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

Construção de Códigos Lineares sobre Grupos

por

Ronaldo Chaves Cavalcanti

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.

Setembro/2000

João Pessoa - Pb

Construção de Códigos Lineares sobre Grupos

por

Ronaldo Chaves Cavalcanti

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. João Bosco Batista Lacerda

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

Setembro/2000

Agradecimentos

1. À Deus, que me concedeu a realização deste trabalho.
2. Aos meus pais Antônio e Carminha, por tudo que sou.
3. Ao meu orientador e amigo Prof. Dr. Antônio de Andrade e Silva pela orientação, paciência, dedicação e amizade.
4. Ao professor Dr. Hélio Pires de Almeida, que nunca negou-se, a tirar as dúvidas.
5. Aos professores do Departamento de Matemática da UFPB - Campus I.
6. Aos colegas de Curso.
7. A minha esposa Edna e aos meus filhos Alexandre e Ana Karoline pela compreenção de tê-los privado da minha presença, por vários momentos importantes de suas vidas.
8. Ao amigo e primo Bel. Luiz Guedes Monteiro Filho.

Dedicatória

À meu pai
"in memoriam"
Antônio Guedes Cavalcanti.

Notação

End(G) - Anel dos endomorfismo do grupo G

$\mathcal{Z}_m$ - Anel dos inteiros módulo m

$Z(G)$ - Centro do grupo G

aH - Classe lateral à esquerda

C - Código

C^d - Código dual de C

$\mathbb{I}$ - Conjunto de índices

$\mathbb{J}$ - Conjunto de informação

$\mathbb{N}$ - Conjunto dos números naturais

$\mathbb{Z}$ - Conjunto dos números inteiros

$\mathbb{R}$ - Conjunto dos números reais

$\mathbb{C}$ - Conjunto dos números complexos

$d_H(,)$ - Distância de Hamming

k - Dimensão do código

W - Espaço de saída

$F^{\mathbb{I}}$ - Espaço de seqüências

G - Grupo

$\mathbb{Z}_m$ - Grupo aditivo dos inteiros módulo m

K - Grupo ciclo

K_n - Grupo das raízes n-ésimas da unidade

G_i - Grupo de saída

HK - Grupo fatorizável em H e K

Aut(G) - Grupo dos automorfismos de G

Inn(G) - Grupo dos automorfismos internos de G

$\widehat{G}$ - Grupo dos caracteres de G

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

R_{ij} - Grupo dos homomorfismos de $\mathbb{Z}_{d_j}$ em $\mathbb{Z}_{d_i}$

$\simeq$ - Isomorfismo

d - Mínima distância de Hamming

ker - Núcleo do homomorfismo

$o(a)$ - Ordem do elemento a

$|G|$ - Ordem do grupo G

$H \times K$ - Produto direto de H por K

$H \rtimes K$ - Produto semi-direto de H por K

ξ - Raiz primitiva da unidade

$\oplus$ - Soma direta

$\leq$ - Subgrupo

$\langle a \rangle$ - Subgrupo gerado pelo elemento a

$\trianglelefteq$ - Subgrupo normal

G' - Subgrupo dos comutadores de G

r - Taxa de informação do código

Sumário

Introdução

No presente trabalho apresentaremos uma construção de códigos sobre grupo que imita a construção de códigos algébricos sobre um corpo finito. O estudo de códigos de grupos para o canal Gaussiano foi inciado por Slepian em [8].

Um código de grupo sobre um grupo G é um subgrupo de G^n. O estudo de códigos de grupos foi motivado pela a observação de que códigos de grupos constitui um ingrediente básico para códigos geometricamente uniforme que inclui diversas classes de códigos: códigos de treliça, códigos reticulados e a constelação de sinais M-PKS casada a grupos.

Embora a distância Euclidiana quadrática mínima seja a medida apropriada para conjunto de sinais casado a grupos, a distância de Hamming de um código de grupo dar um limite inferior para a distância Euclidiana quadrática máxima, cf. em [4].

Dado um $[n, k]$-código, a maior distância mínima de Hamming é $n - k + 1$. Isto é verdade para códigos sobre um qualquer alfabeto. Um $[n, k]$-código cuja distância mínima de Hamming é igual a $n - k + 1$ é chamado de código de máxima dsitância separável (MDS). Códigos MDS foram inicialmente tratados em [4]. Para códigos de grupo sob grupos abelianos a construção técnica foi dada em [1] em termos de homomorfismo de grupos G^k em G ou, equivalentemente, em termos do conjunto de endomorfismo de G.

Quando G é o grupo cíclico $\mathbb{Z}_m$ caracterizaremos os homomorfismos de grupos $\mathbb{Z}_m^k$ em $\mathbb{Z}_m$ que formam $[k + s, k]$-códigos MDS. Como cada um destes homomorfismos pode ser escrito em termos de k endomorfismos $\mathbb{Z}_m$ temos que o $[k + s, k]$-códigos MDS é descrito por um conjunto de ks endomorfismos de $\mathbb{Z}_m$. Mostraremos que uma matriz sobre o anel $\mathcal{Z}_m$ estar associada com o conjunto de ks endomorfismos de $\mathbb{Z}_m$.

Códigos lineares sobre $\mathcal{Z}_m$ são idênticos a códigos de grupos sobre o grupo aditivo $\mathbb{Z}_m$ de $\mathcal{Z}_m$. Mas códigos lineares sobre corpos finitos não são idênticos a códigos de grupos sobre o seu grupo aditivo, o qual é abeliano elementar. Por exemplo, o $[4, 2, 3]$-código de grupo da Tabela 1 é um MDS código sobre $\mathbb{Z}_2 \otimes \mathbb{Z}_2 = \{1, a\} \otimes \{1, b\}$ mas não é um

$(1,1,1,1)$	$(a,1,ab,ab)$	$(b,1,b,b)$	$(ab,1,a,a)$
$(1,a,ab,b)$	$(a,a,1,a)$	$(b,a,a,1)$	(ab,a,b,ab)
$(1,b,b,a)$	(a,b,a,b)	$(b,b,1,ab)$	$(ab,b,ab,1)$
$(1,ab,a,ab)$	$(a,ab,b,1)$	(b,ab,ab,a)	$(ab,ab,1,b)$

Tabela 1: $[4,2,3]$-código de grupo sobre $\mathbb{Z}_2 \otimes \mathbb{Z}_2$

código linear sobre o corpo finito $GF(4)$ cujo grupo aditivo é $\mathbb{Z}_2 \otimes \mathbb{Z}_2$, pois o anel dos endomorfismos de $\mathbb{Z}_m$ é isomorfo a $\mathcal{Z}_m$, enquanto anel dos endomorfismos de $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ é isomorfo a $GF(4)$. Um endomorfismo de $\mathbb{Z}_m$ pode ser definido por um elemento de $\mathcal{Z}_m$ o qual é a imagem de um gerador sob o endomorfismo e isto é a razão para não distinção de códigos de grupos sobre $\mathbb{Z}_m$ e códigos linear sobre $\mathcal{Z}_m$.

A abordagem que faremos nos próximos capítulos, ficará disposta da seguinte forma:

No capítulo 1, faremos uma abordagem sobre a Teoria de Grupos dando ênfaze à homomorfismos de grupos, além disto, algumas definições e resultados clássicos sobre Módulos.

No capítulo 2, apresentaremos as principais definições e parâmetros de códigos de grupos. Além disso, mostraremos que não existe $[4,2,3]$-código de grupo sobre $\mathbb{Z}_{2m}$, para todo $m \geq 2$, no entanto, existe $[4,2,3]$-código linear sobre $GF(4)$.

No capítulo 3, apresentaremos uma construção de códigos de blocos lineares sobre grupos que imita a construção de códigos algébricos sobre corpos finitos. Como vimos, no Capítulo 2, códigos baseados em grupos não abeliano exibem uma pobre distância de Hamming. Assim, focaremos nossa atenção em grupos abelianos.

No capítulo 4, caracterizaremos o conjunto de homomorfismos de grupos que define códigos de grupos com máxima distância separável (MDS) sobre o grupo cíclico $\mathbb{Z}_m$. Além disto, mostraremos que o código dual de um código de grupo com máxima distância separável sobre $\mathbb{Z}_m$, é também um código de grupo com máxima distância separável

Capítulo 1

Resultados Básicos

Neste capítulo apresentaremos alguns resultados básicos da teoria dos grupos e módulos que serão necessários nos capítulos seguintes, o leitor interessado em mais detalhes deve consultar [2, 5].

1.1 Conceitos Básicos

Um conjunto não vazio G equipado com uma operação binária

$$\begin{aligned} * : \quad & G \times G \longrightarrow G \\ & (a, b) \longmapsto a * b \end{aligned}$$

é um *grupo* se as seguintes condições são satisfeitas:

1. $a * (b * c) = (a * b) * c$, para todos $a, b, c \in G$.

2. Existe $e \in G$ tal que $e * a = a * e = a$, para todo $a \in G$.

3. Para todo $a \in G$, existe $b \in G$ tal que $a * b = b * a = e$.

O grupo é *abeliano* ou *comutativo* se também vale

4. $a * b = b * a$, para todos $a, b \in G$.

Com o objetivo de simplificar a notação usaremos ab em vez $a * b$. A *ordem* ou *cardinalidade* de um grupo G é o número de elementos de G e denotaremos por $|G|$. Se

G e H são dois grupos, então o *produto direto* de G com H, denotado por $G \times H$, é o comjunto de todos os pares ordenados (g, h), onde $g \in G$ e $h \in H$, com a operação binária

$$(g, h)(g', h') = (gg', hh').$$

É fácil mostrar que $G \times H$ é um grupo com elemento identidade (e, e) e elemento invertível (g^{-1}, h^{-1}). Assim, $G^2 = G \times G$. Generalizando, temos

$$G^n = G \times G \times \cdots \times G.$$

Sejam G um grupo e H um subconjunto de G. Dizemos que H é um *subgrupo* de G, denotado por $H \leq G$, se as seguintes condições são satisfeitas:

1. $H \neq \emptyset$;
2. $ab^{-1} \in H$, para todos $a, b \in H$.

Sejam G um grupo e H um subgrupo de G. Dizemos que H é um *subgrupo normal* de G, denotado por $H \trianglelefteq G$, se

$$gHg^{-1} = H, \forall g \in G.$$

Exemplo 1.1 *Sejam G um grupo e $X = \{xyx^{-1}y^{-1} : x, y \in G\}$. Então $G' = \langle X \rangle$ é um subgrupo normal de G, chamado de* subgrupo dos comutadores *de G.*

Proposição 1.1 *Sejam G um grupo e H um subgrupo de G. Então H é normal e $\dfrac{G}{H}$ é abeliano se, e somente se, $G' \subseteq H$.* ■

Sejam $g \in G$ e

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

Então é claro que $\langle g \rangle$ é um subgrupo de G chamado de *subgrupo cíclico* de G gerado por g. Um grupo G é dito *cíclico* se existir $g \in G$ tal que $G = \langle g \rangle$. A ordem de um elemento $g \in G$, em símbolos $o(g)$, é definida como $o(g) = |\langle g \rangle|$. É fácil verificar que se $o(g)$ é finita, então $o(g)$ é igual ao menor inteiro positivo k tal que $g^k = e$.

Seja $G = \langle g \rangle$ um grupo cíclico de ordem n. Então g^m é um gerador de G se, e somente se, $\text{mdc}(n, m) = 1$.

Proposição 1.2 *Seja H um subgrupo de G tal que $H \subseteq Z(G)$ e $\dfrac{G}{H}$ é cíclico. Então G é abeliano.* ■

A função $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ dada por

$$\phi(n) = |\{m : 1 \leq m \leq n \text{ e } \text{mdc}(n, m) = 1\}|$$

é chamada de *função de Euler*.

O conjunto

$$K = \{z \in \mathbb{C} : |z| = 1\}$$

é claramente um grupo abeliano chamado de *grupo ciclo*.

Um número complexo $z \in \mathbb{C}$ é uma raiz n-ésima da unidade se $z^n = 1$. Assim, se $z^n = 1$, então

$$|z^n| = |z|^n = 1 \Rightarrow |z| = 1.$$

Logo, é fácil verificar que existe $\theta \in [0, 2\pi]$ tal que

$$z = \exp(i\theta) = \cos\theta + i \operatorname{sen}\theta.$$

Portanto, toda raiz n-ésima da unidade pertence ao grupo K. Assim, substituindo $z = \exp(i\theta)$ em $z^n = 1$, obtemos que $\exp(in\theta) = 1$. Portanto, $n\theta$ é um mútiplo de 2π, ou seja,

$$\theta = \frac{2\pi k}{n}$$

para algum $k \in \mathbb{Z}$. Assim, o valor de

$$\exp(\frac{2\pi k}{n} i)$$

depende apenas da classe de congruência de k módulo n e existem precisamente n raízes n-ésimas da unidade. Fazendo

$$\xi = \exp(\frac{2\pi}{n} i)$$

temos que

$$\xi^k = \exp(\frac{2\pi k}{n} i) \text{ e } K_n = \{1, \xi, \ldots, \xi^{n-1}\}$$

é o conjunto de todas as raízes n-ésimas da unidade. É fácil verificar que K_n é um grupo cíclico de ordem n gerado por ξ. Note que, se $m > n$, então, pelo Algoritmo da Divisão,

$$\xi^m = \xi^{qn+r} = (\xi^n)^q \, \xi^r = 1^q \xi^r = \xi^r,$$

onde $0 \leq r < n$. Um gerador do grupo cíclico K_n é chamado de *raiz n-ésima primitiva da unidade*.

Proposição 1.3 *$\xi^k \in K_n$ é uma raiz n-ésima primitiva da unidade se, e somente se,* $\text{mdc}(n,k) = 1$. ■

Sejam G e K dois grupos. Uma aplicação $\psi : G \longrightarrow K$ é um *homomorfismo de grupos* se

$$\psi(ab) = \psi(a)\psi(b), \forall a, b \in G.$$

Um homomorfismo de grupos $\psi : G \longrightarrow K$ é um *isomorfismo* se ψ é bijetiva. Quando existir um isomorfismo entre G e K dizemos que G e K são *isomorfos* e denotaremos por $G \backsimeq K$. Um *endomorfismo* de um grupo G é um homomorfismo $\psi : G \longrightarrow G$. Denotaremos por

$$\text{End}(G) = \{\psi : G \longrightarrow G : \psi \text{ é um homomorfismo}\}.$$

Um *automorfismo* de um grupo G é um isomorfismo $\psi : G \longrightarrow G$. Denotaremos por

$$\text{Aut}(G) = \{\psi : G \longrightarrow G : \psi \text{ é um isomorfismo}\}.$$

Note que, se G é um grupo abeliano, então $\text{End}(G)$ é um anel com respeito às operações de adição e multiplicação de endomorfismos.

Se $G = \langle g \rangle$ é um grupo cíclico de ordem n, então qualquer $\psi \in \text{End}(G)$ é caracterizado por $\psi(g)$. Assim, temos $|\text{End}(G)| = n$, isto é, $\psi(g) = g^k$, $1 \leq k \leq n$. Em particular,

$$|\text{Aut}(G)| = \phi(n).$$

Proposição 1.4 *Sejam $G = \langle g \rangle$ um grupo cíclico de ordem n, L um grupo qualquer e $b \in L$. Se $o(b)$ divide n, então existe um único homomorfismo $\psi : G \longrightarrow L$ tal que $\psi(g) = b$ e $\psi(g^r) = b^r$.* ■

Um elemento $\psi \in \text{Aut}(G)$ é dito *automorfismo interno* se existir $g \in G$ tal que $\psi(x) = gxg^{-1}$, para todo $x \in G$. Denotaremos por

$$\text{Inn}(G) = \{\psi \in \text{Aut}(G) : \psi \text{ é um automorfismo}\}.$$

Teorema 1.1 *Seja $\psi : G \longrightarrow K$ um homomorfismo de grupos. Então*

$$\frac{G}{\ker \psi} \simeq \text{Im}\,\psi.$$

■

g	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\chi_0(g)$	1	1	1	1
$\chi_1(g)$	1	i	$-i$	-1
$\chi_2(g)$	1	$-i$	i	-1
$\chi_3(g)$	1	-1	-1	i

Tabela 1.1: Caracteres de G

Proposição 1.5 *Seja G um grupo. Então* $\mathrm{Inn}(G)$ *é um subgrupo normal de* $\mathrm{Aut}(G)$ *e*

$$\frac{G}{Z(G)} \backsimeq Inn(G).$$

■

Seja G um grupo abeliano de ordem n. Um *caráter* sobre G é um homomorfismo de grupos $\chi : G \to \mathbb{C}^*$. Como $g^n = e$, para todo $g \in G$, temos que $[\chi(g)]^n = \chi(e) = 1$. Logo, $\chi(g)$ é uma raiz n-ésima da unidade para todo $g \in G$. Além disso,

$$\chi(gh) = \chi(g)\chi(h), \forall g, h \in G.$$

O conjunto

$$\widehat{G} = \{\chi : \chi \text{ é um caráter sobre } G\}$$

é um grupo abeliano com a operação

$$(\chi \circ \psi)(g) = \chi(g)\psi(g), \forall g \in G.$$

O elemento identidade χ_0 é definido por $\chi_0(g) = 1$, para todo $g \in G$, e o elemento inverso χ^{-1} é definido por $\chi^{-1}(g) = \chi(g^{-1})$, para todo $g \in G$. O grupo $\widehat{G}$ é chamado o *dual* ou *grupo dos caracteres* de G.

Exemplo 1.2 *Seja $G = \mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Então $\widehat{G}$ é dado na Tabela* 1.2

Proposição 1.6 *Seja G um grupo finito. Então*:

1. *Se G é um grupo cíclico, então $G \backsimeq \widehat{G}$.*
2. *Se H e K são dois grupos abelianos finitos, então $\widehat{(H \times K)} \backsimeq \widehat{H} \times \widehat{K}$*
3. *Se G é um grupo abeliano, então $G \backsimeq \widehat{G}$.*

$\circ$	χ_0	χ_1	χ_2	χ_3
χ_0	χ_0	χ_1	χ_2	χ_3
χ_1	χ_1	χ_3	χ_0	χ_2
χ_2	χ_2	χ_0	χ_3	χ_1
χ_3	χ_3	χ_2	χ_1	χ_0

Tabela 1.2: O grupo dual de G

Demonstração. 1. Sejam $G = \langle g \rangle$ e $|G| = n$. Então

$$\psi(g) \in K_n = \{1, \xi, \ldots, \xi^{n-1}\}.$$

Como $o(\xi) = n$ e divide $o(g)$ temos, pela Proposição 1.4, que existe um único $\psi \in \widehat{G}$ tal que $\psi(g) = \xi$ e $\psi(g^r) = \xi^r$.

