UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
CURSO DE ESPECIALIZAÇÃO EM MÉTODOS MATEMÁTICOS APLICADOS

ELIANE DE PAULA HUTT

CÓDIGOS GEOMETRICAMENTE UNIFORMES E GRUPOS ALFABETOS GENERALIZADOS: UMA TEORIA UNIFICADA

FRANCISCO BELTRÃO - PR
2019

ELIANE DE PAULA HUTT

CÓDIGOS GEOMETRICAMENTE UNIFORMES E GRUPOS ALFABETOS GENERALIZADOS: UMA TEORIA UNIFICADA

Trabalho de Conclusão apresentado como requisito parcial à obtenção do título de Especialista em Métodos Matemáticos Aplicados da Diretoria de Pesquisa e Pós-Graduação, da Universidade Tecnológica Federal do Paraná.

Orientador: Dr. Eduardo Michel Vieira Gomes

FRANCISCO BELTRÃO - PR

2019

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Francisco Beltrão
Diretoria de Pesquisa e Pós-Graduação
Especialização em Métodos Matemáticos Aplicados

TERMO DE APROVAÇÃO

Trabalho de Conclusão de Curso de Especialização

CÓDIGOS GEOMETRICAMENTE UNIFORMES E GRUPOS ALFABETOS GENERELIZADOS: UMATEORIA UNIFICADA

por

ELIANE DE PAULA HUTT

Trabalho de Conclusão de Curso de Especialização apresentado às 08 horas e 00 min. do dia 26 de Outubro de 2019, como requisito parcial para obtenção do grau de especialista em Métodos Matemáticos Aplicados, da Universidade Tecnológica Federal do Paraná, *Campus* Francisco Beltrão. A candidata foi arguida pela Banca Avaliadora composta pelos professores que abaixo assinam este Termo. Após deliberação, a Banca Avaliadora considerou o trabalho Aprovado (Aprovado ou Reprovado).

Prof. Dr. Eduardo Michel Vieira Gomes
Professor Orientador

NOME_DO_COORIENTADOR
Professor(a) Coorientador(a)

Prof. Dr. Maycow Gonçalves Carneiro
Membro da Banca

Prof. Dr. Waldir Silva Soares Junior
Membro da Banca

Prof. Dr. Vilmar Steffen
Responsável pela Coordenação do CEMMA
Curso de Especialização em Métodos Matemáticos Aplicados

A FOLHA DE APROVAÇÃO ORIGINAL (ASSINADA) ENCONTRA-SE NA COORDENAÇÃO DO CURSO DE ESPECIALIZAÇÃO EM MÉTODOS MATEMÁTICOS APLICADOS.

Ao meu noivo, o meu maior incentivador.

AGRADECIMENTOS

Primeiramente à Deus, pelas bênçãos em forma de luz, esperança e sabedoria.

Aos meus pais, pela proteção e carinho.

Ao meu noivo, que me fortalece nos momentos difíceis.

A coordenação do curso, pela cooperação.

Aos meus grandes amigos, por todo o apoio neste momento tão importante da minha formação acadêmica.

E, agradeço especialmente ao meu orientador, Prof. Dr. Eduardo Michel Vieira Gomes, pela oportunidade cedida de trabalharmos juntos neste estudo. Pela confiança depositada em mim neste momento de escolha. Por sua paciência, que foi fundamental para meu tempo de assimilação. Também, por ter sido o mediador e guia durante toda essa jornada de aprendizagem.

“Ás vezes, são as pessoas que ninguém espera nada que fazem as coisas que ninguém pode imaginar”.

Alan Turing

RESUMO

Os conceitos de Códigos Geometricamente Uniformes, introduzido por Forney, e Grupos Alfabetos Generalizados, desenvolvido por Biglieri, são apresentados e conciliados em uma teoria única e mais ampla. Surgem então, os Grupos Alfabetos Generalizados Enumeráveis que possibilitam gerar códigos a partir de estruturas geométricas singulares e estabelecer novas categorias de rotulamentos de códigos.

Palavras-chave: Códigos Geometricamente Uniformes. Grupos Alfabetos Generalizados. Grupos Alfabetos Generalizados Enumeráveis. Rotulamentos de Códigos.

ABSTRACT

The concepts of Geometrically Uniform Codes, created by Forney, and Generalized Group Alphabets, developed by Biglieri, are presented and reconciled in a unified theory. We then introduce the Generalized Enumerable Group Alphabets that enable us to generate codes from singular geometric structures and establish new categories of code labeling.

Index Terms: Code Labeling. Generalized Group Alphabets. Generalized Enumerable Group Alphabets. Geometrically Uniform Codes.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SÍMBOLOS

$(G,*)$	Grupo
$A \sim B$	A e B são conjuntos equivalentes
$\|A\| = \|B\|$	A e B são conjuntos cardinalmente equivalentes
$H \leq G$	H é subgrupo de G
$\|G\|$	Cardinalidade de um grupo $(G,*)$
$G = < H >$	Um subgrupo H é um conjunto gerador de um grupo $(G,*)$
$< H >$	Grupo gerado por H
aH	classe lateral à direita módulo H em relação à a
Ha	classe lateral à esquerda módulo H em relação à a
G/H	Grupo quociente de G por H
$H \lhd G$	H é subgrupo normal de G
$(G:H)$	Índice de H em G
(M,d)	Espaço métrico
$d(x,y)$	Distância entre os pontos x e y
$ISO(M)$	Grupo das isometrias de M
Id	Identidade
R_r	Reflexão pela reta r
$\rho_{O,\alpha}$	Rotação de centro O e ângulo α
$T_{\vec{v}}$	Translação do vetor $\vec{v}$
R_r	Reflexão pela reta r
$T_{\vec{v}}R_r(P)$	Reflexão deslizante no ponto P
S	Conjunto de sinais
E	Erro
P_i	Probabilidade de ocorrência do evento i
I_i	Quantidade de informação
$H(x)$	Entropia da fonte x
$H(x,y)$	Informação total que se pode obter das duas fontes
C	Capacidade de um canal
L	Limitante da informação média transmitida
R	Ritmo de informação
$\Gamma(S)$	Grupo de simetrias
S/S'	Uma partição geometricamente uniforme

SUMÁRIO

1 INTRODUÇÃO

Nas últimas décadas percebe-se um crescimento acelerado no setor de telecomunicações, motivado pelo aprimoramento de serviços de transmissão e armazenamento de informação. Assim, é fundamental o constante desenvolvimento de sistemas de comunicação que forneçam serviços de ótima qualidade, acompanhando o avanço tecnológico.

Em 1948, uma brilhante análise de um sistema de comunicação é formulada por Claude Shannon, resumidamente este resultado diz que é possível a transmissão de informação em um canal com uma taxa de erro arbitrariamente pequena, através de códigos corretores de erros eficientes. A partir disso, muitas pesquisas foram realizadas nessa área.

Os estudos revelam que os conjuntos de sinais que se mostraram eficazes para os sistemas de comunicação, são aqueles em que há uma ação transitiva de um grupo no conjunto de sinais, chamados de códigos geometricamente uniformes (CGU), que foram introduzidos por David Forney no seu trabalho *Geometrically Uniforme Codes*, no ano de 1991. Esta ideia iniciou-se com David Slepian ao criar o conceito de códigos de grupo, definidos como conjuntos finitos de pontos do espaço euclidiano, gerados por grupos de matrizes ortogonais operando em um ponto inicial, que mais tarde foi generalizado por Forney para qualquer espaço que contenha métrica, e além disso, o grupo gerador é um grupo de isometrias (CARVALHO, 2001).

Alguns anos antes, em 1988, Ezio Biglieri introduziu uma classe de sinais multidimensionais que apresentam ótimo grau de simetria, em seu trabalho intitulado *Multidimensional Modulation and Coding for Band-Limited Digital Channels*, que recebeu o nome de grupo alfabeto generalizado (GAG).

A proposta deste trabalho é a generalização deste conceito desenvolvido por Biglieri, o GAG, e a classe dos códigos geometricamente uniformes criada por Forney, em uma teoria mais ampla, a qual será chamada de grupo alfabeto generalizado enumerável, ou simplesmente GAGE. Esta nova classe de códigos carrega as boas características de ambos os conceitos citados.

O presente trabalho está dividido em 5 capítulos, conforme descritos a seguir:

No capítulo 1, o tema do trabalho é introduzido, apresentando os objetivos e justificativas do estudo.

No capítulo 2, são revisados os conceitos básicos sobre grupos, espaços métricos e isometrias. Descrevendo suas definições principais, propriedades fundamentais e alguns exemplos.

No capítulo 3, primeiramente, é feito um breve resumo de um sistema de comunicação digital. Em seguida, são apresentados os códigos geometricamente uniformes e os rotulamentos casados. E, no final é exibido o conceito de grupos alfabetos generalizados.

No capítulo 4, é fornecida a contribuição deste trabalho. Define-se o novo conjunto de códigos, o grupo alfabeto generalizado enumerável, sua teoria inicial é construída e detalhada neste capítulo.

Por fim, no capítulo 5, o trabalho é finalizado com as últimas análises sobre o tema de estudo e algumas recomendações de trabalhos futuros para dar continuidade nesta área de estudo.

2 GRUPOS, ESPAÇO MÉTRICO E ISOMETRIAS

Neste capítulo, apresenta-se noções gerais dos seguintes conceitos: grupos, espaço métrico e isometrias. Fornecendo definições e propriedades de suma importância para o desenvolvimento e compreensão do presente trabalho. Para um estudo mais detalhado sobre grupos o leitor pode consultar a referência (IEZI, 2003), sobre espaço métrico recomenda-se (LIMA, 1976) e para o estudo de isometrias sugere-se (LIMA, 1996).

2.1 GRUPOS

Nesta seção, a teoria, que se refere as definições, proposições e demonstrações, é baseada no trabalho de Hygino H. Domingues. Enquanto os exemplos são alguns exercícios, que foram resolvidos, propostos por Gelson Iezzi. Para mais detalhes, o leitor pode consultar a referência (IEZI, 2003), que foi desenvolvida por ambos os autores.

A Teoria de Grupos é a área da Matemática que estuda as estruturas algébricas formadas por grupos, tais estruturas são usadas para reproduzir as simetrias geométricas, onde cada figura pode ser relacionada a um grupo que define e reproduz sua simetria.

Dado um conjunto de elementos, a ideia principal desta teoria é tomar dois elementos quaisquer deste conjunto e associá-los a uma operação, formando um terceiro elemento deste mesmo conjunto. Para validar esta estrutura como grupo é necessário que o conjunto, munido da operação, satisfaça algumas propriedades.

Definição 2.1: Dado um conjunto não vazio G e uma operação binária $(x, y) \to x * y$ definida sobre G. O par $(G,*)$ é chamado de *grupo* se $*$ satisfaz as seguintes propriedades:

i) para todo $a, b \in G$ tem-se que $a * b \in G$ *(*G é *fechado* para a operação $*$);

ii) $(a * b) * c = a * (b * c)$, para quaisquer que sejam $a, b, c \in G$ (associatividade);

iii) existe um elemento $e \in G$ tal que $a * e = e * a = a$, para qualquer que seja $a \in G$ (existência de elemento neutro);

iv) existe um elemento $a' \in G$ tal que $a * a' = a' * a = e$, para todo $a \in G$ (existência de simétrico).

Se, além destas, o grupo ainda cumprir a seguinte propriedade:

v) $a * b = b * a$, para quaisquer que sejam $a, b \in G$ (comutatividade);

recebe o nome de *Grupo Abeliano* ou *Grupo Comutativo*.

Como vimos, um grupo será denotado pelo par $(G,*)$, onde o símbolo $*$ indica a operação sobre G. Em situações onde isso está claro, se pode ocultar este símbolo e representar o grupo somente por G.

Um grupo cuja operação é uma "adição" recebe o nome de *Grupo Aditivo*, em tal caso, o simétrico de um elemento a é o *oposto* de a, representado por $-a$. Já um grupo munido da operação "multiplicação" é chamado de *Grupo Multiplicativo*, neste caso, o simétrico de um elemento a é o *inverso* de a, representado por a^{-1}.

