UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE TELEMÁTICA

UMA CONTRIBUIÇÃO À TEORIA DOS CÓDIGOS GEOMÉTRICAMENTE UNIFORMES HIPERBÓLICOS

Henrique Lazari

Orientador: **Prof.Dr. Reginaldo Palazzo Jr.**

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação, FEEC-UNICAMP, como requisito parcial para obtenção do título de DOUTOR EM ENGENHARIA ELÉTRICA.

Fevereiro -2000

Campinas S.P.

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

L457u

Lazari, Henrique
Uma contribuição à teoria dos códigos geometricamente uniformes hiperbólicos / Henrique Lazari.--Campinas, SP: [s.n.], 2000.

Orientador: Reginaldo Palazzo Júnior.
Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Teoria da codificação. 2. Grupos algébricos linares. 3. Códigos de controle de erros (Teoria da informação). 4. Teoria dos sinais. 5. Teoria dos grupos combinatórios. I. Palazzo Júnior, Reginaldo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Agradecimentos

Ao Prof. Dr. Reginaldo Palazzo Jr., pela orientação segura e competente, e tambem pela enriquecedora convivência durante este período.

Ao prof. Dr. Nelo Allan por diversas discussões a respeito dos temas do presente trabalho.

Aos Professores Doutores: Helio Waldman, Max Costa e Marcelo Firer pela participação na banca examinadora.

Resumo

O objetivo do presente trabalho é estabelecer uma teoria de códigos e conjuntos de sinais geométricamente uniformes no plano hiperbólico, bem como obter presentações de subgrupos de grupos de isometrias de tesselações hiperbólicas.

Foi mostrado que a teoria de uniformidade geométrica no plano hiperbólico subsiste mesmo no contexto de grupos de translações não abelianos, desde que imposta a condição que os códigos de rótulos sejam subgrupos normais do alfabeto (ou de seus produtos diretos).

Foram obtidas presentações de fam'lias de subgrupos normais do grupo $[8,8]$, de isometrias da tessselação auto dual $\{8,8\}$, de modo a obter como quocientes os grupos $\mathbb{Z}_n$, D_n, o grupo diedral de grau n, e $\mathbb{Z}_m \times \mathbb{Z}_n$, com m, n inteiros positivos e maiores que 2. No caso não auto dual, foram impostas condições aritméticas para obtenção de presentação de subgrupos de $[p,3]$, que resultaram nos quocientes $\mathbb{Z}_2$, $\mathbb{Z}_3$ e uma sequência de $\mathbb{Z}_2$ e $\mathbb{Z}_3$.

Abstract

The goal of the present work is to establish the theory of geometrically uniform signal sets and codes in the hyperbolic plane, and to obtain presentations of hyperbolic tesselations isometry groups.

It was shown that the theory of geometrically uniforms signal sets partitions subsist, even in the hyperbolic context, with the condition that the label codes be normal subgroups of the (direct products of) alphabets.

Presentations of families of normal subgroups of the group $[8,8]$ (the isometries of the self-dual tesselation $\{8,8\}$), was obtained such that their quotients was the groups $\mathbb{Z}_n, D_n$, the dihedral group of degree n, and $\mathbb{Z}_m \times \mathbb{Z}_n$. In the non self-dual case, arithmetic conditions was imposed to obtain presentations of subgroups of $[p,3]$ such that the quotients $\mathbb{Z}_2, \mathbb{Z}_3$ and one sequence $\mathbb{Z}_2$ and $\mathbb{Z}_3$ was obtained.

Lista de Símbolos

$(G, *)$: grupo.

$MPSK$ ou $\mathbb{Z}_n$: o grupo cíclico de ordem n.

$\prod_{i \in I} G_i$: produto direto dos grupos G_i.

S_n : o grupo simétrico de grau n.

D_m : o grupo diedral de grau m.

$H \leq G$: H é um subgrupo do grupo G.

$H \lhd G$: H é um subgrupo normal do grupo G.

$|G|$: ordem do grupo G.

$\frac{G}{H}$: grupo quociente do grupo G pelo subgrupo H.

$[G : H]$: índice do subgrupo H de G.

$Ker(f)$: núcleo do homomorfismo de grupos $f : G \longrightarrow H$.

$\mathbb{R}^{2\times 2}$: o grupo aditivo das matrizes 2×2 sobre os números reais.

$GL(2, \mathbb{R})$: o grupo linear geral

$Sl^*(2,\mathbb{R})$: o grupo ortogonal.

$Sl(2,\mathbb{R})$: o grupo ortogonal especial

$PSL^*(2,\mathbb{R})$: o grupo ortogonal projetivo.

$PSL(2,\mathbb{R})$: o grupo ortogonal especial projetivo.

$G = K \ltimes Q$: G é um produto semi-direto de K por Q .

$G =< \{g_i\}_{i\in I}; \{R_j = 1\}_{j\in J} >$: presentação do grupo G pelos geradores $\{g_i\}_{i\in I}$ e pelas relações $\{R_j = 1\}_{j\in J}$.

$(A,+,\cdot)$: anel.

$A[X]$: anel de polinômios com coeficientes no anel A.

∂f : grau do polinômio f.

$d(x,y)$: distancia entre os pontos x e y do espaço métrico M.

d_h : distância de Hamming.

d' : distância do máximo em $\mathbb{R}^n$.

$d_{\mathbb{H}}$: distância hiperbólica.

$\|x\|$: norma do vetor x.

$\pi_1(M)$: grupo fundamental do espaço M.

$\mathbb{H}^2$: modelo do semiplano superior do plano hiperbólico.

$\mathbb{D}$: modelo do círculo unitário do plano hiperbólico.

$\mathcal{M}$: conjunto das transformações de Möbius.

$\mathcal{C}$: código em geral.

R : taxa de um código.

S : conjunto de sinais.

$Rv(s)$: região de Voronoi associada ao ponto de sinal s.

$\{p, q\}$: tesselação.

$[p, q]$: grupo de isometrias da tesselação $\{p, q\}$.

Π_g : grupo fundamental da superficie compacta orientável de genero g.

$\Gamma(S)$: grupo das isometrias do conjunto de sinais S.

$U(S)$: grupo gerador do conjunto de sinais geométricamente uniforme S.

S/S' : partição geométricamente uniforme.

$m : \mathcal{A} \longrightarrow \frac{S}{S'}$: rotulamento isométrico.

$C(\frac{S}{S'}, \mathcal{D})$: código de espaços de sinais.

Lista de Figuras

Conteúdo

Introdução

A teoria dos sistemas de comunicações digitais assumiu a forma atual a partir do trabalho fundamental de Shannon, [30], onde foi mostrado que dado um canal de comunicação digital, é possível, com uma codificação adequada, transmitir informações com probabilidade de erro arbitráriamente pequena, desde que a uma taxa menor que uma constante dependente do sistema e chamada de Capacidade do Canal. A partir disto, cresceu a pesquisa em torno de códigos mais eficientes na capacidade de detecção e de correção de erros, surgidos durantre o trânsito pelo canal, e conjuntos de sinais mais eficientes associados a estes códigos.

Os elementos dos códigos corretores de erros são sequências de símbolos pertencentes a um alfabeto (associado a um conjunto de sinais), tomado frequentemente entre os elementos de algum grupo, por exemplo, dígitos binários ou vetores. Mesmo quando os símbolos não tem uma estrutura natural, um procedimento particularmente 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). Naturalmente o processo de formação de produtos permite estruturar de modo natural as sequências ou palavras-código pertencentes aos códigos.

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

Na concepção tradicional de um sistema de comunicação digital, a informação é codificada (em geral pela adição de bits de paridade) e depois então modulada para a transmissão através do canal. Devido ao processo de codificação, a faixa necessária para a transmissão deve ser aumentada. No caso de sistemas de comunicações limitados em faixa e que tenham que dispor de um processo de codificação torna-se necessária a proposta de uma estratégia que viabilize projetar tal sistema de comunicações. A busca desta solução leva à concepção moderna de codificação combinada com modulação onde estruturas algébrica e geométrica são colocadas diretamente no conjunto de sinais utilizado para a transmissão, mais especificamente, o alfabeto do código passa a ser a representação no espaço euclidiano

ou não, de um conjunto de sinais e as palavras-código são sequências destes sinais sujeitas a algum padrão. A forma de padronização que se mostrou mais adequada é aquela em que existe uma ação transitiva de um grupo no conjunto de sinais (ou seja, na sua representação geométrica). Esta situação é descrita dizendo-se que o conjunto de sinais é Geométricamente Uniforme. Sobre estes conjuntos de sinais é então colocada uma estrutura, em geral via classes laterais, que conduz aos assim chamados Códigos Geométricamente Uniformes (de Classes Laterais ou de Espaços de Sinais), bem como as suas partições.

O conceito de conjunto de sinais geometricamente uniforme, introduzido por Forney em [09] se mostrou o mais adequado, no contexto dos espaços e conjuntos de sinais euclidianos, para unificar processos como as partições de Ungerboeck [35] e a Concatenação Generalizada [02], e em certo sentido é a forma mais geral que pode assumir um conjunto de sinais, mantendo ainda boas características do ponto de vista de codificação/decodificação.

Os objetivos principais da teoria dos códigos geométricamente uniformes são relacionados com as construções das partições geométricamente uniformes e dos códigos de espaços de sinais geométricamente uniformes, em particular, os Códigos de Classe Lateral Generalizados

A finalidade do presente trabalho é estender os conceitos de constelações, reticulados e particionamento ao plano hiperbólico, em particular o conceito central em codificação/modulação de uniformidade geométrica, e produzir presentações de grupos

relevantes neste processo.

Apesar da maior complexidade dos grupos de isometrias hiperbólicos quando comparados com os euclidianos, a teoria de partições geométricamente uniformes se estende a estes . Todavia, devemos levar em consideração que no caso euclidiano as regiões fundamentais das tesselações tem sempre um grupo de simetrias abeliano (de ordem 4), mesmo que o grupo de isometrias não seja abeliano , enquanto que no caso hiperbólico os grupos mais gerais tem que ser considerados.

As construções citadas dependem da existência e do conhecimento das partições dos grupos de isometrias envolvidos no processo. Em outras palavras: A existência de tesselações regulares do plano hiperbólico da forma $\{p, q\}$ gerando conjuntos de sinais, justifica a procura de subgrupos e quocientes dos grupos $[p, q]$, que forneçam informações sobre as estruturas dos mesmos.

O Capítulo 1 descreve e fornece as propriedades básicas das estruturas matemáticas (algébricas e métricas) com maior relevância para a teoria de comunicações. Também, conceitos adequados de distância e o processo de avaliação de distâncias entre palavras recebidas e palavras-código, fundamentais no processo de decodificação, são estabelecidos neste primeiro capítulo..

No Capítulo 2 são fornecidos os fundamentos da teoria dos códigos corretores de erros e é estabelecida uma linguagem unificada para tratar de conjuntos de sinais

euclidianos e hiperbólicos. Dentro desta unificação é abordada a relação entre uniformidade geométrica, casamento e uma definição de G-linearidade (Definição 7) e é estabelecido o fato que um conjunto de sinais S é $U(S)$-linear (Teorema 3 (iii)).

No Capítulo 3 são discutidos dois casos de tesselações regulares do plano hiperbólico da forma $\{p, q\}$: 1) O caso auto-dual, onde são obtidas presentações de grupos que tem $[8, 8]$ como extensão, respectivamente, pelos grupos $\mathbb{Z}_n$, $\mathbb{D}_n$, $\mathbb{Z}_m \times \mathbb{Z}_n$, onde m e n são números inteiros positivos; 2) O caso não auto-dual em que o grupo $[p, 3]$, é descrito, para valôres específicos de p, através de um par de extensões sucessivas por $\mathbb{Z}_2$ e por $\mathbb{Z}_3$. Estes resultados fornecem o substrato algébrico para o tratamento formal de conjuntos de sinais do Capítulo 4.

O objetivo do Capítulo 4 é estender a teoria das partições geométricamente uniformes ao plano hiperbólico, de modo a permitir que conjuntos de sinais casados com grupos, como aqueles descritos no Capítulo 3, possam ser decompostos em partições geométricamente uniformes. Obteve-se o resultado do Teorema 3 que mostra que um código de classes laterais generalizado é $U(S)$-linear. A extensão da teoria foi feita sob a hipótese geral de que os códigos de rótulos são subgrupos normais do grupo de rótulos, concluindo então com o resultado fundamental sobre cadeias de partições geométricamente uniformes hiperbólicas, ou seja , que são cadeias geométricamente uniformes (Teorema 4).

1

Grupos e Espaços Métricos

Os conjuntos de sinais e os códigos corretores de erros que os tem como alfabeto (a serem definidos formalmente no Capítulo 2) apresentam, em geral, algum tipo de estrutura capaz de permitir a determinação de suas propriedades e de tornar mais prática a sua implementação. Particularmente, as estruturas algébricas são a base de muitos dos códigos conhecidos e mais importantes. Além disso, o estabelecimento de um conceito adequado de distância e o processo de avaliação de distâncias entre palavras recebidas e palavras-código são fundamentais no processo de decodificação.

Este capítulo descreve e fornece as propriedades básicas das estruturas matemáticas (algébricas e métricas) com maior relevância para a teoria de comunicações.

1.1 Grupos

Os elementos dos códigos corretores de erros são sequências de símbolos

pertencentes a um alfabeto, tomado frequentemente entre os elementos de algum grupo, por exemplo, dígitos binários ou vetores. Mesmo quando os símbolos não tem uma estrutura natural, um procedimento particularmente 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) . Naturalmente o processo de formação de produtos permite estruturar de modo natural as sequências ou palavras-código pertencentes aos códigos. Desenvolvemos neste parágrafo os aspectos da Teoria dos Grupos envolvidos no presente trabalho. As referências básicas são [29], [14], [25] e [10].

Definição 1. Um GRUPO é um par consistindo de um conjunto não vazio G e uma operação binária $* : G \times G \rightarrow G$, onde denotamos $*(a, b)$ por $a * b$, satisfazendo as propriedades:

$G1 : a * (b * c) = (a * b) * c$, para todos a, b e c em G. (Associativa)

$G2$: Existe $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$. (Existência do elemento neutro)

$G3$: Para cada elemento $a \in G$, podemos determinar um elemento $a^* \in G$ tal que $a * a^* = a^* * a = e$. (Existência do Elemento Inverso).

Denotamos o grupo por $(G, *)$, ou mais simplesmente por G, se não houver ambiguidade. No caso de $*$ denotar uma das operações usuais $\cdot$ ou $+$, então denotamos e por 1 ou 0 e a^* por a^{-1} ou $-a$ respectivamente. Um grupo G é dito COMUTATIVO ou ABELIANO se estiver satisfeita a condição adicional:

$G4$: Para todos a e b em G, $a * b = b * a$. (Propriedade Comutativa).

Observação 1. Sempre que não for indicada a operação do grupo, será suposto que a mesma é denotada multiplicativamente.

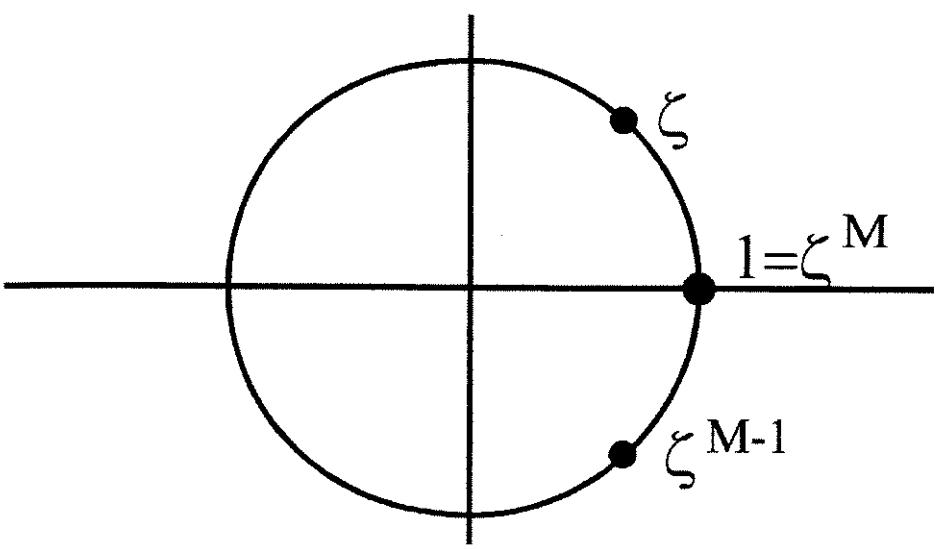

Figura 1.1 - Representação de alguns elementos do grupo $MPSK$.

Exemplo 1 O conjunto $MPSK = \left\{e^{\frac{2k\pi i}{M}} : k = 0, ..., M-1\right\} \subseteq \mathbb{C}$ com a operação usual de multiplicação de números complexos é um grupo chamado de GRUPO CÍCLICO DE ORDEM M. Se denotamos $\zeta = e^{\frac{2\pi i}{M}} = \cos\frac{2\pi}{M} + i\sin\frac{2\pi}{M}$ então temos que $MPSK = \{\zeta^n : n \in \mathbb{Z}\}$, (ver Figura 1.1) e neste caso dizemos que ζ é um gerador do $MPSK$ e denotamos também $MPSK = \langle\zeta\rangle$. $MPSK$ como todo grupo que tem um número finito de elementos é

chamado de GRUPO FINITO. No caso de um grupo G ser finito, chamamos de ORDEM DE G ao número de elementos do conjunto G, denotamos a ordem de G por $|G|$.

Exemplo 2 Nem todo grupo é finito, por exemplo $(\mathbb{Z},+), (\mathbb{Q},+), (\mathbb{R},+), (\mathbb{C},+)$, são todos grupos INFINITOS, ou seja tem um número infinito de elementos.

Exemplo 3 O GRUPO DE KLEIN é um grupo finito com quatro elementos formado pelo conjunto $K = \{e, a, b, c\}$ e pela operação definida pela tabela:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Seja $\{(G_i, *_i); i \in I\}$ uma familia de grupos e $G = \prod_{i \in I} G_i$ o produto cartesiano dos conjuntos G_i. Se $g = \{g_i\}_{i \in I}$ e $h = \{h_i\}_{i \in I}$ são dois elementos de G, definindo o produto $g * h = \{g_i *_i h_i\}_{i \in I}$ obtemos que $(G, *)$ é um grupo chamado PRODUTO DIRETO DA FAMÍLIA $\{G_i\}$. No caso dos grupos serem denotados aditivamente $(G_i, +)$, então o objeto definido neste exemplo é chamado de SOMA DIRETA e denotado $\bigoplus G_i$.

Exemplo 4 Seja $M > 1$ um número inteiro, então o conjunto $\mathbb{Z}_M = \{0, 1, ..., M-1\}$ com a operação de soma modulo M (ou seja $x \oplus y$ é o resto da divisão da soma usual $x + y$

por M) é um grupo, chamado GRUPO DOS INTEIROS MÓDULO M .Em geral se denota a operação deste grupo por $+$ e $\mathbb{Z}_M$ é tambem chamado de grupo cíclico de ordem M como o grupo $MPSK$.

Exemplo 5 Seja X um conjunto finito com $n \geq 1$ elementos, digamos $X = \{x_1, ..., x_n\}$, então denotando por S_X ou S_n o conjunto que consiste de todas as aplicações bijetivas $\sigma : X \to X$ munido da operação de composição de funções, resulta que S_n é um grupo. Chamamos o grupo $(S_n, \circ)$ de GRUPO SIMÉTRICO DE GRAU n. Temos que $|S_n| = n!$

Exemplo 6 Consideremos um polígono regular de M lados assentado no circulo $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ e com um dos vértices no ponto $1 = 1 + 0i$, vamos denotar por D_M o conjunto de todas as simetrias deste polígono, então com a operação de composição de funções, D_M é um grupo. Os seus elementos são:

$R_k = \begin{bmatrix} \cos\frac{2k\pi}{M} & -\sin\frac{2k\pi}{M} \\ \sin\frac{2k\pi}{M} & \cos\frac{2k\pi}{M} \end{bmatrix}$, $k = 0, ..., M-1$ e $S \circ R_k$ onde $S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, notando que $R_k = R^k$ onde $R = \begin{bmatrix} \cos\frac{2\pi}{M} & -\sin\frac{2\pi}{M} \\ \sin\frac{2\pi}{M} & \cos\frac{2\pi}{M} \end{bmatrix}$ e aplicar R^k nos vértices do polígono equivale a multiplicar estes vértices por $e^{\frac{2k\pi i}{M}}$, temos que

$$D_M = \left\{id, R, ..., R^{M-1}, S, S \circ R, ..., S \circ R^{M-1}\right\}$$

Este grupo pode ser também descrito como

$$D_M = \left\langle R, S : R^M = S^2 = id \ ; \ R \circ S = S \circ R^{M-1} \right\rangle.$$

Como $R \neq R^{-1} = R^{M-1}$ se $M > 2$, temos que este grupo não é abeliano. D_M é chamado de GRUPO DIEDRAL DE GRAU M. A Figura 1.2 ilustra o caso $M = 6$.

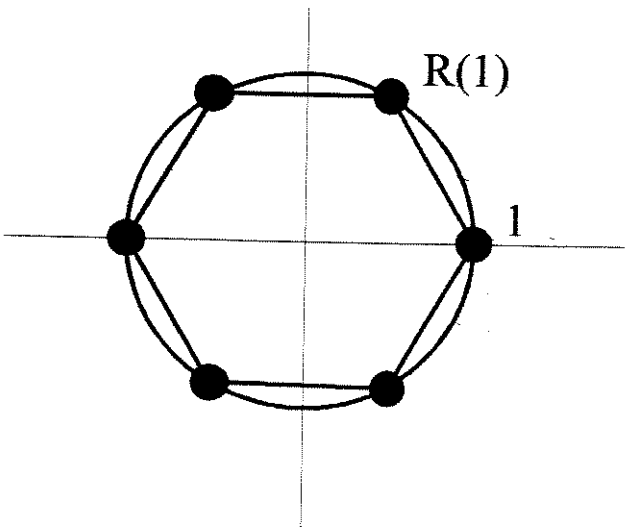

Figura 1.2 - Representação da ação dos elementos do grupo D_6.

Definição 2. Sejam G um grupo e H um subconjunto de G tal que com a restrição da operação de G, H é ele mesmo um grupo, então dizemos que H é um SUBGRUPO de G. Denotamos o fato de H ser um subgrupo de G por $H \leq G$.

Exemplo 7 Seja g um elemento qualquer de um grupo G, então o conjunto $< g >= \{g^n : n \in \mathbb{Z}\}$ é um subgrupo de G, chamado de SUBGRUPO CÍCLICO gerado por g. Se $< g >$ tem ordem finita, então dizemos que g tem ORDEM FINITA e chamamos de ORDEM de g ao número $|g| = |< g >|$. Caso contrário, dizemos que g tem ORDEM INFINITA.

Exemplo 8 $H = \{id, R, R^2, ..., R^{M-1}\}$ é um subgrupo de D_M, e $|R| = M$.

Sejam G um grupo e H um subgrupo de G, então dado $a \in G$ os conjuntos $a * H = \{a * b : b \in H\}$ e $H * a = \{b * a : b \in H\}$ são chamados respectivamente de CLASSE LATERAL À ESQUERDA MODULO H E CLASSE LATERAL À DIREITA MODULO H. Se o número de classes laterais à esquerda ou à direita for finito, são iguais, e então, este valor comum é chamado de ÍNDICE de H em G e denotado por $[G : H]$. No caso em que valer $a * H = H * a$ para todo $a \in G$, dizemos que H é um SUBGRUPO NORMAL de G e denotamos $H \lhd G$. Neste caso, o conjunto $G/H = \{a * H : a \in G\}$ munido da operação $(a * H) * (b * H) := (a * b) * H$ é um grupo denominado GRUPO QUOCIENTE de G pelo subgrupo normal H. É imediato que $|G/H| = [G : H]$.

Dados os grupos G e H , isto é, $(G, *)$ e $(H, \circ)$, dizemos que uma aplicação $f : G \to H$ é um HOMOMORFISMO se valer a seguinte condição: Para todos $g_1, g_2 \in G$, $f(g_1 * g_2) = f(g_1) \circ f(g_2)$. Notemos que a operação no lado esquerdo da igualdade é a operação de G e a operação do lado direito é a de H. Um homomorfismo bijetor é chamado de ISOMORFISMO. Se existir um isomorfismo $f : G \to H$ dizemos que G e H são ISOMORFOS e denotamos $G \simeq H$. A relação $\simeq$ é uma relação de equivalência na classe de todos os grupos. O fato de dois grupos serem isomorfos significa que eles são indistinguiveis sob o ponto de vista da teoria dos grupos.

Exemplo 9 Consideremos o grupo $8PSK = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7\}$, então a função

$f : 8PSK \longrightarrow \mathbb{Z}_8$, $f(\zeta^n) = n$ é um isomorfismo, o que justifica o uso do mesmo nome para os grupos dos Exemplos 1 e 4 . O conjunto $H = \{1, \zeta^2, \zeta^4, \zeta^6\}$ (ou $f(H) = \{0, 2, 4, 6\}$), é um subgrupo de $8PSK$ (ou de $\mathbb{Z}_8$), e como a função $g : 4PSK = \{1, \xi, \xi^2, \xi^3\} \longrightarrow H$ dada por $g(\xi^n) = \zeta^{2n}$ é um isomorfismo, identificamos H com $4PSK$. De modo similar identificamos $\mathbb{Z}_4 = \{0, 2, 4, 6\}$. Em geral este mesmo processo nos permite fazer as identificações: $MPSK \leq NPSK$ e $\mathbb{Z}_M \leq \mathbb{Z}_N$ onde $M|N$, isto é, M é um divisor de N. Como estes grupos são abelianos todos os correspondentes subgrupos são normais . Dessa forma, podemos identificar os grupos quocientes como sendo: $\frac{NPSK}{MPSK} = \left(\frac{N}{M}\right) PSK$ ou $\frac{\mathbb{Z}_N}{\mathbb{Z}_M} = \mathbb{Z}_{\frac{N}{M}}$.

Exemplo 10 Os Grupos Clássicos de ordem 2.

