\mathcal{C}$, que maximiza a vantagem de codificação, é dado por

$$\Delta_{\min}(\mathcal{C}) = \min_{0 \neq \mathbf{X} \in \mathcal{C}} |\det(\mathbf{X})|^2. \tag{4.22}$$

No determinante diferente de zero, temos um limite inferior no determinante mínimo que não depende do tamanho da constelação.

A propriedade de informação sem perdas está relacionada com o *shaping* como apresentado na Seção 3.3. Códigos lineares associados a uma matriz unitária fornecem informações sem perdas. O formato da constelação cúbica de um STBC $\mathcal{C}$ construído a partir de uma álgebra cíclica de divisão, é uma propriedade obtida aplicando uma matriz unitária em um vetor de valores discretos, podendo ser interpretada como pontos geradores em um reticulado algébrico. Como estamos utilizando símbolos QAM, obtemos o reticulado cúbico $\mathbb{Z}^n$ e portanto, a condição de *shaping* cúbico.

A seguir, iremos apresentar o exemplo de um STBC, o chamado código de Ouro, que satisfaz todas as condições acima citadas e portanto é um STBC perfeito.

4.3.1 Código de Ouro

Em [BELFIORE J.-C.; Rekaya e Viterbo 2005] os autores mostraram que o código de Ouro é um STBC 2×2 perfeito, pois é um código de taxa e diversidade máximas, tem determinante diferente de zero (*non-vanishing determinant*) e é energeticamente eficiente (*cubic shaping*), o que está de acordo

com a Definição 4.3.1. Além disso, o código de ouro considerado o melhor STBC para sistemas MIMO com duas antenas transmissoras [OUERTANI et al. 2006]. A seguir iremos apresentar uma construção do código de ouro que possui tais características utilizando uma álgebra de divisão cíclica que está relacionada com o número de ouro $\theta = \frac{1+\sqrt{5}}{2}$, por isso o nome código de Ouro.

Vamos considerar o corpo de números

$$\mathbb{L} = \mathbb{Q}(i, \sqrt{5}) = \{a + b\theta | a, b \in \mathbb{Q}(i)\}, \tag{4.23}$$

como uma extensão quadrática relativa de $\mathbb{K} = \mathbb{Q}(i)$, com polinômio minimal $p(X) = X^2 - X - 1$. As raízes deste polinômio minimal sobre $\mathbb{K} = \mathbb{Q}(i)$ são $\theta = \frac{1+\sqrt{5}}{2}$ e $\bar{\theta} = 1 - \theta = \frac{1-\sqrt{5}}{2}$. O anel de inteiros de é $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[i][\theta]$, com base integral $B_{\mathbb{L}/\mathbb{K}} = \{1, \theta\}$. Agora, vamos considerar a extensão absoluta $\mathbb{L}/\mathbb{Q}$. Neste caso, $\mathrm{L} = \{a + bi + c\theta + di\theta | a, b, c, d \in \mathbb{Q}\}$, com base integral $B_{\mathbb{L}/\mathbb{Q}} = \{1, i, \theta, i\theta\}$.

A fim de garantir que a mesma energia média seja transmitida de cada antena em cada canal de uso, é necessário escolher γ tal que $|\gamma| = 1$ e que não seja uma norma de qualquer elemento de $\mathcal{O}_{\mathbb{L}}$. Nessas condições, temos as seguintes opções $\gamma = \pm 1$ ou $\gamma = \pm i$. Escolhemos $\gamma = i$, para satisfazer a condição de determinante diferente de zero (NVD).

Assim, o código de Ouro será um STBC 2×2 construído utilizando a álgebra de divisão cíclica $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, i)$, em que $\sigma(\theta) = \bar{\theta}$, ou equivalentemente, a álgebra dos quatérnios $\mathcal{A} = (5, i)_{\mathbb{K}}$ sobre $\mathbb{K} = \mathbb{Q}(i)$.

$$\begin{array}{c} \mathcal{A} = (5, i)_{\mathbb{Q}(i)} \\ | \ 2 \\ \mathbb{L} = \mathbb{Q}(\sqrt{5}, i) \\ | \ 2 \\ \mathbb{K} = \mathbb{Q}\,(i) \\ | \ 2 \\ \mathbb{Q} \end{array}$$

Antes da análise do *shaping*, uma palavra-código do código STBC construído a partir desta álgebra tem a seguinte forma:

$$\mathbf{X} = \begin{pmatrix} x_0 + x_1\theta & x_2 + x_3\theta \\ i\,(x_2 - x_3\theta) & x_0 - x_1\theta \end{pmatrix}, \tag{4.24}$$

no qual $\theta = \frac{1+\sqrt{5}}{2}$ e $x_0, x_1, x_2, x_3 \in \mathbb{Z}[i]$. Neste momento, já temos um código linear de taxa máxima e de diversidade máxima pois $\det(\mathbf{X}) \neq 0$, para todo $\mathbf{X} \neq 0$.

Agora, vamos ver como adicionar a propriedade de *shaping* nas palavras-código construídas em (4.24). Para isso, iremos construir um reticulado complexo $\mathbf{M}\mathbb{Z}[i]^2$, em que $\mathbf{M}$ deve ser uma matriz unitária complexa para que não haja perda no formato da constelação do sinal. Equivalente a esse reticulado, é um $\mathbb{Z}^4$-reticulado rotacionado que denotaremos por Λ', ou seja, uma rotação do reticulado $\mathbf{R}\mathbb{Z}^4$, em que $\mathbf{R}$ é uma matriz ortogonal obtida de um ideal de $\mathcal{O}_{\mathbb{L}}$. Temos por (2.28) que

$$\det(\Lambda) = |N_{\mathbb{K}/\mathbb{L}}(\alpha)|^2 |d_{\mathbb{Q}(\sqrt{5})}| = 5|N_{\mathbb{K}/\mathbb{L}}(\alpha)|^2, \tag{4.25}$$

Procuramos, portanto, por um elemento $\alpha \in \mathbb{L}$ tal que $|N_{\mathbb{L}/\mathbb{K}}(\alpha)|^2 = 5$. A fim de encontrar tal elemento, olhamos para a fatoração de 5 em $\mathcal{O}_{\mathbb{L}}$

$$5\mathcal{O}_{\mathbb{L}} = (1 + i - i\theta)^2(1 - i + i\theta)^2, \tag{4.26}$$

em que $\theta = \frac{1+\sqrt{5}}{2}$. Assim, escolhemos

$$\alpha = 1 + i - i\theta. \tag{4.27}$$

Vamos verificar se de fato obtivemos o reticulado correto. Por (2.26) sua matriz geradora é dada por

$$\mathbf{M} = \begin{pmatrix} \alpha & \alpha\theta \\ \sigma(\alpha) & \sigma(\alpha\theta) \end{pmatrix} = \begin{pmatrix} 1 + i(1-\theta) & \theta - i \\ 1 + i(1-\bar{\theta}) & \bar{\theta} - i \end{pmatrix} \tag{4.28}$$

Um cálculo direto mostra que $\mathbf{M}\mathbf{M}^t = 5I_2$. Assim, $\frac{1}{\sqrt{5}}\mathbf{M}$ é uma matriz unitária, que nos fornece a propriedade de *shaping*.

A palavra-código $\mathbf{X}$ pertencente ao código de Ouro tem assim, adicionando a propriedade de *shaping*, a forma:

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(x_0 + x_1\theta) & \alpha(x_2 + x_3\theta) \\ i\sigma(\alpha)\left(x_2 - x_3\sigma(\theta)\right) & \sigma(\alpha)(x_0 - x_1\sigma(\theta)) \end{pmatrix}, \tag{4.29}$$

em que $\theta = \frac{1+\sqrt{5}}{2}$ e x_0, x_1, x_2, x_3 são símbolos QAM.

