Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Códigos de Permutação para o Canal Gaussiano

por

Aldo Trajano Lourêdo

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Junho/2000

João Pessoa - Pb

Códigos de Permutação para o Canal Gaussiano

por

Aldo Trajano Lourêdo

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva

Prof. Dr Hélio Pires de Almeida

Prof. Dr. João Bosco Nogueira

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Junho/2000

Agradecimentos

1. Agradeço à Deus, pois sem ele nada seria possível, a minha família que sempre mim apoio, à minha mãe Lurdes e ao meu pai Antônio, à minha esposa Marinalva, esta que compreendeu tantas vezes a minha ausência.

2. Aos professores: Dr. Osmundo A de Lima e Dr. João Montenegro de Miranda pelo incentivo para fazer o Mestrado.

3. Ao professor Dr. Hélio Pires de Almeida, que nunca se negou, quando o procurei para expor as minhas dúvidas, e aos colegas do Curso de Mestrado.

4. Ao professor Dr. Marivaldo P Matos, em nome do Departamento de Pós-Graduação em Matemática - CCEN - UFPB, pela a minha acolhida nesta Instituição.

5. Ao meu orientador e amigo professor, Dr. Antônio de Andrade e Silva, pela eficaz orientação nesta dissertação, a sua colaboração e ao seu insentivo, e pela paciência que tivera ao longo deste mestrado.

6. A secretária da Pós-Graduação em Matemática Sônia, pelos constantes favores que fizera.

7. Não, poderia deixar de citar o meu irmão que sempre mim apoio, mas infelizmente não se encontra, mas conosco.

8. A CAPES pelo suporte financeiro para a realização do Curso de Mestra do.

Dedicatória

À meu irmã
"in memoriam"
Aroldo Trajano Lourêdo.

Notação

$B_\epsilon(\mathbf{x}_0)$ bola aberta de raio ϵ e centro $\mathbf{x}_0$

χ caráter da matriz

aH classe lateral à esquerda

C código

(M, n) código de grupo em $\mathbb{R}^n$

F corpo

$V - X$ complementar

$\mathcal{L}(V, V)$ conjunto de operadores lineares de V

$S^\perp$ complemento ortogonal

$\mathbb{N}$ conjunto dos números naturais

$\mathbb{Z}$ conjunto dos números inteiros

$\mathbb{R}$ conjunto dos números reais

$\mathbb{C}$ conjunto dos números complexos

$\mathbb{R}^n$ produto cartesiano de $\mathbb{R}$ (n cópias)

$GL(V)$ conjunto dos operadores lineares invertíveis $\mathcal{L}(V, V)$

$GL_n(F)$ conjunto das matrizes invertíveis ordem n

$M_n(F)$ conjunto das matrizes de ordem n

$O(V)$ conjunto dos operadores ortogonais de $GL(V)$

$O(n, \mathbb{R})$ conjunto das matrizes ortogonais com entradas em $\mathbb{R}$

ΔC conjunto das diferenças dos elementos de C

V_G conjunto dos elementos do $\mathbb{R}^n$ que são fixados por G

$V_G^\perp$ conjunto dos elementos ortogonais a V_G

k dimensão do código

d^2 distância quadrática

$S_\epsilon(\mathbf{x}_0)$ esfera de raio ϵ e centro $\mathbf{x}_0$

$F^{\mathbb{I}}$ espaço de seqüências

G_x estabilizador de x

$\overline{X}$ fecho de X

∂X fronteira de X

$M(H, G)$ grupo das matrizes monomiais

$\frac{G}{H}$ grupo quociente

S_n grupo de simetria

$H \rtimes_\varphi K$ holomorfo relativo de H por L

$[.]$ índice

$\simeq$ isomorfismo

X^0 interior de X

$\mathbf{M}^{-1}$ matriz invertível

$\mathbf{M}^t$ matriz transposta

$\mathbf{DP}$ matriz monomial

$\lfloor . \rfloor$ maior inteiro

$\lceil . \rceil$ menor inteiro

$\|.\|$ norma

ker núcleo do homomorfismo

Fix(a) número de elementos que fixa a

T operador linear

$O(x)$ órbita do elemento

$o(a)$ ordem do elemento

$|.|$ ordem do grupo

$(,) \leq (,)$ ordem lexicográfica

$G \wr H$ produto entrelaçado de G por H

$\langle . \rangle$ produto interno

$G = H \rtimes K$ produto semi-direto de H por K

$\backsim$ relação de equivalência

ρ_N representação natural

ρ_R representação regular

$\oplus$ soma direta

$\leq$ subgrupo

$\langle a \rangle$ subgrupo gerado pelo elemento a

$\trianglelefteq$ subgrupo normal

tr traço da matriz

R taxa de informação do código

Sumário

Introdução

0.1 Histórico

O *Canal Gaussiano* é um modelo de comunicação introduzido por Shannom em 1948, no qual mensagens para a transmissão são representadas por vetores em $\mathbb{R}^n$. Quando o vetor $\mathbf{x}$ é transmitido o sinal recebido é representado por um vetor $\mathbf{r} = \mathbf{x} + \mathbf{n}$ que consiste do vetor enviado mais um vetor $\mathbf{n}$ com variáveis aleatórias independente chamado *ruído*, o qual não depende de $\mathbf{x}$. Mais precisamente, o Canal Gaussiano com Ruído Branco Aditivo é um canal onde a medida de probabilidade de transição é uma função apenas da diferença $\mathbf{r} - \mathbf{x}$, isto é,

$$p_{R|X}(\mathbf{r} \mid \mathbf{x}) = p_N(\mathbf{r} - \mathbf{x}),$$

onde $p_N(\mathbf{n})$ é a densidade de probabilidade com uma média zero e uma variânça σ^2.

Em um sistema de comunicações digitais, o objetivo é transmitir dados de uma fonte até um usuário. O meio usado para esta transmissão é o canal (Gaussiano), e pode ser um cabo coaxial, fibra óptica, a atmosfera (no caso de ondas de rádio) etc.

Em um sistema tradicional, os dados gerados pela fonte são símbolos de um alfabeto F. Como cada símbolos tem sua probabilidade de ocorrência, estes dados são processados pelo codificador de fonte, com o objetivo de eliminar redundância, isto é, tornar os símbolos equiprováveis e desta forma compactar a informação.

As seqüências geradas pelo codificador de fonte são então processadas pelo codificador de canal, que introduz redundância gerando seqüências de símbolos de F que são chamadas de palavras código.

Para a transmissão, o modulador associa a cada palavra código $\mathbf{x}$ um símbolo analógico, que é então enviado pelo canal.

A imperfeição do canal gera distorções, e o sinal recebido nem sempre coincide com o

enviado. O demodulador faz então a melhor estimativa, fornecendo uma seqüência $\mathbf{r}$ de símbolos de F. Devido ao ruído $\mathbf{n}$, é possível que $\mathbf{r}$ não seja uma palavra código. Então o decodificador de canal associará uma palavra código, que é a melhor estimativa.

Finalmente, o decodificador de fonte associará a esta palavra código a suposta seqüência original de símbolos enviada.

Na presente dissertação descrevemos uma classe de códigos e uma deco dificação para a transmissão de informação por significado de faixa limitada W na presença do Canal Gaussiano com ruído branco aditivo. O sistema global de transmissão é chamado *modulação de permutação*. O sistema tem muitas características desejáveis, cada palavra código exige a mesma energia para a transmissão. O recebimento, que é por verossimelhança, é do tipo algébrico, um instrumento relativamente fácil, e não exige generalização local da possível mensagem enviada.

Nesta dissertação, consideraremos decodificação por verossimilhança de códigos de grupos. Esta técnica consiste das seguintes etapas. Primeira - representa o código de grupo na forma de um conjunto de vetores em $\mathbb{R}^n$ cujas componentes são obtidas por permutação das componentes de um vetor inicial de acordo com um grupo G de permutação. Segunda - decodificamos o vetor recebido $\mathbf{r}$ pela procura da mais provável permutação no grupo S_n. Terceira - selecionamos um elemento de G mais próximo da permutação encontrada. Aqui focalizaremos nas duas primeiras etapas. Em particular, determinaremos o valor mínimo de n, e mostraremos que qualquer código de grupo pode ser representado como um código de permutação.

0.2 Descrição

Esta dissertação tem como base os artigos [2, 9, 13].

No capítulo 1, faremos uma abordagem sobre a teoria de grupos e alguns resultados sobre álgebra linear, destes últimos resultados, obteremos um algoritmo para encontrar uma matriz ortogonal $\mathbf{O}$ quadrada de ordem m, onde $m = |G|$ e G é um grupo cíclico.

No capítulo 2, definimos representação de grupos, regiões fundamental, códigos de grupo, códigos de permutação e códigos planar. Caracterizamos códigos planar e demonstraremos um teorema que relacionando códigos planar com a representação de um grupo G de matrizes ortogonais.

No capítulo 3, apresentaremos um decodificador sub-ótimo de códigos de grupo. Esta técnica consiste das seguintes etapas. Primeira - representaremos o código de grupo na forma de um conjunto de vetores em $\mathbb{R}^n$ cujas componentes são obtidas por permutação das componentes de um vetor inicial de acordo com um grupo G de permutação. Segunda - decodificamos o vetor recebido $\mathbf{r}$ pela procura da mais provável permutação no grupo S_n. Terceira - selecionamos um elemento de G mais próximo da permutação encontrada.

Capítulo 1

Grupos de Permutação

Neste capítulo apresentaremos algumas definições e resultados básicos da teoria de grupos e que serão necessários para os capítulos subsequentes, o leitor interessado em mais detalhes pode consultar [7].

1.1 Conceitos Básicos

Um conjunto não vazio G munido com uma operação binária $(a, b) \longmapsto a * b$ é um *grupo* se as seguintes condições são satisfeitas:

1. A operação é associativa: $a * (b * c) = (a * b) * c$, $\forall a, b, c \in G$.

2. Existe um elemento neutro, isto é, $\exists\, e \in G$ tal que $e * a = a * e = a$, $\forall a \in G$.

3. Todo elemento possui um elemento inverso, isto é, $\forall\ a \in G$, $\exists\ b \in G$ tal que $a * b = b * a = e$.

O grupo é abeliano ou comutativo se também vale:

4. A operação é comutativa, isto é, $a * b = b * a$, $\forall\ a, b \in G$.

Para simplificar a notação usaremos ab em vez de $a * b$.

Um subconjunto não vazio H de um grupo G é um *subgrupo* de G, denotado por $H \leq G$, quando com a operação herdada de G, H é um grupo.

Proposição 1.1 *Sejam G um grupo e H um subconjunto não-vazio de G. Então H é um subgrupo de G se, e somente se, as seguintes condições são satisfeitas*:

1. para todos $h_1, h_2 \in H$, tem-se $h_1 h_2 \in H$.

2. Para todo $h \in H$, tem-se $h^{-1} \in H$. ■

Sejam X um subconjunto não vazio de G e

$$\mathcal{F} = \{H : H \leq G \text{ e } X \subseteq H\}.$$

Então

$$\langle X \rangle = \bigcap_{H \in \mathcal{F}} H$$

é o menor subgrupo de G contendo X e chamado o *subgrupo gerado* por X. Quanto existir $a \in G$ tal que

$$G = \langle \{a\} \rangle = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

dizemos que G é um *grupo cíclico*.

Sejam G um grupo, H e K subgrupos finito de G. Então

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Uma *partição* de um conjunto não vazio Ω é um conjunto

$$P(\Omega) = \{\Gamma : \Gamma \subset \Omega, \Gamma \neq \varnothing\}$$

tal que as seguintes condições são satisfeitas:

1. $\Gamma_1 \cap \Gamma_2 = \varnothing, \forall \Gamma_1, \Gamma_2 \in P(\Omega), \Gamma_1 \neq \Gamma_2$;

2. $\Omega = \bigcup_{\Gamma \in P(\Omega)} \Gamma$

Sejam G um grupo e H um subgrupo de G. Definimos em G uma *relação de equivalência* (à esquerda) $\backsim$ de H em G, da seguinte maneira, para todos $a, b \in G$,

$$a \backsim b \Longleftrightarrow \exists h \in H \text{ tal que } b = ah.$$

De modo análogo definimos a relação à direita.

A classe de equivalência que contém a é o conjunto

$$aH = \{ah : h \in H\},$$

chamado de *classe lateral à esquerda* de H em G que contém a.

A cardinalidade do conjunto das classes laterais à esquerda (à direita) chama-se o *índice* de H em G, denotado por $[G : H]$.

Teorema 1.1 (Lagrange) *Sejam G um grupo e H um subgrupo de G. Então $|G| = |H|[G:H]$. Em particular, se G é finito, então $|H| \mid |G|$ e $[G:H] \mid |G|$.* ■

Proposição 1.2 *Sejam G um grupo e H, K subgrupos de G tal que $K \leq H \leq G$. Então*

$$[G:K] = [G:H][H:K].$$

■

Um subgrupo H de um grupo G é chamado *normal* de G, em símbolos $H \trianglelefteq G$, se

$$aha^{-1} \in H, \forall a \in G, h \in H.$$

Seja p um número primo. Um grupo G é chamado um *p-grupo* se existir $n \in \mathbb{N}$ tal que $a^{p^n} = e$, para todo $a \in G$. Além disto, pelo Teorema 1.1, todo subgrupo de um p-grupo é um p-subgrupo de G.

Lema 1.1 (Cauchy) *Sejam G um grupo finito e p um primo que divide $|G|$. Então existe $a \in G$, $a \neq e$, tal que $a^p = e$.* ■

Seja Ω um conjunto finito e não vazio. Então o conjunto de todas as bijeções de Ω sobre Ω, em símbolos S_Ω, é chamado o *grupo de simetrias* de Ω. Qualquer subgrupo de S_Ω é chamado de *grupo de permutação*. Quando $\Omega = \{1, 2, \ldots, n\}$ denotaremos S_Ω por S_n.

Sejam G um grupo e Ω um conjunto não vazio. Dizemos que G *age* sobre Ω se existir uma aplicação $\psi : G \times \Omega \longrightarrow \Omega$, com $\psi(a, x) = ax$, tal que as seguintes condições são satisfeitas:

1. $a(bx) = (ab)x$, para todos $a, b \in G, x \in \Omega$;

2. $ex = x$, para todo $x \in \Omega$.

A aplicação ψ é chamado a *ação* de G sobre Ω e Ω é chamado um *G-conjunto*. Se $|\Omega| = n$, então n é chamado o *grau* do G-conjunto Ω.

Exemplo 1.1 *Sejam $G = S_n$ e $\Omega = \{1, 2, \ldots, , n\}$. Então Ω é um G-conjunto sob a ação*

$$\sigma * i = \sigma(i), \sigma \in S_n, i \in \Omega.$$

Observação 1.1 *Seja Ω um G-conjunto. Então para cada $a \in G$ fixado, a aplicação $\varphi_a(x) = ax$ é uma permutação de Ω.*

Teorema 1.2 *Sejam G um grupo e Ω um conjunto.*

1. *Se Ω é um G-conjunto, então a ação de G sobre Ω induz um homomorfismo $\psi : G \longrightarrow S_\Omega$.*

2. *Qualquer homomorfismo $\psi : G \longrightarrow S_\Omega$ induz uma ação de G sobre Ω.*

Demonstração. 1. Vamos definir $\psi : G \longrightarrow S_\Omega$ por $\psi(a) = \varphi_a$. Dados $a, b \in G$ temos, para todo $x \in \Omega$, que

$$\begin{aligned}(\psi(ab))(x) &= \varphi_{ab}(x) = (ab)x \\ &= a(bx) = \varphi_a(bx) \\ &= \varphi_a(\varphi_b(x)) = \varphi_a \circ \varphi_b(x) \\ &= \psi(a) \circ \psi(b)(x),\end{aligned}$$

isto é, $\psi(ab) = \psi(a)\psi(b)$, para todos $a, b \in G$. Portanto, ψ é um homomorfismo.

2. Definindo $ax = (\psi(a))(x)$, para todo $a \in G$ e $x \in \Omega$. É fácil verificar que isto é uma ação de G em Ω. ■

Seja Ω um G-conjunto não vazio. Então para cada $x \in \Omega$ o conjunto

$$G_x = \{a \in G : ax = x\}$$

é um subgrupo de G chamado o *estabilizador* de x. O conjunto

$$O(x) = \{ax : a \in G\}$$

é chamado a *órbita* de x.

Proposição 1.3 *Sejam Ω um G-conjunto e $x \in \Omega$. Então*

$$|O(x)| = [G : G_x].$$

Em particular, se G é finito, então $|O(x)| \mid |G|$.

Demonstração. Vamos definir

$$\varphi : O(x) \to \frac{G}{G_x}$$

por $\varphi(ax) = aG_x$. É fácil verificar que φ está bem definida e injetiva. Agora, dado $a \in G$, existe $ax \in O(x)$ tal que $\varphi(ax) = aG_x$, isto é, φ é sobrejetiva. Portanto,

$$|O(x)| = [G : G_x].$$

Se G é finito, então, pelo Teorema1.1, temos que $|O(x)| \mid |G|$. ■

Seja Ω um G-conjunto não vazio. Então, dados $x, y \in \Omega$, definimos

$$y \backsim x \Leftrightarrow \text{ existe } a \in G \text{ tal que } y = ax.$$

É claro que $\backsim$ é uma relação de equivalência em Ω e a classe de equivalência determinada por x é igual a órbita de x. Além disto, se $y \backsim x$, então existe $a \in G$ tal que $G_y = aG_xa^{-1}$.

Lema 1.2 *Se $a \in G - G_x$, então $G_x \cap G_xaG_x = \varnothing$.*

Demonstração. Se $b \in G_x \cap G_xaG_x$, então $bx = x$ e $b = cad$, onde $c, d \in G_x$. Logo,

$$bx = cadx = cax \Longrightarrow c^{-1}bx = ax \Longrightarrow c^{-1}x = ax \Longrightarrow ax = x \Longrightarrow a \in G_x,$$

o que é uma contradição. ■

Proposição 1.4 *Seja G um grupo de ordem $2k$, com k ímpar. Então G possui um subgrupo de índice 2.*

Demonstração. Seja G um grupo de ordem $2k$. Então, pelo Teorema 1.2, existe para cada $a \in G$ um homomorfismo injetivo φ_a de G em S_{2k}. Assim, G é isomorfo $K = \varphi_a(G)$ e $|K| = 2k$.

Afirmação. K contém uma permutação ímpar, isto é, $A_{2k} \neq K$.

De fato. Pelo Lema 1.1, existe $b \in K$ tal que $o(b) = 2$. Considerando K como um $\langle b \rangle$-conjunto, obtemos que

$$K = \bigcup_{x \in K} \{x, bx\}$$

é uma união disjunta de órbitas. Assim, dado $a \in G$ com $o(a) = 2$ temos

$$a \longleftrightarrow b = \varphi_a = (x_1bx_1) \ldots (x_kbx_k),$$

é uma permutação ímpar, pois k é ímpar. Portanto, K contém uma permutação ímpar e $A_{2k} \neq K$. Logo, $A_{2k} \nsubseteq KA_{2k}$ e $S_{2k} = KA_{2k}$. Daí,

$$2 = \frac{|S_{2k}|}{|A_{2k}|} = \frac{|KA_{2k}|}{|A_{2k}|} = \frac{|K|}{|A_{2k} \cap K|} = [K : A_{2k} \cap K].$$

Assim, basta tomar $H = \varphi_a^{-1}(A_{2k} \cap K)$. ■

1.2 Grupos Multiplamente Transitivo

Nesta seção apresentaremos algumas definições e resultados sobre grupos multiplamente transitivo (m-transitivo). O leitor interessado em maiores detalhes pode consultar [5, 12].

Dizemos que G *age transitivamente* sobre Ω, se para quaisquer $x, y \in \Omega$, existir $a \in G$ com $ax = y$ ou, equivalentemente, $\Omega = O(x), \forall x \in \Omega$. Dizemos que G *age fortemente transitivo* sobre Ω se dados $x, y \in \Omega$, então existir um único $a \in G$ tal que $y = ax$. Neste caso, $|G| = |\Omega|$.

Observação 1.2 *G age transitivamente sobre cada órbita.*

Teorema 1.3 *Sejam G um grupo, $H \leq G$ e $\Lambda = \frac{G}{H}$ um G-conjunto. Seja π_H a representação por permutação induzida por esta ação. Então*:

1. *G age transitivamente sobre Λ.*

2. *O estabilizador em G do ponto $H \in \Lambda$ é o subgrupo H.*

3. *O núcleo da ação é dado por*

$$\ker \pi_H = \bigcap_{b \in G} bHb^{-1}$$

e $\ker \pi_H$ é o maior subgrupo normal de G contido em H.

Demonstração.1. Para ver que G age transitivamente sobre Λ. Sejam aH, $bH \in \Lambda$ e $c = ba^{-1} \in G$. Então

$$caH = (ba^{-1})aH = bH.$$

2. O estabilizador do ponto H é

$$G_H = \{a \in G : aH = H\} = H.$$

3. Por definição de π_H temos que

$$\begin{aligned}\ker \pi_H &= \{a \in G : abH = bH, \forall b \in G\} \\ &= \{a \in G : b^{-1}ab \in H, \forall b \in G\} \\ &= \{a \in G : a \in bHb^{-1}, \forall b \in G\} \\ &= \bigcap_{b \in G} bHb^{-1}.\end{aligned}$$

A segunda afirmação, segue do fato de que

$$\ker \pi_H \lhd G \text{ e } \ker \pi_H \leq H.$$

Finalmente, se $N \lhd G$ e $N \subset H$ então

$$N = xNx^{-1} \leq xHx^{-1}, \forall x \in G.$$

Assim, $N \leq \ker \pi_H$. ■

Corolário 1.1 (Cayley) *Todo grupo é isomorfo a um grupo de permutação.* . ■

Dizemos que um subconjunto $\Gamma \subseteq \Omega$ é *G-invariante* se

$$G\Gamma = \{\sigma(i) : i \in \Gamma\} \subseteq \Gamma,$$

onde $\sigma \in G$ e G é um grupo de permutações sobre Ω.