Se

$$\mathbb{R}^{2\times 2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\},$$

então temos que $(\mathbb{R}^{2\times 2}, +)$ é um grupo . Por outro lado, se denotamos o conjunto das matrizes 2×2 com elementos em $\mathbb{R}$ por $GL(2, \mathbb{R})$ de modo que:

$$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{R}^{2\times 2} : ad - bc \neq 0 \right\}$$

então $(GL(2, \mathbb{R}), \cdot)$ é um grupo, só que agora para a operação de multiplicação de matrizes. Este grupo é denominado GRUPO LINEAR GERAL DAS MATRIZES 2×2 SOBRE $\mathbb{R}$. Um subgrupo de $GL(2, \mathbb{R})$ que tem importancia no presente contexto é o grupo denotado por

$SL^*(2,\mathbb{R})$, consistindo das matrizes $A \in GL(2,\mathbb{R})$ tais que $(det(A))^2 = 1$. Com isso, podemos escrever que:

$$SL^*(2,\mathbb{R}) = \{A \in GL(2,\mathbb{R}) : \det A = \pm 1\}$$

O subconjunto $SL(2,\mathbb{R})$ de $SL^*(2,\mathbb{R})$ consistindo das matrizes $A \in SL^*(2,\mathbb{R})$ tais que $detA = 1$ é um subgrupo de $SL^*(2,\mathbb{R})$ chamado de GRUPO ESPECIAL e os seus elementos são chamados de MATRIZES ESPECIAIS , formalmente definido como

$$SL(2,\mathbb{R}) = \{A \in GL(2,\mathbb{R}) : \det A = 1\}$$

Associados a estes grupos temos os quocientes:

$$PS^*L(2,\mathbb{R}) = SL^*(2,\mathbb{R})/\{\pm I\}$$

$$PSL(2,\mathbb{R}) = SL(2,\mathbb{R})/\{\pm I\}$$

Notemos que o índice de $PS^*L(2,\mathbb{R})$ em $SL^*(2,\mathbb{R})$ é

$$[SL^*(2,\mathbb{R}) : PS^*L(2,\mathbb{R})] = [SL(2,\mathbb{R}) : PSL(2,\mathbb{R})] = [SL^*(2,\mathbb{R}) : SL(2,\mathbb{R})] = 2$$

O GRUPO ORTOGONAL denotado por $O(\mathbb{R}^2)$, consistindo das matrizes $A \in GL(2,\mathbb{R})$ tais que $A \cdot A^t = I$, onde A^t denota a matriz transposta da matriz A, e portanto $\det(A) \cdot \det(A^t) = \det I = 1$ ou $(det(A))^2 = 1$, assim $O(\mathbb{R}^2) \leq SL^*(2,\mathbb{R})$. O GRUPO ORTOGONAL ESPECIAL $SO(\mathbb{R}^2) = \{A \in O(\mathbb{R}^2) : \det A = 1\}$. Os elementos destes grupos são simetrias de qualquer círculo centrado na origem e no mesmo sentido que uma

circunferência pode ser considerada um limite de polígonos regulares, os grupos $O(\mathbb{R}^2)$ e $SO(\mathbb{R}^2)$ podem ser considerados como limites de D_M e do $MPSK$ respectivamente, quando $M \to \infty$.

Se $f : G \to H$ é um homomorfismo de grupos, então a IMAGEM de f é o conjunto $\operatorname{Im} f = \{f(g) : g \in G\}$ e o NÚCLEO de f é o conjunto $Kerf = f^{-1}(e_H) = \{g \in G : f(g) = e\}$. Pode-se mostrar que $Kerf \lhd G$ ([14]) , Assim,

Teorema 1 (Teorema do Homomorfismo) Seja $f : G \to H$ um homomorfismo, então $\frac{G}{Kerf} \simeq \operatorname{Im} f$.

Definição 3. Dizemos que um grupo G AGE sobre um conjunto $A \neq \emptyset$ se existe um homomorfismo $\varphi : G \to S_A$. Denotamos $g \cdot x = g(x) = \varphi(g)(x)$. Dado o elemento $x \in A$, a ORBITA de x é o conjunto $G_x = \{\sigma(x) : \sigma \in G\}$ e o ESTABILIZADOR de x é o conjunto $E_x = \{\sigma \in G : \sigma(x) = x\}$. Decorre imediatamente que $G_x \subseteq A$ e $E_x \leq G$.

Definição 4. Sejam K e Q grupos, então uma EXTENSÃO de K por Q é um grupo G tal que:

(i) K é um subgrupo normal de G.

(ii) $\frac{G}{K}$ é isomorfo a Q.

Observação. O fato do grupo G ser uma extensão de K por Q não implica necessáriamente na existência de um subgrupo de G isomorfo a Q , como mostra o

Exemplo 11 $\frac{\mathbb{Z}}{2\mathbb{Z}}$ é isomorfo a $\mathbb{Z}_2$, mas $\mathbb{Z}$ não tem nenhum subgrupo isomorfo a $\mathbb{Z}_2$ pois o seu único subgrupo finito é $\{0\}$.

Costuma-se denotar o fato que G é uma extensão de K por Q com o diagrama:

$$\{e\} \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow \{e\}$$

chamado de SEQUÊNCIA EXATA, onde a seta $\{e\} \longrightarrow K$ indica que $K \longrightarrow G$ é um homomorfismo injetor, $Q \longrightarrow \{e\}$ indica que $G \longrightarrow Q$ é um homomorfismo sobrejetor, e finalmente $K \longrightarrow G \longrightarrow Q$ indica que a imagem do homomorfismo $K \longrightarrow G$ coincide com o núcleo do homomorfismo $G \longrightarrow Q$.

Definição 5. Sejam G um grupo e K, Q subgrupos de G tais que:

(i) $K \lhd G$

(ii) $K \cdot Q = G$

(iii) $K \cap Q = \{1\}$

Dizemos então que G é um PRODUTO SEMI-DIRETO de K por Q, denotado $K \ltimes_{\varphi} Q$ ou simplesmente $K \ltimes Q$.

Se $G = K \ltimes Q$, então G é uma extensão de K por Q ([29], pg 136).

Observação. Dados os grupos K e Q podemos ter mais de um grupo sendo produto semidireto de K por Q, de fato: $S_3 = 3PSK \ltimes 2PSK$ e $6PSK = 3PSK \ltimes 2PSK$.

Se G é um produto semidireto de K por Q, então existe um homomorfismo $\theta : Q \to Aut(K)$ de modo que $\theta(x)(k) = xkx^{-1}$. Por outro lado, dados K, Q e $\theta : Q \to$

$Aut(K)$, dizemos que um produto semi-direto G de K por Q , denotado por $K \times_\theta Q$, REALIZA θ se $\theta(x)(k) = xkx^{-1}$ para todos $k \in K$ e $x \in Q$.

1.2 Presentação de Grupos, O Algoritmo de Reidemeister-Schreier

Nesta secção discutimos o Algoritmo de Reidemeister-Schreier, técnica da Teoria Combinatória dos Grupos que será usada na descrição e rotulamento de conjuntos de sinais hiperbólicos. A referência básica é [25]

Seja $(G, \cdot)$ um grupo, dizemos que a família $\{g_i\}_{i \in I}$ de elementos de G GERA G se todo elemento g de G é da forma $g = \prod_{k=1}^{n} g_{i_k}^{e_{i_k}}$ para algum $n \in \mathbb{N}$ e $e_{i_k} \in \{\pm 1\}$. Dizemos, então, que $\{g_i\}_{i \in I}$ é uma FAMÍLIA DE GERADORES de G. As expressões do tipo $U = \prod_{k=1}^{n} g_{i_k}^{e_{i_k}}$ são chamadas de PALAVRAS nos g_i 's. Dadas as palavras U e V, definimos $U^{-1} = \prod_{k=1}^{n} g_{i_k}^{-e_{i_k}}$ e $U \cdot V$ por simples justaposição. Como consequência, temos $U \cdot U^{-1} = 1$ (o elemento neutro de G). Vamos chamar de RELATOR a qualquer palavra W que represente o elemento neutro 1. Dadas duas palavras V e W dizemos que $V = W$ é uma RELAÇÃO em G se $V \cdot W^{-1}$é um relator.

Se $\{R_j\}_{j \in J}$ é uma família de relatores de G , dizemos que um relator W é DERIVÁVEL DOS R_j se W puder ser transformado na PALAVRA TRIVIAL 1 por aplicações repetidas das seguintes operações:

(i) Inserção de um dos R_j ou R_j^{-1} ou relatores da forma $g \cdot g^{-1}$ entre símbolos de W, no seu início ou no fim.

(ii) Eliminação dos relatores citados em (i) se ocorrerem como blocos de símbolos consecutivos em W.

Definição 6. Seja G um grupo gerado pela família $\{g_i\}_{i\in I}$ e $\{R_j\}_{j\in J}$ uma família de relatores tal que todo outro relator de G é derivável dos $\{R_j\}_{j\in J}$, então os $\{R_j\}_{j\in J}$ são chamados de RELATORES DEFINIDORES de G, e com isto, dizemos que a sequência $< \{g_i\}_{i\in I}; \{R_j = 1\}_{j\in J} >$ é uma PRESENTAÇÃO de G que denotamos por:

$$G =< \{g_i\}_{i\in I}; \{R_j = 1\}_{j\in J} >$$

Dizemos que G é FINITAMANTE GERADO, FINITAMENTE RELACIONADO ou TEM PRESENTAÇÃO FINITA se, respectivamente, I é finito, J é finito ou ambos são finitos.

Exemplo 12 $D_M =< R, S; R^M = S^2 = (RS)^2 = 1 >$

Exemplo 13 Um importante grupo de isometrias do plano complexo é o grupo das TRANSFORMAÇÕES DE MÖBIUS dado por:

$$PSL(2,\mathbb{Z}) = \left\{ T(z) = \frac{az+b}{cz+d} : a,b,c,d \in \mathbb{Z} \text{ e } ad-bc = 1 \right\}.$$

Se denotamos por x a função complexa dada por $\left(z \to -\frac{1}{z}\right)$ e por y a função complexa

dada por $\left(z \longrightarrow \frac{1}{-z+1}\right)$, então temos que $PSL(2,\mathbb{Z})$ tem a seguinte presentação:

$PSL(2,\mathbb{Z}) =< x, y; x^2 = y^3 = 1 >$

Definição 7. Dizemos que um grupo F com uma família de geradores $\{g_i\}_{i\in I}$ é um GRUPO LIVRE nos $\{g_i\}_{i\in I}$ se $F =< \{g_i\}_{i\in I}; \emptyset >$ ou seja, F não tem nenhum relator definidor.

Um fato importante da teoria dos grupos é que todo grupo é quociente de algum grupo livre. Este resultado é consequência do teorema mais geral:

Teorema 2 (Teorema de Presentação de Quocientes) Sejam G um grupo com a presentação

$$G =< \{g_i\}_{i\in I}; \{R_j = 1\}_{j\in J} >$$

e N o subgrupo normal de G gerado pelas palavras $\{s_k\}_{k\in K}$,então:

$$\frac{G}{N} =< \{g_i\}_{i\in I}; \{R_j = 1\}_{j\in J}, \{s_k = 1\}_{k\in K} > .$$

Sejam $G =< a_1, ..., a_n; \{R_\mu(a_1, ..., a_n) = 1\}_{\mu\in M} >$ um grupo e H um subgrupo de G. Se $W(a_\nu) \rightarrow \overline{W(a_\nu)}$ é uma função entre palavras tal que:

(i) $\left\{\overline{W(a_\nu)}\right\}$ é um conjunto completo de representantes das classes laterais à direita de G modulo H e:

(ii) Se $K = \prod_{j=1}^{n} a_j^{e_j}$ é um representante em $\left\{\overline{W(a_\nu)}\right\}$, então para cada $m < n$, $\prod_{j=1}^{m} a_j^{e_j}$ é também um representante em $\left\{\overline{W(a_\nu)}\right\}$.

Nestas condições mostra-se que H é gerado pelos elementos da forma $s_{K,a_\nu} = Ka_\nu\overline{Ka_\nu}^{-1}$

onde K é um representante arbitrário em $\left\{\overline{W(a_\nu)}\right\}$.Agora, denotando $\tau\left(a_{\nu_1}^{e_1},...a_{\nu_r}^{e_r}\right) = s_{K_1,a_{\nu_1}}^{e_1}\cdot...\cdot s_{K_r,a_{\nu_r}}^{e_r}$ temos o seguinte resultado:

Teorema 3 (Schreier) Com as notações acima,

$$H =< \{s_{K,a_\nu}\}; \{s_{M,a_\lambda} = 1\}, \left\{\tau\left(KR_\mu K^{-1}\right) = 1\right\} >,$$

onde os pares M, a_λ são tais que Ma_λ e $\overline{Ma_\lambda}$ determinam o mesmo elemento no grupo livre gerado pelos $\{a_1, ..., a_n\}$ (denotamos este fato por $Ma_\lambda \approx \overline{Ma_\lambda}$).

O próximo teorema, [25] Theorem 4.12 pg 266, fornece uma caracterização de uma classe de grupos cujo único elemento de ordem finita é a identidade.

Teorema 4 Seja $G =< a_1, ..., a_n; R(a_1, ..., a_n) = 1 >$, então G tem um elemento $(\neq 1)$ de ordem finita, se $R(a_1, ..., a_n)$ é a $k-$ésima potência de alguma palavra no grupo livre nos $\{a_1, ..., a_n\}$

O Grafo de Cayley de um Grupo

Seja G um grupo gerado por $\{g_i\}_{i\in I}$, podemos construir uma nova estrutura do seguinte modo: Um conjunto de VÉRTICES rotulado pelos elementos de G, um conjunto de ARESTAS rotulado por pares ordenados de elementos de G (ou vértices), onde (x, y) é uma aresta se, e somente se, existir um gerador g_i de modo que $y = g_i x$. Tal estrutura é denominada de GRAFO DE CAYLEY DO GRUPO G .

Exemplo 14 O grupo de Klein tem a seguinte presentação

$$K =< a, b : a^2 = b^2 = (ab)^2 = e >$$

e o grafo de Cayley de K tem a seguinte forma:

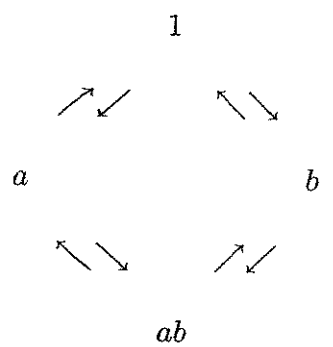

Figura 1.3 - O Grafo de Cayley do Grupo de Klein.

1.3 Outras Estruturas Algébricas

Frequentemente códigos são definidos usando símbolos pertencentes a espaços vetoriais (sobre corpos finitos ou não) além de modelos euclidianos de espaços não euclidianos. Por outro lado, importantes classes de códigos (por exemplo os códigos cíclicos) são definidos algébricamente a partir de anéis de polinômios. As referências para esta secção são [10] e [14]

Um conjunto não vazio A é dito um ANEL se A estiver munido de duas operações binárias denotadas $+$ e $\cdot$ de modo que $(A,+)$ é um grupo abeliano e também valem as propriedades:

$M1 : a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todos a, b e c em A. (Associativa)

$M2$: Existe $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in A$. (Existência do elemento neutro)

$D : a \cdot (b+c) = a \cdot b + a \cdot c$ e $(a+b) \cdot c = a \cdot c + b \cdot a$, para todos a, b e c em A (Propriedade Distributiva).

Se além destas, valer:

$M4$: Para todos a e b em A, $a \cdot b = b \cdot a$. (Propriedade Comutativa)

então dizemos que o anel A é COMUTATIVO.

Um anel A é dito um DOMÍNIO DE INTEGRIDADE se for comutativo e se para todos $a, b \in A$, $a \cdot b = 0$ implica $a = 0$ ou $b = 0$. Um CORPO é um anel comutativo K tal que dado $a \in K$, se $a \neq 0$, então existe o elemento $a^{-1} \in K$ tal que $a \cdot a^{-1} = 1$. Dado um anel A, um subgrupo J de (A,+) é um IDEAL (bilateral) de A se para todos $a \in A$ e $x \in J$, temos que $a \cdot x \in J$ e $x \cdot a \in J$. Definindo no grupo quociente A/J a operação $(a + J) \cdot (b + J) = a \cdot b + J$ obtemos uma estrutura natural de anel em A/J chamada de ANEL QUOCIENTE.

Dado um corpo K, um grupo abeliano V é um ESPAÇO VETORIAL sobre K

se estiver definida uma função $\phi : K \times V \to V$ onde denotamos $\phi(x, v) = xv$ satisfazendo as propriedades: (1) $1 \cdot v = v$ para todo $v \in V$. (2) $(x+y)v = xv + yv$ para todos $x, y \in K$ e $v \in V$. (3) $x(v+w) = xv + xw$ para todos $x \in K$ e $v, w \in V$. (4) $x(yv) = (xy)v$ para todos $x, y \in K$ e $v \in V$. Os elementos de V são chamados de VETORES. Os fatos básicos sobre espaços vetoriais podem ser encontrados em [14].

Exemplo 15 $(\mathbb{Z}_n, +, \cdot), (\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ são exemplos de anéis sendo que todos com exceção do primeiro são domínios de integridade e os três últimos são corpos. Se p é um número primo, então $\mathbb{Z}_p$ é um corpo e quando queremos destacar esta estrutura denotamo-la por $\mathbb{F}_p$. Para cada inteiro $n > 1$ existe um corpo $\mathbb{F}_{p^n} (\neq \mathbb{Z}_{p^n})$ com p^n elementos que tem $\mathbb{F}_p$ como subcorpo (subanel com os mesmos elementos 0 e 1) e é um espaço vetorial de dimensão finita n sobre $\mathbb{F}_p$. Denotamos este fato por $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Exemplo 16 Se A é um domínio de integridade podemos construir o ANEL DE POLINÔMIOS COM COEFICIENTES EM A, $A[X]$, que consiste de todas as sequências do tipo $f = \sum_{i=1}^{n} a_i X^i$ onde os $a_i \in A$ e X é um símbolo fixado , o GRAU de f é o número $\partial f = n$, o maior índice i tal que $a_i \neq 0$ .Os conceitos usuais de divisibilidade valem em $A[X]$. Dados $f, g \in A[X]$, se existe $h \in A[X]$ tal que $f = gh$ então dizemos que g DIVIDE f e denotamos por $g|f$. O máximo divisor comum (mdc) de dois ou mais polinômios é definido de modo usual ($d = mdc\{f, g\}$ se, $d|f, d|g$ e se $e|f, e|g$ então $d|e$). Dizemos que um polinômio $f \in A[X]$ é IRREDUTÍVEL se sempre que pudermos escrever $f = gh$

em $A[X]$, devemos ter $\partial g = 0$ ou $\partial h = 0$. Dado um polinômio $f \in A[X]$, o conjunto $< f >= \{f \cdot g : g \in A[X]\}$ é um ideal de $A[X]$ e todo ideal de $\mathbb{K}[X]$ é desta forma. Se $\mathbb{K}$ é um corpo, o ideal $< f >$ é chamado de IDEAL PRINCIPAL gerado por f, e existe um único polinômio mônico (i.e. com o maior coeficiente não nulo igual a 1) g tal que $< f >=< g >$, g é chamado de GERADOR MÔNICO do ideal. Se f é irredutível então $\frac{A[X]}{< f >}$ é um corpo.

Exemplo 17 Se $\mathbb{K}$ é um corpo , então

$$\mathbb{K}^{n\times n} = \left\{ A = \begin{bmatrix} a_{11} & \cdots\cdots & a_{1n} \\ . & \cdots\cdots & . \\ a_{n1} & \cdots\cdots & a_{nn} \end{bmatrix} : a_{ij} \in \mathbb{K} \right\},$$

o conjunto de todas as matrizes $n \times n$ sobre $\mathbb{K}$, com as operações usuais de soma, multiplicação de matrizes multiplicação de número por matriz, tem uma estrutura dupla de anel e de espaço vetorial, e por isto, dizemos que $\mathbb{K}^{n\times n}$ é uma ÁLGEBRA sobre $\mathbb{K}$. Se A é um elemento de $\mathbb{K}^{n\times n}$, então o TRAÇO de A é: $tr(A) = \sum_{i=1}^{n} a_{ii}$.

1.4 Espaços Métricos

Nesta seção, inicialmente é apresentada a definição de espaço métrico que constitui a formalização do conceito usual de distância , e são apresentados modelos de distâncias em espaços relevantes para a Teoria de Comunicações. É apresentada a definição

de Isometria e fornecida uma definição de Superficie adequada ao tratamento de Conjuntos de Sinais. Para Espaços Métricos, nos referimos a [18] e [19]

Definição 8. Um conjunto M é dito um ESPAÇO MÉTRICO se existe uma função $d : M \times M \longrightarrow \mathbb{R}$, chamada métrica ou distância satisfazendo para todos $x, y, z \in M$:

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

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

(iii)$d(x, z) \leq d(x, y) + d(y, z)$

Em geral denotamos o espaço métrico por (M, d) ou simplesmente M se não acarretar ambiguidade.

Em um espaço métrico (M, d) chamamos um subconjunto $A \subseteq M$ de ABERTO, se existe $\epsilon > 0$ tal que o conjunto $B(x, \epsilon) = \{y \in M : d(x, y) < \epsilon\} \subseteq A$. O conjunto $B(x, \epsilon)$ é chamado de BOLA ABERTA DE CENTRO x E RAIO ϵ. Uma aplicação $f : M \longrightarrow N$ entre espaços métricos é chamada de CONTÍNUA se, para cada $a \in M$ e cada bola aberta $B(f(a), \epsilon) \subseteq N$, existe uma bola aberta $B(a, \delta) \subseteq M$ tal que $f(B(a, \delta)) \subseteq B(f(a), \epsilon)$. Dado um subconjunto A de um espaço métrico M, dizemos que $x \in A$ é um PONTO INTERIOR de A se existe $\epsilon > 0$ tal que $B(x, \epsilon) \subseteq A$. O conjunto de todos os pontos interiores de A é denominado de INTERIOR de A e denotado por $\mathring{A}$. Como consequência temos que um conjunto A é aberto se todo ponto de A é ponto interior. Um ponto x é dito FRONTEIRA de A se para todo $\epsilon > 0, B(x, \epsilon) \cap A \neq \emptyset$ e $B(x, \epsilon) \cap (M \backslash A) \neq \emptyset$. O conjunto dos elementos

da fronteira de A é denotado por frA. O conjunto $\mathfrak{T}_M$ cujos elementos são os conjuntos abertos do espaço métrico M satisfaz as seguintes propriedades:

(i) $M, \emptyset \in \mathfrak{T}_M$

(ii) Se $\{B_i\}_{i \in I}$ é uma familia de elementos de $\mathfrak{T}_M$, então $\bigcup_{i \in I} B_i \in \mathfrak{T}_M$.

(iii)Se $B_1, ..., B_n$ são elementos de $\mathfrak{T}_M$, então $B_1 \cap ... \cap B_n \in \mathfrak{T}_M$

Em geral, um conjunto $\mathfrak{T}$ com as propriedades (i), (ii), (iii) acima é chamado de uma TOPOLOGIA em M.

Exemplo 18 No espaço vetorial $\mathbb{R}^n$ definimos a NORMA de um vetor $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{R}^n$ como o número real positivo $\|x\| = \sqrt{x_1^2 + ... + x_n^2}$. Definimos $d(x, y) = \|x - y\| = \sqrt{(x_1 - y_1)^2 + ... + (x_n - y_n)^2}$ para $x = (x_1, ..., x_n)$ e $\mathbf{y} = (y_1, ..., y_n)$ em $\mathbb{R}^n$. Temos então que $(\mathbb{R}^n, d)$ é um espaço métrico. A distância d é chamada de MÉTRICA EUCLIDIANA OU USUAL. De modo similar, definimos para $z = a + bi \in \mathbb{C}$; $\|z\| = a^2 + b^2$ e $d(z, w) = \|z - w\|$ é uma norma em $\mathbb{C}$. A função $d' : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ definida por $d'(x, y) = \sum_{i=1}^{n} |x_i - y_i|$ é chamada de DISTÂNCIA DO MÁXIMO em $\mathbb{R}^n$

Exemplo 19 Seja A um conjunto finito, então existe uma métrica em A chamada de MÉTRICA DISCRETA definida por

$$d(x, y) = \begin{cases} 0 \text{ se } x = y \\ 1 \text{ se } x \neq y \end{cases}$$

que se estende de modo natural a A^n por $d_h(x,y) = \sum_{i=1}^{n} d(x_i, y_i)$. d_h é chamada de MÉTRICA DE HAMMING em A^n. Na prática $d_h(x,y)$ mede o número de coordenadas em que x e y diferem. Se $n = 1$ a métrica de Hamming é a métrica discreta. Se A é o corpo finito $\mathbb{F}_q$ e $x \in \mathbb{F}_q^n$, a NORMA ou PESO DE HAMMING de x é o número inteiro $w_h(x) = d_h(x, 0)$ que é o número de coordenadas não nulas de x. Ainda em $\mathbb{F}_q^n$ definimos o PESO DE LEE de $x = (x_1, ..., x_n)$ como $w_L(x) = \sum_{i=1}^{n} |x_i|$ onde

$$|x_i| = \begin{cases} x_i \text{ se } 0 \leq x_i \leq q/2 \\ q - x_i \text{ se } q/2 < x_i \leq q-1 \end{cases}$$

e a DISTANCIA DE LEE entre $x, y \in \mathbb{F}_q^n$ é $d_L(x,y) = w_L(x-y)$.

Definição 9. Se M e N são espaços métricos com distâncias d_M e d_N respectivamente, então dizemos que uma aplicação $f : M \to N$ é uma ISOMETRIA se f é uma bijeção contínua e para todos $x, y \in M$, $d_N(f(x), f(y)) = d_M(x,y)$.

Observação. Se M é um espaço métrico e $f, g : M \to M$ são isometrias de M, então f^{-1} e $g \circ f$ também são isometrias de M e, portanto, o conjunto $Isom(M)$ de todas as isometrias de M é um grupo para a composição de funções, chamado o GRUPO DAS ISOMETRIAS de M.

Exemplo 20 Seja G um grupo onde está definida uma função d que é uma métrica. Dizemos que d é compatível com a estrutura de G ou é uma MÉTRICA DE GRUPO se para todos $x, y \in G$, $d(x,y) = d(x \cdot y^{-1}, 1)$, ou em notação aditiva $d(x,y) = d(x-y, 0)$.

Denotando por I o intervalo fechado unitário $[0,1]$, um CAMINHO em um espaço métrico M é uma função contínua $\alpha : I \to M$. Dizemos que dois caminhos $\alpha, \beta : I \to M$ são HOMOTÓPICOS, denotado por $\alpha \simeq \beta$, se existe uma função contínua $H : I \times I \to M$ tal que $H(s,0) = \alpha(s)$; $H(s,1) = \beta(s)$; $H(0,t) = \alpha(0) = \beta(0)$; $H(1,t) = \alpha(1) = \beta(1)$ para todos $s,t \in I$. Denotamos o fato de α ser homotópico a β por $\alpha \simeq \beta$. Dados dois caminhos α e β tais que $\alpha(1) = \beta(0)$, definimos $\alpha \cdot \beta(s) = \begin{cases} \alpha(2s) \text{ se } s \in [0, \frac{1}{2}] \\ \beta(2s-1) \text{ se } s \in [\frac{1}{2}, 1] \end{cases}$ temos então que a relação $\alpha \simeq \beta$ é uma relação de equivalência na coleção de todos os caminhos em M. Agora, denotando por $[\alpha]$ a classe de equivalência de α, temos então que fica bem definida uma operação no conjunto quociente por $[\alpha] \cdot [\beta] = [\alpha \cdot \beta]$. Considere agora um ponto $x \in M$ fixado, então um CAMINHO EM M COM BASE NO PONTO x é um caminho $\alpha : I \to M$ tal que $\alpha(0) = \alpha(1) = x$. O conjunto $\pi_1(M,x)$ constituído pelas classes de homotopia de caminhos fechados em M com base no ponto x constitui um grupo para a operação definida acima. Se M é um espaço conexo por caminhos (ou seja , dados dois pontos x e y quaisquer de M existe um caminho $\alpha : I \to M$ tal que $\alpha(0) = x$ e $\alpha(1) = y$) , então para todos $x, y \in M$, $\pi_1(M,x)$ e $\pi_1(M,y)$ são isomorfos, e neste caso, $\pi_1(M,x)$ é chamado de GRUPO FUNDAMENTAL DE M COM BASE EM x, e denotado por $\pi_1(M)$.

Chamamos de SUPERFÍCIE a um espaço métrico M tal que para todo ponto $x \in M$ existem conjuntos abertos A de M , B de $\mathbb{R}^2$ e uma bijeção $f : A \to B$ tal que f e f^{-1} são contínuas.