Exemplo 2.2: Seja $\mathbb{Z}$ o conjunto dos números inteiros munido da operação adição $+$, denotado por $(\mathbb{Z}, +)$. Para $(\mathbb{Z}, +)$ ser considerado um grupo, deve satisfazer as condições *i), ii), iii),* e *iv)* da definição. Então,

i) $\forall\, a, b \in Z \rightarrow a + b \in Z$

ii) $\forall\, a, b, c \in Z \rightarrow a + (b + c) = (a + b) + c$

iii) $\exists\, 0 \in Z : \forall\, a \in Z \rightarrow 0 + a = a$

iv) $\forall\, a \in Z \rightarrow \exists - a \in Z: \rightarrow (-a) + a = 0$

logo, $(\mathbb{Z}, +)$ é grupo. Note que o elemento neutro é o zero e para um número inteiro qualquer a, o seu oposto é o inteiro $-a$.

Exemplo 2.3: Considere $\mathbb{Z}^-$ o conjunto dos números inteiros não-positivos, munido da operação adição $+$, denotado por $(\mathbb{Z}^-, +)$. Temos que $(\mathbb{Z}^-, +)$ não é grupo, pois, não satisfaz a condição *iv)* da definição de grupo, que se refere a existência do simétrico de cada elemento no conjunto.

Exemplo 2.4: Considere o conjunto $B = \{1, -1\}$ munido da operação multiplicação $\bullet$, denotado por $(B, \bullet)$. Para $(B, \bullet)$ ser um grupo, deve satisfazer as condições *i), ii), iii)* e *iv)* da definição. Então,

i) $\forall\, a, b \in B \rightarrow a \bullet b \in B$

ii) $\forall\, a, b, c \in B \rightarrow a \bullet (b \bullet c) = (a \bullet b) \bullet c$

iii) $\exists\, 1 \in B : \forall\, a \in B \rightarrow 1 \bullet a = a \bullet 1 = a$

iv) $\forall\, a \in B \;\rightarrow \exists - a \in B\colon \rightarrow (-a) \bullet a = 1$

logo, $(B,\ \bullet)$ é grupo.

Todo grupo $(G,*)$ formado por um conjunto G finito, é chamado de *grupo finito*. O número de elementos deste conjunto, ou a medida do seu tamanho, é chamada de *cardinalidade*, ou *ordem*, e será denotado por $|G|$. Caso, o grupo G tenha um número infinito de elementos então ele será dito *grupo infinito*.

Dois conjuntos quaisquer A e B são *equivalentes,* denotados por $A \sim B$, se existir uma bijeção $f\colon A \rightarrow B$. Estes, possuem a mesma cardinalidade e são chamados de *cardinalmente equivalentes*, denotados por $|A| = |B|$.

Um subconjunto H de um grupo G é um *conjunto de geradores* de G, se todo elemento de G pode ser escrito como uma composição de elementos de H e seus inversos. Neste caso, escrevemos $G = < H >$. Se H é finito, então $G = < H >$ é dito *finitamente gerado*, e, se G tem somente um único gerador, então G é chamado de *grupo cíclico*.

Exemplo 2.5: Seja $(G,\ \bullet)$ um grupo de ordem 2 e $a \in G$. Como o elemento neutro deve estar no grupo, então, $a^{-1} = a$. Assim, temos que o a é o elemento gerador, então,

$$< a > = \{a^m, m \in \mathbb{Z}\} = \{a^0, a^1\} = \{1, a\} = G$$

logo, $(G,\ \bullet)$ é um grupo cíclico.

2.1.1 Subgrupos

Definição 2.6: Dado um grupo $(G,*)$, diz-se que um subconjunto não vazio $H \subset G$ é um *subgrupo* de G, denotado por $H \leq G$, se:

i) H é fechado para a operação $*$ (ou seja, se $a, b\ \in H$ então $a * b\ \in H$*);*

ii) $(H,*)$ também é um grupo (o símbolo * indica a restrição da operação de G aos elementos de H).

Caso e seja o elemento neutro de G, então, $\{e\}$ é um subgrupo de G. Além disso, o próprio G é um subgrupo de si mesmo. Estes, recebem o nome de *subgrupos triviais* de G.

Exemplo 2.7: Seja $(\mathbb{R}, +)$ um grupo, formado pelos conjuntos dos números reais e munido da operação adição. Note que $\mathbb{Z}$, o conjunto dos números inteiros, é um subconjunto de $\mathbb{R}$ que satisfaz as seguintes propriedades:

i) $\mathbb{Z}$ é fechado para a adição (ou seja, a soma de dois números inteiros resulta em um número inteiro);

ii) $(\mathbb{Z}, +)$ onde $+$ indica a adição de $\mathbb{R}$ restrita aos elementos de $\mathbb{Z}$ também é um grupo.

Por isso, podemos dizer que $\mathbb{Z}$ é um subgrupo de $\mathbb{R}$ com relação a operação de adição.

2.1.2 Homomorfismo

A ideia básica de Homomorfismo é de separar os grupos em classes disjuntas em que as propriedades deduzidas para um grupo dado de uma certa classe possam ser levadas para todos os grupos dessa classe, e apenas para estes. Sejam G e J dois grupos, para pertencerem à mesma classe necessita-se definir uma bijeção $f: G \to J$ que preserve as operações, ou seja, possibilite transferir os cálculos de um para outro, garantindo que G e J tenham ordens equivalentes. [9]

Definição 2.8: Dá-se o nome de homomorfismo de um grupo $(G, *)$ em outro grupo (J, Δ), toda aplicação $f: G \to J$ tal que, quaisquer que sejam $x, y \in G$:

$$f(x * y) = f(x)\, \Delta\, f(y)$$

Com isso, podemos nos referir a $f: G \to J$ como um *homomorfismo de grupos*. Quando se tratar do mesmo grupo, o que pressupõe $G = J$ e a mesma operação, então f será chamada de *automorfismo* de G.

O homomorfismo classifica-se em injetor e sobrejetor. Se a aplicação for injetora, então é chamado de *homomorfismo injetor*. Caso a aplicação seja sobrejetora, teremos um *homomorfismo sobrejetor*. E, quando a aplicação for bijetora se refere ao conceito de *isomorfismo*.

Exemplo 2.9: A aplicação $f: \mathbb{Z} \to \mathbb{Z}$ dada por $f(x) = Kx$, sendo $\mathbb{Z}$ o grupo aditivo dos inteiros e K um inteiro dado, temos que, f é um homomorfismo. Pois, temos $\mathbb{Z}$ um grupo inteiro aditivo, ou seja, $(\mathbb{Z}, +)$ para todo $x,\ y \in \mathbb{Z}$ e $f: \mathbb{Z} \to \mathbb{Z}$, teremos:

$$f(x + y) = K(x + y)$$

$$f(x + y) = Kx + Ky$$

$$f(x + y) = f(x) + f(y),$$

assim, podemos concluir que f é um homomorfismo de grupos.

Exemplo 2.10: A aplicação $f: \mathbb{Z} \to \mathbb{R}_+^*$ dada por $f(x) = 2^x$, sendo $\mathbb{Z}$ um grupo aditivo e $\mathbb{R}_+^*$ um grupo multiplicativo, temos que, f é um homomorfismo.

Pois, temos:

$$\mathbb{Z} = (\mathbb{Z}, +) \text{ e } \mathbb{R}_+^* = (\mathbb{R}_+^*, \bullet), \quad \forall\, x, y \in \mathbb{Z} \text{ então,}$$

$$f(x + y) = 2^{x+y}$$

$$f(x + y) = 2^x \bullet 2^y$$

$$f(x + y) = f(x) \bullet f(y),$$

Logo podemos concluir que f é um homomorfismo de grupos.

2.1.3 Classes Laterais

Considere $(G,*)$ um grupo, H um subgrupo de G, a um elemento de G e b um elemento de H.

Proposição 2.11: $i)$ A relação $\approx$ sobre G, definida por "$a \approx b$ se, e somente se, $a^{-1} * b \in H$" é uma relação de equivalência. $ii)$ Se $a \in G$, então a classe de equivalência determinada por a é o conjunto $aH = \{a * h \mid h \in H\}$.

Definição 2.12: Para cada $a \in G$, a classe de equivalência aH definida pela relação $\approx$, é chamada de *classe lateral à direita* módulo H em relação à a.

Dessa forma, temos que os subconjuntos $aH = \{a * b : b \in H\}$ e $Ha = \{b * a : b \in H\}$ correspondem, respectivamente, a *classe lateral à direita* módulo H em relação à a, e *classe lateral à esquerda* módulo H em relação à a.

Uma decorrência imediata da proposição anterior, é o conjunto de três propriedades de classes laterais, que determinam uma partição em G, ou seja:

i) se $a \in G$, então $aH \neq \emptyset$;

ii) se $a, b \in G$, então $aH = bH$ ou $aH \cap bH = \emptyset$;

iii) a união de todas as classes laterais é igual a G.

O conjunto quociente de G munido desta operação, denotado por G/H, é o conjunto das classes laterais aH $(a \in G)$. O próprio H é um elemento deste conjunto, já que $H = eH$.

Proposição 2.13: Seja *H* um subgrupo de *G*. Então duas classes laterais quaisquer módulo *H* são subconjuntos de *G* que têm a mesma cardinalidade.

Exemplo 2.14: Dado o subgrupo $H = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ no grupo aditivo $\mathbb{Z}_{12}$, suas classes laterais são $\mathbb{Z}_{12}|H = \{H, H+1, H+2\}$.
Pois,

$$\bar{0} + H = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} = H$$
$$\bar{1} + H = \{\bar{1}, \bar{4}, 7, \overline{10}\} = H + 1$$
$$\bar{2} + H = \{\bar{2}, \bar{5}, \bar{8}, \overline{11}\} = H + 2$$

logo, a união destas 3 classes laterais resulta no conjunto dos H.

Um subgrupo H de um grupo G recebe o nome de *subgrupo normal*, denotado por $H \lhd G$, se para todo elemento a pertencente a G, a classe lateral à direita for igual a classe lateral à esquerda módulo H, ou seja, satisfaz a seguinte igualdade

$$aH = Ha.$$

Se o grupo G é finito, temos que o conjunto G/H também é finito. Então, a quantidade de classes à direita e à esquerda é igual, esta quantidade recebe o nome de *índice* de H em G, indicada por $(G:H)$.

Em um grupo G, o subgrupo formado pelo elemento neutro, $\{e\}$, e pelo o próprio G são subgrupos triviais e são normais. O grupo G será chamado de *grupo simples* se seus únicos subgrupos normais forem $\{e\}$ e G.

Teorema 2.15: Seja G um grupo finito e $H \leq G$. Temos, $|G| = |H|(G:H)$, então, $|H|||G|$, ou seja, a ordem de H divide a ordem de G. (Lagrange)

Demonstração: Se G é um grupo finito então $\mathrm{G:H}$ é finito. Seja $(\mathrm{G:H}) = \mathrm{r}$, então, $\mathrm{G/H} = \{\mathrm{a_1H}, \mathrm{a_2H}, \dots, \mathrm{a_rH}\}$. Assim, temos que $\mathrm{G} = \{\mathrm{a_1H} \cup \mathrm{a_2H} \cup \dots \cup \mathrm{a_rH}\}$ e $\mathrm{a_iH} \cap \mathrm{a_jH} = \emptyset$ sempre que $\mathrm{i} \neq \mathrm{j}$. Também vimos que o número de elementos de cada uma das classes laterais é igual ao número de elementos de H, ou seja, igual a $|\mathrm{H}|$. Portanto, $|\mathrm{G}| = |\mathrm{H}| + |\mathrm{H}| + \cdots + |\mathrm{H}|$, onde o número de parcelas é $\mathrm{r} = (\mathrm{G:H})$. De onde, $|\mathrm{G}| = |\mathrm{H}|(\mathrm{G:H})$ e $|\mathrm{H}|||\mathrm{G}|$.■

2.2 ESPAÇOS MÉTRICOS

Nesta seção, é apresentado o conceito de espaço métrico, onde é possível definir as distâncias entre quaisquer elementos de um conjunto, sendo esta a medida que será adotada para o estudo e definição de propriedades neste trabalho.

Definição 2.16: Seja M um conjunto não vazio e $d = M \times M \to \mathbb{R}$ uma aplicação. Considere *d* uma *métrica* sobre M se satisfaz as seguintes condições:

i) $d(x,y) \geq 0 \; e \; d(x,y) = 0 \leftrightarrow x = y$;

ii) $d(x,y) = d(y,x)$;

iii) $d(x,y) \leq d(x,z) + d(z,y), \forall\, x,y,z \in M$.

