

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

CÓDIGOS GEOMETRICAMENTE UNIFORMES EM ESPAÇOS HIPERBÓLICOS

Por

ANA PAULA FARIA MACHADO

Orientador: **Prof. Dr. MÁRIO JOSÉ DE SOUZA**

DISSERTAÇÃO DE MESTRADO EM MATEMÁTICA

GOIÂNIA, GOIÁS

2008

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
COORDENAÇÃO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Códigos Geometricamente Uniformes em Espaços Hiperbólicos

por

Ana Paula Faria Machado

Área de concentração: Álgebra

Orientador: Prof. Dr. Mário José de Souza

Dissertação submetida à Banca Examinadora designada pelo Conselho Diretor do Instituto de Matemática e Estatística, como parte dos requisitos necessários à obtenção do grau de Mestre em Matemática.

Goiânia - Goiás

2008

A Deus.

DEDICO

Agradecimentos

A Deus, o Senhor de todas as coisas, quem me criou e me capacitou a chegar até aqui.

À Nossa Senhora e à Santa Edwirges, que sempre intercederam por mim.

Ao Professor Doutor Mário José de Souza pela grande atenção, paciência e dedicação que teve comigo durante as orientações. Seu auxílio foi fundamental no meu desenvolvimento. Muito obrigada!

À minha família, em especial aos meus pais Maurita e Sebastião que sempre me apoiaram incondicionalmente, me incentivando a cada dia. Eu os amo muito.

Ao meu amado Dalmo Luiz, por todo amor e compreensão.

Aos professores do Corpo Docente do Mestrado em especial àqueles com quem cursei alguma disciplina.

Aos meus colegas que, durante o período de aula, tanto contribuíram para a minha formação em bons momentos de estudo.

À Banca Examinadora pela disponibilidade e atenção dispensada ao meu trabalho.

Ao CNPq pelo apoio financeiro.

Sumário

Introdução	1
1 Preliminares	3
1.1 Grupos	3
1.1.1 Subgrupos	4
1.1.2 Classes Laterais	5
1.1.3 Grupos Quocientes	5
1.1.4 Homomorfismos	6
1.1.5 Ações de grupos	7
1.2 Espaços Métricos	8
1.3 Geometria Hiperbólica	10
1.4 Códigos Corretores de Erros	12
1.5 Códigos Lineares	13
2 Códigos Geometricamente Uniformes	17
2.1 Isometrias	17
2.2 Conjuntos de Sinais Geometricamente Uniformes	19
2.3 Conjuntos de Sinais Geometricamente Uniformes e a Comunicação Digital	20
2.4 Propriedades Simétricas de Conjuntos de Sinais Geometricamente Uniformes	21
2.5 Partições Geometricamente Uniformes	23

2.6	Rotulamentos Isométricos	25
2.7	Propriedades Elementares dos Rotulamentos Isométricos	26
2.8	Rotulamentos Binários Isométricos	27
2.9	Códigos Geometricamente Uniformes em Espaços de Sinais	29
2.9.1	Espaços de Seqüências	29
2.9.2	Códigos em Espaços de Sinais	30
2.9.3	Classes Laterais de Códigos Generalizadas	31
2.10	Outras Noções de Uniformidade	33
2.10.1	Linearidade	33
2.10.2	Subconjunto Tempo-Zero	35
2.10.3	Rotulamentos Regulares	36
3	Códigos Hiperbólicos Geometricamente Uniformes	38
3.1	Tesselações Hiperbólicas	39
3.2	Conjuntos de Sinais Associados a Grupos	40
3.3	Conjuntos de Sinais Geometricamente Uniformes Hiperbólicos	41
3.4	Partições Geometricamente Uniformes Hiperbólicas	41
3.5	Códigos Geometricamente Uniformes em Espaço de Sinais Hiperbólicos	42
	Conclusão	48
	Referências Bibliográficas	49

Resumo

Nesta dissertação definimos códigos geometricamente uniformes em espaços euclidianos, apresentando algumas propriedades simétricas destes códigos. Construímos partições geometricamente uniformes e a partir destas definimos classes laterais de códigos generalizadas. Estendemos aos espaços hiperbólicos o conceito de códigos geometricamente uniformes. Mostramos também uma caracterização de classes laterais generalizadas através do conceito de códigos G – *lineares*.

Abstract

In this dissertation we define geometrically uniform codes in Euclidean spaces, presenting some symmetrical properties of these codes. Build geometrically uniform partitions and starting these we define generalized coset codes. We generalize the concept of geometrically uniform codes to hyperbolic spaces. We show a characterization of generalized coset codes through the concept of $G - linear$ codes.

Introdução

A teoria dos códigos corretores de erros e dos sistemas de comunicação digital assumiu a forma atual a partir do trabalho fundamental de Shannon [10], do laboratório de Bell, publicado em 1948. Neste trabalho foi mostrado que dado um canal de comunicação digital é possível, com uma codificação adequada, transmitir informações com probabilidade de erro arbitrariamente pequena. O trabalho inicial para aquisição de bons códigos foi árduo, pois exigia um profundo conhecimento de álgebra abstrata e teoria da probabilidade, sendo desenvolvido por um grupo restrito composto apenas por matemáticos nas décadas de 50 e 60.

Os elementos dos códigos corretores de erros são seqüências de símbolos pertencentes a um alfabeto, tomado freqüentemente entre os elementos de algum grupo, por exemplo, dígitos binários ou vetores. Mesmo quando os símbolos não têm uma estrutura natural, um procedimento natural e útil é produzir um rotulamento dos símbolos do alfabeto por elementos de algum grupo (ou seja, definir uma aplicação injetora do alfabeto no grupo, sujeita a determinadas condições).

Os conjuntos de sinais e os códigos corretores de erros que os têm como alfabeto apresentam, em geral, algum tipo de estrutura capaz de permitir a determinação de suas propriedades e tornar mais prática a sua implementação. As estruturas algébricas são a base de muitos códigos conhecidos e importantes, além disso, o estabelecimento de um conceito adequado de distância e o processo de avaliação de distâncias entre as palavras e as palavras-código são fundamentais no processo de decodificação.

O conceito de conjunto de sinais geometricamente uniforme foi introduzido por

David Forney [4] em 1991. Foram utilizados neste contexto espaços e conjuntos de sinais euclidianos.

Em 2005 Henrique Lazzari e Reginaldo Palazzo em [7] estendem os conceitos de constelações, reticulados e particionamento ao plano hiperbólico. Apesar dos grupos de isometrias hiperbólicos apresentarem maior complexidade quando comparados aos grupo de isometrias euclidianos, a teoria de partições geometricamente uniformes se estende a estes.

O Capítulo 1 traz uma descrição das propriedades básicas de estruturas algébricas e métricas de maior importância para a teoria de comunicação. Também traz uma introdução à teoria de códigos corretores de erros. Uma grande parte das demonstrações deste capítulo foram omitidas podendo ser encontradas em [6], [9], [11] e [5].

No Capítulo 2 são definidos conjuntos de sinais geometricamente uniformes em espaços euclidianos e verificamos algumas propriedades simétricas destes conjuntos. Apresentamos a teoria das partições geometricamente uniformes, em seguida, definimos rotulamentos isométricos e suas propriedades. Introduzimos o conceito de códigos geometricamente uniformes em espaços de sinais e encerramos o capítulo com outras noções de uniformidade.

Finalizamos no Capítulo 3 definindo G – *linearidade*, tesselações regulares e estendendo ao plano hiperbólico a teoria das partições geometricamente uniformes, através do conceito de códigos G – *lineares*.

Capítulo 1

Preliminares

Neste capítulo são apresentadas noções gerais sobre Teoria de Grupos, Espaços Métricos, Geometria Hiperbólica e Códigos. Muitas demonstrações são omitidas. Para maiores detalhes em relação às noções acima mencionadas indicamos [5], [6], [9] e [11].

1.1 Grupos

Uma operação binária num conjunto não vazio G é uma função

$$\mu : G \times G \rightarrow G$$

que a cada par ordenado (a, b) de elementos de G associa um elemento $\mu(a, b)$ de G , chamado de produto de a e b , o qual denotaremos por ab . Uma operação binária é dita associativa se $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para quaisquer $a, b, c \in G$.

Definição 1.1. Um grupo consiste num conjunto não vazio G munido de uma operação binária que satisfaz as seguintes propriedades:

G1: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associatividade)

G2: Existe $e \in G$ tal que $e \cdot a = a \ \forall a \in G$ (Elemento neutro)

G3: $\forall a \in G$, existe $b \in G$ tal que $b \cdot a = e$ (Existência de inverso)

Exemplo 1.2. O grupo geral linear $GL(n, \mathbb{R})$. Se $G = GL(n, \mathbb{R})$ denota o conjunto de todas as matrizes $n \times n$ invertíveis com entradas reais e μ é a multiplicação usual de matrizes $(A, B) \mapsto AB$, então G é um grupo.

Exemplo 1.3. O grupo das permutações de um conjunto X . Seja $G = S(X)$ o conjunto de todas funções bijetivas $\phi : X \rightarrow X$ munido da operação composição de funções.

Exemplo 1.4. O conjunto $G = \mathbb{Z}$ com a operação usual de adição de números inteiros também é um grupo.

Observação 1.5. Seja G um grupo, se para todos $x, y \in G$ temos $x \cdot y = y \cdot x$ dizemos que G é um grupo comutativo ou abeliano.

1.1.1 Subgrupos

Seja G um grupo e H um subconjunto de G dizemos que H é um subgrupo de G se verificar as seguintes condições:

S1: H não é vazio.

S2: Se $a, b \in H$, então $a \cdot b \in H$

S3: Se $a \in H$, então $a^{-1} \in H$

Usaremos a notação $H \leq G$ para indicar que H é um subgrupo de G .

Definição 1.6. Se S é um subconjunto não vazio de um grupo G , definimos o grupo gerado por S , e denotado por $\langle S \rangle$, como:

$$\langle S \rangle = \bigcap_j H_j$$

onde H_j são os subgrupos de G que contêm S . Assim $\langle S \rangle$ é o menor subgrupo de G que contém S .

Definição 1.7. Um subgrupo de G da forma $\langle a \rangle$, para algum $a \in G$, é chamado um subgrupo cíclico de G .

Definição 1.8. Se $G = \langle g \rangle$ onde $g \in G$ dizemos que G é um grupo cíclico.

Definição 1.9. Um grupo G é dito um grupo finito, se como conjunto G é finito. Nesse caso, o seu número de elementos é denotado por $|G|$, e chamado a ordem de G .

1.1.2 Classes Laterais

Seja H um subgrupo de um grupo G e $x \in G$ o subconjunto de G

$$Hx = \{hx; h \in H\}$$

é chamado classe lateral a direita de H em G . De maneira análoga se define classe lateral a esquerda de H em G . Quando o conjunto das classes laterais (à direita ou à esquerda) de H em G for um conjunto finito, dizemos que H é um subgrupo de índice finito em G e o número de classes laterais é chamado o índice de H em G e denotado por $|G : H|$.

Teorema 1.10. (*Lagrange*) Se G é um grupo finito e H é um subgrupo de G então

$$|G| = |H||G : H|.$$

1.1.3 Grupos Quocientes

Sejam G um grupo e $H \leq G$. Ao conjunto de todas as classes laterais à esquerda (à direita) denominamos conjunto quociente e o denotamos por $\frac{G}{H}$.

Definição 1.11. Um subgrupo H de um grupo G diz-se normal em G se ocorre uma (e portanto todas) das condições equivalentes

1. $Hx = xH$, para todo $x \in G$

2. $xHx^{-1} = H$, para todo $x \in G$

3. $xHx^{-1} \subset H$, para todo $x \in G$

Escrevemos $H \trianglelefteq G$ para dizer que H é um subgrupo normal de G .

Quando $H \trianglelefteq G$, $\frac{G}{H}$ é um grupo chamado de grupo quociente de G por H . No caso de $\frac{G}{H}$ ser um grupo finito a sua ordem é o índice $|G : H|$ de H em G . Se o próprio G for finito, o Teorema de Lagrange diz que

$$\left| \frac{G}{H} \right| = \frac{|G|}{|H|}.$$

1.1.4 Homomorfismos

Definição 1.12. Sejam $(G, \cdot)$ e $(G', *)$ dois grupos. Uma aplicação $f : G \rightarrow G'$ satisfazendo

$$f(a \cdot b) = f(a) * f(b)$$

para todos $a, b \in G$, é dita um homomorfismo de grupos. Se f for também uma função bijetora, dizemos que f é um isomorfismo entre G e G' . Se G e G' são isomorfos escrevemos $G \cong G'$.