Exemplo 1.2 *Sejam* $\Omega = \{1, 2, 3\}$ *e* $S_\Omega = \{e, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2\}$. *Então*

$$G = \{e, \tau_1\} \leq S_\Omega \text{ se } \Gamma = \{2, 3\} \text{ então } G\Gamma = \Gamma.$$

Observação 1.3 *Todo grupo de permutação sobre* Ω *possui pelo menos dois G-conjuntos invariantes* Ω *e* $\varnothing$*, chamados de trivias e qualquer outro será chamado de não trivial.*

Se os únicos G-conjuntos invariantes de Ω são os triviais, então dizemos que Ω é um *G-conjunto transitivo.* Caso contrário, Ω é um *G-conjunto intransitivo.*

Para cada $a \in G$ fixado, denotamos por $\mathrm{Fix}(a)$ o número de elementos de $x \in \Omega$ fixados por a, isto é,

$$\mathrm{Fix}(a) = |\{x \in \Omega : ax = a\}|.$$

Proposição 1.5 (Cauchy-Frobenius) *Seja Ω um G-conjunto. Então*

$$\sum_{a\in G} \mathrm{Fix}(a) = k\,|G|\,,$$

onde k é igual ao número de órbitas de G.

Demonstração. Considere o conjunto

$$\Gamma = \{(a,x) \in G \times \Omega : ax = x\},$$

contaremos o número de elementos de Γ de duas maneiras distintas. Primeiro, suponha que as órbitas de G são $\Omega_1, \ldots, \Omega_k$. Então, pela Proposição 1.3, temos

$$|\Gamma| = \sum_{i=1}^{k} \sum_{x\in\Omega_i} \frac{|G|}{|\Omega_i|} = \sum_{i=1}^{k} |G| = k\,|G|\,.$$

Por outro lado,

$$|\Gamma| = \sum_{a\in G} \mathrm{Fix}\,(a)\,.$$

Portanto,

$$\sum_{a\in G} \mathrm{Fix}\,(a) = k\,|G|$$

■

Dizemos que um G-conjunto Ω é *semi-regular* se $G_x = \{e\}$, $\forall x \in \Omega$ e se, além disto, Ω é um G-conjunto transitivo, então dizemos que G é *regular*.

Proposição 1.6 *Todas as órbitas de um G-conjunto semi-regular têm o mesmo comprimento, a saber, $|G|$.*

Demonstração. Pelo Proposição1.3, $|O(x)| = [G : G_x]$, $\forall x \in \Omega$. Como por hipótese G é semi-regular temos que $G_x = \{e\}$. Portanto, $|O(x)| = |G|$. ■

Proposição 1.7 *Seja Ω um G-conjunto semi-regular. Então $|G|$ divide $|\Omega|$. Além disto, um G-conjunto transitivo Ω é regular se, e somente se, G age fortemente transitivo sobre Ω.*

Demonstração. Seja Ω um G-conjunto semi-regular. Então

$$\Omega = \bigcup_{x\in\Omega} O(x).$$

e pela Proposição1.3, $|\Omega| = k\,|G|$, onde k é o número de órbitas. Portanto, $|G|$ é um divisor de $|\Omega|$. Finalmente, suponhamos que Ω é um G-conjunto é regular, isto é, Ω é semi-regular e transitivo. Então, $|\Omega| = k\,|G|$. Como Ω é transitivo temos que $k = 1$. Portanto, $|\Omega| = |G|$.

Reciprocamente, suponhamos que $|\Omega| = |G|$. Como Ω é transitivo temos, pelo Teorema 1.1 e a Proposição 1.3, que

$$[G : G_x]\,|G_x| = |G| = |\Omega| = |O(x)| = [G : G_x].$$

Logo, $|G_x| = 1$. Portanto, $G_x = \{e\}$. ■

Proposição 1.8 *Seja Ω um G-conjunto transitivo com G abeliano. Então G é regular.*

Demonstração. Para cada $x \in \Omega$ fixado, temos que existe, para cada $y \in \Omega$, $a \in G$ tal que $ax = y$, $\forall y \in \Omega$. Logo,

$$\begin{aligned} G_y &= G_{ax} = \{b \in G : bax = ax\} \\ &= \{b \in G : abx = ax\} \\ &= \{b \in G : bx = x\} = G_x. \end{aligned}$$

Assim, $G_x = \{e\}$, pois $y \in \Omega$ é arbitrário. Portanto, G é regular. ■

Um subconjunto Λ de um G-conjunto transitivo Ω é *imprimitivo* se

$$a\Lambda = \Lambda \text{ ou } \; a\Lambda \cap \Lambda = \varnothing.$$

Observação 1.4 *Seja Ω um G-conjunto transitivo. Então todo subconjunto não vazio Λ de Ω tal que $\Lambda = \Omega$ ou $|\Lambda| = 1$ é imprimitivo e chamados de triviais.*

Dizemos que Ω um G-conjunto transitivo é *imprimitivo* se existe um subconjunto imprimitivo não trivial em Ω. Caso contrário, Ω é *primitivo.*

Exemplo 1.3 *Sejam $\Omega = \{1, 2, 3, 4\}$ e $G = \{e, \tau_1, \tau_2, \tau_3\} \lhd S_4$. Então Ω é um G-conjunto transitivo e imprimitivo, pois*

$$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\} \text{ e } \{3, 4\}$$

são imprimitivos em Ω.

Observação 1.5 *Se existir um subconjunto imprimitivo Λ em um G-conjunto transitivo Ω, então*

$$\Omega = \bigcup_{a \in G} a\Lambda,$$

união disjunta e $|\Lambda|$ divide $|\Omega|$.

Proposição 1.9 *Seja Ω um G-conjunto transitivo de grau primo. Então Ω é primitivo.*

Demonstração. Seja $\Lambda \subseteq \Omega$. Então, pela Observação 1.5 $|\Lambda|$ divide $|\Omega|$. Como a $|\Omega|$ é primo temos que $|\Lambda| = 1$ ou $|\Lambda| = |\Omega|$. Portanto, Ω é primitivo. . ■

Proposição 1.10 *Seja Ω um G-conjunto transitivo. Então Ω é primitivo se, e somente se, para cada $x \in \Omega$, G_x é um subgrupo maximal de G.*

Demonstração. Suponhamos que exista um subgrupo H de G tal que $G_x \leq H \leq G$. Então, fazendo $\Lambda = xH \subseteq \Omega$, temos duas possibilidades:

Se $\Lambda = \Omega$, então H é transitivo e

$$|\Omega| = [G : G_x] = [H : G_x].$$

Portanto, $G = H$.

Se $\Lambda = \{x\}$, então $H \leq G_x$. Portanto, $G_x = H$.

Reciprocamente, suponhamos, por absurdo, que Ω contenha um subconjunto imprimitivo Λ não trivial. Então definimos $H \leq G$ por

$$H = \{a \in G : a\Lambda = \Lambda\}$$

Agora, escolha $x \in \Lambda$. Se $ax = x$, então $x \in \Lambda \cap a\Lambda$ e, assim, $a\Lambda = \Lambda$. Portanto, $G_x \leq H$. Como Λ é não trivial temos que existe $y \in \Lambda$, com $y \neq x$. Por hipótese, existe $a \in G$ tal que $ax = y$. Logo,

$$y \in \Lambda \cap a\Lambda$$

e $a\Lambda = \Lambda$. Assim, $a \in H$ e $a \notin G_x$, pois $ax = y \neq x$, isto é, G_x é um subgrupo próprio de$H$. Pela maximalidade G_x temos que $G = H$. Logo, $a\Lambda = \Lambda$, para todo $a \in G$, isto é, $\Omega = \Lambda$, o que é uma contradição. ■

Sejam Ω um G-conjunto e $m \in \mathbb{N}$. Dizemos que Ω é *m-transitivo* se dado quaisquer dois subconjuntos ordenados

$$\Lambda = \{x_1, \ldots, x_m\} \text{ e } \Gamma = \{y_1, \ldots, y_m\},$$

de Ω existir $a \in G$ tal que

$$ax_i = y_i, i \in \{1, \ldots, m\}.$$

Exemplo 1.4 *Sejam $\Omega = \{1, \ldots, n\}$. Então, Ω é um S_n-conjunto n-transi tivo e Ω é um A_n-conjunto $(n-2)$-transitivo mas não é $(n-1)$-transitivo.*

Solução. Ω é um S_n-conjunto n-transitivo, pois S_n contém qualquer permutação de Ω. Dados

$$\Gamma = \{x_1, \ldots, x_{n-2}\} \text{ e } \Lambda = \{y_1, \ldots, y_{n-2}\}.$$

Então, exatamente uma das seguintes permutações é par.

$$\sigma(x_i) = y_i \text{ e } \varphi(x_i) = \begin{cases} y_i & \text{se } 1 \leq i \leq n-2 \\ y_n & \text{se } i = n-1 \\ y_{n-1} & \text{se } i = n, \end{cases}$$

onde x_{n-1}, x_n, y_{n-1} e y_n são elementos restantes. Assim, Ω é um A_n-conjunto $(n-2)$-transitivo, pois existe $\phi \in A_n$ tal que $\phi(x_i) = y_i$, $\forall i = 1, \ldots, n-2$, mas não é $(n-1)$-transitivo. ■

Proposição 1.11 *Sejam Ω um G-conjunto transitivo e $m \in \mathbb{N}$, com $m \leq |\Omega|$. Então Ω é m-transitivo se, e somente se, $\Omega - \{x\}$ é um G_x-conjunto $(m-1)$-transitivo.*

Demonstração. Suponhamos que Ω é m-transitivo. Então dados

$$\Gamma = \{x_1, \ldots, x_{m-1}\} \text{ e } \Lambda = \{y_1, \ldots, y_{m-1}\}$$

dois conjuntos ordenados em $\Omega - \{x\}$. É claro que

$$\Gamma' = \{x_1, \ldots, x_{m-1}, x\} \text{ e } \Lambda' = \{y_1, \ldots, y_{m-1}, x\}$$

são conjuntos ordenados de Ω. Por hipótese, existe $a \in G$ tal que

$$ax_i = y_i, \forall i = 1, \ldots, m-1 \text{ e } ax = x.$$

Logo, $a \in G_x$. Portanto, $\Omega - \{x\}$ é um G_x-conjunto $(m-1)$-transitivo.

Reciprocamente, suponhamos que $\Omega - \{x\}$ é um G_x-conjunto $(m-1)$-transitivo. Como Ω é transitivo temos que $\Omega - \{x\}$ é um G_x-conjunto $(m-1)$-transitivo, para todo $x \in \Omega$. Assim, dados subconjuntos ordenados

$$\{x_1, \ldots, x_m\} \text{ e } \{y_1, \ldots, y_m\}$$

de Ω, podemos escolher $a \in G$ tal que $ax_1 = y_1$. Por hipótese, existe $b \in G_{y_1}$ tal que $b(ax_i) = y_i$, para todo $i = 2, \ldots, m$. Logo, para cada $i = 1, 2, \ldots, m$ temos que $(ba)x_i = y_i$. Portanto, G é m-transitivo. ■

Proposição 1.12 *Sejam Ω um G-conjunto transitivo. Então Ω é 2-transitivo se, e somente se, $G = G_x \cup G_x a G_x$, para todo $a \in G - G_x$.*

Demonstração. Suponhamos que Ω é 2-transitivo. Então dado $b \in G - G_x$, $ax = y$ e $bx = z$, com $x \notin \{y, z\}$. Pela Proposição 1.11, $\Omega - \{x\}$ é G_x-transitivo. Logo, existe $c \in G_x$ tal que $cy = z$. Portanto,

$$cax = cy = z = bx \Longrightarrow a^{-1}c^{-1}bx = x \Longrightarrow a^{-1}c^{-1}b \in G_x.$$

Assim, $b \in G_x a G_x$, pois

$$b = c(c^{-1}b) = ca(a^{-1}c^{-1}b),$$

com $ca \in G_x a$ e $a^{-1}c^{-1}b \in G_x$. Portanto, pelo Lema 1.2, $G = G_x \cup G_x a G_x$.

Reciprocamente, suponhamos que $G = G_x \cup G_x a G_x$. Dados $y, z \in \Omega - \{x\}$, por hipótese, existem $b, c \in G$ tais que $bx = y$ e $cx = z$. Como $b, c \notin G_x$ temos que $b \in G_x a G_x$ e $c \in G_x a G_x$. Logo, existem $r, s, t, u \in G_x$ tais que

$$b = ras \text{ e } c = tau \Rightarrow c = t(r^{-1}bs^{-1})u.$$

Assim,

$$\begin{aligned} z &= cx = t(r^{-1}bs^{-1})ux = (tr^{-1}b)s^{-1}x \\ &= tr^{-1}bx = tr^{-1}y. \end{aligned}$$

Logo, $\Omega - \{x\}$ é um G_x-conjunto transitivo. Portanto, pela Proposição 1.11, G é 2-transitivo. ■

Observação 1.6 *Os subgrupos da Proposição acima são maximais. Além disto, Se Ω é um G-conjunto 2-transitivo, então Ω é primitivo.*

Proposição 1.13 *Seja Ω um G-conjunto transitivo. Então*

$$\sum_{a \in G} \mathrm{Fix}(a)^2 = k|G|,$$

onde k é o número de óbitas de G_x. Em particular, Ω é 2-transitivo se, e somente se,

$$\sum_{a \in G} \mathrm{Fix}(a)^2 = 2|G|.$$

Demonstração. Seja

$$\Gamma = \{(a, x, y) : x, y \in \Omega \text{ e } a \in G_x \cap G_y\}.$$

Então para calcular $|\Gamma|$, procedemos como segue. Pela Proposição 1.5, para cada $a \in G$ fixado, o número de pares ordenados (x, y) com $(a, x, y) \in \Gamma$ é dado por $\text{Fix}(a)^2$. Assim,

$$|\Gamma| = \sum_{a \in G} \text{Fix}(a)^2.$$

Por outro lado, como Ω é um G-conjunto transitivo temos, para algum $x \in \Omega$ fixado, que

$$|\Gamma| = |\Omega||\Lambda|,$$

onde

$$\Lambda = \{(a, y) : a \in G_x \text{ e } ay = y\}.$$

Mas

$$|\Lambda| = k\,|G_x|\,,$$

onde k é o número de órbitas de G_x. Pela Proposição 1.5 e Teorema 1.1 temos que

$$\sum_{a \in G} \text{Fix}(a)^2 = k\,|G_x|\,|\Omega| = k\,|G_x|\,[G : G_x] = k\,|G|\,.$$

■

1.3 Produto Entrelaçado

Neste seção apresentaremos um dos mais importantes método para a construção de grupos a partir de grupos conhecidos.

Sejam G um grupo, H e K dois subgrupos. Dizemos que G é um *produto semi-direto* de H por K, em símbolos $G = H \rtimes K$, se as seguintes condições são satisfeitas:

1. $G = HK$;
2. $H \trianglelefteq G$;
3. $H \cap K = \{e\}$.

Neste caso, K é um *complemento* de H e $K \simeq \frac{G}{H}$.

Teorema 1.4 *Sejam G um grupo e H um subgrupo normal de G. Então as seguintes condições são equivalentes*:

1. *G é um produto semi-direto de H por $\frac{G}{H}$;*

2. *Existe um homomorfismo de grupos $\varphi : \frac{G}{H} \longrightarrow G$, com*

$$\pi \circ \varphi = id_{\frac{G}{H}},$$

   onde $\pi : G \longrightarrow \frac{G}{H}$ é o homomorfismo canônico;

3. *Existe um homomorfismo de grupos $\phi : G \longrightarrow G$, com $\ker \phi = H$ e $\phi(x) = x$ para todo $x \in \operatorname{Im} \phi$.*

Demonstração. (1. $\Longrightarrow$ 2.) Seja K um complemento de H em G, isto é, $K \simeq \frac{G}{H}$. Então, cada $a \in G$ pode ser escrito de modo único na forma $a = hk$ com $h \in H$ e $k \in K$. Seja

$$\varphi : \frac{G}{H} \longrightarrow G$$

definida por $\varphi(Ha) = k$. Então é fácil verificar que φ é um homomorfismo bem definido com

$$\pi \circ \varphi = id_{\frac{G}{H}}.$$

(2. $\Longrightarrow$ 3.) Vamos definir $\phi : G \longrightarrow G$ por $\phi = \varphi \circ \pi$. Se $x \in \operatorname{Im} \phi$, então existe $a \in G$ tal que $x = \phi(a)$. Logo,

$$\phi(x) = \phi(\phi(a)) = \varphi \circ (\pi \circ \varphi)(\pi(a)) = \varphi \circ \pi(a) = \phi(a) = x,$$

isto é, $\phi(x) = x$ para todo $x \in \operatorname{Im} \phi$. Se $a \in \ker \phi$, então $\phi(a) = \varphi \circ \pi(a) = e$. Logo, $k = e$ e $a \in H$, isto é, $\ker \phi \subseteq H$. Reciprocamente, se $a \in H$, então

$$\phi(a) = \varphi \circ \pi(a) = \varphi(Ha) = \varphi(H) = e,$$

e, assim, $a \in \ker \phi$.

(3. $\Longrightarrow$ 1.) Fazendo $K = \operatorname{Im} \phi$. Obtemos que $G = HK$, pois

$$a = ae = a\phi(a)^{-1}\phi(a) = [a\phi(a^{-1})]\phi(a) \in HK,$$

para todo $a \in G$. Finalmente, se $x \in H \cap K$, então $\phi(x) = e$ e $x = \phi(x)$. Logo, $x = e$, isto é,

$$H \cap K = \{e\}.$$

Como

$$K = \operatorname{Im}\phi \simeq \frac{G}{H}$$

temos que G é o produto semi-direto de H por $\frac{G}{H}$. ■

Seja G o produto semi-direto de H por K. Então, cada $a \in G$ pode ser escrito de modo único na forma:

$$a = hk, h \in H \text{ e } k \in K.$$

Assim, dados $a_1, a_2 \in G$, digamos $a_1 = h_1k_1$ e $a_2 = h_2k_2$, com $h_1, h_2 \in H$ e $k_1, k_2 \in K$, obtemos que

$$a_1a_2 = (h_1k_1)(h_2k_2) = (h_1k_1h_2k_1^{-1})(k_1k_2) = (h_1h_2^{k_1})(k_1k_2),$$

onde $h_2^{k_1} = k_1h_2k_1^{-1}$. Agora, seja K agindo em G por conjugação, isto é,

$$k \cdot a = kak^{-1}.$$

Então, para cada $k \in K$:

1. $\sigma_k : H \longrightarrow H$, $\sigma_k(h) = k \cdot h$ é um automorfismo.

2. $\varphi : K \longrightarrow \operatorname{Aut}(H) \leq S_G$ definida por $\varphi(k) = \sigma_k$ é um homomorfismo.

De fato. 1.

$$\begin{aligned} \sigma_k \circ \sigma_{k^{-1}}(h) &= \sigma_k(\sigma_{k^{-1}}(h)) \\ &= \sigma_k(khk^{-1}) \\ &= k(k^{-1}hk)k^{-1} = h. \end{aligned}$$

De modo análogo,

$$\sigma_{k^{-1}} \circ \sigma_k(h) = h, \forall h \in H.$$

Logo, $\sigma_{k^{-1}}$ é a inversa de σ_k e σ_k é bijetiva. Dados $h_1, h_2 \in H$,

$$\begin{aligned} \sigma_k(h_1h_2) &= k(h_1h_2)k^{-1} \\ &= (kh_1k^{-1})(kh_2k^{-1}) \\ &= \sigma_k(h_1)\sigma_k(h_2). \end{aligned}$$

Logo, $\sigma_k \in \operatorname{Aut}(H)$, $\forall k \in K$.

2. Basta mostrar que $\sigma_{k_1k_2} = \sigma_{k_1} \circ \sigma_{k_2}$, $\forall k_1, k_2 \in K$. De fato, dado $h \in H$,

$$\begin{aligned} \sigma_{k_1k_2}(h) &= (k_1k_2)h(k_1k_2)^{-1} = k_1(k_2hk_2^{-1})k_1^{-1} \\ &= \sigma_{k_1}(k_2hk_2^{-1}) = \sigma_{k_1}(\sigma_{k_2}(h)) \\ &= \sigma_{k_1} \circ \sigma_{k_2}(h). \end{aligned}$$

Assim, a multiplicação em G torna-se

$$a_1a_2 = (h_1k_1)(h_2k_2) = (h_1\varphi(k_2)h_2)(k_1k_2).$$

Neste caso, G é o produto semi-direto de H por K via φ, isto é, $G = H \rtimes_\varphi K$.

Sejam G, H grupos, Ω um H-conjunto finito e

$$\{G_x : x \in \Omega\}$$

uma família de cópias isomorfas de G indexada por Ω.

Seja

$$K = \prod_{x \in \Omega} G_x.$$

Então o *produto entrelaçado* de G por H, denotado por $G \wr H$, é o produto semi-direto de K por H, onde H age sobre K por

$$\mathbf{a}_x \cdot h = \mathbf{a}_{hx}$$

para todo $h \in H$ e $\mathbf{a}_x \in K$. O subgrupo normal K de $G \wr H$ é chamado a *base* do produto entrelaçado.

Note que, se G é finito, então

$$|K| = |G|^{|\Omega|},$$

e se H também é finito, então

$$|G \wr H| = |K \rtimes H| = |K|\,|H| = |G|^{|\Omega|}\,|H|.$$

Seja Λ um G-conjunto. Então $\Lambda \times \Omega$ pode ser considerado um $(G \wr H)$-conjunto. De fato, dado $a \in G$ e $x \in \Omega$, definimos $\widehat{\mathbf{a}}_x \in S_{\Lambda \times \Omega}$, como segue:

$$\widehat{\mathbf{a}}_x\,(\lambda, y) = \begin{cases} (a\lambda, y) & \text{se } y = x, \\ (\lambda, y) & \text{se } y \neq x. \end{cases}$$

É fácil verificar que $\widehat{\mathbf{a}}_x\widehat{\mathbf{b}}_x = \widehat{\mathbf{ab}}_x$ e, assim, $\widehat{G}_x$ definido por

$$\widehat{G}_x = \{\widehat{\mathbf{a}}_x : a \in G\},$$

é um subgrupo de $S_{\Lambda\times\Omega}$. Além disto, a aplicação $\psi : G \longrightarrow \widehat{G}_x$, dada por $a \longmapsto \widehat{\mathbf{a}}_x$ é um isomorfismo.