Uma SUPERFÍCIE COMPACTA ORIENTÁVEL de gênero $g \geq 1$ é uma superfície construída do seguinte modo: Considere um polígono regular de $4g$ lados rotulados sequencialmente do seguinte modo:

$$a_1, b_1, a_1^{-1}, b_1^{-1}, \cdots a_g, b_g, a_g^{-1}, b_g^{-1}$$

onde em cada 4-upla $a_i, b_i, a_i^{-1}, b_i^{-1}$ os lados são orientados de acordo com o seguinte esquema:

$$\xrightarrow{a_i} \quad \xrightarrow{b_i} \quad \xleftarrow{a_i} \quad \xleftarrow{b_i} .$$

Considerando, agora, a relação de equivalência que identifica os lados $\xrightarrow{x}$ e $\xleftarrow{x}$ coerentemente com as setas e mantem os outros pontos fixos (ou seja, "colamos " os lados de acordo com a orientação) , obtemos então a superfície. No diagrama abaixo ilustramos o caso $g = 2$:

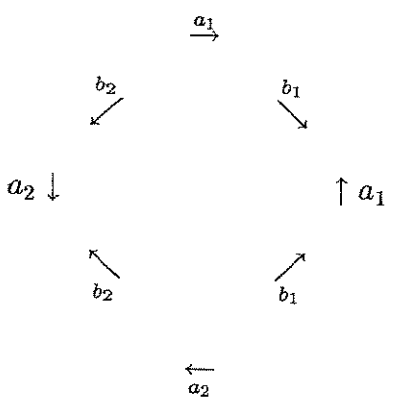

Figura 1.4 - Identificação para $g = 2$.

O aspecto da superficie é mostrado na Figura 1.5

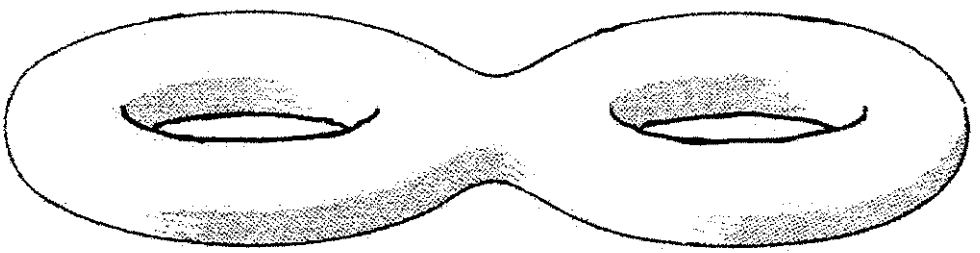

Figura 1.5 - Aspecto da superfície para $g = 2$.

1.5 O Plano Hiperbólico

Apresentamos agora as duas versões do Plano Hiperbólico de Poincaré, e os fatos básicos a respeito de grupos discretos e geometria hiperbólica que tem como referências [01], [16], [08], [24]e [15] .

Seja $\mathbb{H}^2 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ o semiplano superior do plano complexo $\mathbb{C}$. Definimos para $z, w \in \mathbb{H}^2$; $d_{\mathbb{H}}(z,w) = \log \dfrac{|z-\overline{w}| + |z-w|}{|z-\overline{w}| - |z-w|}$. Com esta função, o par $(\mathbb{H}^2, d_{\mathbb{H}})$ constitui um espaço métrico, chamado de PLANO HIPERBÓLICO . Chamamos de retas hiperbólicas aos semi-círculos e semi-retas ortogonais ao eixo real e contidos em $\mathbb{H}^2$. O plano hiperbólico satisfaz os axiomas básicos da geometria euclidiana com a exceção do 5^o Axioma ou Axioma das Paralelas. Assim, podemos ter por um ponto A fora de uma determinada reta mais de uma reta passando por A não encontrando a reta dada. (Mais de

uma paralela). Dizemos então que $\mathbb{H}^2$ é um modelo da Geometria Hiperbólica Plana ou de Lobachevski. (Figura 1.6)

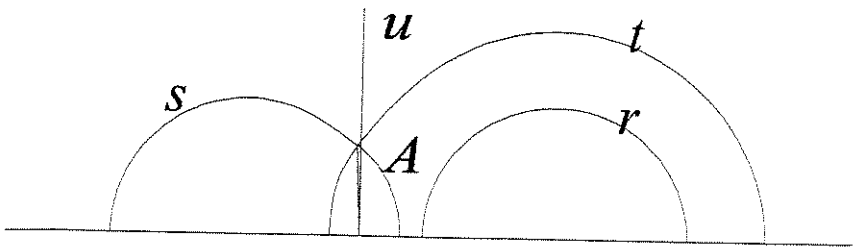

Figura 1.6 - Modelo do Semiplano Superior

Um outro modelo da Geometria Hiperbolica Plana é obtido tomando o conjunto $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ (Figura 1.7) com a métrica $d_{\mathbb{D}}(x,y) = \log \dfrac{|1 - z\overline{w}| + |z - w|}{|1 - z\overline{w}| - |z - w|}$ $z, w \in \mathbb{D}$. As retas hiperbólicas, agora, são as intersecções de $\mathbb{D}$ com as circunferências ortogonais a $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. De fato a função

$$f : \mathbb{H}^2 \to \mathbb{D}$$
$$f(z) = \frac{z + i}{z - i}$$

é uma isometria entre $(\mathbb{H}^2, d_{\mathbb{H}})$ e $(\mathbb{D}, d_{\mathbb{D}})$ e sempre que não houver ambiguidade, qualquer

das métricas $d_{\mathbb{D}}$ ou $d_{\mathbb{H}}$ será denotada simplesmente por d.

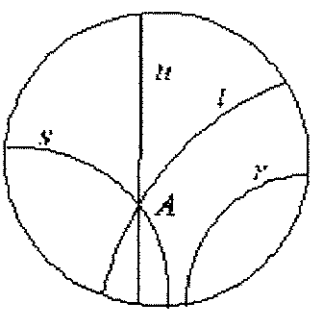

Figura 1.7 - Modelo do Círculo Unitário

Definição 10. O ÂNGULO HIPERBÓLICO entre duas retas hiperbólicas que se encontram no ponto $z \in \mathbb{H}^2$, é o ângulo entre os seus vetores tangentes (no sentido da Geometria Euclidiana) no ponto z.

Exemplo 21 Na Figura 1.8 , Δ é um triângulo com ângulos internos respectivamente de $0, \frac{\pi}{2}$ e $\frac{\pi}{3}$.

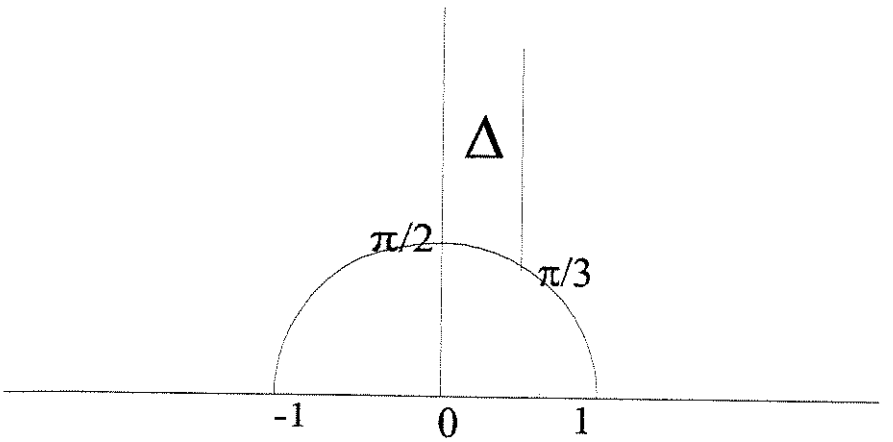

Figura 1.8 - O triângulo hiperbólico Δ

No plano hiperbólico, qualquer triângulo com ângulos internos α, b e γ satisfaz

$$\alpha + \beta + \gamma < \pi.$$

O próximo teorema permite, através da decomposição em triângulos, determinar a área (hiperbólica) de qualquer polígono em $\mathbb{H}^2$:

Teorema 5 (Gauss-Bonnet) Se um triângulo hiperbólico Δ têm ângulos internos α, β e γ respectivamente, então:

$$\acute{a}rea(\Delta) = \pi - (\alpha + \beta + \gamma)$$

Exemplo 22 O triângulo do Exemplo 21 tem área $\pi - (0 + \frac{\pi}{2} + \frac{\pi}{3}) = \frac{\pi}{6}$

1.6 Isometrias do Plano Hiperbólico e Grupos Contínuos

A uniformidade geométrica de um conjunto de sinais é uma propriedade associada ao seu grupo de isometrias, assim, a extensão deste conceito ao plano hiperbolico exige o conhecimento das isometrias hiperbólicas, bem como as suas propriedades geométricas, assunto da presente seção.

Vamos denotar por $\mathcal{M}$ o conjunto de todas as transformações de Möbius, ou seja, transformações lineares fracionárias complexas da forma:

$$T(z) = \frac{az+b}{cz+d},$$

onde $a, b, c, d \in \mathbb{R}$, e $ad - bc \neq 0$. Se denotamos $\Delta = ad - bc$, então

$$T(z) = \frac{\left(\frac{a}{\sqrt{\Delta}}\right) z + \frac{b}{\sqrt{\Delta}}}{\left(\frac{c}{\sqrt{\Delta}}\right) z + \frac{d}{\sqrt{\Delta}}} \text{ e } \frac{a}{\sqrt{\Delta}}\frac{d}{\sqrt{\Delta}} - \frac{b}{\sqrt{\Delta}}\frac{c}{\sqrt{\Delta}} = 1$$

e com isso podemos supor que $ad-bc = 1$. Nestas condições $\mathcal{M}$ é um grupo para a operação de composição de funções. Com isso, temos as propriedades adicionais: Se $T(z) = \frac{az+b}{cz+d}$ e $U(z) = \frac{ez+f}{gz+h}$, então denotando $A_T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ e $A_U = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, segue que $A_{T\circ U} = A_T \cdot A_U$ e $A_{T^{-1}} = (A_T)^{-1}$. Por outro lado, como $T(z) = \frac{(-a)z+(-b)}{(-c)z+(-d)}$ resulta que $-A_T$

também representa T , e assim, podemos considerar

$$\Phi : SL(2,\mathbb{R}) \to \mathcal{M}$$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto T(z) = \frac{az+b}{cz+d}.$$

Segue, então, que se $\Phi(A) = T$ e $\Phi(B) = U$, então $\Phi(AB) = T \circ U$ e $\Phi(A^{-1}) = T^{-1}$ de onde concluímos que Φ é um homomorfismo sobrejetor de grupos . Além disso, como $Ker(\Phi) = \{\pm I\}$, pelo Teorema do Homomorfismo temos

$$\mathcal{M} \simeq \frac{SL(2,\mathbb{R})}{\{\pm I\}} = PSL(2,\mathbb{R}).$$

Dessa forma, podemos denotar o GRUPO PROJETIVO ESPECIAL LINEAR das matrizes 2×2 sobre $\mathbb{R}$ por

$$PSL(2,\mathbb{R}) = \left\{ T(z) = \frac{az+b}{cz+d} : a,b,c,d \in \mathbb{R}; ad-bc = 1 \right\}.$$

Dada uma matriz A qualquer, vale a assertiva de que $tr(-A) = -tr(A)$ de modo que $tr^2(A) = tr^2(-A)$. Assim, dados $T(z) = \frac{az+b}{cz+d} \in PSL(2,\mathbb{R})$ e $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, fica bem definida a função:

$$Tr : PSL(2,\mathbb{R}) \to \mathbb{R}$$

$$Tr(T) = |tr(A)| = |a+d|.$$

A funçao Tr é chamada de FUNÇÃO TRAÇO e permite uma classificação dos elementos de $PSL(2,\mathbb{R})$.

Definição 11. Seja $T(z) = \dfrac{az+b}{cz+d} \in PSL(2,\mathbb{R})$, então dizemos que T é um elemento:

elíptico se $Tr(T) < 2$

parabólico se $Tr(T) = 2$

hiperbólico se $Tr(T) > 2$

Consideremos, agora, a função complexa $U(z) = -\overline{z}$. Então, dado $T(z) = \dfrac{az+b}{cz+d} \in PSL(2,\mathbb{R})$ temos que $T \circ U(z) = T(-\overline{z}) = \dfrac{-a\overline{z}+b}{-c\overline{z}+d}$ e $-ad+bc = -1$. Assim, toda aplicação da forma $T \circ U$ é do tipo $W(z) = \dfrac{\alpha\overline{z}+\beta}{\gamma\overline{z}+\delta}$ com $\alpha\delta - \beta\gamma = -1$. Como $W \circ W = id$, vamos indicar por $\mathbb{Z}_2$ o subgrupo de $PSL(2,\mathbb{R})$ gerado por W. Estas considerações estão contidas no seguinte resultado.

Teorema 6 O grupo de todas as isometrias do plano hiperbólico $\mathbb{H}^2$ é isomorfo ao grupo $PS^*L(2,\mathbb{R})$, e consequentemente:

$$PS^*L(2,\mathbb{R}) = PSL(2,\mathbb{R}) \ltimes \mathbb{Z}_2.$$

Considere a ação natural de $PS^*L(2,\mathbb{R})$ sobre $\mathbb{H}^2$ (por isomorfismos). Como $PS^*L(2,\mathbb{R}) = PSL(2,\mathbb{R}) \cup W \circ PSL(2,\mathbb{R})$, então os elementos de $PSL(2,\mathbb{R})$ são denominados ELEMENTOS CONFORMES. Consequentemente, os elementos de $W \circ PSL(2,\mathbb{R})$ são denominados ELEMENTOS ANTI-CONFORMES. Os elementos conformes são aqueles que preservam ângulos hiperbólicos e os elementos anti-conformes são os que preservam o valor absoluto mas invertem o sentido dos ângulos hiperbólicos.

O grupo $SL(2,\mathbb{R})$ se identifica naturalmente com o subconjunto X de $\mathbb{R}^4$ dado por

$$X = \left\{(a,b,c,d) \in \mathbb{R}^4 : ad - bc = \pm 1\right\}.$$

Assim, $SL(2,\mathbb{R})$ tem uma topologia métrica $\|T-U\|$ induzida pela norma

$$\|T\| = \sqrt{a^2+b^2+c^2+d^2}.$$

Como $\sqrt{a^2+b^2+c^2+d^2} = \sqrt{(-a)^2+(-b)^2+(-c)^2+(-d)^2}$, então fica bem definida uma norma $\|T\| = \sqrt{a^2+b^2+c^2+d^2}$, e portanto uma topologia em $PSL(2,\mathbb{R})$ que torna $\|\cdot\|$ uma métrica de grupo . De modo similar, se constroi uma topologia em $PS^*L(2,\mathbb{R})$.

Definição 12. Um subgrupo Γ de $PS^*L(2,\mathbb{R})$ é DISCRETO se Γ é um subespaço topológico discreto de $PS^*L(2,\mathbb{R})$.

Observação. Γ ser discreto é equivalente à seguinte propriedade: Se $T_n \to id$ em Γ, então existe m tal que $T_n = id$ se $n > m$.

Definição 13. Um GRUPO FUCHSIANO é um subgrupo discreto de $PSL(2,\mathbb{R})$.

Observação. Se Γ é um subgrupo discreto de $PS^*L(2,\mathbb{R})$, então $\Gamma_F = \Gamma \cap PSL(2,\mathbb{R})$ é

um grupo fuchsiano e $[\Gamma : \Gamma_F] \leq 2$. O diagrama abaixo explicita esta associação.

$$\begin{array}{ccc} & PS^*L(2,\mathbb{R}) & \\ & | \quad \diagdown & \\ \Gamma & & PSL(2,\mathbb{R}) \\ & \diagdown \quad | & \\ & & \Gamma_F \end{array}$$

Teorema 7 Seja Γ um subgrupo de $PS^*L(2,\mathbb{R})$, então Γ é um grupo fuchsiano se, e somente se, a ação de Γ sobre $\mathbb{H}^2$ é PROPRIAMENTE DESCONTÍNUA (i.e. para cada $x \in \mathbb{H}^2$ existe uma vizinhança $V(x) = V$ tal que $T(V) \cap V \neq \emptyset$ somente para um número finito de $T \in \Gamma$).

Os grupos cíclicos gerados por elementos hiperbólicos e parabólicos são sempre fuchsianos. Um grupo cíclico gerado por um elemento elíptico é fuchsiano se, e somente se, é finito.

Exemplo 23 Seja $PSL(2,\mathbb{Z}) = \left\{ T(z) = \dfrac{az+b}{cz+d} : a,b,c,d \in \mathbb{Z}; ad-bc = 1 \right\}$ o GRUPO MODULAR. Este é um subgrupo discreto de $PSL(2,\mathbb{R})$, logo um grupo fuchsiano.

Definição 14. Uma região fechada $F \subseteq \mathbb{H}^2$ é uma REGIÃO FUNDAMENTAL para um grupo G de isometrias de $\mathbb{H}^2$ se:

$(i) \bigcup_{T \in G} T(F) = \mathbb{H}^2$

(ii) $\overset{\circ}{F} \cap T(\overset{\circ}{F}) = \emptyset$ para todos $T \in G \setminus \{id\}$

$(iii)\{T(F) : T \in G\}$ é a TESSELAÇÃO de $\mathbb{H}^2$

Se Γ é um grupo fuchsiano e F_1, F_2 são regiões fundamentais de Γ com $área(frF_1) = área(frF_2)$, então:

$$área(F_1) = área(F_2).$$

Sejam Γ um grupo discreto de isometrias de $\mathbb{H}^2$ e Λ um subgrupo de índice finito n em Γ com $[\Gamma/\Lambda] = \{T_1, ..., T_n\}$ ou seja:

$$\Gamma = T_1\Lambda \cup \cdots \cup T_n\Lambda$$

Se F é uma região fundamental para Γ, então:

(i)$F_1 = T_1(F) \cup \cdots \cup T_n(F)$ é uma região fundamental de Λ,

(ii) Se $área(F) < \infty$ e $área(frF) = 0$, então:

$$área(F_1) = n \cdot área(F).$$

Considerando agora Γ em grupo fuchsiano e $p \in \mathbb{H}^2$ não fixado por nenhum elemento de $\Gamma \backslash \{id\}$, então a REGIÃO DE DIRICHLET de Γ centrada em p é o conjunto:

$$D_p(\Gamma) = \left\{ z \in \mathbb{H}^2 : d(z,p) \leq d(z, T(p)) \text{ para todo } T \in \Gamma \right\}$$

A Região de Dirichlet é uma região fundamental conexa para Γ na forma de um polígono. A tesselação de $\mathbb{H}^2$ determinada por uma Região de Dirichlet F e suas imagens por Γ é chamada de TESSELAÇÃO DE DIRICHLET.

Observação. Considerando o grupo fuchsiano Γ atuando em $\mathbb{H}^2$ de modo que o espaço quociente $\mathbb{H}^2/\Gamma$ seja tal que $área(\ \mathbb{H}^2/\Gamma) < \infty$ (os elementos de $\mathbb{H}^2/\Gamma$ são as Γ-órbitas, e $área(\ \mathbb{H}^2/\Gamma) = área(\ F)$ para toda região fundamental F), então $\mathbb{H}^2/\Gamma$ é homeomorfo ao quociente F/Γ de uma região fundamental F por Γ.[16]

Dizemos que dois lados L_1 e L_2 de uma Região de Dirichlet F de um grupo fuchsiano Γ são CONGRUENTES ou EMPARELHADOS se existe $T \in \Gamma$ com $L_2 = T(L_1)$. Os lados de uma Região de Dirichlet se particionam em pares de lados congruentes, e assim:

Teorema 8 Seja Γ um grupo fuchsiano, então existe uma região fundamental convexa com um número finito de lados, se, e somente se, Γ é finitamente gerado. Se F é uma Região de Dirichlet de Γ nestas condições e $\{T_i\}_{i\in I}$ é o subconjunto de Γ consistindo dos elementos que emparelham os lados de F, então:

$$\Gamma =< \{T_i\}_{i\in I} > .$$

O resultado fundamental da teoria dos grupos fuchsianos é apresentado a seguir:

Teorema 9 (Poincaré) Sejam $g \geq 0\ ; r \geq 0, m_i \geq 0, (1 \leq i \leq r)$ números inteiros tais que:

$$(2g-2) + \sum_{i=1}^{r} \left(1 - \frac{1}{m_i}\right) > 0.$$

Então existe um grupo fuchsiano F tal que o espaço das órbitas $\mathbb{H}^2/\Gamma$ é uma superfície compacta orientável de gênero g com r pontos marcados correspondentes às classes de

equivalências maximais de elementos elípticos de ordens $m_1, ..., m_r$ (neste caso, dizemos que Γ tem ASSINATURA $(g; m_1, ..., m_r)$).

Observação. Neste trabalho, os grupos fuchsianos de interesse são aqueles que tem uma região fundamental de área hiperbólica finita, e que, por [16] pg 103, são todos do primeiro tipo (ou seja se $\Lambda(\Gamma)$ é o conjunto que consiste de todos os limites $\lim T_n(z)$ onde os $\{T_n\}$ são sequências de elementos distintos de Γ e $z \in \mathbb{H}^2$, então $\Lambda(\Gamma) = \mathbb{R}$ (no caso do modelo $\mathbb{D}$, $\Lambda(\Gamma) = S^1$)).

2

Códigos e Conjuntos de Sinais

Na concepção tradicional de um sistema de comunicação digital, a informação é codificada (em geral pela adição de bits de paridade) e depois então modulada para a transmissão através do canal. Devido ao processo de codificação, a faixa necessária para a transmissão deve ser aumentada. No caso de sistemas de comunicações limitados em faixa e que tenham que dispor de um processo de codificação é mais do que necessária a proposta de uma estratégia que viabilize projetar tal sistema de comunicações. A busca desta solução leva à concepção moderna de codificação combinada com modulação onde estruturas algébrica e geométrica são colocadas diretamente no conjunto de sinais utilizado para a transmissão, mais especificamente, o alfabeto do código passa a ser a representação no espaço euclidiano ou não, de um conjunto de sinais e as palavras-código são sequências destes sinais sujeitas a algum padrão. A forma de padronização que se mostrou mais adequada é aquela em que existe uma ação transitiva de um grupo no conjunto de sinais (ou seja, na sua representação geométrica). Esta situação é descrita dizendo-se que o conjunto de sinais é Geométricamente

Uniforme. Sobre estes conjuntos de sinais é então colocada uma estrutura, em geral via classes laterais, que conduz aos assim chamados Códigos Geométricamente Uniformes (de Classes Laterais ou de Espaços de Sinais), bem como as suas partições.

2.1 Códigos

Um sistema de comunicações digital pode ser descrito de modo sumário pelo diagrama:

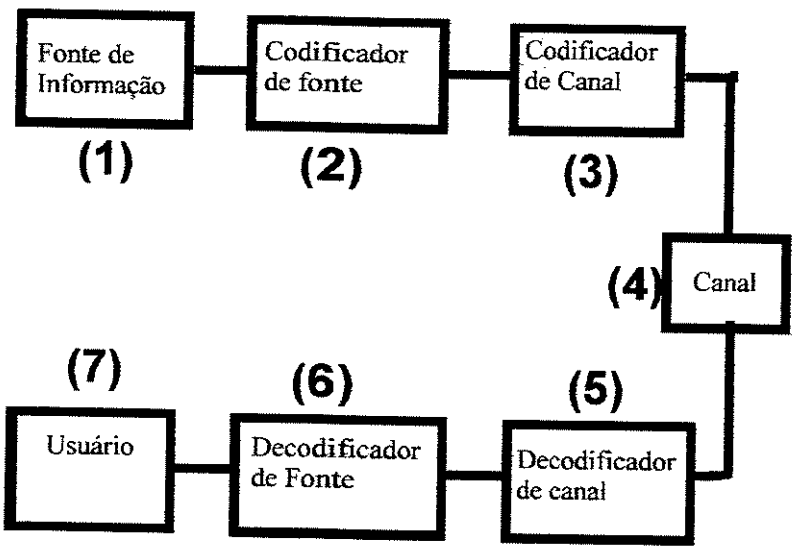

Figura 2.1 - Sistema de Comunicações Digital

A mensagem na saída da fonte de informação, em geral, na forma digital é processada pelo bloco codificador de fonte com o objetivo de realizar a compactação ou compressão da informação a ser transmitida de tal forma a garantir a eficiência da trans-

missão. Por outro lado, o bloco codificador de canal realiza a operação de inserção de redundância suficiente de maneira a garantir uma transmissão confiável. Neste bloco é selecionado um conjunto particular de sinais chamado CÓDIGO , elaborado de modo que os seus elementos sejam facilmente distinguíveis mesmo em presença de ruído. Somente os sinais associados às palavras-código do código são transmitidos através do canal .O codificador de canal (3) alimentado pela saída do codificador de fonte, realiza a substituição de sua entrada por uma das palavras-codigo que é transmitida através do canal. O decodificador de canal (5) recebe o sinal do canal (4) e faz uma estimativa do sinal recebido que é convertida pelo decodificador de fonte (6) na (suposta) mensagem original, que é enviada ao usuário (7).

Cada sinal é uma função $f : I \subseteq \mathbb{R} \rightarrow \mathbb{R}$ na variável $t \in I$, onde $I = [0, T]$ para algum $T \in \mathbb{R}$. T é a DURAÇÃO do sinal em segundos. Pelo Teorema da Amostragem ([27]), se todos as componentes de $f(t)$ têm frequência $\leq WHz$, então f pode ser completamante recuperado pelas $n = 2TW$ amostras

$$\left(f(0), f(\frac{1}{2W}), ..., f(\frac{n-1}{2W})\right)$$

Note que a função f está sendo vista geométricamente como um ponto do espaço $\mathbb{R}^n$. Formalmente, podemos então supor que no canal (4) se transmitam sequências de vetores que são somadas com outras sequências correspondentes do ruído. O objetivo do processo de decodificação é recuperar com o menor erro possível, o sinal que foi transmitido. Existem dois modelos ideais para o canal descrito acima: 1) O canal discreto sem memória

, e 2) O canal contínuo. Os canais de maior interêsse em aplicações são o CANAL BINÁRIO DISCRETO SEM MEMÓRIA, BSC (*binary symmetric channel*) e o CANAL GAUSSIANO BRANCO ADITIVO, $AWGN$ (ruido gaussiano branco aditivo).

No caso do canal $AWGN$, um sinal transmitido $f(t)$ é associado a $F = \left(f(0), f(\frac{1}{2W}), ..., f(\frac{n-1}{2W})\right) \in \mathbb{R}^n$ como acima, e o sinal recebido é representado por $R = F + Y$, onde $Y = (y_1, ..., y_n)$ e os y_i são variáveis aleatórias gaussianas independentes com média 0 e variância σ^2 . Para este canal, o codigo é um conjunto $S \subseteq \mathbb{R}^n$ com M elementos e cada $F \in S$ representa um sinal de faixa W e com duração de T segundos. Com isso, a taxa de transmissão é

$$R = \frac{1}{T} \log_2 M \text{ bits/seg}$$

Consideraremos que o processo de decodificação é de máxima verossimilhança, isto é, se o sinal recebido é $r \in \mathbb{R}^n$, então r é decodificado como F, onde F é o ponto de S mais próximo de r, (no sentido que a norma $\|r - F\|$ é minima). Um erro de decodificação ocorrerá se a norma $\|r - F'\|$ for a menor dentre todas as outras normas e tal que $F' \neq F$, onde F é o sinal transmitido.