Afirmação. $\widehat{G} = \langle \psi \rangle$. De fato, seja $\varphi \in \widehat{G}$. Então

$$(\varphi(g))^n = \varphi(g^n) = \varphi(e) = 1,$$

ou seja, $\varphi(g)$ é uma raiz n-ésima da unidade. Logo,

$$\varphi(g) \in K_n \Longrightarrow \varphi(g) = \xi^k,$$

para algum $k \in \mathbb{Z}$, ou seja,

$$\varphi(g) = \xi^k = (\psi(g))^k \Longrightarrow \varphi \in \langle \psi \rangle.$$

2. Sejam

$$\widehat{H} \times \widehat{K} = \{(\varphi, \psi) : \varphi \in \widehat{H} \text{ e } \psi \in \widehat{K}\}.$$

e

$$\omega: \begin{array}{l} \widehat{H} \times \widehat{K} \to \widehat{(H \times K)} \\ (\varphi, \psi) \mapsto \omega((\varphi, \psi)) \end{array} \quad \text{e} \quad \omega((\varphi, \psi)): \begin{array}{l} H \times K \to \mathbb{C}^* \\ (h, k) \mapsto \varphi(h)\psi(k) \end{array}.$$

É claro que ω é um homomorfismo de grupos sobrejetor. Dado $(\varphi, \psi) \in \ker \omega$. Então

$$\omega((\varphi, \psi))((h, k)) = 1,$$

isto é, $\varphi(h)\psi(k) = 1$, para todo $(h, k) \in H \times K$. Em particular, $\varphi(h) = \varphi(h)\psi(e) = 1$, para todo $h \in H$. Portanto, $\varphi = id$. De modo análogo, mostra-se que $\psi = id$. Assim, ω é injetora.

3. Se G é um grupo abeliano. Então,

$$G \backsimeq G_1 \times \cdots \times G_s,$$

onde G_i é um grupo cíclico, para cada $i = 1, \ldots, s$. Pelo item 1, temos que $G_i \backsimeq \widehat{G_i}$, para cada $i = 1, \ldots, s$. Logo,

$$G \backsimeq \widehat{G_1} \times \cdots \times \widehat{G_s}$$

e pelo item 2,

$$G \backsimeq \widehat{\widehat{G}}.$$

■

Proposição 1.7 *Seja G um grupo. Então $\psi \in \mathrm{End}(G)$ se, e somente se,*

$$H = \{(g, \psi(g)) : g \in G\}$$

é um subgrupo de $G \times G$.

Demonstração. Suponhamos que $H \leq G \times G$. Dados $(g_1, \psi(g_1)), (g_2, \psi(g_2)) \in H$. Então

$$(g_1 g_2, \psi(g_1)\psi(g_2)) = (g_1, \psi(g_1))(g_2, \psi(g_2)) \in H.$$

Logo, $\psi(g_1 g_2) = \psi(g_1)\psi(g_2)$, isto é, $\psi \in \mathrm{End}(G)$. Reciprocamente, é claro que $H \neq \emptyset$. Dados $(g_1, \psi(g_1)), (g_2, \psi(g_2)) \in H$. Então

$$\begin{aligned}(g_1, \psi(g_1))(g_2, \psi(g_2))^{-1} &= (g_1, \psi(g_1))(g_2^{-1}, \psi(g_2^{-1})) \\ &= (g_1 g_2^{-1}, \psi(g_1)\psi(g_2^{-1})) \\ &= (g_1 g_2^{-1}, \psi(g_1 g_2^{-1})) \in H.\end{aligned}$$

Assim, temos $H \leq G \times G$. ■

Proposição 1.8 *Sejam G, H grupos e $\psi : G \times H \longrightarrow G \times H$ um homomorfismo de grupos definido por*

$$\psi(g, h) = (g, \varphi(g)),$$

onde φ é um homomorfismo de grupos de G em H. Então $K = \psi(G \times H) \trianglelefteq G \times H$ se, e somente se, $\varphi(G) \subseteq Z(H)$.

Demonstração. $(g,h)(c,\varphi(c))(g^{-1},h^{-1}) \in K$, para todo $g,c \in G$ e $h \in H$ se, e somente se, $(gcg^{-1}, h\varphi(c)h^{-1}) \in K$, para todos $g,c \in G$ e $h \in H$, se e somente se, $\varphi(c)d = d\varphi(c)$, para todos $g,c \in G$ e $d = \varphi(g^{-1})h \in H$ se, e somente se, $\varphi(G) \subseteq Z(H)$. ■

Proposição 1.9 *Seja G um grupo. Então G é abeliano se, e somente se, $\psi : G \times G \longrightarrow G$ dado por $\psi(a,b) = ab$ é um homomorfismo.* ■

Proposição 1.10 *Todo homomorfismo de grupos $\psi : G^k \longrightarrow G$ admite a decomposição*

$$\psi(g_1,\ldots,g_k) = \prod_{i=1}^{k} \psi(e,\ldots,g_i,\ldots,e),$$

onde os fatores no produto podem ser tomados em qualquer ordem.

Demonstração. A decomposição é imediata da definição de homomorfismo. Para demonstrar a comutatividade, consideremos $k = 2$.

$$\psi(g_1,g_2) = \psi[(g_1,e)(e,g_2)] = \psi(g_1,e)\psi(e,g_2)$$

e

$$\psi(g_1,g_2) = \psi[(e,g_2)(g_1,e)] = \psi(e,g_2)\psi(g_1,e).$$

Assim, temos que

$$\psi(g_1,g_2) = \psi(g_1,e)\psi(e,g_2) = \psi(e,g_2)\psi(g_1,e),$$

pois os elementos (g_1,e) e (e,g_2) comutam. ■

Sejam G um grupo e $H_1,\ldots,H_n$ subgrupos de G. Dizemos que G é *produto direto interno* de $H_1,\ldots,H_n$, em símbolos $G = H_1 \oplus \cdots \oplus H_n$ se as seguites condições são satisfeitas:

1. Para todo $g \in G$ existem únicos $h_1 \in H_1,\ldots,h_n \in H_n$ tais que

$$g = h_1 \cdots h_n.$$

2. $hk = kh$, para todo $h \in H_i$ e $k \in H_j$, com $i \neq j$.

Teorema 1.2 *Sejam G um grupo e $H_1,\ldots,H_n$ subgrupos de G. Então $G = H_1 \oplus \cdots \oplus H_n$ se, e somente se, as seguintes condições são satisfeitas*:

1. $G = H_1 \cdots H_n$;

2. $H_i \trianglelefteq H$, *para cada* $i = 1, \ldots, n$;

3. $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$, *para cada* $i = 1, \ldots, n$. ■

Corolário 1.1 *Sejam G um grupo e $H_1, \ldots, H_n$ subgrupos de G. Se $G = H_1 \oplus \cdots \oplus H_n$, então G é isomorfo ao produto direto $H_1 \times \cdots \times H_n$.* ■

Sejam G um grupo e H, K subgrupos próprios de G. Dizemos que G é *fatorizável* em H e K se as seguites condições são satisfeitas:

1. $G = HK$.

2. $hk = kh$, para todo $h \in H$ e $k \in K$.

Um grupo G é *decomponível* se G é fatorizável e

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

Note que, todo produto direto de grupos $H \times K$ é fatorizável. A recíproca não é necessariamente verdade.

Exemplo 1.3 *Sejam*

$$G = \{(x, y, xy) : x, y \in \mathbb{Z}_3^*\},$$

um grupo e

$$H = \{(x, 1, x) : x \in \mathbb{Z}_3^*\}, K = \{(1, y, y) : y \in \mathbb{Z}_3^*\}.$$

subgrupos próprios de G. Então

$$G = HK \neq H \times K.$$

Mas H, K são isomorfos a $\mathbb{Z}_2$ e $G \backsimeq \mathbb{Z}_2 \times \mathbb{Z}_2$.No entanto, se G é decomponível, então ele é isomorfo a um produto direto.

Proposição 1.11 *Seja G um grupo fatorizável com $G = HK$. Então*:

1. *H e K são subgrupos normais de G*;

2. *$H \cap K$ é um subgrupo central, isto é, $H \cap K \subseteq Z(G)$*;

3. *Se H e K são abelianos, então G é decomponível*;

4. *Se $H \cap K = \{e\}$, então G é decomponível*;

5. *Se H ou K é abeliano, então G é decomponível ou K é um subgrupo normal de H e $G = H$*;

6. *Se H e K são não abelianos e $H \cap K \neq \{e\}$, então $|G| \geq 32$.*

Demonstração. 1. Dados $g \in G$ e $a \in H$ temos que $g = hk = kh$, com $h \in H$ e $k \in K$. Logo,

$$gag^{-1} = hka(hk)^{-1} = hkak^{-1}h^{-1} = hah^{-1} \in H,$$

ou seja, H é um subgrupo normal. De maneira análoga mostra-se que K é normal.

2. Dados $g \in G$ e $a \in H \cap K$. Então $g = hk = kh$ com $h \in H$ e $k \in K$. Logo,

$$ag = a(hk) = (ah)k = (ha)k = h(ka) = (hk)a = ga.$$

Assim, $H \cap K \subseteq Z(G)$.

3. Se H e K são abelianos, então para todos $g, g' \in G$ temos que

$$\begin{aligned} gg' &= (hk)(h'k') = h(kh')k' = h(h'k)k' \\ &= (hh')(kk') = (h'h)(k'k) = h'(hk')k \\ &= (h'k')(hk) = g'g. \end{aligned}$$

Logo, G é abeliano. Portanto, H e K são subgrupos normais de G, ou seja, G é decomponível.

4. Se $H \cap K = \{e\}$, então G é produto direto de dois subgrupos normais. Portanto, G é decomponível.

5. Seja $L = H \cap K$. Se H é abeliano, obtemos que $H = LM$ com $L \cap M = \{e\}$. Assim, $H = L \times M$. Portanto, $G = MK$ com $M \cap K = \{e\}$ e $MK = KM$. Assim, temos que G é decomponível ou $M = \{e\}$.

6. Sejam $L = H \cap K$ e $\varphi : G \longrightarrow \dfrac{H}{L} \times \dfrac{H}{L}$ dado por $\varphi(g) = (hl, kl)$. É fácil verificar que φ é um homomorfismo sobrejetor. Assim,

$$\frac{G}{L} \backsimeq \frac{H}{L} \times \frac{H}{L} \text{ e } |G| = |L| \left|\frac{H}{L}\right| \left|\frac{K}{L}\right|.$$

Como $|L| \geq 2$, H e K são não abelianos temos, pela Proposição 1.2, que

$$\left|\frac{H}{L}\right| \geq 4 \text{ e } \left|\frac{K}{L}\right| \geq 4.$$

Portanto, $|G| \geq 32$. ■

1.2 Módulos

Seja R um anel comutativo com unidade. Um *R-módulo* V sobre R é grupo comutativo aditivo junto com uma aplicação $R \times V \to V$, $(x, \mathbf{v}) \to x\mathbf{v}$, tal que as seguintes propriedades valem:

1. $x(y\mathbf{v}) = (xy)\mathbf{v}$, para todos $x, y \in R$ e $\mathbf{v} \in V$.

2. $x(\mathbf{u} + \mathbf{v}) = x\mathbf{u} + x\mathbf{v}$, para todo $x \in R$ e $\mathbf{u}, \mathbf{v} \in V$.

3. $(x + y)\mathbf{v} = x\mathbf{v} + y\mathbf{v}$, para todos $x, y \in R$ e $\mathbf{v} \in V$.

4. $1\mathbf{v} = \mathbf{v}$, para todo $\mathbf{v} \in V$.

Note que, se R é um corpo, então um R-módulo é espaço vetorial sobre R. Além disto, se V é um R-módulo, então a aplicação

$$\phi : R \to \mathrm{End}(V) \text{ dada por } \phi(x) = \varphi_x,$$

onde $\varphi_x(\mathbf{v}) = x\mathbf{v}$, para cada $x \in R$, é um homomorfismo de anéis. Reciprocamente, seja V é grupo comutativo aditivo e suponhamos que $\phi : R \to \mathrm{End}(V)$ é um homomorfismo de anéis tal que $\phi(1) = id_V$. Então a aplicação $R \times V \to V$, $(x, \mathbf{v}) \to \phi(x)(\mathbf{v}) = x\mathbf{v}$ induz em V uma estrutura de R-módulo.

Um subconjunto não vazio W de um R-módulo V é um *R-submódulo* de V se as seguintes condições são satisfeitas:

1. para todos $\mathbf{v}, \mathbf{w} \in W$, tem-se $\mathbf{v} - \mathbf{w} \in W$;

2. Para todo $x \in R$ e $\mathbf{w} \in W$, tem-se $x\mathbf{w} \in W$.

Exemplo 1.4 *Seja G qualquer grupo abeliano e escrito a operação de G como $+$. Então é fácil verificar que G é um $\mathbb{Z}$-módulo com a operação*

$$\mathbb{Z} \times G \to G, (n, g) \to ng,$$

onde

$$ng = \begin{cases} (n-1)g + g & se\ n > 0 \\ 0 & se\ n = 0 \\ (-n)(-g) & se\ n < 0. \end{cases}$$

Sejam U e V dois R-módulos. Uma aplicação $\psi : U \longrightarrow V$ é um *R-homomorfismo* se as seguintes condições são satisfeitas:

1. $\psi(uv) = \psi(u)\psi(v), \forall u, v \in U$;

2. $\psi(xu) = x\psi(u), \forall u \in U$ e $x \in R$.

Um R-homomorfismo $\psi : U \longrightarrow V$ é um *R-isomorfismo* se ψ é bijetiva.. Denotaremos por

$$\mathrm{Hom}_R(U, V) = \{\psi : U \longrightarrow V : \psi \text{ é um } R\text{-homomorfismo}\}.$$

Em particular, quando $U = V$ temos que $\mathrm{Hom}_R(U, V) = \mathrm{End}_R(V)$. Note que, o Teorema 1.2, aplica-se para R-módulos.

Proposição 1.12 *Sejam V um R-módulo, $W_1, \ldots, W_n$ R-submódulos de V e π_i as projeções associadas a W_i. Se $V = W_1 \oplus \cdots \oplus W_n$, então as seguintes condições são satisfeitas*:

1. $\sum_{i=1}^{n} \pi_i = id_V$;

2. $\pi_i^2 = \pi_i$, *para cada* $i = 1, \ldots, n$;

3. $\pi_i \pi_j = 0_V$, *para cada* $i, j = 1, \ldots, n$, *com* $i \neq j$.

Reciprocamente, se $\pi_i \in \mathrm{End}_R(V)$ satisfaz 1., 2. *e* 3. *e $W_i = \mathrm{Im}\,\pi_i$, então $V = W_1 \oplus \cdots \oplus W_n$ e π_i são as projeções associadas a W_i.* ■

Teorema 1.3 *Sejam V um R-módulo e $W_1, \ldots, W_n$ R-submódulos de V. Se $V = W_1 \oplus \cdots \oplus W_n$ e $\phi \in \mathrm{End}_R(V)$, então*

$$\phi = \sum_{i,j=1}^{n} \pi_i \phi \pi_j.$$

Demonstração. Queremos demonstrar que

$$\phi(\mathbf{v}) = \sum_{i,j=1}^{n} \pi_i \phi \pi_j(\mathbf{v}), \forall \mathbf{v} \in V.$$

Como $\mathbf{v} = \mathbf{w}_1 + \cdots + \mathbf{w}_n$ temos, pela Proposição 1.12, que

$$\begin{aligned}
\phi(\mathbf{v}) &= id_V(\phi(\mathbf{v})) \\
&= \sum_{i=1}^{n} \pi_i(\phi(\mathbf{v})) \\
&= \sum_{i=1}^{n} (\pi_i \phi)(\sum_{j=1}^{n} \pi_j(\mathbf{v})) \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} (\pi_i \phi \pi_j)(\mathbf{v}).
\end{aligned}$$

■

Corolário 1.2 *Sejam V um R-módulo e $W_1, \ldots, W_n$ R-submódulos de V. Se $V = W_1 \oplus \cdots \oplus W_n$ e $\phi \in \mathrm{End}_R(V)$, então $\mathrm{End}_R(V)$ é isomorfo ao conjunto das matrizes quadradas de ordem n, $\mathbf{A} = (\phi_{ij})$, onde $\phi_{ij} = \pi_i \phi \pi_j \in \mathrm{Hom}_R(W_j, W_i)$.* ■

Exemplo 1.5 *Se $V = \mathbb{Z}_3 \oplus \mathbb{Z}_2$, então $\mathrm{End}_{\mathbb{Z}}(V)$ é isomorfo ao conjunto das matrizes*

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

Vamos denotar por $\mathcal{Z}_n$ o anel dos inteiros módulo n. Neste caso, é fácil verificar que o anel $\mathrm{End}(\mathbb{Z}_n)$ é isomorfo ao anel $\mathcal{Z}_n$.

O *expoente* de um grupo finito G é o menor inteiro positivo m tal que $g^m = e$. Um grupo aditivo G é *abeliano elementar* se o expoente de G é um número primo p.

Proposição 1.13 *Um grupo G é abeliano elementar com expoente p se, e somente se, $G \backsimeq \mathcal{Z}_p^m$, para algum $m \geq 1$.*

Demonstração. Suponhamos que G é abeliano elementar com expoente p. Então $pg = 0$, para todo $g \in G$. Seja

$$\cdot : \mathcal{Z}_p \times G \longrightarrow G \text{ dada por } \cdot(\overline{x}, g) = xg.$$

Então é fácil verificar que G com esta operação é um espaço vetorial sobre $\mathcal{Z}_p$ de dimensão m, para algum $m \geq 1$. Portanto, G é isomorfo a $\mathcal{Z}_p^m$. ■

Note que, o grupo aditivo de qualquer corpo finito F é abeliano elementar e, reciprocamente, qualquer grupo abeliano elementar pode ser dado um estrutura de um corpo finito.