Para cada $h \in H$, definimos $\widehat{\mathbf{h}} \in S_{\Lambda\times\Omega}$, como segue:

$$\widehat{\mathbf{h}}\,(\lambda, y) = (\lambda, hy)$$

e

$$\widehat{H} = \{\widehat{\mathbf{h}} : h \in H\}.$$

É fácil verificar que $\widehat{H}$ é um subgrupo de $S_{\Lambda\times\Omega}$ e que a aplicação $\varphi : H \longrightarrow \widehat{H}$ dada por $h \longmapsto \widehat{\mathbf{h}}$ é um isomorfismo.

Teorema 1.5 *Sejam G, H grupos, Ω um H-conjunto finito e Λ um G-conjunto. Se Ω e Λ são transitivos, então $\Lambda \times \Omega$ é um $(G \wr H)$-conjunto transitivo.*

Demonstração. Sejam $(\lambda, x), (\gamma, y) \in \Lambda\times\Omega$. Como G age transitivamente sobre Λtemos que existe $a \in G$ tal que $a\lambda = \gamma$ e H age transitivamente sobre Ω temos que existe $h \in H$ tal que $hx = y$.

Afirmação: $\widehat{\mathbf{h}}\widehat{\mathbf{a}}_x\,(\lambda, x) = (\gamma, y)$.

De fato.

$$\begin{aligned}
\widehat{\mathbf{h}}\widehat{\mathbf{a}}_x\,(\lambda, x) &= \widehat{\mathbf{h}}\,(\widehat{\mathbf{a}}_x\,(\lambda, x)) \\
&= \widehat{\mathbf{h}}\,(a\lambda, x) \\
&= (a\lambda, hx) \\
&= (\gamma, y).
\end{aligned}$$

■

Se $L \subseteq \mathrm{Aut}(H)$, então um *holomorfo relativo* de H por L, em símbolos $\mathrm{Hol}(H, L)$, é igual $H \rtimes_\varphi K$, onde $\varphi : K \longrightarrow L$ é um isomorfismo. Se H e K são fixados, então $\mathrm{Hol}(H, L)$ é único, a menos de isomorfismo.

Seja H um grupo qualquer agindo em $\Omega = H$ por multiplicação à esquerda, isto é,

$$h \cdot a = ha.$$

Então para cada $h \in H$ fixado, $\sigma_h : \Omega \longrightarrow \Omega$ dada por $\sigma_h(a) = ha$ é uma bijeção. Se

$$L = \{\varphi(h) = \sigma_h : h \in H\} = \mathrm{Aut}(H),$$

então

$$\mathrm{Hol}(H, L) = \mathrm{Hol}(H) = H \rtimes L.$$

Exemplo 1.5 *Mostrar que* $G = \mathrm{Hol}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_4$. *Note que* $L = \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3$, *pois todo elemento de* $\mathbb{Z}_2 \times \mathbb{Z}_2 - \{(\overline{0}, \overline{0})\}$ *tem ordem dois. Agora, se* $H = \mathbb{Z}_2 \times \mathbb{Z}_2$, *então* $G = H \rtimes L$ *e* $|G| = 24$. *Finalmente, seja*

$$\Omega = \frac{G}{L} = \{hL : h \in H\}.$$

Então $g \cdot (hL) = ghL$ *é uma ação de* G *sobre* Ω. *Logo,*

$$\varphi : G \to S_\Omega$$

definida por $\varphi(g) = \sigma_g$, *onde* $\sigma_g(hL) = ghL$ *e* $\sigma_g \in S_\Omega \simeq S_4$, *é homomorfismo injetivo. De fato.*

$$\begin{aligned} \ker \varphi &= \{g \in G : \varphi(g) = I_\Omega\} \\ &= \{g \in G : \varphi(g)(hL) = hL, \forall h \in H\} \\ &= \{g \in G : g(hL) = hL, \forall h \in H\} \\ &= \bigcap_{h \in H} G_{hL} = \{e\}. \end{aligned}$$

Portanto, $\mathrm{Hol}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_4$.

Sejam $\Omega = \{1, 2, \ldots, n\}$, $n \geq 2$, K um grupo e

$$H = \prod_{i=i}^{n} K = K^n.$$

Então $\sigma \cdot i = \sigma(i)$, $\forall \sigma \in S_n$ e $i \in \Omega$, é uma ação de S_n em Ω, isto é, Ω é um S_n-conjunto. Assim,

$$\varphi : S_n \longrightarrow \mathrm{Aut}(H)$$

definida por

$$\varphi(\sigma)(h_i)_{i=1}^n = (h_{\sigma^{-1}(i)})_{i=1}^n$$

é um homomorfismo injetivo de grupos, pois se $\sigma \in \ker \varphi$ e $\sigma \neq I_\Omega$, então existe $i \in \Omega$ tal que $\sigma(i) \neq i$. Logo, existe $(h_j)_{j=1}^n \in H$ tal que

$$h_i \neq h_{\sigma^{-1}(i)} \text{ e } \varphi(\sigma)(h_j)_{j=1}^n \neq (h_j)_{j=1}^n.$$

Portanto, $\varphi(\sigma) \neq I_H$.

Se $L = S_n$, então o produto entrelaçado de K por L, em símbolos $K \wr L$, é dado por $\mathrm{Hol}(H, L)$. Se $\Omega = G$ é um grupo, então o produto entrelaçado $K \wr S_n$ é chamado de *regular*.

Sejam F um corpo e $\mathbf{I} = [\mathbf{e}_1 \cdots \mathbf{e}_n]$ a matriz identidade sobre F, com vetores colunas $\mathbf{e}_i$, $i = 1, \ldots, n$. Uma matriz de permutação sobre F é uma matriz $\mathbf{P}$ obtida permutando as colunas de $\mathbf{I}$, isto é, existe $\sigma \in S_n$ tal que

$$\mathbf{P} = [\mathbf{e}_{\sigma(1)} \cdots \mathbf{e}_{\sigma(n)}].$$

Afirmação: O conjunto P_n de todas as matrizes de permutação é um grupo.

De fato. Dados $\mathbf{P}, \mathbf{Q} \in P_n$, digamos

$$\mathbf{P} = [\mathbf{e}_{\sigma(1)} \cdots \mathbf{e}_{\sigma(n)}] \text{ e } \mathbf{Q} = [\mathbf{e}_{\tau(1)} \cdots \mathbf{e}_{\tau(n)}],$$

onde $\sigma, \tau \in S_n$, então

$$\mathbf{PQ} = [\mathbf{e}_{\sigma\tau(1)} \cdots \mathbf{e}_{\sigma\tau(n)}] \in P_n,$$

pois $\sigma\tau \in S_n$. Assim, temos a associatividade em P_n e $\mathbf{I}$ é elemento identidade de P_n. É fácil verificar que

$$\mathbf{P}\mathbf{P}^t = \mathbf{P}^t\mathbf{P} = \mathbf{I}.$$

Finalmente, a aplicação $f : S_n \to P_n$ dada por

$$f(\sigma) = \mathbf{P} = [\mathbf{e}_{\sigma(1)} \cdots \mathbf{e}_{\sigma(n)}]$$

é um isomorfismo de grupos.

Seja G um grupo multiplicativo qualquer. Uma *matriz monomial* $\mathbf{A}$ sobre G é uma matriz de permutação $\mathbf{P}$ cujas entradas não nulas são substituídas pelos elementos de G, isto é, $\mathbf{A} = \mathbf{DP}$, onde

$$\mathbf{D} = \mathrm{diag}(a_1, \ldots, a_n), \forall a_i \in G,$$

é uma matriz diagonal de ordem n. Dizemos que $\mathbf{P}$ é o *suporte* de $\mathbf{A}$. Logo, o conjunto

$$M(G, P_n) = \{\text{todas as matrizes monomiais } A \text{ sobre } G \text{ com suporte em } P_n\}$$

é claramente um grupo. Além disto,

$$P_n \simeq M(\{e\}, P_n) \leq M(G, P_n) \text{ e } M(G, \{\mathbf{I}\}) \simeq G^n.$$

Teorema 1.6 *$M(G, P_n) = M(G, \{\mathbf{I}\}) \rtimes M(\{e\}, P_n)$. Neste caso,*

$$M(G, P_n) \backsimeq G \wr P_n.$$

Demonstração. Por definição temos que

$$M(G, P_n) = M(G, \{\mathbf{I}\}) M(\{e\}, P_n).$$

Assim, basta mostrar que

$$M(G, \{\mathbf{I}\}) \trianglelefteq M(G, P_n) \text{ e } M(G, \{\mathbf{I}\}) \cap M(\{e\}, P_n) = \{e\mathbf{I}\}.$$

Dados $\mathbf{A} = \mathbf{DP} \in M(G, P_n)$ e $\mathbf{D}' \in M(G, \{\mathbf{I}\})$, temos que

$$\begin{aligned} \mathbf{AD}'\mathbf{A}^{-1} &= \mathbf{DPD}'\mathbf{P}^{-1}\mathbf{D}^{-1} \\ &= \mathbf{DD}''\mathbf{D}^{-1} \in M(G, \{\mathbf{I}\}). \end{aligned}$$

Finalmente, dado

$$\mathbf{A} \in M(G, \{\mathbf{I}\}) \cap M(\{e\}, P_n),$$

temos que $\mathbf{A} = \mathbf{DI}$ e $\mathbf{A} = \text{diag}(e, \ldots, e)\mathbf{P}$, isto é,

$$\mathbf{D} = \text{diag}(a_1, \ldots, a_n) = \text{diag}(e, \ldots, e).$$

Portanto, $\mathbf{A} = e\mathbf{I}$. ■

Exemplo 1.6 *Sejam $G = \{1, -1\}$ um grupo multiplicativo e*

$$P_2 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

o grupo das matrizes de permutação. Então

$$M(G, P_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}$$

é isomorfo ao grupo diedral D_4.

1.4 Operadores Lineares

Nesta seção apresentaremos algumas definições e resultados básicos sobre Álgebra Linear, que serão necessários para o entendimento dos capítulos subsequentes, o leitor interessado em mais detalhes pode consultar [6].

Seja F um corpo. Um conjunto não vazio V equipado com duas operações $(\mathbf{u}, \mathbf{v}) \mapsto \mathbf{u}+\mathbf{v}$ e $(\alpha, \mathbf{u}) \mapsto \alpha\mathbf{u}$, é um *espaço vetorial* sobre F se as seguintes condições são satisfeitas:

1. $(V, +)$ é um grupo comutativo;

2. $\alpha(\beta\mathbf{u}) = (\alpha\beta)\mathbf{u}$, para todos $\alpha, \beta \in F$ e $\mathbf{u} \in V$;

2. $(\alpha + \beta)\mathbf{u} = \alpha\mathbf{u} + \beta\mathbf{u}$ e $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$, para todos $\alpha, \beta \in F$ e $\mathbf{u}, \mathbf{v} \in V$;

3. $1\mathbf{u} = \mathbf{u}$, para todo $\mathbf{u} \in V$.

Um espaço vetorial V, salvo menção explicíta em contrário, significa um espaço veorial sobre $\mathbb{R}$ com dimensão $\dim(V) = n$. Um *operador linear* de V é uma aplicação $T : V \to V$ tal que

$$T(\alpha\mathbf{u} + \mathbf{v}) = \alpha T(\mathbf{u}) + T(\mathbf{v}), \forall \mathbf{u}, \mathbf{v} \in V \text{ e } \alpha \in \mathbb{R}.$$

Denotaremos por $\mathcal{L}(V, V)$ o conjunto de todos os operadores lineares de V. Neste caso, $\mathcal{L}(V, V)$ é um espaço vetorial com $\dim(\mathcal{L}(V, V)) = n^2$.

Um escalar $\lambda \in \mathbb{R}$ é um *autovalor* $T \in \mathcal{L}(V, V)$, se existir $\mathbf{u} \in V$, $\mathbf{v} \neq \mathbf{0}$ tal que

$$T(\mathbf{u}) = \lambda\mathbf{u}.$$

O vetor $\mathbf{u}$ é chamado o *autovetor* de T associado ao autovalor λ.

Lema 1.3 *Autovetores associados a autovalores distintos são sempre linearmente independentes.* ■

Um elemento $T \in \mathcal{L}(V, V)$ é chamado de *estrutura simples* se T possui n autovetores linearmente independentes.

Assim, um operador T possui uma estrutura simples se todas as raízes da equação característica são distintas e pertencem a $\mathbb{R}$. Note que, estas condições não são necessárias, pois existe operadores de estrutura simples cuja equação característica possui raízes múltiplas.

Seja $\mathbf{v} \in V$. Então, obtemos a sequência de vetores

$$\mathbf{v}, T(\mathbf{v}), T^2(\mathbf{v}), \ldots.$$

Como a $\dim(V) = n$, existe $m \in \mathbb{Z}$, com $0 \leq m \leq n$, tal que os vetores

$$\mathbf{v}, T(\mathbf{v}), \ldots, T^{m-1}(\mathbf{v})$$

são linearmente independentes e

$$T^m(\mathbf{v}) = \alpha_0\mathbf{v} + \alpha_1 T(\mathbf{v}) + \cdots + \alpha_{m-1}T^{m-1}(\mathbf{v}),$$

onde $\alpha_i \in \mathbb{R}$.

Sejam W um subespaço de V e $T \in \mathcal{L}(V, V)$. Dizemos que W é *invariante* em relação a T se $T(W) \subseteq W$, isto é,

$$T(\mathbf{w}) \in W, \forall \mathbf{w} \in W.$$

Lema 1.4 *Seja $W \neq \{\mathbf{0}\}$ um subespaço de V invariante em relação a $T \in \mathcal{L}(V, V)$. Então existe $\mathbf{w} \in W - \{0\}$, tal que $T(\mathbf{w}) = \lambda\mathbf{w}$.* ■

Demonstração. Seja $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ uma base para W. Então relativo a esta base T é representado por uma matriz $\mathbf{A} = (a_{ij})$. Seja

$$\mathbf{w} = \sum_{i=1}^{k} \alpha_i \mathbf{w}_i$$

Então, por hipótese,

$$\mathbf{A}\mathbf{w} = \sum_{i=1}^{k} \beta_i \mathbf{w}_i.$$

Neste caso,

$$\beta_i = \sum_{j=1}^{k} \alpha_j a_{ij}, i \in \{1, 2, \ldots, k\}$$

Afirmação: A equação vetorial $\mathbf{A}\mathbf{w} = \lambda\mathbf{w}$ tem uma solução não nula.

De fato. Note que, a equação polinomial $\det(\mathbf{A} - \lambda\mathbf{I}) = 0$ tem pelo menos uma raiz (em geral complexa) não nula λ_0 Logo, sistema

$$(a_{ii} - \lambda_0)\alpha_i + \sum_{\substack{j=1 \\ i \neq j}}^{k} a_{ij}\alpha_j = 0, i \in \{1, 2, \ldots, k\}$$

tem uma solução não nula $\gamma_1, \ldots, \gamma_k$. Assim, fazendo

$$\mathbf{w}_0 = \sum_{i=1}^{k} \gamma_i \mathbf{w}_i \in W^*,$$

obtemos que

$$\mathbf{A}\mathbf{w}_0 = \lambda_0 \mathbf{w}_0,$$

isto é, $\mathbf{w}_0$ é um autovetor não nulo de T associado ao autovalor $\lambda_0 = \lambda(T)$. ■

Lema 1.5 *Seja G um subgrupo abeliano finito (infinito) de $\mathcal{L}(V,V)$. Então existe $\mathbf{u} \in V$ tal que $T(\mathbf{u}) = \lambda \mathbf{u}$, para todo $T \in G$ e $\lambda = \lambda(T)$.*

Demonstração. A demonstração é feito por indução sobre $\dim V = n$. Para $n = 1$, nada há a demonstrar. Suponhamos que o resultado seja válido para todo espaço vetorial de dimensão menor ou igual a $n - 1$.

Se cada $\mathbf{u} \in V$ é tal que $T(\mathbf{u}) = \lambda(T)\mathbf{u}$, para todo $T \in G$, então o lema está demonstrado, pois $T = \alpha I$. Assim, suponhamos que exista $\mathbf{u} \in V$ tal que $T(\mathbf{u}) \neq \lambda \mathbf{u}$ para algum $T \in G$ Seja

$$W_\alpha = \{\mathbf{v} \in V : T(\mathbf{v}) = \alpha \mathbf{v}\} \cup \{\mathbf{0}\}$$

Logo, se $\mathbf{v} \in W_\alpha$, então $U\mathbf{v} \in W_\alpha$, para todo $U \in G$, pois

$$TU(\mathbf{v}) = UT(\mathbf{v}) = \alpha U(\mathbf{v}),$$

isto é, W_α é invariante em relação a qualquer elemento de G. Além disto, pelo Lema 1.4,

$$\{\mathbf{0}\} \subsetneq W_\alpha \subsetneq V.$$

Portanto, pela hipótese de indução, existe $\mathbf{v} \in W_\alpha$ tal que $T(\mathbf{v}) = \lambda(T)\mathbf{v}$, para todo $T \in G$. ■

Um elemento $T^t \in \mathcal{L}(V,V)$ é chamado o *transposto* ou *auto-adjunto* de $T \in \mathcal{L}(V,V)$ se

$$\langle T^t(\mathbf{u}), \mathbf{v} \rangle = \langle \mathbf{u}, T^t(\mathbf{v}) \rangle, \forall \mathbf{u}, \mathbf{v} \in V.$$

Um elemento $T \in \mathcal{L}(V,V)$ é chamado *normal* se $TT^t = T^tT$ e *ortogonal* se

$$\langle T(\mathbf{u}), T(\mathbf{v}) \rangle = \langle \mathbf{u}, \mathbf{v} \rangle, \forall \mathbf{u}, \mathbf{v} \in V.$$

O conjunto das transformações ortogonais de $\mathcal{L}(V,V)$, será denotado por $O(V)$. Note que, $T \in O(V)$ se, e somente se, $TT^t = I$. Além disto, se $T \in O(V)$, então $\det(T) = \pm 1$. Se $\det T = 1$, então dizemos que T é de *primeira espécie* (ou *próprio*), caso contrário de *segunda espécie* (ou *imprório*).

Seja S um subconjunto não vazio de V. O conjunto

$$S^{\perp} = \{\mathbf{u} \in V : \langle \mathbf{u}, \mathbf{v} \rangle = 0, \forall \mathbf{v} \in S\},$$

é um subespaço de V, chamado o *complemento ortogonal* de $\langle S \rangle$. Além disto, se W é um subespaço de V invariante com relação a T, então $W^{\perp}$ é invariante com relação a T^t.

Para o estudo de operadores lineares no espaço vetorial Euclidiano V sobre $\mathbb{R}$ estenderemos V ao espaço unitário $\widetilde{V}$, isto é, ao espaço com produto interno $\widetilde{V}$ sobre $\mathbb{C}$. Esta extensão é feita da seguinte maneira:

1. Os vetores de V são chamados vetores "reais";

2. Introduzimos vetores "complexo" $\mathbf{z} = \mathbf{u} + i\mathbf{v}$, onde $\mathbf{u}, \mathbf{v} \in V$;

3. As operações de adição de vetores complexos e a multiplicação são definidas de modo natural. Então o conjunto dos vetores complexos formam um espaço vetorial $\widetilde{V}$ sobre $\mathbb{C}$, com $\dim \widetilde{V} = n$, o qual contém V como subespaço;

4. Se $\mathbf{z}_1 = \mathbf{u}_1 + i\mathbf{v}_1$ e $\mathbf{z}_2 = \mathbf{u}_2 + i\mathbf{v}_2$, para todos $\mathbf{u}_i, \mathbf{v}_i \in V$, então

$$\langle \mathbf{z}_1, \mathbf{z}_2 \rangle = \langle \mathbf{u}_1, \mathbf{u}_2 \rangle - \langle \mathbf{v}_1, \mathbf{v}_2 \rangle + i(\langle \mathbf{v}_1, \mathbf{u}_2 \rangle + \langle \mathbf{u}_1, \mathbf{v}_2 \rangle)$$

é o produto interno em $\widetilde{V}$. Fazendo $\overline{\mathbf{z}}_1 = \mathbf{u}_1 - i\mathbf{v}_1$ e $\overline{\mathbf{z}}_2 = \mathbf{u}_2 - i\mathbf{v}_2$, obtemos que

$$\langle \overline{\mathbf{z}}_1, \overline{\mathbf{z}}_2 \rangle = \overline{\langle \mathbf{z}_1, \mathbf{z}_1 \rangle}.$$

Se escolhermos uma base real de V, então $\widetilde{V}$ será o conjunto de todos os vetores com coodenadas complexas e V o conjunto de todos os vetores com coordenadas reais nesta base. Assim, todo elemento $T \in \mathcal{L}(V,V)$ pode ser estendido de modo único a um elemento $\mathcal{L}(\widetilde{V}, \widetilde{V})$:

$$T(\mathbf{u} + i\mathbf{v}) = T(\mathbf{u}) + iT(\mathbf{v})$$

Dentre todos os operadores de $\mathcal{L}(\widetilde{V}, \widetilde{V})$ os que podem ser caracterizados pelo fato $T(V) \subseteq V$, serão chamados *operadores reais*. Seja T um operador real. Então, para cada

$$\mathbf{z} = \mathbf{u} + i\mathbf{v}, \overline{\mathbf{z}} = \mathbf{u} - i\mathbf{v} \in \widetilde{V},$$

com $\mathbf{u}, \mathbf{v} \in V$ e $\mathbf{v} \neq \mathbf{0}$, temos que

$$T(\mathbf{z}) = T(\mathbf{u}) + iT(\mathbf{v}) \text{ e } T(\overline{\mathbf{z}}) = T(\mathbf{u}) - iT(\mathbf{v}),$$

onde $T(\mathbf{u}), T(\mathbf{v}) \in V$.