Assim, podemos dizer que cada imagem $d(x,y)$ é a distância de x a y e o par (M,d) é um *espaço métrico*. Quando não houver possibilidade de dúvida diremos simplesmente "espaço métrico M".

Se (M,d) é um espaço métrico, então qualquer subconjunto $S \subset M$, pode ser naturalmente considerado um espaço métrico. Para tal, entre os elementos de S emprega-se a mesma distância que eles possuíam como elementos de M. Diante disso, S chama-se um *subespaço métrico* de M e a métrica de S é chamada de *métrica induzida* pela de M.

Como exemplo de um espaço métrico temos a reta, ou seja, o conjunto dos números reais $\mathbb{R}$, onde a distância entre dois pontos $x,y \in \mathbb{R}$ é obtida por $d(x,y) = |x-y|$.

2.3 ISOMETRIAS

Uma isometria é uma aplicação que preserva distâncias entre os pontos e as medidas dos ângulos, ou seja, formas e dimensões são invariantes. O conceito de código geometricamente uniforme, que será estudado no próximo capítulo, é definido através de grupos de isometrias.

Definição 2.17: Considere os espaços métricos M e N. Uma aplicação $\varphi: M \to N$ é uma *imersão isométrica* se

$$d(x,y) = d\big(\varphi(x), \varphi(y)\big), \quad \forall\, x,y \in M.$$

Toda imersão isométrica φ é uma aplicação injetiva, ou seja, transforma pontos distintos em pontos distintos. Se, além disso, φ for sobrejetiva, diremos que φ é uma *isometria* e os espaços métricos M e N são *isométricos.*

Proposição 2.18: Considere φ_1 e φ_2 isometrias entre espaços métricos, então, a composta $\varphi_1 \circ \varphi_2$ também é isometria.

Demonstração: Sejam as isometrias $\varphi_1: (N, d_N) \to (P, d_P)$ *e* $\varphi_2: (M, d_M) \to (N, d_N)$. *Para todo* $x, y \in M$, *então* $\varphi_2(x), \varphi_2(y) \in N$, *logo*

$$d_M(x,y) = d_N\big(\varphi_2(x), \varphi_2(y)\big) = d_P(\varphi_1(\varphi_2(x)), \varphi_1(\varphi_2(y))) =$$
$$d_P((\varphi_1 \circ \varphi_2)(x), (\varphi_1 \circ \varphi_2\,)(y))$$

Portanto, a aplicação composta $\varphi_1 \circ \varphi_2$ é uma isometria.■

Seja M um espaço métrico, o conjunto de todas as isometrias de M em M, munido da operação de composição de isometrias é um grupo que será denotado por $ISO(M)$.

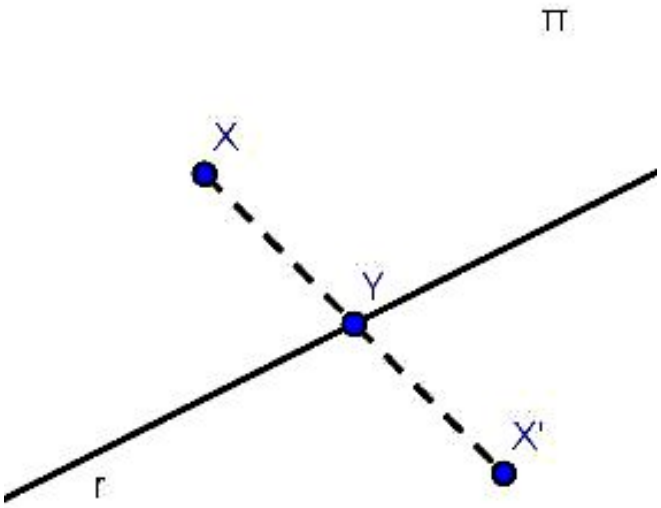
Outra proposição importante diz que toda e qualquer isometria é uma bijeção, com isso, temos que a sua inversa também é uma isometria.

Estas são algumas propriedades isométricas essenciais para o trabalho. Além disso, é de suma importância conhecer os tipos de isometrias existentes, que classificam-se em: reflexão, rotação, translação e reflexão deslizante. A identidade, denotada por Id, é a isometria mais evidente. A seguir, é apresentado cada uma delas considerando o espaço euclidiano.

Definição 2.19: Considere uma reta r, no plano Π, como eixo de simetria. A *reflexão* em torno de r é a função $R_r: \Pi \to \Pi$, definida por $R_r(X) = X$, $\forall\, X \in r$, e $\forall\, X \notin r$, $R_r(X) = X'$, tal que a reta r é a mediatriz do segmento $\overline{XX'}$, ou seja, X' é o simétrico de X em relação a r, e Y é o ponto médio de $\overline{XX'}$.

Na reflexão, a reta r é o eixo de simetria que divide a figura em duas partes que coincidem por sobreposição, porém, a orientação no plano é oposta. Esta situação pode ser representada ao posicionar-se em frente a um espelho, o reflexo formado do outro lado representa a transformação de reflexão sobre a pessoa, e o espelho pode ser considerado o eixo de simetria. Como exemplo temos a figura 1 a seguir.

Figura 1: Reflexão de um ponto em torno de uma reta



Fonte: Adaptado de Lima (1996)

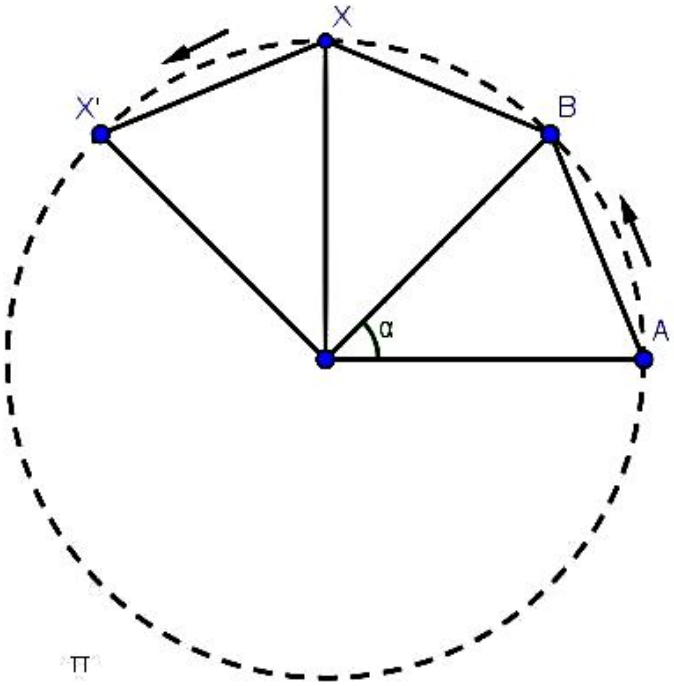
Definição 2.20: Considere O um ponto no plano Π e $\alpha = A\hat{O}B$ $(0 \leq \alpha < 2\pi)$ um ângulo de vértice O. Temos que a *rotação* de um ângulo α em torno de um ponto O é a função $\rho_{O,\alpha} : \Pi \to \Pi$, definida por, $\rho_{O,\alpha} : (O) = O$, e para todo $X \neq O$ em Π a função é definida por $\rho_{O,\alpha} : (X) = X'$, ponto de Π, onde

$$d(X, O) = d(X', O), \quad X\hat{O}X' = \alpha$$

O sentido de rotação de A para B equivale ao de X para X', e a condição $X\hat{O}X' = \alpha$, diz que dados os pontos A e B, se $\overline{0A} = \overline{0B} = \overline{0X} = \overline{0X'}$ então $\overline{AB} = \overline{XX'}$. Chama-se o ponto O de centro de rotação e o ângulo α de ângulo de rotação.

Desse modo, a rotação descreve um movimento circular, segundo um ângulo, que um objeto faz em torno de um eixo central, como pode ser observado na figura 2.

Figura 2: Rotação de um ponto em torno do eixo central



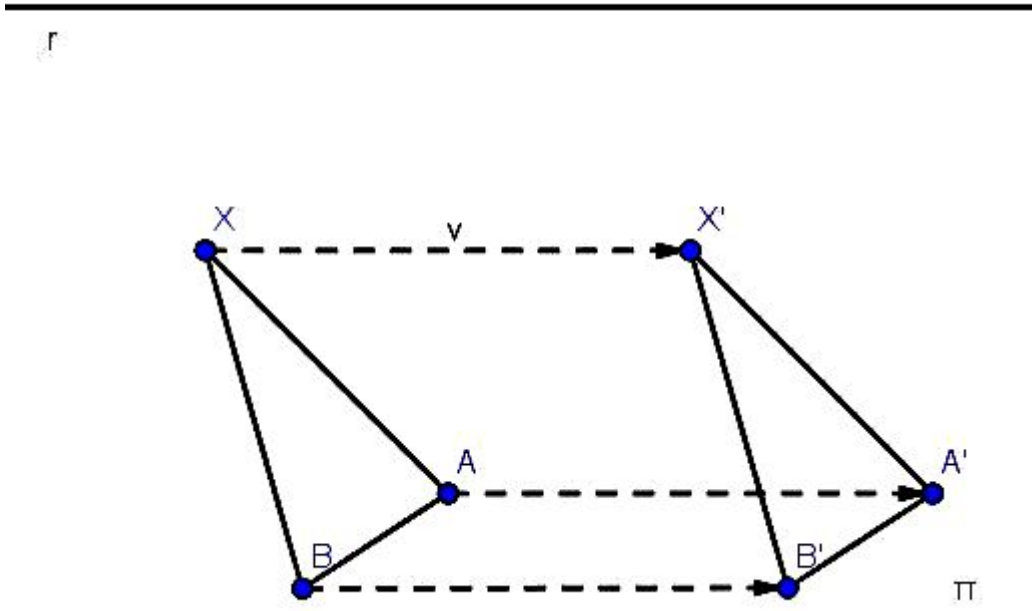
Fonte: Adaptado de Lima (1996)

Definição 2.21: Considere $\vec{v}$ um vetor do plano Π. Uma função que a cada ponto X de Π associa um ponto X' tal que $\overline{XX'} = \vec{v}$, é uma *translação* do vetor $\vec{v}$, denotada por $T_{\vec{v}}$. Pode ser escrita da seguinte forma,

$$T_{\vec{v}}(X) = X + \vec{v}\,.$$

Nesta isometria, a figura muda de posição se deslocando paralelamente em relação a uma reta. Assim, todos os seus pontos se deslocam em uma mesma distância, conforme mostra a figura 3.

Figura 3: Translação de um objeto paralelamente a uma reta

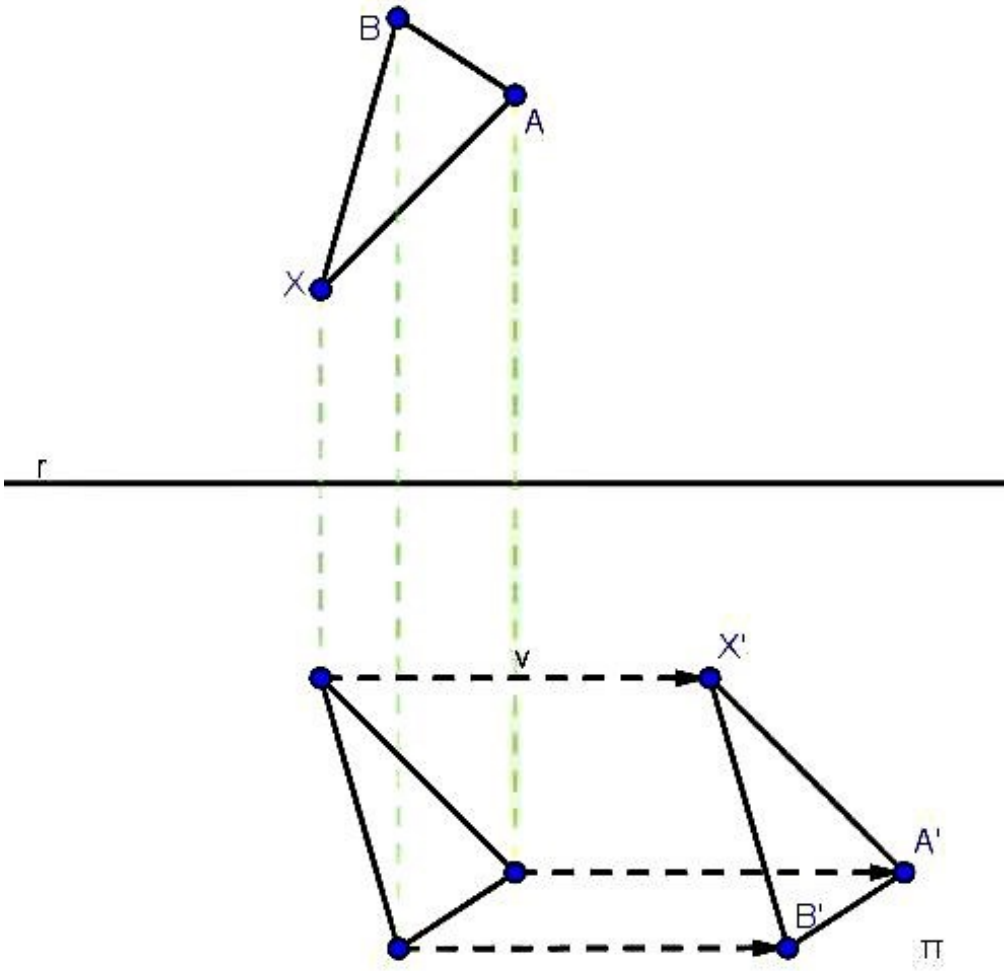


Fonte: Adaptado de Lima (1996)

Definição 2.22: Considere um vetor não-nulo $\vec{v}$ e uma reta r paralela a $\vec{v}$ no plano Π, a *reflexão deslizante* é a isometria $T = T_{\vec{v}} \circ R_r : \Pi \to \Pi$, dada pela reflexão R_r seguida da translação $T_{\vec{v}}$.