Seja G um grupo abeliano e m um inteiro positivo. Então

$$mG = \{mg : g \in G\}$$

é um subgrupo de G, pois mG é imagem do homomorfismo grupos $\varphi : G \longrightarrow G$ definido por $\varphi(g) = mg$. Assim, todo grupo abeliano, com $mG = \{0\}$ é um $\mathcal{Z}_m$-módulo.

Proposição 1.14 *Se o expoente n de G não é um número primo e m é divisor de n, então mG é um subgrupo de G com expoente $\frac{n}{m}$. Além disto, se $\frac{n}{m}$ é um número primo, então mG é grupo abeliano elementar.*

Demonstração. Para todo $h \in mG$ existe $g \in G$ tal que $h = mg$. Logo,

$$(\frac{n}{m})h = \frac{n}{m}mg = ng = 0.$$

Agora devemos mostrar que $\frac{n}{m}$ é o menor inteiro positivo tal que $\frac{n}{m}h = 0$, para todo $h \in mG$.

Suponhamos que $kh = 0$ e $h = mg$. Então $kmg = 0$, ou seja, $km = rn$ para algum $r \in \mathbb{Z}$. Portanto, $\frac{n}{m}$ divide k. ■

Para finalizar esta seção vamos considerar o seguinte grupo

$$G = \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_m},$$

onde

$$d_1|d_2| \cdots |d_m.$$

Seja g_i o gerador de $\mathbb{Z}_{d_i}$. Então cada $g \in G$ tem a forma

$$g = g_1^{\alpha_1} \cdots g_m^{\alpha_m},$$

para $0 \leq \alpha_i \leq (d_i - 1)$. Assim, uma base normal para G é o conjunto

$$\{g_1, \ldots, g_m\}.$$

É útil considerar os α_i como elementos do anel $\mathcal{Z}_{d_i}$, de modo que a exponenciação define um isomorfismo entre o grupo cíclico $\mathbb{Z}_{d_i}$ e o grupo cíclico aditivo dos inteiros módulo d_i. Note que se $s \mid t$, então

$$\mathcal{Z}_s \simeq \frac{\mathcal{Z}_t}{s\mathcal{Z}_t}.$$

Seja R_{ij} o grupo de homomorfismos de grupos de $\mathbb{Z}_{d_i}$ em $\mathbb{Z}_{d_j}$ (quando $i = j$, $R_{ii} = \text{End}(\mathbb{Z}_{d_i})$). Então o anel $\text{End}(G)$ é isomorfo ao anel das matrizes quadradas de ordem m, $A = (\varphi_{ij})$, onde $\varphi_{ij} \in R_{ij}$.

De fato, se $g \in G$ e

$$g = g_1 \cdots g_m, g_i \in \mathbb{Z}_{d_i},$$

então é claro que $\varphi : G \longrightarrow G$ dada por

$$\varphi(g) = \prod_{i=1}^{m} \prod_{j=1}^{m} \varphi_{ij}(g_i)$$

é um endomorfismo.

Reciprocamente, dado $\varphi \in \mathrm{End}(G)$. Se $g_i \in \mathbb{Z}_{d_i}$ e $\varphi(g_i) = \prod_{j=1}^{m} g_{ij}$, com $g_{ij} \in \mathbb{Z}_{d_j}$, então

$$\varphi_{ij} : \mathbb{Z}_{d_i} \longrightarrow \mathbb{Z}_{d_j}$$

dada por $\varphi_{ij}(g_i) = g_{ij}$ é um homomorfismo. Não é difícil mostrar que esta correspondência preserva soma e produto.

Finalmente, de $\varphi \in \mathrm{End}(G)$ temos que

$$\varphi(g) = \prod_{i=1}^{m} \varphi(g_i)^{\alpha_i} \quad \text{e} \quad \varphi(g_i) = \prod_{j=1}^{m} \varphi_{ij}(g_i),$$

onde $\varphi_{ij}(g_i) = g_j^{\alpha_{ij}}$, com $0 \leq \alpha_{ij} \leq (d_{ij} - 1)$. Como $[\varphi(g_i)]^{d_i} = e$ se, e somente se, $g_j^{d_i \alpha_{ij}} = e$ para $j = 1, \ldots, m$, se, e somente se, $d_j |_{d_i \alpha_{ij}}$ para $j = 1, \ldots, m$, temos que

1. Se $j \leq i$, então $d_j | d_i$ e $a_{ij} \in \mathcal{Z}_{d_j}$.

2. Se $j > i$, então $d_i | d_j$ e

$$a_{ij} \in \frac{d_j}{d_i} \mathcal{Z}_{d_i}.$$

Portanto,

$$\varphi(g) = \prod_{i=1}^{m} g_i^{\sum_{i=1}^{m} a_{ij} a_i}.$$

Assim, podemos identificar φ com a matriz $A = (\alpha_{ij})$, $\alpha_{ij} \in \mathcal{Z}_{d_j}$ se $j \leq i$ e $\alpha_{ij} \in \frac{d_j}{d_i} \mathcal{Z}_{d_i}$ se $j > i$.

Do resultado acima segue que o grupo de automorfismos de G é isomorfo ao grupo multiplicativo das matrizes, $A = (a_{ij})$, que tem inverso no anel de todas estas matrizes.

Note que, podemos assumir, sem perda de generalidade, que $\widehat{\alpha}_{ij} \in \mathcal{Z}_{d_m}$ e

$$A = \begin{bmatrix} \widehat{\alpha}_{11} & \frac{d_2}{d_1}\widehat{\alpha}_{12} & \ldots & \frac{d_m}{d_1}\widehat{\alpha}_{1m} \\ \widehat{\alpha}_{21} & \widehat{\alpha}_{22} & \ldots & \frac{d_m}{d_2}\widehat{\alpha}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \widehat{\alpha}_{m1} & \widehat{\alpha}_{m2} & \ldots & \widehat{\alpha}_{mm} \end{bmatrix},$$

Logo, todas as matrizes A' com a estrutura acima e tal que $\theta\,(A') = A$, onde

$$\theta(\widehat{\alpha}'_{ij}) = \begin{cases} \widehat{\alpha}'_{ij}\,(\mathrm{mod}\,d_j) & \text{se } j \leq i \\ \widehat{\alpha}'_{ij}\,(\mathrm{mod}\,d_i) & \text{se } j > i, \end{cases}$$

descreve o mesmo endomorfismo como A. Pode-se mostrar que θ preserva a não-singularidade de uma matriz.

Capítulo 2

Distância de Hamming

O objetivo deste capítulo é estudar, sobre certas condições, a mínima distância de Hamming de um código sob um grupo qualquer.

2.1 Códigos

Um alfabeto é qualquer conjunto não vazio F. Um código C sobre um alfabeto F é qualquer subconjunto não vazio do conjunto $F^{\mathbb{I}}$ de todas as seqüências

$$\mathbf{c} = \{c_i : i \in \mathbb{I}\} = (c_i)_{i\in\mathbb{I}},$$

onde $c_i \in F$ e $\mathbb{I} \subseteq \mathbb{Z}$. Quando

$$\mathbb{I} = \{i : 1 \leq i \leq n\}$$

temos que $F^n = F^{\mathbb{I}}$.

Um *código de bloco* C de comprimento n sobre um alfabeto F é qualquer subconjunto não vazio do conjunto F^n de todas as palavras (ou seqüências)

$$\mathbf{c} = \{c_i : i \in \mathbb{I}\}.$$

O alfabeto F, salvo menção explícita em contrário, será finito.

A *dimensão do código* C é $k = \log_{|F|} |C|$ símbolos por blocos. Note que k não necessariamente é inteiro. A taxa do código é

$$r = \frac{k}{n}.$$

Também notamos que $|C|$ é limitado, isto é,

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

A *distância de Hamming* $d_H(\mathbf{c},\mathbf{c}')$ entre duas palavras $\mathbf{c}$, $\mathbf{c}' \in F^n$ é o número de componentes nas quais elas diferem.

Se $|C| \geq 2$, então a mínima distância de Hamming $d_H(C)$ de C é definida por

$$d_H(C) = \min\{d_H(\mathbf{c}, \mathbf{c}') : \mathbf{c}, \mathbf{c}' \in C, \mathbf{c} \neq \mathbf{c}'\}$$

Note que, $1 \leq d_H(C) \leq n$. Se $|C| = 1$, então $d_H(C) = \infty$ por convenção.

Um código de bloco de comprimento n com dimensão k e mínima distância de Hamming $d = d_H(C)$ é chamado um $[n, k, d]$-código.

Definição 2.1 *Seja $\mathbb{J}$ um subconjunto de $\mathbb{I}$. Então a projeção sobre $\mathbb{J}$ é o mapeamento*

$$\begin{aligned} P_{\mathbb{J}}: \quad & F^{\mathbb{I}} \longrightarrow F^{\mathbb{J}} \\ & \mathbf{c} \longmapsto P_{\mathbb{J}}(\mathbf{c}), \end{aligned}$$

onde $P_{\mathbb{J}}(\mathbf{c}) = \{c_i; i \in \mathbb{J}\}$.

Observação 2.1 *A imagem de C sobre $P_{\mathbb{J}}$ é*

$$P_{\mathbb{J}}(C) = \{P_{\mathbb{J}}(\mathbf{c}) : \mathbf{c} \in C\}.$$

Como $P_{\mathbb{J}}(C)$ é um subconjunto de $F^{\mathbb{J}}$ temos que $|P_{\mathbb{J}}(C)| \leq |F|^{|\mathbb{J}|}$.

Exemplo 2.1 *Sejam*

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

um $[4,2,2]$-código sobre o alfabeto $F = \{0,1\}$, $\mathbb{I} = \{1,2,3,4\}$ e $\mathbb{J} = \{3,4\}$. Então

$$P_{\mathbb{J}}(C) = \{(0,0), (1,1)\} \neq F^{\mathbb{J}} = \{(0,0), (1,0), (0,1), (1,1)\}.$$

Proposição 2.1 (Singleton Bound) *Se C é um $[n, k, d]$-código sobre um alfabeto F, com $k > 0$, então $d \leq n - k + 1$.*

Demonstração. Suponhamos, por absurdo, que $d > n - k + 1$, ou ainda, $k > n - d + 1$. Consideremos qualquer subconjunto $\mathbb{J}$ de $\mathbb{I}$, com $|\mathbb{J}| = n - d + 1$. Como

$$|P_{\mathbb{J}}(C)| \leq |F|^{|\mathbb{J}|} = |F|^{n-d+1} < |F|^k = |C|$$

temos que a projeção sobre $\mathbb{J}$ de pelo menos duas palavras distintas $\mathbf{c}$ e $\mathbf{c}'$ são iguais, isto é, $P_{\mathbb{J}}(\mathbf{c}) = P_{\mathbb{J}}(\mathbf{c}')$, com $\mathbf{c} \neq \mathbf{c}'$. Portanto,

$$d_H(\mathbf{c}, \mathbf{c}') \leq n - |\mathbb{J}| = n - (n - d + 1) = d - 1 < d,$$

o que é uma contradição. ■

Definição 2.2 *Um $[n, k, d]$-código sobre um alfabeto F, com $k > 0$, tal que $d = n - k + 1$ é chamado um código de máxima distância separável (MDS).*

Observação 2.2 *Como n e d são inteiros temos que a dimensão k do código MDS é um inteiro, pois $d = n - k + 1$ ou $k = n - d + 1$.*

Definição 2.3 *Um conjunto de informação para um código C com dimensão inteira k é qualquer subconjunto $\mathbb{J}$ de $\mathbb{I}$, com $|\mathbb{J}| = k$, tal que $P_{\mathbb{J}}(C) = F^{\mathbb{J}}$, isto é, $P_{\mathbb{J}}$ restrito a C é uma bijeção.*

Exemplo 2.2 *Sejam*

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

um $[4, 2, 2]$-código sobre o alfabeto $F = \{0, 1\}$, $\mathbb{I} = \{1, 2, 3, 4\}$ e $\mathbb{J} = \{3, 4\}$. Então

$$P_{\mathbb{J}}(C) = \{(0,0), (1,1)\} \neq F^{\mathbb{J}} = \{(0,0), (1,0), (0,1), (1,1)\}.$$

Portanto, $\mathbb{J} = \{3, 4\}$ não é um conjunto de informação. Se $\mathbb{J} = \{2, 3\}$, então $\mathbb{J}$ é um conjunto de informação, pois

$$P_{\mathbb{J}}(C) = \{(0,0), (1,0), (0,1), (1,1)\} = F^{\mathbb{J}}.$$

Proposição 2.2 *Se C é um $[n, k, d]$-código MDS sobre um alfabeto F, com $k \geq 1$, então todo subconjunto $\mathbb{J}$ de $\mathbb{I}$, com $|\mathbb{J}| = k$, é um conjunto de informação de C.*

Demonstração. Suponhamos, por absurdo, que exista $\mathbb{J} \subseteq \mathbb{I}$, com $|\mathbb{J}| = k$, que não seja um conjunto de informação de C. Então, existem $\mathbf{c}, \mathbf{c}' \in C$, $\mathbf{c} \neq \mathbf{c}'$ tais que $P_{\mathbb{J}}(\mathbf{c}) = P_{\mathbb{J}}(\mathbf{c}')$, pois caso contrário, $P_{\mathbb{J}}$ restrito a C seria bijeção. Logo, $\mathbf{c}$ e $\mathbf{c}'$ têm $|\mathbb{J}| = k$ componentes iguais. Portanto,

$$d_H(\mathbf{c}, \mathbf{c}') = n - k < n - k + 1 = d,$$

o que é uma contradição, pois C é um MDS. ■

Observação 2.3 *Se C não é um código MDS não implica que $\mathbb{J}$ é um conjunto de informação. Confira o exemplo anterior, onde $d = 2$ e $\mathbb{J} = \{3, 4\}$.*

Quando $F = GF(q) = F_q$ é o corpo de Galois com q elementos, um código de comprimento n sobre F_q é *linear* se ele é um subespaço do espaço vetorial F_q^n. Neste caso, o peso de Hamming $w_H(\mathbf{c})$ de uma palavra código não nula $\mathbf{c} \in F_q^n$ é o número de componentes diferentes de zero. Assim,

$$d_H(\mathbf{c}, \mathbf{c}') = d_H(\mathbf{c} - \mathbf{c}', \mathbf{0}) = w_H(\mathbf{c} - \mathbf{c}')$$

e a dimensão do código é um número inteiro.

Seja C um $[n, k, d]$-código linear sobre F_q. Se $\{\mathbf{c}_1, \ldots, \mathbf{c}_k\}$ é uma base de C, então a imersão $g : F_q^k \hookrightarrow F_q^n$ dada por,

$$g((u_1, \ldots, u_k)) = \left(\sum_{i=1}^{k} u_i c_{i1}, \ldots, \sum_{i=1}^{k} u_i c_{in} \right),$$

onde $\mathbf{c}_i = (c_{i1}, \ldots, c_{in}), 1 \leq i \leq k$, é um *codificador* para o código C. A $k \times n$ matriz $\mathbf{G} = (c_{ij})$ que descreve a aplicação linear g é chamada uma *matriz geradora* do código C. Assim, C consiste de q^k combinações lineares $\mathbf{uG}$, onde $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ é chamada uma *seqüência de informação* ou *mensagem*.

Exemplo 2.3 *Uma matriz geradora para o $[7, 4, 3]$-código linear C sobre F_2 é*

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

Observação 2.4 *Como a base para um $[n, k, d]$-código linear C sobre F_q não é única temos que a matriz geradora $\mathbf{G}$ para C também não é única. Desde que operações elementares de linhas deixa o código C invariante, podemos escolher uma base para C tal que a matriz geradora $\mathbf{G}'$ é da forma*

$$\mathbf{G}' = [\ \mathbf{I}_k \quad \mathbf{P}\ ],$$

onde $\mathbf{I}_k$ é a $k \times k$ matriz identidade e $\mathbf{P}$ é uma $k \times (n - k)$ matriz. Neste caso, dizemos que $\mathbf{G}'$ está na forma canônica.

Se a matriz geradora $\mathbf{G}$ de um $[n, k, d]$-código linear C sobre F_q está na forma canônica, então os primeiros k símbolos de uma palavra código $\mathbf{c} \in C$ são chamados de *símbolos de informações*, os quais são escolhidos arbitrariamente e o restante, chamados *símbolos de verificação de paridade*, são determinados. Sejam C_1 e C_2 dois $[n, k, d]$-código linear sobre F_q. Dizemos que C_1 e C_2 são *equivalentes* se existirem matrizes geradoras $\mathbf{G}_1$ e $\mathbf{G}_2$ para C_1 e C_2, respctivamente, e uma matriz de permutação $\mathbf{Q}$ tal que

$$\mathbf{G}_2 = \mathbf{G}_1\mathbf{Q}.$$

Um $[n, k, d]$-código linear C sobre F_q é *sistemático* se ele possui um conjunto de informação, isto é, se existir um subconjunto $\mathbb{J}$ de $\mathbb{I}$ tal que $|\mathbb{J}| = k$ ou, equivalentemente, se existir exatamente uma palavra código para todas as possíveis escolhas de coordenadas nas k-posições, isto é, a matriz geradora $\mathbf{G}$ do código C é da forma

$$\mathbf{G} = [\ \mathbf{I}_k \quad \mathbf{P}\ ].$$

Seja $g : F_q^k \hookrightarrow F_q^n$ um codificador para o $[n, k, d]$-código C sobre F_q, com matriz geradora

$$\mathbf{G} = [\ \mathbf{I}_k \quad \mathbf{P}\ ]$$

Então a aplicação linear $h : F_q^n \to F_q^{n-k}$ definida pela $(n - k) \times n$ matriz

$$\mathbf{H} = [\ -\mathbf{P}^t \quad \mathbf{I}_{n-k}\ ]$$

tem as seguintes propriedades:

1. $\ker h = \operatorname{Im} g$;

2. $\mathbf{c} \in C$ se, e somente se, $\mathbf{H}\mathbf{c}^t = \mathbf{0}$.