Definição 1.13. Se $f : G \rightarrow G'$ é um homomorfismo de grupos, o subconjunto

$$\ker(f) = \{g \in G : f(g) = e_{G'}\}$$

é chamado núcleo de f .

Encerramos esta subseção, apresentando um resultado que avalia os subgrupos de $\frac{G}{H}$ em função dos subgrupos de G

Teorema 1.14. *Seja H um subgrupo normal de um grupo G e $\pi : G \rightarrow \frac{G}{H}$ a projeção canônica. Então π induz uma correspondência bijetora entre o conjunto S_H dos subgrupos de G que contêm H e o conjunto S dos subgrupos de $\frac{G}{H}$, dada por:*

$$V \in S_H \rightarrow \pi(V) = \frac{V}{H} \in S.$$

Além disso, tem-se:

(a) Se $V, L \in S_H$, então $V \subseteq L \Leftrightarrow \pi(V) \subseteq \pi(L)$.

(b) Se $V, L \in S_H$, com $V \subseteq L$, então $|L : V| = |\pi(L) : \pi(V)|$.

(c) Se $V, L \in S_H$, então $V \trianglelefteq L \Leftrightarrow \pi(V) \trianglelefteq \pi(L)$.

(d) Se $V, L \in S_H$, com $V \trianglelefteq L$, então $\frac{L}{V} \trianglelefteq \frac{\pi(L)}{\pi(V)}$.

1.1.5 Ações de grupos

Uma ação (à esquerda) de um grupo G num conjunto X é uma função

$$\varphi : G \times X \rightarrow X$$

satisfazendo:

(A1) $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$, $\forall g, h \in G$, $\forall x \in X$.

(A2) $\varphi(e, x) = x$, $\forall x \in X$ ($e \in G$ é a identidade de G).

Analogamente define-se uma ação à direita de um grupo G num conjunto X .

Exemplo 1.15. $G = GL(n, \mathbb{R})$ e $X = \mathbb{R}^n$. A ação φ é a multiplicação usual de uma matriz $n \times n$ por um vetor (coluna) $n \times 1$.

Exemplo 1.16. Seja G um grupo e $X = G$. A função definida por $(g, x) \mapsto gxg^{-1}$ é uma ação de G em G chamada **ação por conjugação**.

Definição 1.17. Se um grupo G age num conjunto X e $x \in X$, o subconjunto de X ,

$$O(x) = \{g \cdot x : g \in G\},$$

é chamado de órbita de x .

Lema 1.18. Se G é um grupo agindo num conjunto X , então:

(a)

$$X = \bigcup_{x \in X} O(x),$$

(b) Se $x, y \in X$, então $O(x) \cap O(y) = \emptyset$, ou $O(x) = O(y)$.

Definição 1.19. Um subconjunto S de X que corta cada órbita da ação de G em X em um único ponto é chamado conjunto de representantes de órbitas. (Tal conjunto sempre existe, pelo Axioma da Escolha).

Definição 1.20. Se G age num conjunto X e $x \in X$, o subgrupo de G

$$G_x = \{g \in G : g \cdot x = x\}$$

é chamado estabilizador de x ou grupo de isotropia de x .

Se para algum $x_0 \in X$, $G_{x_0} = G$, diz-se que x_0 é um ponto fixo pela ação de G . O conjunto dos pontos fixos de X é denotado por $Fix(X)$.

Exemplo 1.21. $G = GL(n, \mathbb{R})$ e $X = \mathbb{R}^n$. $\frac{G}{X}$ possui dois elementos $\{\pm I\}$ e $Fix(X) = \{(0, \dots, 0)\}$.

Definição 1.22. Uma ação de um grupo G num conjunto X diz-se transitiva se ocorrer uma (e portanto todas) das três condições equivalentes:

- (i) $\exists x \in X$ tal que $O(x) = X$
- (ii) $\forall x, y \in X, \exists g \in G$ tal que $x = g.y$.
- (iii) $\forall x \in X, O(x) = X$.

1.2 Espaços Métricos

Definição 1.23. Um conjunto E é dito um espaço métrico se existe uma função

$$d : E \times E \rightarrow \mathbb{R}$$

denominada métrica ou distância satisfazendo para todos $x, y, z \in E$ as seguintes propriedades:

E1) $d(x, y) \geq 0$ e $d(x, y) = 0$ se, e somente se, $x = y$,

E2) $d(x, y) = d(y, x)$,

E3) $d(x, z) \leq d(x, y) + d(y, z)$.

Geralmente o espaço métrico é denotado por (E, d) ou simplesmente E , quando não houver ambiguidade.

Exemplo 1.24. Um conjunto E finito torna-se um espaço métrico munido com a métrica definida por:

$$d(x, y) = \begin{cases} 0, & \text{se } x=y; \\ 1, & \text{se } x \neq y. \end{cases} \quad (1.1)$$

Então d é denominada **métrica discreta**. Sejam E^n um espaço n -dimensional e

$$d_{\mathbb{H}} = \sum_{i=1}^n d(x_i, y_i),$$

com $d(x_i, y_i)$ a métrica discreta. Então $d_{\mathbb{H}}$ é uma métrica em E^n , chamada de **métrica de Hamming**. Seja $E = \mathbb{F}_q$ um corpo finito, onde q é uma potência de um número primo. Definamos para um $x \in \mathbb{F}_q^n$ o peso de Lee do elemento x por: $\omega_L(x) = \sum_{i=1}^n |x_i|$, onde

$$|x_i| = \begin{cases} x_i, & \text{se } 0 \leq x_i \leq \frac{q}{2}; \\ q - x_i, & \text{se } \frac{q}{2} \leq x_i \leq q - 1. \end{cases} \quad (1.2)$$

Desse modo a distância de Lee entre $x, y \in \mathbb{F}_q^n$ é dada por $d_L(x, y) = \omega_L(x - y)$.

Seja p um elemento num espaço métrico E e $\delta > 0$ um valor real. A bola aberta de centro p e raio δ é o conjunto $S(p, \delta)$ dos elementos de E cuja distância ao ponto p é menor do que δ , simbolicamente,

$$S(p, \delta) = \{x \in E : d(p, x) < \delta\}.$$

Dado um ponto $p \in E$ dizemos que o mesmo é um ponto isolado quando ele é uma bola aberta em E , isto é, quando existe $\delta > 0$ tal que $S(p, \delta) = \{p\}$. Um espaço métrico é denominado discreto quando todos seus pontos são isolados.

1.3 Geometria Hiperbólica

Existem vários modelos interessantes para a geometria hiperbólica. Aqui apresentamos um modelo para o plano hiperbólico, baseado no semi-plano direito:

$$SPD = \{z = x + iy \in \mathbb{C} | \operatorname{Re}(z) > 0\}.$$

As retas (geodésicas) em SPD são os seguintes subconjuntos: as semi-retas ortogonais ao eixo imaginário

$$y = c, \quad c \in \mathbb{R},$$

e os semicírculos ortogonais ao eixo imaginário dados por

$$x^2 + (y - p)^2 = R^2,$$

com $p, R \in \mathbb{R}$, $R > 0$.

A seguir definimos uma distância entre os pontos do SPD .

Seja $\gamma : [a, b] \rightarrow SPD$ uma curva continuamente diferenciável (de classe C^1), tal que $\gamma(t) = (x(t), y(t))$. Definimos seu comprimento por

$$\begin{aligned} \|\gamma\| &= \int_a^b \frac{\|\gamma'(t)\|}{x(t)} dt \\ &= \int_a^b \frac{\sqrt{(dx/dt)^2 + (dy/dt)^2}}{x(t)} dt. \end{aligned}$$

Pela regra da cadeia, verifica-se que este comprimento depende apenas do traço da curva, isto é, se $\phi : [a', b'] \rightarrow [a, b]$ for um difeomorfismo, então $\bar{\gamma} = \gamma \circ \phi$ é uma curva com o mesmo traço e $\|\gamma\| = \|\bar{\gamma}\|$. Desse modo, consideramos as curvas no intervalo $I = [0, 1]$.

A função $d_{SPD} : SPD \times SPD \rightarrow \mathbb{R}^+$ tal que $d_{SPD}(z, w) = \inf \|\gamma\|$, para todo γ de classe C^1 com $\gamma(0) = z$ e $\gamma(1) = w$, é uma métrica.

Determinaremos a seguir as isometrias de (SPD, d_{SPD}) .

Uma matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{R})$ (matrizes com determinante 1) induz uma transformação

$$\begin{aligned}
T_A : \quad SPD &\rightarrow SPD \\
z &\mapsto T_A(z) = \frac{a\bar{z}+bi}{-c\bar{z}+d}
\end{aligned} \tag{1.3}$$

onde $\bar{z}$ denota o complexo conjugado de $z = x + iy$.

Temos que

$$Re\left(\frac{a\bar{z}+bi}{-c\bar{z}+d}\right) = Re\left(\frac{(a\bar{z}+bi)(\overline{-c\bar{z}+d})}{|-c\bar{z}+d|^2}\right).$$

De modo que

$$Re\left(\frac{a\bar{z}+bi}{-c\bar{z}+d}\right) > 0 \Leftrightarrow Re((a\bar{z}+bi)(\overline{-c\bar{z}+d})) > 0.$$

Mas

$$Re((a\bar{z}+bi)(\overline{-c\bar{z}+d})) = Re([a(x-iy)+ib][(d-cy)+icx]) = x(ad-bc) = x,$$

pois $ad-bc=1$, de modo que $Re(z) > 0$ se, e somente se, $Re(T_A(z)) > 0$, ou seja, T_A é uma transformação do SPD .

Teorema 1.25. *As transformações $T_A : SPD \rightarrow SPD$ são isometrias, ou seja, preservam comprimento de curvas $\|T_A \circ \gamma\| = \|\gamma\|$ e, conseqüentemente, também a distância entre pontos ($d(z, w) = d(T_A(z), T_A(w))$).*

Demonstração: Seja $\gamma : [a, b] \rightarrow SPD$ diferenciável.

O caminho $T_A \circ \gamma : [a, b] \rightarrow SPD$ é tal que

$$\begin{aligned}
\|T_A \circ \gamma\| &= \int_a^b \frac{\|T_A'(\gamma(t))\gamma'(t)\|}{ReT_A(\gamma(t))} dt \\
&= \int_a^b \frac{\|T_A'(\gamma(t))\|}{ReT_A(\gamma(t))} \|\gamma'(t)\| dt \\
&= \int_a^b \frac{\|\gamma'(t)\|}{Re(\gamma(t))} = \|\gamma(t)\|.
\end{aligned}$$

Logo, $d_{SPD}(z, w) = \inf \|\gamma\|; \gamma(a) = z$ e $\gamma(b) = w$

$\Rightarrow d_{SPD}(z, w) = \inf \|T_A \circ \gamma\|; T_A \circ \gamma(a) = T_A(z)$ e $T_A \circ \gamma(b) = T_A(w)$

$\Rightarrow d_{SPD}(z, w) = d_{SPD}(T_A(z), T_A(w)) \quad \forall z, w \in SPD.$

Portanto, T_A é uma isometria de (SPD, d_{SPD}) . □

1.4 Códigos Corretores de Erros

Seja A um conjunto finito chamado de *alfabeto*, um *código corretor de erros* é um subconjunto próprio qualquer C de A^n , onde n é um número natural, e uma palavra $u \in A^n$ será representada por $(u_1, u_2, \dots, u_n)$.

Definição 1.26. Dados $u, v \in A^n$, a distância de Hamming entre u e v é definida como

$$d(u, v) := |\{i : u_i \neq v_i, 1 \leq i \leq n\}|.$$

E a distância mínima de um código C é o número

$$d(C) := \min\{d(u, v) : u, v \in C \text{ e } u \neq v\}.$$

Proposição 1.27. *Dados $u, v, w \in A^n$, valem as seguintes propriedades:*

- i. *Positividade:* $d(u, v) \geq 0$, valendo a igualdade se, e somente se, $u = v$
- ii. *Simetria:* $d(u, v) = d(v, u)$
- iii. *Desigualdade Triangular:* $d(u, v) \leq d(u, w) + d(w, v)$

Demonstração: As propriedades i e ii são de fácil verificação, demonstraremos a seguir a terceira propriedade.