Nesta situação, a recíproca também é válida, como mostra a figura 4.

Figura 4: Reflexão deslizante



Fonte: Adaptado de Lima (1996)

3 SISTEMAS DE COMUNICAÇÃO DIGITAL, CÓDIGOS GEOMETRICAMENTE UNIFORMES E GRUPOS ALFABETOS GENERALIZADOS

Neste capítulo, inicialmente apresenta-se um breve resumo sobre os sistemas de comunicação digital, para um estudo mais aprofundado recomenda-se as referências (SHANNON, 1948; ABRANTES, 2003; SILVA, 2012). Em seguida, é definido o conceito de códigos geometricamente uniformes, para mais detalhes sobre este conteúdo indica-se (FORNEY, 1970; GOMES, 2017). E, encerra-se com a conceituação dos grupos alfabetos generalizados, este tema encontra-se em (BIGLIERI, 1988).

3.1 SISTEMAS DE COMUNICAÇÃO DIGITAL

Na era digital a área de telecomunicações vem crescendo rapidamente, em consequência dos serviços de transmissão e armazenamento de informação. Com isso, é essencial o constante desenvolvimento de sistemas de comunicação que ofereçam serviços de ótima qualidade, acompanhando a evolução tecnológica.

Estudos nesta área integram diversos ramos do conhecimento, como a computação, a matemática e algumas engenharias. Estes estudos são necessários para melhorar a eficiência da comunicação, que tem como objetivo transmitir uma informação de um lugar para outro, por meio de um processo. A mensagem ao ser transmitida, por melhor que o sistema de comunicação seja arquitetado, pode sofrer algumas perturbações ocasionadas pelas imperfeições do sistema, falha humana, ruídos ou interferências de sinais gerados por outras fontes. Desse modo, a mensagem ao chegar no seu destino pode estar modificada.

A teoria de códigos busca identificar e corrigir esses erros ocasionados durante o processo de transmissão de informação. Para compreender este campo de pesquisa é necessário conhecer o conceito de código e entender como a informação pode ser medida, fato essencial para que esta possa ser comparada, controlada e armazenada.

Um *código* é formado por um conjunto finito denominado *alfabeto*, que é composto por sequências finitas de símbolos, chamadas de *palavras-código* (MILIES, 2009).

Definição 3.1: Seja (M, d) um espaço métrico. Um código S é qualquer conjunto não vazio de M. Caso S seja discreto, então será chamado de *conjunto de sinais* (GOMES, 2017)**.**

Dado um espaço métrico (M, d). Suponha que em uma transmissão um ponto x, com interferência de um ruído, é transmitido como outro ponto y. O *erro*, denotado por ε, é distância entre os pontos x e y, ou seja,

$$\varepsilon = d(x, y).$$

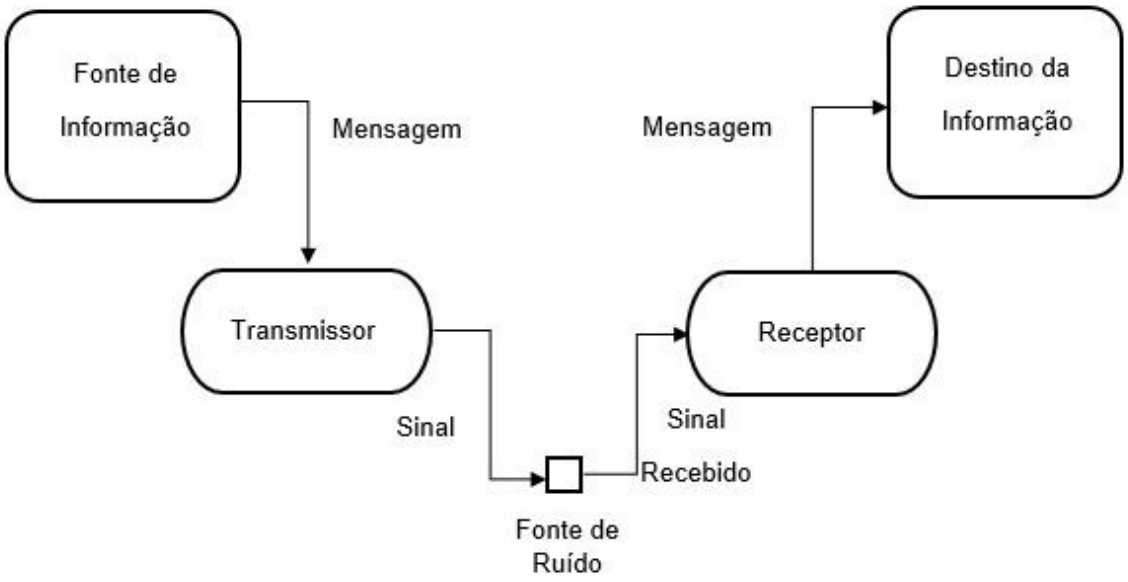
O processo de detecção e correção de erro em um código é chamado de *decodificação* (MILIES, 2009).

Os sistemas de comunicação estão divididos em analógico e digital. O sistema analógico transmite a informação através de pulsos eletrônicos, o sinal enviado é contínuo e varia em função do tempo. Enquanto no sistema digital, a informação é enviada por uma sequência de mensagens discretas. A mesma, é codificada, transmitida através de um canal e decodificada por meio de um dispositivo para que o receptor receba a informação original. Desta forma, neste sistema é possível corrigir erros que possam ter ocorrido durante a transferência da informação, garantindo a qualidade do sinal (GOMES, 2017).

Conhecido como o “pai da teoria da informação”, Claude Elwood Shannon, no ano de 1948 publicou o seu artigo intitulado “*A Mathematical Theory of Communication*”, onde ele apresentou uma teoria da informação que explica as transmissões de informações por meio de sistemas de comunicação com o intuito de corrigir erros entre a fonte e o destino da informação.

Em seus estudos, Shannon descreve como opera um sistema de comunicação digital e representa-o por um diagrama, conforme pode ser observado na figura 5.

Figura 5: Diagrama de um sistema de comunicação digital



Fonte: Adaptado de Shannon (1948)

Neste sistema, primeiramente uma mensagem digital é produzida pela fonte de informação, esta mensagem pode ser uma sequência de letras ou uma função, por exemplo. Ela é processada por um transmissor que age produzindo sinais adequadamente codificados para serem transmitidos através de um canal até o receptor. Então, o receptor realiza a decodificação e exibição da mensagem inicial. Esta, é reproduzida com possíveis ruídos devido a irregularidades do sistema e enviada ao seu destino. Para exemplificar a situação temos o sistema da telefonia, nesta operação a pressão do som é alterada e codificada em uma corrente elétrica proporcional, e o canal de transmissão seria os fios ou cabos (SHANNON, 1948).

Além da telefonia, mídias sociais, rádio, TV digital e sistema de armazenamento, são exemplos de sistemas de comunicação que codificam as informações transmitidas.

Estes sistemas estão divididos em: discreto, contínuo e misto. No sistema discreto a mensagem e o código são sequências de sinais discretos. Os sinais digitais são discretos, um bom exemplo é a telegrafia, onde a mensagem é uma sequência

de letras e o código uma sequência de pontos. No sistema contínuo o código é representado por funções contínuas. Os sinais analógicos são contínuos, neste caso podemos citar os microfones. Já no sistema misto há a junção das variáveis discretas e contínuas, como acontece com a transmissão PCM (modulação por código de pulso), que representa digitalmente um sinal analógico. Neste trabalho será considerado o sistema de comunicação discreto (SHANNON, 1948).

A *informação* compreende muitos significados e Shannon a definiu matematicamente como sendo uma redução da incerteza, baseando-se na ideia de que quanto mais esporádico um evento é, maior quantidade de informação ele transmite, ou seja, quanto maior a variabilidade dos sinais maior será a quantidade de informação ligada a fonte. A mesma, é medida como o número de possibilidades eliminadas em razão de todas as possíveis (SILVA, 2012).

Definição 3.2: Se a probabilidade de ocorrência do evento i em uma sequência de eventos for dada por P_i, então a *quantidade de informação* I_i associada ao evento i é,

$$I_i = \log\left(\frac{1}{P_i}\right)$$

Para calcular a quantidade de informação pode-se usar o logaritmo em qualquer base, desde que se use a mesma para todos os cálculos. Ela que determina a unidade de medida da quantidade de informação. Se for usada a base 2 a unidade é o bit, que representa o número de vezes que a informação eliminou metade das possibilidades totais do evento. Dessa forma, ao eliminar metade das alternativas um bit de informação é comunicado (SILVA, 2012).

Se há um conjunto de m símbolos diferentes em uma sequência de N símbolos a *probabilidade de ocorrência* de cada um dos m símbolos na sequência é definida por

$$Pi = \frac{Fi}{N}, \quad i = 1, 2, 3, \dots, m$$

A entropia é outra grandeza importante na teoria da informação, definida como a média da quantidade de informação contida em um conjunto de sinais. Segundo Silva (2012), é a medida estatística que representa a média que um transmissor comunica a cada mensagem que envia.

Definição 3.3: Dada uma fonte de informação x, um conjunto de mensagens P que x pode enviar e a probabilidade da i-ésima mensagem ser enviada P_i. A *entropia* da fonte x, denotada por $H(x)$, é calculada pela seguinte equação

$$H(x) = \sum_{i=i}^{k} P_i(-\log_2 P_i).$$

A entropia de um conjunto de símbolos é sempre positiva ou nula, ou seja, $H(x) \geq 0$. Será igual a zero quando um dos valores da sequência tiver probabilidade 1 e os demais probabilidades nulas.

Quando a distribuição dos m valores na sequência de N símbolos for uniforme, com $P_i = \left(\frac{1}{m}\right)$, temos o valor máximo da entropia, ou seja, é a maior incerteza sobre os valores de uma sequência.

Considere x a fonte que gera a mensagem e y o canal de transmissão, quando uma informação é transmitida de uma fonte para um receptor. $H(x)$, a entropia da informação da fonte, $H(y)$, a medida após trafegar o canal. E, a informação comum T é a parte da informação da fonte que de fato foi transmitida. Dessa forma, $H_y(x)$ é a informação média obtida da fonte x, a mensagem original, ou seja, a mensagem que faz parte da informação gerada na fonte que ainda não foi para o meio, enquanto, $H_x(y)$ é a informação que faz parte do canal que não fazia parte da mensagem original, representando o ruído. Enfim, a informação total que se pode obter das duas fontes, que inclui a informação transmitida, perdida e o ruído, é detonada por $H(x, y)$ (SILVA, 2012).

Os canais de transmissão de uma informação têm a capacidade limitada. Shannon apresentou a equação que mede a capacidade do canal.