De fato. A aplicação linear $h \circ g : F_q^k \to F_q^{n-k}$ é identicamente nula, pois

$$\begin{aligned}
\mathbf{G}\mathbf{H}^t &= [\ \mathbf{I}_k \quad \mathbf{P}\ ] \begin{bmatrix} -\mathbf{P} \\ \mathbf{I}_{n-k} \end{bmatrix} \\
&= \mathbf{I}_k(-\mathbf{P}) + \mathbf{P}\mathbf{I}_{n-k} \\
&= -\mathbf{P} + \mathbf{P} = \mathbf{0}.
\end{aligned}$$

Logo, $\operatorname{Im} g \subseteq \ker h$. Desde que as últimas $n - k$ colunas de $\mathbf{H}$ formam a base canônica do espaço vetorial F_q^{n-k} temos que $\operatorname{Im} h$ gera F_q^{n-k} e contém q^{n-k} elementos. Assim, pelo

Primeiro Teorema de Isomorfismos,

$$|\ker h| = \frac{\left|F_q^n\right|}{|\mathrm{Im}\, h|} = \frac{q^n}{q^{n-k}} = q^k.$$

Portanto, $\ker h = \mathrm{Im}\, g$, pois $|\mathrm{Im}\, g| = q^k$.

A matriz $\mathbf{H}$ é chamada de *matriz de verificação de paridade* para o $[n, k, d]$-código C sobre F_q. Se $\mathbf{c} = (c_1, \ldots, c_k, c_{k+1}, \ldots, c_n) \in C$, então temos o sistema de equações $\mathbf{Hc}^t = \mathbf{0}$ ou, equivalentemente,

$$c_{k+j} = \sum_{i=1}^{k} c_i h_{ij}, 1 \leq j \leq n-k,$$

onde h_{ij} são as entradas da matriz $\mathbf{P}$.

Exemplo 2.4 *A matriz de verificação de paridade para o $[7, 4, 3]$-código linear C sobre F_2 é*

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

Se $\mathbf{c} = (c_1, c_2, c_3, c_4, c_5, c_6, c_7) \in C$, então $\mathbf{Hc}^t = \mathbf{0}$. Logo, temos o seguinte sistema de equações de verificação de paridade:

$$\begin{aligned} c_1 + c_3 + c_4 + c_5 &= 0 \\ c_1 + c_2 + c_4 + c_6 &= 0 \\ c_1 + c_2 + c_3 + c_7 &= 0 \end{aligned}$$

ou, equivalentemente,

$$\begin{aligned} c_5 &= c_1 + c_3 + c_4 \\ c_6 &= c_1 + c_2 + c_4 \\ c_7 &= c_1 + c_2 + c_3. \end{aligned}$$

Assim, as aplicações $\phi_i : F_2^4 \to F_2$, $i = 1, 2, 3$, definidas por

$$\begin{aligned} \phi_1((c_1, c_2, c_3, c_4)) &= c_1 + c_3 + c_4 \\ \phi_2((c_1, c_2, c_3, c_4)) &= c_1 + c_2 + c_4 \\ \phi_3((c_1, c_2, c_3, c_4)) &= c_1 + c_2 + c_3 \end{aligned}$$

são lineares. Portanto, toda palavra código de C pode ser escrita na forma

$$(\mathbf{u} \mid \phi_1(\mathbf{u}), \phi_2(\mathbf{u}), \phi_3(\mathbf{u})),$$

onde $\mathbf{u} = (c_1, c_2, c_3, c_4)$ *e* ϕ_1, ϕ_2, ϕ_3 *são aplicações lineares.*

Seja C um $[n, k, d]$-código linear sobre F_q. Então o *código dual* a C é definido por

$$C^{\perp} = \{\mathbf{x} \in F_q^n : \langle \mathbf{x}, \mathbf{c} \rangle = 0, \forall \mathbf{c} \in C\}.$$

Teorema 2.1 *Se C é um $[n, k, d]$-código linear sobre F_q, então $C^{\perp}$ é um $[n, n-k, d^*]$-código linear sobre F_q.*

Demonstração. É fácil verificar que $C^{\perp}$ é um subespaço vetorial de F_q^n. Assim, basta mostrar que $\dim C^{\perp} = n-k$. Seja $\mathbf{G}$ uma matriz geradora para C. Então podemos supor, sem perda de generalidade, que

$$\mathbf{G} = [\ \mathbf{I}_k \quad \mathbf{P}\ ].$$

Consideremos

$$\mathbf{H} = [\ -\mathbf{P}^t \quad \mathbf{I}_{n-k}\ ]$$

e seja $\langle \mathbf{H} \rangle$ o subespaço vetorial de F_q^n gerado pelas linhas de $\mathbf{H}$. Então $\dim\langle \mathbf{H} \rangle = n - k$.

Afirmação. $C^{\perp} = \langle \mathbf{H} \rangle$.

De fato. Como $\mathbf{G}\mathbf{H}^t = \mathbf{0}$ temos que as linhas de $\mathbf{H}$ são ortogonais as linhas de $\mathbf{G}$, isto é, $\langle \mathbf{H} \rangle \subseteq C^{\perp}$. Sejam $\mathbf{x} \in C^{\perp}$, onde $\mathbf{x} = (x_1, \ldots, x_n)$ e

$$\mathbf{y} = \mathbf{x} - \sum_{i=1}^{n-k} x_{k+i}\mathbf{h}_i,$$

onde $\mathbf{h}_i$ são as linhas de $\mathbf{H}$. Como $\langle \mathbf{H} \rangle \subseteq C^{\perp}$ e $\mathbf{x} \in C^{\perp}$ temos que $\mathbf{y} \in C^{\perp}$. Logo,

$$\mathbf{y} = (y_1, \ldots, y_k, 0, \ldots, 0) \in C^{\perp}$$

e $\mathbf{y}\mathbf{G} = \mathbf{0}$ implica que $y_j = 0$, $j = 1, \ldots, k$. Portanto,

$$\mathbf{x} = \sum_{i=1}^{n-k} x_{k+i}h_i$$

e $C^{\perp} \subseteq \langle \mathbf{H} \rangle$. ■

Um código C em F_q^n é um *código cíclico* se $\mathbf{c} = (c_1, \ldots, c_n) \in C$, então $\tilde{\mathbf{c}} = (c_n, c_1, \ldots, c_{n-1}) \in C$. É conveniente representar a palavra código $\mathbf{c} = (c_1, \ldots, c_n) \in C$ pelo polinômio

$$c(x) = c_1 + c_2 x + \cdots + c_n x^{n-1}$$

no anel

$$R_n(x) = \frac{F_q[x]}{\langle x^n - 1 \rangle}.$$

Então $xc(x)$ representa um deslocamento cíclico da palavra código $\mathbf{c}$ e, assim, um código cíclico linear é representado por um ideal em $R_n(x)$. Portanto, C pode ser gerado por um único polinômio $g(x)$, chamado *polinômio gerador* do código. Neste caso, se

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$$

é o polinômio gerador do $[n, k, d]$-código cíclico C sobre F_q, então os polinômios

$$g(x), xg(x), \ldots, x^{k-1} g(x)$$

são as palavras código de C. Assim, uma matriz geradora de C é dada por

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}.$$

Observação 2.5 *Para qualquer corpo F_q e qualquer inteiro positivo n existem os seguintes códigos lineares MDS.*

1. *O $[n, n.1]$-código universal $C = F_q^n$.*

2. *O $[n, n-1, 2]$-código de verificação de paridade simples (CVPS)*

$$C = \{\mathbf{c} \in F_q^n : \sum_{i=1}^{n} c_i = 0\}.$$

3. *O $[n, 1, n]$-código de repetição*

$$C = \{(\alpha, \alpha, \ldots, \alpha) \in F_q^n : \alpha \in F_q\}.$$

Teorema 2.2 (Códigos de Reed-Solomon) *Sejam F_q um corpo e $n \leq q + 1$. Então existe um $[n, k, d]$-código linear MDS sobre F_q, onde $1 \leq k \leq n$.*

Demonstração. Sejam $n = q + 1$ e $\varphi : F_q^k \longrightarrow F_q^n$ dada por

$$\varphi(f) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_q), f_{k-1}),$$

onde $\alpha_1, \alpha_2, \ldots, \alpha_q$ são todos os q elementos de F_q e

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1} \in F_q[x].$$

Assim, é fácil ver que φ é uma aplicação linear injetiva. Logo, $C = \varphi(F_q^k)$ é um código linear com comprimento n e dimensão k.

Se $f_{k-1} \neq 0$, então pelo Teorema Fundamental da Álgebra, $f(x)$ possui no máximo $k-1$ raízes. Assim, o peso de Hamming de qualquer palavra código não nula $\mathbf{c}$ é

$$w_H(\mathbf{c}) \geq n - (k-1).$$

Assim, pela Proposição 2.1,

$$w_H(\mathbf{c}) = n - k + 1.$$

Se $f_{k-1} = 0$, então pelo Teorema Fundamental da Álgebra, $f(x)$ possui no máximo $k-2$ raízes. Logo,

$$w_H(\mathbf{c}) \geq n - [(k-2) + 1] = n - k + 1.$$

Assim, pela Proposição 2.1,

$$w_H(\mathbf{c}) = n - k + 1.$$

Logo, C é um MDS. Se $n < q + 1$, então obtemos este código simplesmente omitindo componentes no código acima. ■

Proposição 2.3 *Não existe* $[4, 2, 3]$*-código* (*linear ou não*) *sobre* F_2.

Demonstração. Suponhamos, por absurdo, que exista um $[4, 2, 3]$-código C sobre F_2. Como

$$d_H(C) = d_H(C + \mathbf{a})$$

para todo $\mathbf{a} \in F_2^4$ podemos supor, sem perda de generalidade, que $(0, 0, 0, 0) \in C$. Sendo C um código MDS temos, Proposição 2.2, que cada par de posições é um conjunto de informação. Assim, existe uma palavra código com $(0, 1)$ nas duas primeiras posições, a qual deve ser $(0, 1, 1, 1)$, pois caso contrário, $d_H(C) < 3$. Similarmente, C contém $(1, 0, 1, 1), (1, 1, 0, 1)$ e $(1, 1, 1, 0)$. Mas a distância de Hamming entre qualquer duas palavras é igual a 2, o que é uma contradição. ■

Observação 2.6 *A Proposição mostra que não existe um* $[4,2,3]$*-código sobre* F_2*, no entanto, o Teorema* 2.2*, mostra que existe um* $[4,2,3]$*-código linear sobre* F_3 *ou* F_4*. Assim, podemos notar que sobre corpos grandes temos bons parâmetros de códigos.*

2.2 Códigos sobre Grupos não Abelianos

Nesta seção o alfabeto F será um grupo G com a operação de multiplicação e elemento identidade e.

Um código de bloco C de comprimento n sobre G é *código de grupo* se C é um subgrupo do produto direto G^n.Se C é um código de grupo sobre G, então a mínima distância de Hamming é o mínimo peso de Hamming. Um código linear C sobre F_q é um código de grupo sobre o grupo aditivo de F_q.

Proposição 2.4 *Seja* G *um grupo finito. Então existe um* $[n, n-1, 2]$*-código sobre* G*, para todo* $n \geq 2$*.*

Demonstração. Seja

$$C = \{\mathbf{c} \in G^n : \prod_{i=1}^{n} c_i = e\}.$$

Então, é claro que C é um subconjunto não vazio de G^n. Se $\mathbf{c} = (c_1, \ldots, c_n) \in C$, então podemos escolher $c_1, c_2, \ldots, c_{n-1}$, arbitrariamente de G, enquanto, c_n é completamente determinado por $c_1, c_2, \ldots, c_{n-1}$, isto é,

$$c_n = \prod_{i=1}^{n-1} c_{n-i}^{-1}.$$

Assim, $|C| = |G|^{n-1}$ e mais nenhuma palavra código pode diferenciar de outra, numa única componente. Pois, se

$$\mathbf{c} = (c_1, \ldots, c_n) \text{ e } \mathbf{c}' = (c_1', c_2', \ldots, c_n'),$$

diferenciassem em apenas uma componente, digamos c_n, então

$$c_n = \sum_{i=1}^{n-1} c_{n-i}^{-1} = \sum_{i=1}^{n-1} c_{n-i}'^{-1} = c_n',$$

o que é uma contradição. Portanto, $d_H(C) \geq 2$. Por outro lado, pela Proposição 2.1, temos que

$$d \leq n - k + 1 = n - (n-1) + 1 = 2.$$

Portanto, $d_H(C) = 2$. ■

Proposição 2.5 *Seja G um grupo não abeliano. Então não existe $[n, n-1, 2]$-código de grupo sobre G para $n \geq 3$.*

Demonstração. Dividiremos a prova em dois casos:

1º Caso - Suponhamos que $n = 3$ e que exista um $[3, 2, 2]$-código de grupo C sobre G. Então, pela Proposição 2.2, cada subconjunto $\mathbb{J}$ de $\mathbb{I}$, com $|\mathbb{J}| = 2$, é um conjunto de informação de C. Assim, todo par de elementos de G aparece em $\mathbb{J}$ para algum $\mathbf{c} \in C$. Sejam $a, b \in G$ tais que $ab \neq ba$ e $\mathbf{c} = (e, a, a^{-1})$ e $\mathbf{d} = (b^{-1}, b, e)$ duas palavras código. Então

$$\mathbf{cd} = \left(b^{-1}, ab, a^{-1}\right) \text{ e } \mathbf{dc} = \left(b^{-1}, ba, a^{-1}\right)$$

são duas palavras código com distância de Hamming igual a 1, o que é uma contradição.

2º Caso - Suponhamos que $n > 3$ e que exista um $[n, n-1, 2]$-código de grupo C sobre G. Dado um subconjunto $\mathbb{J}$ de $\mathbb{I}$, com $|\mathbb{J}| = 3$. Então

$$C' = \{\mathbf{c} \in C : c_j = e \text{ se } j \notin \mathbb{J}\}$$

é um subgrupo de C com $|C'| = |G|^2$. De fato, se $\mathbf{c}, \mathbf{d} \in C'$, digamos

$$\mathbf{c} = (a, b, c, e, \ldots, e) \text{ e } \mathbf{d} = (a', b', c', e, \ldots, e)$$

com $abc = e$ e $a'b'c' = e$, então $\mathbf{cd} \in C'$, pois C é grupo. Portanto, a projeção $P_{\mathbb{J}}(C')$ de C' sobre $\mathbb{J}$ deve ser um $[3, 2, 2]$-código de grupo sobre G, o que é, pelo primeiro caso, uma contradição. ■

Proposição 2.6 *Se C é código de grupo sobre um grupo não abeliano G com dois conjuntos de informações distintos $\mathbb{J}$ e $\mathbb{J}'$ tais que $\mathbb{J} \cap \mathbb{J}' \neq \emptyset$, então para cada $g \in G'$ e $j \in \mathbb{J} \cap \mathbb{J}'$ existe $\mathbf{c} \in C$ com $c_j = g$ e $c_i = e$ se $i \in (\mathbb{J} \cup \mathbb{J}') - \{j\}$..*

Demonstração. Sejam $a, b \in G$ tais que $ab \neq ba$. Então considerando duas palavras código $\mathbf{c}$ e $\mathbf{d}$ tais que $c_j = a$ e $c_i = e$, $d_j = b$ e $d_l = e$ se $i, l \in \mathbb{J} - \{j\}$. Então, $\mathbf{cd}$ e $\mathbf{dc}$ são duas palavras código que coincide em $\mathbb{J} \cup \mathbb{J}'$ exceto na j-ésima componente, onde $\mathbf{cd}$ e $\mathbf{dc}$ tem componentes ab e ba, respectivamente. Como $\mathbf{cdc}^{-1}\mathbf{d}^{-1} \in C$ e suas componentes são todas iguais a e, exceto a j-ésima que é igual a $aba^{-1}b^{-1}$ temos, para cada $g \in G'$ e $j \in \mathbb{J} \cap \mathbb{J}'$, que existe $\mathbf{c}' \in C$, com $c'_j = g$ e $c'_i = e$ se $i \in (\mathbb{J} \cup \mathbb{J}') - \{j\}$. ■

Proposição 2.7 *Seja C um $[n, k, d]$-código de grupo sobre um grupo não abeliano G. Então*:

1. Se $k > \frac{n}{2}$ e C tem dois conjuntos de informação cuja união é $\mathbb{I}$, então $d = 1$.
2. Se $k \leq \frac{n}{2}$ e C tem dois conjuntos de informação que se interceptam em uma única posição, então $d \leq n - 2k + 2$.

Demonstração. 1. Suponhamos que $k > \frac{n}{2}$ e C tenha dois conjuntos de informações $\mathbb{J}$ e $\mathbb{J}'$ tais que $\mathbb{J} \cup \mathbb{J}' = \mathbb{I}$. Então $\mathbb{J} \cap \mathbb{J}' \neq \emptyset$, pois $k > \frac{n}{2}$. Assim, pela Proposição 2.6, para cada $g \in G'$ e $j \in \mathbb{J} \cap \mathbb{J}'$ existe $\mathbf{c} \in C$, com $c_j = g$ e $c_i = e$ se $i \in (\mathbb{J} \cup \mathbb{J}') - \{j\}$. Portanto, $d = 1$.

2. Suponhamos que $k \leq \frac{n}{2}$ e C tenha dois conjuntos de informações $\mathbb{J}$ e $\mathbb{J}'$ tais que $|\mathbb{J} \cap \mathbb{J}'| = 1$. Então

$$m = |\mathbb{J} \cup \mathbb{J}'| = 2k - 1 < n.$$

Assim, pela Proposição 2.6, existe $\mathbf{c} \in C$ com $w_H(\mathbf{c}) = 1$ dentro de $\mathbb{J} \cup \mathbb{J}'$. Logo,

$$\begin{aligned} d &\leq 1 + (n - m) \\ &= 1 + n - (2k - 1) \\ &= n - 2k - 2. \end{aligned}$$

Portanto, $d \leq n - 2k + 2$. ■

Observação 2.7 *A Proposição mostra que códigos de grupos sobre grupos não abelianos, iniciando do $[n, 1, n]$-código, todo símbolo de informação adicional custa duas unidades de distância, enquanto para códigos MDS, todo símbolo de informação adicional custa apenas uma unidade de distância.*

Corolário 2.1 *Seja G um grupo não abeliano. Então não existe $[n, k, d]$-código de grupo MDS sobre G, com $1 < k < n$.*

Demonstração. Suponhamos, por absurdo, que exista um $[n, k, d]$-código de grupo MDS sobre G com $1 < k < n$. Assim, temos dois casos há serem considerados.