Por fim, vamos calcular o determinante e o determinante mínimo do código de Ouro. Uma vez que

$$\alpha\sigma(\alpha) = 2 + i, \tag{4.30}$$

temos

$$\begin{aligned} \det(\mathbf{X}) &= \frac{2+i}{5}[(x_0 + x_1\theta)(x_0 + x_1\sigma_2(\theta)) - i(x_2 + x_3\theta)(x_2 + x_3\sigma_2(\theta))] \\ &= \frac{1}{2-i}[x_0^2 + x_0x_1 - x_1^2 - i(x_2^2 + x_2x_3 - x_3^2)] \neq 0, \end{aligned} \tag{4.31}$$

para todo x_0, x_1, x_2, x_3 não todos nulos. Como o valor mínimo de $[x_0^2 + x_0x_1 - x_1^2 - i(x_2^2 + x_2x_3 - x_3^2)]$ é 1, segue que

$$\Delta_{\min}(\mathcal{C}) \geq \min_{0 \neq \mathbf{X} \in \mathcal{C}} |\det(\mathbf{X})|^2 = \frac{1}{5}. \tag{4.32}$$

Resumindo, o código de Ouro é um código perfeito, pois possui:

- Diversidade máxima: $n_t \cdot n_r = 2 \cdot 2 = 4$ canais independentes que podem ser explorados.
- Taxa máxima: o número de sinais transmitidos corresponde ao número de símbolos de informação a serem enviados.

- Determinante diferente de zero e determinante mínimo limitado inferiormente por $\frac{1}{5}$ independente do tamanho da constelação M-QAM.
- Formato (*shaping*) cúbico: matriz $\mathbf{M}$ complexa unitária, a fim de otimizar a eficiência energética.
- Energia média uniforme transmitida por antena: todos os símbolos codificados na matriz $\mathbf{X}$ da palavra-código têm a mesma energia média uma vez que $|i|^2 = 1$.

5 RESULTADOS E DISCUSSÃO

Neste capítulo, iremos apresentar os resultados obtidos das simulações realizadas no *software* MATLAB. A princípio, vamos realizar na Seção 5.1 as simulações do código de Alamouti para sistemas de duas antenas de transmissão e uma de recepção (2×1) e para duas antenas de transmissão e duas de recepção (2×2). Em seguida, na Seção 5.2, vamos realizar as simulações para o código de Ouro para duas antenas de transmissão e duas de recepção (2×2). O foco das simulações é analisar o desempenho de cada um dos códigos citados através da relação da taxa de erro de símbolo (*Symbol Error Rate* - SER) pela relação sinal ruído (*Signal-to-Noise Ratio* - SNR). Além disso, iremos fazer uma comparação entre os dois códigos para analisar desempenho de ambos para modulações M-QAM de ordens diferentes.

Para realizar as simulações, foi empregado o método de Monte Carlo que é baseado na seleção de número aleatórios [Jacoboni e Lugli 2011]. Nesse método, a mesma rotina de caráter aleatório é simulada por um número elevado de vezes com o objetivo de descobrir o comportamento do sistema e assim obter um resultado numérico aproximado, podemos dizer que quanto maior o número de repetições mais preciso será o resultado. As rotinas foram simuladas 10^6 vezes devido a capacidade da memória RAM do computador utilizado, no entanto, para obter curvas mais suaves com menos erros de ponto flutuante, seria necessário aumentar o número de simulações de Monte Carlo.

As rotinas do código de Alamouti e do código Ouro geram N símbolos de inteiros (de 1 até $M-1$) aleatórios uniformemente distribuídos que são modulados utilizando o esquema M-QAM, estes símbolos modulados são codificados e enviados, passando por um canal de desvanecimento Rayleigh com ruído do tipo AWGN, ambos utilizando números aleatórios normalmente distribuídos. O sinal recebido é demodulado e decodificado por um decodificador de máxima verossimilhança (ML - *Maximum Likelihood*) de força bruta.

5.1 SIMULAÇÕES DO CÓDIGO DE ALAMOUTI

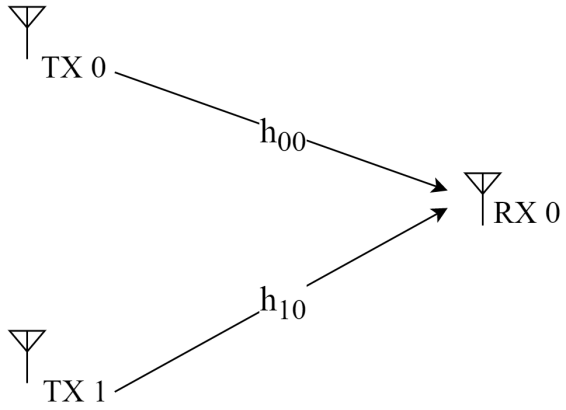
O código de Alamouti foi o código que deu origem aos STBCs. Este esquema de codificação, para um sistema 2×1, possibilita obter diversidade máxima sem penalizar a taxa de dados. Na Seção 3.2.1 o código de Alamouti 2×1 e 2×2 foi estudado com mais detalhes. E como visto na Seção 4.1, o código de Alamouti 2×2 também pode ser apresentado a partir da álgebra dos quatérnios de Hamilton $\mathbb{H}$.

Nos esquemas 2×1, os sinais são transmitidos conforme a Figura 7. A palavra-código $\mathbf{X}$, dada pela Equação 3.5, é transmitida pelo canal de desvanecimento Rayleigh quase-estático e plano. Nesse esquema temos dois canais cujos coeficientes seguem a distribuição de Rayleigh, onde tal distribuição pode ser relacionada com a distribuição gaussiana através de duas variáveis aleatórias independentes normalmente distribuídas $\mathfrak{a} \sim \mathcal{N}(0,1)$ e $\mathfrak{b} \sim \mathcal{N}(0,1)$, assim temos que a variável aleatória distribuída de Rayleigh é $\mathbf{h} = \mathfrak{a} + i\mathfrak{b}$ [Fletcher].

Ao chegar no receptor, os sinais recebidos, obtidos na Equação 3.7, passam pelo combinador e pelo estimador de canal, dessa forma obtemos os sinais dados pela Equação 3.12, que então são enviados ao

decodificador ML.

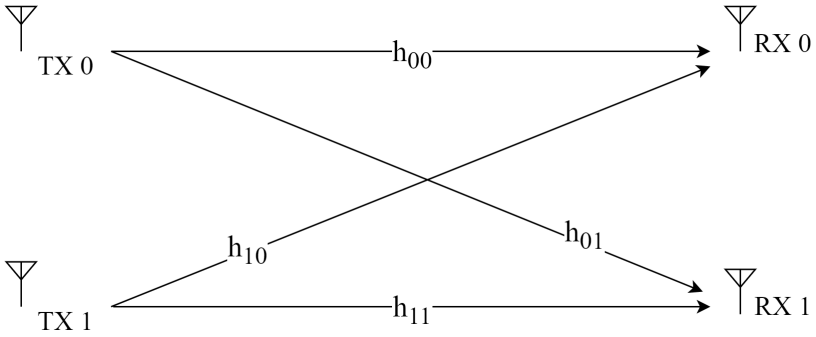
Figura 7 – Esquema de transmissão para sistema com uma antena receptora.



Fonte: Próprio autor.

O mesmo ocorre para os esquemas 2×2, como pode ser visto na Figura 8. A mesma palavra-código é transmitida, nesse caso, temos quatro canais cujos coeficientes seguem a distribuição de Rayleigh, isto é, $\mathbf{h} = \mathfrak{a} + i\mathfrak{b}$, em que $\mathfrak{a}$ e $\mathfrak{b}$ são variáveis aleatórias gaussianas de média zero e variância unitária. Os sinais recebidos, conforme Equação 3.13, passam também pelo combinador e pelo estimador de canal, e assim obtemos os sinais da Equação 3.18 que são enviados para o decodificador ML.