Se $T(\mathbf{z}) = \lambda\mathbf{z}$, então $T(\overline{\mathbf{z}}) = \overline{\lambda}\overline{\mathbf{z}}$. Logo, o espaço bi-dimensional

$$\widetilde{W} = \{\alpha\mathbf{z} + \beta\overline{\mathbf{z}} : \alpha, \beta \in \mathbb{C}\} = \langle \mathbf{z}, \overline{\mathbf{z}} \rangle$$

tem uma base real.

$$\mathbf{u} = \frac{1}{2}(\mathbf{z} + \overline{\mathbf{z}}) \text{ e } \mathbf{v} = \frac{1}{2i}(\mathbf{z} - \overline{\mathbf{z}})$$

e o plano em V gerado por esta base é chamado *plano invariante* de T associado ao par de autovalores λ e $\overline{\lambda}$.

Seja $\lambda = \mu + i\nu$. Então, é fácil verificar que

$$T(\mathbf{u}) = \mu\mathbf{u} - \nu\mathbf{v} \text{ e } T(\mathbf{v}) = \nu\mathbf{u} + \mu\mathbf{v}.$$

Consideremos um operador real T de estrutura simples com autovalores

$$\begin{aligned} \lambda_{2k-1} &= \mu_k + iv_k \\ \lambda_{2k} &= \mu_k - iv_k,\ k = 1, \ldots, q, \\ \lambda_l &= \mu_l,\ l = 2q+1, \ldots, n, \end{aligned}$$

onde $\mu_k, v_k, \mu_l \in \mathbb{R}$ e $\nu_k \neq 0$ para $k = 1, 2, \ldots, q$. Então, os autovetores $\mathbf{z}_1, \ldots, \mathbf{z}_n$ associados a estes autovalores podem ser escolhidos tais que

$$\begin{aligned} \mathbf{z}_{2k-1} &= \mathbf{u}_k + i\mathbf{v}_k, \\ \mathbf{z}_{2k} &= \mathbf{u}_k - i\mathbf{v}_k,\ k = 1, \ldots, q, \\ \mathbf{z}_l &= \mathbf{u}_l,\ l = 2q+1, \ldots, n. \end{aligned}$$

O conjunto de vetores

$$\{\mathbf{u}_1, \mathbf{v}_1, \mathbf{u}_2, \mathbf{v}_2, \ldots, \mathbf{u}_q, \mathbf{v}_q, \mathbf{u}_{2q+1}, \ldots, \mathbf{u}_n\}, \tag{1.1}$$

forma uma base de V. Neste caso,

$$\begin{cases} T(\mathbf{u}_k) = \mu_k\mathbf{u}_k - \nu_k\mathbf{v}_k, \\ T(\mathbf{v}_k) = \nu_k\mathbf{u}_k + \mu_k\mathbf{v}_k,\ k = 1, \ldots, q, \\ T(\mathbf{u}_l) = \mu_l\mathbf{u}_l,\ l = 2q+1, \ldots, n. \end{cases} \tag{1.2}$$

Assim, o operador T é equivalente à matriz pseudo-diagonal

$$B = \left(A_{1,}A_2, \ldots, A_q, \mu_{2q+1}, \ldots, \mu_n\right),$$

onde

$$A_k = \begin{bmatrix} \mu_k & \nu_k \\ -\nu_k & \mu_k \end{bmatrix}$$

em relação à base (1.1). Em particular, no caso de operadores ortogonais os coeficientes da Equação (1.2) devem satisfazer

$$\begin{aligned} \mu_k^2 + v_k^2 &= 1,\ k = 1, \ldots, q, \\ \mu_l &= \pm 1,\ l = 2q+1, \ldots, n. \end{aligned}$$

Como a base (1.1) pode ser assumida ortonormal. As fórmulas (1.2) podem ser representadas na forma

$$\begin{aligned} T(\mathbf{u}_k) &= \mathbf{u}_k \cos\theta_k - \mathbf{v}_k \operatorname{sen}\theta_k, \\ T(\mathbf{v}_k) &= \mathbf{u}_k \operatorname{sen}\theta_k + \mathbf{v}_k \cos\theta_k,\ k = 1, \ldots, q, \\ T(\mathbf{u}_l) &= \pm\mathbf{u}_l,\ l = 2q+1, \ldots, n. \end{aligned}$$

Teorema 1.7 *Seja G um subgrupo normal abeliano finito (infinito) de o peradores de $\mathcal{L}(V,V)$, onde V é um espaço vetorial com produto interno sobre $\mathbb{C}$. Então existe uma base ortonormal $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ para V tal que*

$$T(\mathbf{u}_i) = \lambda_i \mathbf{u}_i$$

para todo $T \in G$ e $\lambda_i = \lambda_i(T)$.

Demonstração. Pelo Lema 1.5, existe $\mathbf{u}_1 \in V$ tal que

$$T(\mathbf{u}_1) = \lambda_1(T)\mathbf{u}_1$$

para todo $T \in G$. Seja

$$W_1 = \{\mathbf{v} \in V : \langle \mathbf{v}, \mathbf{u}_1 \rangle = 0\}.$$

Como $\dim W_1 = n-1$ e W_1 é invariante com relação a todo $T \in G$ temos, pelo Lema 1.4, que existe $\mathbf{u}_2 \in W_1$tal que

$$T(\mathbf{u}_2) = \lambda_2(T)\mathbf{u}_2$$

para todo $T \in G$. Seja

$$W_2 = \{\mathbf{v} \in V : \langle \mathbf{v}, \mathbf{v}_i \rangle = 0, i = 1, 2\}.$$

Como $\dim W_2 = n-2$ e W_2 é invariante com relação a todo $T \in G$ temos, pelo Lema 1.4, que existe $\mathbf{u}_3 \in W_2$ tal que

$$T(\mathbf{u}_3) = \lambda_3(T)\mathbf{u}_3$$

para todo $T \in G$. Proseguindo assim, obtemos uma base de vetores orto gonais $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ formada de autovetores comuns a todo $T \in G$. Como estes vetores podem ser normalizados temos o resultado. ■

Corolário 1.2 *Seja G um subgrupo normal abeliano finito (infinito) de o peradores de $\mathcal{L}(V,V)$, onde V é um espaço vetorial com produto interno sobre $\mathbb{R}$. Então existe uma base canônica ortonormal*

$$\{\mathbf{u}_1, \mathbf{v}_1, \mathbf{u}_2, \mathbf{v}_2, \ldots, \mathbf{u}_q, \mathbf{v}_q, \mathbf{u}_{2q+1}, \ldots, \mathbf{u}_n\}$$

para V tal que

$$\begin{cases} T(\mathbf{u}_k) = \mu_k(T)\mathbf{u}_k - \nu_k(T)\mathbf{v}_k, \\ T(\mathbf{v}_k) = \nu_k(T)\mathbf{u}_k + \mu_k(T)\mathbf{v}_k, \ k = 1, \ldots, q, \\ T(\mathbf{u}_l) = \mu_l(T)\mathbf{u}_l, \ l = 2q+1, \ldots, n. \end{cases}$$

para todo $T \in G$.

Demonstração: Como $\dim \mathcal{L}(V,V) = n^2$, podemos escolher um número finito de operadores normais que são linearmente independentes, digamos $T_1, T_2, \ldots T_k$. Façamos a imersão de V em $\widetilde{V}$. Então, pelo Teorema 1.7, existe uma base ortonormal $\{\mathbf{z}_1, \ldots, \mathbf{z}_n\}$ para $\widetilde{V}$ tal que

$$T_j(\mathbf{z}_i) = \lambda_i(T_j)\mathbf{z}_i$$

Seja

$$T = \alpha_1 T_1 + \alpha_2 T_2 + \cdots, \alpha_i \in \mathbb{R}$$

Então, T é um operador normal real em $\widetilde{V}$ e

$$\begin{aligned} T(\mathbf{z}_j) &= \lambda_j \mathbf{z}_j, \\ \lambda_j &= \alpha_1 \lambda_j(T_1) + \alpha_2 \lambda_j(T_2) + \cdots \end{aligned} \tag{1.3}$$

Como os autovalores de T são formas lineares em α_i e T é real, temos que estas formas podem ser fatoradas em pares de complexos conjugados e uns reais; com uma reenumeração,

se necessário, de todos os autovalores, obtemos que

$$\begin{aligned} \lambda_{2k-1} &= \mu_k + i\nu_k, \\ \lambda_{2k} &= \mu_k - i\nu_k,\ k = 1, \ldots, q, \\ \lambda_l &= \mu_l,\ l = 2q+1, \ldots, n, \end{aligned}$$

onde μ_k, ν_k e μ_l são formas linear reais em α_i.

Podemos assumir, na Equação (1.3), que os vetores $\mathbf{z}_{2k-1}$ e $\mathbf{z}_{2k}$ são conjugados complexos e os $\mathbf{z}_l$ reais:

$$\begin{aligned} \mathbf{z}_{2k-1} &= \mathbf{u}_k + i\mathbf{v}_k, \\ \mathbf{z}_{2k} &= \mathbf{u}_k - i\mathbf{v}_k,\ k = 1, \ldots, q, \\ \mathbf{z}_l &= \mathbf{u}_l,\ l = 2q+1, \ldots, n. \end{aligned}$$

Não é difícil mostrar que o conjunto de vetores reais

$$\{\mathbf{u}_1, \mathbf{v}_1, \mathbf{u}_2, \mathbf{v}_2, \ldots, \mathbf{u}_q, \mathbf{v}_q, \mathbf{u}_{2q+1}, \ldots, \mathbf{u}_n\}$$

da Equação (1.3) forma uma base ortonormal de V. Nesta base canônica,

$$\begin{cases} T(\mathbf{u}_k) = \mu_k \mathbf{u}_k - \nu_k \mathbf{v}_k, \\ T(\mathbf{v}_k) = \nu_k \mathbf{v}_k + \mu_k \mathbf{u}_k,\ k = 1, \ldots, q, \\ T(\mathbf{u}_l) = \mu_l \mathbf{u}_l,\ l = 2q+1, \ldots, n. \end{cases}$$

Desde que todos os operadores do dado conjunto são obtidos de T para valores especiais de α_i, a base da Equação (1.3), não depende destes parâmetros, é uma base canônica comum ■

1.5 Algoritmo

O objetivo desta seção é transformar o Corolário 1.2 em um algoritmo construtivo para obter uma matriz $\mathbf{O}$ ortogonal de ordem m tal que:

$$\mathbf{OCO}^t = \begin{cases} \text{diag}(1, \mathbf{A}_1, \ldots, \mathbf{A}_{k-1}) & \text{se } m = 2k-1, \\ \text{diag}(1, -1, \mathbf{A}_1, \ldots, \mathbf{A}_{k-1}) & \text{se } m = 2k, \end{cases}$$

onde

$$\mathbf{A}_l = \begin{bmatrix} \cos(\frac{2l\pi}{m}) & -\operatorname{sen}(\frac{2l\pi}{m}) \\ \operatorname{sen}(\frac{2l\pi}{m}) & \cos(\frac{2l\pi}{M}) \end{bmatrix},$$

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

com $\mathbf{C}$ uma matriz circulante e $G = \langle \mathbf{C} \rangle$.

Vamos considerar primeiro o caso em que $|G| = m$ ímpar.

1. Sejam $\varepsilon = \exp \frac{2\pi i}{m}$ e $\overline{\varepsilon} = \overline{\exp \frac{2\pi i}{m}}$;

2. Considere a matriz quadrada $\mathbf{Q}$ de ordem m

$$\mathbf{Q} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \varepsilon & \varepsilon^2 & \cdots & \varepsilon^{2(k-1)} \\ 1 & \overline{\varepsilon} & \overline{\varepsilon}^2 & \cdots & \overline{\varepsilon}^{2(k-1)} \\ 1 & \varepsilon^2 & \varepsilon^4 & \cdots & \varepsilon^{4(k-1)} \\ 1 & \overline{\varepsilon}^2 & \overline{\varepsilon}^4 & \cdots & \overline{\varepsilon}^{4(k-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \varepsilon^{v-1} & \varepsilon^{2(k-1)} & \cdots & \varepsilon^{2(k-1)^2} \\ 1 & \overline{\varepsilon}^{k-1} & \overline{\varepsilon}^{2(k-1)} & \cdots & \overline{\varepsilon}^{2(k-1)^2} \end{bmatrix};$$

3. Considere a matriz quadrada $\mathbf{T}$ de ordem m

$$\mathbf{T} = \operatorname{diag}\left(1, \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}, \ldots, \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}\right);$$

4. Considere a matriz quadrada $\mathbf{B}$ de ordem m

$$\mathbf{B} = m \operatorname{diag}(1, 2, 2, \ldots, 2).$$

Então a matriz $\mathbf{O}$ é dada por:

$$\mathbf{O} = \mathbf{B}^{-\frac{1}{2}}\mathbf{T}\mathbf{Q}$$

Demonstração Usando o fato de que $\varepsilon^m = 1$ e $\overline{\varepsilon} = \varepsilon^{m-1}$ verificar-se que

$$\mathbf{QCQ}^t = m\,\mathrm{diag}\left(1, \begin{bmatrix} 0 & \varepsilon \\ \overline{\varepsilon} & 0 \end{bmatrix}, \begin{bmatrix} 0 & \overline{\varepsilon}^2 \\ \overline{\varepsilon}^2 & 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 & \varepsilon^{k-1} \\ \overline{\varepsilon}^{k-1} & 0 \end{bmatrix}\right)$$

Como $\mathbf{T}$ e $\mathbf{QCQ}^t$ exibem uma forma pseudo-diagonal, para calcular

$$\mathbf{T}(\mathbf{QCQ}^t)\mathbf{T}^t$$

é suficiente considerar o produto

$$\begin{bmatrix} 1 & 1 \\ i & -1 \end{bmatrix}\begin{bmatrix} 0 & \varepsilon^q \\ \overline{\varepsilon}^q & 0 \end{bmatrix}\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} = \begin{bmatrix} 2\cos\dfrac{2\pi q}{m} & 2\,\mathrm{sen}\,\dfrac{2\pi q}{m} \\ -2\,\mathrm{sen}\,\dfrac{2\pi q}{m} & 2\cos\dfrac{2\pi q}{m} \end{bmatrix}$$

Assim,

$$\mathbf{T}(\mathbf{QOQ}^t)\mathbf{T}^t = m\,\mathrm{diag}\left(\begin{array}{c} 1, \begin{bmatrix} 2\cos\dfrac{2\pi}{m} & 2\,\mathrm{sen}\,\dfrac{2\pi}{m} \\ -2\,\mathrm{sen}\,\dfrac{2\pi}{m} & 2\cos\dfrac{2\pi}{m} \end{bmatrix}, \ldots; \\ \begin{bmatrix} 2\cos\dfrac{2\pi(k-1)}{m} & 2\,\mathrm{sen}\,\dfrac{2\pi(k-1)}{m} \\ -2\,\mathrm{sen}\,\dfrac{2\pi(k-1)}{m} & 2\cos\dfrac{2\pi(k-1)}{m} \end{bmatrix} \end{array}\right)$$

Multiplicando $\mathbf{T}(\mathbf{QOQ}^t)\mathbf{T}^t$ à esquerda por $\mathbf{B}^{-\frac{1}{2}}$ e à direita por $(\mathbf{B}^{-\frac{1}{2}})^t$ obtemos a matriz desejada. Seja

$$\mathbf{O} = \mathbf{B}^{-\frac{1}{2}}\mathbf{TQ}$$

Então $\mathbf{O}$ é ortogonal. De fato, é fácil verificar que

$$(\mathbf{TQ})(\mathbf{TQ})^t = \mathbf{B}.$$

Logo,

$$(\mathbf{B}^{-\frac{1}{2}}\mathbf{TQ})(\mathbf{B}^{-\frac{1}{2}}\mathbf{TQ})^t = \mathbf{B}^{-\frac{1}{2}}\mathbf{TQQ}^t\mathbf{T}^t(\mathbf{B}^{-\frac{1}{2}})^t = \mathbf{B}^{-\frac{1}{2}}\mathbf{B}(\mathbf{B}^{-\frac{1}{2}})^t = \mathbf{I}.$$

Portanto, $\mathbf{O}$ é ortogonal.

Finalmente, no caso $|G| = m$ par, faz-se

$$\begin{aligned}
\mathbf{Q} &= \begin{bmatrix}
1 & 1 & 1 & 1 & \dots & 1 \\
1 & -1 & 1 & -1 & \dots & -1 \\
1 & \varepsilon & \varepsilon^2 & \varepsilon^3 & \dots & \varepsilon^{2k-1} \\
1 & \overline{\varepsilon} & \overline{\varepsilon}^2 & \overline{\varepsilon}^3 & \dots & \overline{\varepsilon}^{2k-1} \\
\dots & \dots & \dots & \dots & \dots & \dots \\
1 & \varepsilon^k & \dots & \dots & \dots & \varepsilon^{2k^2-1} \\
1 & \overline{\varepsilon}^k & \dots & \dots & \dots & \overline{\varepsilon}^{2k^2-1}
\end{bmatrix}, \\
\mathbf{T} &= \operatorname{diag}\left(1, 1, \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}, \dots, \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}\right), \\
\mathbf{B} &= m \operatorname{diag}(1, 1, 2, \dots, 2)
\end{aligned}$$

e se procede de modo análogo para obter $\mathbf{O}$. ■

Capítulo 2

Códigos de Grupo

Neste capítulo apresentaremos algumas definições e reultados básicas sobre representação de grupos, códigos de grupo e regiões fundamentais, o leitor interessado em mais detalhes pode consultar [3, 8].

2.1 Representação de Grupos

Seja V um espaço vetorial sobre F. Então o conjunto de todos os ope radores lineares invertíveis sobre V será denotado por

$$GL(V).$$

Uma *representação* de um grupo finito G é um homomorfismo

$$\rho : G \longrightarrow GL(V), \rho(ab) = \rho(a)\rho(b), \forall a, b \in G.$$

Segue desta definição que

$$\rho(e) = I, \rho(a^{-1}) = (\rho(a))^{-1}, \forall a \in G$$

Neste caso, dizemos que V é o *espaço representação* e a *dimensão* da re presentação ρ é a dimensão de V. Se ρ e φ são representações do grupo G com espaços representação V_1 e V_2, respectivamente, então dizemos que ρ e φ são representação *equivalente* ou *isomorfa* se existir um isomorfismo T de V_1 sobre V_2, tal que

$$T\rho(a) = \varphi(a)T, \forall a \in G.$$

Sejam

$$M_n(F) = \{\mathbf{A} : \mathbf{A} \text{ é uma matriz de ordem } n \text{ sobre } F\}$$

e

$$GL_n(F) = \{\mathbf{A} \in M_n(F) : \det(\mathbf{A}) \neq 0\}.$$

Então fixada uma base para V sobre F podemos definir um isomorfismo entre $GL(V)$ e $GL_n(F)$ associando cada elemento de $GL(V)$ a sua matriz na base dada em $GL_n(F)$.

Uma representação matricial de G sobre F de grau n é um homomorfismo $\phi : G \longrightarrow GL_n(F)$. Assim, se

$$T : GL_n(F) \longrightarrow GL(V)$$

é um isomorfismo, então

$$T\phi : G \longrightarrow GL(V)$$

é uma representação de G. De modo análogo, a cada representação de G,

$$\phi : G \longrightarrow GL(V),$$

podemos associar uma representação matricial

$$T^{-1}\phi : G \longrightarrow GL_n(F).$$

Por causa disto, não faremos distinção explícita entre representação e representação matricial. Seja

$$\phi : G \longrightarrow GL_n(F)$$

definida por $\phi(a) = \mathbf{I}$, para todo $a \in G$. Então ϕ é claramente uma representação de G, e é chamada de *representação unitária* quando $n = 1$.

Observação 2.1 *Uma representação de dimensão* 1 *de um grupo* G *é um homomorfismo* $\psi : G \longrightarrow F^*$.

Exemplo 2.1 (A representação natural) *Se* $G = S_n$*, então existe uma* representação natural *em termos de matrizes de permutação. Denotaremos esta representação por* ρ_N*. Seja*

$$\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$$

uma base para V*. Definimos a transformação linear de* V *em* V *por*

$$\rho_N(\sigma)(\mathbf{v}_i) = \mathbf{v}_{\sigma(i)}, \sigma \in G.$$

Exemplo 2.2 (A representação regular) *Sejam G um grupo de ordem n e V um espaço vetorial de dimensão n com uma base*

$$\{\mathbf{v}_a : a \in G\}.$$

Definimos uma transformação linear de V em V por

$$\rho_R(a)\mathbf{v}_h = \mathbf{v}_{ah}, a, h \in G.$$

Isto é a representação regular *de G. Em termos de matrizes, é conviniente ordenar os elementos $a_i \in G, i = 1, 2, ..., n$. Então*

$$\boldsymbol{\rho}_R(a_k) = \begin{cases} 1 & se,\ a_i = a_k a_j \\ 0 & se,\ a_i \neq a_k a_j \end{cases}$$

e isto produz uma representação matricial de G por matrizes de permutação.

Sejam ρ uma representação do grupo G e V seu espaço representação. Dizemos que um subespaço W de V é *invariante* sob ρ se

$$\rho(a)(\mathbf{w}) \in W, \forall \mathbf{w} \in W, \text{ e } a \in G.$$

Logo, a restrição de ρ a W é também uma representação de G com espaço representação W. Se $\dim(V) = n$ e $\dim(W) = k$ com $0 < k < n$, então é claro que a matriz correspondente a esta representação pode ser escrita na forma

$$\boldsymbol{\rho}(a) = \begin{bmatrix} \boldsymbol{\gamma}(a) & \boldsymbol{\alpha}(a) \\ \mathbf{O} & \boldsymbol{\beta}(a) \end{bmatrix},$$

onde $\gamma = \rho|_W$ é uma representação k-dimensional com espaço de representação W. Essa forma matricial é obtida primeiro escolhendo uma base para W e estendendo para uma base de V.