Definição 3.4: Seja C a quantidade máxima de informação que o canal pode transmitir e L o limitante da informação média transmitida. Então, quando se aumenta a quantidade de informação gerada na fonte x, a informação transmitida L cresce até atingir a capacidade máxima do canal, conforme a seguinte equação

$$\lim_{H(x)\to\infty} L = C$$

Este cálculo fornece o valor máximo que se pode atingir, porém, se o valor real atinge ou não este valor vai depender da fonte de informação que alimenta o canal.

Segundo Abrantes (2003), a teoria da informação é baseada em três conceitos: capacidade de um canal de comunicações de transferir informação, medida da informação e a codificação. Estes conceitos relacionados formam o teorema a

seguir, que foi proposto por Shannon, e recebeu o nome de *Teorema Fundamental da Teoria da Informação.*

Teorema 3.5: Dado um canal de capacidade C e uma fonte com ritmo de informação R, então se $R \leq C$ existe uma técnica de codificação tal que a saída da fonte pode ser transmitida através do canal com uma frequência arbitrariamente pequena de erros, apesar da presença de ruído. Se $R > C$, não é possível a transmissão sem erros.

Shannon garantiu a possibilidade da codificação da informação transmitindo-a com uma probabilidade de erro mínima. A partir disso, diversas pesquisas surgiram buscando sistemas de comunicações que revelem altas taxas de transmissão e de capacidade de armazenamento, apresentando também baixa taxa de erros.

3.2 CÓDIGOS GEOMETRICAMENTE UNIFORMES

Esta seção fornece a definição dos códigos geometricamente uniformes e seus primeiros resultados baseados nas ideias de Forney, um estudo mais aprofundado pode ser feito ao consultar a referência (FORNEY, 1970).

Segundo Carvalho (2001), o método mais eficaz de composição das sequências finitas de símbolos que formam os códigos é aquele no qual os símbolos são determinados por elementos de um conjunto que carregam uma estrutura algébrica.

Este método de determinação dos elementos é por meio de uma aplicação injetora de um subconjunto finito de pontos de um espaço de sinais em uma estrutura algébrica, de outra maneira, identificando a representação geométrica relacionada à estrutura algébrica obtendo a caracterização do alfabeto do código, se tal caso ocorre o subconjunto finito de pontos é geometricamente uniforme (CARVALHO, 2001). Com isso, estes conjuntos de sinais dão origem aos Códigos Geometricamente Uniformes.

A princípio, no modelo de comunicação chamado Canal Gaussiano, onde as mensagens transmitidas são representadas por vetores no espaço euclidiano, Slepian (1968) estudou os Códigos de Grupos e descreveu suas propriedades notáveis. Forney une este conceito aos Códigos Reticulados, que são conjuntos infinitos de pontos dispostos de forma regular e formados através de uma técnica de alocação de pontos, desenvolvendo assim uma única classe de códigos, que são os Códigos Geometricamente Uniformes. Nesta generalização, há a ação transitiva de um grupo

ao gerar estes códigos, e além disso, considera todas as isometrias do espaço (GOMES, 2017).

Considere (M, d) um espaço métrico e S um conjunto de sinais.

Definição 3.6: Uma isometria f que deixa S invariante, ou seja, $f(S) = S$, é uma *simetria* de S.

Definição 3.7: As simetrias de S, formam um grupo sob a composição de funções, que é chamado de *grupo de simetrias*, denotado por $\Gamma(S)$.

Definição 3.8: Um conjunto de sinais S definido sobre um espaço métrico (M, d) é um *Código Geometricamente Uniforme* se, dados quaisquer dois pontos s_1 e s_2 em *S*, existe uma isometria $u_{s_1,s_2}: \mathrm{M} \to \mathrm{M}$ que transforma s_1 em s_2 enquanto

$$u_{s_1,s_2}(S) = S$$

Então, S é geometricamente uniforme se a ação do grupo de simetrias $\Gamma(S)$ de S é transitiva. Chamaremos um Código Geometricamente Uniforme de *CGU* para facilitar a notação.

Um conjunto de sinais geometricamente uniforme, denotado por S, é uma *constelação uniforme* se este conjunto for *finito*, caso S seja *infinito* será chamado de *reticulado uniforme.*

Definição 3.9: Dado um código geometricamente uniforme S. Um grupo gerador mínimo $U(S)$ de S é um subgrupo do grupo de simetrias de S que satisfaz $\forall s_0 \in S$

$$S = \{\mu(s_0), \mu \in U(S)\}$$

e a função $m : U(S) \to S$, dada por $m(\mu) = \mu(s_0)$ é injetora.

Há códigos geometricamente uniformes que não têm grupo gerador mínimo. E, também aqueles que admitem mais que um grupo gerador minimal que não são isomorfos entre si.

Definição 3.10: Uma partição geometricamente uniforme, denotada por S/S', é uma partição de um conjunto de sinais geometricamente uniforme S, com um grupo gerador $U(S)$ que é induzido por um subgrupo normal $U'(S)$ de $U(S)$. Os elementos da partição S/S', são subconjuntos de S que correspondem às classes laterias de $U'(S)$ em $U(S)$.

Teorema 3.11: Seja S/S' uma partição geometricamente uniforme. Então os subconjuntos de S na partição são geometricamente uniformes, mutuamente congruentes e tem $U'(S)$ como grupo gerador em comum.

Um grupo de rótulos para uma partição geometricamente uniforme S/S' é um grupo isomorfo ao grupo quociente $U(S)/U'(S)$, estes, $U(S)$ e $U'(S)$ são os grupos geradores de S e S', respectivamente.

Definição 3.12: Seja G um grupo de rótulos para uma partição $U(S)/U'(S)$. Um rotulamento isométrico é uma aplicação injetiva $m: G \rightarrow S/S'$ obtida pela composição do isomorfismo entre G e $U(S)/U'(S)$ e a aplicação injetiva induzida por m à $U(S)/U'(S)$ em S/S'.

Proposição 3.13: Uma partição S/S' admite um rotulamento isométrico por um grupo G se:

i) S é geometricamente uniforme;

ii) seus subconjuntos são geometricamente uniformes e mutuamente congruentes;

iii) existem grupos de isometrias $U(S)$ e $U'(S)$ tais que $U(S)$ é um grupo gerador de S, $U'(S)$ é um grupo gerador comum dos subconjuntos de S, normal em $U(S)$ e S é isomorfo a $U(S)/U'(S)$.

3.2.1 Rotulamento Casado

Rotulamento casado, que é outro conceito de suma importância para o trabalho, foi criado por Hans Loeliger (1991) no mesmo período em que os CGUs foram desenvolvidos. Nesta seção são apresentados os seus principais resultados.

Os códigos geometricamente uniformes geram na maioria das vezes classes de bons códigos de espaços de sinais, apresentando uniformidade geométrica, regiões congruentes, grupo gerador isomorfo a um grupo de permutação transitivo, entre outras propriedades vantajosas (SILVA, 2015).

Nesses códigos, a estrutura do grupo gerador pertence ao grupo de simetrias, onde o mapeamento induz uma estrutura de grupos no conjunto de sinais que é isomorfa ao grupo gerador, assim, o processo de mapeamento requer a técnica de rotulamento casado (SILVA, 2015).

Em princípio, dizemos que um código é rotulado por um grupo de simetrias, se este grupo age livre e transitivamente, ou seja, durante a ação do grupo em um conjunto inicial não vazio, será livre se o elemento neutro for o único elemento do grupo, e, transitiva se entre a ação de cada par pertencente ao conjunto inicial existir

um único ponto no grupo que corresponde a um dos elementos do par em questão. Além disso, o objetivo principal é fornecer uma estrutura algébrica para códigos não-lineraes (ALVES, 2002).

Definição 3.14: Diz-se que um conjunto de sinais S de (M, d) é casado a um grupo $(G,*)$ se existe uma aplicação m de G em S em que, para todo g e h em G,

$$d\big(m(g), m(h)\big) = d(m(g^{-1} * h); m(e)),$$

onde e é o elemento neutro de G. Se m satisfaz esta condição, então m é uma *aplicação casada*. No caso em que m for injetiva então m^{-1} é chamado de *rotulamento casado*.

Lema 3.15: Considere m uma aplicação tal que o conjunto de sinais S de (M, d) esteja casado a um grupo G e $x_e = m(e)$. Se $H = m^{-1}(x_e)$ então H é um subgrupo de G e, também, $m(g) = m(g') \leftrightarrow gH = g'H$ para qualquer g, g' em G. Isto é, g e g' pertencem a mesma classe lateral à esquerda de H em relação à G.

Definição 3.16: Seja m uma aplicação que torna S um conjunto de sinais casado a um grupo G e H um subgrupo normal de G. Então, diz-se que a aplicação m é *efetivamente casada* se H não contém subgrupos normais não triviais de G. Neste caso, diz-se que S e G são *efetivamente casados*.

Temos ainda, que S é casado ao quociente G/H, além disso, S está efetivamente casado ao grupo quociente G/N, em que N é o maior subgrupo normal de G contido em H.

Teorema 3.17: Se o conjunto de sinais S de M está casado com G e $f: S \to f(S)$ é uma isometria, então $f(S)$ também está casado com G.

Proposição 3.18: Seja um conjunto de sinais S casado a um grupo G por meio da aplicação casada $m: G \to S$ se, e somente se, G é homomorfo a um subgrupo transitivo de $\Gamma(S)$, o grupo de simetrias de S.

Corolário 3.19: Existe um rotulamento casado entre o conjunto de sinais S e o grupo G se, e somente se, G é isomorfo a um subgrupo transitivo de $\Gamma(S)$.

Corolário 3.20: Se um conjunto de sinais S está efetivamente casado a um grupo G, então G é isomorfo a um subgrupo transitivo de $\Gamma(S)$, o grupo de simetrias de S.

Apesar de Forney e Loeliger, em seus trabalhos considerarem apenas o espaço métrico euclidiano, os resultados são verdadeiros independentemente do espaço métrico adotado. Estudos desse tema já foram realizados utilizando espaços

métricos não-euclidianos, como pode ser encontrado nas referências (LAZARI, 2000; GOMES, 2017).

A seguir, serão apresentados três exemplos de CGUs formados por diferentes isometrias.

Exemplo 3.21: Considere o ponto $s_1 = (1,\ 0)$ definido sobre $\mathbb{R}^2$ e uma rotação de 90° aplicada neste ponto. Após 4 aplicações da isometria obtenha o conjunto de sinais S.
Dado um ponto $s_1 = (1,\ 0)$ definido sobre $\mathbb{R}^2$,

Precisamos,

$$u_{s1s2}(S) = S$$

Definimos,

$$u_{s1s2}\colon \mathbb{R}^2 \to \mathbb{R}^2$$

Aplicando quatro rotações de 90°:

$$u(x,\ y) : (x\cos\theta - y\sin\theta\ ,\ x\sin\theta + y\cos\theta)$$

$$u(1,\ 0) : (1\cos 90° - 0\sin 90°\ ,\ 1\sin 90° + 0\cos 90°) = (0,\ 1)$$

$$u(0,\ 1) : (0\cos 90° - 1\sin 90°\ ,\ 0\sin 90° + 1\cos 90°) = (-1{,}0)$$

$$u(-1,\ 0) : (-1\cos 90° - 0\sin 90°\ ,\ -1\sin 90° + 0\cos 90°) = (0,-1)$$

$$u(0,\ -1) : (0\cos 90° + 1\sin 90°\ ,\ 0\sin 90° - 1\cos 90°) = (1{,}0)$$

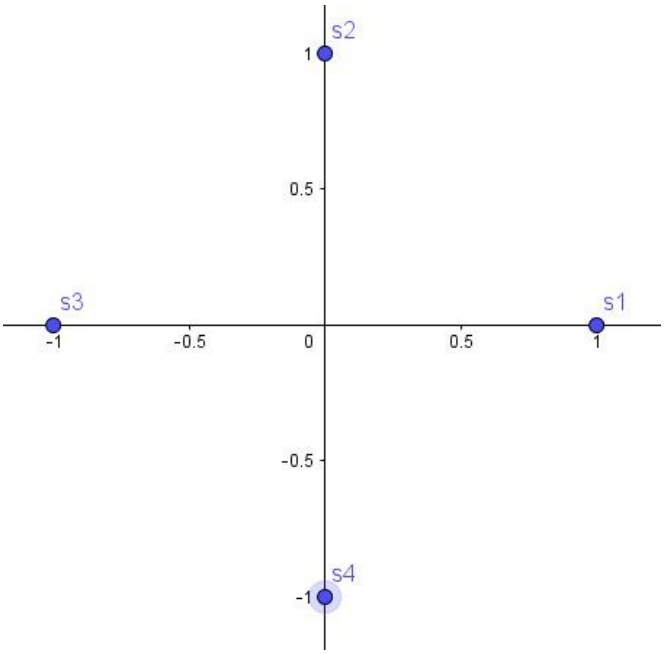
$$Logo, \mathrm{S} = \{(0,\ 1),\ (-1,\ 0),\ (0,-1),\ (1,\ 0)\}$$

Então, temos que

$$\mathrm{S} = \{(0,\ 1),\ (-1,\ 0),\ (0,-1),\ (1,\ 0)\}\ \text{é}\ um\ CGU.$$

O resultado pode ser observado na Figura 6.