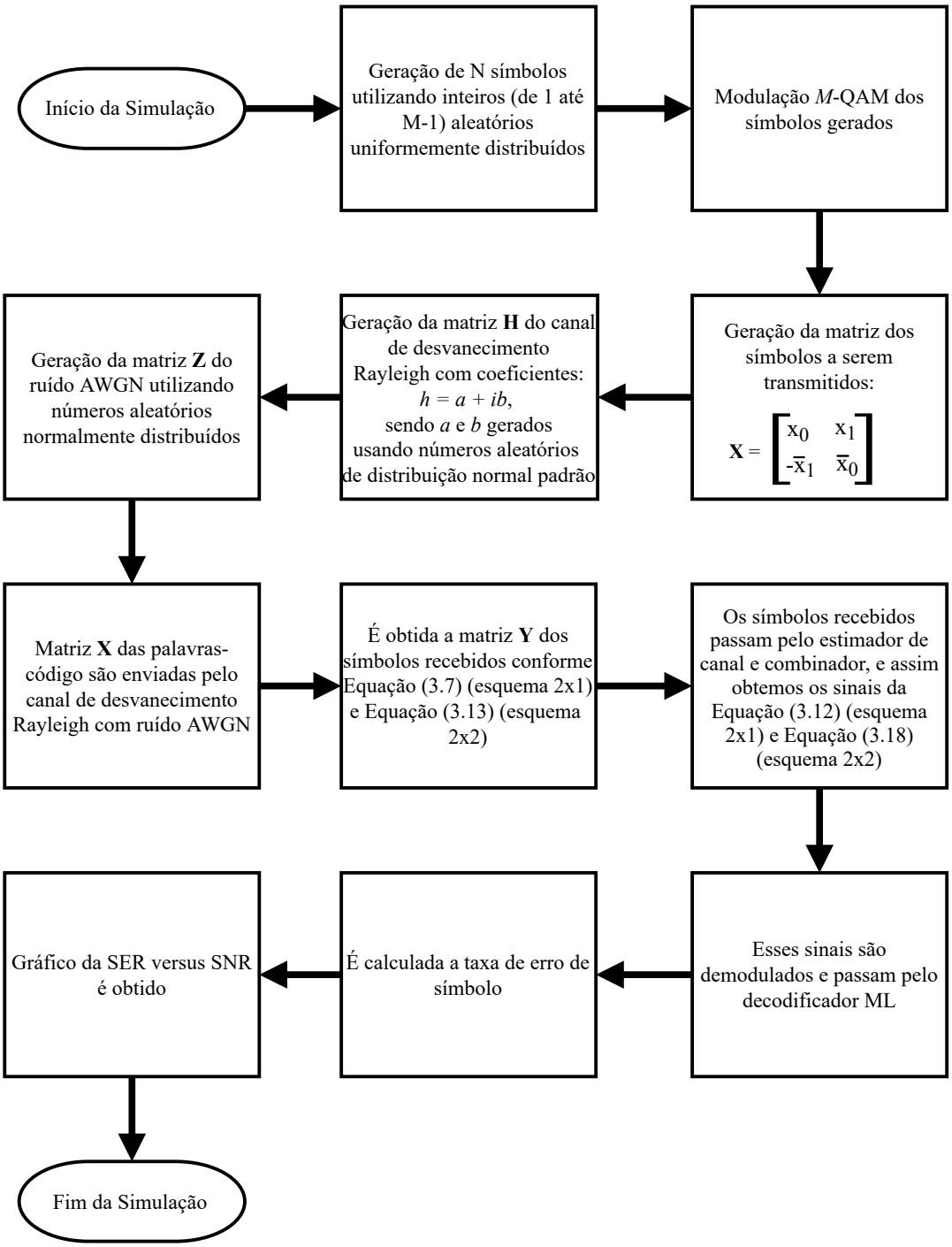
Figura 8 – Esquema de transmissão para sistema com duas antenas receptoras.



Fonte: Próprio autor.

A Figura 9 apresenta o fluxograma da rotina implementada no MATLAB para a simulação do código de Alamouti, tanto no esquema 2×1 quanto no esquema 2×2.

Figura 9 – Fluxograma da rotina de simulação do código de Alamouti com modulações M-QAM.



Fonte: Próprio autor.

As simulações foram realizadas para os códigos de Alamouti 2×1 e 2×2 para modulações 4, 16, 64 e 256-QAM com uma SNR de 0 a 35 dB. Em cada simulação foi considerada a energia média da constelação respectiva de cada ordem de modulação M-QAM, podemos calcular essa energia para constelações quadradas pela equação a seguir [Kamalov 2016]

$$E_{M-QAM} = \frac{(M-1)}{6} d_{min}^2 \tag{5.1}$$

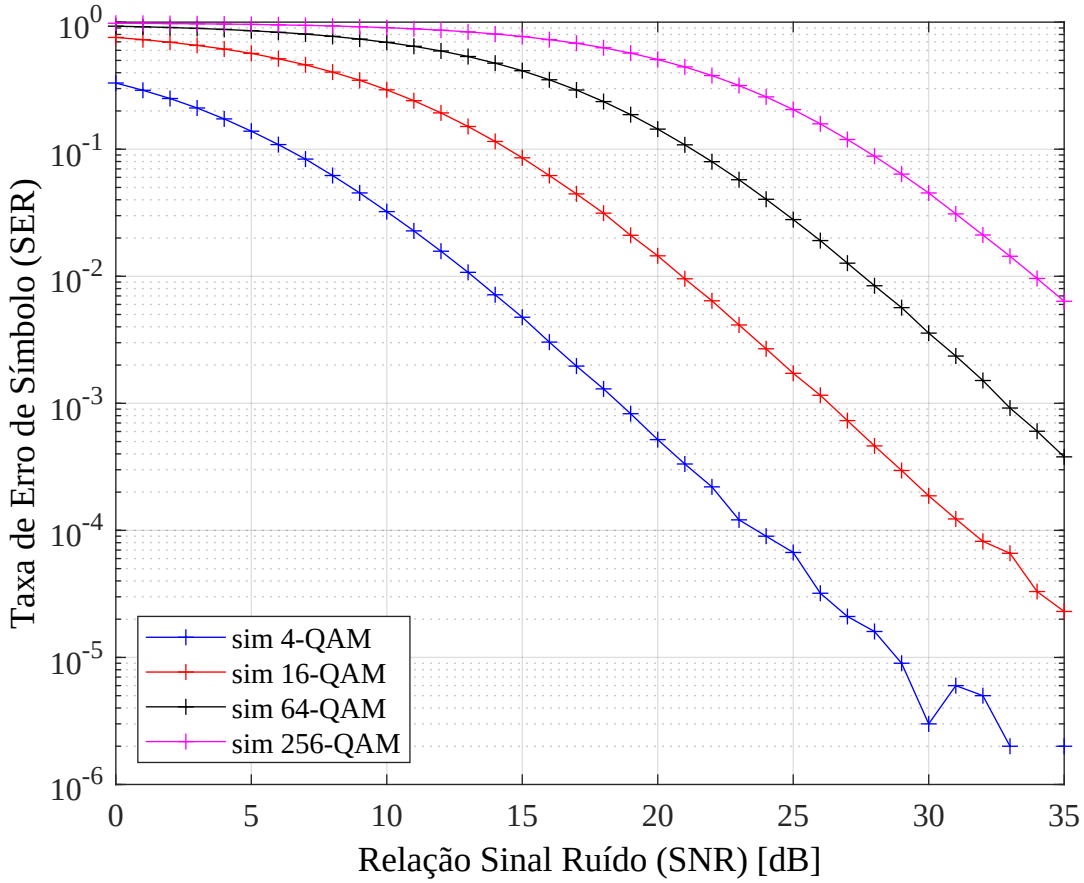
Considerando que a distância Euclidiana $d_{min} = 2$, temos a energia média das constelações 4, 16, 64 e 256-QAM apresentadas na Tabela 4.

Tabela 4 – Energia média da constelação M-QAM.

M	E_{M-QAM}
4	2
16	10
64	42
256	170

Como temos duas antenas transmissoras, foi utilizado nas simulações o dobro da energia E_{M-QAM} para cada M-QAM. A Figura 10 apresenta as curvas da simulação do código de Alamouti 2×1, a Figura 11 apresenta as curvas da simulação do código de Alamouti 2×2 e a Figura 12 apresenta uma comparação entre as curva das simulações anteriores.