1º Caso - Se $k > \frac{n}{2}$, então pela Proposição 2.7, $d = 1$. Logo, $n - k + 1 = 1$ e $n = k$, que é uma contradição.

2º Caso. Se $k \leq \frac{n}{2}$, então pela Proposição 2.7,

$$\begin{aligned} n - k + 1 &= d \leq n - 2k + 2 \\ &\Rightarrow k \leq 1, \end{aligned}$$

o que é uma contradição. ■

Observação 2.8 *Seja G um grupo não abeliano com $|G| = p^m$. Então, pelo Teorema 2.2, existe um $[n, k, d]$-código MDS sobre G para cada $n \leq p^m + 1$ e $1 < k < n$. Mas pelo Corolário um código com estes parâmetros não pode ser código de grupo. Assim, concluímos que para códigos sobre grupos não abelianos, a propriedade de grupos é, em geral, incompatível com o alcance da melhor mínima distância de Hamming.*

Um código de grupo C de comprimento n sobre um grupo G é um *código normal* se C é um subgrupo normal de G^n.

Dado um código de grupo C e $i \in \mathbb{I}$, o *grupo de saída* G_i, no instante i, será definido como o conjunto de todo $g \in G$ que já ocorre como componente $c_i = P_{\{i\}}(c)$ das palavras código $\mathbf{c} \in C$, isto é,

$$G_i = P_{\{i\}}(C).$$

Usualmente $G_i = G$ para todo $i \in \mathbb{I}$, mas não está excluída da definição a possibilidade de G_i ser um subconjunto próprio de G. Portanto, G_i pode ser abeliano sem que G o seja. É claro que, se i pertence a um conjunto de informação $\mathbb{J}$, então

$$G_i = P_{\{i\}}(C) = G^{\{i\}} = G.$$

O código C é assim um subgrupo de $W = \prod_{i=1}^{n} G_i$, o qual será chamado *espaço de saída* de C. W é abeliano se, e somente se, G_i é abeliano, para cada $i = 1, \ldots, n$. Se G_i' é o comutador de G_i, então $W' = \prod_{i=1}^{n} G_i'$ é o comutador de W.

Proposição 2.8 *Seja C um código de grupo sobre um grupo G. Então C é normal em W se, somente se, $W' \subseteq C$. Além disto, se C é normal em W, então $\dfrac{W}{C}$ abeliano*

Demonstração. Suponhamos que C é normal em W. Dados $i \in \mathbb{I}$ e $a, b \in G_i$. Sejam $\mathbf{c} \in C$, com $c_i = a$, $c_j = e$ se $i \neq j$ e $\mathbf{w} \in W$, com $w_i = b$, $w_j = e$ se $i \neq j$. Logo, por hipótese,

$$\mathbf{m} = \mathbf{wcw}^{-1} \in C.$$

Assim,

$$\mathbf{d} = \mathbf{cm}^{-1} = \mathbf{c}\left(\mathbf{wcw}^{-1}\right)^{-1} = \mathbf{cwc}^{-1}\mathbf{w}^{-1} \in C,$$

com $d_i = aba^{-1}b^{-1}$ e $d_j = e$ se $i \neq j$. Portanto, $W' \subseteq C$, pois i é arbitrário.

A recíproca, segue da Proposição 1.1. ■

Teorema 2.3 *Sejam C um código normal sobre um grupo G e W não abeliano. Então a mínima distância de Hamming de C é igual a* 1.

Demonstração. Se C é normal em G^n, então C é normal em W, pois W é um subgrupo de G^n. Assim, pela Proposição 2.8, $W' \subseteq C$. Como W é não abeliano temos que existem $\mathbf{a}, \mathbf{b} \in W$ tais que $\mathbf{ab} \neq \mathbf{ba}$, ou seja,

$$\mathbf{aba}^{-1}\mathbf{b}^{-1} \neq \mathbf{e}.$$

Logo $W' \neq \{\mathbf{e}\}$ e pelo menos um G_i' contém um elemento $g \neq e$. Assim, a palavra código $\mathbf{c}$, com $c_i = g$ e $c_j = e$ se $i \neq j$ é um elemento de W' e de C. Portanto, $w_H(\mathbf{c}) = 1$. ■

Corolário 2.2 *Seja G um grupo não abeliano. Então um $[n, 1, n]$-código de repetição sobre G é um código de grupo mas não é um código normal para $n \geq 2$.*

Demonstração. Suponhamos, por absurdo, que o $[n, 1, n]$-código de repetição seja normal. Então, pelo Teorema, temos que $d = n = 1$, o que é uma contradição. ■

Teorema 2.4 *Sejam C um $[n, k, d]$-código de grupo sobre um grupo abeliano G com expoente q, p um fator primo de q e $pm = q$. Se C possui um conjunto de informação $\mathbb{J}$, então existe $[n, k, d]$-código de grupo D sobre $K = mG$.*

Demonstração. Pela Proposição 1.14, o grupo $K = mG$ é um grupo abeliano elementar, com expoente p. O código $D = mC$ é um subcódigo de C e um código de grupo sobre K. Como C possui um subconjunto de informação $\mathbb{J}$ temos que $|\mathbb{J}| = k$ e existem $|K|^k$ palavras código em D correspondendo a toda k-uplas de elementos de K em $\mathbb{J}$. Ora, sendo D um subcódigo de C temos que a mínima distância de Hamming de D é pelo menos d. Portanto, D é um $[n, k, d]$-código de grupo sobre K. ■

Corolário 2.3 *Seja $G = \mathbb{Z}_{2m}$, para todo $m \geq 2$. Então não existe $[4, 2, 3]$-código de grupo sobre G.*

Demonstração. Suponhamos, por absurdo, que exista um $[4, 2, 3]$-código de grupo sobre G. Então, pela Proposição 2.2, C possui um conjunto de informação $\mathbb{J}$, com $|\mathbb{J}| = 2$. Pelo Teorema 2.4, $D = mC$ é um $[4, 2, 3]$-código de grupo sobre $K = mG \backsimeq \mathbb{Z}_2$, o que é, pela Proposição 2.3, uma contradição. ■

Observação 2.9 *O Corolário mostra que não existe $[4, 2, 3]$-código de grupo sobre $\mathbb{Z}_4$, no entanto, pelo Teorema 2.2 existe um $[4, 2, 3]$-código linear sobre F_4. Assim, o Corolário mostra simplesmente que um tal código não é de grupo.*

Capítulo 3

Códigos de Bloco Lineares Sobre Grupos

Neste capítulo consideraremos uma construção de códigos de bloco lineares sobre grupos que imita a construção de códigos algébricos sobre corpos finitos. Como vimos, códigos baseados em grupos não abeliano exibem uma pobre distância de Hamming, focaremos pois nossa atenção em grupos abelianos.

3.1 Matriz de Verificação de Paridade

Sejam G um grupo e

$$C = \{\mathbf{c} \in G^n : c_1^{a_{i1}} \cdots c_n^{a_{in}} = e, 1 \leq i \leq m \text{ e } a_{ij} \in \mathbb{Z}\}.$$

Então, é claro que C é um código sobre G, pois $C \neq \varnothing$. Note que, este código é descrito por uma "matriz de verificação de paridade" $\mathbf{H} = (a_{ij})$, cujas entradas são os expoentes $a_{ij} \in \mathbb{Z}$, $1 \leq i \leq m$ e $1 \leq j \leq n$.

Exemplo 3.1 *$O\,[3,2]$-código de verificação de paridade simples C sobre G é definido pela relação $c_1c_2c_3 = e$, isto é, pela matriz*

$$\mathbf{H} = [111].$$

C é linear se, e somente se, G é abeliano. De fato, dados $a, b, c, d \in G$ temos que $(a, b, b^{-1}a^{-1}), (c, d, d^{-1}c^{-1}) \in C$. Portanto,

$$\left(a, b, b^{-1}a^{-1}\right)\left(c, d, d^{-1}c^{-1}\right) = \left(ac, bd, b^{-1}a^{-1}d^{-1}c^{-1}\right) \in C$$

se, e somente se,

$$b^{-1}a^{-1}d^{-1}c^{-1} = (bd)^{-1}(ac)^{-1}.$$

Fazendo, $a = c$ *e* $b = d$*, temos que*

$$b^{-1}a^{-1}b^{-1}a^{-1} = (bb)^{-1}(aa)^{-1}$$

se, e somente se, $ab = ba$*.*

Exemplo 3.2 *O* $[3,1]$*-código de repetição* C *sobre* G *é definido pelas relações* $c_1c_2^{-1}c_3^0 = e$ *e* $c_1c_2^0c_3^{-1} = e$*, isto é, pela matriz*

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

Assim, temos que $C = \{(a,a,a) : a \in G\}$*.*

Exemplo 3.3 *A matriz*

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

define um $[7,4]$*-código. Este código é chamado* código de Hamming*, o qual é linear se* G *é abeliano. Pode ser mostrado, por cálculos direto, que a mínima distância de Hamming é igual a* 3*.*

Exemplo 3.4 *Pela Proposição* 1.7 *o conjunto*

$$C = \{(g \mid \varphi_2(g), \varphi_3(g), \ldots, \varphi_n(g)) : g \in G\}$$

é um $[n,1]$*-código linear do tipo repetição sobre* G *se, e somente se,* $\varphi_i \in \mathrm{End}(G)$*. Se* $\varphi_i \in \mathrm{Aut}(G)$*, então o código* C *é chamado* código linear do tipo repetição automorfo*.*

Proposição 3.1 *Um* $[n,1]$*-código linear do tipo repetição* C *tem mínima distância de Hamming igual a* n *se, e somente se,* C *é automorfo.*

Demonstração. Suponhamos que exista pelo menos um $\varphi_i \in \mathrm{End}(G)$ tal que $\varphi_i \notin \mathrm{Aut}(G)$. Então

$$\ker \varphi_i = \{g \in G : \varphi_i(g) = e\} \neq \{e\}.$$

Assim, existe $g \in G$ com $\varphi_i(g) = e$ e $g \neq e$. A correspondente palavra código possui pelo mensos um elemento identidade (i-ésima posição), de modo que sua distância de Hamming à palavra código identidade é no máximo $n-1$. Portanto, a mínima distância de Hamming não pode exceder a $n-1$. ■

Exemplo 3.5 *Seja $G = S_3$ o grupo simétrico. Então a matriz*

$$\mathbf{H} = \begin{bmatrix} 2 & 0 & 3 & 0 & 0 \\ 2 & 3 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{bmatrix}$$

define um $[5,2]$-código C sobre G sem conjunto de informação. De fato, se

$$G = \{e, r, r^2, s, sr, sr^2\},$$

com $r^3 = s^2 = e$ e $rsrs = e$, então as palavras código têm a forma

$$(abc \mid ab),$$

onde

$$b, c \in \{e, r, r^2\} \ \text{ e } \ a \in \{e, s, sr, sr^2\}.$$

Fazendo a tabela dos elementos de G temos que $|C| = 36$, e portanto $k = 2$.

Na teoria da codificação algébrica a "clássica" construção de códigos lineares concatena uma k-upla de símbolos de informação com $(n-k)$ símbolos de verificação de paridade escolhidos de modo a satisfazer certas equações de verificação de paridade. A seguir mostraremos como esta construção pode ser imitada para gerar códigos lineares sobre grupos, no entanto, esta construção não é bastante geral: é suficiente observar que para grupos não abelianos a ordem dos elementos é relevante. Assim, não podemos usar um procedimento baseado na matriz de verificação de paridade para definir códigos lineares sobre grupos gerais.

Um $[n,k]$-código C sobre um grupo G é sistemático se suas $|G|^k$ palavras códigos são n-uplas da forma:

$$(c_1, \ldots, c_k \mid d_{k+1}, \ldots, d_n)$$

com $d_{k+i} = \varphi_i(c_1, \ldots, c_k)$, onde φ_i são $(n-k)$ aplicações de G^k em G, $i = 1, \ldots, n-k$.

Proposição 3.2 *O $[n,k]$-código sistemático C sobre G é linear se, e somente se, as aplicações φ_i de G^k em G são homomorfismos de grupos.*

Demonstração. Sejam

$$\begin{aligned}(c_1,\ldots,c_k \mid d_{k+1},\ldots,d_n) &\in C\\ (x_1,\ldots,x_k \mid y_{k+1,},\ldots,y_n) &\in C.\end{aligned}$$

Então seu produto é uma palavra código se, e somente se,

$$\varphi_i(c_1,\ldots,c_k)\,\varphi_i(x_1,\ldots,x_k)=\varphi_i(c_1x_1,\ldots,c_kx_k)$$

se, e somente se, φ_i são homomorfismos de grupos. ■

Um $[n,k]$-codigo sistemático linear C sobre G é a imagem de um $\psi\in \mathrm{End}(G^n)$ tal que

$$\psi(c\mid d)=(c\mid \varphi(c)),$$

onde φ é um homomorfismo de G^k em G^{n-k}.

Observação 3.1 *Pela Proposição* 1.8 *um $[n,k]$-código sistemático linear C sobre um grupo G é normal se, e somente se, φ é um homomorfismo de G^k em $Z\left(G^{n-k}\right)$.* ■

Proposição 3.3 *Todos os $[n,k]$-códigos sistemáticos lineares sobre G são isomorfos a G^k.*

Demonstração. Sejam C um $[n,k]$-código sistemático linear sobre o grupo G e π a projeção de G^n sobre $G^k\times\{e\}^{n-k}$, ou seja,

$$\pi(g_1,\ldots,g_k\mid g_{k+1},\ldots,g_n)=(g_1,\ldots,g_k\mid e,\ldots,e).$$

É claro que π é um homomorfismo de grupos e mais π restrito à

$$C=\{(c,\varphi(c)):\varphi \text{ é um homomorfismo de } G^k \text{ em } G^{n-k}\}$$

é um isomorfismo de C em $G^k\times\{e\}$, ou seja, $C\backsimeq G^k$. ■

A Proposição mostra que a estrutura algébrica abstrata de um código linear não é tão relevante, no sentido de que não carrega muita informação sobre as propriedades do código em si, pois em grupos isomorfos gerais pode ser pensado como sendo o mesmo

grupo, o mesmo não é verdade para códigos lineares, os quais por exemplo, podem ter diferentes distâncias de Hamming.

Um $[n,k]$-código de bloco sistemático linear é *decomponível* (*fatorizável*) se ele é um grupo decomponível (fatoriazável).

Exemplo 3.6 *O* $[3,2,2]$*-código sobre* $\mathbb{Z}_2$ *é decomponível em* $C = C_1C_2$*, onde*

$$C_1 = \{(x, e \mid x) : x \in \mathbb{Z}_2\}$$

e

$$C_2 = \{(e, y \mid y) : y \in \mathbb{Z}_2\}.$$

Além disto, $C \neq C_1 \times C_2$ *mas* C_1*,* C_2 *são isomorfos a* $\mathbb{Z}_2$ *e* $C \backsimeq \mathbb{Z}_2 \times \mathbb{Z}_2$*.*

Proposição 3.4 *A mínima distância de Hamming de um código fatoriazável* $C = C_1C_2$ *não pode exceder a menor entre as mínimas distâncias de Hamming de* C_1 *e* C_2*.* ■

Proposição 3.5 *Um* $[n,k]$*-código de bloco sistemático linear sobre um grupo fatorizável* G *é fatorizável.*

Demonstração. Por definição $G = HK$ com $HK = KH$. Então $G^l = H^lK^l$ para todo $l \in \mathbb{Z}$. Tomando $\mathbf{c} \in G^k$ temos que $\mathbf{c} = \mathbf{c}_1\mathbf{c}_2$ com $\mathbf{c}_1 \in H^k$ e $\mathbf{c}_2 \in K^k$. Como φ é um homomorfismo temos que

$$\begin{aligned}(\mathbf{c} \mid \varphi(\mathbf{c})) &= (\mathbf{c}_1\mathbf{c}_2 \mid \varphi(\mathbf{c}_1\mathbf{c}_2)) \\ &= (\mathbf{c}_1 \mid \varphi(\mathbf{c}_1))(\mathbf{c}_2 \mid \varphi(\mathbf{c}_2)).\end{aligned}$$

Note que, embora

$$\varphi(\mathbf{c}_1), \varphi(\mathbf{c}_2) \in H^{n-k}K^{n-k}$$

pode ocorrer que $\varphi(\mathbf{c}_1) \notin H^{n-k}$ ou $\varphi(\mathbf{c}_2) \notin K^{n-k}$. ■

3.2 Códigos Assintoticamente Maus.

Nesta seção mostraremos, do ponto de vista da distância de Hamming, que códigos lineares sobre grupos não abelianos são assintoticamente maus.

Seja G um grupo não abeliano. Com as notações da Proposição 1.10, um $[n,k]$-código linear é caracterizado por $(n-k)$ homomorfismos de grupos

$$\phi_i : G^k \longrightarrow G$$

cada um deles é caracterizado por k endomorfismo

$$\varphi_j : G \longrightarrow G$$

tais que, para $j \neq l$,

$$\varphi_l(G)\,\varphi_j(G) = \varphi_j(G)\,\varphi_l(G),$$

elemento a elemento. O grupo

$$W = \varphi_1(G)\,\varphi_2(G)\cdots\varphi_k(G)$$

é um subgrupo de G. Considerando agora um dos φ_j, temos o seguinte resultado:

Proposição 3.6 *Sejam G um grupo não abeliano e ϕ um homomorfismo sobrejetor de G^k em G. Se*

$$\phi(g_1,\ldots,g_k) = \varphi_1(g_1)\cdots\varphi_k(g_k),$$

onde $\varphi_i \in \mathrm{End}(G)$, então:

1. *Se G não é fatorizável em subgrupos próprios não centrais, então $\varphi_i \in \mathrm{Aut}(G)$ para algum i e $\varphi_j(G) \subseteq Z(G)$, para todo j com $i \neq j$.*

2. *Se G é indecomponível, então $|G| \geq 32$.*

Demonstração.1. Como ϕ é sobrejetor temos que

$$G = \prod_{i=1}^{k} \varphi_i(G) = \varphi_j(G)\,W_j,$$

onde

$$W_j = \prod_{i=1}^{k} \varphi_i(G),$$

com $i \neq j$. Assim, por hipótese,

$$\varphi_j(G) = G \text{ e } W_j \subseteq Z(G)$$

ou

$$\varphi_j(G) \subseteq Z(G) \text{ e } W_j = G.$$

Se $\varphi_j(G) = G$ e $W_j \subseteq Z(G)$ acabou. Mas se $\varphi_j(G) \subseteq Z(G)$ e $W_j = G$, repete-se o mesmo argumento em $W_j = G$ até obtermos o automorfismo φ_i.