Denotando por $P = \frac{1}{T} \int_0^T f(t)^2 dt$ a potência média do sinal e $C = W \log_2 \left[1 + (\frac{P}{\sigma^2})\right]$, a capacidade do canal temos o seguinte resultado:

Teorema 1 .**(Shannon)** [13] [30] Para cada taxa $R < C$, fazendo T (logo $n = 2WT$) suficientemente grande, existe um codigo de taxa R cuja probabilidade de erro é arbitrariamente

pequena.

Para o caso do canal binário simétrico (BSC), existe uma versão equivalente do Teorema de Shannon. Usa-se uma definição de código suficientemente geral para englobar os diferentes casos possíveis, inclusive o caso presente em que os sinais estão em um espaço hiperbólico e não euclidiano.

Definição 1. . Dados os conjuntos $\mathcal{A}$ e I , um CÓDIGO sobre $\mathcal{A}$ é um subconjunto não vazio $\mathcal{C} \subseteq \mathcal{A}^I$. (Tipicamente, $\mathcal{A} = \mathbb{R}$, $\mathcal{A} = \mathbb{H}^2$ ou $\mathcal{A} = \mathbb{F}_q$) . Chamamos $\mathcal{A}$ de $alfabeto$ do código e os elementos de $\mathcal{C}$ são chamados de PALAVRAS-CÓDIGO . Consideraremos que o conjunto I é enumerável. Com isso, dizemos que $\mathcal{C}$ é um CÓDIGO DE BLOCO ou UM CÓDIGO CONVOLUCIONAL (DE TRELIÇA), conforme I seja finito ou infinito.

Um CÓDIGO DE BLOCO BINÁRIO DE COMPRIMENTO n é um subconjunto de $\mathbb{F}_2^n$. De uma maneira geral, um codigo de bloco q-ário é um subconjunto de $\mathbb{F}_q^n$. Este código é utilizado nos CANAIS SIMÉTRICOS q-ÁRIOS .

Dado um código de bloco $\mathcal{C}$, a DISTÂNCIA MÍNIMA deste código é dada por:

$$d = \min \{d_h(u, v) : u, v \in \mathcal{C}, u \neq v\}$$

Supondo que a palavra-código $x \in \mathbb{F}_q^n$ foi transmitida e que $y = x + e$ é o vetor recebido, onde $e \in \mathbb{F}_q^n$ é o vetor êrro, então: Se o peso de Hamming de e (Exemplo 19, página 21) é $w_h(e) \leq d - 1$, então e pode ser detectado (já que duas palavras codigo

diferem em pelo menos d coordenadas). Definindo o RAIO DE EMPACOTAMENTO de $\mathcal{C}$ como $\delta = \left[\frac{1}{2}(d-1)\right]$, temos que se $w_H(e) \leq \delta$, então o erro pode ser corrigido pelo código. De fato, se $\overline{x} \in \mathcal{C}$, $\overline{x} \neq x$, então, como $d(x,\overline{x}) \geqslant d$ temos que $d(x,y) < d(\overline{x},y)$ (de fato, temos que $d(x,\overline{x}) \leq d(x,y) + d(\overline{x},y)$ ou seja: $d(\overline{x},y) \geq d(x,\overline{x}) - d(x,y) \geq d - \frac{d-1}{2} > \frac{d-1}{2} > d(x,y)$) e consequentemente, resulta a estimativa $\widehat{x} = x$ (Ver a Figura 2.2).

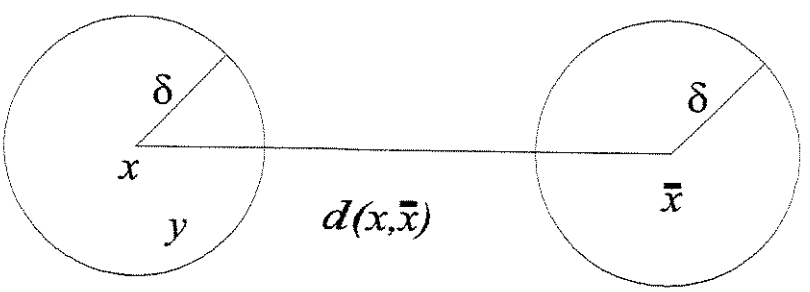

Figura 2.2 - Detecção e Correção de Erros.

Um CÓDIGO LINEAR ou UM CÓDIGO DE BLOCO DE COMPRIMENTO n , $\mathcal{C}$ sobre $\mathbb{F}_q$ é um subespaço vetorial de $\mathbb{F}_q^n$. A DIMENSÃO de $\mathcal{C}$ é a sua dimensão como um $\mathbb{F}-$subespaço vetorial , denotando $k = \dim \mathcal{C}$, ou seja , $|\mathcal{C}| = q^k = M$, então a TAXA de $\mathcal{C}$ é:

$$R = \frac{1}{n}\log_2 M = \frac{k}{n}\log_2 q$$

Um código de comprimento n, dimensão k e distância mínima d é dito um (n,k,d)-código linear, e é imediato que:

$$d = \min\{w_H(u) : 0 \neq u \in \mathcal{C}\}.$$

O que se espera de um bom código é que n seja o menor possível e M e d os maiores possíveis. Como esses objetivos são incompatíveis, o que é procurada é uma solução que faça a otimização desse compromisso em cada caso.

Definição 2. Dizemos que dois códigos $\mathcal{C}$ e $\mathcal{C}'$ sobre $\mathbb{F}_q$ são EQUIVALENTES se existe uma matriz B de ordem $n \times n$ obtida por permutação de linhas ou colunas de $I_{n\times n}$ tal que

$$\mathcal{C}' = \mathcal{C}B = \{uB : u \in \mathcal{C}\}.$$

Note que isto equivale a dizer que existe $\sigma \in S_n$, tal que $\mathcal{C}' = \sigma\mathcal{C} = \{\sigma u : u \in \mathcal{C}\}$, mais especificamente, σ é o elemento de S_n tal que $\sigma I_{n\times n} = B$.

Um (n, k, d)-código linear $\mathcal{C}$ pode ser especificado por uma MATRIZ GERADORA ou seja, uma matriz $k \times n$ M com coeficientes em $\mathbb{F}_q$ de modo que $\mathcal{C}$ consiste de todas as $\mathbb{F}_q$–combinações lineares das linhas de M . É sempre possível determinar um código equivalente a $\mathcal{C}$ com matriz geradora na forma

$$M = [I_{k\times k} : A] \ ; A \in \mathbb{F}_q^{k\times(n-k)}.$$

Denotando por M a matriz geradora de $\mathcal{C}$, temos que se $m = (m_1, ..., m_k) \in \mathbb{F}_q^k$ é uma sequência de dados de entrada, então $x = mM$ é uma palavra-código , logo,

$$\mathcal{C} = \{x = mM \in \mathbb{F}_q^n : m \in \mathbb{F}_q^k\},$$

onde $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$. Definimos então a MATRIZ DE VERIFICAÇÃO DE PARIDADE

de $\mathcal{C}$ como a matriz $H = [-A^t, I_{(n-k)\times(n-k)}]$, então

$$MH^t = 0.$$

Assim, $x \in \mathcal{C}$ se, e somente se, $xH^t = 0$ $(xH^t = mMH^t = m0 = 0)$. Para um vetor qualquer $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$ chamamos de SÍNDROME de x ao vetor $s = xH^t$. Dessa forma $x \in \mathcal{C}$ se, e somente se, $s = 0$. Note que o fato de $s = 0$ não é suficiente para determinar que o vetor recebido seja a palavra-código transmitida, que certamente é uma palavra pertencente a $\mathcal{C}$.

O CÓDIGO DUAL de $\mathcal{C}$ é o código

$$\mathcal{C}^* = \left\{x \in \mathbb{F}_q^n : x \cdot u = 0, \text{ para todo } u \in \mathcal{C}\right\}.$$

Se $\mathcal{C}$ tem uma matriz geradora M , então $\mathcal{C}^*$ tem matriz geradora

$$H = \left[-A^t : I_{(n-k)\times(n-k)}\right].$$

Exemplo 1 O código $(n, 0, n)$ de comprimento n tem somente a palavra $(0, ..., 0)$ e é chamado de CÓDIGO NULO ou ZERO . O seu dual é o codigo $(n, n, 1)$ consistindo de todo o $\mathbb{F}_q^n$, este codigo é chamado de CÓDIGO UNIVERSAL . Chamamos de CÓDIGO DE REPETIÇÃO ao codigo $(n, 1, n)$ consistindo dos vetores da forma $(a, a, ..., a) \in \mathbb{F}_q^n$.

Definição 3. Dizemos que um código $\mathcal{C}$ é CÍCLICO se C é linear e sempre que se $(c_0, c_1, ..., c_{n-2}, c_{n-1}) \in \mathcal{C}$, então $(c_1, c_2, ..., c_{n-1}, c_0) \in \mathcal{C}$.

Seja $q = p^a$, onde p é primo, e $\mathcal{C}$ é um (n, k, d)-código cíclico sobre $\mathbb{F}_q$, então denotando $c = (c_0, ..., c_{n-1}) \in \mathcal{C}$ por $c = c(X) = c_0 + c_1X + c_2X^2 + ... + c_{n-1}X^{n-1} \in \frac{\mathbb{F}_q[X]}{< X^n - 1 >}$, temos que $Xc(X)$ representa $(c_1, ..., c_{n-1}, c_0) \in \mathcal{C}$. Podemos redefinir dizendo que um código cíclico é um ideal de $\frac{\mathbb{F}_q[X]}{< X^n - 1 >}$. Como consequência, $\mathcal{C}$ tem um gerador mônico $g(X)$, o POLINÔMIO GERADOR DO CÓDIGO CÍCLICO $\mathcal{C}$. Assim, $g|X^n - 1$ e $dim\ \mathcal{C} = k = n - \partial g$.

Exemplo 2 O código universal é gerado por $g(X) = 1$ e o codigo de repetição é gerado por $g = 1 + X + ...X^{n-1}$.

Exemplo 3 Uma das versões do CODIGO BINÁRIO DE HAMMING $\mathcal{H}_7$ pode ser representado por um código cíclico binário $(7, 4, 3)$ que tem como polinômio gerador o polinômio $g = 1 + X + X^3$. A matriz geradora correspondente é dada por:

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

Uma outra classe de códigos a ser considerada é a classe dos códigos convolucionais. Iremos supor que os dados de entrada formam uma sequência infinita enumerável (ou seja supomos I infinito enumerável) onde cada conjunto de n bits da sequência codificada depende não só dos k bits da sequência de entrada, como também dos m dígitos an-

teriores de entrada. Dizemos então neste caso, que o codificador tem memória m e e que o código é um (m, k, n)-CÓDIGO CONVOLUCIONAL COM TAXA $R = \frac{k}{n}$. Antes de formalizar o conceito de um código convolucional iremos apresentá-lo através de um exemplo:

Exemplo 4 Considere o codificador convolucional como mostrado na Figura 2.3. Este codificador está associado com um código convolucional com parâmetros: taxa $R = \frac{1}{2}$ e memória $m = 3$.

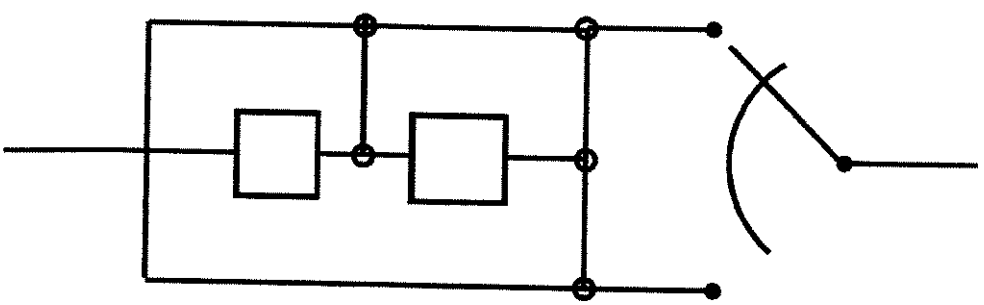

Figura 2.3 - Codificador Convolucional.

A associação que é realizada ao codificador mostrado na Figura 2.3 é a de um sistema linear com uma entrada e duas saídas. Desta figura notamos também que cada saída depende somente da entrada. Logo podemos caracterizar v_1 e v_2 como sendo a resposta deste sistema à entrada u . Matemáticamente podemos escrever isto como sendo

$$v_1 = u * g_1 \qquad \text{e} \qquad v_2 = u * g_2$$

$$g_1 = (1, 1, 1) \qquad\qquad g_2 = (1, 0, 1)$$

onde g_1 e g_2 são denominadas as respostas ao impulso , e $*$ denota a operação de convolução. De modo a simplificar as operações de convolução na determinação de v_1 e v_2 , iremos

utilizar a "transformada X ". Com isso,

$$v_1(X) = u(X) \cdot g_1(X) \qquad \text{e} \qquad v_2(X) = u(X) \cdot g_2(X)$$

onde $g_1(X) = 1 + X + X^2$ e $g_2(X) = 1 + X^2$. Note que X denota o "atraso ".

Se considerarmos $u = (1, 0, 0, 1, 1)$, então $u(X) = 1 + X^3 + X^4$. Consequentemente,

$$v_1(X) = (1 + X^3 + X^4) \cdot (1 + X + X^2) = 1 + X + X^2 + X^3 + X^6$$

$$v_2(X) = (1 + X^3 + X^4) \cdot (1 + X^2) = 1 + X^2 + X^3 + X^4 + X^5 + X^6.$$

A anti-transformada X de $v_1(X)$ e $v_2(X)$ conduz a:

$$v_1 = (1, 1, 1, 1, 0, 0, 1) \quad \text{e} \quad v_2 = (1, 0, 1, 1, 1, 1, 1).$$

Finalmente a palavra-código associada a $u = (1, 0, 0, 1, 1)$ é $v = (11, 10, 11, 11, 01, 01, 11)$.

2.2 Conjuntos de Sinais

A representação de conjuntos de sinais (constelações) como pontos de um espaço euclidiano representou um modelo geométrico bem sucedido do processo de modulação. Por outro lado, a proposta de particionamento do conjunto de sinais representa a introdução de estruturas algébricas no processo de codificação.

O objetivo do presente trabalho é estender os conceitos de constelações, reticulados e particionamento ao plano hiperbólico, em particular o conceito central em codificação/ modulação de uniformidade geométrica. Iniciamos com uma definição formal:

Definição 4. Um CONJUNTO DE SINAIS é um subconjunto discreto S de um espaço $\mathbb{E}$ que pode ser euclidiano ou hiperbólico. Para cada ponto $s \in S$ definimos a REGIÃO DE VORONOI de s como o conjunto $R_V(s) = \left\{x \in \mathbb{E} : d(x,s) = \min_{t \in S} d(x,t)\right\}$ ou seja, $R_V(s)$ é o conjunto de todos os pontos de $\mathbb{E}$ que estão mais perto de s que de qualquer outro ponto de S.

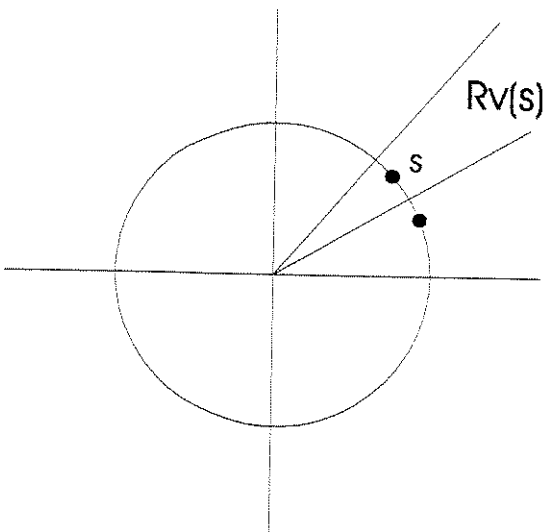

Figura 2.4 - Região de Voronoi

Exemplo 5 A representação no plano $\mathbb{R}^2$ dos elementos de um grupo cíclico $MPSK$ com M elementos é um conjunto de sinais chamado de CÓDIGO DE SLEPIAN correspondente a um esquema de modulação por fase. As regiões de Voronoi são as regiões internas entre pares de semi-retas (bissetrizes dos ângulos determinados por $\zeta^i O \zeta^{i+1}$), passando pela origem (Figura 2.4).

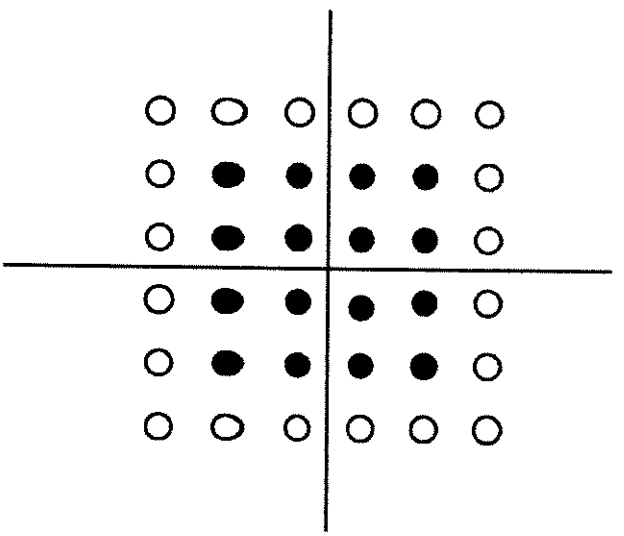

Figura 2.5 - Modulação QAM.

Exemplo 6 Os subgrupos discretos do grupo $(\mathbb{R}^2, +)$ são gerados sobre $\mathbb{Z}$ por $r \leq 2$ vetores linearmente independentes, ou seja, são da forma $\Gamma = \{n_1\, v + n_2 w : n_1, n_2 \in \mathbb{Z}$ e $v, w \in \mathbb{R}^2$ são vetores fixos$\}$. No caso em que v e w são ambos não nulos e distintos , o grupo Γ é chamado de RETICULADO [34]. Os conjuntos do tipo $\Gamma = \Lambda + v$ onde Λ é um reticulado e v é um elemento qualquer de $\mathbb{R}^2$, são conjuntos de sinais. Chamamos o transladado Γ, do reticulado Λ, de ARRANJO REGULAR. Considere agora o arranjo regular $\Gamma = \mathbb{Z}^2 + (\frac{1}{2}, \frac{1}{2})$ e o subgrupo $\Delta = 4\mathbb{Z}^2 + (\frac{1}{2}, \frac{1}{2})$, então temos que $\Delta \lhd \Gamma$, com índice $[\Gamma : \Delta] = 16$. Com isto, temos um conjunto completo de representantes de Γ/Δ, $[\Gamma/\Delta] = \{(\pm\frac{1}{2}, \pm\frac{1}{2}), (\pm\frac{1}{2}, \pm\frac{3}{2}), (\pm\frac{3}{2}, \pm\frac{1}{2}), (\pm\frac{3}{2}, \pm\frac{3}{2})\}$. A Figura 2.5 é representaçãao geométrica de $[\Gamma/\Delta]$.

Este conjunto $[\Gamma/\Delta]$ representa uma modulação QAM (simultaneamente em amplitude e em fase). No caso QAM, vemos que as regiões de Voronoi não são todas iguais. Forney descreveu este fenômeno como uniformidade com efeito de fronteira (*boundary effects*) [09] pg 1247.

2.3 Conjuntos de Sinais Hiperbólicos

No plano hiperbólico $\mathbb{H}^2$ podemos obter conjuntos de sinais a partir das, assim, chamadas tesselações regulares, que tem a vantagem de poder ser estudadas a partir dos grupos associados às mesmas.[08] e [06].

Definição 5. Uma TESSELAÇÃO REGULAR do plano hiperbólico $\mathbb{H}^2$ é uma partição de $\mathbb{H}^2$ por polígonos regulares não sobrepostos todos com o mesmo número de lados sujeitos à restrição de se interceptarem somente em suas arestas ou em vértices , onde se encontram sempre o mesmo número de polígonos. Uma tesselação regular em que q p-ágonos regulares se encontram em cada vértice é denotada por $\{p, q\}$.

Como a soma dos ângulos internos de um triângulo hiperbólico é sempre menor que π temos então (Figura 2.6) que existe uma tesselação hiperbólica {p,q} se, e somente se

$$(p-2)(q-2) > 4$$

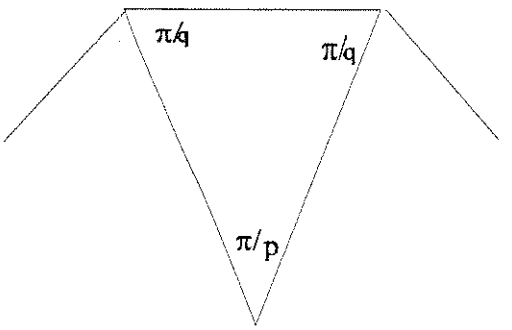

Figura 2.6 - Triângulo Hiperbólico.

Associado a cada tesselação $\{p, q\}$ existe um grupo $[p, q]$, denominado o GRUPO COMPLETO DE SIMETRIAS de $\{p, q\}$ que é o subgrupo de $Isom(\mathbb{H}^2)$ gerado pelas reflexões em torno de todas as retas (hiperbólicas) nas quais a tesselação $\{p, q\}$ se reflete nela mesma [06], ou seja $[p, q]$ consiste das isometrias de $\mathbb{H}^2$ que aparentemente deixam $\{p, q\}$ invariante [08] . Por [06] pg 53 temos que o grupo $[p, q]$ é gerado pelas reflexões r_1, r_2 e r_3 nos lados do triângulo hiperbólico com ângulos $\frac{\pi}{2}, \frac{\pi}{p}, \frac{\pi}{q}$ como mostrado na Figura 2.7.

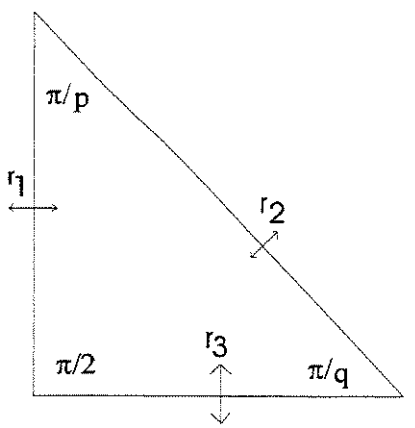

Figura 2.7 - Reflexões Geradoras.

A presentação do grupo $[p,q]$ é então

$$[p,q] =< r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_2 r_1)^p = (r_3 r_2)^q = (r_1 r_3)^2 = e > .$$

Deve-se notar que $[p,q]$ não é um grupo fuchsiano, pois por exemplo $r_1(z) = -\overline{z}$ e, portanto, $r_1 \notin PSL(2,\mathbb{R})$.

Dada uma tesselação $\{p,q\}$ com grupo $[p,q]$ então a sua tesselação dual é $\{q,p\}$ com grupo $[q,p]$. É imediato que $[p,q]$ e $[q,p]$ são isomorfos, mas as tesselações $\{p,q\}$ e $\{q,p\}$ coincidem se, e somente se, $p = q$. O caso $p = q$ é chamado de AUTO-DUAL e se $p = q = 4g$, para algum inteiro $g \geq 2$, então a tesselação $\{4g, 4g\}$ é tal que a identificação dos lados dos polígonos torna $\mathbb{H}^2$ um recobrimento da superfície compacta orientável M de gênero g (ou seja, existe uma aplicação $p : \mathbb{H}^2 \to M$, a saber, $p(x)$ é o ponto da região fundamental correspondente ao que x ocupa no elemento da tesselação de $\mathbb{H}^2$ que o contém, e p é tal que para cada $m \in M$, existe um conjunto aberto V contendo m , tal que $p^{-1}(m) = \bigcup_{\alpha} A_\alpha$ onde os A_α são abertos dois a dois disjuntos e para cada α , $p|A_\alpha : A_\alpha \to V$ é uma bijeção contínua e com inversa contínua, portanto um homeomorfismo ([19]) e o seu grupo $[4g, 4g]$ tem como subgrupo normal o grupo fundamental desta superfície.

Definindo o grupo fundamental desta superfície por:

$$\Pi_g =< a_1, ..., a_g, b_1, ..., b_g : \prod_{i=1}^{g} [a_i, b_i] = 1 >$$

resulta que $\Pi_g \lhd [4g, 4g]$, e que

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

A Figura 2.8 ilustra a tesselação de $\mathbb{H}^2$ por $[8, 8]$ cuja região fundamental é um polígono hiperbólico regular de 8 lados.

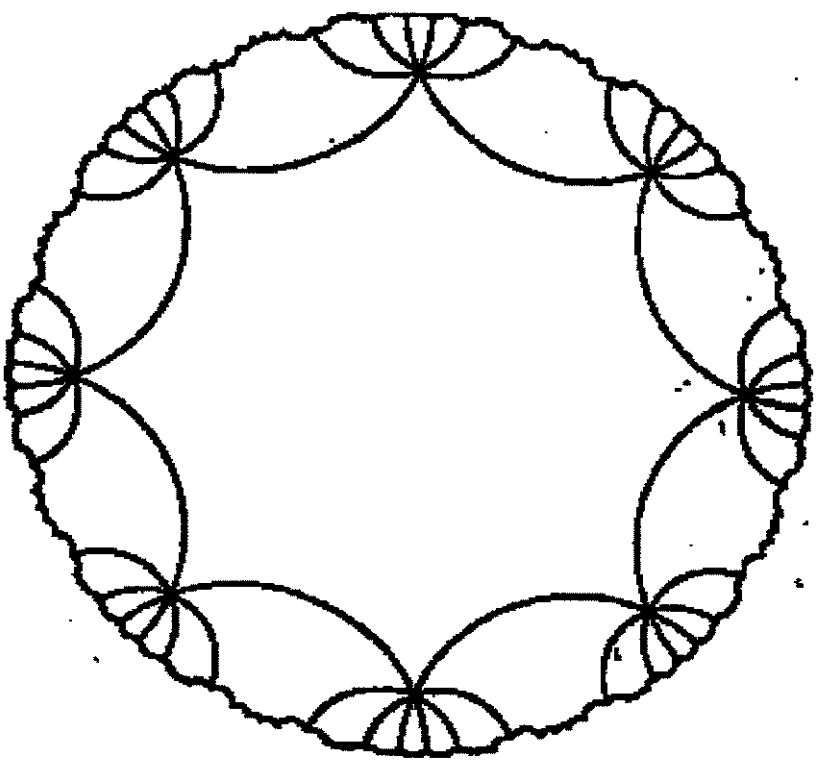

Figura 2.8 - A tesselação $\{8, 8\}$.

O grupo $[p, q]$ pode também ser obtido como um subgrupo de índice $2p$ do grupo $\Gamma^*(2, p, q)$, este chamado de GRUPO DE TRIÂNGULO tendo como região fundamental

um triângulo Δ^* cujos ângulos são $\frac{\pi}{2}, \frac{\pi}{p}, \frac{\pi}{q}$. Associado ao mesmo temos o grupo fuchsiano

$$\Gamma(2,p,q) = \Gamma^*(2,p,q) \cap PSL(2,\mathbb{R})$$

com assinatura $(0;2,p,q)$ e região fundamental $\Delta^* \cup r_1(\Delta^*)$.