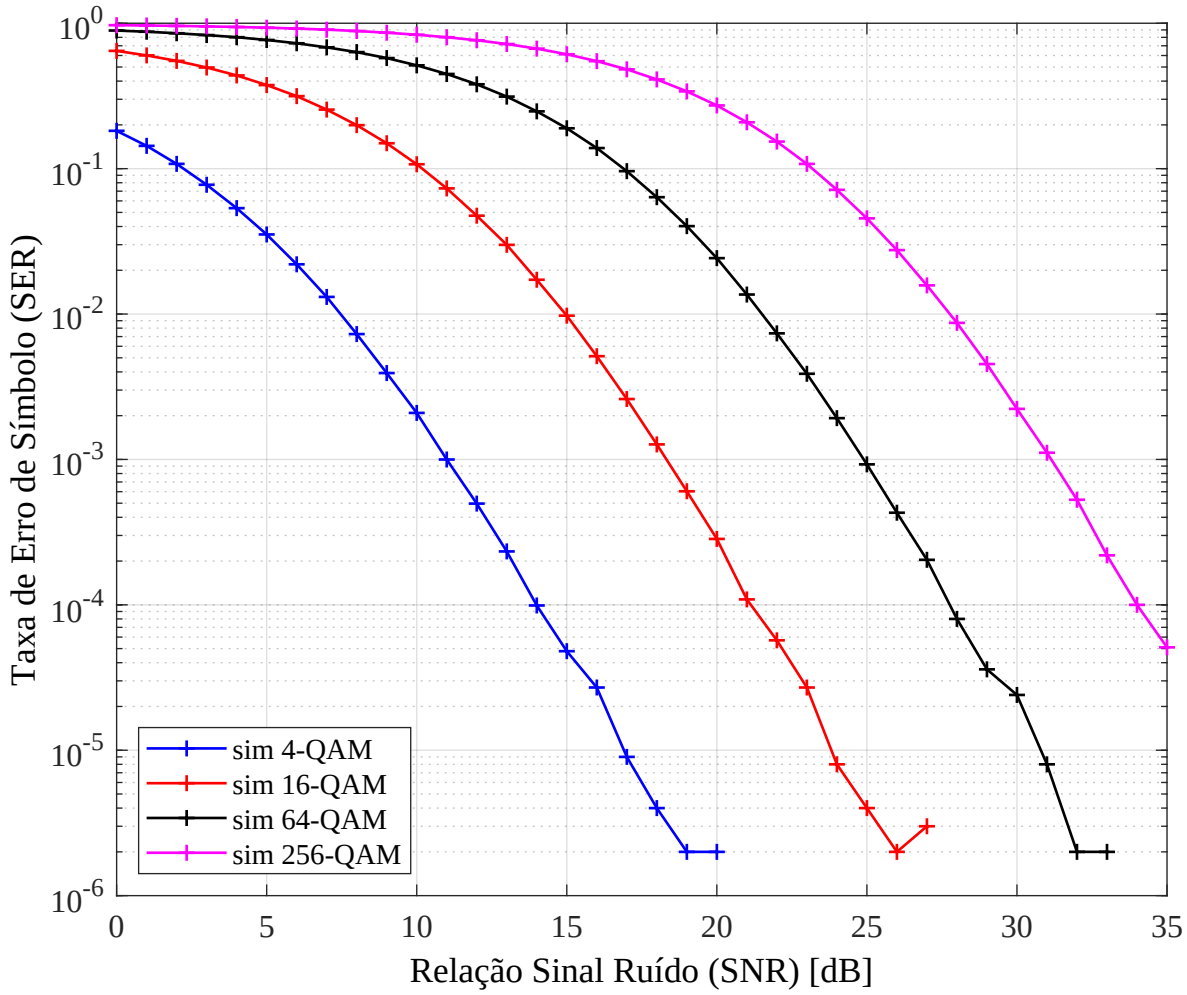
Figura 10 – Simulação da SER do código de Alamouti 2×1 com modulações 4, 16, 64 e 256-QAM.



Fonte: Próprio autor.

É possível observar que conforme aumentamos a modulação maior é a taxa de erro de símbolo, ou seja, quanto mais aumentamos a ordem da modulação mais energia é necessária para alcançar uma dada SER [Mindaudu e Miyim 2012]. Isso se deve ao fato que cada modulação M-QAM tem uma energia média da constelação utilizada para transmissão.

Figura 11 – Simulação da SER do código de Alamouti 2×2 com modulações 4, 16, 64 e 256-QAM.

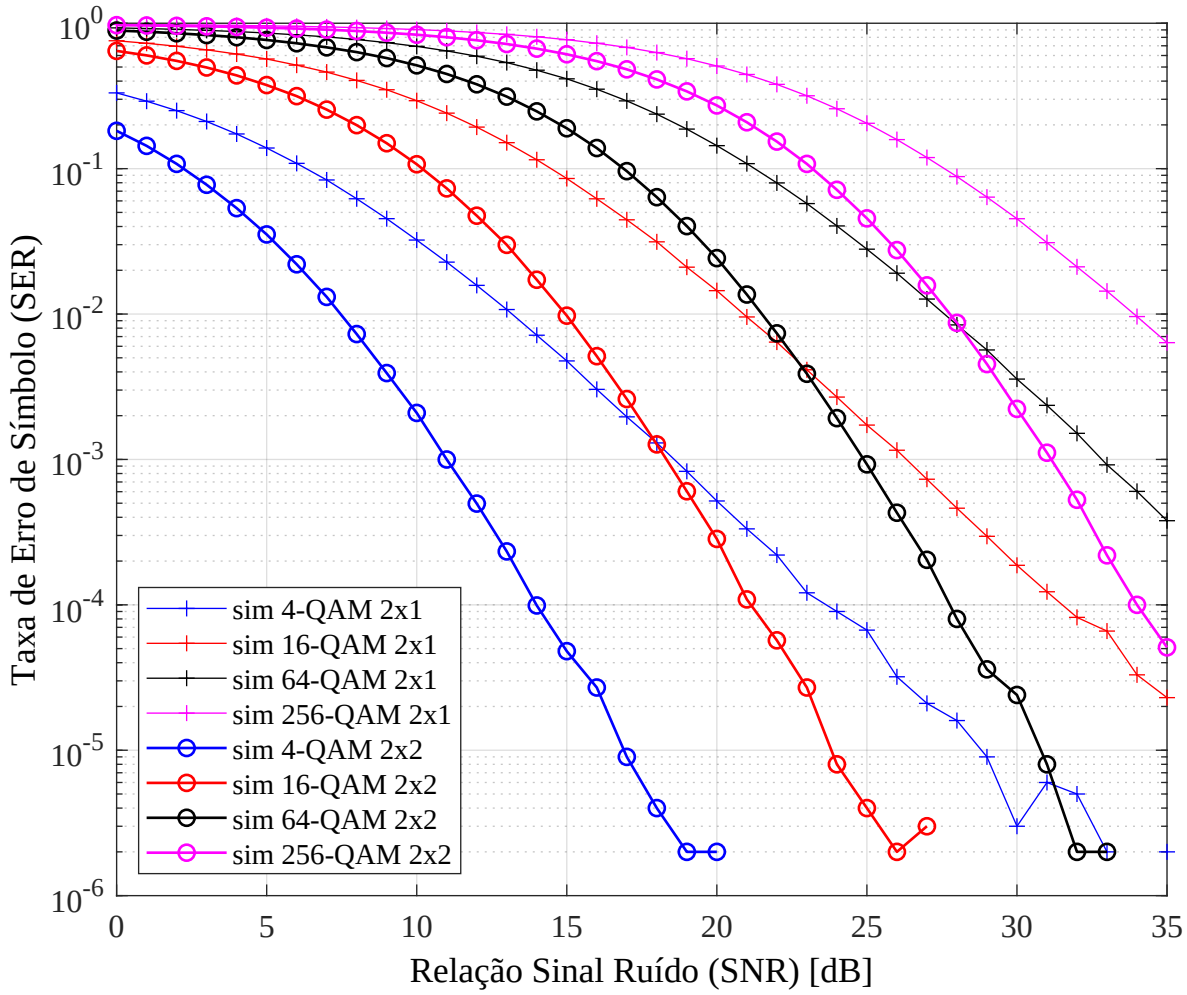


Fonte: Próprio autor.

Pela Figura 12 vemos que para mesma ordem de modulação, o caso 2×2 possui uma melhor taxa de erro de símbolo em comparação ao caso 2×1. Para ser obter uma taxa de erro de símbolo de 10^{-4}, em uma modulação 4-QAM, é necessária uma SNR de 14 dB para o caso 2×2, já para o caso 2×1 é necessária uma SNR de 24 dB.

Essa diferença ocorre pela aumento do número de antenas receptoras, para o caso 2×1 temos apenas dois canais independentes, já para o caso 2×2 temos quatro canais independentes, é possível observar este fato pela Figura 7 e Figura 8. Isso aumenta a ordem de diversidade de $2n_r$ [Alamouti 1998], isto é, para o esquema 2×1 temos uma diversidade de 2 e para esquema o 2×2 temos uma diversidade de 4.

Figura 12 – Simulação da SER do código de Alamouti 2×1 e 2×2 com modulações M-QAM.