2. Se G é indecomponível, então $H_j = W_j \cap \varphi_i(G) \subseteq Z(G)$ e $|H_j| \geq 2$. Pelo item 3 da Proposição 1.11, W_j e $\varphi_i(G)$ são não abelianos e finalmente pelo item 6 da Proposição 1.11, $|G| \geq 32$. ■

Vamos supor primeiro que G é indecomponível e que pelo menos um dos $\varphi_i \in \mathrm{Aut}(G)$, (isto, como temos visto, é certamente o caso se $|G| < 32$). Então, mostraremos que todo $[n,k]$-código sistemático linear sobre G é decomponível em k código do tipo repetição.

De fato, considere o símbolo de verificação de paridade

$$d_{k+i} = \phi_i(c_1, \ldots, c_k),$$

onde ϕ_i é um homomorfismo de grupos de G^k em G. Assim, se G é indecomponível, então

$$d_{k+i} = \phi_i(e, \ldots, c_{j_i}, \ldots, e)\, Z_i,$$

onde $\phi_i \in \mathrm{End}(G)$, cuja imagem $\phi_i(G)$ pode ser um subgrupo não comutativo e

$$Z_i = \prod_{h=1}^{k} \phi_i(e, \ldots, c_h, \ldots, e) \in Z(G), h \neq j_i.$$

Note que, o homomorfismo ϕ_i pode ser associado naturalmente com um automorfismo, possivelmente o automorfismo identidade, como segue:

$$d_{k+i} = \varphi_i(e, \ldots, c_{j_i}, \ldots, e)\, Z_i = \theta_i(c_{j_i})\, Z_i.$$

Já sabemos que a palavra código é

$$\left(c_1, \ldots, c_k \mid \theta_1(c_{j_1})\, Z_1, \ldots, \theta_{n-k}\left(c_{j_{n-k}}\right) Z_{n-k}\right)$$

Agora, sejam $\mathbf{c}$ e $\mathbf{d}$ duas palavras código. Então

$$\mathbf{c} = \left(c_1, \ldots, c_k \mid \theta_1(c_{j_1})\, Z_1, \ldots, \theta_{n-k}\left(c_{j_{n-k}}\right) Z_{n-k}\right)$$

e

$$\mathbf{d} = \left(d_1, \ldots, d_k \mid \theta_1(d_{j_1})\, U_1, \ldots, \theta_{n-k}\left(d_{j_{n-k}}\right) U_{n-k}\right)$$

com $Z_i, U_i \in Z(G)$. Logo,

$$\begin{aligned}(\mathbf{cd})(\mathbf{dc})^{-1} &= ((c_1d_1)(d_1c_1)^{-1} \cdots (c_kd_k)(d_kc_k)^{-1} \mid \\ &\quad \theta_1((c_{j_1}d_{j_1})(d_{j_1}c_{j_1})^{-1}) \cdots \theta_{n-k}(\left(c_{j_{n-k}}d_{j_{n-k}}\right)\left(d_{j_{n-k}}c_{j_{n-k}}\right)^{-1}),\end{aligned}$$

pois

$$(Z_i U_i)\,(U_i Z_i)^{-1} = e,$$

de modo que obtemos um subcódigo decomponível num número conveniente de códigos do tipo repetição de dimensão 1.

Finalmente, se G é decomponível, digamos $G = HK$, com H indecomponível e não abeliano, então restringimos o subcódigo a H. Assim, o argumento acima aplica-se e o código linear é necessariamente decomponível em um produto de k código do tipo repetição.

Proposição 3.7 *Seja G um grupo não abeliano. Então nenhum $[4,2]$-código de bloco sistemático linear C sobre G tem mínima distância de Hamming excedendo a 2.*

Demonstração. Qualquer palavra de C tem a forma:

$$(c_1 c_2 \mid \varphi_1(c_1)\,\phi_1\,(c_2)\,\varphi_2(c_1)\phi_2\,(c_2)),$$

onde

$$\varphi_1, \varphi_2, \phi_1, \phi_2 \in \mathrm{End}\,(G) \;\text{ e }\; \varphi_i\,(G)\,\phi_i\,(G) = \phi_i\,(G)\,\varphi_i\,(G)\,,\; i = 1, 2.$$

Se um dos quatros endomorfismos, digamos $\varphi_1 \notin \mathrm{Aut}\,(G)$, então o subcódigo de C com palavras código

$$(c_1 e \mid \varphi_1\,(c_1)\,\varphi_2\,(c_1))$$

não é automorfo. Logo, pela Proposição 3.1, sua mínima distância de Hamming não pode exceder a 2. Portanto, pela Proposição 3.4, a mínima distância de Hamming de C não pode exceder a 2. ■

Para limitar a mínima distância de Hamming d, observamos que, no melhor evento, todos estes códigos do tipo repetição de dimensão 1 tem um e o mesmo comprimento $\dfrac{n}{k}$, o qual é a maior mínima distância de cada subcódigo. Portanto, obtemos uma cota superior para a mínima distância de Hamming:

$$d \leq \left\lfloor \frac{n}{k} \right\rfloor$$

Fazendo $r = \dfrac{n}{k}$ e $\delta = \dfrac{d}{k}$, obtemos a cota assintótica

$$r\delta \leq \frac{1}{n}$$

a qual mostra que $r\delta$ aproxima-se de zero quando n cresce. Note que, esta cota superior melhora o resultado da Proposição 2.7.

3.3 Códigos sobre Grupos Abelianos.

Nesta seção examinaremos com mais detalhes a construção de códigos lineares sobre grupos abelianos.

Um $[n,k]$-código sistemático linear sobre o grupo abeliano G é um subgrupo de G^n com ordem $|G|^k$, descrito por $(n-k)$ homomorfismos de grupos de G^k sobre G. Suas palavras código são:

$$(c_1, c_2, \ldots, c_k \mid d_{k+1}, \ldots, d_n),$$

onde

$$\begin{aligned} d_{k+l} &= \phi_l(c_1, c_2, \ldots, c_k) \\ &= \prod_{j=1}^{k} \phi_l(e, \ldots, c_j, \ldots, e) \end{aligned} \tag{3.1}$$

e todo ϕ_l é caracterizado por k matrizes quadradas de ordem m,

$$A(l,h), h = 1, \ldots, k$$

com elementos em $\mathcal{Z}_{d_m}$.

Usando uma base normal para G temos que

$$c_h = \prod_{i=1}^{m} g_i^{c_{ih}} \text{ e } d_l = \prod_{i=1}^{m} g_i^{d_{il}}$$

e pela equação 3.1, para cada $l = 1, \ldots, (n-k)$,

$$\begin{aligned} d_l &= \prod_{h=1}^{k} \prod_{i=1}^{m} g_i^{\sum_{j=1}^{m} \alpha_{ij}(l,h) c_{ih}} \\ &= \prod_{i=1}^{m} g_i^{\sum_{h=1}^{k} \sum_{j=1}^{m} \alpha_{ij}(l,h) c_{ih}}. \end{aligned}$$

Assim, comparando expoente obtemos um conjunto de equações de verificação de paridade

$$\sum_{h=1}^{k} \sum_{j=1}^{m} \alpha_{ij}(l,h) c_{ih} - d_{il} = 0 \tag{3.2}$$

onde $i = 1, \ldots, m$ e $l = 1, \ldots, (n-k)$.

Definimos agora m vetores d_j cujas $(n-k)$ componentes são os expoentes dos símbolos de paridade e m vetores c_i cujas k componentes são os expoentes dos símbolos de informação. O conjunto de equações em (3.2) pode ser ser escrito na forma matricial

$$\begin{bmatrix} A_{11} & \cdots & A_{1m} & -I_{n-k} & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \cdots \\ A_{m1} & \cdots & A_{mm} & 0 & \cdots & -I_{n-k} \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_m \\ \cdots \\ d_1 \\ \vdots \\ d_m \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}, \tag{3.3}$$

onde A_{ij} são $(n-k) \times k$ matizes e I_{n-k} são $(n-k) \times (n-k)$ matrizes identidades. A

$$m\,(n-k) \times mn$$

matriz dos coeficientes que aparece na forma escalonada em (3.3) descreve um código e pode ser chamada sua matriz de verificação de paridade $\mathbf{H}$, a qual nos permite limitar, e possilvelmente avaliar, a mínima distância de Hamming do código. Vamos numerar as primeiras mk colunas de $\mathbf{H}$ (as quais corresponde a localização de informação), como

$$h_1 + mh_2, h_1 = 1, \ldots, k, h_2 = 0, \ldots, k-1.$$

As colunas com o mesmo índice h_1 serão chamadas de "colunas companheiras de informação". Estas colunas ocupam a mesma posição dentro das submatrizes A_{ij}. Similarmente, podemos definir "colunas companheiras de verificação de paridade" numerando da mesma maneira o restante $(n-k)$ colunas (correspondendo a localização de verificação de paridade).

Teorema 3.1 *Seja C um $[n,k]$-código sistemático linear sobre $\mathbb{Z}_t$. Então, a matriz de verificação de paridade $\mathbf{H}$ é uma matriz escalonada $(n-k) \times n$ sobre $\mathcal{Z}_t$. A mínima distância de Hamming d do código é igual ao número mínimo de colunas linearmente dependentes de $\mathbf{H}$.*

Demonstração. Seja g um gerador de $\mathbb{Z}_t$. Então o número mínimo de colunas linearmente dependentes em $\mathbf{H}$ dar o número mínimo de expoentes não nulos para g numa dada palavra código. Este é o número de posições em que uma palavra código difere da palavra código identidade de C. ■

Exemplo 3.7 *Um* $[5,2,2]$*-código sistemático linear sobre* $\mathbb{Z}_8$ *é definido pela matriz de verificação de paridade sobre* $\mathcal{Z}_8$

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & -1 & 0 & 0 \\ 3 & 1 & 0 & -1 & 0 \\ 5 & 1 & 0 & 0 & -1 \end{bmatrix} = (h_1, h_2, h_3, h_4, h_5).$$

Como $4h_1 + 4h_2 = 0$ *temos que* $d = 2$*. Seja* g *um gerador de* $\mathbb{Z}_8$*. Então as palavras código têm a forma*

$$\left(g^{c_1}, g^{c_2} \mid g^{c_1+c_2}, g^{3c_1+c_2}, g^{5c_1+c_2}\right)$$

Exemplo 3.8 *Um* $[5,2,3]$*-código sistemático linear sobre* $\mathbb{Z}_8$ *é definido pela matriz de verificação de paridade sobre* $\mathcal{Z}_8$*.*

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix} = (h_1, h_2, h_3, h_4, h_5)$$

Como $h_1 + h_3 + h_5 = 0$ *temos que* $d = 3$*. Seja* g *um gerador de* $\mathbb{Z}_8$*. Então as palavras código têm a forma*

$$\left(g^{c_1}, g^{c_2} \mid g^{c_1+c_2}, g^{c_2}, g^{c_1}\right)$$

Este é um exemplo de um código ótimo, pois o Corolário 2.3 *exclui a existência de um* $[5,2,4]$ *sobre* $\mathbb{Z}_8$*.*

Teorema 3.2 *Seja* C *um* $[n,k]$*-código sistemático linear sobre um grupo abeliano* G *de expoente* d_m*. Então, a matriz de verificação de paridade* $\mathbf{H}$ *é uma matriz escalonada* $m(n-k) \times mn$ *sobre* $\mathcal{Z}_{d_m}$*. A mínima distância de Hamming* d *do código é igual ao número mínimo de colunas linearmente dependentes de* $\mathbf{H}$ *do sistema homogêneo* (3.3) *sobre* $\mathcal{Z}_{d_m}$*, com cada conjunto de colunas companheiras contando uma vez.*

Demonstração. Observe que a mínima distância é caracterizada pelo número mínimo de elementos diferentes da identidade na palavra código. Diferentes geradores na mesma posição não aumenta a distância . Logo, colunas companheiras que define elementos associados com diferentes geradores de G mas localizado na mesma posição da palavra código conta exatamente uma vez no mesmo peso da palavra código. ■

Exemplo 3.9 *Um* $[5,2,3]$*-código sistemático linear sobre* $\mathbb{Z}_2 \times \mathbb{Z}_4$ *é definido pela matriz de verificação de paridade sobre* $\mathcal{Z}_4$*.*

$$\mathbf{H} = \begin{bmatrix} A_{11} & A_{12} & -I_3 & 0 \\ A_{21} & A_{22} & 0 & -I_3 \end{bmatrix}$$
$$= (h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, h_9, h_{10}),$$

onde

$$A_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 3 \end{bmatrix}, A_{12} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$A_{21} = \begin{bmatrix} 3 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}, A_{22} = \begin{bmatrix} 2 & 2 \\ 2 & 0 \\ 1 & 2 \end{bmatrix}.$$

Como $2(h_1 + h_3) + 2(h_2 + h_4) + 2h_7 = 0$ *temos que* $d = 3$*. Sejam* g_1, g_2 *os dois geradores de* $\mathbb{Z}_2 \times \mathbb{Z}_4$*. Então eles satisfazem as relações*

$$g_2^4 = g_1^2 = e \;\; e \;\; g_1 g_2 = g_2 g_1$$

e as palavras código têm a forma

$$(g_1^{c_1}, g_2^{d_1}, g_1^{c_2}, g_2^{d_2} \mid g_1^{c_1+c_2}, g_2^{3c_1+d_1+2c_2+2d_2}, g_1^{d_1+d_2}, g_2^{c_1+d_1+2c_2}, g_1^{c_1+3d_1+c_2}, g_2^{d_1+c_2+2d_2})$$

Exemplo 3.10 *Um* $[5,2,3]$*-código sistemático linear sobre* $\mathbb{Z}_2$ *é definido pela matriz de verificação de paridade sobre* $\mathbb{Z}_2$*.*

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} = (h_1, h_2, h_3, h_4, h_5)$$

Como $h_1 + h_3 + h_5 = 0$ *temos que* $d = 3$*. Seja* g *um gerador de* $\mathbb{Z}_2$*. Então as palavras código têm a forma*

$$(g^{c_1}, g^{c_2} \mid g^{c_1+c_2}, g^{c_2}, g^{c_1})$$

3.4 Códigos de Grupos Multiníveis

Nesta seção apresentaremos uma construção de códigos de grupos a partir de códigos conhecidos.

Sejam G um grupo, H e K dois subgrupos. Dizemos que G é um *produto semidireto* 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 $K \simeq \frac{G}{H}$.

Seja G o produto semidireto de H por K. Então, cada $g \in G$ pode ser escrito de modo único na forma:

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

Teorema 3.3 *Sejam $G = H \rtimes K$, $C_H \subseteq H^{\mathbb{I}}$ e $C_K \subseteq K^{\mathbb{I}}$ códigos de grupos. Então o conjunto*

$$C_G = \{\mathbf{hk} : \mathbf{h} \in C_H \text{ e } \mathbf{k} \in C_K\}$$

é um código de grupo sobre G se $\mathbf{khk}^{-1} \in C_H$, para todo $\mathbf{h} \in C_H$ e $\mathbf{k} \in C_K$. O código C_G é chamado código estendido *e denotado por $C_G = C_H \odot C_K$.*

Demonstração. Sabemos que $\mathbf{e} \in C_H$ e $\mathbf{e} \in C_K$. Logo,

$$\mathbf{e} = \mathbf{ee} \in C_G \text{ e } C_G \neq \emptyset.$$

Dados $\mathbf{g}_1, \mathbf{g}_2 \in C_G$. Então $\mathbf{g}_1 = \mathbf{h}_1\mathbf{k}_1$ e $\mathbf{g}_2 = \mathbf{h}_2\mathbf{k}_2$, para algum $\mathbf{h}_1, \mathbf{h}_2 \in C_H$ e $\mathbf{k}_1, \mathbf{k}_2 \in C_K$. Logo,

$$\begin{aligned}
\mathbf{g}_1\mathbf{g}_2^{-1} &= (\mathbf{h}_1\mathbf{k}_1)(\mathbf{h}_2\mathbf{k}_2)^{-1} \\
&= \mathbf{h}_1\mathbf{k}_1(\mathbf{k}_2^{-1}\mathbf{h}_2^{-1}) \\
&= \mathbf{h}_1(\mathbf{k}_1\mathbf{k}_2^{-1}\mathbf{h}_2^{-1}) \\
&= \mathbf{h}_1(\mathbf{k}_1\mathbf{k}_2^{-1}\mathbf{h}_2^{-1}\mathbf{k}_2\mathbf{k}_1^{-1})(\mathbf{k}_1\mathbf{k}_2^{-1}) \in C_G.
\end{aligned}$$

Portanto, C_G é um código de grupo sobre G. ■

Corolário 3.1 *Sejam $G = H \times K$ um grupo abeliano aditivo, $C_H \subseteq H^{\mathbb{I}}$ e $C_K \subseteq K^{\mathbb{I}}$ códigos de grupos. Então o código estendido $C_G = C_H \odot C_K$*

$$C_G = \{\mathbf{h} + \mathbf{k} : \mathbf{h} \in C_H \text{ e } \mathbf{k} \in C_K\}$$