Seja ρ uma representação de G com espaço representação V. Se V não contém subespaço invariante próprio W, dizemos que ρ é uma *representação irredutível*. Caso contrário, ρ é dita *representação redutível*.

Dizemos que uma representação ρ de G é *completamente redutível*, se

$$V = W_1 \oplus \cdots \oplus W_r,$$

onde $\rho_i = \rho|_{W_i}$ é irredutível para cada $i = 1, \ldots, r$. Neste caso, escrevemos

$$\rho = \rho_1 \oplus \cdots \oplus \rho_r.$$

Note que, todas essas definições tem uma interpretação matricial e que as noções irredutíveis, redutível e completamente redutível são preservadas por similaridade.

Em termos de matrizes, uma representação matricial ρ de G de grau n é *redutível* se existir uma matriz não singular $\mathbf{M}$, com coeficientes no corpo F tal que:

$$\mathbf{M}^{-1}\boldsymbol{\rho}(a)\,\mathbf{M} = \begin{bmatrix} \boldsymbol{\phi}(a) & \boldsymbol{\varphi}(a) \\ \mathbf{O} & \boldsymbol{\psi}(a) \end{bmatrix}, \forall a \in G,$$

onde $\boldsymbol{\phi}$ e $\boldsymbol{\psi}$ são os *constituintes* de $\boldsymbol{\rho}$. Uma representação matricial é *irredutível* se não for redutível.

Uma representação matricial $\boldsymbol{\rho}$ de G de grau n é *completamente redutível* se existir uma matriz não singular $\mathbf{M}$, com coeficientes em F tal que:

$$\begin{aligned} \mathbf{M}^{-1}\boldsymbol{\rho}(a)\,\mathbf{M} &= \begin{bmatrix} \boldsymbol{\rho}_1(a) & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \boldsymbol{\rho}_2(a) & \cdots & \mathbf{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{O} & \mathbf{O} & \cdots & \boldsymbol{\rho}_r(a) \end{bmatrix} \\ &= \boldsymbol{\rho}_1(a) \oplus \cdots \oplus \boldsymbol{\rho}_r(a), \forall a \in G, \end{aligned}$$

onde cada constituinte $\boldsymbol{\rho}_i(a)$ é irredutível.

Observação 2.2 *Note que, a noção de irredutibilidade depende do corpo F que estar sendo considerado. Por exemplo, seja $G = \langle a \rangle$ um grupo cíclico de ordem 4 e defina*

$$\boldsymbol{\rho} : G \longrightarrow GL_2(F) \text{ por } \boldsymbol{\rho}(a) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Então, se $F = \mathbb{R}$, então $\boldsymbol{\rho}$ é irredutível, pois as raízes do polinômio característico associado a matriz $\boldsymbol{\rho}(a)$ são $i, -i \in \mathbb{C}$. No entanto, se $F = \mathbb{C}$, então $\boldsymbol{\rho}$ é redutível.

A seguir provaremos o Teorema de Maschke que vale para FG-módulos, onde F é um corpo de característica zero ou com característica não dividindo a ordem do grupo finito G. Demonstraremos apenas para espaço vetorial.

Teorema 2.1 (Maschke) *Sejam G um grupo e F um corpo, onde a característica de F é igual a zero ou não divide a ordem do grupo G. Então, toda representação matricial de G é completamente redutível.*

Demonstração. Seja $\boldsymbol{\rho}$ uma representação matricial de G de grau n. A demonstração é por indução sobre n.

Se $n = 1$, então $\boldsymbol{\rho}$ é irredutível e não há nada para demonstrar.

Suponhamos que o resultado seja válido para toda representação matricial de G com grau $< n$. Se $\boldsymbol{\rho}$ é irredutível o teorema está demonstrado. Assim podemos assumir $\boldsymbol{\rho}$ é redutível, isto é,

$$\boldsymbol{\rho}(a) = \begin{bmatrix} \boldsymbol{\phi}(a) & \boldsymbol{\varphi}(a) \\ \mathbf{O} & \boldsymbol{\psi}(a) \end{bmatrix}, \forall a \in G.$$

Como

$$\boldsymbol{\rho}(ab) = \boldsymbol{\rho}(a)\,\boldsymbol{\rho}(b), \forall a, b \in G$$

temos que

$$\begin{aligned} \boldsymbol{\phi}(ab) &= \boldsymbol{\phi}(a)\,\boldsymbol{\phi}(b), \\ \boldsymbol{\psi}(ab) &= \boldsymbol{\psi}(a)\,\boldsymbol{\psi}(b), \\ \boldsymbol{\varphi}(ab) &= \boldsymbol{\phi}(a)\,\boldsymbol{\varphi}(b) + \boldsymbol{\varphi}(a)\,\boldsymbol{\psi}(b), \forall a, b \in G. \end{aligned} \tag{2.1}$$

Multiplicando à direita por $\boldsymbol{\psi}(b^{-1})$ a última equação de (2.1), obtemos que

$$\begin{aligned} \boldsymbol{\varphi}(ab)\,\boldsymbol{\psi}\left(b^{-1}\right) &= [\boldsymbol{\varphi}(ab)\,\boldsymbol{\psi}((ab)^{-1})]\boldsymbol{\psi}(a) \\ &= \boldsymbol{\phi}(a)\,\boldsymbol{\varphi}(b)\,\boldsymbol{\psi}\left(b^{-1}\right) + \boldsymbol{\varphi}(a), \forall a, b \in G. \end{aligned}$$

Somando em $b \in G$ obtemos que,

$$\left[\sum_{c \in G} \boldsymbol{\varphi}(c)\,\boldsymbol{\psi}\left(c^{-1}\right)\right]\boldsymbol{\psi}(a) = \boldsymbol{\phi}(a)\left[\sum_{b \in G} \boldsymbol{\varphi}(b)\,\psi\left(b^{-1}\right)\right] + |G|\,\boldsymbol{\varphi}(a).$$

Se a característica de F é zero ou um número primo p não dividindo $|G|$, podemos dividir por $|G|$ para obtermos

$$\boldsymbol{\varphi}(a)\mathbf{M} = \boldsymbol{\phi}(a)\,\mathbf{M} + \varphi(a), \forall a \in G, \tag{2.2}$$

onde $\mathbf{M}$ é a matriz retangular definida por:

$$\mathbf{M} = \frac{1}{|G|}\sum_{c \in G} \boldsymbol{\varphi}(c)\,\boldsymbol{\psi}\left(c^{-1}\right).$$

Seja

$$\mathbf{A} = \begin{bmatrix} \mathbf{I} & \mathbf{M} \\ \mathbf{O} & \mathbf{I} \end{bmatrix},$$

uma matriz não singular. Então, para cada $a \in G$ temos, pela Equação (2.2), que

$$\mathbf{A}^{-1}\boldsymbol{\rho}(a)\,\mathbf{A} = \boldsymbol{\phi}(a) \oplus \boldsymbol{\psi}(a), \forall g \in G.$$

Por hipótese de indução, $\boldsymbol{\phi}$ e $\boldsymbol{\psi}$ são completamente redutíveis. Portanto, $\boldsymbol{\rho}$ é completamente redutível. ■

Observação 2.3 *O Teorema anterior tem uma importante implicação: se ρ é uma representação com espaço representação V e um subespaço W invariante sobre ρ, então existe uma base de V tal que a representação matricial pode ser expressa na forma*

$$\boldsymbol{\rho}(a) = \begin{bmatrix} \boldsymbol{\gamma}(a) & 0 \\ 0 & \boldsymbol{\beta}(a) \end{bmatrix},$$

e ambos $\gamma(a)$ e $\beta(a)$ são também representações de G. Quando a representação pode assim ser reduzida, escrevemos

$$\rho(a) = \gamma(a) \oplus \beta(a), a \in G.$$

O *caráter* da matriz $\boldsymbol{\rho}(a)$ associada a representação ρ é definido como sendo o traço da matriz $\boldsymbol{\rho}(a)$. Em símbolos

$$\chi(a) = \mathrm{tr}(\boldsymbol{\rho}(a))$$

Observação 2.4 *Note que o caráter da representação natural do Exemplo* 2.1 *é igual ao número de pontos fixados por $\sigma \in S_n$. De fato, sejam $\mathbf{e}_1, \ldots, \mathbf{e}_n$ as colunas da matriz identidade $\mathbf{I}$. Se $\sigma(i) = i$, então $\rho_N(\sigma)\mathbf{e}_i = \mathbf{e}_{\sigma(i)} = \mathbf{e}_i$. Portanto,* $\mathrm{Fix}(\sigma) = \chi_N(\sigma)$.

Teorema 2.2 *Sejam ρ uma representação de G com grau n e caráter χ. Então:*

1. $\chi(e) = \dim \rho$;
2. χ *é uma função classe de* G;
3. $\chi(a^{-1}) = \overline{\chi}(a)$;
4. *Se χ_1 e χ_2 são caracteres das representações ρ e σ, então o caráter de $\rho \oplus \sigma$ é $\chi_1 + \chi_2$.*

Demonstração.1. Para qualquer representação matricial $\boldsymbol{\rho}(e) = \mathbf{I}$. Logo,

$$\chi(e) = \mathrm{tr}(\boldsymbol{\rho}(e)) = n = \dim \rho.$$

2. Devemos mostrar que, para cada $a \in G$ fixado temos que

$$\chi(bab^{-1}) = \chi(a), \forall b \in G.$$

De fato, basta notar que

$$\mathrm{tr}(\boldsymbol{\rho}(a)) = \mathrm{tr}(\boldsymbol{\rho}(b)\boldsymbol{\rho}(a)\boldsymbol{\rho}(b)^{-1}).$$

3. Se $\lambda_1, \ldots, \lambda_n$ são os elementos da diagonal principal de $\boldsymbol{\rho}(a)$, então

$$\begin{aligned} \chi(a^{-1}) &= \mathrm{tr}(\boldsymbol{\rho}(a^{-1})) \\ &= \mathrm{tr}(\boldsymbol{\rho}(a)^{-1}) \\ &= \sum_{i=1}^{n} \lambda_i^{-1} \\ &= \sum_{i=1}^{n} \overline{\lambda}_i = \overline{\chi}(a) \end{aligned}$$

4. Seja $\phi = \rho \oplus \sigma$. Então a representação matricial de ϕ é dada por

$$\boldsymbol{\phi}(a) = \begin{bmatrix} \boldsymbol{\rho}(a) & 0 \\ 0 & \boldsymbol{\sigma}(a) \end{bmatrix}, \forall a \in G.$$

Portanto, o caráter de $\rho \oplus \sigma$ é $\chi_1 + \chi_2$. ■

Definimos um *produto interno* sobre dois *caracteres* χ_1 e χ_2 de G por

$$\begin{aligned} \langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_{a \in G} \chi_1(a)\overline{\chi}_2(a) \\ &= \frac{1}{|G|} \sum_{a \in G} \chi_1(a)\chi_2(a^{-1}). \end{aligned}$$

Teorema 2.3 *Sejam ρ uma representação de G com grau n e caráter χ. Então*:

1. *Uma representação ρ é irredutível se, e somente se, $\langle \chi, \chi \rangle = 1$;*

2. *Se ρ_i e ρ_j são representações irredutível, então $\langle \chi_i, \chi_j \rangle = \delta_{ij}$;*

3. *Em qualquer decomposição de uma representação arbitrária ρ em uma soma direta de representações irredutíveis, o número de somandos equi valente na representação*

irredutível ρ_i é dado por $\langle \chi, \chi_i \rangle$, onde ρ tem caráter χ. Assim, duas representações com o mesmo caráter são equivalentes e o número de representações na soma direta que são equivalentes a ρ_i, o qual chamamos a multiplicidade m_i de ρ_i em ρ, é independente da decomposição particular;

4. *Se a multicidade de ρ_i em ρ é m_i, então $\langle \chi, \chi \rangle = \sum_i m_i^2$.* ■

Como $ah \neq h$, se $a \neq e$, temos que os elementos de $\boldsymbol{\rho}_R(a)$ na diagonal principal são todos nulos. Logo, o caráter da representação regular $\boldsymbol{\rho}_R$, denotado por χ_R, é dado por

$$\chi_R(a) = \begin{cases} |G| & \text{se } a = e \\ 0 & \text{se } a \neq e \end{cases}.$$

Se χ_i é o caráter de uma representação irredutível de dimensão n_i, então

$$\begin{aligned} \langle \chi_R, \chi_i \rangle &= \frac{1}{|G|} \sum_{a \in G} \chi_R(a) \chi_i(a^{-1}) \\ &= \frac{1}{|G|} |G| \, \chi_i(e) = n_i. \end{aligned}$$

Assim, qualquer representação irredutível de dimensão n_i tem multiplicidade n_i na representação regular. Contudo, isto implica que existe um número finito de representações irredutíveis não equivalentes de G, $\rho_1, \ldots, \rho_k$ de dimensão $n_1, \ldots, n_k$, tal que

$$\sum_{l=1}^{k} n_i^2 = |G| \, .$$

Teorema 2.4 *O número de representações irredutíveis e não equivalentes de um grupo G sobre $\mathbb{C}$ é igual ao número de classes de conjungação em G.* ■

Sejam G um grupo, H um subgrupo normal de G e ρ uma representação de $\dfrac{G}{H}$ com espaço de representação V. Definimos uma representação σ sobre G por

$$\begin{aligned} \sigma : \; & G \to GL(V) \\ & a \mapsto \rho(bH) \end{aligned}$$

se $a \in bH$. De fato. Sejam $a_1 = b_1 h_1$ e $a_2 = b_2 h_2$, onde $h_1, h_2 \in H$ e b_1, b_2 são representantes de classes laterais à esquerda de H em G. Então

$$\begin{aligned} \sigma(a_1) \, \sigma(a_2) &= \rho(b_1 H) \, \rho(b_2 H) \\ &= \rho(b_1 b_2 H) = \sigma(a_1 a_2), \end{aligned}$$

pois $a_1a_2 = b_1h_1b_2h_2$ e

$$\begin{aligned} a_1a_2 &= b_1(h_1b_2)h_2 \\ &= b_1(b_2h_3)h_2 \\ &= b_1b_2(h_3h_2). \end{aligned}$$

Assim, uma representação do grupo quociente é também uma representação do grupo e a definição é independente dos representantes de classe laterais. Note que, toda representação irredutível de um grupo abeliano finito é de dimensão 1

De fato. Seja $\rho = \rho_1 \oplus \cdots \oplus \rho_k$. a representação de um grupo abeliano finito G, onde os ρ_i são representações irredutíveis. Se a multiplicidade de ρ_i em ρ é n_i, então pelos Teoremas 2.3 e 2.4 temos que

$$\sum_{i=1}^{|G|} n_i^2 = |G|\,,$$

pois existem $|G|$ classes de conjugação, o único conjunto de inteiros positivos satisfazendo esta relação é

$$n_i = 1, i = 1, \ldots, |G|.$$

Teorema 2.5 *O número de representações irredutíveis de dimensão* 1 *de um grupo* G *é igual a* $[G : G']$

Demonstração. Segue da observação acima que toda representação irredutível de $\dfrac{G}{G'}$ é uma representação irredutível de G de dimensão 1, pois $\dfrac{G}{G'}$ é abeliano.

Reciprocamente, suponhamos que ρ é uma representação irredutível de G de dimensão 1. Neste caso, temos que

$$\rho(a) = \chi(a), \forall a \in G.$$

Portanto,

$$\chi(a_1^{-1}a_2^{-1}a_1a_2) = \chi(a_1^{-1})\chi(a_2^{-1})\chi(a_1)\chi(a_2) = 1.$$

Logo, $\chi(a) = 1, \forall a \in G'$. Assim, ρ é uma representação irredutível de dimensão 1 sobre $\dfrac{G}{G'}$ e podemos concluir que o número de representações irredutíveis de G de dimensão 1 é $[G : G']$. ■

Seja Ω um G-conjunto. Um subconjunto Γ de Ω é um *constituinte transitivo* de G se as seguintes condições são satisfeitas:

1. $\sigma x \in \Gamma$, para todo $\sigma \in G$ e $x \in \Gamma$;

2. Se $x, y \in \Gamma$, então existe $\sigma \in G$ tal que $\sigma x = y$.

Lema 2.1 *Seja Ω um G-conjunto, com k constituintes transitivos $\Gamma_1, \ldots, \Gamma_k$ e $|\Gamma_i| = m_i, i = 1, \ldots, k$. Então*

$$\sum_{\sigma \in G} \chi_N(\sigma) = k\,|G|$$

e ρ_N contém a representação identidade k vezes.

Demonstração. Pela Observação 2.4 temos que $\chi_N(\sigma) = \mathrm{Fix}(\sigma)$. Assim, pela Proposição 1.5, temos que

$$\sum_{\sigma \in G} \chi_N(\sigma) = \sum_{\sigma \in G} \mathrm{Fix}(\sigma) = k\,|G|\,.$$

■

Lema 2.2 *Sejam Ω um G-conjunto transitivo de grau n e H um subgrupo de G fixando $x_1 \in \Omega$. Então*

$$\sum_{\sigma \in G} \chi_N^2(\sigma) = k\,|G|\,,$$

onde k é o número constituintes de H.

Demonstração. Pela Observação 2.4 temos que $\chi_N(\sigma) = \mathrm{Fix}(\sigma)$. Assim, pela Proposição 1.13, temos que

$$\sum_{\sigma \in G} \chi_N^2(\sigma) = \sum_{\sigma \in G} \mathrm{Fix}(\sigma)^2 = k|G|.$$

■

Teorema 2.6 *Seja Ω um G-conjunto duplamente transitivo de grau n. Então a ρ_N de G é à soma direta da representação unitária e uma representação irredutível de dimensão $(n-1)$.*

Demonstração. Seja H um subgrupo de G fixando x_1. Como Ω é duplamente transitivo temos que G tem um constituinte e H tem dois

$$\{x_1\} \text{ e } \{x_2, \ldots, x_n\}.$$

Pelo Lema 2.2, temos que

$$\begin{aligned}\sum_{\sigma\in G}\chi_N^2(\sigma) &= 2\,|G| \\ &= \sum_{\sigma\in G}\chi_N(\sigma)\overline{\chi}_N(\sigma).\end{aligned}$$

Logo, se ρ_N tem a decomposição

$$\rho_N = m_1\rho_1 \oplus \cdots \oplus m_s\rho_s,$$

onde ρ_i é uma representação irredutível com caráter χ_i e multiplicidade m_i, então pelo Teorema 2.3,

$$\begin{aligned}2\,|G| &= \sum_{\sigma\in G}\left[\sum_{i=1}^{s} m_i\chi_i(\sigma)\cdot\sum_{i=1}^{s} m_i\overline{\chi}_i(\sigma)\right] \\ &= |G|\sum_{i=1}^{s} m_i^2.\end{aligned}$$

Pelo Lema 2.1, ρ_N contém a representação identidade uma vez. Assim, a única solução da equação

$$\sum_{i=1}^{s} m_i^2 = 2$$

é $m_1 = 1$ e $m_i = 1$, para algum $i = 1, \ldots, s$. Portanto,

$$\rho_N = \rho_1 \oplus \rho_i,$$

onde ρ_i é uma representação irredutível de dimensão $(n-1)$. ■

2.2 Região Fundamental

O objetivo desta seção é descrever uma construção que produz uma região fundamental para qualquer subgrupo finito do grupo das transfomações invertíveis de um espaço vetorial de dimensão finita.

Seja V um espaço vetorial de dimensão n sobre $\mathbb{R}$ equipado com o produto interno usual. A *norma quadrática* ou *peso Euclidiano* $N(\mathbf{x}) = ||\mathbf{x}||^2$ de um vetor $\mathbf{x} \in V$ é a soma dos quadrados de suas componentes, isto é,

$$N(\mathbf{x}) = \langle \mathbf{x}, \mathbf{x}\rangle = \mathbf{x}\cdot\mathbf{x}^t$$

A *distância Euclidiana quadrática* entre dois vetores $\mathbf{x}, \mathbf{y} \in V$ é a norma quadrática de sua diferença, isto é,

$$d^2(\mathbf{x}, \mathbf{y}) = N(\mathbf{x} - \mathbf{y}).$$

Fixado $\mathbf{x}_0 \in V$ e um número real $\varepsilon > 0$, o conjunto

$$S_\epsilon(\mathbf{x}_0) = \{\mathbf{x} \in V : d(\mathbf{x}, \mathbf{x}_0) = \varepsilon\}$$

é chamado a *esfera* de raio ε e centro $\mathbf{x}_0$ e o conjunto

$$B_\epsilon(\mathbf{x}_0) = \{\mathbf{x} \in V : d(\mathbf{x}, \mathbf{x}_0) < \varepsilon\}$$

é chamado a *bola aberta* de raio ε e centro $\mathbf{x}_0$.

Um subconjunto U de V é *aberto* se, e somente se, para cada $\mathbf{x} \in U$ existir $\varepsilon > 0$ tal que

$$B_\epsilon(\mathbf{x}) \subseteq U.$$

Note que, a interseção finita e a união de conjuntos abertos é aberto. Um subconjunto X de V é *fechado* se, e somente se, o seu complementar $U = V - X$ é aberto. Assim a intersecção e a união finita de conjuntos fechados é fechado.