Observação. Tesselações regulares da forma $\{4g,4g\}$ podem ser encontradas como subtesselações da tesselação associada a um grupo de triângulo Γ^*, ou à sua parte fuchsiana Γ com região fundamental Δ^*, ou $\Delta = \Delta^* \cup r_1(\Delta^*)$, a partir da determinação de $4g$-ágonos, formados por reuniões de cópias de Δ ou Δ^*, com as respectivas identificações de seus lados de forma a gerar uma superfície orientável de gênero g . Esse procedimento é equivalente a determinar um subgrupo de Γ isomorfo a Π_g , o grupo fundamental da superfície compacta orientável de gênero g. Assim, os grupos de triângulo se tornam o ambiente adequado para busca de tesselações relevantes para comunicações. O problema de obtenção de Π_n como subgrupo de $\Gamma(2,p,q)$ tem respostas conhecidas . O exemplo a seguir, ilustra este fato.

Exemplo 7 [24] O grupo fundamental Π_2 pode ser obtido como subgrupo normal de índice 24 do grupo $\Gamma(2,6,4)$. O grupo $\Gamma^*(2,6,4)$ tem como região fundamental o triângulo hiperbólico Δ^* com ângulos $\frac{\pi}{2}, \frac{\pi}{6}$ e $\frac{\pi}{4}$ e área hiperbólica $\pi - \left(\frac{\pi}{2} + \frac{\pi}{6} + \frac{\pi}{4}\right) = \frac{\pi}{12}$. Assim, o grupo fuchsiano $\Gamma(2,6,4) = \Gamma^*(2,6,4) \cap PSL(2,\mathbb{R})$ tem como região fundamental (região de Dirichlet) o triângulo hiperbólico $\Delta = \Delta^* \cup r_1\Delta^*$ com ângulos $\frac{\pi}{3}, \frac{\pi}{4}$ e $\frac{\pi}{4}$ com área hiperbólica $\frac{\pi}{6}$ (r_1 é a reflexão sobre a reta que contem o lado de Δ^* onde estão os

ângulos de $\frac{\pi}{2}$ e $\frac{\pi}{6}$, r_2 é a reflexão sobre a reta que contem o lado de Δ^* onde estão os ângulos de $\frac{\pi}{4}$ e $\frac{\pi}{6}$, r_3 é a reflexão sobre a reta que contem o lado de Δ^* onde estão os ângulos de $\frac{\pi}{2}$ e $\frac{\pi}{4}$) (Figura 2.9)

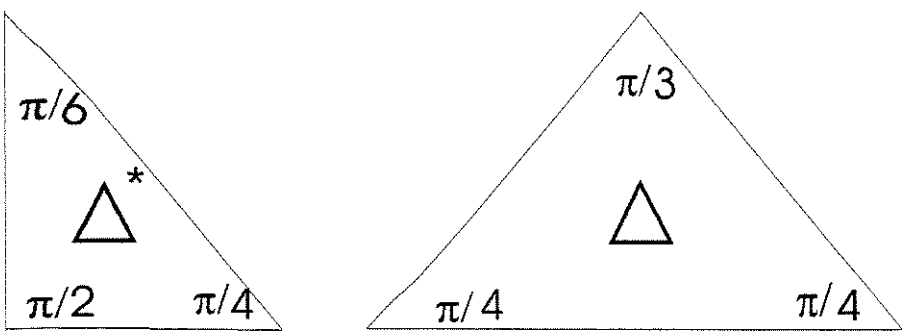

Figura 2.9 - Os Triângulos Hiperbólicos Δ e Δ^*.

Considerando os geradores a e b de $\Gamma(2,6,4)$, onde $a = r_3 r_1$ e $b = r_1 r_2$, temos então que as relações satisfeitas por a e b são

$$a^2 = b^6 = (ab)^4 = 1.$$

Considerando, agora, o subgrupo normal Θ de $\Gamma(2,6,4)$ gerado por $b_0 = b$ e $b_1 = aba^{-1}$, temos que se $x \in \Gamma(2,6,4)$, então, todas as ocorrências de b são reduzidas à identidade em $\frac{\Gamma}{\Theta}$ .Com isso, resulta de $a^2 = 1$ que $\frac{\Gamma}{\Theta} \simeq \mathbb{Z}_2$, ou seja , $[\Gamma : \Theta] = 2$ e os geradores de Θ satisfazem as relações

$$b_0^6 = b_1^6 = (b_0 b_1)^2 = 1.$$

Considere, agora, o subgrupo normal Φ de Θ gerado por

$$c_k = b_0^k b_1 b_0^{1-k} \ , \ k = 0, 1, ..., 5,$$

resulta que cada elemento $y \in \Theta$ é congruente a uma potência b_0^i módulo Φ, e portanto, $\frac{\Theta}{\Phi} \simeq \mathbb{Z}_6$, ou seja, $[\Theta : \Phi] = 6$ e os geradores de Φ satisfazem

$$c_k^2 = 1 \ , \ c_0 c_5 c_4 c_3 c_2 c_1 = 1.$$

Denotando agora por Ψ o subgrupo normal de Φ gerado por

$$u_{i+1} = c_{i+1} c_i \ , \ i = 1, 2, 3, 4,$$

temos então que se $t \in \Phi$, inserindo pares da forma $c_i c_i$ e eliminando os pares da forma $c_{i++1} c_i$ e os da forma c_i^2 obtemos que t é congruente a $c_0 c_5$ ou a $c_1 c_0$ modulo Ψ o que resulta em $[\Phi : \Psi] = 2$. Consequentemente os geradores de Ψ denotados por

$$x = u_2^{-1},$$

$$y = u_3^{-1},$$

$$z = u_4^{-1},$$

$$w = u_5^{-1},$$

satisfazem a única relação

$$xyzwz^{-1}x^{-1}w^{-1}y^{-1} = 1.$$

Se reescrevemos esta relação como

$$z^{-1}y^{-1} \cdot x \cdot yz \cdot x^{-1} \cdot xw \cdot z^{-1}y^{-1}yx^{-1} \cdot w^{-1}x^{-1} \cdot xy^{-1}yz = 1,$$

e denotando $a_1 = z^{-1}y^{-1}, b_1 = x, a_2 = xw, b_2 = z^{-1}y^{-1}yx^{-1}$, obtemos então a presentação de Ψcomo sendo dada por

$$\Psi =< a_1, b_1, a_2, b_2 : [a_1, b_1][a_2, b_2] = 1 > .$$

Pela simetria da única relação definidora de Ψ temos que $\Psi \lhd \Gamma$ e como $\Psi \simeq \Pi_2$ obtemos finalmente que Π_2 é um subgrupo normal de Γ com indice 24. (ou $[\Pi_2 : \Gamma^*] = 48$).

2.4 Conjuntos de Sinais Casados a Grupos

Definição 6. [22] Um conjunto de sinais S é CASADO a um grupo G se existir uma aplicação sobrejetora

$$m : G \longrightarrow S,$$

tal que para todos $g, g' \in G$,

$$d(m(g), m(g')) = d(m(g^{-1} \cdot g'), m(e))$$

chamamos m de APLICAÇÃO CASADA, e se m é injetora dizemos que m^{-1} é um ROTULAMENTO CASADO.

Se $m : S \to G$ é uma aplicação casada então $H = m^{-1}(m(e))$ é um subgrupo de G e $g \equiv g' \bmod H$ se, e somente se, $m(g) = m(g')$. Assim, qualquer aplicação casada

m corresponde a uma bijeção $gH \longmapsto m(g)$ das classes laterais à esquerda de H em G nos elementos de S. É imediato que se $H \lhd G$, então a aplicação quociente $m : \frac{G}{H} \to S$ é um rotulamento casado. Dizemos que um rotulamento $m : G \to S$ é um ROTULAMENTO EFETIVO se H não contem um subgrupo normal de G não trivial (ou seja $\neq \{e\}$). Neste caso, dizemos que S é EFETIVAMENTE CASADO a G . Esta é a situação mais geral porque se S não é efetivamente casado a G, então tomando H' como o maior subgrupo normal de G contido em H , resulta que a função $m : \frac{G}{H'} \to S$ fica bem definida ($m(g) = m(g')$ se, e somente se, $gH' = g'H'$ e $g'g^{-1} \in H' \subseteq H$).

Exemplo 8 Sejam S um espaço métrico com métrica d_S e G um grupo que possui uma métrica de grupo d_G tal que existe uma função $m : G \to S$ que é uma isometria, então temos para quaisquer $g, h \in G$ que $d_S(m(g), m(h)) = d_G(g, h) = d_G(g \cdot h^{-1}, e) = d_S(m(g \cdot h^{-1}), m(e))$ de onde resulta que m é um rotulamento casado.

Teorema 2 Existe um rotulamento casado entre um conjunto de sinais S e um grupo G se, e somente se, G é isomorfo a um subgrupo transitivo de $\Gamma(S)$, o grupo das isometrias de S

Demonstração: Seja Θ um subgrupo transitivo de $\Gamma(S)$ com $\Theta \simeq G$, digamos $S = \{\theta(s) : \theta \in \Theta\}$ para um $s \in S$ fixo. Definimos, então, $m : \Theta \to S$ por $m(\sigma) = \sigma(s)$. Com isso temos para $\sigma, \tau \in \Theta$ que $d_S(m(\sigma), m(\tau)) = d_S(\sigma(s), \tau(s)) = d_S(\sigma^{-1}\sigma(s), \sigma^{-1}\tau(s)) = d_S(s, \sigma^{-1}\tau(s)) = d_S(m(e), m(\sigma^{-1}\tau))$ o que mostra que m é um rotulamento casado.

Reciprocamente, se $m : G \to S$ é um rotulamento casado (ou seja, podemos escrever $S = \{m(g) : g \in G\})$, vamos definir para cada $h \in G$, $f(h) : S \to S$, $f(h)(m(g)) = m(h \cdot g)$ para cada $m(g) \in S$, então temos que $d_S(f(h)(m(g_1)), f(h)(m(g_2)))$= $d_S(m(h \cdot g_1), m(h \cdot g_2))$ =$d_S(m(g_1^{-1}h^{-1}hg_2), m(e)) = d_S(m(g_1^{-1}g_2), m(e)) = d_S(m(g_1), m(g_2))$ e portanto, $f(h)$ é uma isometria de S para cada h . Com isto, fica definida uma função $f : G \to \Gamma(S)$. Se $h_1, h_2 \in G$, temos que para todo $s = m(g) \in S$, $f(h_1 \cdot h_2)(m(g)) = m((h_1 \cdot h_2) \cdot g) = m(h_1(h_2 g)) = f(h_1)(m(h_2 g)) = f(h_1)(f(h_2)(m(g))) = f(h_1) \circ f(h_2)(m(g))$. Logo, f é um homomorfismo. Além disso, se $f(h)(m(g)) = m(g)$ para todo $m(g) \in S$, então $m(hg) = m(g)$ e como m é um rotulamento casado, resulta que $hg = g$ ou $h = e$. Portanto, $Ker(f) = \{e\}$ e f é injetora. Assim, $G \simeq \mathrm{Im}(f) = \Theta \leq \Gamma(S)$. Finalmente , dado $s = m(e)$, se $h \in G$ é tal que $m(h) = s' \in S$, então $m(h) = m(h \cdot e) = f(h)(m(e))$, ou seja $f(h)(s) = s'$ e desse modo Θ é um subgrupo transitivo. ■

2.5 G-Linearidade

Em [12] foi demonstrado que determinados códigos binários não lineares podem ser imagens de códigos lineares sobre $\mathbb{Z}_4$, permitindo o uso de métodos de decodificação mais eficazes. Em [11] foi considerada a possibilidade e as limitações das possíveis extensões deste conceito, principalmente na direção da $\mathbb{Z}_{2^k}$ -linearidade.

A seguir, formulamos então uma definição geral do seguinte modo:

Definição 7. Dizemos que um código $\mathcal{C} \subseteq S^I$ é $G-$LINEAR se existem uma isometria $\mu : G \to S$, um codigo de grupo $\mathcal{D} \leq G^I$ e uma permutação $\sigma \in S_I$ tal que $\sigma(\mathcal{C}) = \mu(\mathcal{D})$, onde denotamos também por μ a extensão $\mu : G^I \to S^I$.

$$\begin{array}{ccc} & \mathcal{D} \leq G^I & \\ & \overset{m}{\swarrow} \quad \overset{\mu}{\searrow} & \\ \mathcal{C} \subseteq S^I & \xrightarrow{\sigma} & S^I \end{array}$$

Observação. Considerando a função $m = \sigma^{-1} \circ \mu : G^I \to S^I$ temos que :

$d_{S^I}(m(g), m(g')) =$

$d_{S^I}(\sigma^{-1}(\mu(g)), \sigma^{-1}(\mu(g'))) = d_{S^I}(\mu(g), \mu(g')) = d_{G^I}(g, g') = d_{G^I}(g \cdot g'^{-1}, e)$

$= d_{S^I}(\mu(gg'^{-1}), \mu(e)) = d_{S^I}(\sigma^{-1}\mu(gg'^{-1}), \sigma^{-1}\mu(e)) = d_{S^I}(m(gg'^{-1}), m(e))$ de onde

$m : G^I \to S^I$ é um rotulamento casado e tambem o é $m : \mathcal{D} \to \mathcal{C}$. Pelo Teorema 2, $\mathcal{D}$ é isomorfo a um grupo transitivo de simetrias de $\mathcal{C}$.

2.6 Conjuntos de Sinais Geometricamente Uniformes

O conceito de conjunto de sinais geometricamente uniforme foi introduzido por Forney em [09]. No contexto dos espaços e conjuntos de sinais euclidianos este conceito se mostrou o mais adequado para unificar processos como as partições de Ungerboeck [35] e a Concatenação generalizada [02], e em certo sentido é a forma mais geral que pode

assumir um conjunto de sinais , mantendo ainda boas características do ponto de vista de codificação/decodificação.

Definição 8. Um conjunto de sinais S é GEOMÉTRICAMENTE UNIFORME se a ação de $\Gamma(S)$ em S é transitiva.

Observação. Mais explicitamente, a definição acima diz o seguinte: Dados $x, y \in S$, deve existir $u \in \Gamma(S)$ tal que $u(x) = y$, ou para cada $x \in S$, a sua órbita por $\Gamma(S)$ é todo S , $S = \{u(x) : u \in \Gamma(S)\}$

Exemplo 9 No plano hiperbolico $\mathbb{H}^2$ consideremos a tesselação $\{8, 8\}$, então o conjunto S constituído pelos centros dos octógonos da tesselação (ou equivalentemente dos vértices dos octógonos da tesselação dual) é geometricamemte uniforme, já que para cada $x \in S$ fixo, temos que $S = \{T(x) : T \in [8, 8]\}$. Como $[8, 8] = \Pi_8 \ltimes D_8$, onde $D_8 = \mathbb{Z}_8 \ltimes \mathbb{Z}_2$, então $D_8(x) = \{T(x) : x \in D_8\} = P$ é um octógono (dual), e P é ele mesmo geométricamente uniforme com $\Gamma(P) = D_8$. Todavia, $|P| = 8$ e $|D_8| = 16$. Assim, $\Gamma(P)$ tem mais elementos que o necessário para gerar P. Contudo, tomando os subgrupos $G_1 = \mathbb{Z}_8$ e $G_2 = \mathbb{Z}_4 \ltimes \mathbb{Z}_2$ contidos em D_8 então, temos, que $P = G_1(x) = G_2(x)$. Como G_1 e G_2 não são isomorfos e são subgrupos próprios de D_8 , concluimos que um conjunto de sinais pode ter um grupo de simetrias com mais elementos que o próprio conjunto, como pode ter grupos de simetrias com o mesmo número de elementos , grupos estes não isomorfos.

Observação. Em [32] é apresentado um exemplo de um conjunto S de sinais com 10

elementos em $\mathbb{R}^5$ que não é orbita de nenhum subgrupo de simetrias de $\mathbb{R}^5$. Portanto, nem todo conjunto de sinais, mesmo euclidiano, é geométricamente uniforme.

Definição 9. Dado um conjunto de sinais S, dizemos que um subgrupo $U(S)$ de $\Gamma(S)$ é um GRUPO GERADOR de S, se $S = \{u(s_0) : u \in U(S)\}$, para s_0 fixo em S, e $U(S)$ é minimal para a geração de S no sentido de que a função $m : U(S) \to S$, $m(u) = u(s_0)$ é uma bijeção.

Observação. Obviamente, m induz em S uma estrutura de grupo isomorfa à de $U(S)$.

Teorema 3 Seja S um conjunto de sinais, então são equivalentes as seguintes afirmações:

(i) S é geométricamente uniforme;

(ii) Existe um rotulamento casado entre S e o grupo $U(S)$;

(iii) S é $U(S)$-linear com $m : U(S) \to S$.

Demonstração $(i) \iff (ii)$ é o Teorema 2 e $(i) \iff (iii)$ Segue imediatamente da Observação logo após a Definição 7.□

Lema 4 Seja S um conjunto de sinais geométricamente uniforme e $x, y \in S$ quaisquer, então existe uma isometria $u \in \Gamma(S)$ tal que $u(x) = y$, e que $u(R_V(x)) = R_V(y)$. Em outras palavras, as regiões de Voronoi são todas congruentes.

Demonstração. Temos que $v \in R_V(x)$ se, e somente se, $d(x,v) = \min\limits_{z \in S} \{d(z,v)\}$ mas $d(u(v),y) = d(u(v),u(x)) = d(v,x) = \min\limits_{z \in S} \{d(v,z)\} = \min\limits_{z \in S} \{d(u(v),u(z))\} = \min\limits_{w \in S}$

$\{d(u(v), w)\}$. Logo $u(v) \in R_V(y)$ e $u(R_V(x)) \subseteq R_V(y)$. Tomando u^{-1}, obtemos a outra desigualdade, e portanto $u(R_V(x)) = R_V(y)$ ■

Observação. Se o conjunto de sinais é determinado por uma tesselação $\{p, q\}$, então é imediato que cada polígono é uma região de Voronoi. No caso geral de um grupo fuchsiano, uma região de Voronoi é uma região de Dirichlet.

Observação. A congruência das regiões de Voronoi é que determina as propriedades de importância em comunicações, isto é, os perfis de distâncias e a probabilidade de erro associada a cada sinal na constelação é determinada localmente.

3

Grupos Hiperbólicos

Os objetivos principais da teoria dos códigos geométricamente uniformes são relacionados com as construções das partições geométricamente uniformes e dos códigos de espaços de sinais geométricamente uniformes, em particular, os Códigos de Classe Lateral Generalizados (Capítulo 4). As construções citadas dependem da existência e do conhecimento das partições dos grupos de isometrias envolvidos no processo. Em outras palavras: A existência de tesselações regulares do plano hiperbólico da forma $\{p, q\}$ gerando conjuntos de sinais, justifica a procura de subgrupos e quocientes dos grupos $[p, q]$, que forneçam informações sobre as estruturas dos mesmos. Neste capítulo são discutidos dois casos: 1) O caso auto-dual, onde são obtidas presentações de grupos que tem $[8, 8]$ como extensão respectivamente, pelos grupos $\mathbb{Z}_n$, D_n, $\mathbb{Z}_m \times \mathbb{Z}_n$, onde m e n são números inteiros positivos; 2) O caso não auto-dual em que o grupo $[p, 3]$, é descrito, para valôres específicos de p, através de um par de extensões sucessivas por $\mathbb{Z}_2$ e por $\mathbb{Z}_3$. Estes resultados fornecem o substrato algébrico para o tratamento formal de conjuntos de sinais do Capítulo 4.

3.1 O Caso Auto-Dual

O caso do conjunto de sinais com tesselação auto-dual é o que está menos distante do caso euclidiano, pois a tesselação determinada pelo seu grupo de isometrias é idêntica à tesselação dual (determinada pelo grafo de Cayley) .

3.1.1 Determinação dos Subgrupos z_n

O objetivo deste parágrafo é determinar para cada $n \geq 2$ um subgrupo normal z_n de $[8,8]$ de modo que $[8,8]$ seja uma extensão de z_n por $\mathbb{Z}_n$. Isto permite a descrição de uma região fundamental correspondente a n cópias da região original, permitindo a descrição de conjuntos de sinais onde cada ponto de sinal corresponde ao centro de uma cópia da região fundamental de $[8,8]$, generalizando de modo natural a teoria nos espaços euclidianos.

Consideremos o grupo

$$\Pi = \Pi_2 =< a_1, b_1, a_2, b_2 : [a_1,b_1][a_2,b_2] = 1 > .$$

Denotando agora por z_n o subgrupo normal de Π gerado por a_1^n, b_1, a_2 e b_2,ou seja, $z_n =< a_1^n, b_1, a_2, b_2 >$, temos então pelo Teorema de Presentação de Quocientes (Teorema 2 do Capítulo 1) que

$$\frac{\Pi}{z_n} =< a_1, b_1, a_2, b_2 : [a_1,b_1][a_2,b_2] = 1 \ e \ a_1^n = b_1 = a_2 = b_2 = 1 >=< a_1 : a_1^n = 1 >= \mathbb{Z}_n$$

Assim,$\{1, a_1, a_1^2, ..., a_1^{n-1}\}$ é um sistema completo de representantes de Schreier para Π modulo z_n. Como no quociente $\frac{\Pi}{z_n}$ os elementos b_1, a_2, b_2 são todos reduzidos à

identidade, então:

$$U(a_1, b_1, a_2, b_2) = a_1^{\sigma_{a_1}(U) \bmod n}.$$

Os $4n$ potenciais geradores de z_n na forma s_{K,a_ν} são indexados por: $K \in \{1, a_1, a_1^2, ..., a_1^{n-1}\}$ e $a_\nu \in \{a_1, b_1, a_2, b_2\}$.

Como para todos M e a_λ tais que M e a_λ determinam o mesmo elemento no grupo livre gerado pelos a_λ (Definição 7 do Capítulo 1) , então estes elementos podem ser eliminados da presentação (que denotamos por $\overline{Ma_\lambda} \approx Ma_\lambda$). Assim s_{M,a_λ} é um relator, e além disso, $\overline{a_1^j \cdot a_1} = \overline{a_1^{j+1}} = a_1^{j+1}$ se $j+1 < n$ ou $j < n-1$. Portanto, $s_{a_1^j,a_1} \approx 1$ se $j = 0, 1, \cdots, n-2$.

Como existe um só relator $R_\mu = [a_1,b_1][a_2,b_2]$, para determinarmos (com as notações do Teorema 3 do Capítulo 1) $\tau(KR_\mu K^{-1})$ calculamos os m $\tau(U)$ onde:

$U = a_1^j[a_1,b_1][a_2,b_2]a_1^{-j}$ para $j = 0, 1, ..., n-1$.

Vamos agora determinar os elementos W_i, e a partir dos mesmos, usando a fórmula:

$$K_j = \begin{cases} \overline{W_j}, \text{ se } \epsilon_j = 1 \\ \overline{W_j a_{\nu_j}^{-1}}, \text{ se } \epsilon_j = -1 \end{cases}$$

obter os representantes K_i como se segue:

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = a_1$ ..... $K_2 = a_1$

. . . . . .

$W_j = a_1^{j-1}$ ..... $K_j = a_1^{j-1}$

$W_{j+1} = a_1^j$ ..... $K_{j+1} = a_1^j$

$W_{j+2} = a_1^{j+1}$ $\quad K_{j+2} = a_1^{j+1}$ se $j < n-1$ e $K_{j+2} = 1$ se $j = n-1$

$W_{j+3} = a_1^{j+1} \cdot b_1$ ..... $K_{j+3} = a_1^j$

$W_{j+4} = a_1^{j+1} b_1 a_1^{-1}$ ..... $K_{j+4} = a_1^j$

$W_{j+5} = a_1^j [a_1, b_1]$ ..... $K_{j+5} = a_1^j$

$W_{j+6} = a_1^j [a_1, b_1] a_2$ ..... $K_{j+6} = a_1^j$

$W_{j+7} = a_1^j [a_1, b_1] a_2 b_2$ ..... $K_{j+7} = a_1^j$

$W_{j+8} = a_1^j [a_1, b_1] a_2 b_2 a_2^{-1}$ ..... $K_{j+8} = a_1^j$

$W_{j+8+1} = a_1^j [a_1, b_1][a_2, b_2]$ ..... $K_{j+8+1} = a_1^{j-1}$

$W_{j+8+2} = a_1^j [a_1, b_1][a_2, b_2] a_1^{-1}$ ..... $K_{j+8+2} = a_1^{j-2}$

$W_{j+8+3} = a_1^j [a_1, b_1][a_2, b_2] a_1^{-2}$ ..... $K_{j+8+3} = a_1^{j-3}$

. . . . . .

$W_{j+8+j-1} = a_1^j [a_1, b_1][a_2, b_2] a_1^{-(j-2)}$ ..... $K_{j+8+j-1} = a_1$

$W_{j+8+j} = a_1^j [a_1, b_1][a_2, b_2] a_1^{-(j-1)}$ ..... $K_{j+8+j} = 1$

Com isto, estamos então em condições de determinar o relator $\tau(U)$ em função dos geradores definidores s_{K,a_ν} , ou seja:

$$\tau(U) = \left\{ \begin{array}{ccccccccc} s_{1,a_1} & \cdot & \cdot & \cdot & \cdot & \cdot & s_{a_1^{j-1},a_1} & \cdot \\ s_{a_1^j,a_1} & \cdot & s_{*,b_1} & \cdot & s_{a_1^j,a_1} & \cdot & s_{a_1^j,b_1} & \cdot \\ s_{a_1^j,a_2} & \cdot & s_{a_1^j,b_2} & \cdot & s^{-1}_{a_1^j,a_2} & \cdot & s^{-1}_{a_1,b_2} & \cdot \\ s^{-1}_{a_1^j,a} & \cdot & \cdot & \cdot & \cdot & \cdot & s^{-1}_{1,a_1} & \cdot \end{array} \right.$$

de onde concluimos que $\tau(U) = s_{*,b_1} \cdot s^{-1}_{a_1^j,b_1} \cdot [s_{a_1^j,a_2}, s_{a_1^j,b_2}]$, com $* = a_1^{j+1}$ se $j < n-1$ e $* = 1$ se $j = n-1$.

Observação. Denotando $c_j = s_{a_1^j,b_1}$, $d_j = s_{a_1^j,a_2}$, $e_j = s_{a_1^j,b_2}$, temos que

$$z_n =< \{c_i\}, \{d_i\}, \{e_i\}, 0 \leq i \leq n-1 : c_{i+1}c_i^{-1}[d_i, e_i] = 1 : 0 \leq (i-1) \bmod n > .$$

Desse modo, acabamos de provar o seguinte resultado:

Teorema 1 .Seja $\Pi = \Pi_2 =< a_1, b_2, a_2, b_2 : [a_1,b_1][a_2,b_2] = 1 >$ o grupo fundamental da superfície compacta orientável de gênero 2, então, para cada número natural $n \geq 2$, Π é uma extensão de z_n por $\mathbb{Z}_n$, ou seja,

$$\frac{\Pi}{z_n} \simeq \mathbb{Z}_n,$$

onde:

$$z_n =< \{c_i\}, \{d_i\}, \{e_i\}, 0 \leq i \leq n-1 : c_{i+1}c_i^{-1}[d_i, e_i] = 1 : 0 \leq (i-1) \bmod n > .$$

3.1.2 Determinação dos Subgrupos d_n

O objetivo deste parágrafo é determinar para cada $n \geq 2$ um subgrupo normal d_n de $[8,8]$ de modo que $[8,8]$ seja uma extensão de d_n por D_n, o que permite a descrição de uma região fundamental correspondente a $2n$ cópias da região original, permitindo a descrição de conjuntos de sinais onde cada ponto de sinal corresponde ao centro de uma cópia da região fundamental de $[8,8]$, generalizando de modo natural a teoria nos espaços euclidianos.