A contribuição das i -ésimas coordenadas de u e v para $d(u, v)$ é igual a zero se $u_i = v_i$ e igual a um se $u_i \neq v_i$.

No caso em que a contribuição é zero, certamente a contribuição das i -ésimas coordenadas a $d(u, v)$ é menor ou igual a das i -ésimas coordenadas a $d(u, w) + d(w, v)$ ($= 0, 1$ ou 2).

No outro caso, temos que $u_i \neq v_i$ e, portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$. Consequentemente, a contribuição das i -ésimas coordenadas a $d(u, w) + d(w, v)$ é maior ou igual a 1, que é a contribuição das i -ésimas coordenadas a $d(u, v)$. $\square$

As propriedades contidas na Proposição 1.27 mostram que a distância de Hamming caracteriza uma *métrica* em A^n a chamada *métrica de Hamming*.

Definição 1.28. Dado um código C com distância mínima d , define-se $\kappa = \lfloor \frac{d-1}{2} \rfloor$ onde κ representa a parte inteira de um número real $\frac{d-1}{2}$.

Teorema 1.29. *Seja C um código com distância mínima d . Então C pode corrigir até κ erros e detectar até $d - 1$ erros.*

Demonstração: Se ao transmitirmos uma palavra c do código cometemos t erros com $t \leq \kappa$, recebendo a palavra r , então $d(c, r) = t \leq \kappa$; enquanto que a distância de r a qualquer outra palavra do código é maior do que κ . Isso determina c de modo único a partir de r .

Por outro lado, dada uma palavra do código, podemos nela introduzir até $d - 1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível. $\square$

1.5 Códigos Lineares

Consideremos o corpo finito K com q elementos como sendo o alfabeto. Portanto, temos, para cada número natural n , um K -espaço de dimensão n , denotado por K^n .

Definição 1.30. Um código $C \subset K^n$ será chamado de Código Linear se for um subespaço vetorial de K^n . Os elementos de C são chamados de palavras-código.

Definição 1.31. Dado $u \in K^n$, define-se o peso de u como sendo o número inteiro

$$\omega(u) := d(u, o) = |\{i : u_i \neq 0, 1 \leq i \leq n\}|,$$

onde o denota o vetor nulo. O peso de C é o inteiro

$$\omega(C) := \min\{\omega(u) : u \in C\}.$$

Como $d(u, v) = d(u - v, 0) = \omega(u - v)$ e C é um espaço linear, a distância mínima de C é equivalente a

$$d(C) := \min\{\omega(x) : x \in C, x \neq o\}.$$

A terna de inteiros $[n, k, d]$ é chamada de *parâmetros de código linear* C , onde n é o comprimento das palavras de C , k é a dimensão de C sobre K e d é a distância mínima de C . Note que o número de elementos de C é igual a q^k , onde q é o número de elementos de K .

Uma maneira de descrever subespaços vetoriais de um espaço vetorial K^n é como imagem de transformações lineares. Para tal, precisamos da matriz da transformação, chamada *matriz geradora do código*.

Definição 1.32. Uma matriz geradora de um código linear C com parâmetros $[n, k, d]$ é uma matriz G de ordem $k \times n$ cujas linhas formam uma base para C .

Definição 1.33. Seja $C \subset K^n$ um código linear com parâmetros $[n, k, d]$.

(i) O Código Dual de C , $C^\perp$, é o complemento ortogonal do subespaço C de K^n ,

$$C^\perp = \{v \in K^n : \langle v, u \rangle = 0, \forall u \in C\}.$$

(ii) Uma matriz teste de paridade H para um código linear C é uma matriz geradora para o código dual $C^\perp$, cuja ordem é $(n - k) \times n$.

Se tomarmos a matriz G acima descrita e nela realizarmos operações do tipo permutação de duas linhas e/ou duas colunas, multiplicação de uma linha e/ou uma coluna por um escalar não nulo e adição de um múltiplo escalar de uma linha a outra, de forma a obtermos uma matriz do tipo $G' = (Id_k \mid A)$, onde Id_k é a matriz identidade $k \times k$ e A é uma matriz $k \times (n - k)$, temos uma matriz padrão de G , ou seja, $G' = (Id_k \mid A)$ é a matriz G na forma padrão. Deste modo, a matriz teste de paridade H é da forma $H = (-A^t \mid Id_{n-k})$.

Lema 1.34. Se $C \subset K^n$ é um código linear, com matriz geradora G , então

- i) $C^\perp$ é um subespaço vetorial de K^n ;
- ii) $x \in C^\perp$ se, e somente se, $Gx^t = 0$.

Demonstração: i) Sejam dados $u, v \in C^\perp$ e $\lambda \in K$. Temos, para todo $x \in C$, que

$$\langle u + \lambda v, x \rangle = \langle u, x \rangle + \lambda \langle v, x \rangle = 0 + \lambda 0 = 0.$$

Portanto, $(u + \lambda v) \in C^\perp$, provando que $C^\perp$ é um subespaço vetorial de K^n .

ii) $x \in C^\perp$ se, e somente se, x é ortogonal a todos os elementos de C , se, e somente se, x é ortogonal a todos os elementos de uma base de C , o que é equivalente a dizer que $Gx^t = 0$, pois as linhas de G são uma base de C . $\square$

A proposição abaixo nos dá um método simples de determinar se uma palavra v pertence ou não a um código C . Assim, H tem a finalidade de diminuir os cálculos relacionados a um código C . E o vetor Hv^t é chamado de *síndrome* de v .

Proposição 1.35. *Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^\perp$. Temos, então, que $v \in C$ se, e somente se, $Hv^t = 0$.*

Demonstração: Temos, pelo fato de que $(C^\perp)^\perp = C$ e pelo Lema 1.34 item (ii), que $v \in C$ se, e somente se, $v \in (C^\perp)^\perp$ se, e somente se, $Hv^t = 0$. $\square$

Proposição 1.36. *Seja H a matriz teste de paridade de um código C . Temos que o peso de C é maior ou igual a s se, e somente se, quaisquer $s - 1$ colunas de H são linearmente independentes.*

Demonstração: Suponhamos, inicialmente, que cada conjunto de $s - 1$ colunas de H é linearmente independente. Seja $c = (c_1, \dots, c_n)$ uma palavra não nula de C , e sejam $h_1, \dots, h_n$ as colunas de H . Como $Hc^t = 0$, temos que

$$0 = H \cdot c^t = \sum c_i h_i \quad (1.4)$$

Visto que $w(c)$ é o número de componentes não nulas de c , segue que se $w(c) \leq s - 1$, teríamos por 1.4 uma combinação nula de um número t , com $1 \leq t \leq s - 1$, de colunas de H , o que é contraditório. Logo, $w(c) \geq s$ e, portanto, $w(C) \geq s$.

Reciprocamente, suponhamos que $w(C) \geq s$. Suponhamos também, por absurdo, que H tenha $s - 1$ colunas linearmente dependentes, digamos $h_{i_1}, \dots, h_{i_{s-1}}$. Logo, existiriam $c_{i_1}, \dots, c_{i_{s-1}}$, no corpo, nem todos nulos, tais que

$$c_{i_1} h_{i_1} + \dots + c_{i_{s-1}} h_{i_{s-1}} = 0.$$

Portanto, $c = (0, \dots, c_{i_1}, 0, \dots, c_{i_{s-1}}, 0, \dots, 0) \in C$ e consequentemente, $w(c) \leq s - 1 < s$, o que seria um absurdo. $\square$

Teorema 1.37. *Seja H a matriz teste de paridade de um código C . Temos que o peso de C é igual a s se, e somente se, quaisquer $s - 1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração: De fato, suponhamos que $w(C) = s$, logo, todo conjunto de $s - 1$ colunas de H é linearmente independente. Por outro lado, existem s colunas de H linearmente dependentes, pois, caso contrário teríamos $w(C) \geq s + 1$.

Reciprocamente, suponhamos que todo conjunto de $s - 1$ vetores colunas de H é linearmente independente e existem s colunas linearmente dependentes. Logo temos que $w(C) \geq s$. Mas $w(C)$ não pode ser maior do que s , pois, neste caso, nos diria que todo conjunto com s colunas de H é linearmente independente, o que é uma contradição. $\square$

Capítulo 2

Códigos Geometricamente Uniformes

Forney [4] generalizou os códigos de grupos de Slepian e códigos reticulados permitindo que os elementos do grupo gerador sejam isometrias arbitrárias do espaço euclidiano $\mathbb{R}^n$, ao invés de transformações ortogonais ou translações consideradas de forma separadas. Tais códigos foram denominados códigos geometricamente uniformes apresentando propriedades simétricas altamente desejáveis tais como: todas as regiões de Voronoi são congruentes, o perfil de distâncias é o mesmo para toda palavra-código, as palavras-código possuem a mesma probabilidade de erro e o grupo gerador é isomorfo a um grupo de permutações transitivas sobre as palavras-código.

2.1 Isometrias

Nesta seção definiremos isometrias daremos alguns exemplos de isometrias e grupos isométricos, em seguida definiremos uniformidade geométrica.

Definição 2.1. Seja M um espaço métrico com métrica d e T uma transformação em M , dizemos que T é uma isometria se T preserva a distância d , ou seja,

$\forall x, y \in M$ temos que

$$d(x, y) = d(T(x), T(y)).$$

Neste capítulo vamos considerar o $\mathbb{R}^n$, um n-espaco métrico com a métrica Euclidea dada por:

$$d^2(x, y) = \|x - y\|^2.$$

No $\mathbb{R}^n$ importantes classes de isometrias são:

- Translações: $t_a(x) = x + a$ para algum $a \in \mathbb{R}^n$.
- Transformações ortogonais: $r_A(x) = Ax$ onde A é uma matriz $n \times n$ ortogonal, ou seja, $A^T A = I$ onde I é a matriz identidade e A^T é a matriz transposta de A .

Definição 2.2. Uma figura geométrica S é um conjunto de pontos no $\mathbb{R}^n$. Duas figuras S_1 e S_2 são geometricamente congruentes se existe uma isometria u de $\mathbb{R}^n$ tal que $u(S_1) = S_2$.

Definição 2.3. Duas figuras S_1 e S_2 são geometricamente equivalentes se existem uma isometria u e um escalar $\alpha > 0$ tal que $u(\alpha S_1) = S_2$.

Definição 2.4. Uma isometria u de $\mathbb{R}^n$ S invariante (ou seja, $U(S) = S$) é denominada uma simetria de S .

É fácil verificar que as simetrias de um conjunto S formam um grupo com a operação composição, este grupo denotaremos por $\Gamma(S)$.

Definição 2.5. O conjunto de todas as translações simétricas de S formam um subgrupo de $\Gamma(S)$ denotado por $T(S)$. O conjunto formado por todos os vetores das translações simétricas dado por

$$\Lambda(S) = \{a; t_a \in T(S)\}$$

é um espaço vetorial de dimensão $n' \leq n$ chamado de reticulado de S .

2.2 Conjuntos de Sinais Geometricamente Uniformes

Para comunicação digital as figuras interessantes são os conjuntos de pontos discretos S , ou seja, se $s \in S$ então existe uma vizinhança $V(s)$ de s tal que $V(s) \cap S = \{s\}$.

Definição 2.6. Um conjunto de sinais S é geometricamente uniforme se dado quaisquer dois pontos $s, s' \in S$ existe uma isometria u tal que

- $u(s) = s'$
- $u(S) = S$

Um conjunto finito de sinais S geometricamente uniforme é chamado *constelação uniforme* e um conjunto infinito de sinais S é chamado de *arranjo regular*.

Exemplo 2.7. Consideremos o conjunto $S = \{(-1, -1), (-1, 1), (1, -1), (1, 1)\} \subset \mathbb{R}^2$, existem oito simetrias deste quadrado, estas simetrias são os elementos do grupo diedral D_4 , o qual pode ser representado pelo seguinte grupo de matrizes ortogonais:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Podemos notar que um conjunto S é geometricamente uniforme se a ação do grupo simétrico $\Gamma(S)$ em S for transitiva, ou se a órbita de qualquer ponto $s \in S$ sobre $\Gamma(S)$ é S .

Definição 2.8. Um *grupo gerador* $U(S)$ de S é o menor subgrupo de $\Gamma(S)$ suficiente para gerar S .