Fonte: Próprio autor.

5.2 SIMULAÇÕES DO CÓDIGO DE OURO

O código de Ouro é um código de bloco espaço-tempo de dispersão linear construído a partir de álgebras de divisão cíclica e está relacionado com o número de Ouro $\theta = \frac{1+\sqrt{5}}{2}$ [BELFIORE J.-C.; Rekaya e Viterbo 2005]. Na Seção 4.3, apresentamos a definição de STBC perfeito e depois construímos o código de Ouro via álgebra de divisão cíclica. Essa estrutura algébrica proporciona as principais características de um código perfeito: taxa máxima, posto máximo, diversidade máxima, determinante diferente de zero e *shaping* cúbico. Tais características são critérios importantes para a eficiência do código, como já explorado na Seção 3.3.

Como visto na Seção 4.3, o código de Ouro é construído utilizando uma álgebra de divisão cíclica do tipo

$$\mathcal{A} = (L/K = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i), \sigma, \gamma), \tag{5.2}$$

com $\sigma : \sqrt{5} \mapsto -\sqrt{5}$ e $\gamma = i$.

Com a matriz da palavra-código $\mathbf{X}$ dada pela Equação 4.29, temos que $\theta = \frac{1+\sqrt{5}}{2}$ (número de

Ouro), $\sigma(\theta) = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i\sigma(\theta)$ e $\sigma(\alpha) = 1 + i\theta$. Podemos reescrever a matriz da palavra-código usando as relações de $\theta\sigma(\theta) = -1$ e $\theta + \sigma(\theta) = 1$, assim temos

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} [1 + i\sigma(\theta)]x_0 + [\theta - i]x_1 & [1 + i\sigma(\theta)]x_2 + [\theta - i]x_3 \\ [i - \theta]x_2 + [1 + i\sigma(\theta)]x_3 & [1 + i\theta]x_0 + [\sigma(\theta) - i]x_1 \end{bmatrix}. \tag{5.3}$$

Dessa forma, podemos remodelar $\mathbf{X}$, empilhando a matriz coluna a coluna, para obter uma matriz 4×1:

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} [1 + i\sigma(\theta)]x_0 + [\theta - i]x_1 \\ [i - \theta]x_2 + [1 + i\sigma(\theta)]x_3 \\ [1 + i\sigma(\theta)]x_2 + [\theta - i]x_3 \\ [1 + i\theta]x_0 + [\sigma(\theta) - i]x_1 \end{bmatrix}. \tag{5.4}$$

Agora, pegamos a matriz que foi remodelada e separamos a parte real da parte imaginária, obtendo uma matriz de tamanho 8×1:

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \mathrm{Re}(x_0) - \sigma(\theta)\mathrm{Im}(x_0) + \theta\mathrm{Re}(x_1) + \mathrm{Im}(x_1) \\ \sigma(\theta)\mathrm{Re}(x_0) + \mathrm{Im}(x_0) - \mathrm{Re}(x_1) + \theta\mathrm{Im}(x_1) \\ -\theta\mathrm{Re}(x_2) - \mathrm{Im}(x_2) + \mathrm{Re}(x_3) - \sigma(\theta)\mathrm{Im}(x_3) \\ \mathrm{Re}(x_2) - \theta\mathrm{Im}(x_2) + \sigma(\theta)\mathrm{Re}(x_3) + \mathrm{Im}(x_3) \\ \mathrm{Re}(x_2) - \sigma(\theta)\mathrm{Im}(x_2) + \theta\mathrm{Re}(x_3) + \mathrm{Im}(x_3) \\ \sigma(\theta)\mathrm{Re}(x_2) + \mathrm{Im}(x_2) - \mathrm{Re}(x_3) + \theta\mathrm{Im}(x_3) \\ \mathrm{Re}(x_0) - \theta\mathrm{Im}(x_0) + \sigma(\theta)\mathrm{Re}(x_1) + \mathrm{Im}(x_1) \\ \theta\mathrm{Re}(x_0) + \mathrm{Im}(x_0) - \mathrm{Re}(x_1) + \sigma(\theta)\mathrm{Im}(x_1) \end{bmatrix}, \tag{5.5}$$

que pode ser reescrita como

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -\sigma(\theta) & \theta & 1 & 0 & 0 & 0 & 0 \\ \sigma(\theta) & 1 & -1 & \theta & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\theta & -1 & 1 & \sigma(\theta) \\ 0 & 0 & 0 & 0 & 1 & -\theta & \sigma(\theta) & 1 \\ 0 & 0 & 0 & 0 & 1 & -\sigma(\theta) & \theta & 1 \\ 0 & 0 & 0 & 0 & \sigma(\theta) & 1 & -1 & \theta \\ 1 & -\theta & \sigma(\theta) & 1 & 0 & 0 & 0 & 0 \\ \theta & 1 & -1 & \sigma(\theta) & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} \mathrm{Re}(x_0) \\ \mathrm{Im}(x_0) \\ \mathrm{Re}(x_1) \\ \mathrm{Im}(x_1) \\ \mathrm{Re}(x_2) \\ \mathrm{Im}(x_2) \\ \mathrm{Re}(x_3) \\ \mathrm{Im}(x_3) \end{bmatrix}. \tag{5.6}$$

E assim, podemos dizer que $\mathbf{X} = \mathbf{MF}$, em que

$$\mathbf{M} = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -\sigma(\theta) & \theta & 1 & 0 & 0 & 0 & 0 \\ \sigma(\theta) & 1 & -1 & \theta & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\theta & -1 & 1 & \sigma(\theta) \\ 0 & 0 & 0 & 0 & 1 & -\theta & \sigma(\theta) & 1 \\ 0 & 0 & 0 & 0 & 1 & -\sigma(\theta) & \theta & 1 \\ 0 & 0 & 0 & 0 & \sigma(\theta) & 1 & -1 & \theta \\ 1 & -\theta & \sigma(\theta) & 1 & 0 & 0 & 0 & 0 \\ \theta & 1 & -1 & \sigma(\theta) & 0 & 0 & 0 & 0 \end{bmatrix} e \ \mathbf{F} = \begin{bmatrix} \mathrm{Re}(x_0) \\ \mathrm{Im}(x_0) \\ \mathrm{Re}(x_1) \\ \mathrm{Im}(x_1) \\ \mathrm{Re}(x_2) \\ \mathrm{Im}(x_2) \\ \mathrm{Re}(x_3) \\ \mathrm{Im}(x_3) \end{bmatrix}, \tag{5.7}$$

sendo $\mathbf{M}$ a matriz geradora do código de Ouro e $\mathbf{F}$ a matriz que contém as partes real e imaginária dos símbolos modulados.

Para a simulação do código de Ouro 2×2, a matriz $\mathbf{X}$ é transmitida pelo canal $\mathbf{H}$, e assim temos que a matriz do sinal recebido é $\mathbf{Y} = \mathbf{HX} + \mathbf{Z}$, sendo que a matriz $\mathbf{H}$ pode ser expandida para uma matriz 8×8 com valores reais, como se segue

$$\mathbf{H} = \begin{bmatrix} \mathrm{Re}(h_{00}) & -\mathrm{Im}(h_{00}) & \mathrm{Re}(h_{10}) & -\mathrm{Im}(h_{10}) & 0 & 0 & 0 & 0 \\ \mathrm{Im}(h_{00}) & \mathrm{Re}(h_{00}) & \mathrm{Im}(h_{10}) & \mathrm{Re}(h_{10}) & 0 & 0 & 0 & 0 \\ \mathrm{Re}(h_{01}) & -\mathrm{Im}(h_{01}) & \mathrm{Re}(h_{11}) & -\mathrm{Im}(h_{11}) & 0 & 0 & 0 & 0 \\ \mathrm{Im}(h_{01}) & \mathrm{Re}(h_{01}) & \mathrm{Im}(h_{11}) & \mathrm{Re}(h_{11}) & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathrm{Re}(h_{00}) & -\mathrm{Im}(h_{00}) & \mathrm{Re}(h_{10}) & -\mathrm{Im}(h_{10}) \\ 0 & 0 & 0 & 0 & \mathrm{Im}(h_{00}) & \mathrm{Re}(h_{00}) & \mathrm{Im}(h_{10}) & \mathrm{Re}(h_{10}) \\ 0 & 0 & 0 & 0 & \mathrm{Re}(h_{01}) & -\mathrm{Im}(h_{01}) & \mathrm{Re}(h_{11}) & -\mathrm{Im}(h_{11}) \\ 0 & 0 & 0 & 0 & \mathrm{Im}(h_{01}) & \mathrm{Re}(h_{01}) & \mathrm{Im}(h_{11}) & \mathrm{Re}(h_{11}) \end{bmatrix} \tag{5.8}$$

E assim, a matriz $\mathbf{X} = \mathbf{MF}$, então a matriz do sinal recebido se torna $\mathbf{Y} = \mathbf{HMF} + \mathbf{Z}$.