Seja

$$\mathcal{F} = \{Y \subseteq V : X \subseteq Y \text{ e } Y \text{ é aberto em } V\}.$$

Então o conjunto

$$X^0 = \bigcup_{Y \in \mathcal{F}} Y$$

é chamado o *interior* de X. Seja

$$\mathcal{F}' = \{Y \subseteq V : X \subseteq Y \text{ e } Y \text{ é fechado em } V\}.$$

Então o conjunto

$$\overline{X} = \bigcap_{Y \in \mathcal{F}'} Y$$

é chamado o *fecho* de X. A *fronteira* de X em V é dada por

$$\partial X = \overline{X} - X^0.$$

Seja X um subconjunto de V fixado e $Y \subseteq X$. Então Y é chamado *aberto relativamente* a X se, e somente se, existir um aberto U de V tal que

$$Y = X \cap U.$$

Se $\dim V = n$, com $n \geq 2$, então podemos escolher dois vetores linearmente independentes $\mathbf{v}_1, \mathbf{v}_2 \in V$. Assim, para cada $\lambda \in \mathbb{R}$ definimos o subespaço de V

$$V_\lambda = \langle \mathbf{v}_1 + \lambda \mathbf{v}_2 \rangle^\perp.$$

Logo, se $\lambda \neq \mu$, então V_λ e V_μ são subespaço distintos de dimensão $n-1$, isto é, existem infinitos subespaço de V com dimensão $n-1$.

Proposição 2.1 *Se* $\dim V = n$*, então* V *não é uma união de um número finito de subespaços próprios.*

Demonstração. Se $\dim V = 1$, então$\{0\}$ é o único subespaço próprio de V. Suponhamos, como hipótese de indução, que o resultado seja válida para todo os espaços de dimensão $n-1$. Suponhamos, por absurdo, que

$$V = V_1 \cup \cdots \cup V_m,$$

onde cada V_i é um subespaço próprio de V e W um subespaço qualquer de V de dimensão $n-1$. Então

$$\begin{aligned} W &= W \cap V \\ &= W \cap (\bigcup_{i=1}^{m} V_i) \\ &= (W \cap V_i) \cup \cdots \cup (W \cap V_m). \end{aligned}$$

Por hipótese de indução $W = W \cap V_i$ para algum i. Como $\dim W = n-1$ temos que $\dim V_i \leq n-1$ e $W \subseteq V_i$ implica que $W = V_i$. Portanto, todo subespaço W de dimensão $n-1$ ocorre como um dos subespaços $V_1, \ldots, V_m$, o que é uma contradição, pois V tem infinitos subespaços de dimensão $n-1$. . ■

Seja G é um grupo finito de $O(V)$. Um subconjunto R de V é chamado uma *região fundamental* para G em V se as seguintes condições são satisfeitas:

1. R é fechado;
2. Se $I \neq T \in G$, então $R \cap T(R) \subseteq \partial R$;
3. $V = \bigcup\{T(R) : T \in G\}$.

Mais geralmente, se W é um subespaço de V invariante sob G, então um subconjunto R de W é uma região fundamental para G em W se as seguintes condições são satisfeitas:

1. R é fechado relativamente a W;

2. Se $I \neq T \in G$, então $R \cap T(R) \subseteq \partial R$;

3. $W = \bigcup\{T(R) : T \in G\}$.

Como cada $T \in G$ é uma transformação linear temos que o conjunto

$$V_T = \{\mathbf{x} \in V : T(\mathbf{x}) = \mathbf{x}\}$$

é um subespaço de V e $V_T = \ker(T - I)$. Se $T \neq I$, então V_T é um subespaço próprio de V. Logo, pela Proposição 2.1, temos que

$$V \neq \bigcup\{V_T : T \in G\}.$$

Assim, podemos escolher um ponto $\mathbf{x}_0 \in V - V_T$. Portanto, $G_{\mathbf{x}_0} = \{I\}$ e pela Proposição 1.3,

$$|O(\mathbf{x}_0)| = [G : G_{\mathbf{x}_0}] = |G|.$$

Se $G = \{T_0, T_1, \ldots, T_{M-1}\}$, com $T_0 = I$ e $T_i\mathbf{x}_0 = \mathbf{x}_i$, então

$$O(\mathbf{x}_0) = \{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{M-1}\}.$$

Se $i \neq 0$, então o segmento de reta ligando $\mathbf{x}_0$ a $\mathbf{x}_i$ é definido por

$$L_\lambda = \{\mathbf{x}_0 + \lambda(\mathbf{x}_i - \mathbf{x}_0) : 0 \leq \lambda \leq 1\}.$$

Logo, $\mathbf{x}_i - \mathbf{x}_0$ é um vetor paralelo a L_λ. Como o ponto médio é o vetor $\frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i)$ temos que

$$d(\mathbf{x}_0, \frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i)) = d(\mathbf{x}_i, \frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i)), \forall i = 0, \ldots, M-1.$$

Se $H_i = \langle \mathbf{x}_0 - \mathbf{x}_i \rangle^\perp$ é o hiperplano, então $\frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i) \in H_i$, pois

$$\begin{aligned} \langle \frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i), \mathbf{x}_0 - \mathbf{x}_i \rangle &= \frac{||\mathbf{x}_0||^2 - ||\mathbf{x}_i||^2}{2} \\ &= \frac{||\mathbf{x}_0||^2 - ||T_i\mathbf{x}_0||^2}{2} \\ &= \frac{||\mathbf{x}_0||^2 - ||\mathbf{x}_0||^2}{2} = 0. \end{aligned}$$

Portanto, H_i é o "bissector perpendicular" de L_λ.

Seja $\mathbf{x} \in V$. Então $\mathbf{x} \perp (\mathbf{x}_0 - \mathbf{x}_i)$ se, e somente se, $d(\mathbf{x}, \mathbf{x}_0) = d(\mathbf{x}, \mathbf{x}_i)$. Assim, como $T_i\mathbf{x}_0 = x_i$ temos que

$$H_i = \{\mathbf{x} \in V : d(\mathbf{x}, \mathbf{x}_0) = d(\mathbf{x}, \mathbf{x}_i)\}.$$

O conjunto

$$X_i = \{\mathbf{x} \in V : d(\mathbf{x}, \mathbf{x}_0) \leq d(\mathbf{x}, \mathbf{x}_i)\}, 1 \leq i \leq M-1.$$

é chamado *semi-espaço* de V determinado por H_i e pode ser pensado como o conjunto de todos os pontos que estão no mesmo lado de H_i como $\mathbf{x}_0$.

Teorema 2.7 *O conjunto*

$$R = \bigcap_{i=1}^{M-1} X_i$$

é uma região fundamental para G em V.

Demonstração. Como cada X_i é fechado temos que R é fechado. Se $T_i \neq I$, então

$$T_i(R) = T_i\left(\bigcap_{j=1}^{M-1} X_j\right)$$

ou

$$\begin{aligned} T_i(R) &= T_i(\{\mathbf{x} : d(\mathbf{x}, \mathbf{x}_0) \leq d(\mathbf{x}, \mathbf{x}_j), 1 \leq j \leq M-1\}) \\ &= \{T_i(\mathbf{x}) : d(T_i(\mathbf{x}), T_i(\mathbf{x}_0)) \leq d(T_i(\mathbf{x}), T_iT_j(\mathbf{x}_0)), 1 \leq j \leq M-1\} \\ &= \{\mathbf{y} : d(\mathbf{y}, \mathbf{x}_i) \leq (d\mathbf{y}, T_k(\mathbf{x}_0)), 0 \leq k \leq M-1, k \neq i\} \end{aligned}$$

pois

$$\{T_iT_j : 1 \leq j \leq M-1\} = G - \{T_i\}.$$

Assim,

$$T_i(X_j) = \{\mathbf{x} : d(\mathbf{x}, \mathbf{x}_i) \leq d(\mathbf{x}, \mathbf{x}_j)\}$$

para todos i e j, com $j \neq i$. Se $\mathbf{x} \in R \cap T_i(R)$, então

$$d(\mathbf{x}, \mathbf{x}_0) \leq d(\mathbf{x}, \mathbf{x}_i) \text{ e } d(\mathbf{x}, \mathbf{x}_i) \leq d(\mathbf{x}, \mathbf{x}_0).$$

Assim, $d(\mathbf{x}, \mathbf{x}_0) = d(\mathbf{x}, \mathbf{x}_i)$ e $R \cap T_i(R) \subseteq \partial R$, para todo $T_i \neq I$. Finalmente, se $\mathbf{x} \in V$, escolha um índice i para o qual $d(\mathbf{x}, \mathbf{x}_i)$ seja minima e, portanto, $d(\mathbf{x}, \mathbf{x}_i) \leq d(\mathbf{x}, \mathbf{x}_j)$ para todo j. Como

$$T_i(R) = \{\mathbf{x} : d(\mathbf{x}, \mathbf{x}_i) \leq d(\mathbf{x}, \mathbf{x}_j)\}, 0 \leq j \leq M-1.$$

temos que $\mathbf{x} \in T_i R$. Portanto,

$$V = \bigcup \{T_i(R) : 0 \leq i \leq M-1\}$$

e R é uma região fundamental para G em V. ■

2.3 Códigos de Grupo

Seja F um alfabeto com q símbolos, digamos

$$F = \{0, 1, \ldots, q-1\}.$$

Um *espaço de seqüências* é o conjunto

$$F^{\mathbb{I}} = \{(c_i)_{i \in I} : c_i \in F\},$$

onde $\mathbb{I} \subseteq \mathbb{Z}$. Quando

$$\mathbb{I} = \{1, 2, \ldots, n\}$$

denotamos $F^{\mathbb{I}}$ por F^n.

Um *código* C sobre F é qualquer subconjunto não vazio de $F^{\mathbb{I}}$. Um código C sobre F é um *código de bloco* de comprimento n se C um subconjunto de F^n. A *dimensão* de um código C é o número

$$k = \log_{|F|} |C|.$$

Note que k não é necessariamente inteiro.

Um código de bloco C de comprimento n e dimensão k é chamado (n, k)-*código*. Neste caso,

$$1 \leq |C| \leq |F|^n.$$

Um (M, n)-*código esférico* para o canal Gaussiano é uma coleção

$$C = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M\}$$

de vetores distintos em $\mathbb{R}^n$ tais que

1. C gera $\mathbb{R}^n$ como um espaço vetorial;

2. Todos os vetores de C tem a mesma norma.

Se o conjunto de vetores disponíveis para a transmissão é um (M, n)-código esférico, onde cada palavra código tem a mesma probabilidade de transmissão, então o critério de decodificação para a palavra recebida a qual minimiza a probabilidade média de erro é o de máxima verossimilhança. Isto é, a palavra recebida ótima decodifica $\mathbf{y}$ como os $\mathbf{x}_i$ que minimiza a distância Euclidiana

$$\{d(\mathbf{y}, \mathbf{x}_j)\}.$$

Sejam C e $\widehat{C}$ dois (M, n)-códigos esférico para o canal Gaussiano. Dizemos que C e $\widehat{C}$ são *equivalentes* se existir $\mathbf{O} \in O(n, \mathbb{R})$ tal que $\mathbf{O}C = \widehat{C}$.

Códigos equivalentes têm a mesma coleção de palavras com a mesma distância. Isto é, para cada $\mathbf{x}_i, \mathbf{x}_j \in \widehat{C}$,

$$d(\mathbf{x}_i, \mathbf{x}_j) = d(\mathbf{O}\mathbf{x}_i^t, \mathbf{O}\mathbf{x}_j^t), \forall \mathbf{O} \in O(n, \mathbb{R}).$$

Um (M, n)-*código de grupo* C é um (M, n)-código esférico tal que existe um subgrupo finito G de $O(n, \mathbb{R})$ e um vetor unitário $\mathbf{x} \in \mathbb{R}^n$ tal que

$$G\mathbf{x} = \{\mathbf{O}\mathbf{x}^t : \mathbf{O} \in G\} = C$$

ou, equivalentemente, C é a órbita de $\mathbf{x}$. O código C é dito gerado pelo *vetor inicial* $\mathbf{x}$ e o grupo G.

Observação 2.5 *Uma das vantagens de usar um código de grupo é que todas as palavras código tem a mesma probabilidade de erro e a mesma disposição de palavras código vizinhas.*

Teorema 2.8 *Seja C um (M, n)-código de grupo em $\mathbb{R}^n$. Então*:

1. *Todas as regiões fundamentais de C são congruentes;*

2. *Todas as palavras código têm a mesma probabilidade de erro;*

3. *O grupo G é isomorfo a um subgrupo transitivo do grupo das permutações em S_M.*

Demonstração. 1. Seja $C = \{\mathbf{x}_1, \ldots, \mathbf{x}_M\}$ um código de grupo em $\mathbb{R}^n$. Sejam $\mathbf{x}_i$ e $\mathbf{x}_j$

$\in C$ com $i \neq j$. Por hipótese, existe $\mathbf{O} \in G$ tal que $\mathbf{O}\mathbf{x}_i = \mathbf{x}_j$. Dado $\mathbf{x} \in R_i$, temos que:

$$\begin{aligned} N(\mathbf{O}\mathbf{x} - \mathbf{x}_j) &= N(\mathbf{O}\mathbf{x} - \mathbf{O}\mathbf{x}_i) \\ &= N(\mathbf{x} - \mathbf{x}_i) \\ &\leq N(\mathbf{x} - \mathbf{x}_k) \\ &= N(\mathbf{O}\mathbf{x} - \mathbf{O}\mathbf{x}_k) \\ &= N(\mathbf{O}\mathbf{x} - \mathbf{x}_l), \end{aligned}$$

onde $j \neq l$ e $\mathbf{x}_l = \mathbf{O}\mathbf{x}_k, \forall \mathbf{x}_k \in C$. Logo, $\mathbf{O}\mathbf{x} \in R_j$. Portanto, $R_j = \mathbf{O}(R_i)$, onde $\mathbf{O} \in G$.

2. Segue de 1.

3. Dados $\mathbf{x}_i$ e $\mathbf{x}_j \in C$. Então existe $\mathbf{O} \in G$ tal que $\mathbf{O}\mathbf{x}_i = \mathbf{x}_j$, isto é, $\mathbf{O}$ corresponde a uma permutação $\sigma \in S_M$ tal que $\sigma(i) = j$. Logo, G é isomorfo a um subgrupo transitivo de S_M , pois

$$C = \{\mathbf{O}x : \mathbf{O} \in G\},$$

para algum $\mathbf{x} \in C$. ■

Seja C um código de grupo. Então as palavras código que estão à mesma distância (mínima) de uma palavra código fixada de C são chamadas de *palavras código ativas* e os elementos do grupo que geram estas palavras códigos são chamados de *elementos ativos* do grupo.

Exemplo 2.3 *Considere um quadrado de centro na origem e lado* 2*. Então os pontos* $(-1, 1)$ *e* $(1, -1)$ *são palavras código ativas referentes a* $(1, 1)$*.*

Um (M, n)-código de grupo C cujos vetores terminam em um hiperplano de dimensão $(n - 1)$ é chamado um *código de grupo planar.*

Exemplo 2.4 *Seja*

$$C = \{(1, 0, 1), (1, 1, 0), (1, 0, -1), (1, -1, 0)\}.$$

Então C *é um código de grupo planar.*

Lema 2.3 *Sejam* C *um* (M, n)*-código esférico em* $\mathbb{R}^n$ *e*

$$\Delta C = \{\mathbf{x} - \mathbf{x}' : \mathbf{x}, \mathbf{x}' \in C\}.$$

Então

$$\sum_{\mathbf{x}\in C}\mathbf{x}=\mathbf{0}$$

se, e somente se, $\dim C=\dim \Delta C$.

Demonstração. Seja C um (M,n)-código esférico em $\mathbb{R}^n$ tal que

$$\sum_{\mathbf{x}\in C}\mathbf{x}=\mathbf{0}.$$

É claro que $\Delta C\subset\langle C\rangle$, pois $\langle C\rangle$ é um subespaço de $\mathbb{R}^n$. Logo,

$$\dim\Delta C\leq\dim\langle C\rangle=\dim C,$$

pois C gera $\mathbb{R}^n$. Por hipótese, temos que

$$|C|\,\mathbf{x}'=\sum_{\mathbf{x}\in C}\mathbf{x}'-\sum_{\mathbf{x}\in C}\mathbf{x}=\sum_{\mathbf{x}\in C}(\mathbf{x}'-\mathbf{x}),\forall\mathbf{x}'\in C.$$

Logo

$$C\subset\Delta C \text{ e } \dim C\leq\dim\Delta C.$$

Reciprocamente, seja

$$G=\{\mathbf{O}_i\}_{i=1}^{M}\leq O(n,\mathbb{R})$$

tal que

$$C=\{\mathbf{O}\mathbf{x}:\mathbf{O}\in G\} \text{ e } \mathbf{x}\in\mathbb{R}^n.$$

Como C é a órbita de $\mathbf{x}$ sob G, temos que

$$\mathbf{O}_i\mathbf{x}, i\in\{1,\ldots,M\}$$

são todos distintos. Vamos mostrar que

$$\sum_{\mathbf{O}\in G}\mathbf{O}\mathbf{x}=\mathbf{0},$$

pois,

$$\mathbf{O}\mathbf{x}=\mathbf{x}\Leftrightarrow\sum_{\mathbf{O}\in G}\mathbf{O}\mathbf{x}=\sum_{\mathbf{x}\in C}\mathbf{x}.$$

Seja

$$\{\mathbf{x}_1-\mathbf{x}_1',\ldots,\mathbf{x}_k-\mathbf{x}_k'\}$$

uma base para o subespaço $\langle \Delta C \rangle$. Como, por hipótese $\dim C = \dim \Delta C$, temos que

$$\mathbf{x} = \sum_{i=1}^{k} \alpha_i \left(\mathbf{x}_i - \mathbf{x}'_i \right), \alpha_i \in \mathbb{R}.$$

Logo,

$$\begin{aligned} \sum_{\mathbf{O} \in G} \mathbf{O}\mathbf{x} &= \sum_{\mathbf{O} \in G} \mathbf{O} \left(\sum_{i=1}^{k} \alpha_i \left(\mathbf{x}_i - \mathbf{x}'_i \right) \right) \\ &= \sum_{i=1}^{k} \alpha_i \left(\sum_{\mathbf{O} \in G} \mathbf{O} \left(\mathbf{x}_i - \mathbf{x}'_i \right) \right) = \mathbf{0}, \end{aligned}$$

pois

$$\{\mathbf{O}\mathbf{x}_1, \ldots, \mathbf{O}\mathbf{x}_M\} = \{\mathbf{O}\mathbf{x}'_1, \ldots, \mathbf{O}\mathbf{x}'_M\}.$$

■

Sejam $G = O(n, \mathbb{R})$ e a representação

$$\phi_G : \begin{array}{l} G \to GL(\mathbb{R}^n) \\ \mathbf{O} \mapsto \phi_G(\mathbf{O}) \end{array} \quad \text{e} \quad \phi_G(\mathbf{O}) : \begin{array}{l} \mathbb{R}^n \to \mathbb{R}^n \\ \mathbf{x} \mapsto \mathbf{O}\mathbf{x}^t \end{array}.$$

Então, ϕ_G é uma representação linear fiel n-dimensional do grupo G.

Proposição 2.2 *Sejam $\Omega = \{1, \ldots, n\}$ um G-conjunto, k o número de órbitas e χ_G o caráter de ϕ_G. Então*

$$\sum_{a \in G} \chi_G(a) = k \left| G \right|.$$

Demonstração. Basta notar que $\chi_G(a) = \mathrm{Fix}(a)$ e o resultado segue pela Proposição1.5.

■

Teorema 2.9 *Seja C um (M, n)-código de grupo em $\mathbb{R}^n$. Então as seguintes condições são equivalentes*:

1. *C é planar*;
2. *ϕ_G contém a representação identidade I_G quando escrita como uma soma direta de representações irredutível*;
3. $V_G = \{\mathbf{y} \in \mathbb{R}^n : G\mathbf{y} = \{\mathbf{y}\}\} \neq \{\mathbf{0}\}$.

Demonstração. (1. $\Longrightarrow$ 2.) Suponhamos, por absurdo, que ϕ_G não contenha a representação unitária I_G, quando escrita como soma direta de representações irredutível. Então existe $\mathbf{x}_i \in C$ tal que a j-ésima componente de $\mathbf{x}_i$ não é fixada, pois $\phi_G(X) \subseteq X$. Isto é, X não é planar.

(2. $\Longrightarrow$ 3.) Seja

$$\phi_G = I_G \oplus \varphi_2 \oplus \cdots \oplus \varphi_r$$

escrito coma soma direta de representações irredutíveis. Sejam V_i os espaços de representação associados a I_G, φ_i, $i = 2, \ldots, r$. Logo

$$\mathbb{R}^n = \mathbb{V}_{\nVdash} \oplus \cdots \oplus \mathbb{V}_{\approx}.$$

Seja $\mathbf{y} \in V_G \subset \mathbb{R}^n$ dado por

$$\mathbf{y} = \mathbf{y}_1 + \cdots + \mathbf{y}_r, \mathbf{y}_i \in V_i.$$

Então

$$\phi_G(\mathbf{O})(\mathbf{y}) = (I_G(\mathbf{O}) + \cdots + \varphi_r(\mathbf{O}))(\mathbf{y}).$$

Assim,

$$\mathbf{y} = \phi_G(\mathbf{O})(\mathbf{y}) = I_G(\mathbf{O})(\mathbf{y}) + \cdots + \varphi_r(\mathbf{O})(\mathbf{y}) \neq \mathbf{0}, \text{pois} I_G(\mathbf{O})(\mathbf{y}) \neq \mathbf{0}.$$

Logo,

$$V_G \neq \{\mathbf{0}\}.$$

(3. $\Longrightarrow$ 1.) Seja

$$C = \{\mathbf{x}_1, \ldots, \mathbf{x}_M\}$$

um código de grupo em $\mathbb{R}^n$ tal que $\dim C = n$ e

$$\mathbf{x} = \sum_{i=1}^{M} \mathbf{x}_i$$

Então $G\mathbf{x} = \mathbf{x}$ e $\mathbf{x} \in V_G \neq \{\mathbf{0}\}$. Assim, fazendo

$$C' = \{\mathbf{x}'_1, \ldots, \mathbf{x}'_M\} \text{ onde } \mathbf{x}'_i = \mathbf{x}_i - \frac{\mathbf{x}}{M}, \forall i \in \{1, \ldots, M\},$$

obtemos que

$$\sum_{i=1}^{M} \mathbf{x}'_i = \mathbf{0}.$$

Como

$$\{\mathbf{O}\mathbf{x}_1' : \mathbf{O} \in G\} = \{\mathbf{O}(\mathbf{x}_1 - \frac{\mathbf{x}}{M}) : \mathbf{O} \in G\} = \{\mathbf{O}\mathbf{x} - \frac{\mathbf{x}}{M} : \mathbf{O} \in G\} = C',$$

pois

$$C = \{\mathbf{O}\mathbf{x} : \mathbf{O} \in G\},$$

temos que C' é a órbita de $\mathbf{x}_1'$ sob G. Isto é, C' é um código de grupo. Mas

$$\Delta C' = \Delta C \subset \langle C \rangle$$

implica, pelo Lema 2.3, que

$$\dim C' = \dim \Delta C < \dim C.$$

Assim,

$$\dim C = \dim C' + 1, \text{ pois } C = C' + \frac{\mathbf{x}}{M}.$$

Portanto, C é planar. ■

Teorema 2.10 *Seja C um (M, n)-código de grupo em $\mathbb{R}^n$ com $V_G \neq \{\mathbf{0}\}$ e*

$$V_G^{\perp} = \{\mathbf{y} \in \mathbb{R}^n : \langle \mathbf{z}, \mathbf{y} \rangle = 0, \forall \mathbf{z} \in V_G\}.$$

Então o vetor inicial ótimo $\mathbf{x}$ para C pertence a $V_G^{\perp}$. Neste caso, $G\mathbf{x} = C$ não pode gerar $\mathbb{R}^n$.