No Exemplo 2.7 podemos notar que o subgrupo formado pelas 4 primeiras matrizes é suficiente para gerar o conjunto S dado, tal subgrupo é o grupo das rotações puras R_4 , rotações por inteiros múltiplos de 90° .

2.3 Conjuntos de Sinais Geometricamente Uniformes e a Comunicação Digital

Os conjuntos de sinais mais utilizados em comunicações digitais são os conjuntos de sinais geometricamente uniformes. A seguir alguns exemplos de tais conjuntos são dados.

Exemplo 2.9. Seja $S = \{\omega^j s_0, 0 \leq j \leq M\}$ onde ω é uma raiz M -ésima primitiva da unidade e s_0 é um número complexo diferente de zero, este conjunto é um conjunto de sinais geometricamente uniforme o qual é denominado *constelação de sinais M -PSK*. Um grupo gerador natural para S é o conjunto de rotações múltiplas de $360^\circ/M$. Este grupo é isomorfo a $\mathbb{Z}_M$, o grupo dos inteiros aditivos módulo M .

O grupo simétrico de S é $\Gamma(S) = V \cdot R_M$, onde V é um grupo com dois elementos a identidade e uma reflexão pelo ponto médio, este grupo é isomorfo ao grupo M -ário diedral D_M .

Exemplo 2.10. Seja $S = \{-d, d\}$, onde $d \in \mathbb{R}$. S é um conjunto de sinais geometricamente uniforme unidimensional onde o grupo simétrico de $\Gamma(S) = V$ é isomorfo ao $\mathbb{Z}_2$. O produto cartesiano de conjuntos geometricamente uniforme é um conjunto geometricamente uniforme, basta considerarmos a composição de isometrias para cada entrada separadamente, desta forma temos que o conjunto $S = \{(-d, d, -d, d, \dots, -d, d)\}$ é uma constelação de sinais. Um grupo gerador natural para esta constelação é o grupo V^n com 2^n elementos, as n -uplas agindo em cada coordenada individualmente. Segue que V^n pode ser representado pelo conjunto de matrizes ortogonais $A = \text{diag}(-1, 1, -1, 1, \dots, -1, 1)$. O grupo V^n é isomorfo ao $(\mathbb{Z}_2)^n$.

Exemplo 2.11. O conjunto de sinais do tipo reticulado, dado por $S = \mathbb{Z}^2 + (1/2, 1/2)$, possui $T(\mathbb{Z}^2)$ como seu grupo gerador, o conjunto de todas as translações por inteiros em cada coordenada.

2.4 Propriedades Simétricas de Conjuntos de Sinais Geometricamente Uniformes

Um conjunto de sinais geometricamente uniforme S tem a importante propriedade de que cada um de seus pontos tem a mesma perspectiva com relação aos outros pontos.

Definição 2.12. Seja $s \in S$, o conjunto de todos os pontos de $\mathbb{R}^n$ que estão mais perto de s do que qualquer outro ponto $s' \in S$ é chamado a *Região de Voronoi* associada a s . Tal conjunto será denotado da seguinte forma,

$$R_V(s) = \{x \in \mathbb{R}^n : \|x - s\|^2 = \min_{s' \in S} \|x - s'\|^2\}.$$

Definição 2.13. Seja $s \in S$. O conjunto dado por,

$$DP(s) = \{\|s - s'\|^2; s' \in S\}$$

é chamado de distância perfil global.

Teorema 2.14. Se S é um conjunto de sinais geometricamente uniforme, então:

- a. Toda Região de Voronoi $R_V(s)$ tem a mesma forma e $R_V(s') = u_{ss'}[R_V(s)]$, onde $u_{ss'}$ é uma isometria que leva s em s' ;
- b. A distância perfil global $DP(s)$ é a mesma para todo $s \in S$.

Demonstração: Pela definição de Região de Voronoi, $x \in \mathbb{R}^n$ está em $R_V(s)$ se, e somente se,

$$\|x - s\|^2 = \min_{s'' \in S} \|x - s''\|^2.$$

Seja $s' \neq s$ outro ponto em S , então pela definição de uniformidade geométrica existe uma simetria $u_{ss'}$ tal que $u_{ss'}(s) = s'$. Desta forma temos que $u_{ss'}(x) \in R_V(s')$ pois

$$\begin{aligned}
\|u_{ss'}(x) - s'\| &= \|u_{ss'}(x) - u_{ss'}(s)\| & (2.1) \\
&= \|x - s\| \\
&= \min_{s'' \in S} \|x - s''\| \\
&= \min_{u_{ss'}(s'') \in S} \|u_{ss'}(x) - u_{ss'}(s'')\| \\
&= \min_{y \in S} \|u_{ss'}(x) - y\|
\end{aligned}$$

onde podemos observar que s'' varia em S , assim $y = u_{ss'}(s'')$ também varia em S . De modo análogo,

$$\begin{aligned}
DP(s) &= \{\|s - s''\|^2, s'' \in S\} & (2.2) \\
&= \{\|u_{ss'}(s) - u_{ss'}(s'')\|^2; s'' \in S\} \\
&= \{\|s' - u_{ss'}(s'')\|^2; u_{ss'}(s'') \in S\} \\
&= \{\|s' - y\|; y \in S\} \\
&= DP(s').
\end{aligned}$$

Desta forma temos que a distância perfil global é a mesma para todos os pontos. $\square$

O fato de toda região de Voronoi de um conjunto de sinais S geometricamente uniforme ter a mesma forma é uma propriedade simétrica muito forte porque a forma da região de Voronoi determina quase todas as propriedades de S que são importantes no estabelecimento do sistema de comunicação digital. A recíproca deste teorema não é verdadeira. Em [2], é mostrado que conjunto de sinais, cujas regiões de Voronoi tenham a mesma forma não implica que o mesmo seja geometricamente uniforme. Em [13] é mostrado que se um conjunto de sinais apresenta o mesmo perfil de distâncias, independente do ponto considerado, isto não implica que o mesmo seja geometricamente uniforme. Podemos tomar alguma região de Voronoi $R_V(s)$ como uma típica Região de Voronoi de um conjunto de sinais S , e chamá-la *A região de Voronoi de S* denotada por $R_V(S)$.

Da região de Voronoi de S podemos determinar as seguintes propriedades:

- a. O volume de $R_V(S)$ denominado volume fundamental de S denotado por $V(S)$ é finito se, e somente se o reticulado de S tem posto N inteiro.
- b. A distância perfil local $DP_V(S) = \{\|s - s'\|^2; s' \in S_V\}$ onde S_V é um conjunto finito de face definida de pontos s' próximos a s .
- c. De forma particular a distância $DP_V(S)$ permite determinar a distância mínima ao quadrado $d_{min}^2(S)$ entre os pontos de S , ou o "raio de empacotamento".
- d. A probabilidade de erro

$$P_r(E) = 1 - \int_{R_V(s)} (2\pi\sigma^2)^{-N/2} e^{(\|z-s\|^2/2\sigma^2)} dz,$$

onde s é o ponto transmitido sob um canal Gaussiano com variância σ^2 depende somente do quadrado da distância $\|z - s\|^2$.

O Teorema 2.14 garante que se S é geometricamente uniforme então todas estas propriedades são as mesmas para todo ponto em S .

2.5 Partições Geometricamente Uniformes

Seja S um conjunto de sinais geometricamente uniforme, U' um subgrupo normal ao grupo gerador de S , $U(S)$, e seja $U(S)/U'$ o grupo quociente correspondente as classes laterais de U' em $U(S)$. Se S é a órbita de um ponto s_0 sob $U(S)$, então as órbitas de s_0 sob as classes laterais de U' são disjuntas e a união delas é todo S .

Definição 2.15. Uma partição geometricamente uniforme denotada por S/S' é uma partição do conjunto geometricamente uniforme S com grupo gerador $U(S)$ induzida por um subgrupo normal U' de $U(S)$. Os elementos da partição S/S' são os subconjuntos de S que correspondem a classes laterais de U' em $U(S)$.

Teorema 2.16. *Seja S/S' uma partição geometricamente uniforme. Então os subconjuntos de S nesta partição são geometricamente uniformes mutuamente congruentes e têm U' como um grupo gerador comum.*

Demonstração: Se U' é um subgrupo normal de $U(S)$ então as classes laterais à esquerda e à direita de U' são idênticas. Desta forma consideremos a classe lateral à esquerda de U' , $u_a U'$, de todas as composições de alguma $u_a \in U(S)$ fixa com todas $u \in U'$. Daí temos que o subconjunto correspondente $S'(a)$ é:

$$S'(a) = \bigcup_{u \in U'} u_a [u(s_0)] = u_a \left[\bigcup_{u \in U'} u(s_0) \right] = u_a(S'). \quad (2.3)$$

Portanto, todo subconjunto $S'(a)$ é congruente a S' .

Consideremos agora uma classe lateral à direita de U' dada por $U' u_a$, segue que o subconjunto $S'(a)$ correspondente é dado por,

$$S'(a) = \bigcup_{u \in U'} u[u_a(s_0)].$$

Assim todo subgrupo $S'(a)$ é a órbita de um ponto $u_a(s_0)$ sob U' , logo $S'(a)$ é geometricamente uniforme e tem U' como grupo gerador. $\square$

Exemplo 2.17. Seja M uma potência de 2 e M' um divisor de M . Um conjunto de sinais $M - PSK$ pode ser particionado em k conjuntos de sinais $M' - PSK$, onde $k = |R_M/R_{M'}| = M/M'$. O quociente $R_M/R_{M'}$ é isomorfo a $\mathbb{Z}_{M/M'}$.

Exemplo 2.18. A constelação hipercubo n -dimensional tem como grupo gerador V^n que é isomorfo a $(\mathbb{Z}_2)^n$. Um código binário linear (n, k) é um subgrupo de $(\mathbb{Z}_2)^n$ de ordem 2^k . Pelo Teorema 2.16 este subgrupo induz uma partição geometricamente uniforme do hipercubo em 2^{n-k} partições geometricamente uniformes e mutuamente congruentes.

2.6 Rotulamentos Isométricos

Definição 2.19. Seja S um conjunto de sinais geometricamente uniforme com grupo gerador $U(S)$, U' um subgrupo normal a $U(S)$ e consideremos A um grupo isomorfo a $U(S)/U'$. Chamaremos A de grupo de rótulos das classes de U' em $U(S)$.

A partição S/S' é induzida por uma aplicação injetora entre os subconjuntos de S e os elementos de $U(S)/U'$, assim como o isomorfismo entre os grupos A e $U(S)/U'$.

Definição 2.20. A aplicação $m : A \rightarrow S/S'$ que leva um rótulo $a \in A$ no subconjunto $m(a) \in S$ induzido pela partição S/S' é denominada aplicação rótulo.

Notamos que o elemento identidade de A é levado por m em S' e $|S/S'| = |U(S)/U'| = |A|$.

Definição 2.21. Seja A um grupo de rótulos de uma partição geometricamente uniforme S/S' . Chamaremos o isomorfismo $A \simeq U(S)/U'$ de isomorfismo rotulado. A aplicação rótulo $m : A \rightarrow S/S'$ definida pela composição do isomorfismo rotulado com a aplicação injetora que leva $U(S)/U'$ em S/S' será denominada rotulamento isométrico.

O teorema a seguir mostra uma condição necessária e suficiente para se obter um rotulamento isométrico.

Teorema 2.22. *Uma aplicação rótulo $m : A \rightarrow S/S'$ é um rotulamento isométrico se, e somente se, para todo $a \in A$ existe uma isometria $u_a : S/S' \rightarrow S/S'$ tal que para todo $b \in A$, $m(ab) = u_a(m(b))$.*

Demonstração: Se $m : A \rightarrow S/S'$ é um rotulamento isométrico, do isomorfismo $A \simeq U(S)/U'$ temos $ab \mapsto u_{ab}U'$ e $ab \mapsto u_aU'u_bU' = u_{ab}U'$ de onde obtemos,

$$\begin{aligned} u_{ab}U' &= u_a u_b U' = \{(u_a u_b)u(s_0); u \in U'\} \\ &= \{u_a[u_b u(s_0)]; u \in U'\} = u_a(m(b)). \end{aligned} \tag{2.4}$$

Reciprocamente, se $m(ab) = u_a(m(b)) \forall a, b \in A$ então $u_{ab}(S') = u_a u_b(S')$, isto implica que $m(ab) = m(a)m(b)$, portanto m é um homomorfismo, desta forma o rotulamento é isométrico. □

2.7 Propriedades Elementares dos Rotulamentos Isométricos

Dado um rotulamento isométrico $m : A \rightarrow S/S'$ existem várias transformações de rotulamentos simples que resultam em rotulamentos isométricos. A seguir apresentaremos alguns resultados elementares dos rotulamentos isométricos.