Figura 6: Exemplo 3.21 da isometria rotação



Fonte: Autoria própria

Em seguida, utilizando os mesmos dados será apresentado um exemplo de CGU em que a aplicação utilizada é uma translação.

Exemplo 3.22: Considere o ponto $s_1 = (1,\ 0)$ definido sobre $\mathbb{R}^2$ e aplique a seguinte isometria $T(x,\ y) : (x,\ y + 1)$, obtendo o conjunto de sinais S.

Dado o ponto $s_1 = (1,\ 0)$ definido sobre $\mathbb{R}^2$,

Precisamos,

$$u_{s1s2}(S) = S$$

Definimos,

$$u_{s1s2}\colon \mathbb{R}^2 \to \mathbb{R}^2$$

Aplicando a translação dada:

$$(x,\ y) : (x,\ y + 1)$$

$$u(1,\ 0) : (1,\ 0 + 1) = (1,\ 1) = s_2$$

$$u(1,\ 1) : (1,\ 1 + 1) = (1,\ 2) = s_3$$

$$u(1,\ 2) : (1,\ 2 + 1) = (1,\ 3) = s_4$$

$$\vdots$$

$$u(1,\ n) : (1,\ n+1) = (1,\ n+1) = s_m$$

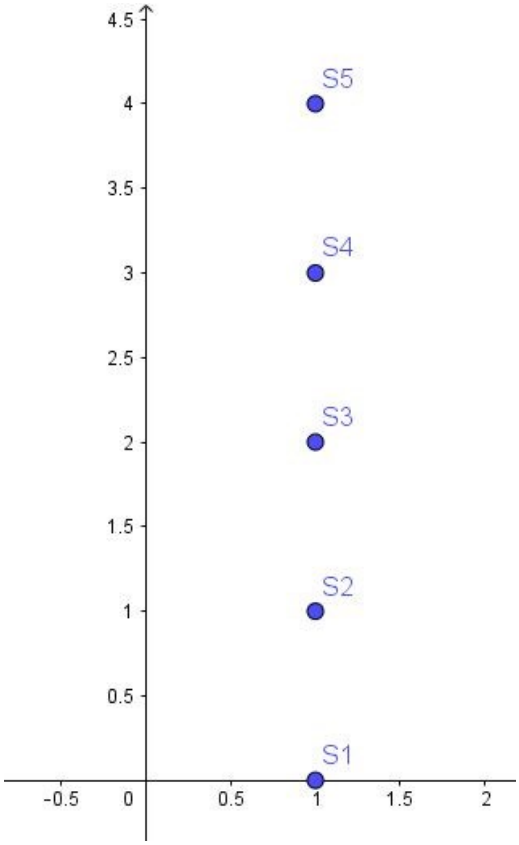
$$S = \{(1,\ 0),\ (1,\ 1),\ (1,\ 2),\ (1,\ 3), \ldots\}$$

Então,

$S = \{(1,\ 0),\ (1,\ 1),\ (1,\ 2),\ (1,\ 3), \ldots\}$ é um CGU

Este resultado pode ser observado na Figura 7.

Figura 7: Exemplo 3.22 da isometria translação



Agora, será apresentado um exemplo de CGU por meio de uma aplicação de reflexão no eixo y.

Exemplo 3.23: Considere o ponto $s_1 = (1,\ 0)$ definido sobre $\mathbb{R}^2$, aplique a isometria $R(x,\ y) : (-x,\ y)$, obtendo o conjunto de sinais S.

Dado o ponto $s_1 = (1,\ 0)$ definido sobre $\mathbb{R}^2$,

Precisamos,

$$u_{s1s2}(S) = S$$

Definimos,

$$u_{s1s2}\colon \mathbb{R}^2 \to \mathbb{R}^2$$

Aplicando a reflexão dada:

$$(x,\ y) : (-x,\ y)$$

$$u(1,\ 0) : (-1,\ 0) = s_2$$

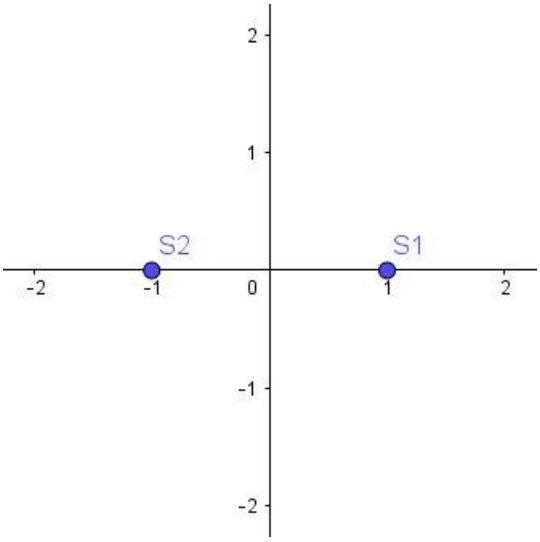
$$u(-1,\ 0) : (1,\ 0) = (1,\ 0) = s_3$$

$$S = \{(1,\ 0),\ (-1,\ 0)\}$$

obtemos S, que é um CGU.

O resultado pode ser observado na Figura 8.

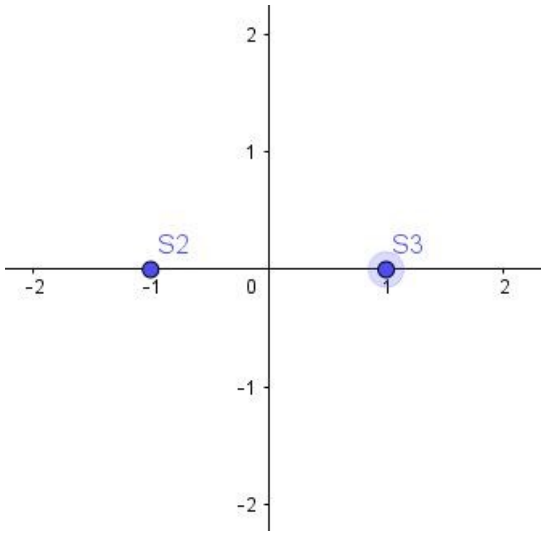
Figura 8: Exemplo 3.23 de CGU operando na primeira reflexão



Fonte: Autoria própria

Nota-se pela Figura 9, que ao realizar uma segunda reflexão será obtido novamente o ponto $(1,\ 0)$.

Figura 9: Exemplo 3.23 de CGU operando na segunda reflexão



Fonte: Autoria própria

Note que nos exemplos anteriores de CGU, vimos um exemplo de cada isometria e que em cada exemplo o conjunto inicial é sempre formado por apenas um elemento.

3.3 GRUPOS ALFABETOS GENERALIZADOS

Esta seção apresenta o conceito grupos alfabetos generalizados, sua definição e principais resultados. Para um estudo mais detalhado desta teoria recomenda-se a referência (BIGLIERI, 1988), que fundamenta quase que por completo esta seção.

Em seu trabalho intitulado Multidimensional Modulation and Coding for Band-Limited Digital Channels, Biglieri introduziu uma classe de sinais multidimensionais fundada no que chamamos de grupos alfabetos generalizados (GAG). Esta classe generaliza os “códigos de grupo” de Slepian e exibem, como característica principal, um grau de simetria bem significativo.

De acordo com Biglieri (1988), os GAGs compõem uma vasta família de códigos, a maioria dos bons alfabetos que foram propostos para trabalhar em espaço multidimensional pertencem a essa classe.

A seguir, serão mostradas as propriedades básicas e principais características desses códigos.

Considere um conjunto n-dimensional de k vetores, denotado por $X = \{x_1, \dots, x_k\}$, que será chamado de conjunto inicial. E, L matrizes nxn ortogonais, $S_1, \dots, S_n$, que formam um grupo G finito sob multiplicação.

Definição 3.24: O conjunto de vetores $Gx_1, Gx_2, \dots, Gx_k$, obtido a partir da ação de G nos vetores do conjunto inicial é chamado de *grupo alfabeto generalizado* e G é seu *grupo gerador*.

Definição 3.25: Um GAG é chamado *separável* se os vetores do conjunto inicial forem transformados por G em conjuntos vetoriais disjuntos ou coincidentes, ou seja, para todo $x_j \in X$ tal que $Gx_j \neq \emptyset$, temos:

$$Gx_j \cap Gx_k \neq \emptyset \rightarrow Gx_j = Gx_k, \ \forall\, x_j, x_k \in X$$

Definição 3.26: Um GAG é chamado *regular* se o número de vetores em cada sub-alfabeto $Gx_j,\ j = 1, \dots, k,$ não depende de j, ou seja, cada vetor do conjunto inicial é transformado por G no mesmo número de vetores distintos. Um GAG regular é chamado *fortemente regular* se cada conjunto Gx_j conter exatamente k vetores distintos.

Com base nessas definições temos os resultados a seguir.

Proposição 3.27: Seja S, formado por um conjunto de vetores, um GAG regular múltiplo de k. Se o GAG for fortemente regular, então $|S| = |X|k$.

Agora, serão apresentadas algumas propriedades de distância dos elementos de um grupo alfabeto generalizado. Escolha uma partição do código em m subconjuntos $Z_1, Z_2, \dots, Z_m$. Para cada subconjunto Z_i, podemos definir o *conjunto de intradistância* como o conjunto de todas as distâncias euclidianas entre pares de vetores em Z_i. Para qualquer par de subconjuntos distintos Z_i, Z_j, definimos o *conjunto de interdistância* como sendo o conjunto de todas as distâncias euclidianas entre um vetor no subconjunto Z_i e um vetor em Z_j.

Definição 3.28: A partição de um GAG separável em m subconjuntos $Z_1, Z_2, \dots, Z_m$ é chamada de *justa* se todos os seus subconjuntos são distintos, possui o mesmo número de vetores e seus conjuntos de intradistância são iguais.

Agora, é exibido um método construtivo para gerar partições justas de um GAG. Considere G um grupo gerador do GAG, H um de seus subgrupos, e a partição de G na classe lateral esquerda de H. Assim, teremos o seguinte resultado.

Teorema 3.29: Se as classes laterais esquerdas do subgrupo H são aplicadas ao conjunto inicial de um GAG fortemente regular, esse procedimento resulta em uma partição justa do GAG. Da mesma forma, se H é um subgrupo normal, então as classes laterais esquerdas e direitas dão origem à mesma partição justa.

A demonstração deste teorema pode ser encontrada em (Biglieri, 1988).

Teorema 3.30: Seja H um subgrupo normal de G. A partição de um GAG fortemente regular obtida pela aplicação das classes laterais esquerdas de H ao conjunto inicial X tem a seguinte propriedade: o conjunto de intradistância associado a quaisquer duas classes laterais, digamos S_1H e S_2H, é uma função apenas da classe lateral S_3H, onde $S_3 = S_1^T S_2$ e não de S_1, S_2 separadamente.