Demonstração. Fazendo

$$\mathbf{x} = \alpha\mathbf{e} + \beta\mathbf{f},$$

onde $\mathbf{e}$ é um vetor unitário em V_G, $\mathbf{f}$ é um vetor unitário em $V_G^{\perp}$ e $\alpha, \beta \in \mathbb{R}$, com $\alpha^2 + \beta^2 = 1$. Então para cada $\mathbf{O} \in G$,

$$\begin{aligned} d^2(\mathbf{O}\mathbf{x}, \mathbf{x}) &= d^2(\mathbf{O}(\alpha\mathbf{e} + \beta\mathbf{f}), (\alpha\mathbf{e} + \beta\mathbf{f})) \\ &= d^2(\alpha\mathbf{e} + \beta\mathbf{O}\mathbf{f}, \alpha\mathbf{e} + \beta\mathbf{f}) \\ &= d^2(\beta\mathbf{O}\mathbf{f}, \beta\mathbf{f}) \\ &= \beta^2 d^2(\mathbf{O}\mathbf{f}, \mathbf{f}). \end{aligned}$$

Portanto, para obter o máximo dentro as distâncias mínima, basta tomar $\mathbf{x} \in V_G^{\perp}$, pois se $\mathbf{x} \in V_G$, então

$$d^2(\mathbf{O}\mathbf{x}, \mathbf{x}) = d^2(\mathbf{x}, \mathbf{x}) = 0.$$

Finalmente, como $V_G^{\perp}$ é G-invariante, pois dados $\mathbf{y} \in V_G$, $\mathbf{z} \in V_G^{\perp}$ e $\mathbf{O} \in G$, temos que

$$\begin{aligned} \langle \mathbf{y}, \mathbf{Oz} \rangle &= \langle \mathbf{O}^{-1}\mathbf{y}, \mathbf{O}^{-1}(\mathbf{Oz}) \rangle \\ &= \langle \mathbf{O}^{-1}\mathbf{y}, \mathbf{z} \rangle \\ &= \langle \mathbf{y}, \mathbf{z} \rangle = \mathbf{0}. \end{aligned}$$

Portanto, $G\mathbf{x} = C$ está contido em $V_G^{\perp}$ e não pode gerar $\mathbb{R}^n$, pois $\mathbb{R}^n = \mathbb{V}_{\mathbb{G}} \oplus \mathbb{V}_{\mathbb{G}}^{\perp}$. ■

Observação 2.6 *Se estamos interessados em gerar códigos de grupo ótimo para um grupo de matrizes G que satisrfaça as hipóteses do Teorema, então o código resultante não gerar o $\mathbb{R}^n$ mas um subespaço de $V_G^{\perp}$. Portanto, o código resultante não satisfaz a definição de um (M, n)-código de grupo, em vez disto, um (M, k)-código de grupo com $k < n$.*

2.4 Códigos de Permutação

Seja $G = S_n$ agindo sobre o conjunto $\Omega = \{1, 2, \ldots, n\}$. Já sabemos que este grupo pode ser representado por um grupo de matrizes de permutação P_n, isto é, G é imagem da representação natural do grupo de permutação.

Proposição 2.3 *Qualquer código de grupo gerado por G é planar.*

Demonstração. Seja $C = G\mathbf{x}$ um código de grupo. Então

$$V_G = \{\mathbf{y} \in \mathbb{R}^n : Gy = \{y\}\} \neq \{0\},$$

pois

$$\mathbf{y} = (1, 1, \ldots, 1) \in V_G.$$

Portanto, pelo Teorema 2.9, C é planar. ■

Seja V um espaço vetorial de dimensão n sobre $\mathbb{R}$ com base

$$B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}.$$

Então

$$\begin{aligned} * : \ & G \times V \to V \\ & (\sigma, \mathbf{v}_i) \mapsto \mathbf{v}_{\sigma(i)} \end{aligned}$$

é claramente uma ação de G sobre V. Assim

$$\varphi: \begin{array}{l} G \to GL(V) \\ \sigma \mapsto \boldsymbol{\varphi}(\boldsymbol{\sigma}) \end{array} \text{ e } \boldsymbol{\varphi}(\boldsymbol{\sigma}): \begin{array}{l} V \to V \\ \mathbf{v}_i \mapsto \mathbf{v}_{\sigma(i)} \end{array}.$$

é uma representação linear fiel de G com grau n. A matriz de $\boldsymbol{\varphi}(\boldsymbol{\sigma})$ com respeito à base B tem 1 na i-ésima linha e j-ésima coluna se $\mathbf{v}_{\sigma(j)} = \mathbf{v}_i$ e 0 nas outras entradas (cf. 2.2).

Se ϕ é qualquer representação de permutação de um grupo K, então

$$\varphi \circ \phi : K \longrightarrow GL(V)$$

é uma representação linear de K, onde

$$k * \mathbf{v}_i = \mathbf{v}_{\phi(k)(i)}, \forall k \in K \text{ e } \varphi \circ \phi(k)(\mathbf{v}_i) = \mathbf{v}_{\phi(k)(i)}.$$

A matriz de $\boldsymbol{\varphi} \circ \boldsymbol{\phi}(k)$ com respeito a B tem 1 na i-ésima entrada da diagonal se $\phi(k)(i) = i$. Caso contrário, tem 0. Portanto, se χ é o caráter de $\varphi \circ \phi$, então $\chi(k)$ é igual ao número de pontos fixados k em $\Omega = \{1, 2, \ldots, n\}$.

Teorema 2.11 *Sejam Ω um G-conjunto, k é o número de órbitas de Ω e ϕ_G é a representação de G. Então as seguintes condições são equivalentes*:

1. *ϕ_G contém a representação unitária k vezes*;
2. $\dim V_G = k$;
3. $\dim V_G^{\perp} = n - k$.

Demonstração. Se m é a multiplicidade da representação unitária em ϕ_G, então pela Proposição 2.2,

$$m = \langle \chi_G, I_G \rangle = \frac{1}{|G|} \sum_{a \in G} \chi_G(a) I_G(a) = k.$$

Logo,

$$\boldsymbol{\phi}_G = \begin{bmatrix} \mathbf{I}_k & \mathbf{O} \\ \mathbf{O} & \mathbf{B}_{n-k} \end{bmatrix}.$$

Assim, $\mathbb{R}^n = \mathbb{V}_{\mathbb{G}} \oplus \mathbb{V}_{\mathbb{G}}^{\perp}$ e as condições são equivalentes. ■

Corolário 2.1 *Se Ω é um G-conjunto transitivo, então* $\dim V_G^{\perp} = n - 1$.

Demonstração. Como Ω é um G-conjunto transitivo temos que $k = 1$. Assim, pelo Teorema 2.11, $\dim V_G^{\perp} = n - 1$. ■

Observação 2.7 *No Teorema* 2.11 *o espaço representação pode ser tomado como sendo* $V_G^{\perp}$. *De fato,* $V_G^{\perp}$ *sendo um* G*-conjunto* 2*-transitivo implica que* $V_G^{\perp}$ *é um* G*-conjunto transitivo. Assim, pelo Corolário* 2.1, $\dim V_G^{\perp} = n - 1$.

Proposição 2.4 *Nenhum subespaço de* $V_G^{\perp}$ *pode ser* G*-invariante.*

Demonstração. Segue do fato de que a representação de dinensão $(n-1)$ ser irredutível e $\dim V_G^{\perp} = (n-1)$. ■

O código ótimo gerado por G está contido em $V_G^{\perp}$ e o subespaço gerado pelo código é G-invariante, pois coincide com $V_G^{\perp}$. Portanto, o código gerado por $V_G^{\perp}$ será de dimensão $(n-1)$.

Observação 2.8 *Para qualquer grupo de permutação* G *temos que*

$$V_G^{\perp} \subseteq \{\mathbf{y} \in \mathbb{R}^n : \sum_{i=1}^{n} y_i = 0\}.$$

De fato, para

$$\mathbf{y} = (1, \ldots, 1) \in V_G \; e \; \mathbf{x} = (x_1, \ldots, x_n) \in V_G^{\perp}$$

temos que

$$0 = \langle \mathbf{x}, \mathbf{y} \rangle = x_1 + \cdots + x_n \Longrightarrow \mathbf{x} \in \{\mathbf{y} \in \mathbb{R}^n : \sum_{i=1}^{n} \mathbf{y}_i = 0\}.$$

Assim, um vetor inicial ótimo tem a propriedade

$$\sum_{i=1}^{n} x_i = 0.$$

Sejam G um grupo de permutação e $\mathbf{x}$ um vetor inicial para G. O código de grupo

$$C = \langle G, \mathbf{x} \rangle = G\mathbf{x}$$

gerado por G e $\mathbf{x}$ é chamado de *variante I*. O código de grupo

$$C = G\mathbf{x} \cup \{\mathbf{y} \in \mathbb{R}^n : y_i = \pm z_i \; \text{para} z \in Gx\}$$

gerado por G e $\mathbf{x}$ é chamado de *variante II*.

Sejam $H = \{1, -1\}$ um grupo multiplicativo e $M(H, G)$ o grupo das matrizes monomiais. Então o código variante II é $M(H, G)\mathbf{x}$. Portanto, pelo Teorema 1.6, $M(H, G) \simeq H \wr G$.

Teorema 2.12 *$K = M(H, G)$ é um grupo de matrizes irredutíveis se, e somente se, G é transitivo.*

Demonstração. Seja χ_K o carater de ϕ_K. Então K é um grupo de matrizes irredutíveis se, e somente se,

$$\sum_{a' \in K} \chi_K(a')\overline{\chi_K(a')} = |K|$$

Pelo Teorema2.3 se, e somente se,

$$\sum_{a' \in K} [\chi_K(a')]^2 = |K| \,.$$

Para $a \in G$, seja $F(a)$ o subconjunto de $\mathbb{N}$ fixado por a. Fixe $a \in G$ e suponha que $|F(a)| = m$. Então

$$\begin{aligned} \sum_{h \in H} [\chi_K(ha)]^2 &= \sum_{k=0}^{m} \binom{m}{k} [k - (m-k)]^2 2^{n-m} \\ &= 2^{n-m} \left[m^2 \sum_{k=0}^{m} \binom{m}{k} - 4m \sum_{k=0}^{m} \binom{m}{k} k + 4 \sum_{k=0}^{m} \binom{m}{k} k^2 \right] \\ &= 2^n m. \end{aligned}$$

Por outro lado,

$$\sum_{a' \in K} [\chi_K(a')]^2 = \sum_{a \in G} \sum_{h \in H} [\chi_K(ha)]^2 = \sum_{a \in G} 2^n \, |F(a)| = 2^n k \, |G| = |K|$$

se, e somente se, $k = 1$ se, e somente se, G é transitivo. ■

Capítulo 3

Modulação de Permutação

Neste capítulo apresentaremos um decodificador sub-ótimo de códigos de grupo. Esta técnica consiste das seguintes etapas. Primeira - representa-se o código de grupo na forma de um conjunto de vetores em $\mathbb{R}^n$ cujas componentes são obtidas por permutação das componentes de um vetor inicial de agordo com um grupo G de permutação. Segunda - decodifica-se o vetor recebido $\mathbf{r}$ pela procura da mais provável permutação no grupo S_n. Terceira - seleciona-se um elemento de G mais próximo da permutação encontrada.

3.1 Introdução

Um sistema de comunicação digital é dito com *decisão abrupta* quando o demodulador passa ao decodificador somente a informação do sinal do símbolo. O sistema de comunicação digital é de *decisão suave* quando o demo dulador, além do sinal, passa ao decodificador a informação de confiabilidade ou probabilidade do símbolo recebido.

Consideremos, como motivação, a decodificação de um (n, k)-código de bloco binário C sobre o Canal Gaussiano com ruído branco aditivo por meio do modulador padrão m definido por:

$$\begin{array}{rcl} m : GF(2) & \longrightarrow & \mathbb{R} \\ 0 & \longmapsto & -1 \\ 1 & \longmapsto & 1. \end{array}$$

Assim, a *decodificação suave* (máxima verossimilhança) de C é realizada escolhendo a palavra código $\mathbf{c}$ mais próxima do vetor recebido $\mathbf{r} \in \mathbb{R}^n$, onde

$$\mathbf{c} \leftrightarrow \mathbf{x} = (m(t), \ldots, m(t)) \in \mathbb{R}^n \text{ e } t \in GF(2).$$

Note que,

$$N(\mathbf{r}-\mathbf{x}) = N(\mathbf{r}) + N(\mathbf{x}) - 2\langle \mathbf{r}, \mathbf{x}\rangle \tag{3.1}$$

Assim, é bastante determinar $\mathbf{c} \in C$ que maximiza $\langle \mathbf{r}, \mathbf{x}\rangle$. A *decodificação abrupta* de C pode ser vista como uma aproximação de decodificação por máxima verossimilhança efetuada em duas etapas. Primeira - o uso preliminar de regiões de decisões formadas por partes (octantes) de $\mathbb{R}^n$para obter

$$\mathbf{y} \in m^{-1}\{\pm 1\} \times \cdots \times m^{-1}\{\pm 1\} \subseteq GF(2)^n.$$

Segunda - decodificação algébrica transformando y em uma palavra código. Assim, todo o procedimento pode ser visto como uma aproximação das regiões fundamentais do código pela união do octantes de $\mathbb{R}^n$.

Exemplo 3.1 *Seja* $C = \{(0,0,0),(1,1,1)\}$ *o* $(3,1)$*-código de repetição. Então suas regiões fundamentais são dadas pelos semi-espaços*

$$r_1 + r_2 + r_3 > 0 \; e \; r_1 + r_2 + r_3 < 0,$$

onde $\mathbf{r} = (r_1, r_1, r_1) \in \mathbb{R}^3$*. Assim, a decodificação abrupta é equivalente a escolher como regiões de decisões os semi-espaços*

$$\{r_1 > 0, r_2 > 0\} \cup \{r_1 > 0, r_3 > 0\} \cup \{r_2 > 0, r_3 > 0\}$$

e

$$\{r_1 < 0, r_2 < 0\} \cup \{r_1 < 0, r_3 < 0\} \cup \{r_2 < 0, r_3 < 0\}.$$

Assim, as regiões de decisões são uniões de quatro octantes de $\mathbb{R}^3$*, pois os pontos* $(-1,-1,-1)$ *e* $(1,1,1)$ *são vértices de um cubo.*

Este procedimento funciona, pois enquanto a determinação de uma entre as regiões fundamentais na qual $\mathbf{r}$ está caindo é uma tarefa complexa, podemos fazê-la facilmente aproximando-os por uma uma união de regiões tal que seja fácil determinar em qual o único vetor recebido está caindo. Neste capítulo, aplicaremos estas idéias para códigos de grupo. Suas regiões fundamentais são aproximadas por uma união de regiões menores com a propriedade que determinando a posição de $\mathbf{r}$ com respeito a elas seja uma tarefa fácil.

Seja $C = G\mathbf{x}$ um código de grupo. Os vetores de C transmitido sobre o Canal Gaussiano com ruído branco aditivo, a decodificação por máxima verossimilhança do vetor recebido $\mathbf{r} = \mathbf{x}' + \mathbf{n}$, onde $\mathbf{x}' \in C$ e o vetor ruído $\mathbf{n}$ é uma variável aleatório Gaussiana de média zero e variânça σ^2, escolhe como o mais provável vetor transmitido o único que produz

$$\min_{\mathbf{x}' \in C} ||\mathbf{r} - \mathbf{x}'||^2 \tag{3.2}$$

se G não é dotado com qualquer estrutura especial de decodificacão. A solução da Equação (3.2) é obtida por procura exaustiva entre todos candidatos $\mathbf{x}' \in C$. Isto exige um de número de cálculos

$$\eta_c = nM.$$

(M produto escalares de n termos cada um) e uma armazenagem de

$$\eta_s = nM$$

números reais (M vetores de n componentes cada). Realmente para isto, o mínimo para ser determinado requer η_M operações.

Como a taxa de informação do (n, k)-código (ou trasmitida pela constelação) é o número

$$R = \frac{k}{n} = \frac{1}{n} \log_{|F|} |C|$$

e para o caso binário

$$R = \frac{1}{n} \log_2 M.$$

temos que

$$\eta_c = \eta_s = n2^{nR},$$

a qual mostra que a complexidade da decodificacão cresce exponencialmente com o número de dimensões e com o número de bits por dimensão.

Em um sistema de modulação de permutação o código

$$C = \{\mathbf{x}_1, \ldots, \mathbf{x}_M\}$$

é escolhido de maneira especial. Existem dois tipos diferentes de códigos de modulação de permutação. No primeiro tipo chamado variante I, uma seqüência prescrita de n números reais, não necessariamente distintos, é tomado como a primeira palavra código $\mathbf{x}$. O restante das palavras código do código consiste de todas as seqüências distintas que

podem ser formadas permutando a ordem dos n números que forma a primeira palavra código, isto é, $C = G\mathbf{x}$, onde $G = P_n$ é o grupo de matrizes de permutações. No segundo tipo de código, chamado variante II, uma seqüência prescrita de n números não-negativos, não necessariamente distintos, é tomado para a primeira palavra código. O restante das palavras códigos do código consiste de todas as seqüências distintas que podem ser formadas permutando-se a ordem ou escolhendo-se o sinal dos n números que forma a primeira palavra código, isto é, $C = G\mathbf{x}$, onde $G = M(H, P_n)$ é o grupo de matrizes monomiais e $H = \{1, -1\}$.

A decodificação para um código de permutação (variante I) transforma uma seqüência recebida

$$\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$$

em uma palavra código, substituindo a primeira

$$r_i = \max_{1 \leq j \leq n} \{r_j\}$$

de $\mathbf{r}$ pela

$$x_i = \max_{1 \leq j \leq n} \{x_j\}$$

da primeira palavra do código $\mathbf{x}$. Mais precisamente, seja

$$\mathbf{x} = (u_1, \ldots, u_1, u_2, \ldots, u_2, \ldots, u_k, \ldots, u_k) \tag{3.3}$$

a primeira palavra código do código variante I, onde

$$u_1 < u_2 < \cdots < u_k$$

onde u_i aparece m_i vezes, para $i = 1, \ldots, k$. Logo,

$$n = m_1 + m_2 + \cdots + m_k.$$

Como as outras palavras código são obtidas permutando a ordem dos $u's$ na Equação (3.3) temos que o código tem

$$M = \frac{n!}{m_1! m_2! \cdots m_k!}$$

palavras código.

Finalmente, a decodificação ideal de um vetor recebido

$$\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$$

afirma que $\mathbf{x}_i$ foi transmitido quando

$$N(\mathbf{r}-\mathbf{x}_i)^2 = N(\mathbf{r}) + N(\mathbf{x}_i) - 2\langle \mathbf{r}, \mathbf{x}_i\rangle, \forall i = 1, \ldots, M$$

é mínima. Como $N(\mathbf{r})$, $N(\mathbf{x}_i)$ são independentes de i, pois

$$\mathbf{x}_i = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

para todo $\sigma \in S_n$, onde $\mathbf{x} = (x_1, \ldots, x_n)$ é o vetor inicial, temos que a decodificação procura encontrar a palavra código $\mathbf{x}_i$ que maximiza

$$\langle \mathbf{r}, \mathbf{x}_i\rangle = \sum_{j=1}^{n} r_j x_{ji}$$

Teorema 3.1 *Seja* $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$. *Então*

$$\langle \mathbf{r}, \mathbf{x}\rangle = \sum_{i=1}^{n} r_i x_{\sigma(i)} \tag{3.4}$$

alcança o valor máximo para toda $\sigma \in S_n$ *se o primeiro*

$$r_i = \max_{1\leq j\leq n}\{r_j\}$$

de $\mathbf{r}$ *é casado com o primeiro*

$$x_i = \max_{1\leq j\leq n}\{x_j\}$$

de $\mathbf{x}$ *e, assim por diante.*

Demonstração. Vamos usar indução sobre n. Se $n = 1$ nada há para demonstrar. Assim, suponhamos que o resultado seja válido para todo k, com $1 < k < n$. Sejam

$$\widehat{r} = \max_{1\leq j\leq n}\{r_j\} \text{ e } \widehat{x} = \max_{1\leq j\leq n}\{x_j\}$$

o primeiro máximo de $\mathbf{r}$ e $\mathbf{x}$, respectivamente. Então, se $\widehat{r}$ não é casado com $\widehat{x}$ na soma (3.4), então a soma contém dois termos

$$\widehat{r}x + y\widehat{x} \text{ com } x \leq \widehat{x} \text{ e } y \leq \widehat{r}.$$

Assim, se x e y são permutados, então a nova soma é maior do que a soma (3.4), pois

$$(\widehat{r}\widehat{x} + yx) - (\widehat{r}x + y\widehat{x}) = (\widehat{r} - y)(\widehat{x} - x) \geq 0.$$

Logo, existe um casamento de $\mathbf{r}$ e $\mathbf{x}$ para o qual a soma (3.4) alcança o valor máximo e $\widehat{r}$ é casado com $\widehat{x}$. Portanto, se eliminarmos $\widehat{r}\widehat{x}$ da soma (3.4), então pela hipótese de indução, o segundo

$$r_i = \max_{1 \leq j \leq n} \{r_j\}$$

de $\mathbf{r}$ é casado com o segundo

$$x_i = \max_{1 \leq j \leq n} \{x_j\}$$

de $\mathbf{x}$ e, assim por diante. ■

Exemplo 3.2 *Seja* $\mathbf{x} = (-1, 0, 1) \in \mathbb{R}^3$ *a palavra código inicial do código variante I. Então*

$$C = \{(-1, 0, 1), (0, -1, 1), (1, 0, -1), (-1, 1, 0), (0, 1, -1), (1, -1, 0)\}.$$

Suponhamos que o vetor recebido é

$$\mathbf{r} = (-\frac{3}{2}, -\frac{1}{2}, \frac{6}{5}) \in \mathbb{R}^3.$$

Então a palavra código decodificada é $\mathbf{x} = (-1, 0, 1)$.