Proposição 2.23. *Se $m : A \rightarrow S/S'$ é um rotulamento isométrico e $T : A \rightarrow A$ é um automorfismo, então o rotulamento $mT : A \rightarrow S/S'$ definido por $a \mapsto m[T(a)]$ é também um rotulamento isométrico.*

Demonstração: Como T é um automorfismo de A temos que T leva todos elementos de A em elementos de A , logo como m é um rotulamento isométrico temos que mT também é um rotulamento isométrico. □

Proposição 2.24. *Se $m : A \rightarrow S/S'$ é um rotulamento isométrico então o rotulamento $mt_b : A \rightarrow S/S'$ definido por $a \mapsto m(ab)$ para algum $b \in A$ é também um rotulamento isométrico.*

Demonstração: Como m é um rotulamento isométrico temos pelo Teorema 2.22 que existe uma isometria $u_a : S/S' \rightarrow S/S'$ tal que $m(ab) = u_a(m(b))$, $\forall a, b \in A$. Logo temos que mt_b é um rotulamento isométrico. □

As duas proposições acima implicam que se a partição S/S' admite um rotulamento isométrico com grupo de rótulos A , então alguma transformação afim definida

por $a \mapsto T(a) + b$ onde $a, b \in A$, também produz um rotulamento isométrico. É interessante notar que em um espaço onde a métrica natural é a métrica de Hamming uma transformação é uma isometria.

Proposição 2.25. *Se $m : A \rightarrow S/S'$ é um rotulamento isométrico, e u é uma simetria em $U(S)$, então o rotulamento $u \cdot m : A \rightarrow S/S'$ definido por $a \mapsto u[m(a)]$ é um rotulamento isométrico.*

Demonstração: A demonstração desta proposição decorre diretamente do Teorema 2.22. □

2.8 Rotulamentos Binários Isométricos

Nesta seção estamos interessados em partições S/S' que admitem rotulamentos isométricos por alfabetos $n - bit$ binários, ou seja, alfabetos da forma $A = (\mathbb{Z}_2)^n$. A seguir definiremos um *Rotulamento Binário de Ungerboeck*.

Definição 2.26. Consideremos uma partição S/S' geometricamente uniforme 2^n -caminhos. Se existe um refinamento desta partição em n partições 2-caminhos, $S = S_0/S_1/.../S_n = S'$ tal que os rótulos dos 2^n subconjuntos são escolhidos em $(\mathbb{Z}_2)^n$ de modo que os rótulos de todos os subconjuntos do j -ésimo nível que pertencem a um mesmo subconjunto tenham as últimas coordenadas iguais, então este rotulamento é chamado de Ungerboeck.

A distância mínima quadrada entre dois pontos com rótulos a e a' é maior ou igual a $d_{min}^2(S_j)$ onde j é o número de zeros na soma $mod 2$ de $a \oplus a'$. Esta distância recebe o nome de *distância limite de Ungerboeck*.

Teorema 2.27. *Se S/S' é uma partição geometricamente uniforme que admite um rotulamento binário isométrico, e $S = S_0/S_1/.../S_n = S'$ é uma cadeia de partições 2-caminhos geometricamente uniformes, então S/S' admite um rotulamento isométrico de Ungerboeck consistente com esta cadeia.*

Demonstração: Se S/S' admite um rotulamento binário isométrico então existem grupos geradores $U(S)$ e $U(S')$ tais que $U(S)/U(S') \simeq (\mathbb{Z}_2)^n = A$, e se

$$S = S_0/S_1/\dots/S_n = S'$$

é uma cadeia de partições geometricamente uniformes, então existe uma cadeia correspondente de grupos geradores

$$U(S) = U(S_0)/U(S_1)/\dots/U(S_n) = U(S').$$

Seja A_j a posição do conjunto de rótulos incluído no subconjunto S_j de S . A cadeia correspondente

$$A = A_0/A_1/\dots/A_n = \{0\}$$

é uma cadeia de espaços vetoriais binários, onde a dimensão de A_j é igual a $n - j$. Consideremos a respectiva classe não nula na partição A_j/A_{j+1} , $0 \leq j \leq n - 1$ tomada como algum rótulo $(x)^{n-j-1}(10)^j$ onde $x, (10) \in (\mathbb{Z}_2)^2$. Então temos que $A_j/A_n = A_j$ o espaço vetorial binário $(n - j)$ dimensional consistindo de todos os rótulos $x^{n-j}(10)^j$ e os subconjuntos no j -ésimo nível consistem da união de todos n -ésimos subconjuntos que têm um $j - bit$ em comum em seu rótulo. Temos assim um rotulamento de Ungerboeck. $\square$

Os bits conduzidos no rotulamento de Ungerboeck são chamados *bits mais significantes* e os bits restantes são chamados *bits menos significantes*.

Corolário 2.28. *Uma partição tipo reticulado $S = \Lambda + \tau$ em classes laterais de um subreticulado Λ' admite um rotulamento de Ungerboeck se $\mathbb{Z}^n/\Lambda/\Lambda'/4\mathbb{Z}^n$ forma uma cadeia de partições reticulada.*

Demonstração: Existe um rotulamento isométrico de Ungerboeck $2n - bits$ de $\mathbb{Z}^n/4\mathbb{Z}^n$, se $|\mathbb{Z}^n/\Lambda| = 2^j$ e $|\Lambda'/4\mathbb{Z}^n| = 2^{2n-j'}$, então um rotulamento de Ungerboeck de Λ/Λ' pode ser obtido se desconsiderarmos os $(2n - j')$ - *bits* mais significantes e os $j - bits$ menos significantes do rotulamento de $\mathbb{Z}^n/4\mathbb{Z}^n$. $\square$

Os reticulados de $\mathbb{Z}^n$ que têm como um subreticulado o $4\mathbb{Z}^n$ são chamados de *reticulados binários mod 4* e as partições Λ/Λ' tal que $\mathbb{Z}^n/\Lambda/\Lambda'/4\mathbb{Z}^n$ é uma cadeia de partições reticulada, são chamadas de partições de profundidade $\mu \leq 4$. Assim todas as partições de profundidade $\mu \leq 4$ admitem rotulamentos isométricos de Ungerboeck.

2.9 Códigos Geometricamente Uniformes em Espaços de Sinais

Dado uma partição geometricamente uniforme S/S' e um rotulamento isométrico com um grupo de rótulos A , a especificação de um código em espaço de sinais $\mathbb{C}$ é completa se for especificado um código rótulo C cujos elementos são seqüências de rótulos que selecionam uma seqüência de subconjuntos de S através do rotulamento isométrico. Devemos notar que C é um grupo código sobre o grupo rótulo A .

2.9.1 Espaços de Seqüências

Seja S/S' uma partição geometricamente uniforme e A um grupo de rótulos associado a esta partição, temos que um espaço de A^I é o conjunto de todas as seqüências $a = \{a_k; k \in I\}$ onde os elementos a_k pertencem ao grupo de rótulos A e o conjunto de índices I é um subconjunto dos inteiros $I \subset \mathbb{Z}$. Se I é finito, ou seja, $I = \{k; 1 \leq k \leq n\}$ então A^I é o produto n cartesiano de A . Se I é infinito temos que A^I é o produto cartesiano infinito de A . Se A é um grupo com a operação binária $*$ então o espaço de seqüências A^I também é um grupo sob $*$ usando a extensão usual, isto é, $\forall a, b \in A^I, a * b = \{a_k * b_k; k \in I\}$. A seguir definiremos um código sobre o alfabeto A .

Definição 2.29. Um código C sobre o grupo de rótulos A é um conjunto de seqüências de elementos de A . Tal código é um subconjunto do espaço de seqüências A^I .

2.9.2 Códigos em Espaços de Sinais

Um código rótulo C sobre um grupo de rótulos A define um código em um espaço de sinais como segue:

Definição 2.30. Sejam S/S' uma partição geometricamente uniforme, C um código rótulo sobre o alfabeto A , I o conjunto de índices e $m : A \rightarrow S/S'$ uma aplicação rótulo. Um código em um espaço de sinais é a união disjunta

$$\mathbb{C}(S/S'; C) = \bigcup_{c \in C} m(c)$$

das seqüências de subconjuntos $m(c) = \{m(c_k); k \in I\}$.

Uma seqüência de sinais s é uma seqüência de códigos em $\mathbb{C}(S/S'; C)$ se $s \in m(c)$ para algum $c \in C$, isto é, se $s = \{s_k \in m(c_k); k \in I\}$. Desta forma temos que um código em espaço de sinais $\mathbb{C}(S/S'; C)$ é um subconjunto do espaço de seqüências S^I , o conjunto de todas as seqüências de elementos do conjunto de sinais S .

Exemplo 2.31. Se S é um subconjunto de $\mathbb{R}^n$, então S^I e $\mathbb{C}(S/S'; C)$ são subconjuntos do espaço de seqüências $(\mathbb{R}^n)^I$, o conjunto de todas as seqüências reais de n -*uplas*. O produto cartesiano $(\mathbb{R}^n)^I$ é ainda um espaço Euclidiano com a métrica usual do espaço Euclidiano.

Uma codificação para um código rótulo C gera uma seqüência de códigos rótulos $c = \{c_k\}$ que permanecem em C . A seqüência particular c é determinada por uma seqüência apropriada de entrada de dados.

A seqüência rótulo c é então aplicada a uma seqüência de subconjuntos $m(c) = \{m(c_k); k \in I\}$ através da aplicação rótulo m . Uma segunda operação então seleciona uma específica seqüência de sinal $s \in m(c)$ para transmissão sobre o canal, de acordo com uma segunda seqüência de entrada de dados. A segunda operação é de importância secundária uma vez que as propriedades do código gerador para tal codificação são determinadas primeiramente pelas propriedades do código em espaço de sinais $\mathbb{C}(S/S'; C)$ que são determinadas no primeiro nível.

2.9.3 Classes Laterais de Códigos Generalizadas

Sejam S/S' uma partição geometricamente uniforme gerada pelo grupo gerador da partição $U(S)/U(S')$, A um grupo rótulo isomorfo a $U(S)/U(S')$ abeliano, $m : A \rightarrow S/S'$ um rotulamento isométrico e C um grupo código sobre o espaço de seqüências A^I . Como A é um grupo abeliano temos que A^I é também um grupo abeliano e qualquer subgrupo C de A^I é um subgrupo normal. A seguir definiremos uma classe lateral de código generalizada .

Definição 2.32. Uma classe lateral de código generalizada $\mathbb{C}(S/S'; C)$ é o conjunto de todas as seqüências de sinais $s \in m(c); c \in C$.

Podemos notar que o rotulamento $m : A \rightarrow S/S'$ pode ser estendido para $m : A^I \rightarrow (S/S')^I$ sem perder as suas propriedades e que a partição $(S/S')^I = S^I/S'^I$ é também uma partição geometricamente uniforme. Se o grupo gerador de S é $U(S)$ temos que o grupo gerador do conjunto de sinais S^I é o grupo $[U(S)]^I$ pois cada elemento $s = \{s_k\} \in S^I$ pode ser levado em algum outro elemento de S^I por composição de isometrias em $U(S)$ agindo em cada componente s_k de s individualmente. Além disso, se $U(S')$ é um subgrupo normal de $U(S)$ então $[U(S')]^I$ é um subgrupo normal de $[U(S)]^I$ logo o grupo quociente $[U(S')]^I/[U(S)]^I$ induz a partição geometricamente uniforme S^I/S'^I de S^I . O espaço rótulo A^I é isomorfo a $[U(S')]^I/[U(S)]^I$, desta forma temos que a aplicação rótulo estendida $m : A^I \rightarrow (S/S')^I$ é um rotulamento isométrico.

Se C é um subgrupo de A^I então $\mathbb{C}(S/S'; C)$ é um subgrupo de S^I , e o quociente $S^I/\mathbb{C}$ é isomorfo a A^I/C , sobre a estrutura de grupo induzida a S^I por $[U(S)]^I$. Além disso, S'^I é um subgrupo de $\mathbb{C}$ e a cadeia $S^I/\mathbb{C}/S'^I$ é isomorfa a $A^I/C/\{0\}^I$.