é um código de grupo sobre G. ■

(e,e,e,e,e)	(s,s,s,e,e)	(e,e,s,s,s)	(s,s,e,s,s)
(r,r,r,e,e)	(sr^2,sr^2,sr^2,e,e)	(r,r,sr^2,s,s)	(sr^2,sr^2,r,s,s)
(r^2,r^2,r^2,e,e)	(sr,sr,sr,e,e)	(r^2,r^2,sr,s,s)	(sr,sr,r^2,s,s)
(e,e,r,r,r)	(s,s,sr^2,r,r)	(e,e,sr^2,sr^2,sr^2)	(s,s,r,sr^2,sr^2)
(e,e,r^2,r^2,r^2)	(s,s,sr,r^2,r^2)	(e,e,sr,sr,sr)	(s,s,r^2,sr,sr)
(r,r,r^2,r,r)	(sr^2,sr^2,sr,r,r)	(r,r,sr,sr^2,sr^2)	$(sr^2,sr^2,r^2,sr^2,sr^2)$
(r,r,e,r^2,r^2)	(sr^2,sr^2,s,r^2,r^2)	(r,r,s,sr,sr)	(sr^2,sr^2,e,sr,sr)
(r^2,r^2,e,r,r)	(sr,sr,s,r,r)	(r^2,r^2,s,sr^2,sr^2)	(sr,sr,e,sr^2,sr^2)
(r^2,r^2,r,r^2,r^2)	(sr,sr,sr^2,r^2,r^2)	(r^2,r^2,sr^2,sr,sr)	(sr,sr,r,sr,sr)

Tabela 3.1: $[5,2,3]$-código de grupo sobre G

Exemplo 3.11 *Seja*

$$G=\{e,r,r^2,s,sr,sr^2\},$$

com $r^3=s^2=e$ *e* $sr=r^2s$. *Então* $G=H\rtimes K$, *onde* $H=\{e,r,r^2\}$ *e* $K=\{e,s\}$. *Sejam*

$$C_H=\langle(r,r,r,e,e),(e,e,r,r,r)\rangle\subseteq H^5$$

e

$$C_K=\langle(s,s,s,e,e),(e,e,s,s,s)\rangle\subseteq K^5$$

$[5,2,3]$*-códigos de grupos. É fácil verificar que* $\mathbf{khk}^{-1}\in C_H$, *para todo* $\mathbf{h}\in C_H$ *e* $\mathbf{k}\in C_K$. *O código estendido* C_G *é o* $[5,2,3]$*-código dado pela Tabela* 3.1

Sejam $G=H\rtimes K$ e $C_G\subseteq G^{\mathbb{I}}$ um código de grupo. Então toda palavra código $\mathbf{g}\in C_G$ pode ser escrita de modo único na forma

$$\mathbf{g}=\mathbf{h}_g\mathbf{k}_g$$

Teorema 3.4 *Sejam* $G=H\rtimes K$ *e* $C_G\subseteq G^{\mathbb{I}}$ *um código de grupo. Então*

$$C_G=\{\mathbf{hk}:\mathbf{h}\in C_H\ e\ \mathbf{k}\in C_K\}$$

se, e somente se, $\mathbf{h}_g,\mathbf{k}_g\in C_G$, *para todo* $\mathbf{g}\in C_G$.

Demonstração. Se $\mathbf{g}\in C_G$, então $\mathbf{g}=\mathbf{hk}$, com $\mathbf{h}\in C_H$ e $\mathbf{k}\in C_K$. Como C_H e C_K são códigos de grupos temos que $\mathbf{e}\in C_H$. Assim, $\mathbf{k}=\mathbf{ek}\in C_G$. De modo análogo, $\mathbf{h}=\mathbf{he}\in C_G$.

A recíproca é imediata. ■

Corolário 3.2 *Todo código de grupo sobre:* $G = \mathbb{Z}_m \times \mathbb{Z}_n$, *com* $\mathrm{mdc}\,(m,n) = 1$, *pode ser obtido como códigos estendido de um código de grupo sobre* $\mathbb{Z}_m$ *e um código de grupo sobre* $\mathbb{Z}_n$. ■

Capítulo 4

Códigos MDS

Neste capítulo caracterizaremos o conjunto de homomorfismos de grupos que define códigos de grupos com máxima distância separável (MDS) sobre o grupo cíclico $\mathbb{Z}_m$. Além disto, mostraremos que o código dual de um código de grupo com máxima distância separável sobre $\mathbb{Z}_m$ é também um código de grupo com máxima distância separável

4.1 Códigos MDS sobre Grupos Cíclicos

Nesta seção identificaremos os homomorfismos que define códigos de grupos com máxima distância separável (MDS) sobre o grupo cíclico $\mathbb{Z}_m$.

Sabemos que um $[n,k]$-código sistemático linear C sobre o grupo abeliano G é um subgrupo de G^n com ordem $|G|^k$, descrito por $(n-k)$ homomorfismo de grupos ϕ_l de G^k sobre G. Suas palavras código são:

$$(c_1, c_2, \ldots, c_k \mid d_{k+1}, \ldots, d_n),$$

onde

$$\begin{aligned} d_{k+l} &= \phi_l(c_1, c_2, \ldots, c_k) \\ &= \prod_{j=1}^{k} \phi_l(e, \ldots, c_j, \ldots, e), \forall l = 1, \ldots, n-k. \end{aligned} \tag{4.1}$$

Assim, um único homomorfismo de $\mathbb{Z}_m^k$ para $\mathbb{Z}_m$ define um $[k+1,k]$-código sistemático linear sobre $\mathbb{Z}_m$. Qualquer componente nos últimos termos da equação 4.1,

$$\phi_l(e, \ldots, c_j, \ldots, e)$$

é essencialmente um elemento de End($\mathbb{Z}_m$). Assim, qualquer palavra código

$$(c_1, c_2, \ldots, c_k \mid d_{k+1}, \ldots, d_{k+s})$$

de um $[k+s, k]$-código grupo sobre $\mathbb{Z}_m$ é da forma

$$(c_1, c_2, \ldots, c_k \mid \prod_{j=1}^{k} \varphi_{j1}(c_j), \ldots, \prod_{j=1}^{k} \varphi_{js}(c_j)),$$

onde $c_i \in \mathbb{Z}_m$, φ_{jl} são k endomorfismos de $\mathbb{Z}_m$ e os ϕ_l são ditos decompostos como estes endomorfismos, que denotaremos por

$$\phi_l = \varphi_{1l} \cdots \varphi_{kl}, \forall l = 1, \ldots, s.$$

Dizemos que um homomorfismo $\phi : \mathbb{Z}_m^k \longrightarrow \mathbb{Z}_m$ é *homomorfismo com distância crescente* (HDC) se

$$\ker \phi = \{\mathbf{e}\} \text{ ou } d_H(\ker \phi) = 2.$$

Proposição 4.1 *Um $[k+1, k]$-código de grupo sobre $\mathbb{Z}_m$ é MDS se, e somente se, $\phi : \mathbb{Z}_m^k \longrightarrow \mathbb{Z}_m$ é um HDC.*

Demonstração. Suponhamos que C é um $[k+1, k]$-código de grupo MDS sobre $\mathbb{Z}_m$. Então

$$d_H(C) = k + 1 - k + 1 = 2,$$

isto é, toda palavra código de C tem pelo menos duas componentes diferentes de e. Se $\ker \phi \neq \{\mathbf{e}\}$, então existe

$$\mathbf{c} = (e, \ldots, c_i, \ldots, c_j, \ldots, e \mid \phi((e, \ldots, c_i, \ldots, c_j, \ldots, e))) \in C - \{\mathbf{e}\},$$

com $i \neq j$ tal que

$$\phi((e, \ldots, c_i, \ldots, c_j, \ldots, e)) = e.$$

Logo, $d_H(\ker \phi) = 2$. Portanto, $\phi : \mathbb{Z}_m^k \longrightarrow \mathbb{Z}_m$ é um HDC.

Reciprocamente, suponhamos que $\phi : \mathbb{Z}_m^k \longrightarrow \mathbb{Z}_m$ é um HDC. Então para cada

$$\mathbf{c} = (c_1, c_2, \ldots, c_k \mid \phi((c_1, c_2, \ldots, c_k))) \in C$$

temos dois casos há serem considerados:

1º Caso - Se $\phi((c_1, c_2, \ldots, c_k)) = e$, então

$$(c_1, c_2, \ldots, c_k) = (e, e, \ldots, e)$$

ou $d_H(\mathbf{c}) \geq 2$.

$2^{\underline{0}}$ Caso - Se $\phi((c_1, c_2, \ldots, c_k)) \neq e$, então pelo menos um dos $c_i \neq e$. Logo, $d_H(\mathbf{c}) \geq 2$.

Portanto, em qualquer um dos casos, temos que $d_H(\mathbf{c}) \geq 2$. Pela Proposição 2.1,

$$d_H(\mathbf{c}) \leq k + 1 - k + 1 = 2.$$

Portanto, C é um $[k+1, k]$-código de grupo MDS sobre $\mathbb{Z}_m$. ■

Proposição 4.2 *Seja $\phi : \mathbb{Z}_m^k \longrightarrow \mathbb{Z}_m$ um homomorfismo de grupos, onde $\phi = \varphi_1\varphi_2\cdots\varphi_k$. Então ϕ é HDC se, e somente se, $\varphi_i \in \mathrm{Aut}(\mathbb{Z}_m)$, para cada $i = 1, \ldots, k$.*

Demonstração. Suponhamos, por absurdo, que $\varphi_i \notin \mathrm{Aut}(\mathbb{Z}_m)$, para algum $i = 1, \ldots, k$. Então existe $c_i \in \mathbb{Z}_m$, $c_i \neq e$ tal que $c_i \in \ker \varphi_i$. Logo,

$$\phi\left((e, \ldots, c_i, \ldots, e\right) = \varphi_i\left(c_i\right) = e,$$

isto é, $d_H(\ker \phi) = 1$, o que é uma contradição.

Reciprocamente, Suponhamos que $\varphi_i \in \mathrm{Aut}(\mathbb{Z}_m)$, para cada $i = 1, \ldots, k$, e

$$\mathbf{d} = (e, \ldots, d_i, \ldots, e) \in \mathbb{Z}_m^k,$$

com $d_i \neq e$. Então $\phi\left(\mathbf{d}\right) = \varphi_i\left(d_i\right) \neq e$ e a mínima distância do código definido por ϕ é igual a 2. Assim, pela Proposição 4.1, temos que ϕ é HDC ■

Sejam $\Phi_s = \{\phi_i\}_{i=1}^s$ um conjunto de homomorfismos de $\mathbb{Z}_m^k$ em $\mathbb{Z}_m$ e

$$\ker\left(\phi_1 \cdots \phi_s\right) = \ker \phi_1 \cap \cdots \cap \ker \phi_s.$$

Se para cada r, $1 \leq r \leq s$,

$$\ker\left(\phi_{i_1} \cdots \phi_{i_r}\right) = \{\mathbf{e}\} \text{ ou } d_H(\ker\left(\phi_{i_1} \cdots \phi_{i_r}\right)) = r + 1, \forall i_j \in \{1, \ldots, s\},$$

então dizemos que Φ_s é um *conjunto com distância crescente de homomorfismos* (CDCH).

Observação 4.1 *Se Φ_s é um CDCH, então todo subconjunto de Φ_s também o é.*

Teorema 4.1 *Um $[k+s, k]$-código de grupo sobre $\mathbb{Z}_m$ definido por Φ_s é MDS se, e somente se, Φ_s é um CDCH.*

Demonstração. Suponhamos que C seja um $[k+s,k]$-código de grupo MDS sobre $\mathbb{Z}_m$ definido por Φ_s. Então

$$d_H(C) = k + s - k + 1 = s + 1,$$

isto é, toda palavra código de C tem pelo menos $s+1$ componentes diferentes de e. Assim, se

$$\mathbf{c} = (c_1, c_2, \ldots, c_k \mid d_{k+1}, \ldots, d_{k+s}) \in C$$

tem exatamente r, $0 \leq r \leq s$, elementos $d_{k+i_j} \in \{d_{k+1}, \ldots, d_{k+s}\}$ são iguais e, com $j = 1, \ldots, r$, então a palavra código

$$\widehat{\mathbf{c}} = (c_1, c_2, \ldots, c_k \mid d_{k+i_1}, \ldots, d_{k+i_r})$$

é tal que

$$\begin{aligned} d_H(\widehat{\mathbf{c}}) &\geq (s+1) - (s-r) \\ &= r + 1. \end{aligned}$$

Logo, $\Phi_{i_r} = \{\phi_{i_j}\}_{j=1}^{r}$ é um CDCH. Portanto, Φ_s é um CDCH.

Reciprocamente, suponhamos que Φ_s é um CDCH e

$$\begin{aligned} \mathbf{c} &= (c_1, c_2, \ldots, c_k \mid d_{k+1}, \ldots, d_{k+s}) \\ &= (c_1, c_2, \ldots, c_k \mid \phi_1(c_1, c_2, \ldots, c_k), \ldots, \phi_s(c_1, c_2, \ldots, c_k)) \in C. \end{aligned}$$

Se exatamente r, $0 \leq r \leq s$, elementos $d_{k+i_j} \in \{d_{k+1}, \ldots, d_{k+s}\}$ são diferentes de e, com $j = 1, \ldots, r$, então, eliminando estas componentes, a parte restante $\widehat{\mathbf{c}}$ de $\mathbf{c}$ é uma palavra código do código definido por um subconjunto de $\Phi_{(s)}$ consistindo de $s-r$ homomorfismos. Logo, por definição

$$d_H(\widehat{\mathbf{c}}) \geq s - r + 1.$$

Assim,

$$\begin{aligned} d_H(\mathbf{c}) &\geq r + (s - r + 1) \\ &= s + 1. \end{aligned}$$

Portanto, pela Proposição 4.1, temos que o código definido por Φ_s é um MDS. ■

Corolário 4.1 *Se*

$$C = \{(c_1, c_2, \ldots, c_k \mid \phi_1(c_1, c_2, \ldots, c_k), \ldots, \phi_s(c_1, c_2, \ldots, c_k)) : c_i \in \mathbb{Z}_m\}$$

é um $[k+s,k]$-código de grupo MDS, então o $[k+t,k]$-código de grupo C_t definido por um subconjunto de t homomorfismo definindo C é MDS, para todo $t = 1, \ldots, s-1$,. ■

4.2 Caracterização Matricial de Códigos MDS

Sabemos que cada $\varphi \in \mathrm{End}(\mathbb{Z}_m)$ é unicamente definido pela imagem do gerador de $\mathbb{Z}_m$ sob φ. Além disto, $\mathrm{End}(\mathbb{Z}_m) \simeq \mathcal{Z}_m$ e $\varphi(g) = g^\alpha \in \mathrm{Aut}(\mathbb{Z}_m)$, onde $\mathbb{Z}_m = \langle g \rangle$, se, e somente se, $\mathrm{mdc}(m, \alpha) = 1$ ou, equivalentemente, $\alpha \in U(\mathcal{Z}_m)$ o conjunto das unidades de $\mathcal{Z}_m$.

Seja

$$C = \{(c_1, c_2, \ldots, c_k \mid \phi_1(c_1, c_2, \ldots, c_k), \ldots, \phi_s(c_1, c_2, \ldots, c_k)) : c_i \in \mathbb{Z}_m\}$$

um $[k+s, k]$-código de grupo sobre $\mathbb{Z}_m$. Então a matriz

$$\mathbf{P} = (\alpha_{ij})_{k \times s} \tag{4.2}$$

sobre $\mathcal{Z}_m$, onde

$$\phi_j = \varphi_{1j}\varphi_{2j}\cdots\varphi_{kj}, \forall j = 1, \ldots, s \text{ e } \varphi_{ij}(g) = g^{\alpha_{ij}}, i = 1, \ldots, k$$

é chamada *matriz associada* ao código C. Assim, a matriz geradora $\mathbf{G}$ de C pode ser escrita na forma

$$\mathbf{G} = [\ \mathbf{I}_k \quad \mathbf{P}\ ]$$

e a palavra código $\mathbf{c}$ corespondente à mensagem $\mathbf{u} = (c_1, \ldots, c_k)$ é dada por

$$\mathbf{c} = \mathbf{uG}.$$

As equações de verificação de paridades são

$$d_{k+r} = \sum_{i=1}^{k} c_i \alpha_{ir}, r = 1, \ldots, s,$$

as quais, na forma matricial, tornam-se

$$[\ -\mathbf{P}^t \quad \mathbf{I}_s\ ]\mathbf{c}^t = \mathbf{O}.$$

A matriz de verificação de paridade $\mathbf{H}$ do código C é dada por

$$\mathbf{H} = [\ -\mathbf{P}^t \quad \mathbf{I}_{s\times s}\ ].$$

Note que, esta matriz $\mathbf{H}$ pode ser obtida da matriz de verificação de paridade dada no Capítulo anterior para códigos de grupos sobre grupos abelianos restrigindo a grupos cíclicos.

Proposição 4.3 *[7, Corollary3, pp.319] Seja $q = p^a$, onde p é primo e $a \in \mathbb{N}$. Então $[n, k, d]$-código linear C sobre F_q é MDS se, e somente se, qualquer k colunas da matriz geradora $\mathbf{G}$ de C são linearmente independentes.* ■

O próximo teorema é uma generalização de um resultado dado em [7, Theorem 8, pp. 321].

Teorema 4.2 *Seja*

$$C = \{(c_1, c_2, \ldots, c_k \mid \phi_1(c_1, c_2, \ldots, c_k), \ldots, \phi_s(c_1, c_2, \ldots, c_k)) : c_i \in \mathbb{Z}_m\}$$

um $[k+s, k]$-código de grupo sobre $\mathbb{Z}_m$. Então C é MDS se, e somente se, o determinante de qualquer submatriz $t \times t$ da matriz associada é uma unidade em $\mathcal{Z}_m$, para cada $t = 1, \ldots, \min\{s, k\}$.