Consideremos agora o subgrupo normal d_n de Π gerado pelos elementos $a_1^n, a_2^2, a_1 b_1^{-1}, a_2 b_2^{-1}, (a_1 a_2)^2$. Então pelo Teorema de Presentação de Quocientes, $\frac{\Pi}{d_n}$ tem como geradores os elementos a_1, b_1, a_2, b_2 e como relações $[a_1,b_1][a_2,b_2] = a_1^n = a_2^2 = a_1 b_1^{-1} = a_2 b_2^{-1} = (a_1 a_2)^2 = 1$ de onde obtemos:

$$\frac{\Pi}{d_n} =< a_1, a_2 : a_1^n = a_2^2 = 1 \text{ e } a_2 a_1 = a_1^{-1} a_2 >= D_n,$$

o grupo diedral de grau n.

Agora, se $\{1, a_1, ..., a_1^{n-1}, a_1 a_2, ..., a_1^{n-1} a_2\}$ é um sistema completo de representantes de Schreier de Π modulo d_n , com $K \in \{1, a_1, ..., a_1^{n-1}$, $a_1 a_2, ..., a_1^{n-1} a_2\}$ e $a_\nu \in \{a_1, b_1, a_2, b_2\}$ então d_n pode ter no máximo $8n$ geradores s_{K,a_ν}. Para determinarmos $\overline{U(a_1, b_1, a_2, b_2)}$, iremos utilizar as relações definidoras em $\frac{\Pi}{d_n}$.

Como $\overline{a_1^j a_1} = \overline{a_1^{j+1}} = a_1^{j+1}$ se $j+1 < n$ ou $j < n-1$, então $\overline{a_1^j a_1}$ e $a_1^j a_1$ determinam o mesmo elemento no grupo livre gerado pelos a_λ ($\overline{M a_\lambda} \approx M a_\lambda$) . Neste caso,

$s_{a_1^j,a_1} = 1$ e nos demais casos esta igualdade não ocorre.

Desta forma, temos que determinar os relatores derivados de palavras das formas:

$$a_1^j[a_1,b_1][a_2,b_2]a_1^{-j} \ e \ a_1^j a_2[a_1,b_1][a_2,b_2]a_2^{-1}a_1^{-j}.$$

Para isto, consideramos $U = a_1^j[a_1,b_1][a_2,b_2]a_1^{-j}$ e vamos agora determinar os elementos W_i, e a partir dos mesmos, usando a fórmula:

$$K_j = \begin{cases} \overline{W_j}, \text{ se } \epsilon_j = 1 \\ \overline{W_j a_{\nu_j}^{-1}}, \text{ se } \epsilon_j = -1 \end{cases}$$

obter os representantes K_i como se segue:

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = a_1$ ..... $K_2 = a_1$

. . .

$W_j = a_1^{j-1}$ ..... $K_j = a_1^{j-1}$

$W_{j+1} = a_1^j$ ..... $K_{j+1} = a_1^j$

$W_{j+2} = a_1^{j+1}$ ..... $K_{j+2} = \begin{cases} a_1^{j+1} \text{ se } j < n-1 \\ 1 \text{ se } j = n-1 \end{cases}$

$W_{j+3} = a_1^{j+1}b_1$ ..... $K_{j+3} = \begin{cases} a_1^{j+1} \text{ se } j < n-1 \\ 1 \text{ se } j = n-1 \end{cases}$

$W_{j+4} = a_1^{j+1}b_1a_1^{-1}$ ..... $K_{j+4} = a_1^j$

$W_{j+5} = a_1^j[a_1, b_1]$ ..... $K_{j+5} = a_1^j$

$W_{j+6} = a_1^j[a_1,b_1]a_2$ ..... $K_{j+6} = a_1^j a_2$

$W_{j+7} = a_1^j[a_1,b_1]a_2b_2$ ..... $K_{j+7} = a_1^j a_2$

$W_{j+8} = a_1^j[a_1,b_1]a_2b_2a_2^{-1}$ ..... $K_{j+8} = a_1^j$

$W_{j+8+1} = a_1^j[a_1,b_1][a_2,b_2]$ .....$K_{j+8+1} = a_1^{j-1}$

$W_{j+8+2} = a_1^j[a_1,b_1][a_2,b_2]a_1^{-1}$ .....$K_{j+8+2} = a_1^{j-2}$

. . .

$W_{j+8+j} = a_1^j[a_1,b_1][a_2,b_2]a_1^{-(j-1)}$ ..... $K_{j+8+j} = a_1^{-(j-1)}$

Com isto, estamos então em condições de determinar o relator $\tau(U)$ em função dos geradores definidores s_{K,a_ν} , ou seja:

$$\tau(U) = \begin{cases} s_{1,a_1} \cdot \cdot \cdot \cdot \cdot s_{a_1^{j-1},a_1} \cdot \\ s_{a_1^j,a_1} \cdot s_{*,b_1} \cdot s^{-1}_{*,a_1} \cdot s^{-1}_{a_1^j,b_1} \cdot \\ s_{a_1^j,a_2} \cdot s_{a_1^j a_2,b_2} \cdot s^{-1}_{a_1^j,a_2} \cdot s^{-1}_{a_1,b_2} \cdot \\ s^{-1}_{a_1^{j-1},a_1} \cdot \cdot \cdot \cdot \cdot s^{-1}_{1,a_1} \cdot \end{cases}$$

onde $* = a_1^{j+1}$ se $j < n-1$ ou $* = 1$ se $j = n-1$.

Tomamos agora $U = a_1^j a_2[a_1,b_1][a_2,b_2]a_2^{-1}a_1^{-j}$:

Vamos agora determinar os elementos W_i, e a partir dos mesmos, usando a fórmula:

$$K_j = \begin{cases} \overline{W_j}, \text{ se } \epsilon_j = 1 \\ \overline{W_j a_{\nu_j}^{-1}}, \text{ se } \epsilon_j = -1 \end{cases}$$

obter os representantes K_i como se segue:

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = a_1$ ..... $K_2 = a_1$

. . .

$W_j = a_1^{j-1}$ ..... $K_j = a_1^{j-1}$

$W_{j+1} = a_1^j$ ..... $K_{j+1} = a_1^j$

$W_{j+2} = a_1^j a_2$ ..... $K_{j+2} = a_1^j a_2$

$W_{j+3} = a_1^j a_2 a_1$ ..... $K_{j+3} = a_1^j a_2$

$W_{j+4} = a_1^j a_2 a_1, b_1$ ..... $K_{j+4} = a_1^{j-1} a_2$

$W_{j+5} = a_1^j a_2 a_1 b_1 a_1^{-1}$ ..... $K_{j+5} = a_1^j a_2$

$W_{j+6} = a_1^j a_2 [a_1, b_1]$ ..... $K_{j+6} = a_1^j a_2$

$W_{j+7} = a_1^j a_2 [a_1, b_1] a_2$ ..... $K_{j+7} = a_1^j$

$W_{j+8} = a_1^j a_2 [a_1, b_1] a_2 b_2$ .....$K_{j+8} = a_1^j$

$W_{j+9} = a_1^j a_2 [a_1, b_1] a_2 b_2 a_2^{-1}$ ..... $K_{j+9} = a_1^j a_2$

$W_{j+10} = a_1^j a_2 [a_1, b_1][a_2, b_2]$ .....$K_{j+10} = a_1^j a_2$

$W_{j+10+1} = a_1^j a_2 [a_1, b_1][a_2, b_2] a_2^{-1}$ ..... $K_{j+10+1} = a_1^j$

$$W_{j+10+2} = a_1^j a_2 [a_1, b_1][a_2, b_2] a_2^{-1} a_1 \quad \ldots\ldots\ldots\ldots \quad K_{j+10+2} = a_1^{j-1}$$

. . .

$$W_{j+10+j} = a_1^j a_2 [a_1, b_1][a_2, b_2] a_2^{-1} a_1^{-j} \quad \ldots\ldots\ldots\ldots \quad K_{j+10+j} = a_1$$

Com isto, estamos então em condições de determinar o relator $\tau(U)$ em função dos geradores definidores s_{K,a_ν} , ou seja:

$$\tau(U) = \left\{ \begin{array}{ccccccccccccccc} s_{1,a_1} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & s_{a_1^{j-1},a_1} & \cdot \\ s_{a_1^j,a_2} & \cdot & s_{a_1^j a_2,a_1} & \cdot & s_{a_1^{j-1} a_2,b_1} & \cdot & s^{-1}_{a_1^{j-1},a_1} & \cdot & s^{-1}_{a_1^j a_2,b_1} & \cdot \\ s_{a_1^j a_2,b_1} & \cdot & s_{a_1^j,b_2} & \cdot & s^{-1}_{a_1^j,a_2} & \cdot & s^{-1}_{a_1^j,b_2} & \cdot & s^{-1}_{a_1^j a_2,a_2} & \cdot \\ s^{-1}_{a_1^{j-1},a_1} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & s^{-1}_{1,a_1} & \cdot \end{array} \right.$$

Como no caso z_n temos $s_{a_1^{n-1},a_1} \approx 1$. Denotando:

$$a_i = s_{a_1^i,a_1}, \quad \alpha_i = s_{a_1^i a_2,a_1},$$

$$b_i = s_{a_1^i,b_1}, \quad \beta_i = s_{a_1^i a_2,b_1},$$

$$c_i = s_{a_1^i,a_2}, \quad \gamma_i = s_{a_1^i a_2,a_2},$$

$$d_i = s_{a_1^i,b_2}, \quad \delta_i = s_{a_1^i a_2,b_2},$$

Denotando então:

$$\Phi_j = b_{j+1} a_{j+1} c_j \delta_j c_j^{-1} d_j^{-1}$$

e

$$\Psi_j = c_j \alpha_j \gamma_j d_j c_j^{-1} d_j^{-1} \gamma_j^{-1}$$

onde j é tomado modulo n , temos como consequência que a presentação de d_n é dada por:

$d_n =< \{a_i\}, \{b_i\}, \{c_i\}, \{d_i\}, \{\alpha_i\}, \{\beta_i\}, \{\gamma_i\}, \{\delta_i\} : \Phi_i = 1, \Psi_i = 1, i \in \{0, ..., n-1\} >$.

Com isto, temos então o seguinte resultado:

Teorema 2 Seja $\Pi = \Pi_2 =< a_1, b_2, a_2, b_2 : [a_1,b_1][a_2, b_2] = 1 >$ o grupo fundamental da superfície compacta orientável de gênero 2 então para cada número inteiro $n \geq 2$,

$$\frac{\Pi}{d_n} \simeq D_n$$

onde:

$d_n =< \{a_i\}, \{b_i\}, \{c_i\}, \{d_i\}, \{\alpha_i\}, \{\beta_i\}, \{\gamma_i\}, \{\delta_i\} : \Phi_i = 1, \Psi_i = 1, i \in \{o, ..., n-1\} >$

Ou seja, Π é uma extensão de d_n por D_n.

3.1.3 Determinação dos Subgrupos $z_{m,n}$

O objetivo deste parágrafo é determinar para cada $n \geq 2$ um subgrupo normal $z_{m\times n}$ de $[8, 8]$ de modo que $[8, 8]$ seja uma extensão de $z_{m\times n}$ por $\mathbb{Z}_m \times \mathbb{Z}_n$. Isto permite a descrição de uma região fundamental correspondente a $m \cdot n$ cópias da região original, e também a descrição de conjuntos de sinais onde cada ponto de sinal corresponde ao centro de uma cópia da região fundamental de $[8, 8]$, generalizando de modo natural a teoria nos espaços euclidianos.

Vamos considerar agora os subgrupos $z_{m,n}$ de Π gerados por a_1^m, b_1^n, a_2, b_2 , pelo Teorema de Presentação do Quociente obtemos que $\frac{\Pi}{z_{m,n}}$ tem os mesmos geradores

que Π e relações $[a_1,b_1][a_2,b_2]=1, a_1^m=b_1^n=a_2=b_2=1$, mas $a_2=b_2=1$ implica que $[a_2,b_2]=1$, logo devemos ter $[a_1,b_1]=1$ ou seja $a_1b_1=b_1a_1$ e isto resulta na presentação:

$$\frac{\Pi}{z_{m,n}} =< a_1,b_1 : a_1^m=b_1^n=1 \text{ e } a_1b_1=b_1a_1 >= \mathbb{Z}_m \times \mathbb{Z}_n.$$

Temos que $\{a_1^i b_1^j : 0 \leq i < m, 0 \leq j < n\}$ é um sistema completo de representantes de Schreier de Π modulo $z_{m,n}$. Tomando agora $K \in \{a_1^i b_1^j : 0 \leq i < m, 0 \leq j < n\}$ e $a_\nu \in \{a_1,b_1,a_2,b_2\}$ vão existir no máximo $4mn$ geradores de $z_{m,n}$ na forma s_{K,a_ν}.

Na determinação dos elementos da forma $\overline{Ma_\lambda} \approx Ma_\lambda$, temos que $\overline{a_1^j b_1^k b_1} = \overline{a_1^j b_1^{k+1}} = a_1^j b_1^{k+1}$ se $k+1<n$ ou seja $s_{\overline{a_1^j b_1^k},b_1} \approx 1$ se $k<n-1$.

Fazemos $U = a_1^j b_1^k [a_1,b_1][a_2,b_2] b_1^{-k} a_1^{-j}$.

Vamos agora determinar os elementos W_i, e a partir dos mesmos, usando a fórmula:

$$K_j = \begin{cases} \overline{W_j}, \text{ se } \epsilon_j = 1 \\ \overline{W_j a_{\nu_j}^{-1}}, \text{ se } \epsilon_j = -1 \end{cases}$$

obter os representantes K_i como se segue:

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = a_1$ ..... $K_{2=} = a_1$

. . ..

$W_{j-1} = a_1^{j-2}$ ..... $K_{j-1} = a_1^{j-2}$

$W_j = a_1^{j-1}$ ..... $K_j = a_1^{j-1}$

$W_{j+1} = a_1^j$ ..... $K_{j+1} = a_1^j$

. . .

$W_{j+k-1} = a_1^j b_1^{k-2}$ ..... $K_{j+k-1} = a_1^j b_1^{k-2}$

$W_{j+k} = a_1^j b_1^{k-1}$ ..... $K_{j+k} = a_1^j b_1^{k-1}$

$W_{j+k+1} = a_1^j b_1^k$ ..... $K_{j+k+1} = a_1^j b_1^k$

$W_{j+k+2} = a_1^j b_1^k a_1$ ..... $K_{j+k+2} = a_1^j b_1^k$

$W_{j+k+3} = a_1^j b_1^k a_1 b_1$ ..... $K_{j+k+3} = a_1^j b_1^{k+1}$

$W_{j+k+4} = a_1^j b_1^k a_1 b_1 a_1^{-1}$ ..... $K_{j+k+4} = a_1^j b_1^k$

$W_{j+k+5} = a_1^j b_1^k [a_1, b_1]$ ..... $K_{j+k+5} = a_1^j b_1^k$

$W_{j+k+6} = a_1^j b_1^k [a_1, b_1] a_2$ ..... $K_{j+k+6} = a_1^j b_1^k$

$W_{j+k+7} = a_1^j b_1^k [a_1, b_1] a_2 b_2$ ..... $K_{j+k+7} = a_1^j b_1^k$

$W_{j+k+8} = a_1^j b_1^k [a_1, b_1] a_2 b_2 a_2^{-1}$ ..... $K_{j+k+8} = a_1^j b_1^k$

$W_{j+k+8+1} = a_1^j b_1^k [a_1, b_1][a_2, b_2]$ ..... $K_{j+k+8+1} = a_1^j b_1^{k-1}$

$W_{j+k+8+2} = a_1^j b_1^k [a_1, b_1][a_2, b_2] b_1^{-1}$ ..... $K_{j+k+8+2} = a_1^j b_1^{k-2}$

. . .

$W_{j+k+8+k} = a_1^j b_1^k [a_1, b_1][a_2, b_2] b_1^{-(k-1)}$ ..... $K_{j+k+8+k} = a_1^j$

$W_{j+k+8+k+1} = a_1^j b_1^k [a_1, b_1][a_2, b_2] b_1^{-k}$ ..... $K_{j+k+8+k+1} = a_1^{j-1}$

. . .

$W_{j+k+8+k+j} = a_1^j b_1^k [a_1, b_1][a_2, b_2] b_1^{-k} a_1^{-(j-1)}$ ..... $K_{j+k+8+k+j} = 1$

Com isto, estamos então em condições de determinar o relator $\tau(U)$ em função dos geradores definidores s_{K,a_ν} , ou seja:

$$\tau(U) = \left\{ \begin{array}{ccccccc} s_{1,a_1} & \cdot & s_{a_1 a_1} & \cdots\cdots & s_{a_1^{j-2},a_1,} & \cdot & s_{a_1^{j-1},a_1,} \\ s_{a_1^j b_1,} & \cdot & s_{a_1^j b_1,b_1} & \cdots\cdots & s_{a_1^j b_1^{k-2},b_1} & \cdot & s_{a_1^j b_1^{k-1},b_1} \\ s_{a_1^j b_1^k,a_1} & \cdot & s_{a_1^{j+1} b_1^k,b_1} & \cdot & s^{-1}_{a_1^j b_1^{k+1},a_1} & \cdot & s_{a_1^j b_1^k,b_1} \\ s_{a_1^j b_1^k,a_2} & \cdot & s_{a_1^j b_1^k,b_2} & \cdot & s^{-1}_{a_1^j b_1^k,a_2} & \cdot & s^{-1}_{a_1^j b_1^k,b_2} \\ s^{-1}_{a_1^j b_1^{k-1},b_1} & \cdot & s^{-1}_{a_1^j b_1^{k-2},b_1} & \cdot & \cdots\cdots & \cdot & s^{-1}_{a_1^j,b_1} \\ s_{a_1^{j-1},a_1} & \cdot & \cdots\cdots & \cdot & s^{-1}_{a_1,a_1} & \cdot & s^{-1}_{1,a_1} \end{array} \right.$$

Denotando então $a_{j,k} = s_{a_1^j b_1^k,a_1}$, $b_{j,k} = s_{a_1^j b_1^k,b_1}$, $c_{j,k} = s_{a_1^j b_1^k,a_2}$, $d_{j,k} = s_{a_1^j b_1^k,b_2}$ e também $R_{j,k} = a_{j,k} b_{j,k} a^{-1}_{j,k+1} b_{j,k} [c_{j,k}, d_{j,k}]$ temos que $z_{m,n}$ tem a presentação:

$$z_{m,n} =< a_{j,k}, b_{j,k}, c_{j,k}, d_{j,k} : R_{j,k} = 1; 0 \leq j \leq m-1 \text{ e } 0 \leq k \leq n-1 > .$$

Como consequência obtemos o seguinte resultado:

Teorema 3 Seja $\Pi = \Pi_2 =< a_1, b_2, a_2, b_2 : [a_1, b_1][a_2, b_2] = 1 >$ o grupo fundamental da superfície compacta orientável de gênero 2 então:

$$\frac{\Pi}{z_{m,n}} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$$

onde

$$z_{m,n} =< a_{j,k}, b_{j,k}, c_{j,k}, d_{j,k} : R_{j,k} = 1;\ 0 \leq j \leq m-1 \ e\ 0 \leq k \leq n-1 >,$$

ou seja, Π é uma extensão de $z_{m,n}$ por $\mathbb{Z}_m \times \mathbb{Z}_n$.

3.2 O Caso não Auto-Dual - Os Grupos [p,3]

No caso auto-dual, apesar de alguma restrição sobre p , obtemos resultados sobre $\{p,3\}$, que se apresenta como um caso dos mais adequado para implementações.

Consideremos o grupo

$$[p,3] =< r_1, r_2, r_3 : r_1^2 = r_2^2 = r_3^2 = (r_1 r_2)^p = (r_2 r_3)^3 = (r_1 r_3)^2 = 1 > .$$

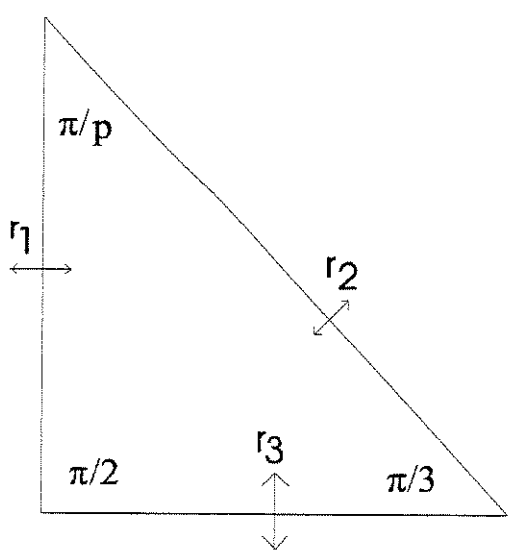

Figura 3.1 - As Reflexões Geradoras

Então $[p,3]$ é o grupo completo de simetrias da tesselação $\{p,3\}$, onde $r_1(z) = -\overline{z}$. Vamos denotar $P = P_{p,3} = [p,3] \cap PSL(2,\mathbb{R})$ ou seja P é a parte fuchsiana de $[p,3]$, consistindo de todos os elementos conformes que são representados por um número par

de reflexões. Como $\{1, r_1\}$ é um sistema completo de representantes de Schreier de $[p, 3]$ modulo P, estamos em condições de aplicar o algoritmo de Reidemeister-Schreier:

Considerando $K \in \{1, r_1\}$ e $a_\nu \in \{r_1, r_2, r_3\}$ temos que os geradores s_{K,a_ν} de P são tomados no conjunto:$\{s_{1,r_1}, s_{1,r_2}, s_{1,r_3}, s_{r_1,r_1}, s_{r_2,r_1}, s_{r_1,r_3}\}$. Como $1 \cdot r_1$ e $\overline{1 \cdot r_1}$ determinam o mesmo elemento no grupo livre gerado pelos a_ν ($1 \cdot r_1 \approx \overline{1 \cdot r_1}$) então o símbolo gerador s_{1,r_1} é um relator.Desse modo, tanto o símbolo como a identidade $s_{1,r_1} = 1$ podem ser eliminados da presentação . Os outros relatores são obtidos na forma $\tau(KR_\mu K^{-1}) = 1$ onde os R_μ são as relações definidoras do grupos $[p, 3]$ e $K \in \{1, r_1\}$ o sistema de Schreier de $[p, 3]$ modulo P.

Vamos considerar agora cada relator individualmente:

(i) $\tau(1 \cdot r_1^2 \cdot 1^{-1}) = \tau(r_1^2) = s_{1,r_1} \cdot s_{r_1,r_1}$

$U = r_1 r_2$ e $W_1 = 1 \quad K_1 = \overline{1} = 1$

$W_2 = r_1 \quad K_2 = \overline{r_2} = r_2$

de onde $\tau(r_1 r_2) = s_{1,r_1} \cdot s_{r_1,r_1}$. Como s_{1,r_1} é um relator, temos que s_{r_1,r_1} também é um relator , ou seja, podemos eliminar o par s_{r_1,r_1} nos geradores e $s_{r_1,r_1} = 1$ nos relatores definidores.

(ii) $\tau(r_1 \cdot r_1^2 \cdot r_1^{-1}) = (s_{1,r_1} \cdot s_{r_1,r_1})^2$

$U = r_1 r_1 r_1 r_1$

$W_1 = 1$ ..... $K_1 = 1 = 1$

$W_2 = r_1$ ..... $K_2 = \overline{r_1} = r_1$

$W_3 = r_1^2$ ..... $K_3 = \overline{r_1^2} = 1$

$W_4 = r_1^3$ ..... $K_4 = \overline{r_1^3 r_1^{-1}} = 1$

de onde $\tau(r_1 r_1^2 r_1) = s_{1,r_1} \cdot s_{r_1,r_1} \cdot s_{1,r_1} \cdot s_{r_1,r_1}$ que é o mesmo que no item (i)

(iii) $\tau(1 \cdot r_2^2 \cdot 1^{-1}) = \tau(r_2^2) = s_{1,r_2} \cdot s_{r_1,r_2}$

$U = r_2 r_2$

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = r_2$ ..... $K_2 = r_1$

(iv) $\tau(r_1 \cdot r_2^2 \cdot r_1^{-1}) = s_{r_1,r_2} \cdot s_{1,r_2}$

$U = r_1 r_2 r_2 r_1^{-1}$

$W_1 = 1$ ..... $K_1 = \overline{1} = 1$

$W_2 = r_1$ ..... $K_1 = \overline{r_1} = r_1$

$W_3 = r_1 r_2$ ..... $K_1 = \overline{r_1 r_2} = 1$

$W_1 = r_1 r_2^2$ ..... $K_1 = \overline{r_1 r_2^2 r_1^{-1}} = 1$

$\tau(U) = s_{r_1,r_2} \cdot s_{r_1,r_2} \cdot s_{1,r_2} \cdot s_{1,r_1}^{-1}$

De (iii) e de (iv) temos que s_{1,r_2} e s_{r_1,r_2}^{-1} definem o mesmo elemento. Com

isto, temos a relação definidora:

$$s_{1,r_2} = s_{r_1,r_2}^{-1}.$$

(v) $\tau(1 \cdot r_3^2 \cdot 1^{-1}) = s_{1,r_3} \cdot s_{r_1,r_3}$ similar ao caso (iii)

$(vi)\tau(r_1 \cdot r_2^2 \cdot r_1^{-1}) = s_{r_1,r_3} \cdot s_{1,r_3}$ similar ao caso (iv)

Como em (iii) e (iv), obtemos a relação definidora:

$$s_{1,r_3} = s_{r_1,r_3}^{-1}$$

(vii) $\tau(1 \cdot (r_1r_2)^p \cdot 1^{-1}) = \tau((r_1r_2)^p) = \tau(r_1r_2)^p = (s_{1,r_1} \cdot s_{r_1,r_2})^p$

$U = r_1r_2$

$W_1 = 1$ ..... $K_1 = \overline{1} = 1$

$W_2 = r_1$ ..... $K_2 = \overline{r_1} = r_1$

$\tau(r_1r_2) = (s_{1,r_1} \cdot s_{r_1,r_2})$

Em (vii) usamos o fato que se U define um elemento do subgrupo, então $\tau(U^n) = \tau(U)^n$. Este fato será usado nos ítens que se seguem.