A seguir definiremos um rótulo transladado a partir de uma classe lateral de C .

Definição 2.33. As classes laterais de C podem ser escritas como $C \oplus a$, onde $a \in A^I$. Para cada classe lateral o rotulamento $m : A^I \rightarrow (S/S')^I$ define subconjun-

tos de S^I chamados de rótulos transladados de $\mathbb{C}$ dados por

$$\mathbb{C}(S/S'; C \oplus a) = \bigcup_{c \in C} m(c \oplus a).$$

Os rótulos transladados de $\mathbb{C}$ são as classes laterais de $\mathbb{C}$ em S^I sobre a estrutura de grupo induzida.

Teorema 2.34. *Se $\mathbb{C}(S/S'; C)$ é uma classe lateral generalizada de códigos, então $S^I/\mathbb{C}/S'^I$ é uma cadeia de partições geometricamente uniformes, e os rótulos transladados $\mathbb{C}(S/S'; C \oplus a)$ de $\mathbb{C}$ são geometricamente uniformes, mutuamente congruentes e tem $U(\mathbb{C})$ como grupo gerador em comum.*

Demonstração: Seja $S^I/\mathbb{C}/S'^I$ estabelecida como uma cadeia de partições geometricamente uniforme com a estrutura de grupo induzida sobre S^I por $[U(S)]^I$ como observamos acima. Desta forma temos que o Teorema 2.34 é um simples corolário do Teorema 2.16. $\square$

O teorema acima nos garante que qualquer classe lateral generalizada de código $\mathbb{C}$ é geometricamente uniforme. Além disso, ele afirma que o conjunto S^I de todas as seqüências de sinais em S tem uma partição no rótulo transladado de $\mathbb{C}$ que é congruente a $\mathbb{C}$. Segue então de forma direta o seguinte corolário.

Corolário 2.35. *Se $\mathbb{C}$ é uma classe lateral de código generalizada, então:*

- a. *A região de Voronoi associada a quaisquer duas seqüências de códigos $s, s' \in \mathbb{C}$ são congruentes.*
- b. *A distância perfil $DP(s) = \{\|s - s'\|^2; s' \in \mathbb{C}\}$ de uma seqüência $s \in \mathbb{C}$ para toda seqüência $s' \in \mathbb{C}$ independe da seqüência s .*

Muitos códigos em espaços Euclidianos são baseados nos códigos binários lineares C sobre o corpo binário $F = \mathbb{Z}_2$.

Exemplo 2.36. O produto n-cartesiano do rotulamento binário usual $m : \{0, 1\} \rightarrow \{-1, +1\}$ do conjunto de sinais binário é um rotulamento binário isométrico do hipercubo N-dimensional usando o alfabeto rótulo F^n .

Qualquer subgrupo aditivo de F^n é também um espaço vetorial de alguma dimensão k sobre F , isto é, um (n, k) bloco binário linear do código C . Consequentemente os códigos de espaços binários $\mathbb{C}$ correspondentes a qualquer bloco binário de código C são geometricamente uniformes. As classes de C aplicadas em conjuntos de sinais geometricamente uniformes são todas congruentes a $\mathbb{C}$, e $\mathbb{C}$ e suas classes laterais formam assim uma partição do hipercubo.

2.10 Outras Noções de Uniformidade

Nesta seção compararemos as noções de uniformidade usadas até agora com outros tipos de simetrias que serão previamente introduzidos.

2.10.1 Linearidade

Para partições Λ/Λ' de um reticulado Λ em classes laterais de um subreticulado Λ' de Λ , é possível ter um rotulamento que é linear no seguinte sentido.

Definição 2.37. Um rotulamento $m : \Lambda \rightarrow \Lambda/\Lambda'$ definido por $m(a) = \Lambda' + t(a)$, onde $t(a) \in \mathbb{R}^n$, de uma partição reticulada é linear se:

$$\begin{aligned} m(a \oplus b) &= \Lambda' + t(a \oplus b) \\ &= \Lambda' + t(a) + t(b) \\ &= m(b) + t(a) \end{aligned}$$

onde $+$ é a adição em $\mathbb{R}^n$.

Pelo Teorema 2.22 um rotulamento linear é um rotulamento isométrico com a isometria u_a dada pela translação $t(a)$. Isto implica que $t(0)$ deve ser um elemento de Λ' pois $m(0) = \Lambda' + t(0) = \Lambda'$.

Se $\mathbb{C}(\Lambda/\Lambda'; C)$ é um código em espaço de sinais baseado numa partição reticulada Λ/Λ' e em um rotulamento linear, então $\mathbb{C}$ é linear no sentido de que $\mathbb{C}$ é um grupo aditivo sob uma seqüência aditiva no espaço de seqüências $(\mathbb{R}^n)^I$. Sejam s

e s' quaisquer duas seqüências de códigos em $\mathbb{C}$, pertencentes às classes laterais de seqüências $(\Lambda')^I + t(c)$ e $(\Lambda')^I + t(c')$, respectivamente. Então a seqüência $s + s'$ pertence a classe lateral $(\Lambda')^I + t(c) + t(c') = (\Lambda')^I + t(c \oplus c')$ e está em $\mathbb{C}$, assim como $c \oplus c'$ está no código C .

Uma classe lateral de um código tipo reticulado é um código em espaço de sinais $\mathbb{C}[(\Lambda + \tau)/\Lambda'; C]$ baseada na partição do translado $\Lambda + \tau$ de Λ em classes laterais de Λ' . Temos que

$$\mathbb{C}[(\Lambda + \tau)/\Lambda'; C] = \mathbb{C}(\Lambda/\Lambda'; C) + \tau^I$$

assim tal código é meramente um translado de um código $\mathbb{C}(\Lambda/\Lambda'; C)$ baseado na partição do próprio Λ . Ele não é rigorosamente linear, mas pode ser considerado efetivamente linear. Alternativamente ele pode ser considerado como uma classe lateral generalizada de códigos com um rotulamento isométrico onde todas as isometrias são translações.

Lema 2.38. *Um grupo G é isomorfo a $(\mathbb{Z}_2)^n$ para algum inteiro positivo n se, e somente se, G é um grupo finito tal que todo elemento $g \in G$ satisfaz $g^2 = e$ onde e é o elemento neutro de G .*

Demonstração: Se $G \simeq (\mathbb{Z}_2)^n$, então G é finito e abeliano e qualquer g satisfaz $g^2 = e$. Reciprocamente, se todo elemento de G é seu próprio inverso, então para quaisquer $a, b \in G$ temos que $(ab)^2 = e$ que implica que $ab = b^{-1}a^{-1} = ba$, assim G é abeliano. Denotaremos a identidade de G por 0 e a operação de G por $+$. Como G é abeliano e todo elemento de G é seu próprio inverso temos que $g + g = 0$, a soma envolvendo múltiplos de algum $g \in G$ depende somente se o número de ocorrências é par ou ímpar. Agora se $G \neq \{0\}$, escolha algum $g_1 \in G$ não nulo, o grupo gerado por g_1 é portanto um grupo de dois elementos $G_1 = \{0, g_1\}$. Se $G = G_1$ a afirmativa é verdadeira. Se $G \neq G_1$ escolha g_2 não nulo tal que g_2 não pertença a G_1 , o grupo gerado por $\{g_1, g_2\}$ é o grupo $G_2 = \{\sum_{1 \leq j \leq 2} a_j g_j; a_j \in \{0, 1\}\}$. Se $G \neq G_2$ continue

este processo que é finito pois G é finito. A correspondência

$$\sum_{1 \leq j \leq n} a_j g_j \leftrightarrow a \in (\mathbb{Z}_2)^n$$

é então um isomorfismo entre G e $(\mathbb{Z}_2)^n$.

□

Portanto Λ/Λ' é isomorfo a $(\mathbb{Z}_2)^n$ se, e somente se, cada classe não nula de Λ' em Λ é sua própria inversa sobre a adição módulo Λ' .

Teorema 2.39. *Se Λ' é um subreticulado de Λ e Λ/Λ' é finito então existe um rotulamento binário linear de Λ/Λ' se, e somente se, 2Λ é um subreticulado de Λ' .*

Demonstração: Seja $\Lambda' + t$, $t \in \Lambda$, alguma classe lateral de Λ' em Λ . Então $(\Lambda' + t) + (\Lambda' + t) = \Lambda' + 2t$ é igual a classe lateral do zero se, e somente se, $2t \in \Lambda'$. Segue que, toda classe lateral de Λ' em Λ é inversa dela mesma se, e somente se, $2t \in \Lambda' \forall t \in \Lambda$, isto é, se, e somente se, 2Λ é um subreticulado de Λ' . □

Muitas classes laterais generalizadas de códigos $\mathbb{C}(\Lambda/\Lambda'; C)$ que utilizam códigos binários C são baseadas em partições reticuladas Λ/Λ' que não admitem rotulamentos binários lineares isométricos.

Exemplo 2.40. Não existe rotulamento binário linear da partição 4-caminhos $\mathbb{Z}/4\mathbb{Z}$ por $A = (\mathbb{Z}_2)^2$, visto que se a é o rótulo para a classe lateral $4\mathbb{Z} + 1$, então $a \oplus a = (00)$ precisa aplicar-se a $4\mathbb{Z}$, não a $4\mathbb{Z} + 2$, assim a linearidade não pode ser obtida.

2.10.2 Subconjunto Tempo-Zero

Nesta subseção definiremos subconjunto *Tempo-Zero* utilizando códigos binários lineares convolucionais. A seguir daremos a definição de códigos convolucionais.

Definição 2.41. Um código convolucional é um tipo de código corretor de erro em que cada conjunto de m sinais é transformado em um conjunto de n sinais, onde $n \geq m$.

Seja $\mathbb{C}(S/S'; C)$ um código em um espaço de sinais reticulado, com C um código binário linear convolucional de índice k/n . Então quando a codificação está no estado "zero" a próxima codificação pode produzir 2^k valores $a \in F^n$. Se C é linear estes valores formam um grupo aditivo ou um subespaço de F^n . Este subespaço denotado por C_0 é denominado código *Tempo-Zero*.

Definição 2.42. Seja

$$m(C_0) = \{m(a); a \in C_0\}$$

a imagem do código tempo-zero. Este conjunto recebe o nome de *subconjunto de tempo-zero* do conjunto de sinais S .

Se $\mathbb{C}$ é uma classe lateral generalizada de códigos, então o Teorema 2.16 aplica-se de forma direta ao Teorema 2.43 enunciado abaixo.

Teorema 2.43. *Se S/S' é uma partição geometricamente uniforme com um rotulamento isométrico binário $m : A \rightarrow S/S'$, onde $A = (\mathbb{Z}_2)^n$, então:*

- i. *O subconjunto Tempo-zero $m(C_0)$ é geometricamente uniforme.*
- ii. *Os rótulos transladados $m(C_0 \oplus b)$ são todos congruentes a $m(C_0)$*
- iii. *A partição 2^{n-k} -caminhos de S no rótulo transladado $mC_0 \oplus b$ é uma partição geometricamente uniforme.*

A maior parte dos códigos reticulados utilizam códigos convolucionais binários C de taxa $k/(k+1)$. Neste caso existem apenas dois rótulos transladados, o subconjunto tempo-zero $m(C_0)$ e seu complemento.

2.10.3 Rotulamentos Regulares

Definiremos abaixo duas noções de regularidades, primeiramente uma noção fraca e em seguida uma noção forte de regularidade.

Definição 2.44. Uma aplicação rótulo $m : A \rightarrow \Lambda/\Lambda'$ definida por $m(a) = \Lambda' + t(a)$ é regular no sentido fraco se a distância mínima ao quadrado entre os elementos de duas classes laterais depende somente da diferença dos rótulos:

$$d_{min}^2[m(a), m(a')] = d_{min}^2[\Lambda' + t(a), \Lambda' + t(a')] = N^2(-a \oplus a')$$

Definição 2.45. Uma aplicação rótulo $m : A \rightarrow \Lambda/\Lambda'$ definida por $m(a) = \Lambda' + t(a)$ é regular no sentido forte se o conjunto das distâncias entre qualquer elemento da classe lateral $\Lambda' + t(a)$ e todos os elementos de outra classe lateral $\Lambda' + t(a')$ dependem somente da diferença dos rótulos, isto é, se o peso perfil de qualquer diferença $\Lambda' - t(a) + t(a')$ é igual ao peso perfil da classe lateral $\Lambda' - t(0) + t(-a \oplus a')$.