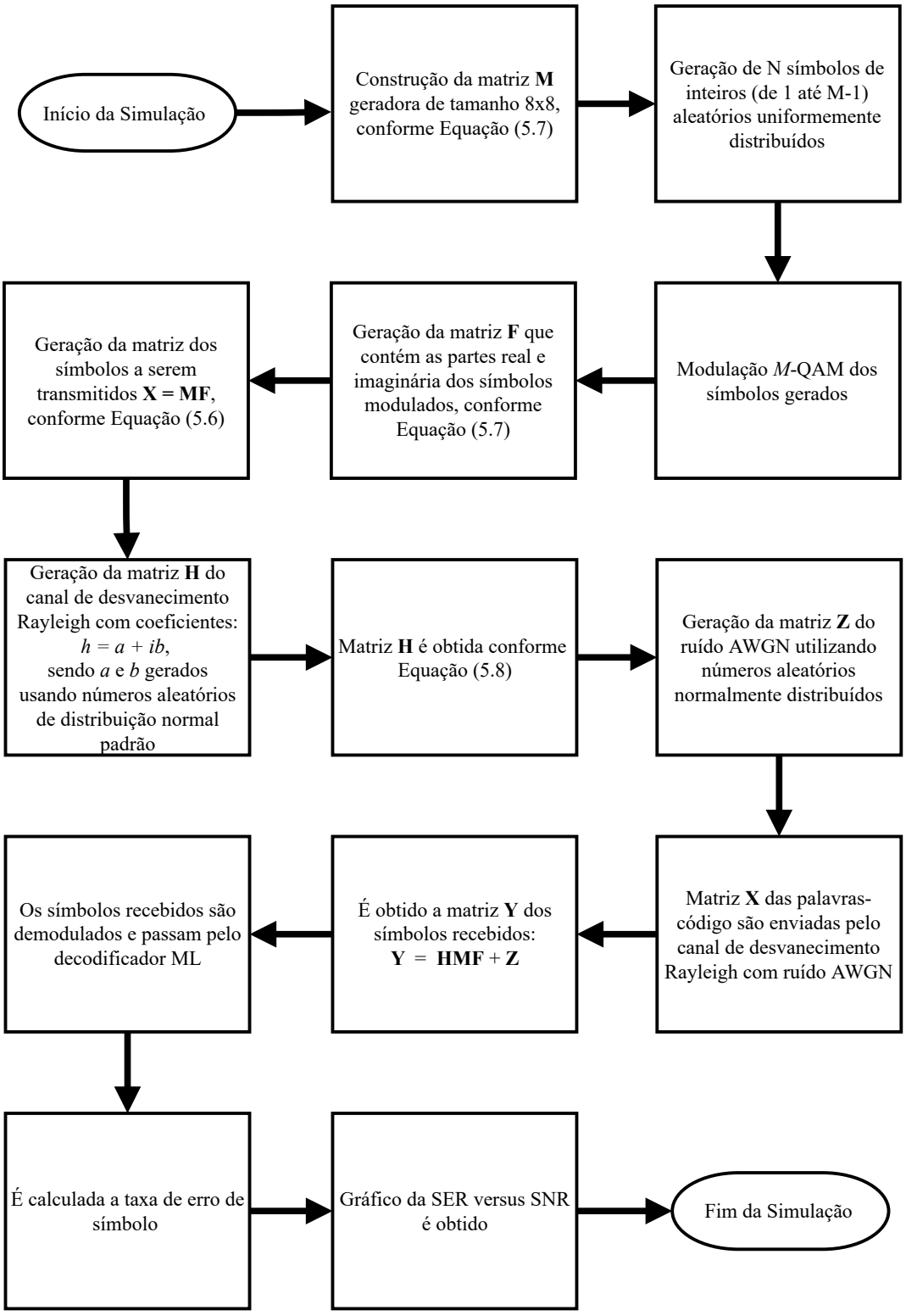
A Figura 13 apresenta o fluxograma da rotina implementada no MATLAB para a simulação do código de Ouro 2×2.

As simulações foram realizadas para o código de Ouro 2×2 para modulação 4-QAM em comparação ao código de Alamouti para modulações 4 e 16-QAM com uma SNR de 0 a 20 dB. Assim como nas simulações anteriores, foi considerada a energia média da constelação respectiva de cada ordem de modulação M-QAM, calculada utilizando a Equação 5.1. Porém, por se tratar de um STBC perfeito e ter uma constelação de formato cúbico, foi considerada a distância Euclidiana $d_{min} = 1$, então temos a energia média da constelação 4-QAM é dada por

$$E_{4-QAM} = \frac{(M-1)}{6} d_{min}^2 = \frac{(4-1)}{6} 1^2 = 0,5. \tag{5.9}$$

E por temos duas antenas transmissoras, foi utilizado nas simulações o dobro da energia (E_{M-QAM}).

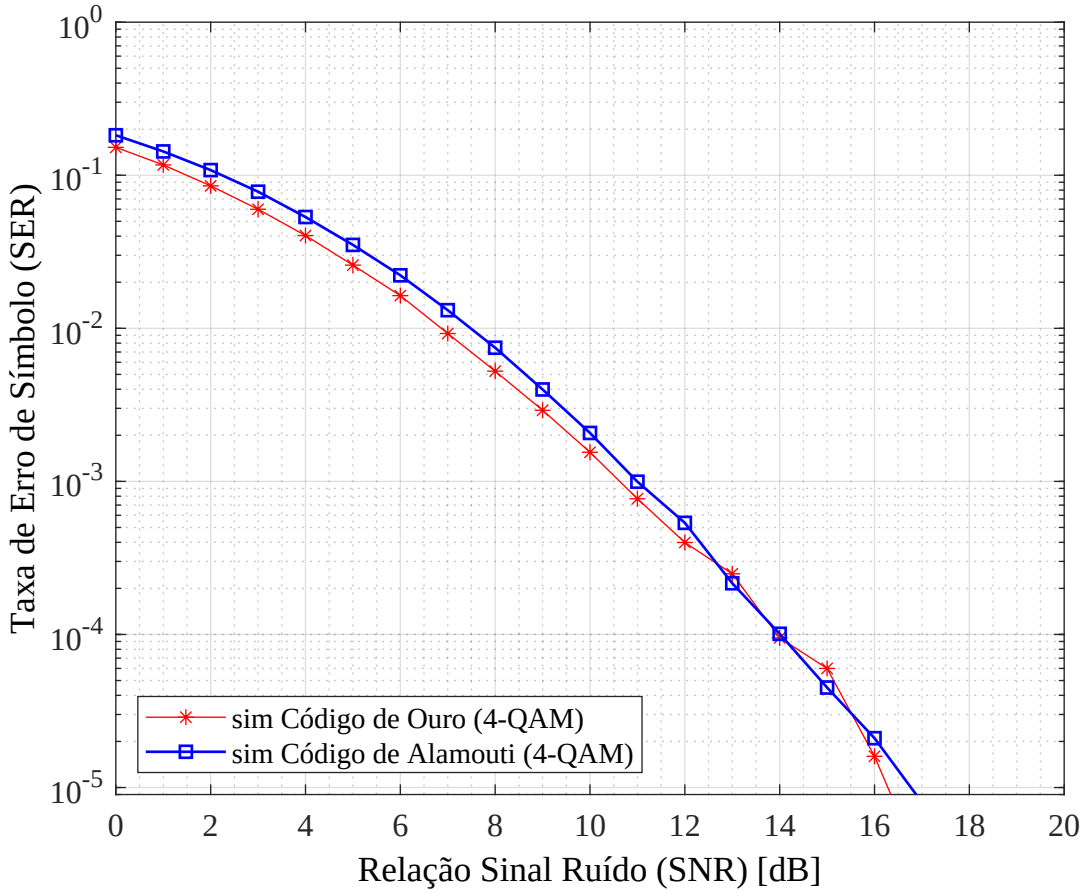
Figura 13 – Fluxograma da rotina de simulação do código de Ouro com modulações M-QAM.