Como temos a relação $s_{1,r_1} = 1$ resulta que (vii) fornece para a presentação a relação:

$$s_{r_1,r_2}^p = 1.$$

$(viii)$ $\tau(r_1 \cdot (r_1r_2)^p \cdot (r_1)^{-1}) = \tau((r_1 \cdot (r_1r_2) \cdot r_1^{-1})^p) = \tau(r_1 \cdot r_1r_2 \cdot r_1^{-1})^p = (s_{r_1,r_2} \cdot s_{1,r_2})^p$

$U = r_1 r_1 r_2 r_1^{-1}$

$W_1 = 1$ ..... $K_1 = \overline{1} = 1$

$W_2 = r_1$ ..... $K_2 = \overline{r_1} = r_1$

$W_3 = r_1 r_1$ ..... $K_3 = \overline{r_1 r_1} = 1$

$W_4 = r_1 r_1 r_2$ ..... $K_4 = \overline{r_1 r_1 r_2 r_1^{-1}} = 1$

de onde $\tau(U) = s_{1,r_1} \cdot s_{r_1,r_1} \cdot s_{1,r_2} \cdot s_{1,r_1}^{-1}$. Com isto, obtemos a relação definidora:

$$s_{1,r_1} = 1.$$

$(ix)\ \tau(1 \cdot (r_2 r_3)^3 \cdot 1^{-1}) = \tau(r_2 r_3)^3 = (s_{1,r_2} \cdot s_{r_1,r_3})^3$

$U = r_2 r_3$

$W_1 = 1$ ..... $K_1 = \overline{1} = 1$

$W_2 = r_2$ ..... $K_2 = \overline{r_2} = r_2$

Dessa forma, $\tau(U) = s_{1,r_2} \cdot s_{r_1,r_3}$. Arelação definidora passa a ser então:

$$(s_{1,r_2} \cdot s_{r_1,r_3})^3 = 1$$

$(x)\ \tau(r_1 \cdot (r_2 r_3)^3 \cdot r_1^{-1}) = \tau(r_1 \cdot r_2 \cdot r_3 \cdot r_1^{-1})^3 = (s_{r_1,r_2} \cdot s_{1,r_3})^3$

$U = r_1 r_2 r_3 r_1^{-1}$

$W_1 = 1$ ..... $K_1 = \overline{1} = 1$

$W_2 = r_1$ ..... $K_2 = \overline{r_1} = r_1$

$W_3 = r_1 r_2$ ..... $K_3 = \overline{r_1 r_2} = 1$

$W_4 = r_1 r_2 r_3$ ..... $K_4 = \overline{r_1 r_2 r_3 r_1^{-1}} = 1$

Desse modo, temos $\tau(U) = s_{1,r_1} \cdot s_{r_1,r_2} \cdot s_{1,r_3} \cdot s_{1,r_1}^{-1}$ de onde a relação definidora fica sendo:

$$(s_{r_1,r_2} \cdot s_{1,r_3})^3 = 1.$$

(xi) $\tau(1 \cdot (r_1 r_3)^2 \cdot 1^{-1}) = \tau(r_1 r_3)^2 = (s_{r_1,r_3})^2$

$U = r_1 r_3$

$W_1 = 1$ ..... $K_1 = \overline{1} = 1$

$W_2 = r_1$ ..... $K_2 = \overline{r_1} = r_1$

Consequentemente $\tau(U) = s_{1,r_1} \cdot s_{r_1,r_3}$ e como s_{1,r_1} é relator temos que a relação definidora é:

$$s_{1,r_3}^2 = 1.$$

(xii) $\tau(r_1 \cdot (r_1 r_3)^2 \cdot r_1^{-1}) = \tau(r_1 \cdot r_1 \cdot r_3 \cdot r_1^{-1})^2 = (s_{1,r_3})^2$

$U = r_1 r_1 r_3 r_1^{-1}$

$W_1 = 1$ ..... $K_1 = \overline{1} = 1$

$W_2 = r_1$ ..... $K_2 = \overline{r_1} = r_1$

$W_3 = r_1 r_1$ ..... $K_3 = \overline{r_1 r_1} = 1$

$W_4 = r_1 r_1 r_3$ ..... $K_4 = \overline{r_1 r_1 r_3 r_1^{-1}} = 1$

Assim, $\tau(U) = s_{1,r_1} \cdot s_{r_1,r_1} \cdot s_{1,r_3} \cdot s_{1,r_1}^{-1}$ Eliminando os relatores obtemos a relação definidora:

$$(s_{1,r_3})^2 = 1.$$

Agora, podemos proceder às simplificações:

De (i) e de (ii) eliminamos os geradores s_{1,r_1} e s_{r_1,r_1}.

De (iii) e de (iv) eliminamos o gerador s_{1,r_2} já que $s_{1,r_2} = s_{r_1,r_2}^{-1}$.

De (v) e de (vi) eliminamos o gerador s_{1,r_3} já que $s_{1,r_3} = s_{r_1,r_3}^{-1}$.

Obtemos então a presentação:

$$P = < s_{r_1,r_2}, s_{r_{r_1},r_3} : s_{r_1,r_2}^p = s_{r_1,r_3}^2 = (s_{r_1,r_2}^{-1} \cdot s_{r_1,r_3})^3 = 1 > .$$

Denotando s_{r_1,r_2} por p_2 e $s_{r_{r_1},r_3}$ por p_3 reescrevemos:

$$P = < p_2, p_3 : p_2^p = p_3^2 = (p_2^{-1} p_3)^3 = 1 >$$

Com a nova transformação $p_1 = p_2^{-1}p_3$, então a presentação fica sendo:

$$P =< p_1, p_2 : p_1^3 = p_2^p = (p_1p_2)^2 = 1 > .$$

Como $(p_1p_2)^2 = 1$ se, e somente se, $(p_2p_1)^2 = 1$, podemos reescrever a presentação como:

$$P =< p_1, p_2 : p_1^p = p_2^3 = (p_1p_2)^2 = 1 > .$$

Com isto, chegamos ao seguinte resultado:

Teorema 4 Dado o número natural $p > 6$ (ou seja $(p-2)(3-2) > 4$) temos que:

$$\frac{[p,3]}{P} \simeq \mathbb{Z}_2,$$

onde $P =< p_1, p_2 : p_1^3 = p_2^p = (p_1p_2)^2 = 1 >$ e $\mathbb{Z}_2 =< r_1 >$ .Consequentemente, $[p,3]$ é uma extensão de P por $\mathbb{Z}_2$.

Nosso objetivo agora é determinar um subgrupo normal N de P tal que $\frac{P}{N} \simeq \mathbb{Z}_3$ .Nesta direção, pelo Teorema de Presentação do Quociente (Teorema 2 do Capítulo 1) se considerarmos um gerador da forma $p_2p_1^{-\alpha}$ para N tal que α satisfaça a condição $(p_1p_2)^2 = 1$, além disso, se considerarmos $p_2 = p_1^{\alpha}$, devemos ter que $(p_1p_2)^2 = (p_1^{\alpha+1})^2 = p_1^{2\alpha+2} = 1$ Além disso, $p_2^p = p_1^{\alpha p} = 1$ implica que

$$\begin{cases} 3|2\alpha+2 & (*) \\ 3|\alpha p & (**) \end{cases}.$$

Mas a congruência $(*)$ tem solução geral da forma $\alpha = 2 + 3n \equiv 2(\mathrm{mod}\, 3)$. Assim, $3 \nmid \alpha$ e como 3 é primo, devemos ter $3|p$ e a construção é possível para todo p tal que $3|p$ e $\alpha \equiv 3 \,\mathrm{mod}\, 3$. Sob estas hipoteses:

$$\frac{P}{N} =< p_1 : p_1^3 = 1 >$$

Consequentemente, temos que $\{1, p_1, p_1^2\}$ é um sistema completo de representantes de Schreier para P modulo N.

Seja $W(p_1, p_2) = \prod_{i=1}^{n} p_1^{u_i} p_2^{v_i}$ uma palavra em p_1 e p_2 que representa um elemento de P. Este elemento tomado modulo N conduz a :

$$W(p_1, p_2) = \prod_{i=1}^{n} p_1^{u_i} p_2^{v_i} = p^{\sum u_i + \sum v_i} = p_1^{\lambda},$$

onde $\lambda = (\sum u_i + \alpha \sum v_i) \,\mathrm{mod}\, 3 = (\sigma_1(W) + \alpha\sigma_2(W)) \,\mathrm{mod}\, 3$.

Agora, para fazer a presentação de N tomamos:

$$K \in \{1, p_1, p_1^2\} \qquad a_\nu \in \{p_1, p_2\},$$

então os geradores de N estão entre os elementos do conjunto

$$\{\, s_{1,p_1}, s_{p_1,p_1}, s_{p_1^2,p_1}, s_{1,p_2}, s_{p_1,p_2}, s_{p_1^2,p_1} \}.$$

Como $\overline{p_1 \cdot 1} \approx p_1$ e $\overline{p_1 \cdot p_1} \approx \overline{p_1^2} \approx p_1^2$ obtemos os relatores triviais:

$$s_{1,p_1} = 1 \qquad s_{p_1,p_1} = 1.$$

Com isto, temos também a lista de relatores definidores $\tau(KR_\mu K^{-1}) = 1$ onde $\tau(KR_\mu K^{-1})$ é especificado para cada um dos nove casos a seguir,:

(i) $\tau(1 \cdot p_1^3 \cdot 1^{-1})$

(ii) $\tau(p_1 \cdot p_1^3 \cdot p_1^{-1})$

(iii) $\tau(p_1^2 \cdot p_1^3 \cdot p_1^{-2})$

(iv) $\tau(1 \cdot p_2^p \cdot 1^{-1})$

(v) $\tau(p_1 \cdot p_2^p \cdot p_1^{-1})$

(vi) $\tau(p_1^2 \cdot p_2^p \cdot p_1^{-2})$

(vii) $\tau(1 \cdot (p_1 \cdot p_2)^2 \cdot 1^{-1})$

$(viii)$ $\tau(p_1 \cdot (p_1 \cdot p_2)^2 \cdot p_1^{-1})$

(ix) $\tau(p_1^2 \cdot (p_1 \cdot p_2)^2 \cdot p_1^{-2})$

Considerando caso a caso, temos:

(i) $\tau(1 \cdot p_1^3 \cdot 1^{-1}) = \tau(p_1^3) = s_{p_1^2,p_1}$

$U = p_1 p_1 p_1$

$W_1 = 1$ ..... $K_1 = 1$

$W_1 = p_1$ ..... $K_2 = p_1$

$W_1 = p_1^2$ ..... $K_3 = p_1^2$

de onde $\tau(U) = s_{1,p_1} \cdot s_{p_1,p_1} \cdot s_{p_1^2,p_1} = s_{p_1^2,p_1}$.Logo o o relator será dado por

$$s_{p_1^2,p_1} = 1.$$

Similarmente, temos que:

(ii) $\tau(p_1 \cdot p_1^3 \cdot p_1^{-1}) = s_{p_1^2,p_1}$

(iii) $\tau(p_1^2 \cdot p_1^3 \cdot p_1^{-2}) = s_{p_1^2,p_1}$

(iv) $\tau(1 \cdot p_2^p \cdot 1^{-1})$

então, $U = \underbrace{p_2 \cdot \cdots \cdot p_2}_{p\ vezes}$, Consequentemente,

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = p_2$ ..... $K_2 = p_1^2$

$W_3 = p_2^2$ ..... $K_3 = p_1$

$W_4 = p_2^3$ ..... $K_4 = 1$

$W_5 = p_2^4$ ..... $K_5 = p_1^2$

$W_6 = p_2^5$ ..... $K_6 = p_1$

. . . . . .

$W_{p-2} = p_2^{p-3}$ ..... $K_{p-2} = 1$

$W_{p-1} = p_2^{p-2}$ ..... $K_{p-1} = p_1^2$

$W_p = p_2^{p-1}$ ..... $K_p = p_1$

Na determinação dos K_j as congruências são usadas diretamente , por exemplo, $K_{p-1} = \overline{p_2^{p-2}} = \overline{p_1^{\alpha(p-2)}} = p_1^2$ pois $p \equiv 0 \bmod 3$, então $p-2 \equiv -2 \equiv 1 \bmod 3$. Como $\alpha \equiv 2 \bmod 3$, $\alpha(p-2) \equiv 2 \cdot 1 \equiv 2 \bmod 3$, obtemos então:$\tau(U) = (s_1, p_2 \cdot s_{p_1^2,p_2} \cdot s_{p_1,p_2})^{\frac{p}{3}}$.

O relator definidor é então

$$(s_1, p_2 \cdot s_{p_1^2, p_2} \cdot s_{p_1, p_2})^{\frac{p}{3}} = 1.$$

(v) $\tau(p_1 \cdot p_2^p \cdot p_1^{-1})$

Então, $U = p_1 \cdot \underbrace{p_2 \cdots p_2}_{p \text{ vezes}} \cdot p_1^{-1}$. Consequentemente,

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = p_1$ ..... $K_2 = p_1$

$W_3 = p_1 p_2$ ..... $K_3 = 1$

$W_4 = p_1 p_2^2$ ..... $K_4 = p_1^2$

$W_5 = p_1 p_2^3$ ..... $K_5 = p_1$

$W_6 = p_1 p_2^4$ ..... $K_6 = 1$

$W_7 = p_1 p_2^5$ ..... $K_7 = p_1^2$

$W_8 = p_1 p_2^6$ ..... $K_8 = p_1$

$W_9 = p_1 p_2^7$ ..... $K_9 = 1$

$W_{10} = p_1 p_2^8$ ..... $K_{10} = p_1^2$

$W_{11} = p_1 p_2^9$ ..... $K_{11} = p_1$

. . . . . .

$W_{p-1} = p_1 p_2^{p-3}$ ..... $K_{p-1} = pl1$

$W_p = p_1 p_2^{p-2}$ ..... $K_p = 1$

$W_{p+1} = p_1 p_2^{p-1}$ ..... $K_{p+1} = p_1^2$

$W_{p+2} = p_1 p_2^p$ ..... $K_{p+2} = \overline{p_1 p_2^p p_1^{-1}} = \overline{p_2^p} = 1$

logo $\tau(U) = (s_{p_1,p_2} \cdot s_{1,p_2} \cdot s_{p_1^2,p_2})^{\frac{p}{3}}$. O relator definidor é então dado por:

$$(s_{p_1,p_2} \cdot s_{1,p_2} \cdot s_{p_1^2,p_2})^{\frac{p}{3}} = 1.$$

(vi) $\tau(p_1^2 \cdot p_2^p \cdot p_1^{-2})$

Então, $U = p_1 \cdot p_1 \cdot \underbrace{p_2 \cdots p_2}_{p \text{ vezes}} \cdot p_1^{-1} \cdot p_1^{-1}$. Consequentemente,

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = p_1$ ..... $K_2 = p_1$

$W_3 = p_1^2$ ..... $K_3 = p_1^2$

$W_4 = p_1^2 p_2$ ..... $K_4 = p_1$

$W_5 = p_1^2 p_2^2$ ..... $K_5 = 1$

$W_6 = p_1^2 p_2^3$ ..... $K_6 = p_1^2$

$W_7 = p_1^2 p_2^4$ ..... $K_7 = p_1$

$W_8 = p_1^2 p_2^5$ ..... $K_8 = 1$

$W_9 = p_1^2 p_2^6$ ..... $K_9 = p_1^2$

$W_{10} = p_1^2 p_2^7$ ..... $K_{10} = p_1$

$W_{11} = p_1^2 p_2^8$ ..... $K_{11} = 1$

. . . . . .

$W_p = p_1^2 p_2^{p-3}$ ..... $K_p = p_1^2$

$W_{p+1} = p_1^2 p_2^{p-2}$ ..... $K_{p+1} = p_1$

$W_{p+2} = p_1^2 p_2^{p-1}$ ..... $K_{p+2} = 1$

$W_{p+3} = p_1^2 p_2^p$ ..... $K_{p+3} = p_1$

$W_{p+4} = p_1^2 p_2^p p_1^{-1}$ ..... $K_{p+4} = 1$

Portanto, $\tau(U) = (s_{p_1^2,p_2} \cdot s_{p_1,p_2} \cdot s_{1,p_2})^{\frac{p}{3}}$. O relator é então dado por

$$(s_{p_1^2,p_2} \cdot s_{p_1,p_2} \cdot s_{1,p_2})^{\frac{p}{3}} = 1.$$

(vii) $\tau(1 \cdot (p_1 \cdot p_2)^2 \cdot 1^{-1})$

Então, $U = p_1 p_2 p_1 p_2$. Consequentemente,

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = p_1$ ..... $K_2 = p_1$

$W_3 = p_1 p_2$ ..... $K_3 = 1$

$W_4 = p_1 p_2 p_1$ ..... $K_4 = p_1$

Logo, $\tau(U) = s_{1,p_1} \cdot s_{p_1,p_2} \cdot s_{1,p_1} \cdot s_{p_1,p_2} = s_{p_1,p_2}^2$. O relator definidor é então

$$s_{p_1,p_2}^2 = 1.$$

$(viii)$ $\tau(p_1 \cdot (p_1 \cdot p_2)^2 \cdot p_1^{-1})$

Então, $U = p_1 p_1 p_2 p_1 p_2 p_1^{-1}$. Consequentemente,

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = p_1$ ..... $K_2 = p_1$

$W_3 = p_1^2$ ..... $K_3 = p_1^2$

$W_4 = p_1^2 p_2$ ..... $K_4 = p_1$

$W_5 = p_1^2 p_2 p_1$ ..... $K_5 = p_1^2$

$W_6 = p_1^2 p_2 p_1 p_2$ ..... $K_6 = \overline{p_1^2 p_2 p_1 p_2 p_1^{-1}} = 1$

Portanto, $\tau(U) = s^2_{p_1^2, p_2}$. O relator definidor é então dado por

$$s^2_{p_1^2, p_2} = 1.$$

(ix) $\tau(p_1^2 \cdot (p_1 \cdot p_2)^2 \cdot p_1^{-2})$

Então, $U = p_1 p_1 p_1 p_2 p_1 p_2 p_1^{-1} p_1^{-1}$. Consequentemente,

$W_1 = 1$ ..... $K_1 = 1$

$W_2 = p_1$ ..... $K_2 = p_1$

$W_3 = p_1^2$ ..... $K_3 = p_1^2$

$W_4 = p_1^3$ ..... $K_4 = 1$

$W_5 = p_1^3 p_2$ ..... $K_5 = p_1^2$

$W_6 = p_1^3 p_2 p_1$ ..... $K_6 =$

$W_7 = p_1^3 p_2 p_1 p_2$ ..... $K_7 = \overline{p_1^3 p_2 p_1 p_2 p_1^{-1}} = p_1$

$W_8 = p_1^3 p_2 p_1 p_2 p_1^{-1}$ ..... $K_8 = \overline{p_1^3 p_2 p_1 p_2 p_1^{-2}} = 1$

Logo $\tau(U) = s_{1,p_2}^2$. O relator definidor é então

$$s_{1,p_2}^2 = 1.$$

Denotando $s_{p_1^j,p_2}$ por b_{j+1}, obtemos as relações:

$b_1^2 = b_2^2 = b_3^2 = 1$ e $(b_1 b_2 b_3)^{\frac{p}{3}} = (b_2 b_1 b_3)^{\frac{p}{3}} = (b_3 b_2 b_1)^{\frac{p}{3}} = 1$. Mas como $(b_3 b_2 b_1) = (b_1 b_2 b_3)^{-1}$ finalmente :

Teorema 5 Dado um número natural p tal que $p > 6$ e $3|p$, então obtemos as extensões de grupos:

$$N \simeq \frac{P}{\mathbb{Z}_3} \text{ e } \frac{[p,3]}{P} = \mathbb{Z}_2$$

onde P é o grupo definido no Teorema 4 e N é dado por

$$N = < b_1, b_2, b_3 : b_1^2 = b_2^2 = b_3^2 = (b_1 b_2 b_3)^{\frac{p}{3}} = (b_2 b_1 b_3)^{\frac{p}{3}} = 1 > .$$

4

Partições Geométricamente Uniformes Hiperbólicas

O conceito de partição geométricamente uniforme foi proposto por Forney, [09], no contexto de conjuntos de sinais euclidianos. Apesar da maior complexidade dos grupos de isometrias hiperbólicos quando comparados com os euclidianos, a teoria de partições geométricamente uniformes se estende a estes, como veremos neste capítulo. Todavia, devemos levar em consideração que no caso euclidiano as regiões fundamentais das tesselações tem sempre um grupo gerador abeliano (de ordem 4), mesmo que o grupo de simetrias não seja abeliano , enquanto que no caso hiperbólico os grupos mais gerais tem que ser considerados. O objetivo deste capítulo é estender a teoria de modo a permitir que conjuntos de sinais casados com grupos, como aqueles descritos no Capítulo 3, possam ser decompostos em partições geométricamente uniformes.

4.1 Partições Geométricamente Uniformes

Seja S um conjunto de sinais geométricamente uniforme, digamos $S = \{u(s_0) : u \in U(S)\}$ para algum s_0 fixo em S. Seja U' um subgrupo normal de $U(S)$. Iremos denotar por $S' = \{u(s_0) : u \in U'\}$ a órbita de U' por S' . Se $U = U' \cup U'a \cup U'b \cup ....$ é a decomposição de U em classes laterais de U', então temos associada uma partição de S

$$S = U's_0 \cup U'as_0 \cup U'bs_0.... \ .$$

Esta partição é denotada por S/S'.

Definição 1. Chamamos de PARTIÇÃO GEOMÉTRICAMENTE UNIFORME de um conjunto de sinais S geométricamente uniforme com grupo gerador $U(S)$ a qualquer partição S/S' induzida por um subgrupo normal U' de $U(S)$.

O conceito de partição geométricamente uniforme é importante tendo em vista o seguinte resultado fundamental:

Teorema 1 [09]Se S/S' é uma partição geométricamente uniforme, então os elementos de S/S' são geométricamente uniformes, mutuamente congruentes e tem U' como grupo gerador comum.

Demonstração. Denotando $\mathcal{A} = U(S)/U'$, então se $a \in \mathcal{A}$; $a = U'u_a = u_aU'$ para algum $u_a \in U(S)$. Denotando por $S'(a)$ o elemento correspondente da partição S/S' temos que:

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

Portanto, $S'(a) \simeq S'$ e para todo $a \in A$, os $S'(a)$ são todos congruentes .

Por outro lado, $S'(a) = U' u_a(s_0) = \bigcup_{u \in U'} u[u_a(s_0)]$ é a órbita de $u_a(s_0)$ por U'. Logo, todos os $S'(a)$ são geométricamente uniformes com grupo gerador comum U'. ■

A partir do Teorema 1 tem sentido utilizar a notação $U(S')$ para U'.

Exemplo 1 As partições de Ungerboeck [35] são partições binárias geométricamente uniformes euclidianas associadas a conjuntos de sinais $MPSK$ com M da forma 2^k e subgrupos (necessáriamente normais) da forma $2^j PSK$ determinando uma sequência de partições. Os polígonos S associados às tesselações hiperbólicas (p-ágonos regulares) tem D_p como grupo de simetrias. Do mesmo modo, são constelações geradas por $pPSK$ $(U(S) = pPSK \leq D_p)$.

Observação. O Teorema 1 generaliza de modo natural a construção de Ungerboeck, por aplicação repetida em uma sequência

$$...U(S'') \lhd U(S') \lhd U(S).$$

Isto conduz naturalmente a uma sequência de partições geométricamente uniformes

$$S/S'/S''/...,$$

onde em cada nível os conjuntos das partições são congruentes e com um grupo gerador comum.

Exemplo 2 No caso euclidiano, se Λ é um reticulado e Λ' é um subreticulado de Λ de índice finito , então qualquer conjunto de sinais $S = \Lambda + a$ é particionado em $|\Lambda/\Lambda'|$ subconjuntos de sinais geométricamente uniformes $\Lambda' + a + v$ com $v \in [\Lambda/\Lambda']$ para algum conjunto completo de representantes $[\Lambda/\Lambda']$ de Λ modulo Λ' .

No caso hiperbólico, temos alguns pontos a considerar: Como a tesselação dual é gerada pelas translações, então a condição equivalente a $T(\Lambda) = \Lambda$ é exatamente o fato de a tesselação ser auto-dual o que equivale a ser do tipo $\{p, p\}$. Em geral, o grupo gerado pelas translações pode ter elementos de ordem finita distintos do elemento neutro. No caso auto-dual, como o grupo Π_n tem uma única relação $(\prod[a_i, b_i] = 1)$, pelo Teorema 4 do Capítulo 1, Π_n só tem o elemento neutro de ordem finita.

4.2 Rotulamentos Isométricos

Definição 2. Seja S/S' uma partição geométricamente uniforme, dizemos que um grupo $\mathcal{A}$ é um GRUPO DE RÓTULOS para S/S' se existe um isomorfismo $m : \mathcal{A} \to \frac{U(S)}{U(S')}$, m é chamado de ISOMORFISMO DE ROTULAMENTO. A aplicação (bijetora) $m : \mathcal{A} \to \frac{S}{S'}$ definida pela composição do isomorfismo de rotulamento com a bijeção $\frac{U(S)}{U(S')} \to \frac{S}{S'}$ é chamada de ROTULAMENTO ISOMÉTRICO dos subconjuntos de S pertencentes à partição S/S'.

Podemos visualizar a Definição 2 pelo diagrama:

$$\begin{array}{ccccc} \mathcal{A} & \longrightarrow & \dfrac{U(S)}{U(S')} & \longrightarrow & \dfrac{S}{S'} \\ a & \longmapsto & u_a U' & \longmapsto & m(a) = u_a(S') = \{u_a u(s_0) : u \in U'\}. \end{array}$$

O fato de m ser uma função bem definida é consequência de que se $u_a U' = vU'$, então $u_a' v^{-1} \in U' = U(S')$. Logo, $u_a v^{-1}(S') = S'$, portanto $u_a(S') = v(S')$.

As seguintes propriedades são imediatas:

(i)$m(e_A) = S'$.

(ii)$\left|\dfrac{S}{S'}\right| = \left|\dfrac{U(S)}{U(S')}\right| = |\mathcal{A}|$.

Observação. Resumindo a discussão acima, temos então que uma partição S/S' admite um rotulamento isométrico por um grupo $\mathcal{A}$ se:

(a) S é geométricamente uniforme;

(b) Os subconjuntos da partição geométricamente uniformes são mutuamente congruentes;

(c) Existem grupos de isometrias $U(S)$ e $U(S')$ tais que:$U(S)$ gera S , $U(S')$ gera S', $U(S') \lhd U(S)$ e $\mathcal{A} \simeq \dfrac{U(S)}{U(S')}$.

Teorema 2 .Uma aplicação de rotulamento (ou seja, uma bijeção) $m : \mathcal{A} \longrightarrow S/S'$ é um rotulamento isométrico se, e somente se, para todo $a \in \mathcal{A}$ existe uma isometria u_a tal que para todo $b \in \mathcal{A}$

$$m(ab) = u_a(m(b))$$

Demonstração Se $m : \mathcal{A} \longrightarrow S/S'$ é um rotulamento isométrico , do isomorfismo $\mathcal{A} \simeq \frac{U(S)}{U(S')}$ temos que: $ab \longmapsto u_{ab}U'$ e $ab \longmapsto u_aU'u_bU' = u_au_bU'$ de onde obtemos que $u_{ab}U' = u_au_bU' = \{(u_au_b)u(s_0) : u \in U' = U(S')\} = \{u_a[u_bu(s_0)] : u \in U(S')\} = u_a[m(b)]$.

Reciprocamente, se vale $m(ab) = u_a(m(b))$, para todos $a, b \in \mathcal{A}$, então $u_{ab}(S') = u_au_b(S')$ de onde $m(ab) = m(a)m(b)$ e m é um homomorfismo.■

Lema 1.(Propriedades elementares dos rotulamentos isométricos): Seja $m : \mathcal{A} \to S/S'$ um rotulamento isométrico,então:

(i)Se $T : \mathcal{A} \to \mathcal{A}$ é um automorfismo de grupos, então $m \circ T : \mathcal{A} \to S/S'$ é um rotulamento isométrico.

(ii) Para cada $b \in \mathcal{A}$, a função $m_b : \mathcal{A} \to S/S'$ definida por $m_b(a) = m(ab)$ é um rotulamento isométrico.