Demonstração: Sejam S_1 e S_2 duas clases laterais, X_i, X_j dois subconjuntos de vetores (não necessariamente distintos) do conjunto inicial X, e S_h, S_k dois elementos de H, as distâncias entre os elementos das classes laterais S_1H e S_2H são

$$d_{ij}(S_1, S_2, S_h, S_k) \triangleq \|S_1 S_h X_j - S_2 S_k X_i\|$$

como S_h, S_k passam por H e X_i, X_j passam por X. Nós temos

$$d_{ij}{}^2(S_1, S_2, S_h, S_k) = \left\|X_j\right\|^2 + \|X_i\|^2 - 2X_j^T S_h^T S_1^T S_2 S_k X_i$$

$$= \left\|X_j\right\|^2 + \|X_i\|^2 - 2X_j^T S_h^T S_3 S_k X_i$$

Finalmente, como H é um subgrupo normal, temos

$$S_1 H S_2 H = S_1 S_2 H = S_3 H;$$

isto é, S_3H é outra classe lateral.■

Definição 3.31: Seja R uma classe lateral esquerda de G em uma partição justa de um GAG e S_g, um elemento de G. Definimos o *perfil de distância* associado a R e S_g, como o polinômio a indeterminada w:

$$F(w, S_g, R) \triangleq \sum_{d^2} a(d^2)\, w^{d^2}$$

onde $a(d^2)$ é o número de elementos de RX que têm a distância ao quadrado d^2 em relação a um elemento do conjunto S_gRX. Um determinado elemento de RX pode ser contado mais de uma vez, pois contribui com distâncias quadradas diferentes em relação a elementos diferentes do conjunto S_gRX. A soma de $a(d^2)$ é igual ao quadrado da cardinalidade de RX.

Definição 3.32: Uma partição justa de um GGA é chamada de *homogênea* se o conjunto $\{F(w,S,R)\}_{S\in G}$ não depende de R. E, chamada de *fortemente homogênea* se $F(w,S,R)$ não depende de R para qualquer S.

Teorema 3.33: Se G é um grupo comutativo, todas as partições geradas por seus subgrupos são fortemente homogêneas.

Demonstração: Tomemos H como sendo um subgrupo de G, e a partição induzida por H é justa. Seja, X_i, X_j dois elementos do conjunto inicial X, S um elemento de G, S_H um elemento de H. Então, para qualquer $S_g \in G$, o cálculo de $F\ (w, S_g, SH)$ envolve enumerar as distâncias quadradas.

$$\|SS_HX_i - S_g\ SS_1HX_j\|^2 = \|SS_HX_i - SS_g\ S_{1H}X_j\|^2$$
$$= \|S_HX_i - S_g\ S_{1H}X_j\|^2$$

que não dependem de S, e portanto, do elemento da partição justa.■

Teorema 3.34: Se H é um subgrupo de G em um GGA fortemente regular, a partição gerada pela classes laterais esquerda de H é homogênea.

Caso o leitor deseje consultar, este teorema foi demonstrado em (Biglieri, 1988)

Em seguida, será exibido um exemplo de grupo alfabeto generalizado, onde o conjunto inicial utilizado é formado por dois pontos e a isometria aplicada é a reflexão.

Exemplo 3.35: Considere $X = \{(1,\ 0),\ (0,\ 1)\}$ o conjunto inicial definido sobre R^2 e $G = \left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\right\}$ um grupo formado por matrizes ortogonais. A partir da ação de G em X, sob a operação multiplicação, é gerado o conjunto de sinais S que corresponde a um GAG.

Sejam,

$$X = \{(1,\ 0),\ (0,\ 1)\}\ e\ G = \left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\right\}$$

um grupo, onde cada matriz é ortogonal. Então,

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix} \qquad \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix}$$

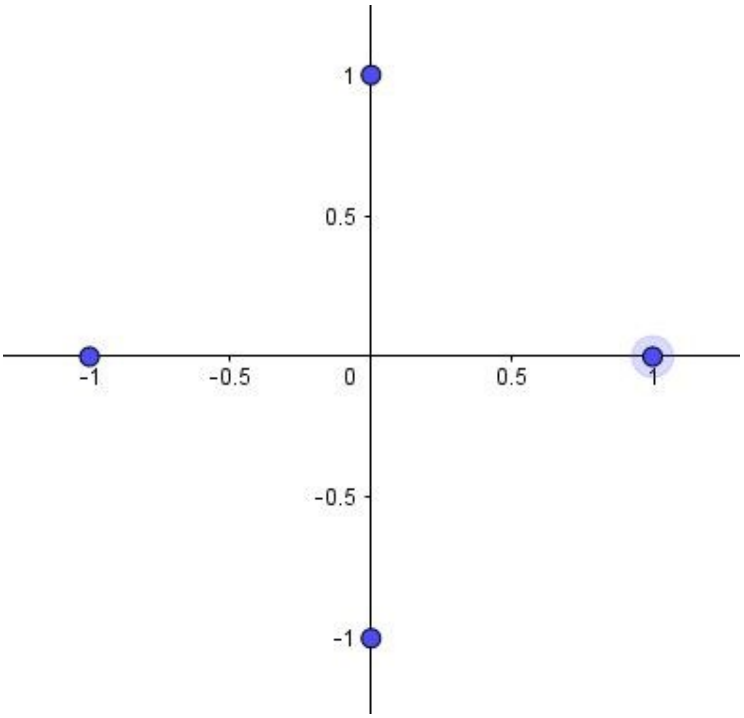
$$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix} \qquad \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \begin{bmatrix}0\\ -1\end{bmatrix}$$

$$\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}-1\\ 0\end{bmatrix} \qquad \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix}$$

$$\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}-1\\ 0\end{bmatrix} \qquad \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \begin{bmatrix}0\\ 1\end{bmatrix}$$

Logo, para $X = \{(1, 0), (0, 1)\}$, temos o conjunto de sinais $S = \{(-1, 0), (1, 0), (0, 1), (0, -1)\}$ que é um GAG. Este resultado pode ser observado na Figura 10.

Figura 10: Exemplo 3.35 de GAG



Fonte: Autoria própria

4 GRUPO ALFABETO GENERALIZADO ENUMERÁVEL

Este capítulo apresenta o conceito de grupo alfabeto generalizado enumerável, também chamado de GAGE, sua definição, características e propriedades iniciais que foram desenvolvidas durante o estudo. Além disso, é feito um comparativo entre esta nova teoria, os códigos CGUs e os GAGs, destacando as vantagens de se trabalhar com os GAGEs. Por fim, é fornecido um exemplo que permite uma melhor compreensão do comportamento desses códigos.

4.1 GRUPO ALFABETO GENERALIZADO ENUMERÁVEL

A proposta deste trabalho é unificar o conceito de código geometricamente uniforme criado por Forney, em seu trabalho *Geometrically Uniforme Codes*, e as ideias de grupo alfabeto generalizado, desenvolvidas por Biglieri no trabalho intitulado *Multidimensional Modulation and Coding for Band-Limited Digital Channels*.

Ambos os autores vislumbraram nos trabalhos supracitados, possibilidades de generalização dos conceitos por eles desenvolvidos. O presente trabalho foi elaborado de forma a atender essas ideias de generalização sugeridas.

O conceito original de CGU faz uso de um único ponto inicial para gerar todo o conjunto de sinais, amplia-se este aspecto baseando-se na ideia de Biglieri de usar múltiplos pontos. Assim, ao invés de termos somente um ponto inicial, serão usados conjuntos que têm uma quantidade enumerável de pontos, extrapolando desta forma, a própria definição de GAG que utiliza conjuntos iniciais finitos.

Em relação ao grupo gerador dos códigos usa-se as isometrias ao invés de considerar apenas rotações, reflexões e a identidade, como ocorre com a técnica de grupo alfabeto generalizado, ou seja, neste novo método as translações também são consideradas, aproximando-se mais, neste aspecto, do conceito de código geometricamente uniforme.

Os autores mencionados anteriormente restringem seus trabalhos ao espaço euclidianos, porém, neste estudo considera-se todo o espaço métrico.

No quadro 1 é possível observar as principais características destacadas em cada técnica.

Quadro 1: Principais características de cada técnica

CONCEITO	CONJUNTO INICIAL	GRUPO GERADOR	ESPAÇO
CGU	Um único ponto	Isometrias	Euclidiano
GAG	Conjunto de pontos finitos	Rotação, reflexão, identidade	Euclidiano
GAGE	Conjunto de pontos enumerável	Isometrias	Espaço Métrico

Fonte: Autoria própria

Com estas considerações inicia-se a construção de um conceito mais amplo, o qual será chamado de grupo alfabeto generalizado enumerável, ou GAGE.

Discorreremos agora, as noções iniciais e os principais resultados desta nova abordagem, que serão suficientes para deixar clara a relação entre o novo conceito e os conceitos anteriores nos quais ele se baseia.

Considere (M, d) um espaço métrico qualquer. Seja $X = \{x_1, x_2, \dots, x_k, \dots\}$ um conjunto inicial enumerável não vazio de M e $G = < g_1, g_2, \dots, g_n, \dots >$ um grupo de isometrias finitamente gerado por $ISO(M)$, com respeito a operação de composição.

Definição 4.1: Um subconjunto S de M formado pelos elementos GX obtidos pela ação de G sobre o conjunto X é chamado de *grupo alfabeto generalizado enumerável.* O conjunto X é chamado *conjunto inicial* e G é chamado *grupo gerador*.

Considerar grupos finitamente gerados traz uma grande vantagem no trabalho com isometrias em espaços hiperbólicos, pois os grupos de isometrias destes espaços que estão relacionados a rotulamentos de constelações de sinais geometricamente uniforme apresentam tal característica. Mais ainda, esta abordagem torna possível o uso da métrica da palavra para o grupo G.

No que diz respeito ao conjunto X, considerá-lo enumerável possibilita considerar grupos de ordem finita mesmo em casos onde o conjunto de sinais é infinito, assim, facilita a criação de rotulamentos casados para códigos.

Esta definição é mais abrangente do que a proposta por Biglieri, essencialmente porque G admite também translações além das rotações, reflexões e a identidade, também por aceitarmos que o conjunto inicial possa ser enumerável e o

conjunto gerador finitamente gerado. Mais ainda, a atual abordagem é construída para um espaço métrico qualquer, em particular, vale também para o espaço métrico euclidiano.

Definição 4.2: Se G for um grupo finito, então S será chamado de *finitamente gerado*.

Definição 4.3: Se X for um conjunto finito, então S será chamado de *inicialmente finito*.

Proposição 4.4: Se $S = GX$ for finitamente gerado e inicialmente finito com $M = E$, então S é $GAGE$.

Ao assumirmos que G *é* finito estamos implicitamente eliminando as translações do grupo.

Definição 4.5: Um $GAGE$ é chamado *separável* se os elementos de seu conjunto inicial são transformados por G em conjuntos vetoriais disjuntos ou coincidentes, isto é, para todo $x_j \in X$ tal que $Gx_j \neq \emptyset$, temos:

$$Gx_j \cap Gx_k \neq \emptyset \rightarrow Gx_j = Gx_k, \ \forall\, x_j, x_k \in X$$

Definição 4.6: Um $GAGE$ é dito *regular* se o número de elementos em cada órbita Gx_j independe de j, isto é, cada elemento do conjunto inicial é transformado por G em um conjunto com a mesma cardinalidade.

Definição 4.7: Um $GAGE$ regular é dito *fortemente regular* se $|Gx_j| = |G|$, ou seja, todas as órbitas têm a mesma cardinalidade de G.

Definição 4.8: Um grupo gerador minimal $U(S)$ de S é um subgrupo do grupo de simetrias de S, tal que $U(S)$ é capaz de gerar S_i para todo i a partir de um ponto inicial s_0 em S de modo que $m: U(S) \rightarrow S$, definida por $m(\mu) = \mu(s_0)$ seja bijetiva.

Considere (M, d) um espaço métrico qualquer. Seja $X = \{x_1, x_2, \dots, x_k, \dots\}$ um conjunto inicial enumerável não vazio de M e $G = < g_1, g_2, \dots, g_n, \dots >$ um grupo de isometrias finitamente gerado por $ISO(M)$, com respeito a operação de composição.

Definição 4.9: Um subconjunto S de M formado pelos elementos GX obtidos pela ação de G sobre o conjunto X é chamado de *grupo alfabeto generalizado enumerável.* O conjunto X é chamado *conjunto inicial* e G é chamado *grupo gerador*.

Exemplo 4.10: Considere $X = \{(1, 0), (1, 1)\}$ definido sobre $\mathbb{R}^2$, o conjunto inicial. Obtenha S, o grupo alfabeto generalizado enumerável, formado a partir de $f(x, y) = (x + 1, y)$.