Segue então que regularidade no sentido forte implica em regularidade no sentido fraco.

Proposição 2.46. *Um rotulamento isométrico de uma partição reticulada é regular no sentido forte.*

Demonstração: Se $m(a) = \Lambda' + t(a)$ é um rotulamento isométrico, então pelo Teorema 2.22 existe uma isometria u_{-a} tal que:

$$m(-a \oplus a') = \Lambda' + t(-a \oplus a') = u_{-a}[\Lambda' + t(a)];$$

$$m(-a \oplus a) = m(0) = \Lambda' + t(0) = u_{-a}[\Lambda' + t(a)].$$

Como u_{-a} é uma isometria, o conjunto das distâncias de qualquer elemento de $\Lambda' + t(a)$ a todos os elementos de $\Lambda' + t(a')$ é o mesmo conjunto de distâncias de qualquer elemento de $\Lambda' + t(0)$ a todos elementos de $\Lambda' + t(-a \oplus a')$, que tem o mesmo peso perfil da classe lateral $\Lambda' - t(0) + t(-a \oplus a')$, que depende somente da diferença entre rótulo $-a \oplus a'$. $\square$

Assim mostramos que existe um rotulamento binário isométrico e portanto regular no sentido forte para qualquer partição Λ/Λ' tal que $\mathbb{Z}^n/\Lambda/\Lambda'/4\mathbb{Z}^n$ é uma partição reticulada.

Capítulo 3

Códigos Hiperbólicos

Geometricamente Uniformes

Neste capítulo generalizaremos o conceito de códigos geometricamente uniformes, primeiramente explorados em espaços Euclidianos, aos espaços Hiperbólicos. Também mostraremos uma caracterização de classes laterais generalizadas de códigos através do conceito de códigos G-lineares.

Um dos principais objetivos de códigos geometricamente uniformes é a construção de partições geometricamente uniformes e em particular classes laterais generalizadas.

Estenderemos os conceitos de conjuntos de sinais, reticulados e conjuntos particionados para o plano hiperbólico, marcando assim o uso das tesselações hiperbólicas regulares associadas aos seus correspondentes grupos de simetrias.

Embora os grupos de isometrias hiperbólicos tenham maior complexidade que os grupos de isometrias Euclidianos os procedimentos e os conceitos para partições geometricamente uniformes podem ser considerados os mesmos.

Em [3] é mostrado que a probabilidade de erro associada a uma constelação de sinais depende da curvatura k , tendo melhor performance quando consideradas superfícies com curvatura constante negativa.

3.1 Tesselações Hiperbólicas

Para a Teoria da Comunicação uma das estruturas algébricas mais importantes é o espaço vetorial, que é um espaço cuja a métrica é compatível com a norma, por exemplo os espaços Euclidianos. O uso desta estrutura possibilita modelar e analisar novos sistemas de comunicação, novos esquemas de modulação, técnicas de processamento de sinais entre outras. A seguir definiremos uma tesselação regular no plano hiperbólico SPD .

Definição 3.1. Uma tesselação regular do plano hiperbólico SPD é uma partição de SPD por polígonos regulares com o mesmo número de lados os quais se interceptam inteiramente ou apenas nos vértices. Uma tesselação regular na qual q polígonos regulares se encontram em cada vértice é denotada por $\{p, q\}$.

Associado com cada tesselação $\{p, q\}$ existe um grupo chamado grupo simétrico de $\{p, q\}$ e denota-se por $[p, q]$. Este grupo é o grupo de isometrias de SPD , gerado por reflexões em retas hiperbólicas em que as tesselações $\{p, q\}$ auto refletem. O grupo $[p, q]$ é gerado pelas reflexões r_1 , r_2 e r_3 no bordo do triângulo hiperbólico com ângulos $\frac{\pi}{2}$, $\frac{\pi}{p}$, $\frac{\pi}{q}$.

A apresentação do grupo $[p, q]$ associado com a tesselação $\{p, q\}$ é dada por,

$$\langle r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_2 r_1)^p = (r_3 r_2)^q = (r_1 r_3)^2 = e \rangle$$

Dado uma tesselação $\{p, q\}$ com grupo simétrico $[p, q]$ a tesselação dual desta é $\{q, p\}$ com grupo simétrico $[q, p]$. Os grupos $[p, q]$ e $[q, p]$ são isomorfos, entretanto as tesselações $\{p, q\}$ e $\{q, p\}$ coincidem se, e somente se, $p = q$. O caso $p = q$ é chamado de dual próprio.

Se $p = q = 4g$, onde g é um inteiro maior ou igual a 2, a tesselação $\{4g, 4g\}$ produz uma cobertura universal para SPD . O grupo fundamental desta superfície de gênero g dado por

$$\pi_g = \langle a_1, \dots, a_g, b_1, \dots, b_g : \prod_{i=1}^g [a_i, b_i] = 1 \rangle$$

é um subgrupo normal de $[4g, 4g]$. Desta forma segue que o grupo $[4g, 4g]$ pode ser escrito como o produto semidireto

$$[4g, 4g] = \pi_g \ltimes D_{4g},$$

onde D_{4g} denota o grupo diedral com $8g$ elementos. Para maiores informações sobre tesselações ver [7].

3.2 Conjuntos de Sinais Associados a Grupos

Assim como no espaço Euclideano um conjunto de sinais em um espaço hiperbólico é um subconjunto discreto de SPD .

Definição 3.2. Um conjunto de sinais S em SPD se corresponde com um grupo G , se existe uma aplicação sobrejetiva $m : G \rightarrow S$ tal que $\forall g, g' \in G$ $d(m(g), m(g')) = d(m(g^{-1}g'), m(e))$. Tal aplicação m é denominada aplicação correspondência. Se m é injetiva, então m^{-1} é um rotulamento de correspondência.

Se $m : G \rightarrow S$ é uma aplicação correspondência então $H = m^{-1}(m(e))$ é um subgrupo de G e $g \equiv g' \text{ mod } H$ se, e somente se, $m(g) = m(g')$. Assim para cada aplicação correspondência m podemos estabelecer uma correspondência bijetiva entre as classes laterais gH e os elementos $m(g)$ de S . Imediatamente segue que se $H \trianglelefteq G$, então a aplicação $m : \frac{G}{H} \rightarrow S$ é um rotulamento de correspondência.

Dizemos que um rotulamento $m : G \rightarrow S$ é um *rotulamento efetivo* se H não contém nenhum subgrupo normal não trivial de G . Neste caso, dizemos que S é efetivamente correspondido à G .

Exemplo 3.3. Seja A um espaço métrico com uma métrica invariante d_A e G um grupo com uma métrica de grupo d_G tal que existe uma aplicação $m : G \rightarrow A$ que é uma isometria. Então para quaisquer $g, h \in G$ temos

$$d_A(m(g), m(h)) = d_G(g, h) = d_G(gh^{-1}, e) = d_A(m(gh^{-1}), m(e))$$

resultando que m é um rotulamento de correspondência.

A seguir definiremos um código G-linear onde G é um grupo.

Definição 3.4. Um código $C \subseteq S^I$ é G-linear se existe uma isometria $\mu : G \rightarrow S$, um grupo código $D \leq G^I$ e uma permutação $\sigma \in S^I$ tal que $\sigma(C) = \mu(D)$, μ também denota a extensão $\mu : G^I \rightarrow S^I$.

3.3 Conjuntos de Sinais Geometricamente Uniformes Hiperbólicos

Conforme Definição 2.6 dada no Capítulo 2 um conjunto de sinais S é chamado geometricamente uniforme se a ação do grupo de simetrias $\Gamma(S)$ em S é transitiva.

Exemplo 3.5. Considere a tesselação $\{8, 8\}$ no plano hiperbólico. Então o conjunto S consistindo de centro de massa dos octógonos da tesselação (ou equivalentemente os vértices dos octógonos da tesselação dual) é geometricamente uniforme, para cada $x \in S$ fixo, temos que $S = \{T(x) : T \in [8, 8]\}$.

Slepian, [12] nos fornece um exemplo de um conjunto de sinais S com 10 sinais em $\mathbb{R}^5$ que não é órbita de qualquer subgrupo de simetrias de $\mathbb{R}^5$. Portanto nem todos os subconjuntos de sinais, mesmo os euclidianos, são geometricamente uniformes.

Como já vimos no Capítulo 2 um subgrupo $U(S)$ de $\Gamma(S)$ é um gerador de S , se $S = \{u(s_0); u \in U(S)\}$.

3.4 Partições Geometricamente Uniformes Hiperbólicas

O conceito de partições geometricamente uniformes mostrado no Capítulo 2 foi introduzido por Forney em [4], no contexto de conjuntos de sinais Euclidianos. Como mencionado anteriormente embora os grupos de isometria hiperbólicos

tenham uma maior complexidade quando comparados aos grupos de isometrias euclidianos, é possível estender o conceito de partições geometricamente uniformes, como exemplificaremos nesta seção.

Exemplo 3.6. As partições de Ungerboeck [15] são partições binárias geometricamente uniformes associadas com um conjunto de sinais $M - PSK$ com $M = 2^k$ e os subgrupos da forma $2^j - PSK$ (não necessariamente normais) determinam uma sequência de partições. Os polígonos S associados às tesselações hiperbólicas (p polígonos regulares) têm D_p como seu grupo de simetrias. Assim os polígonos S são constelações geradas por $p - PSK$.

Exemplo 3.7. No caso Euclidiano, se Λ é um reticulado e Λ' é um subreticulado de Λ de índice finito, então o conjunto de sinais $S = \Lambda + a$ é particionado em $|\Lambda/\Lambda'|$ subconjuntos geometricamente uniformes.

No caso hiperbólico temos alguns pontos a considerar. Como a tesselação dual é gerada por translações então uma condição equivalente a $T(\Lambda) = \Lambda$, onde T denota translação, é exatamente o fato de a tesselação ser auto-dual, do tipo $\{p, p\}$.

3.5 Códigos Geometricamente Uniformes em Espaço de Sinais Hiperbólicos

Seja S/S' uma partição geometricamente uniforme no espaço hiperbólico induzida pelo grupo $U(S)/U(S')$. Seja $A \simeq U(S)/U(S')$, os conceitos de *isomorfismo rótulo* e *rotulamento isométrico* dados no Capítulo 2 se aplicam também a essa partição.

Definição 3.8. Seja S/S' uma partição geometricamente uniforme com grupo rótulo A e $D \trianglelefteq A^I$ então uma classe lateral generalizada de códigos é o subconjunto

$$\mathbb{C}(S/S'; D) = \{m(c) : c \in D\} \subseteq S^I.$$

O próximo teorema promove uma conexão entre G-linearidade e as classes laterais generalizadas de códigos.

Teorema 3.9. *Sobre as hipóteses da Definição 3.8 uma classe lateral generalizada de códigos é um código $U(S)$ – linear.*

Demonstração: Seja

$$\begin{aligned}\mu : U(S) &\rightarrow S \\ u &\mapsto u(s_0)\end{aligned}\tag{3.1}$$

um rotulamento de correspondência para algum ponto fixo $s_0 \in S$.

Tomemos

$$A = U(S)/U(S') = \{uU(S'); u \in U(S)\}$$

e o rotulamento

$$\begin{aligned}m : A &\rightarrow S/S' \\ uU(S') &\mapsto u(S').\end{aligned}\tag{3.2}$$

Temos que se $uU(S') = vU(S')$ então $u^{-1}v \in U(S')$ onde $u^{-1}v(S') = S'$, portanto $u(S') = v(S')$.

Seja $H = \{u \in U(S); uU(S') \in D\}$. Assim se $u, v \in H$, $uU(S'), vU(S') \in D$, como $D \leq A$ segue que $uv^{-1}U(S') \in D$ e $uv^{-1} \in H$. Desta forma, como $e \in H$ temos que $H \leq U(S)$. Em outras palavras, como

$$\mu(H) = \{u(s_0) : u \in H\} = \bigcup_{uU(S') \in D} u(S') = \bigcup m(c) = \mathbb{C}(S/S'; D),$$

isso mostra que $\mathbb{C}(S/S'; D)$ é $U(S)$ – linear. $\square$

No contexto hiperbólico, uma generalização da definição euclideana dada no Capítulo 2 de classes laterais generalizadas de códigos nos obriga a condição que o código D seja um subgrupo normal de A^I .