Fonte: Próprio autor.

A seguir, a Figura 14 apresenta as curvas da simulação do código de Ouro 2×2 em comparação com o código de Alamouti 2×2, ambos utilizando a modulação 4-QAM.

Figura 14 – Simulação da SER do código de Alamouti e do código de Ouro 2×2 com modulação 4-QAM.



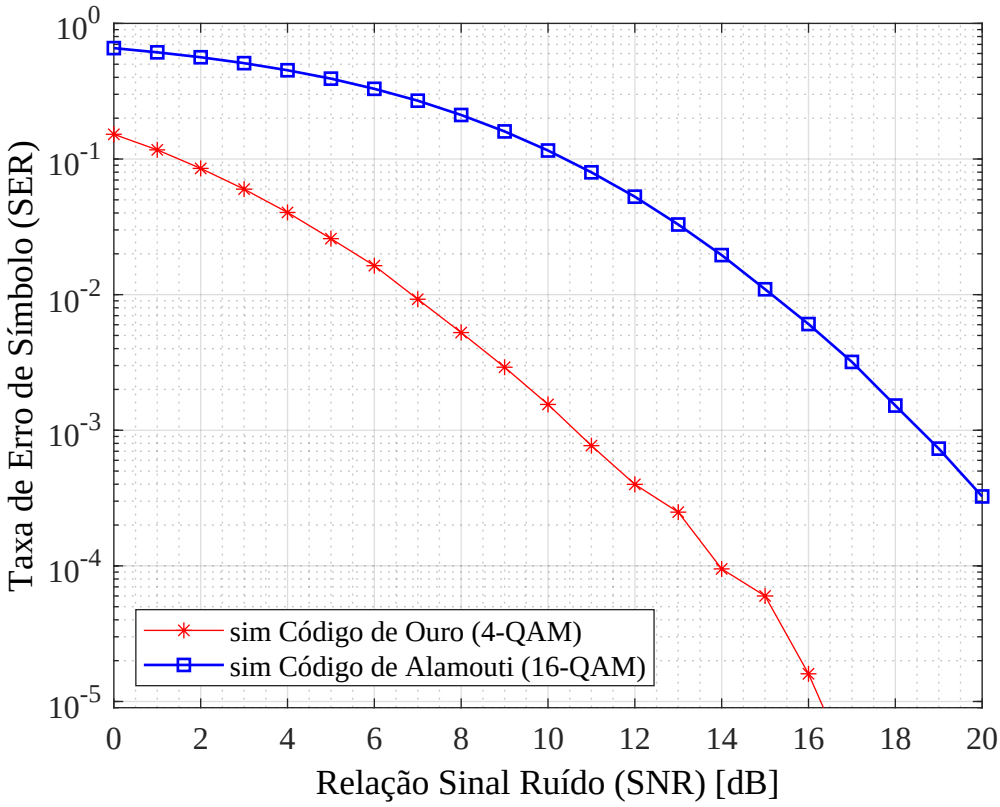
Fonte: Próprio autor.

Podemos notar, exclusivamente pelas curvas, que o código de Ouro tem um desempenho levemente superior ao de Alamouti. No entanto, temos que levar em consideração que o código de Ouro consegue esse resultado utilizando apenas $\frac{1}{4}$ da energia média que o Alamouti gasta.

O código de Ouro transmite 4 símbolos modulados por 4-QAM, ou seja, cada símbolo envia 2 bits, com um total de 8 bits de informação sendo enviados com apenas $\frac{1}{4}$ da energia média que o Alamouti utiliza para enviar 2 símbolos modulados por 4-QAM, isto é, apenas 4 bits de informação. Com essa análise, vemos que o código de Ouro tem uma performance muito elevada, já que tem o dobro da eficiência espectral com somente $\frac{1}{4}$ da energia média, em relação ao código de Alamouti.

A Figura 15 apresenta as curvas das simulações do código de Ouro 2×2 com modulação 4-QAM em comparação com o código de Alamouti 2×2 com modulação 16-QAM.

Figura 15 – Simulação da SER do código de Alamouti e do código de Ouro 2×2 com modulações M-QAM.



Fonte: Próprio autor.

Por ser tratar de modulações de ordens diferentes, a princípio essa comparação pode não parecer justa, já que modulações de ordem superior necessitam de mais energia para transmissão. Porém, comparando a palavra-código $\mathbf{X}$ (Equação 4.29) pertencente ao código de Ouro com a do código de Alamouti (Equação 3.5), vemos que no caso do Alamouti há a transmissão de 2 símbolos modulados por vez, enquanto no caso do código de Ouro há a transmissão de 4 símbolos modulados por vez, ou seja, 8 bits de informação são transmitidos em ambos os casos. Portanto, é necessário o uso de modulações de ordem diferente a fim de obter a mesma eficiência espectral para os dois códigos.

Dessa forma, no caso do código de Ouro temos a mesma quantidade de bits sendo enviados com apenas $\frac{1}{20}$ da energia utilizada por Alamouti, ou seja, o esquema de Alamouti necessita de 20 vezes mais energia.

Por isso essa diferença nas curvas de desempenho, para uma SER de aproximadamente 10^{-3}, é necessário uma SNR de mais ou menos 11 dB para o código de Ouro, ao mesmo tempo que o código de Alamouti necessita de cerca de 19 dB.

6 CONCLUSÃO

Neste trabalho, realizamos um estudo e analisamos o desempenho de códigos de bloco espaço-tempo em canais MIMO 2×2, com foco especial no código de Alamouti e no código de Ouro construídos utilizando álgebras de divisão cíclicas. Para isso estudamos alguns conceitos algébricos necessários para a construção dos STBCs via álgebras de divisão cíclicas, como teoria algébrica dos números, reticulados, estruturas algébricas, entre outros. Após isso, estudamos os canais do tipo MIMO, os códigos de bloco espaço-tempo, focando no código de Alamouti, e por fim, estudamos um pouco sobre os critérios necessários que um STBC deve ter para ser considerado eficiente. A partir destes estudos, apresentamos as construções do código de Alamouti via álgebra dos quatérnios de Hamilton e de STBC's 2×2 via álgebra cíclicas de divisão sobre corpos de números, e então falamos sobre códigos de bloco espaço-tempo perfeitos e a construção do código de Ouro. Para finalizar, apresentamos os resultados e uma análise das simulações realizadas para os códigos de Alamouti e de Ouro.

No código de Alamouti, os dados a serem enviados são codificados no espaço e no tempo, pois os símbolos são transmitidos em períodos diferentes e por antenas diferentes. É um STBC com decodificação por ML de baixa complexidade, graças a sua propriedade de ortogonalidade. Para um esquema MISO 2×1, consegue ser um código de diversidade e taxa máximas quando os símbolos pertencem a uma constelação complexa. Para casos MIMO $2 \times n_r$, sempre oferece um código de diversidade máxima, mas não de taxa máxima. No caso específico de um esquema MIMO 2×2, temos um código de taxa meia, dado que transmite apenas dois símbolos durante dois períodos de uso de canal em duas antenas. os STBCs ortogonais não atingem taxa máxima devido a sua propriedade de ortogonalidade.

Então, para se obter todas as características de um STBC eficiente, temos os códigos de bloco espaço-tempo perfeitos. Um exemplo de STBC perfeito construído a partir de álgebras de divisão cíclica, para canais MIMO 2×2, é o código de Ouro. Esse código é de taxa e diversidade máximas, possui determinante diferente de zero (*non-vanishing determinant*) e energeticamente eficiente, por conta da constelação no formato cúbico (*cubic shaping*).

Para analisar o desempenho dos códigos de Alamouti e de Ouro, realizamos simulações computacionais no *software* MATLAB. Nessas simulações, consideramos que o receptor fosse coerente, ou seja, CSI perfeito, em um canal MIMO 2×2 de desvanecimento Rayleigh quase-estático e plano com ruído AWGN. A performance dos códigos foi analisada através das curvas da taxa de erro de símbolo (SER) versus a relação sinal-ruído (SNR) para diferentes ordens de modulação M-QAM.