Demonstração. Suponhamos que C é um código MDS. Seja $\widehat{C}$ o código obtido de C pela eliminação de todas as componentes exceto as componentes

$$\{c_{j_1}, \ldots, c_{j_t}, c_{k+i_1}, \ldots, x_{k+i_t}\},$$

isto é, $\widehat{C}$ é um $[2t, t]$-código e sua matriz associada será denotada por $\mathbf{P}_t$. É claro que $\widehat{C}$ é um código MDS e $d_H(\widehat{C}) = t + 1$. Considere a seguinte equação matricial.

$$\mathbf{P}_t \widehat{\mathbf{c}}^t = \mathbf{0}. \tag{4.3}$$

Se existir um vetor $\widehat{\mathbf{c}} = (c_1, \ldots, c_t) \neq \mathbf{0}$ satisfazendo a equação 4.3, então o vetor

$$\mathbf{c} = (c_1, \ldots, c_t, 0, \ldots, 0)$$

é uma palavra código de $\widehat{C}$ com $d_H(\mathbf{c}) \leq t$, o que é uma contradição. Logo, a única solução da equação 4.3 é o vetor nulo. Portanto, o determinante de $\mathbf{P}_t$ é uma unidade em $\mathcal{Z}_m$.

Reciprocamente, seja $\mathbf{P}$ a matriz associada do código C e suponhamos que o determinante de qualquer submatriz $t \times t$ de $\mathbf{P}$ seja uma unidade em $\mathcal{Z}_m$, para cada $t = 1, \ldots, \min\{s, r\}$. Considerando

$$\mathbf{c} = (c_1, c_2, \ldots, c_k \mid c_{k+1}, \ldots, c_{k+s}) \in C,$$

com $c_i = g^{\beta_i}$, onde g é um gerador de $\mathbb{Z}_m$ temos que $\mathbf{c}$ pode ser representado por

$$\boldsymbol{\beta} = \left(\beta_1, \ldots, \beta_k, \beta_{k+1}, \ldots, \beta_{k+s}\right).$$

Com esta representação temos que

$$\beta_{k+r} = \alpha_{r1}\beta_1 + \alpha_{r2}\beta_2 + \cdots + \alpha_{rk}\beta_k, r = 1, \ldots, s,$$

onde a soma é efetuada em $\mathcal{Z}_m$.

Suponhamos que no conjunto

$$\{\beta_1, \ldots, \beta_k\}$$

somente t elementos sejam diferentes de zero, digamos $\beta_{j_1}, \ldots, \beta_{j_t}$. Então a equação anterior reduz-se a

$$\beta_{k+r} = \alpha_{rj_1}\beta_{j_1} + \alpha_{rj_2}\beta_{j_2} + \cdots + \alpha_{rj_t}\beta_{j_t}, r = 1, \ldots, s.$$

Suponhamos que t destes elementos sejam zeros, digamos $\beta_{k+i_1}, \ldots, \beta_{k+i_t}$. Então

$$\alpha_{rj_1}\beta_{j_1} + \alpha_{rj_2}\beta_{j_2} + \cdots + \alpha_{rj_t}\beta_{j_t} = 0, r = i_1, \ldots, i_t.$$

Logo, por hipótese,

$$\beta_{j_1} = \beta_{j_2} = \cdots = \beta_{j_t} = 0,$$

que é uma contradição. Logo,

$$\begin{aligned} d_H(\mathbf{c}) &\geq (t+s) - t + 1 \\ &= s + 1. \end{aligned}$$

Portanto, C é um MDS. ■

Exemplo 4.1 *Seja C o $[4,2]$-código de grupo sobre $\mathbb{Z}_9$ definido pela matriz geradora*

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}.$$

Então C é um código MDS com $d_H(C) = 3$, pois $\det(\mathbf{P}) = 1 \in U(\mathcal{Z}_9)$. Note que a matriz de verificação de paridade de C é dada por

$$\mathbf{H} = \begin{bmatrix} 8 & 8 & 1 & 0 \\ 8 & 7 & 0 & 1 \end{bmatrix}.$$

4.3 Sobre a Existência de Códigos MDS

Apresentaremos nesta seção alguns resultados da não existência de códigos MDS sobre $\mathbb{Z}_m$, onde m é um produto de primos distintos, digamos

$$m = p_1^{a_1} \cdots p_l^{a_l}$$

com $a_i \in \mathbb{Z}_+$.

Proposição 4.4 *Seja $m = p^a$, onde p é primo e $a \in \mathbb{N}$. Então existe um $[k+1, k]$-código de grupo MDS sobre $\mathbb{Z}_m$, para todo $k \in \mathbb{N}$.*

Demonstração. Pela Proposição 2.4 existe um $[k+1, k, 2]$-código MDS C sobre $\mathbb{Z}_m$, para todo $k \in \mathbb{N}$. Assim, a matriz geradora de C é dada por

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \cdots & 0 & \alpha_{1(k+1)} \\ 0 & 1 & \cdots & 0 & \alpha_{2(k+1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_{k(k+1)} \end{bmatrix},$$

onde $\alpha_{i(k+1)} \in \mathcal{Z}_m$, para todo $i = 1, \ldots, k$. Como $d_H(C) = 2$ temos que $\alpha_{ik+1} \in U(\mathcal{Z}_m)$, para todo $i = 1, \ldots, k$. Portanto, pelo Teorema 4.2, C é um código de grupo MDS. ■

Proposição 4.5 *Seja $m = p^a$, onde p é primo e $a \in \mathbb{N}$. Então existe um $[1+s, 1]$-código de grupo MDS sobre $\mathbb{Z}_m$, para todo $s \in \mathbb{N}$.*

Demonstração. Seja C um $[1+s, 1]$-código de grupo sobre $\mathbb{Z}_m$, para todo $s \in \mathbb{N}$. Então a matriz geradora de C é dada por

$$\mathbf{G} = \begin{bmatrix} 1 & \alpha_{11} & \cdots & \alpha_{1s} \end{bmatrix},$$

onde $\alpha_{1(i+1)} \in \mathcal{Z}_m$, para todo $i = 1, \ldots, s-1$. Se $\alpha_{1(i+1)} \in U(\mathcal{Z}_m)$, para todo $i = 1, \ldots, s-1$, então, pelo Teorema 4.2, C é um código de grupo MDS. ■

Proposição 4.6 *Seja $m = p^a$, onde p é primo e $a \in \mathbb{N}$. Então não existe $[k+2, k]$-código de grupo MDS sobre $\mathbb{Z}_m$, com $k \geq p$.*

Demonstração. Seja C um $[k+2,k]$-código de grupo sobre $\mathbb{Z}_m$. Então a matriz geradora de C é dada por

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \cdots & 0 & \alpha_{1(k+1)} & \alpha_{1(k+2)} \\ 0 & 1 & \cdots & 0 & \alpha_{2(k+1)} & \alpha_{2(k+2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_{k(k+1)} & \alpha_{k(k+2)} \end{bmatrix},$$

onde $\alpha_{i(k+j)} \in \mathcal{Z}_m$, para todo $i = 1, \ldots, k$ e $j = 1, 2$. Suponhamos que C seja um código de grupo MDS sobre $\mathbb{Z}_m$. Então, pelo Teorema 4.2, cada submatriz

$$\mathbf{P}_2 = \begin{bmatrix} \alpha_{i_1(k+j_1)} & \alpha_{i_1(k+j_2)} \\ \alpha_{i_2(k+j_1)} & \alpha_{i_2(k+j_2)} \end{bmatrix} \tag{4.4}$$

da matriz associada $\mathbf{P}$ tem determinante uma unidade em $\mathcal{Z}_m$. Ou, equivalentemente, o determinante da matriz

$$\mathbf{P}_2' = \begin{bmatrix} 1 & 1 \\ \alpha_{i_1(k+j_1)}^{-1}\alpha_{i_2(k+j_1)} & \alpha_{i_1(k+j_2)}^{-1}\alpha_{i_2(k+j_2)} \end{bmatrix} \tag{4.5}$$

é uma unidade em $\mathcal{Z}_m$. Assim,

$$\alpha_{i_1(k+j_1)}^{-1}\alpha_{i_2(k+j_1)}[1 - \alpha_{i_1(k+j_1)}\alpha_{i_2(k+j_1)}^{-1}\alpha_{i_1(k+j_2)}^{-1}\alpha_{i_2(k+j_2)}] \not\equiv 0 \pmod{p}.$$

e o número de valores diferentes para cada $\alpha_{i_1(k+j_1)}^{-1}\alpha_{i_2(k+j_1)}$ não pode exceder a $p-1$, ou seja, dois elementos de uma classe lateral à esquerda de $\mathcal{Z}_p$ em $\mathcal{Z}_m$ não pode aparecer na segunda linha de 4.5. Logo, existem somente $p-1$ classes laterais à esquerda de $\mathcal{Z}_p$ em $\mathcal{Z}_m$. Portanto, um $[k+2,k]$-código de grupo MDS sobre $\mathbb{Z}_m$ não existe se $k \geq p$. ■

O próximo teorema é uma generalização da Proposição 2.3.

Teorema 4.3 *Seja $m = p^a$, onde p é primo e $a \in \mathbb{N}$. Então não existe $[k+s,k]$-código de grupo MDS sobre $\mathbb{Z}_m$, com* $\max\{s,k\} \geq p$ *e* $k, s \in \mathbb{N} - \{1\}$.

Demonstração. Seja C um $[k+s,k]$-código de grupo sobre $\mathbb{Z}_m$. Então a matriz geradora de C é dada por

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \cdots & 0 & \alpha_{1(k+1)} & \cdots & \alpha_{1(k+s)} \\ 0 & 1 & \cdots & 0 & \alpha_{2(k+1)} & \cdots & \alpha_{2(k+s)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_{k(k+1)} & \cdots & \alpha_{k(k+s)} \end{bmatrix},$$

onde $\alpha_{i(k+j)} \in \mathcal{Z}_m$, para todo $i = 1, \ldots, k$ e $j = 1, \ldots, s$. Suponhamos que C seja um código de grupo MDS sobre $\mathbb{Z}_m$. Então, pelo Teorema 4.2, cada submatriz

$$\mathbf{P}_t = \begin{bmatrix} \alpha_{i_1(k+j_1)} & \alpha_{i_1(k+j_t)} \\ \alpha_{i_t(k+j_1)} & \alpha_{i_t(k+j_t)} \end{bmatrix}, \tag{4.6}$$

onde $t = \min\{s, k\}$, da matriz associada $\mathbf{P}$ tem determinante uma unidade em $\mathcal{Z}_m$. Ou, equivalentemente, o determinante da matriz

$$\mathbf{P}'_t = \begin{bmatrix} 1 & 1 \\ 1 & \alpha \end{bmatrix} \tag{4.7}$$

é uma unidade em $\mathcal{Z}_m$. Assim, dois elementos de uma classe lateral à esquerda de $\mathcal{Z}_p$ em $\mathcal{Z}_m$ não pode aparecer na segunda linha ou coluna de 4.7, exceto a primeira linha e coluna. Logo, existem somente $p-1$ classes laterais à esquerda de $\mathcal{Z}_p$ em $\mathcal{Z}_m$, isto é, $k \leq p-1$. Portanto, um $[k+2, k]$-código de grupo MDS sobre $\mathbb{Z}_m$ não existe se $k \geq p$.■

Corolário 4.2 *Seja $n \in N$. Então não existe $[n, k, d]$-código de grupo MDS sobre F_2, exceto $[n, 1, n]$ e $[n, n-1, 2]$.* ■

Teorema 4.4 *Seja $m = p_1^{a_1} \cdots p_l^{a_l}$, onde p_i são primos distintos e $a_i \in \mathbb{Z}_+$. Então não existe $[k+s, k]$-código de grupo MDS sobre $\mathbb{Z}_m$, com*

$$\max\{s, k\} \geq \min\{p_1, \ldots, p_l\} \;\; e \;\; k, s \in \mathbb{N} - \{1\}.$$

Demonstração. Seja C um $[k+s, k]$-código de grupo sobre $\mathbb{Z}_m$. Então a matriz geradora de C é dada por

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \cdots & 0 & \alpha_{1(k+1)} & \cdots & \alpha_{1(k+s)} \\ 0 & 1 & \cdots & 0 & \alpha_{2(k+1)} & \cdots & \alpha_{2(k+s)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_{k(k+1)} & \cdots & \alpha_{k(k+s)} \end{bmatrix},$$

onde $\alpha_{i(k+j)} \in \mathcal{Z}_m$, para todo $i = 1, \ldots, k$ e $j = 1, \ldots, s$. Seja

$$\mathbf{P}' = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta_{11} & \cdots & \beta_{1(s-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_{(k-1)1} & \cdots & \beta_{(k-1)(s-1)} \end{bmatrix} \tag{4.8}$$

a matriz obtida de $\mathbf{P}$ por multiplicação de cada linha e coluna por unidades apropriadas. Assim , uma condição necessária para o código C ser MDS é que

$$\det \begin{bmatrix} 1 & 1 \\ \beta_{1i} & \beta_{1j} \end{bmatrix} = \beta_{1j} - \beta_{1i}, i \neq j,$$

seja uma unidade em $\mathcal{Z}_m$. Isto significa que, para cada $t = 1, \ldots, l$,

$$\beta_{1j} - \beta_{1i} = \beta_{1j}\left(1 - \beta_{1j}^{-1}\beta_{1i}\right) \not\equiv 0 \pmod{p_t}.$$

Logo, pelos argumentos usados na demonstração da Proposição 4.6 e do Teorema 4.3, temos que o número de valores diferentes para cada β_{1i} não pode exceder ao $\min\{p_1, \ldots, p_m\} - 1$. Portanto, não existe $[k+s, k]$-código de grupo MDS sobre $\mathbb{Z}_m$, com

$$\max\{s, k\} \geq \min\{p_1, \ldots, p_l\} \text{ e } k, s \in \mathbb{N} - \{1\}.$$

■

O próximo corolário é uma generalização do Teorema 2.4.

Corolário 4.3 *Seja $m \in N$ um número par. Então não existe $[n, k]$-código de grupo MDS sobre $\mathbb{Z}_m$, exceto $[k+1, k]$ e $[1+s, 1]$.* ■

4.4 Códigos Duais de Códigos MDS

Nesta seção usaremos o grupo de caracteres de um grupo abeliano G para definir o código dual de um código de grupo sobre G.

Seja C um $[n, k]$-código de grupo sobre um grupo abeliano G. O $[n, n-k]$-*código dual*, denotado por $C^{\perp}$, é definido como

$$C^{\perp} = \{(x_1, \ldots, x_n) \in G^n : \prod_{i=1}^{n} \chi_{c_i}(x_i) = 1, \forall\, (c_1, \ldots, c_n) \in C\},$$

onde $\chi_{c_i} \in \widehat{G}$, para cada $i = 1, \ldots, n$.

Já sabemos que uma matriz $\mathbf{A} = (\alpha_{ij})_{m \times m}$ sobre $\mathcal{Z}_{d_m}$ representa um endomorfismo de G se, e somente se,

$$\alpha_{ij} \in \frac{d_m}{\min\{d_i, d_j\}} \mathcal{Z}_{d_m}.$$

Assim, se φ um endomorfismo G representado pela matriz $\mathbf{A} = (\alpha_{ij})$, então o endomorfismo representado pela matriz $\mathbf{A}^d = (-\alpha_{ji})$ define o *endomorfismo dual* de φ, denotado por φ^d.

Usando as relações dadas pela Equação 4.1, o código dual $C^{\perp}$ do código de grupo C é descrito por k homomorfismo de G^{n-k} sobre G, denotado por ϕ_l^*, $l = 1, \ldots, k$, e consiste das palavras código

$$(x_1, \ldots, x_k \mid y_{k+1} \ldots, y_n),$$

onde

$$\begin{aligned} x_l &= \phi_l^* (y_{k+1}, \ldots, y_n) \\ &= \prod_{j=k+1}^{n} \phi_l^* (e, \ldots, y_j, \ldots, e) \\ &= \prod_{j=k+1}^{n} \varphi_{lj}^* (y_j) \end{aligned}$$

e $\varphi_{lj}^* = \varphi_{jl}^d$, para cada $l = 1, 2, \ldots, k$. Note que, o código dual de um código linear sistemático é também sistemático.

Teorema 4.5 *Se a matriz geradora do código de grupo C sobre $\mathbb{Z}_m$ é*

$$\mathbf{G} = [\ \mathbf{I} \quad \mathbf{P}\ ],$$

então a matriz geradora do código dual $C^{\perp}$ é

$$\mathbf{H} = [\ -\mathbf{P}^t \quad \mathbf{I}\ ].$$

Além disto, se C é MDS, então $C^{\perp}$ também o é ■

Exemplo 4.2 *Seja C o $[4, 2]$-código de grupo sobre $\mathbb{Z}_9$ definido pela matriz geradora*

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}.$$

Então C é um código MDS com $d_H(C) = 3$, pois $\det(\mathbf{P}) = 1 \in U(\mathcal{Z}_9)$. Assim, o código dual $C^{\perp}$ tem matriz geradora

$$\mathbf{H} = \begin{bmatrix} 8 & 8 & 1 & 0 \\ 8 & 7 & 0 & 1 \end{bmatrix}$$

e $d_H(C^{\perp}) = 3$, pois $\det(\mathbf{P}) = -8 = 1 \in U(\mathcal{Z}_9)$. Portanto, $C^{\perp}$ também é MDS.

Referências Bibliográficas

[1] Biglieri, E. and Elia, M., "Construction of linear block codes over groups," *IEEE Int. Symp. on Information Theory*, San Antonio, 1993.

[2] D.S. Dummit and R.M. Foote, *Abstract Algebra*, New Jersey, Prentice Hall, 1991.

[3] Forney, Jr. G. D., "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. 37, 1241-1260, 1991.

[4] Forney, Jr. G. D., "On the Hamming distance property of group codes," *IEEE Trans. Inform. Theory*, vol. 38, 1797-1801, 1992.

[5] Garcia, A.e Lequain, I. *Álgebra: Um curso de introdução*. Projeto Euclides - IMPA. Rio de Janeiro.

[6] Loeliger, H. A., "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol. 37, 1675-1682, 1991.

[7] MacWilliams, F. J. and Sloane, N. J.A., *The Theory of Error-Correcting Codes*, New York, North-Holland, 1977.

[8] Slepian, D., "Groups codes for the Gaussian channel," *B.S.T.J.*, vol. 47, 575-602, 1968.

[9] Zain, A. A. and Sundar Rajan, B., "Algebraic characterization of MDS group codes over cyclic groups," *IEEE Trans. Inform. Theory*, vol. 41, 2052-2056, 1995.