Conclusão: Uma decodificação para modulação de permutação é um algoritmo o qual, quando apresentado com um vetor recebido $\mathbf{r} \in \mathbb{R}^n$, determina $\sigma(\mathbf{x})$ que minimiza a distância Euclidiana quadrática de $\sigma(\mathbf{x})$ a $\mathbf{r}$, isto é, maximiza

$$\langle \mathbf{r}, \sigma(\mathbf{x}) \rangle = \sum_{i=1}^{n} r_i x_i.$$

Em particular, se H um subgrupo qualquer de S_n, então uma modulação de permutação gerada por H pode ser decodificada em duas etapas:

1. Decodifique $\mathbf{r}$ como se $H = S_n$, obtendo como resultado uma permutação σ de n símbolos. Note que, ela pode não pertencer a H.

2. "Decodifique algebricamente" σ em um elemento de H.

Nesta próxima seção trabalharemos a primeira etapa de decodificação. Em particular, mostraremos que todo grupo pode ser representado na forma de um conjunto de sinais de permutação e encontraremos a dimensão mínima de uma tal representação bem como a relevante transformação.

3.2 Representação de Permutação

Agora mostraremos que qualquer grupo pode ser representado na forma de um *conjunto de sinais de permutação* e, consequentemente, pode ser decodificado por meio da decodificação de permutação.

Seja G um grupo de ordem M. Então, pelo Corolário 1.1, G é isomorfo a um subgrupo H de S_M.

Queremos determinar o menor n tal que G é isomorfo a S_n.

Uma condição necessária é que M divide $n!$. Pode ocorrer que $M > n$, pois basta observar os códigos variantes I e II.

Sejam G um grupo finito, H um subgrupo próprio de G e $\Lambda = \{aH : a \in G\}$, onde $|\Lambda| = n$. Então, pelo Teorema 1.3,

$$\sigma : G \to P(\Lambda) \text{ dada por } \sigma(g) = \sigma_g, \text{ onde } \sigma_g(aH) = gaH$$

é um homomorfismo de grupos chamado *representação por permutação.* Além disto, G age transitivamente sobre Λ e

$$\ker \sigma = \bigcap_{g \in G} gHg^{-1}$$

é o maior subgrupo normal de G contido em H. Portanto, qualquer subgrupo H de G induz uma representação de permutação transitiva. Reciprocamente, toda representação de permutação transitiva de G é obtida desta maneira. Em particular, se $H = \{e\}$, então $\sigma = \rho_R$ é a representação regular de G.

Proposição 3.1 *Sejam G um grupo finito, H um subgrupo próprio de G e $\Lambda = \{aH : a \in G\}$, onde $|\Lambda| = n$. Então n é mínimo se, e somente se, $|H|$ é máxima e $\ker \sigma = \{e\}$.*
■

Agora, se K é um subgrupo maximal não normal de G tal que não existe subgrupo normal $L \neq \{e\}$ de G com $L \subseteq K$, então

$$n = \frac{|G|}{|K|}$$

Exemplo 3.3 *Seja G abeliano Então todos os subgrupos de G são normais. Logo, $|K| = 1$ e $n = |G|$.*

Exemplo 3.4 *Seja $G = S_m$, $m = 3$ ou $m \geq 5$. Então, pelo Proposição* 1.10*,*

$$G_i = \{\sigma \in S_m : \sigma(i) = i\} = S_{m-1}$$

subgrupo maximal não normal S_m. Portanto

$$n = \frac{|S_m|}{|S_{m-1}|} = m.$$

Exemplo 3.5 *Seja $|G| = 2k$, com k ímpar. Então, Proposição* 1.4*, G possui um subgrupo normal de ordem k e $n > 2$. Pois, se $\{e\} \neq H$ é um subgrupo maximal não normal de G, então*

$$|H| < k \Longrightarrow \frac{1}{|H|} > \frac{1}{k} \Rightarrow n = \frac{|G|}{|H|} > 2.$$

3.3 Modulação de Permutação

Seja $G = \{g_1, g_2, \ldots, g_n\}$ é um grupo, onde $g_1 = e$. Então uma tabela de multiplicação para G é dada por

$*$	g_1	g_2	$\cdots$	g_n
g_1	g_1	g_2	$\cdots$	g_n
g_2	g_2	g_2^2	$\cdots$	$g_2 g_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g_n	g_n	$g_n g_2$	$\cdots$	g_n^2

A correspondência $g_i \longleftrightarrow \sigma_i$, onde

$$\sigma_i = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_i & g_i g_2 & \cdots & g_i g_n \end{pmatrix},$$

define um mapeamento injetivo de G sobre S_n. Portanto, G pode imerso em S_n. Como P_n é um subgrupo de $O(n, \mathbb{R})$ e S_n é isomorfo a P_n temos que G pode ser imerso em $O(n, \mathbb{R})$, isto é, todo grupo finito pode ser imerso no grupo das matrizes ortogonais. Assim, pelo Exemplo 2.2, todo grupo G possui uma representação regular que consiste de matrizes de permutações de ordem $|G|$.

Observação 3.1 *A representação regular é redutível e contém todas as re presentações irredutíveis de G. De fato. Como $\chi(g_1) = n$, $0 \leq \chi(g_i) < n$, para todo g_i, $i = 2, \ldots, n$ e*

$$\chi(g_1^{-1})\overline{\chi}(g_1) + \cdots + \chi(g_n^{-1})\overline{\chi}(g_n) = \chi^2(g_1^{-1}) + \cdots + \chi^2(g_n^{-1})$$

temos, pelo Teorema 2.2*, que*

$$\sum_{g\in G}\chi^2(g_i^{-1}) > |G|$$

Logo, a representação regular é redutível. A segunda parte segue do Teorema 2.1*.*

Denotando a matriz de permutação associada à representação ρ_R por $\boldsymbol{\rho}_R(g)$. Temos que existe uma matriz ortogonal $\mathbf{M} \in O(n,\mathbb{R})$ tal que

$$\begin{aligned}\mathbf{M}^t\boldsymbol{\rho}_R(a)\mathbf{M} &= \begin{bmatrix} \boldsymbol{\rho}_1(a) & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \boldsymbol{\rho}_2(a) & \cdots & \mathbf{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{O} & \mathbf{O} & \cdots & \boldsymbol{\rho}_r(a) \end{bmatrix} \\ &= \boldsymbol{\rho}_1(a) + \cdots + \boldsymbol{\rho}_r(a),\end{aligned}$$

para todo $a \in G$. Fazendo $\mathbf{U}(g) = \boldsymbol{\rho}_1(a) + \cdots + \boldsymbol{\rho}_r(a)$, obtemos que

$$\mathbf{M}^t\boldsymbol{\rho}_R(a)\mathbf{M} = \mathbf{U}(a),$$

ou ainda,

$$\mathbf{M}\mathbf{U}(a) = \boldsymbol{\rho}_R(a)\mathbf{M}.$$

Portanto, se $\mathbf{x}^0$ denota uma versão aumentada de zeros do vetor inicial $\mathbf{x}$, então

$$\mathbf{M}\mathbf{U}(a)\mathbf{x}^0 = \boldsymbol{\rho}_R(a)\mathbf{y} \text{ onde } \mathbf{y} = \mathbf{M}\mathbf{x}^0 \tag{3.5}$$

Teorema 3.2 *Seja* $H = \{\mathbf{U}(a) : a \in G\} \leq O(n,\mathbb{R})$*. Então* $\widehat{C} = H\mathbf{x}^0$ *é um código de grupo.*

Demonstração. Seja $\mathbf{x}_1 = \mathbf{U}(a_1)\mathbf{x}^0, \mathbf{x}_2 = \mathbf{U}(a_2)\mathbf{x}^0 \in \widehat{C}$. Então devemos demonstrar que existe $\mathbf{H} = \mathbf{U}(a_i) \in H$ tal que $\mathbf{x}_2 = \mathbf{H}\mathbf{x}_1$.

$$\begin{aligned}\mathbf{x}_2 &= \mathbf{U}(a_2)\mathbf{x}^0 \\ &= \mathbf{U}((a_2a_1^{-1})a_1)\mathbf{x}^0 \\ &= (\mathbf{U}(a_2a_1^{-1})\mathbf{U}(a_1))\mathbf{x}^0 \\ &= \mathbf{H}\mathbf{U}(a_1)\mathbf{x}^0 \\ &= \mathbf{H}\mathbf{x}_1\end{aligned}$$

■

Por outro lado, $\boldsymbol{\rho}_R(a)\mathbf{y}$ é código de permutação agindo sobre o vetor inicial $\mathbf{y}$. Logo, a Equação (3.5) expressa o fato que os dois códigos são relacionados pela transformação $\mathbf{M}$. Como $\mathbf{U}(a)$ é uma matriz ortogonal os códigos são equivalentes. Vamos fazer algumas considerações sobre grupo cíclico antes de darmos um exemplo.

Seja $G = \langle a \rangle$ um grupo cíclico de ordem n. Então

$$\rho : G \longrightarrow O(2, \mathbb{R})$$

definida por

$$\rho(a) = \begin{bmatrix} \cos\frac{2\pi}{n} & -\operatorname{sen}\frac{2\pi}{n} \\ \operatorname{sen}\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}$$

define uma representação de grau 2 de G. Agora, pelo Exemplo 2.2, temos que

$$\begin{array}{rl} \rho_R : & G \longrightarrow O(n, \mathbb{R}) \\ & a_k \mapsto (a_{ij}) \end{array},$$

onde

$$a_{ij} = \rho_R(a_k) = \begin{cases} 1 & \text{se}, a_i = a_k a_j \\ 0 & \text{se}, a_i \neq a_k a_j \end{cases}$$

é uma representação de G como matrizes de permutação. Portanto, a matriz de permutação $\boldsymbol{\rho}_R(a)$ associada a representação ρ_R gera um subgrupo cíclico de P_n. Em particular, quando $n = 4$, pelo Algoritmo da Seção 1.5, podemos encontrar uma matriz $\mathbf{O} \in O(4, \mathbb{R})$ tal que:

$$\mathbf{O}\boldsymbol{\rho}_{\mathbf{R}}(a)\mathbf{O}^t = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Exemplo 3.6 *Considere a constelação de sinais 4-PSK em $\mathbb{R}^2$. O 4-PSK pode ser gerado pela ação do grupo cíclico G de quatro matrizes*

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

sobre o vetor inicial $\mathbf{x} = (1, 0)$. Assim, aplicando $\mathbf{O}$ a uma versão aumentada de zeros de $\mathbf{x}$; isto é, $\mathbf{x}^0 = (0, 0, 1, 0)$, obtemos o vetor inicial do código de permutação equivalente a 4-PSK

$$\mathbf{y} = (\varepsilon, \varepsilon, -\sqrt{2}\varepsilon, 0), \text{ onde } \varepsilon = \frac{1}{2}.$$

3.4 Decodificação de Códigos de Permutação

Decodificação de uma constelação de grupo é equivalente encontrar a região fundamental na qual o vetor recebido $\mathbf{r} \in \mathbb{R}^n$ caiu

Suponha agora, que podemos encontrar um código grupo $\widehat{C}$, com $C \subseteq \widehat{C}$, cuja estrutura permita que ele seja facilmente decodificado. As regiões de fundamentais de $\widehat{C}$ são menores que as regiões fundamentais de C. Aproximaremos cada região fundamental de C como uma união regiões fundamentais de $\widehat{C}$ e a operação de decodificação é dividida em duas etapas:

1. Decodifica-se $\mathbf{r}$ como se ele fosse obtido da transmissão de um sinal em $\widehat{C}$;

2. Associa-se o sinal decodifica com um $\mathbf{x} \in C$.

Como cada grupo com M elementos é um subgrupo do grupo simétrico S_M, podemos escolher $\widehat{C}$ como o código gerado por este grupo.

A constelação de sinais gerada pelo grupo de simetria S_M é chamada *Código de Permutação* (variante I)**.** Seu algoritmo de decodificação por máxima verossimilhança ocorre como no Teorema 3.1.

A decodificação por permutação consiste do seguinte:

Particiona o grupo S_M em classes laterais à esquerda G em S_M. Existem $\frac{n!}{M}$ classes laterais.

A região fundamental de cada elemento de C é então aproximada pela a união das regiões fundamentais dos elementos de cada classe lateral.

Para este processo de decoficação precisamos do seguinte Algoritmo, o leitor interessado em mais detalhes pode consultar [10].

Algoritmo (troca "fundida")

Os registros $R_1, \ldots, R_n$ são rearrumados em seus lugares; após a classificação (ordenação) nas "chaves" (índices) serão $K_1, \ldots, K_n$. Suponhamos $n \geq 2$.

1. **Inicializar** p - Seja $p = 2^{t-1}$, onde

$$t = \lceil \log_2 n \rceil$$

é o menor inteiro tal que $2^t \geq n$. (Os Passos 1 a 5 deverão ser executados para $p = 2^{t-1}$, $p = 2^{t-2}, \ldots, 1$).

2. **Inicializar** q, r, d - Sejam $q = p = 2^{t-2}$, $r = 0$, e $d = p$.

3. **Laço controlado por** "i" - Para todo i tal que $0 \leq i \leq N - d$ e $i \wedge p = r$, faça o Passo 4. Depois, vá para o Passo 5. (Aqui $i \wedge p$ significa a operação binária "e" lógica envolvendo as representações binárias de i e p. Cada bit do resultado é zero a não ser que se tenha bit 1 em ambas as representações na mesma posição. Por exemplo,

$$(13) \wedge (21) = (1101)_2 \wedge (10101)_2 = (00101)_2 = 5.$$

Dessa forma, d é um múltiplo ímpar de p e p é uma potência de 2 tais que

$$i \wedge p \neq (i + d) \wedge p.$$

Segue que a ação do Passo 4 pode ser feita para todos os i relevantes, até mesmo ser feita simultameamente).

4. **Compare/Troque** R_{i+1} **e** R_{i+d+1} - Se $K_{i+1} > K_{i+d+1}$, então troque os valores de R_{i+1} e R_{i+d+1} entre si.

5. **Laço controlado por** q - Se $p \neq q$, sejam $d = q - p$, $q = \dfrac{q}{2}$ (ou seja, q é reduzido à sua metade) $r = p$ e volte para o Passo 3.

6. **Laço controlado por** p - (Neste ponto a permutação $K_1, \ldots, K_n$ está p-ordenada) Seja

$$p = \left\lfloor \frac{p}{2} \right\rfloor,$$

ou seja, p é substituído pelo valor $\left\lfloor \dfrac{p}{2} \right\rfloor$. Se $p > 0$, então volte para o Passo 2.

A ordem *lexicográfica* em um conjunto $A \times B$ é definida por

$$(a, b) \leq (c, d) \Longleftrightarrow a < b \text{ ou } a = c \text{ ou } b < d.$$

Exemplo 3.7 *Seja C o 4-PSK. Então, como tinhamos visto isto pode ser implementado na forma da substituição cíclica do vetor inicial*

$$\mathbf{x} = (1, 0, -1, 0).$$

A tabela abaixo mostra a distância Euclidiana quadrática entre as permutações de $\mathbf{x}$*, onde as permutações não cíclicas são numeradas de acordo com a sua ordem lexicográfica. Nestas condições, as menores regiões de fundamentais serão divididas igualmente entre as*

permutações cíclicas. Como um resultado, a distância mínima encontrada pela decodificação abrupta é igual a 2, a qual é metade da distância mínima de decodificação por máxima verossimilhança.

$$
\begin{aligned}
1 = 1234 \leftrightarrow \mathbf{x}_1 = (1,0,0,-1) \quad & 11 = 3124 \leftrightarrow \mathbf{x}_{11} = (-1,1,0,0) \\
2 = 1324 \leftrightarrow \mathbf{x}_2 = (1,-1,0,0) \quad & 12 = 3142 \leftrightarrow \mathbf{x}_{12} = (-1,1,0,0) \\
3 = 1342 \leftrightarrow \mathbf{x}_3 = (1,-1,0,0) \quad & 13 = 3214 \leftrightarrow \mathbf{x}_{13} = (-1,0,1,0) \\
4 = 1423 \leftrightarrow \mathbf{x}_4 = (1,0,0,-1) \quad & 14 = 3241 \leftrightarrow \mathbf{x}_{14} = (-1,0,0,1) \\
5 = 1432 \leftrightarrow \mathbf{x}_5 = (1,0,-1,0) \quad & 15 = 3421 \leftrightarrow \mathbf{x}_{15} = (-1,0,0,1) \\
6 = 2134 \leftrightarrow \mathbf{x}_6 = (0,1,-1,0) \quad & 16 = 4132 \leftrightarrow \mathbf{x}_{16} = (0,1,-1,0) \\
7 = 2143 \leftrightarrow \mathbf{x}_7 = (0,1,-1,0) \quad & 17 = 4213 \leftrightarrow \mathbf{x}_{17} = (0,0,1,-1) \\
8 = 2314 \leftrightarrow \mathbf{x}_8 = (0,-1,1,0) \quad & 18 = 4231 \leftrightarrow \mathbf{x}_{18} = (0,0,-1,1) \\
9 = 2413 \leftrightarrow \mathbf{x}_9 = (0,0,1,-1) \quad & 19 = 4312 \leftrightarrow \mathbf{x}_{19} = (0,-1,1,0) \\
10 = 2431 \leftrightarrow \mathbf{x}_{10} = (0,0,-1,1) \quad & 20 = 4321 \leftrightarrow \mathbf{x}_{20} = (0,-1,0,1)
\end{aligned}
$$

A tabela abaixo dá a distância Euclidiana quadrática entre as menores regiões fundamentais e o conjunto de sinais

	1	2	3	4	5	6	7	8	9	10
1234	2	2	2	2	0	2	4	6	6	2
2341	6	2	2	6	4	6	8	2	6	2
3412	6	6	6	6	8	6	4	2	2	6
4123	2	6	6	2	4	2	0	6	2	6

e

	11	12	13	14	15	16	17	18	19	20
1234	6	6	8	6	6	2	6	2	6	4
2341	6	6	4	2	2	6	6	2	2	0
3412	2	2	0	2	2	6	2	6	2	4
4123	2	2	4	6	6	2	2	6	6	8

,

onde

$$
\begin{aligned}
&1234 \leftrightarrow (1,0,-1,0) \; e \; 2341 \leftrightarrow (0,-1,0,1) \\
&3412 \leftrightarrow (-1,0,1,0) \; e \; 4123 \leftrightarrow (0,1,0,-1)
\end{aligned}
.
$$

Referências Bibliográficas

[1] Biglieri, E. and Elia, M., "Cyclic-Gruop Codes for the Gaussian Channel," *IEEE Trans. Inform. Theory*, vol. 22, 624-629, 1976.

[2] Biglieri, E., Karlof, J. K. and Viterbo, E. "Representig groups codes of permutation codes." *IEEE Trans. Inform. Theory*, vol. 45, 2204-2207, 1999.

[3] Blake, I. F. and Mullin,R. C., *The Mathematical Theory of Coding*. Academic Press. New York. 1975.

[4] Cameron, P. J., "Finite permutation gruops and finite simple gruops." *Bull. London Math. Soc.* 13, pp. 1-22, 1981.

[5] Dixon, J. D. and Mortimer, B.C., *Permutation groups*. Sprringer-Verlag, New Yor, 1996.

[6] Gantmacher, F. R., *The Theory of Matrices*, Vol. 1, New Jersey, Prentice-Hall, 1991.

[7] Garcia, A. e Y. Lequain, I. *Álgebra: Um curso de introdução*. Projeto Euclides - IMPA. Rio Janeiro, 1988.

[8] Gonçalves, A. *Tópicos em representação de grupos.* 9º Colóquio Brasileiro de Matemática. Poços de Caldas. 1973.

[9] Karlof, J. K., "Permutation codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, vol. 35, 726-732, 1989.

[10] Knuth, D. E., *Art of Computer Programming*, Vol. 3, Sorting and Searching, Addison-Wesley, 1975.

[11] MacWilliams, F. J. and Sloane, N. J.A., *The Theory of Error-Correcting Codes*, New York, North-Holland, 1977.

[12] Passman, D.S., *Permutation Gruops*. New York, Benjamin, 1968.

[13] Slepian, D., "Permutation Modulation," *Proc. IEEE Trans. Inform. Theory*, vol. 53, 228-236, 1965.

[14] Van Lint, J. H., *Introduction to Coding Theory*. Sprringer-Verlag. Eindhoven, 1991.