O próximo teorema nos assegura a validade da seguinte versão do Teorema 2.34 nas classes laterais generalizadas de códigos em espaços de sinais hiperbólicos.

Definição 3.10. As classes laterais de D podem ser escritas como Da , onde $a \in A^I$. Para cada classe lateral o rotulamento $m : A^I \rightarrow (S/S')^I$ define subconjuntos de S^I chamados de rótulos transladados de $\mathbb{C}$ dados por

$$\mathbb{C}(S/S'; Da) = \bigcup_{c \in D} m(ca).$$

Teorema 3.11. *Se $\mathbb{C}(S/S'; D)$ é uma classe lateral generalizada de códigos, então $S^I/\mathbb{C}(S/S'; D)/(S')^I$ é uma cadeia de partições geometricamente uniformes e os rótulos transladados $\mathbb{C}(S/S'; Da)$ de $\mathbb{C}(S/S'; D)$ são geometricamente uniformes, mutuamente congruentes e têm o grupo de simetrias $U(\mathbb{C}(S/S'; D)) = V$ em comum.*

A demonstração deste teorema decorre dos três lemas demonstrados a seguir.

Lema 3.12. *Se $\mathbb{C}(S/S'; D)$ é uma classe lateral generalizada de códigos, então*

$$(S^I/(S')^I) \simeq (S/S')$$

é uma partição geometricamente uniforme e $m : A^I \rightarrow (S/S')^I$ é um rotulamento isométrico para esta partição.

Demonstração: Primeiramente vamos mostrar que $U(S^I) = U(S)^I$. De fato, temos $U(S^I) \subseteq U(S)^I$. Agora se $H \leq U(S)^I$ então $H = \prod_{k \in I} H_k$ onde $H_k \leq U(S) \forall k \in I$, e se $U(S^I) = H \subsetneq U(S)^I$ temos que $H_k \subsetneq U(S)$ para qualquer $k \in I$, mas então $S = Hs_0$ contrariando a minimalidade de $U(S)$. Portanto $U(S^I) = U(S)^I$. Temos ainda que $U(S')^I \trianglelefteq U(S)^I$ pois $U(S') \trianglelefteq U(S)$. Assim $m : A^I \rightarrow (S/S')^I$ é uma isometria, onde $U(S)^I/U(S')^I$ produz uma partição geometricamente uniforme $S^I/(S')^I$ com espaço rótulo $A^I \simeq U(S)^I/U(S')^I$. $\square$

Lema 3.13. *Se $D \trianglelefteq A^I$ então com a estrutura induzida, $(S') \leq \mathbb{C}(S/S'; D) \leq S^I$, temos os isomorfismos:*

$$S^I/\mathbb{C}(S/S'; D) \simeq A/D; \quad \mathbb{C}(S/S'; D)/(S')^I \simeq D/e_{A^I} \simeq D; \quad S^I/(S')^I \simeq A^I/e_{A^I} \simeq A^I,$$

que é a cadeia de partições dos grupos $S^I/\mathbb{C}(S/S'; D)/(S')^I$ e $A^I/D/e_{A^I}$ são isomorfas.

Demonstração: Consideremos o caso $|I| = 1$. Para o caso geral basta estender as

considerações a cada coordenada.

$$\begin{array}{ccc}
U(S) & \xrightarrow{f} & S \\
| & & | \\
V & \rightarrow & \mathbb{C}(S/S'; D) \\
| & & | \\
U(S') & \rightarrow & S'
\end{array}$$

- (a) Primeiramente vamos mostrar que $\mathbb{C}(S/S'; D) \leq S$. Se $\phi, \psi \in \mathbb{C}(S/S'; D)$ então existe $c_1, c_2 \in D$ tal que $\phi \in m(c_1)$ e $\psi \in m(c_2)$. Se $f : U(S) \rightarrow S$ é uma bijeção que induz a estrutura de grupo em S , então existe $v, w \in U(S)$ tal que $f(v) = \phi$ e $f(w) = \psi$. Então $vw \in u_{c_1}U(S').u_{c_2}U(S') = u_{c_1}u_{c_2}U(S') = u_{c_1c_2}U(S')$, e $f(vw) = \phi\psi \in m(c_1c_2)$. Portanto, $\phi\psi \in \mathbb{C}(S/S'; D)$. Como $vU(S') = u_{c_1}U(S')$ temos que $(vU(S'))^{-1} = (u_{c_1}U(S'))^{-1}$ ou $v^{-1}U(S') = u_{c_1}^{-1}U(S') = u_{c_1^{-1}}U(S')$. Portanto, $\phi^{-1} \in m(c_1^{-1}) \in \mathbb{C}(S/S'; D)$ e $\mathbb{C}(S/S'; D) \leq S$.
- (b) Agora mostraremos que $S' \leq \mathbb{C}(S/S'; D)$. Como $\mathbb{C}(S/S'; D) = \bigcup_{c \in D} m(c)$, definimos $V = f^{-1}(\mathbb{C}(S/S'; D))$. Isto implica que $V \leq U(S)$ e

$$\begin{aligned}
V &= f^{-1}(\mathbb{C}(S/S'; D)) \\
&= f^{-1}\left(\bigcup_{c \in D} m(c)\right) \\
&= \bigcup_{c \in D} f^{-1}(m(c)) = \bigcup_{c \in D} u_c U(S').
\end{aligned}$$

Em particular, $m(1) = U(S') \subseteq V$, segue que $S' \subseteq \mathbb{C}(S/S'; D)$ ou $S' \leq \mathbb{C}(S/S'; D)$.

- (c) $A/D \simeq S/\mathbb{C}(S/S'; D)$. Como $V = f^{-1}(\mathbb{C}(S/S'; D))$ temos que

$$U(S)/V \simeq S/\mathbb{C}(S/S'; D).$$

Considerando

$$\begin{aligned}
\phi : A &\rightarrow U(S)/V \\
a &\mapsto u_a V
\end{aligned}$$

ϕ é bem definida e o $\text{Ker}\phi = D$. Portanto,

$$A/D \simeq U(S)/V \simeq S/\mathbb{C}(S/S'; D).$$

(d) $D \simeq \mathbb{C}(S/S'; D)/S'$. Considerando,

$$g : A \rightarrow U(S)/U(S')$$

e o isomorfismo rótulo como $g(c) = u_c U(S')$, temos

$$g(D) = V/U(S').$$

(De fato, se $u_c U(S') \in g(D)$, por definição $u_c U(S') \subseteq V$, e assim $u_c U(S') \in V/U(S')$ então $uU(S') = wU(S')$ se

$$w \in \bigcup_{c \in D} u_c U(S') \text{ ou } w = u_c u_1 \text{ para } c \in D \text{ e } u_1 \in U(S').$$

Assim $g(D) = V/U(S')$). Segue que

$$D \simeq V/U(S'). \quad (3.3)$$

Dai, temos que $V/U(S')$ é a imagem de $\mathbb{C}(S/S'; D)$ pelo isomorfismo rótulo, ou equivalentemente,

$$V = \bigcup_{u \in g(D)} uU(S') = \bigcup g(D).$$

Seja $f|V$ temos,

$$V/U(S') \simeq \mathbb{C}(S/S'; D)/S', \quad (3.4)$$

de (3.3) e (3.4) temos que $D \simeq \mathbb{C}(S/S'; D)/S'$.

Por fim $A \simeq S/S'$ decorre diretamente do isomorfismo rótulo. $\square$

Lema 3.14. *Os rótulos transladados de $\mathbb{C}(S/S'; D)$ são as classes laterais à direita de $\mathbb{C}(S/S'; D)$ em S^I sobre a estrutura de grupo induzida.*

Demonstração: Consideremos o caso $|I| = 1$. Para o caso geral basta estender as considerações a cada coordenada. Seja

$$\begin{aligned}
f^{-1}(\mathbb{C}(S/S'; Da)) &= f^{-1}\left(\bigcup_{c \in D} m(c.a)\right) = \bigcup_{c \in D} f^{-1}(m(c.a)) = \bigcup_{c \in D} u_{c.a}U(S') \\
&= \bigcup_{c \in D} u_c u_a U(S') = \left[\bigcup_{c \in D} u_c U(S')\right] u_a = \left[\bigcup_{c \in D} f^{-1}m(c)\right] f^{-1}(f(u_a)) \\
&= \left[f^{-1}\left(\bigcup_{c \in D} m(c)\right)\right] f^{-1}(f(u_a)) = f^{-1}\left[\left[\bigcup_{c \in D} m(c)\right] f(u_a)\right] \\
&= f^{-1}[\mathbb{C}(S/S'; D.a)] f(u_a)
\end{aligned}$$

Segue que $\mathbb{C}(S/S'; D.a) = \mathbb{C}(S/S'; D).f(u_a)$

□

Conclusão

O presente trabalho teve como finalidade estender ao plano hiperbólico as definições de conjuntos de sinais, partições geometricamente uniformes e classes laterais de códigos generalizadas. Além de estabelecer uma relação entre os códigos e a definição de G -linearidade. Para isso estruturamos o texto como a seguir.

No Capítulo 1 apresentamos alguns requisitos para o bom entendimento da dissertação. Descrevemos propriedades básicas de estruturas algébricas e métricas de maior importância para a teoria de comunicação. Introduzimos também a teoria de códigos corretores de erros.

Já no Capítulo 2 foram definidos conjuntos de sinais geometricamente uniformes em espaços euclidianos e verificamos algumas propriedades destes conjuntos. Exibimos a teoria das partições geometricamente uniformes e definimos rotulamentos isométricos. Em seguida, introduzimos o conceito de códigos geometricamente uniformes em espaços de sinais, concluindo este capítulo com outras noções de uniformidade.

No último capítulo, Capítulo 3, definimos G -linearidade, tesselações regulares e estendemos ao plano hiperbólico a teoria das partições geometricamente uniformes.

Referências Bibliográficas

- [1] Agustini, E., Constelações de Sinais em Espaços Hiperbólicos, Tese de Doutorado, IMECC-UNICAMP, Brasil, (2002).
- [2] Biglieri, E. and Elia, M., The Isometry Group of Geometrically Uniform Spherical Signal Sets, in IEEE International Symposium on Information Theory, agosto 1991.
- [3] Cavalcante, R.G. , Performance Analysis of Signal Constellations in Riemannian Varieties, MS Thesis, FEEC-UNICAMP, Brasil, (2002)(portuguese)
- [4] Forney, G.D. Jr., Geometrically uniform codes, IEEE Trans. Inform. Theory, vol. IT37 no. 5, pp. 1241-1260, Sep.(1991).
- [5] Hefez, A., e Villela, M. L. T., Códigos Corretores de Erros, Rio de Janeiro, IMPA, 2002.
- [6] Lima, E.L., Espaços Métricos, Rio de Janeiro, IMPA, 1977.
- [7] Lazari, H., Palazzo Jr, R., Geometrically Uniform Hyperbolic Codes, Computational e Applied Mathematics, SBMAC, vol.24 no.2pp. 173-192, 2005.
- [8] Lazari, H., Uma Contribuição à Teoria dos Códigos Geometricamente Uniformes Hiperbólicos, Tese de Doutorado, FEEC-UNICAMP, Brasil, (2000).
- [9] Rotman, J. J., The Theory of Groups, An Introduction, Boston, Allyn and Bacon, Inc. 1973.

- [10] Shannon, C. E., A Mathematical Theory of Communication, Bell Syst. Tech. J., vol.27, pp. 379-423 e 623-656, julho/outubro 1948.
- [11] Shokranian, S., Geometria Hiperbólica e Teoria do Números, Brasília, UNB, 2004.
- [12] Slepian, D. , Group codes for the gaussian channel, Bell Sys. Tech. Journal, vol. 37 (1968), p. 575-602.
- [13] Slepian, D., On Neighbor distance and symmetry in group codes, IEEE Trans. Inform. Theory, vol.IT-17, pp. 630-632, sept. 1971.
- [14] Souza, M. J., Realizações de Constelações de Sinais Hiperbólicos Densos Associadas a Sistemas Lineares Através das Funções Automorfas, Tese de Doutorado, FEEC-UNICAMP, Brasil, (2005).
- [15] Ungerboeck, G., Channel coding with multilevel/phase signals, IEEE Trans. Inform. Theory, vol. IT 28 no. 1 pp. 55-67, Jan.(1982)