Primeiramente, é necessário encontrar as seguintes aplicações,

$$f(x, y) = (x + 1, y)$$

$$f^2(x,\ y) = (x + 2,\ y)$$
$$\vdots$$
$$f^n(x,\ y) = (x + n,\ y)$$
$$\vdots$$

E suas inversas,

$$f^{-1}(x,\ y) = (x - 1,\ y)$$
$$(f^2)^{-1} = (f^{-1})^2(x,\ y) = (x - 2,\ y)$$
$$\vdots$$
$$(f^n)^{-1} = (f^{-1})^n(x,\ y) = (x - n,\ y)$$
$$\vdots$$

Então, obteremos

$$G = \ < f > \ = \{Id,\ f, f^{-1}, f^2, (f^{-1})^2,\ \ldots, f^n, (f^{-1})^n,\ \ldots\}$$

O conjunto inicial dado é

$$X = \{(1,\ 0),\ (1,\ 1)\}$$

Para $(1,\ 0)$, temos as aplicações

$$f(1,\ 0) = (1 + 1,\ 0) = (2,\ 0)$$
$$f^2(1,\ 0) = (1 + 2,\ 0) = (3,\ 0)$$
$$\vdots$$
$$f^n(1,\ 0) = (1 + n,\ 0)$$
$$\vdots$$

E, as seguintes inversas

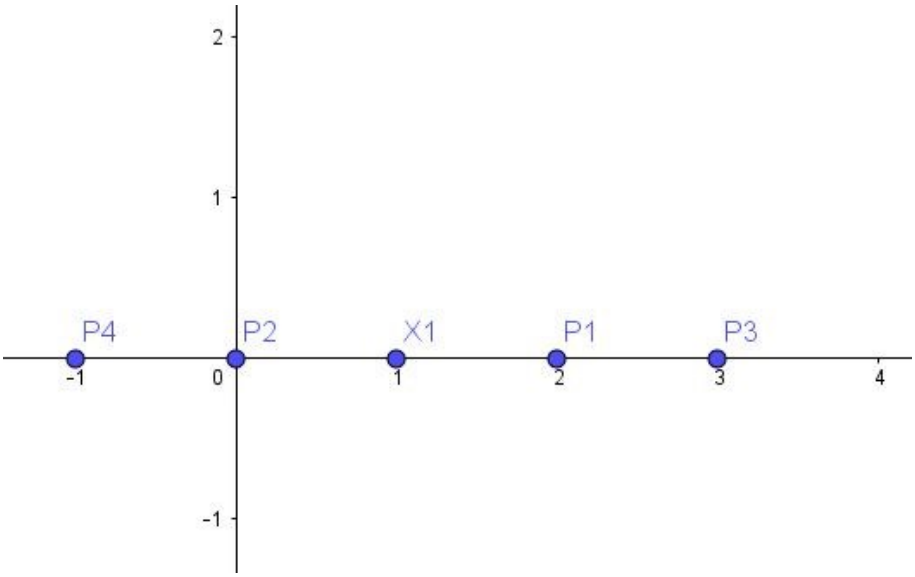
$$f^{-1}(1,\ 0) = (1 - 1,\ 0) = (0,\ 0)$$
$$(f^2)^{-1} = (f^{-1})^2(1,\ 0) = (1 - 2,\ 0) = (-1,\ 0)$$
$$\vdots$$
$$(f^n)^{-1} = (f^{-1})^n(1,\ 0) = (1 - n,\ 0)$$
$$\vdots$$

Logo, obtemos o seguinte grupo

$$G = \ < f > \ = \{Id,\ f, f^{-1}, f^2, (f^{-1})^2, \ldots, f^n, (f^{-1})^n,\ \ldots\}$$

Na figura 11 é possível observar os resultados do GAGE aplicado neste primeiro ponto.

Figura 11: Exemplo 4.10 de GAGE operando no primeiro ponto



Fonte: Autoria própria

Para $(1,\ 1)$, temos as aplicações

$$f(1,\ 1) = (1+1,\ 1) = (2,\ 1)$$
$$f^2(1,\ 1) = (1+2,\ 1) = (3,\ 1)$$
$$\vdots$$
$$f^n(1,\ 1) = (1+n,\ y)$$
$$\vdots$$

E, suas inversas

$$f^{-1}(1,\ 1) = (1-1,\ 1) = (0,\ 1)$$
$$(f^2)^{-1} = (f^{-1})^2(1,\ 1) = (1-2,\ 1) = (-1,\ 1)$$
$$\vdots$$
$$(f^n)^{-1} = (f^{-1})^n(1,\ 1) = (1-n,\ y)$$
$$\vdots$$

obtendo,

$$G = \ < f > \ = \{Id,\ f, f^{-1}, f^2, (f^{-1})^2, \dots, f^n, (f^{-1})^n,\ \dots\}$$

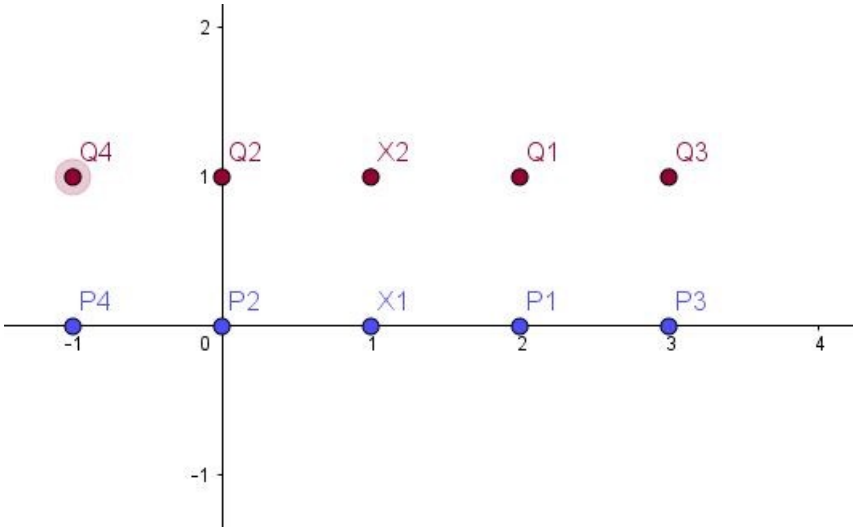
Logo, o GAGE é

GX

$= \{\ldots, (-1, 0), (0, 0), (1,0), (2, 0), (3, 0), \ldots, (-1, 1), (0, 1), (1, 1), (2, 1), (3, 1), \ldots\}$

É possível observar o resultado do GAGE na figura 12.

Figura 12: Exemplo 4.10 de GAGE



Fonte: Autoria própria

Como vimos, este exemplo ressalta as vantagens de se trabalhar com o conceito de grupo alfabeto generalizado enumerável. Pois, empregamos um conjunto inicial formado por dois elementos, o que não seria possível na técnica CGU. E, além disso aplicamos uma translação para diferenciar do método GAG, que não permite o uso de translações em seus procedimentos.

4 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

4.1 CONSIDERAÇÕES FINAIS

A análise dos códigos geometricamente uniformes e dos grupos alfabetos generalizados, possibilitou a identificação das características mais evidentes de cada conceito, conciliando-as, com o intuito de desenvolver uma técnica mais vantajosa. Assim, foram estabelecidas as propriedades algébricas e geométricas, necessárias para a construção do grupo alfabeto generalizado enumerável, ou GAGE.

Esta técnica permite gerar novos códigos e categorias de rotulamentos, através de estruturas algébricas que fazem uso de conjuntos iniciais enumeráveis e isometrias como grupo gerador. Além de se trabalhar em todo o espaço métrico, fato que ainda não foi estudado e desenvolvido na teoria de Biglieri, a qual foi aplicada somente no espaço euclidiano.

Com este estudo, espera-se contribuir com a busca por sistemas de comunicação que operem através de canais com máxima segurança e confiabilidade possível, ou seja, com excelente capacidade de transmissão e armazenamento, apresentando baixa taxa de erro. Satisfazendo, dessa forma, a crescente demanda por transmissão mais eficiente.

O conceito GAGE amplia esta área, promovendo a base necessária para que outras pesquisas sejam realizadas, e estas possibilitem o desenvolvimento de novos dispositivos de comunicação.

Evidentemente, há muita teoria a ser formalizada, examinada e aprofundada, bem como ter suas propriedades compreendidas. Isso já era verdade até mesmo para os conceitos introduzidos por Forney e Biglieri, os quais ainda têm muitos aspectos para serem explorados.

4.2 TRABALHOS FUTUROS

Considerando os resultados obtidos neste trabalho, recomenda-se para trabalhos futuros:

- O estudo do grupo alfabeto generalizado enumerável, teoria introduzida neste trabalho, com o intuito de explorar e aprimorar as suas propriedades. Além disso, desenvolver o conceito apresentando exemplos em espaços métricos não-euclidianos.

REFERÊNCIAS

ABRANTES, S. A. **Apontamentos da Teoria da Informação. Faculdade de Tecnologia da Universidade do Porto.** Departamento de Engenharia Eletrotécnica e de Computadores, 2003.

ALVES, Carina. **Reticulados e Códigos.** Tese de Doutorado, IMECC - UNICAMP, Brasil, 2008.

ALVES, Marcelo M. S. **Rotulamentos de Códigos por Grupos de Simetrias.** Tese de Doutorado, Instituto de Matemática, Estatística e Computação Científica – UNICAMP, Brasil, 2002.

BIGLIERI, Ezio; ELIA, Michele. **Multidimensional Modulation and Coding for Band-Limited Digital Channels.** IEEE Transactions on Information Theory, v. 34, n.4, p. 803-809, 1988.

CARVALHO, Edson Donizete. **Construção e Rotulamentos de Constelações de Sinais Geometricamente Uniformes em Espaços Euclidiano e hiperbólicos.** Tese de Doutorado, FEEC – UNICAMP, Brasil, 2001.

FORNEY JR., G. D. **Algebraic Structure of Convolutional Codes, and Algebraic System Theory.** IEEE Transactions on Information Theory, pages 720-738, 1970.

FORNEY JR., G. D. **Geometrically Uniform Codes.** IEEE Transactions on Information Theory, v. 37, n.5, p. 1241-1260, 1991.

GOMES, Eduardo Michel Vieira. **Rotulamentos de Constelações de Sinais Uniformes e Cadeias de Particionamentos Ungerboeck Hiperbólicas sobre o Bitoro.** 2017.82 f. Tese Doutorado – Universidade Estadual de Maringá. Paraná, Maringá.

IEZZI, Gelson. DOMINGUES, Hygino H. **Álgebra moderna.** 4° ed. São Paulo: editora Atual, 2003.

LAY, David C. **Álgebra linear e suas aplicações.** 2° ed. Rio de Janeiro: LTC, 1999.

LAZARI, H. **Uma Contribuição a Teoria dos Códigos Geometricamente Uniformes Hiperbólicos.** Tese de Doutorado, FEEC-UNICAMP, Brasil, 2000.

LIMA, Elon Lages. **Espaços Métricos.** 3° ed. Rio de Janeiro: Projeto Euclides, 1976.

LIMA, Elon Lages. **Isometrias.** Rio de Janeiro: Sociedade Brasileira de Matemática,1996.

LOELIGER, H. A. **Signal sets matched to groups.** IEEE Transactions on Information Theory, v. 37, n. 6, p. 1675-1682, 1991.

MILIES, C. P. **Breve introdução à Teoria dos Códigos Corretores de Erros.** Campo Grande: Sociedade Brasileira de Matemática, Colóquio de Matemática da Região Centro-Oeste, Departamento de Matemática, Universidade Federal do Mato Grosso do Sul, 2009.

NASCIMENTO, Wallas Santos. **Sobre algumas características da entropia de Shannon para sistemas atômicos confinados.** Dissertação de Mestrado, IFUFBA, Brasil, 2013.

SHANNON, Claude E. **A Mathematical Theory of Communication.** The Bell System Technical Journal v. 27, n. July 1948, p. 379-423, 1948.

SILVA, Antonio de Andrade e; PALAZZO JR., Reginaldo. **Constelações de Sinais Casadas a Grupos Não-Comutativos.** CCEN-UFPB, FEEC-UNICAMP, Brasil, 2015.

SILVA, Diego de Souza. **Compressão e Códigos Corretores de Erros**. FT-UNICAMP, Brasil, 2012.

SLEPIAN, D. **Group Codes for the Gaussian Channel.** Bell Labs Technical Journal, v. 37, p. 575-602, 1968.