(iii)Se $u \in U(S)$, então $m_u : \mathcal{A} \to S/u(S')$ é um rotulamento isométrico.□

4.3 Códigos de Espaços de Sinais Geométricamente Uniformes

Sejam $(\mathcal{A}, *)$ um grupo e I um conjunto (eventualmente finito) $I \subseteq \mathbb{Z}$. Iremos considerar o ESPAÇO DE SEQUÊNCIAS

$$\mathcal{A}^I = \{\{a_k\}_{k \in I} : a_k \in \mathcal{A}, \forall k \in I\},$$

onde $\mathcal{A}$ é o ALFABETO e I de CONJUNTO DE ÍNDICES . $\mathcal{A}^I$ tem uma estrutura natural de grupo estendendo a operação a $\mathcal{A}^I$. Para todos $a = \{a_k\}$ e $b = \{b_k\}$ em $\mathcal{A}$,

$$a * b = \{a_k * b_k\}_{k \in I}.$$

Dados um conjunto de sinais S , uma partição S/S' e um conjunto de rótulos $\mathcal{A}$, a aplicação rotulamento é então

$$m : \mathcal{A} \to S/S',$$

e a sua extensão natural é

$$\underline{m} : \mathcal{A}^I \to (S/S')^I.$$

Desta forma, chamamos de CÓDIGO DE RÓTULOS a qualquer subconjunto $\mathcal{D} \subseteq \mathcal{A}^I$. Logo, $\underline{m}(c) = \{m(c_k)\}_{k \in I}$,$c \in \mathcal{D}$, é a sequência de subconjuntos de S selecionados pela sequência de rótulos $c \in \mathcal{D}$ pela aplicação de rotulamento m. É evidente que o caso de interêsse é aquele onde $\mathcal{A}$ é um grupo e m é um rotulamento isométrico.

Com estas notações temos:

Definição 3. Um CÓDIGO DE ESPAÇO DE SINAIS é qualquer conjunto do tipo

$$C(S/S', \mathcal{D}) = \bigcup_{c \in \mathcal{D}} \underline{m}(c).$$

Observação. Como $C(S/S', \mathcal{D}) = \bigcup_{c \in \mathcal{D}} \underline{m}(c) = \bigcup_{c \in \mathcal{D}} \{m(c_k)\}_{k \in I}$ temos que $C(S/S', \mathcal{D}) \subseteq S^I$. Uma sequência de sinais $s \in S^I$ é uma SEQUÊNCIA CÓDIGO ou, equivalentemente, um

elemento de $C(S/S', \mathcal{D})$ se existe algum $c \in \mathcal{D}$ tal que $s_k \in m(c_k)$, para todo $k \in I$. Se $S \subseteq \mathbb{R}^n$, então $C(S/S', \mathcal{D}) \subseteq (R^n)^I$ .Devemos notar que como $\mathbb{H}^2$ não é um espaço vetorial não há uma forma padrão para produtos.

A Figura 4.1 ilustra um codificador para um código de espaços de sinais:

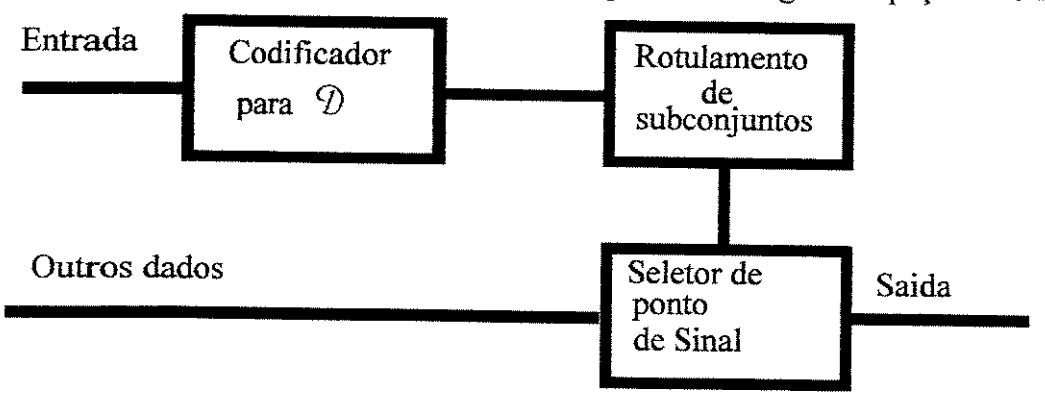

Figura 4.1 - Codificador para código de espaços de sinais.

Um codificador para o código de rótulos $\mathcal{D}$ gera uma sequência codificada de rótulos $c = \{c_k\}$ pertencente a $\mathcal{D}$ .A sequência individual c é determinada por uma sequência adequada de dados na entrada do codificador. Agora , a aplicação de rotulamento m é usada para determinar a sequência de subconjuntos $\underline{m}(c) = \{m(c_k)\}_{k \in I}$. Outros dados de entrada são usados então para determinar um elemento (sequência) específico de $\underline{m}(c)$ para que possa ser transmitido através do canal. Esta última operação é de natureza secundária, as propriedades de um código gerado por um codificador deste tipo dependem fundamentalmente das propriedades do código de espaço de sinais $C(S/S', \mathcal{D})$ que são determinados pela entrada a ser codificada por $\mathcal{D}$.

Seja agora S/S' uma partição geométricamente uniforme gerada por uma partição cujos grupos geradores são $U(S)$ e $U(S')$, e $\mathcal{A} \simeq U(S)/U(S')$ é o grupo de rótulos.

Definição 4. Sejam S/S' uma partição geométricamente uniforme com grupo de rótulos $\mathcal{A}$ e $\mathcal{D} \subseteq \mathcal{A}^I$ um subgrupo normal ($\mathcal{D} \lhd \mathcal{A}^I$), então um CÓDIGO DE CLASSES LATERAIS GENERALIZADO é o subconjunto

$$C(S/S', \mathcal{D}) = \{s \in \underline{m}(c) : c \in \mathcal{D}\} \subseteq S^I.$$

O teorema a seguir fornece uma conexão entre a G-linearidade e os códigos de classes laterais generalizados

Teorema 3 Nas hipóteses da Definição 4 , um código de classes laterais generalizado é um código $U(S)$-linear.

Demonstração Como S é geométricamente uniforme seja o rotulamento dado por:

$$\mu : G = U(S) \longrightarrow S$$

$$u \longmapsto u(s_0)$$

para algum s_0 fixo em S . Denotando $\mathcal{A} = \dfrac{U(S)}{U(S')} = \{uU(S')\}$ e o rotulamento bem definido

$$m : \mathcal{A} \longrightarrow \frac{S}{S'}$$

$$uU(S') \longmapsto u(S')$$

(de fato, se $uU(S') = vU(S')$, então $u^{-1}v \in U(S')$. Logo $u^{-1}v(S') = S'$. Portanto, $u(S') = v(S')$). Seja, agora, $H = \{u \in G : uU(S') \in \mathcal{D}\}$, então se $u, v \in H$, $uU', vU' \in \mathcal{D}$

e como $\mathcal{D} \leq \mathcal{A}$, temos que $uv^{-1}U' \in \mathcal{D}$ e $uv^{-1} \in H$. Como $e \in H$, temos que $H \leq G$. Por outro lado, como

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

isto mostra que $C(S/S', \mathcal{D})$ é $U(S)$-linear.■

Observação. A definição proposta originalmente por Forney, [09] , impõe a condição de que o grupo $\mathcal{A}$ seja abeliano. Em nossa proposta mais geral temos que impor somente a condição de que o código $\mathcal{D}$ seja um subgrupo normal do grupo de rótulos $\mathcal{A}$.

Lema 2. Se $C(S/S', \mathcal{D})$ é um código de classes laterais generalizado, então $\left(\frac{S^I}{S'^I}\right) \simeq \left(\frac{S}{S'}\right)^I$ é uma partição geometricamente uniforme e $\underline{m} : \mathcal{A}^I \to \left(\frac{S}{S'}\right)^I$ é um rotulamento isométrico para esta partição.

Demonstração (a) $U(S^I) = U(S)^I$. De fato, se $s_0 = \{s_{0,k}\}_{k \in I}$ onde $s_{0,k} = s_0$ para todo $k \in I$, então dado $s \in S^I$, $s = \{s_k\}_{k \in I}$, então para todo $k \in I$ existe um $u_k \in U(S)$ tal que $s_k = u_k(s_0)$. Assim, tomando $u = \{u_k\}_{k \in I} \in U(S)^I$ temos que $u \in U(S)^I$ e $u(s_0) = \{u_k(s_0)\}_{k \in I} = s$. Por outro lado, se $H \leq U(S)^I$, então $H = \prod_{k \in I} H_k$ onde $H_k \leq U(S)$ para todo k. Assim , se $U(S^I) = H \lneq U(S)^I$ devemos ter então que $H_k \lneq U(S)$ para algum $k \in I$, mas neste caso teremos $S = Hs_0$, contra a minimalidade de $U(S)$. Portanto $U(S^I) = U(S)^I$.

(b)$U(S')^I \lhd U(S)^I$ segue da definição de normalidade e do fato de que $U(S') \lhd U(S)$ por hipótese.

(c) $\underline{m} : \mathcal{A}^I \longrightarrow \left(\frac{S}{S'}\right)^I$ é uma isometria onde $\frac{U(S)^I}{U(S')^I}$ induz uma partição geometricamente uniforme $\frac{S^I}{S'^I}$ com espaço de rótulos $\mathcal{A}^I \simeq \frac{U(S)^I}{U(S')^I}$. ■

Lema 3. Com as notações anteriores, se $\mathcal{D} \lhd \mathcal{A}^I$, então com as estruturas induzidas,

$$(S')^I \leq C(S/S', \mathcal{D}) \leq S^I.$$

Com isso temos os isomorfismos: $\frac{S^I}{C(S/S', \mathcal{D})} \simeq \frac{\mathcal{A}^I}{\mathcal{D}}$; $\frac{C(S/S', \mathcal{D})}{(S')^I} \simeq \frac{\mathcal{D}}{\{e_{\mathcal{A}}\}^I} \simeq \mathcal{D}$; $\frac{S^I}{(S')^I} \simeq \frac{\mathcal{A}^I}{\{e_{\mathcal{A}}\}^I} \simeq \mathcal{A}^I$ ou seja, as cadeias de partições de grupos $S^I/C(S/S', \mathcal{D})/(S')^I$ e $\mathcal{A}^I/\mathcal{D}/\{e_A\}$ são isomorfas.

Demonstração A demonstração será feita para o caso $|I| = 1$ e o caso geral segue através da consideração de coordenadas. Os diagramas, mostrados a seguir, serão úteis na demonstração:

$$\begin{array}{ccc} U(S) & \xrightarrow{f} & S \\ | & & | \\ V & \longrightarrow & C(S/S', \mathcal{D}) \\ | & & | \\ U(S') & \longrightarrow & S' \end{array}$$

(a)$C(S/S', \mathcal{D}) \leq S$. De fato, sejam $\phi, \psi \in C(S/S', \mathcal{D})$, então existem $c_1, c_2 \in \mathcal{D}$ tais que $\phi \in m(c_1)$ e $\psi \in m(c_2)$. Se $f : U(S) \longrightarrow S$ é a bijeção que induz a estrutura de grupo em

S, então existem $v, w \in U(S)$ tais que $f(v) = \phi$ e $f(w) = \psi$. Com isso,

$$vU' = u_{c_1}U'$$

$$wU' = u_{c_2}U',$$

onde $vw \in u_{c_1}U' \cdot u_{c_2}U' = u_{c_1}u_{c_2}U' = u_{c_1c_2}U'$ e $f(vw) = \phi\psi \in m(c_1c_2)$. Portanto, $\phi\psi \in C(S/S', \mathcal{D})$.

Além disso, como $vU' = u_{c_1}U'$ resulta que $(vU')^{-1} = (u_{c_1}U')^{-1}$ ou $v^{-1}U' = u_{c_1}^{-1}U' = u_{c_1^{-1}}U'$. Portanto, $\phi^{-1} \in m(c_1^{-1}) \in C(S/S', \mathcal{D})$ conduzindo a $C(S/S', \mathcal{D}) \leq S$.

(b) $S' \leq C(S/S', \mathcal{D})$. Como $C(S/S', \mathcal{D}) = \bigcup_{c \in \mathcal{D}} m(c)$, definimos $V := f^{-1}(C(S/S', \mathcal{D}))$. Assim, $V \leq U(S)$ e que $V = f^{-1}(C(S/S', \mathcal{D})) = f^{-1}(\bigcup_{c \in \mathcal{D}} m(c)) = \bigcup_{c \in \mathcal{D}} f^{-1}(m(c)) = \bigcup_{c \in \mathcal{D}} u_c U'$. Em particular, $m(1) = U(S') = U' = 1 \cdot U' \subseteq V$ de onde $S' \subseteq C(S/S', \mathcal{D})$ ou $S' \leq C(S/S', \mathcal{D})$.

(c) $\dfrac{\mathcal{A}}{\mathcal{D}} \simeq \dfrac{S}{C(S/S', \mathcal{D})}$. Como $V = f^{-1}(C(S/S', \mathcal{D}))$, temos por definição de f que $\dfrac{U(S)}{V} \simeq \dfrac{S}{C(S/S', \mathcal{D})}$. Considerando agora $\Phi : \mathcal{A} \longrightarrow \dfrac{U(S)}{V}$, $a \longmapsto u_a V$ (Φ está bem definida porque $u_1U' = u_2U'$ implica $u_1u_2^{-1} \in U' \subseteq V$. Portanto, $u_1V = u_2V$.) temos então que $Ker\Phi = \mathcal{D}$ ($u_a \in V$ se, e somente se, $f(u_a) \in m(c)$ para algum $c \in \mathcal{D}$ se, e somente se, $a \in \mathcal{D}$). Portanto, $\dfrac{\mathcal{A}}{\mathcal{D}} \simeq \dfrac{U(S)}{V} \simeq \dfrac{S}{C(S/S', \mathcal{D})}$

$$\begin{array}{ccccc} & & U(S) & \xrightarrow{f} & S \\ & & | & & | \\ \mathcal{A} & \xrightarrow{g} & \dfrac{U(S)}{U(S')} & \xrightarrow{\tilde{f}} & \dfrac{S}{S'} \end{array}$$

(d) $\mathcal{D} \simeq \dfrac{\mathcal{D}}{\{e\}} \simeq \dfrac{C(S/S', \mathcal{D})}{S'}$. Considerando, agora, $g : \mathcal{A} \longrightarrow \dfrac{U(S)}{U(S')}$ o isomorfismo rotulamento, $g(c) = u_c U'$ temos então que $g(\mathcal{D}) = \dfrac{V}{U(S')}$ (de fato, se $u_c U' \in g(\mathcal{D})$, por definição $u_c U' \subseteq V$, de onde $u_c U' \in \dfrac{V}{U(S')}$ então $uU' = wU'$ de onde $w \in \bigcup_{c \in \mathcal{D}} u_c U'$ ou $w = u_c u_1$ para $c \in \mathcal{D}$ e $u_1 \in U'$. Assim, $g(\mathcal{D}) = \dfrac{V}{U(S')}$) e

$$\mathcal{D} \simeq \frac{V}{U(S')} \text{ (1).}$$

. Desta forma, temos que $\dfrac{V}{U(S')}$ é a imagem de $\mathcal{C}$ pelo isomorfismo de rotulamento, ou equivalentemente, $V = \bigcup_{u \in g(\mathcal{D})} uU' = \bigcup g(\mathcal{D})$.

Fazendo agora $f|V$ e tomando quocientes, temos

$$\frac{V}{U(S')} \simeq \frac{C(S/S', \mathcal{D})}{S'} \text{ (2)}$$

de (1) e (2) temos então que: $\mathcal{D} \simeq \dfrac{C(S/S', \mathcal{D})}{S'}$ ■

As classses laterais à direita de $\mathcal{D}$ em $\mathcal{A}$ (lembramos que foi assumida a hipótese de que $\mathcal{D} \lhd \mathcal{A}$) podem ser escritos na forma $\mathcal{D} \cdot a$, onde a é um elemento da classe lateral. Para tal classe lateral $\mathcal{D} \cdot a$, o rotulamento $m : A \longrightarrow \dfrac{S}{S'}$ define um subconjunto

$C(S/S', \mathcal{D}\cdot a)$ de S^I que é chamado de RÓTULO TRANSLADADO de $C(S/S', \mathcal{D})$,isto é,

$$C(S/S', \mathcal{D} \cdot a) = \bigcup_{c\in\mathcal{D}} \underline{m}(c \cdot a).$$

Lema 4. Os rótulos transladados de $C(S/S', \mathcal{D})$ são as classes laterais à direita de $C(S/S', \mathcal{D})$ em S^I sob a estrutura de grupo induzida.

Demonstração A demonstração será feita para o caso $|I|$ =1 . O caso geral segue da consideração de coordenadas.

$f^{-1}(C(S/S', \mathcal{D}\cdot a)) = f^{-1}(\bigcup_{c\in\mathcal{D}} \underline{m}(c \cdot a)) = \bigcup_{c\in\mathcal{D}} f^{-1}(\underline{m}(c \cdot a)) = \bigcup_{c\in\mathcal{D}} u_{c\cdot a}U' = \bigcup_{c\in\mathcal{D}} u_c u_a U' =$
$\left[\bigcup_{c\in\mathcal{D}} u_c U'\right] u_a = \left[\bigcup_{c\in\mathcal{D}} f^{-1}(\underline{m}(c))\right] f^{-1}(f(u_a)) = \left[f^{-1}(\bigcup_{c\in\mathcal{D}} (\underline{m}(c))\right] f^{-1}(f(u_a)) =$
$f^{-1}\left[\left[\bigcup_{c\in\mathcal{D}} (\underline{m}(c)\right] f(u_a)\right] = f^{-1}\left[[C(S/S', \mathcal{D} \cdot a)]\, f(u_a)\right]$ de onde obtemos que
$C(S/S', \mathcal{D} \cdot a) = C(S/S', \mathcal{D}) \cdot f(u_a)$ ■

Os resultados acima asseguram a validade da extensão do Teorema de Forney para os Códigos de Classes Laterais Generalizados sendo propostos.

Teorema 4 Se $C(S/S', \mathcal{D})$ é um código de classes laterais generalizado, então $S^I/C(S/S', \mathcal{D})/(S')^I$ é uma cadeia de partições geométricamente uniformes e os rótulos transladados $C(S/S', \mathcal{D} \cdot a)$ de $C(S/S', \mathcal{D})$ são geométricamente uniformes, mutuamente congruentes e tem grupo de simetrias comum $U(C(S/S', \mathcal{D})) = V$.

Corolário. Se $C(S/S', \mathcal{D})$ é (um transladado de) um código de classes laterais generalizado

, então:

(a) As regiões de Voronoi associadas com duas sequências-código $s, s' \in C(S/S', \mathcal{D})$ são congruentes.

(b) O perfil de distâncias $DP(s) = \{\|s - s'\| : s' \in C(S/S', \mathcal{D})\}$ de um ponto de sinal fixo $s \in C(S/S', \mathcal{D})$ a todos os pontos $s' \in C(S/S', \mathcal{D})$ independe de s.

Observação. Um código de classes laterais generalizado $C(S/S', \mathcal{D})$ com um conjunto de sinais infinito S é um arranjo regular no espaço de sequências (que pode ter dimensão finita ou infinita). Se S e I são finitos , temos um código tipo Slepian no espaço de sequências (de dimensão finita).

Conclusões e Sugestões

A proposta do presente trabalho foi de estender ao plano hiperbólico a teoria dos códigos, conjuntos de sinais e partições gométricamente uniformes. No Capítulo 4 foram obtidos resultados sobre rotulamentos e partições geométricamente uniformes, que permitiram a extensão da teoria aos grupos de isometrias hiperbólicos (em geral,com grupos de translações não abelianos, ao contrário dos grupos de translações euclidianas), e construções de partições geométricamente uniformes hiperbólicas. Também foi possível obter uma caracterização peculiar, via a G-linearidade, dos códigos de classes laterais generalizados (Teorema 3 do Capítulo 4).

No Capítulo 2 foram fornecidos os fundamentos da teoria dos dos códigos corretores de erros e foi estabelecida uma linguagem unificada para tratar de conjuntos de sinais euclidianos e hiperbólicos. Dentro desta unificação foi abordada a relação entre uniformidade geométrica, casamento e e uma definição de G-linearidade (Definição 7) e o

fato que um conjunto de sinais S é $U(S)$-linear (Teorema 3 (iii)).

No Capítulo 3, para determinar as partições geométricamente uniformes hiperbólicas, foram construidos subgrupos normais dos grupos de isometrias que determinam as tesselações correspondentes, ou equivalentemente, apresentaram-se estes grupos como extensões de subgrupos adequados. Com este objetivo, foram discutidos dois casos: 1) O caso auto-dual, onde são obtidas presentações de grupos que tem $[8,8]$ como extensão respectivamente, pelos grupos $\mathbb{Z}_n$, $\mathbb{D}_n$(o grupo diedral de grau n), $\mathbb{Z}_m \times \mathbb{Z}_n$, onde m e n são números inteiros positivos (Teoremas 1, 2 e 3 do Capítulo 3) ; 2) O caso não auto-dual em que o grupo $[p,3]$, foi descrito, para valôres específicos de p, através de um par de extensões sucessivas por $\mathbb{Z}_2$ e por $\mathbb{Z}_3$, e adequadas condições aritméticas sobre o número p (Teoremas 4 e 5 do Capítulo 3).. Estes resultados forneceram o substrato algébrico para o tratamento formal de conjuntos de sinais do Capítulo 4.

O Capítulo 4 estendeu à teoria das partições geométricamente uniformes ao plano hiperbólico, de modo a permitir que conjuntos de sinais casados com grupos, como aqueles descritos no Capítulo 3, possam ser decompostos em partições geométricamente uniformes. Destaca-se o resultado do Teorema 3 que mostra que um código de classes laterais genersalizado é $U(S)$-linear. A extensão da teoria foi feita sob a hipótese geral de que os códigos de rótulos são subgrupos normais do grupo de rótulos, obtendo então o resultado fundamental sobre cadeias de partições geométricamente uniformes hiperbólicas,

ou seja , que é uma cadeia geométricamente uniforme (Teorema 4).

Dentro do processo de determinação de novas estruturas que permitam gerar partições geométricamenter uniformes hiperbólicas, podemos citar que no caso auto-dual, os resultados se estendem para a forma mais geral $[p, p]$, contudo, a presentação dos subgrupos está por ser determinada, sendo que as técnicas utilizadas no presente trabalho parecem ser as mais adequadas. No caso não auto-dual, os resultados sobre grupos associados a tesselações $\{p, q\}$ mais gerais parecem depender, em parte, de relações de caráter aritmético entre os inteiros p e q.

Uma outra vertente que deve ser levada em conta, é a possibilidade de representação (rotulamento) destes conjuntos de sinais de um modo aritmético (ou seja, como quociente de um anel de inteiros algébricos por um seu ideal primo ou por representação de álgebras de quaternios).

Referências

[01] Beardon,A.F., *The Geometry of Discrete Groups*, New York, Springer,1982.

[02] Biglieri,E.,"*Performance Evaluation of Digital Communication Schemes Based on Generalized Concatenation* " ,Politecnico di Torino, Torino, 1991.

[03] Biglieri,E.,Elia,M., "Multidimensional Modulation and Coding for Band-Limited Digital Channels ",IEEE Trans. Inf. Theory,v.34 no.4, p. 803-809, July 1988.

[04] Biglieri,E.,Elia,M., "On the Existence of Group Codes for the Gaussian Channel ",IEEE Trans. Inf. Theory, v.it-18, no.3, p.399-402, May 1972.

[05] Coxeter,H.M.S., *"Introduction to Geometry "*, Wiley, New York, 1961.

[06] Coxeter,H.M.S., Moser, W.O.J., *Generators And Relations For Discrete Groups*, Berlin,Springer,1965.

[07] Conway,J.H.,Sloane,N.J.A., *"Sphere Packings, Lattices and Groups "*, New York, Springer, 1988.

[08] Firby,P.A.,Gardiner,C.F., *Surface Topology,* New York,Ellis Horwood,1991.

[09] Forney,Jr.G.D.,"Geometrically Uniform Codes ", IEEE Trans. Inf. Theory, v.37 no. 5, p. 1241-1260, Sep. 1991.

[10] Fraleigh,J.B., *A First Course In Abstract Algebra*, Reading, Addison-Wesley,1989.

[11] Geronimo,J.R.,Palazzo Jr,R.,Costa,S.R.,,Interlando,J.C.,Brumatti,P., "On the Existence of $\mathbb{Z}_4 \times \mathbb{Z}_2^{k-2}$-Linear Binary Codes From the Non Existence of $\mathbb{Z}_{2^k}$−Linear Binary Codes, Preprint.

[12] Hammons,Jr.,A.R., Kumar,V., Calderbank,A.R., Sloane,N.A.J., Solé,P., " The $\mathbb{Z}_4$-Linearity of Kerdock,Preparata, Goethals, and Related Codes ",IEEE Trans. Inf. Theory, v.40 no.2, p.301-319, March 1994.

[13] Haykin,S., *Digital Communications,* New York,Wiley, 1988.

[14] Herstein,I.N., "*Topics in Algebra, 2nd. Edition* ". New York, Wiley,1975.

[15] Jones,G.A.,Singerman,S.,*Complex Functions: An Algebraic and Geometric Viewpoint*, Cambridge, Cambridge University Press,1987.

[16] Katok,S., *Fuchsian Groups,* Chicago,University of Chicago Press, 1992.

[17] Lathi,B.O., *"Randon Signals and Communication Systems* ", Seranton, International Textbook Company, 1968.

[18] Lima,E.L., *"Espaços Métricos "*, Rio de Janeiro, IMPA,1977.

[19] Lima,E.L.,*"Grupo Fundamental e Espaços de Recobrimento "*,Rio de Janeiro,IMPA,1993.

[20] Lin,S.,Costello Jr,D.J., "Error Control Coding ",New Jersey, Prentice Hall, 1983.

[21] Lint,J.H.van, *"Introduction to Coding Theory "*, New York,Springer,1992.

[22] Loeliger, H.A.,"Signal Sets Matched To Groups ",IEEE Trans. Inf. Theory, v.37 no.6,p.1675-1682, Nov 1991.

[23] Lyndon,R.C.,Schupp,P.E., *"Combinatorial Group Theory "*,Berlin,Springer,1977.

[24] Magnus,W., *Noneuclidean Tesselations and Their Groups*, New York, Academic Press,1974.

[25] Magnus,W., Karras,A., Solitar,D., *Combinatorial Group Theory*, New York, Interscience,1966.

[26] Palazzo Jr,R,Interlando,J.C., "Construction of Signal Sets Matched to Groups Based on the Concept of d-Path.,Preprint, 1998.

[27] Papoulis,A., *"Probability, Random Variables and Stochastic Processes, 3rd ed. "*, New York, McGrow Hill, 1995.

[28] Roman,S., *"Coding and Information Theory "*,New York,Springer,1992.

[29] Rotman,J.J., "*The Theory of Groups, An Introduction* ".Boston, Allyn and Bacon,1973.

[30] Shannon,C.E., A Mathematical Theory of Communication , Bell Syst. Tech. J., vol 27, p. 379-423 e p. 623-656, julho/outubro 1948.

[31] Slepian,D.,"Group Codes for the Gaussian Channel ", Bell Sys. Tech. J. v. 37, p575-602, 1968.

[32] Slepian,D., "On Neighbor Distances and Symmetry in Group Codes ",IEEE Trans. Inf. Theory, p.630-632, Sep. 1971.

[33] Samuel,P. "*Algebraic Theory of Numbers* " ,Paris, Hermann,1970.

[34] Thurston,W.P., "*Three-dimensional Geometry and Topology* ",Princeton,Princeton,1997.

[35] Ungerboeck,G.,"Channel Coding with Multilevel/Phase Signals ",IEEE Trans. Inf. Theory vol. it-28, no.1 p.55-67, Jan 1982.