Com os resultados obtidos, podemos concluir que o código de Ouro possui o desempenho superior comparado ao código de Alamouti. Na simulação realizada com modulação 4-QAM, o código de Ouro tem o dobro da eficiência espectral com apenas $\frac{1}{4}$ da energia média de transmissão, em relação ao código de Alamouti. Isso ocorre pois o código de Alamouti é de meia taxa, diferente do de Ouro que é de taxa máxima, implicando na transmissão de 8 bits de informação para o código de Ouro, enquanto o de Alamouti transmite 4 bits de informação. E na simulação feita com modulações de

ordens diferentes, 4-QAM no de Ouro e 16-QAM no de Alamouti, temos a mesma eficiência espectral para ambos. No entanto, o código de Alamouti necessita de 20 vezes da energia utilizada pelo de Ouro para transmitir a mesma quantidade de bits (8 bits).

Esses resultados nos mostram que devido ao código de Ouro ser de taxa máxima, ou seja, o número de sinais transmitidos corresponde ao número de símbolos de informação a serem enviados, o que maximiza a taxa de dados, e devido ao seu formato de constelação ser cúbico, isto é, a matriz $\mathbf{M}$ é complexa unitária, o que otimiza a eficiência energética do código, que são obtidas pela sua estrutura construída a partir de álgebras de divisão cíclica, fazem o código de Ouro ser superior em comparação ao código de Alamouti.

REFERÊNCIAS

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

BELFIORE J.-C.; REKAYA, G.; VITERBO, E. *The Golden Code: A 2×2 full-rate space-time code with non-vanishing determinants*. ***IEEE Transactions on Information Theory***, v. 51, n. 4, p. 1432–1436, 2005.

BENEDITO, C. W. O. **Famílias de reticulados algébricos e reticulados ideais**. Tese (Mestrado) — Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas, 2010. Disponível em: <http://hdl.handle.net/11449/94238>.

BENEDITO, C. W. O. **Construção de Grupos Fuchsianos Aritméticos provenientes de Álgebras dos Quatérnios e Ordens Maximais dos Quatérnios associados a Reticulados Hiperbólicos**. Tese (Doutorado em Engenharia Elétrica) — Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas, 2014.

BIGLIERI, E. et al. ***MIMO Wireless Communications***. [S.l.]: Cambridge University Press, 2007. ISBN 9781139461269.

CHIURTU, N.; RIMOLDI, B.; Telatar, E. *On the capacity of multi-antenna Gaussian channels*. In: ***Proceedings. 2001 IEEE International Symposium on Information Theory* (IEEE Cat. No.01CH37252)**. [S.l.: s.n.], 2001. p. 53–.

ELIA, P. et al. *Explicit Space–Time Codes Achieving the Diversity–Multiplexing Gain Tradeoff*. ***IEEE Transactions on Information Theory***, v. 52, n. 9, p. 3869–3884, 2006.

ELIA, P.; SETHURAMAN, B. A.; KUMAR, P. V. *Perfect space-time codes with minimum and non-minimum delay for any number of antennas*. In: ***2005 International Conference on Wireless Networks, Communications and Mobile Computing***. [S.l.: s.n.], 2005. v. 1, p. 722–727.

FALOU, A. E. ***Analysis and design of space-time block codes for coded MIMO transmissions***. Tese (Doutorado) — Télécom Bretagne, Université de Bretagne-Sud, maio 2013. Disponível em: <https://tel.archives-ouvertes.fr/tel-00908835>.

FERRARI, A. J. **Reticulados algébricos via corpos abelianos**. Tese (Mestrado) — Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas, 2008. Disponível em: <http://hdl.handle.net/11449/94237>.

Chapter 3 - Univariate Distribution Theory. In: FLETCHER, S. (Ed.). ***Data Assimilation for the Geosciences: From Theory to Application***. [S.l.]: Elsevier Science.

FOSCHINI, G.; GANS, M. *On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas*. ***Wireless Personal Communications***, v. 6, p. 311–335, 1998.

GESBERT, D. et al. *From theory to practice: an overview of MIMO space-time coded wireless systems*. ***IEEE Journal on Selected Areas in Communications***, v. 21, n. 3, p. 281–302, 2003.

GESBERT, D. et al. *From theory to practice: an overview of MIMO space-time coded wireless systems*. ***IEEE Journal on Selected Areas in Communications***, v. 21, n. 3, p. 281–302, 2003.

GONÇALVES, A. **Introdução à álgebra**. [S.l.]: IMPA, 1999.

HOLLANTI, C. et al. *On the algebraic structure of the Silver code: A 2 × 2 perfect space-time block code*. In: ***2008 IEEE Information Theory Workshop***. [S.l.: s.n.], 2008. p. 91–94.

HUAN YAO; GREGORY W. WORNELL. *Achieving the full MIMO diversity-multiplexing frontier with rotation-based space-time codes*. In: ***in Proc. Allerton Conf. Commun., Contr., Comput.,, IL***. [S.l.: s.n.], 2003.

ITU, I. T. U. ***World Telecommunication/ICT Indicators Database***. 2020.

JACOBONI, C.; LUGLI, P. ***The Monte Carlo Method for Semiconductor Device Simulation***. [S.l.]: Springer Vienna, 2011. (*Computational Microelectronics*). ISBN 9783709174531.

KAMALOV, V. *Foreword by Valey Kamalov*. In: CHESNOY, J. (Ed.). ***Undersea Fiber Communication Systems***. Secunda edição. Academic Press, 2016. p. xxv–xxvi. ISBN 978-0-12-804269-4. Disponível em: <https://www.sciencedirect.com/science/article/pii/B9780128042694000210>.

LIZHONG ZHENG; TSE, D. N. C. *Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels*. ***IEEE Transactions on Information Theory***, v. 49, n. 5, p. 1073–1096, 2003.

MARCUS, D. ***Number Fields***. [S.l.]: Springer International Publishing, 1977.

MINDAUDU, A. S.; MIYIM, A. M. *BER Performance of MPSK and MQAM in* 2×2 *Alamouti MIMO Systems*. ***International Journal of Information Sciences and Techniques (IJIST)***, v. 2, p. 1–10, 2012.

OGGIER, F.; BELFIORE, J.-C.; VITERBO, E. *Cyclic Division Algebras: A Tool for Space-Time Coding*. ***Foundations and Trends® in Communications and Information Theory***, Now Publishers, v. 4, n. 1, p. 1–95, 2007. Disponível em: <https://doi.org/10.1561%2F0100000016>.

OGGIER, F. et al. *Perfect Space Time Block Codes*. ***IEEE Transactions on Information Theory***, IEEE Press, v. 52, n. 9, 09 2006.

OUERTANI, R. et al. *On the Golden Code Performance for MIMO-HSDPA System*. In: ***IEEE Vehicular Technology Conference***. [S.l.: s.n.], 2006. p. 1–5.

SALZ, J.; WINTERS, J. H.; GITLIN, R. D. *The impact of antenna diversity on the capacity of wireless communication systems*. ***IEEE Transactions on Communications***, v. 42, n. 234, p. 1740–1751, 1994.

SAMUEL, P. ***Algebraic Theory of Numbers***. [S.l.]: Dover Publications, 1970.

SETHURAMAN, B.; RAJAN, B.; SHASHIDHAR, V. *Full-diversity, high-rate space-time block codes from division algebras*. ***IEEE Transactions on Information Theory***, v. 49, n. 10, p. 2596–2616, 2003.

SETHURAMAN, B. A.; RAJAN, B. S. *An algebraic description of orthogonal designs and the uniqueness of the Alamouti code*. In: ***Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE***. [S.l.: s.n.], 2002. p. 1088 – 1092 vol.2. ISBN 0-7803-7632-3.

SETHURAMAN, B. A.; RAJAN, B. S. *Full-rank, full-rate STBCs from division algebras*. In: ***Proceedings of the IEEE Information Theory Workshop***. [S.l.: s.n.], 2002. p. 69–72.

SIBILLE, A.; OESTGES, C.; ZANELLA, A. ***MIMO: From Theory to Implementation***. [S.l.]: Academic Press, 2011. ISBN 9780123821942.

STEWART, I.; TALL, D. ***Algebraic Number Theory***. [S.l.]: Chapman and Hall/CRC, 1987.

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

TAROKH, V.; SESHADRI, N.; CALDERBANK, R. *Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction*. ***Information Theory, IEEE Transactions on***, v. 44, p. 744 – 765, 04 1998.