UNIVERSIDADE ESTADUAL DE CAMPINAS

FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

DEPARTAMENTO DE TELEMÁTICA

Caracterizações Algébrica e Geométrica dos Códigos Propelineares.

Martinho da Costa Araujo

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

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

Maio - 2000

Campinas - SP

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

Ar15c

Araujo, Martinho da Costa
Caracterizações algébrica e geométrica dos códigos propelineares / Martinho da Costa Araujo.--Campinas, SP: [s.n.], 2000.

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

1. Teoria de grupos. 2. Teoria da codificação. 3. Isometria (Matemática). 4. Grupos de simetria. I. Palazzo Júnior, Reginaldo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Para

Fernanda,
Eduardo e *Felipe*.

Agradecimentos

- Ao Professor Doutor Reginaldo Palazzo Júnior, pela sua orientação eficiente e segura fator indispensável na realização deste trabalho. Em especial, pela sua amizade.

- Aos Professores da Banca Examinadora: Profa. Dra. Sueli Irene Rodrigues Costa do IMECC - UNICAMP, Prof. Dr. Antonio de Andrade e Silva do CCEN - DM - UFPB, Prof. Dr. Celso de Almeida do DECOM - FEEC - UNICAMP e ao Prof. Dr. Walter da Cunha Borelli do DT - FEEC - UNICAMP.

- À Profa. Dra. Sueli Irene Rodrigues Costa do IMECC - UNICAMP, pelas valiosas sugestões.

- Aos Profs. Drs. José Carmelo Interlando, Jorge Pedraza Arpasi e João Roberto Gerônimo, pelas discussões e sugestões.Em particular, ao doutorando Marcelo Muniz Silva Alves

- Aos colegas do Curso, pelo companheirismo e ajuda mútua. De modo particular, aos amigos José Raimundo Gomes Pereira, Ivo Silva Junior, Luciano Souza Costa, Lenimar Nunes de Andrade e Hélio Pires de Almeida.

- Aos colegas do Departamento de Matemática do Campus Universitário de Rondonópolis da UFMT, que possibilitaram minha permanência na FEEC - UNICAMP, para a realização deste trabalho.

- À minha esposa Fernanda e aos meus filhos Eduardo e Felipe.
- A Deus, por tudo.

Resumo

Neste trabalho, estudamos a classe dos códigos propelineares e a subclasse dos códigos propelineares invariantes por translação. Tratamos estes códigos como subgrupos do produto semi-direto de $\mathbb{Z}_m^n$ por $\mathbf{S}_n$ e do ponto de vista geométrico como códigos sobre grupos de isometrias de um dado alfabeto. Nesta direção, apresentamos resultados que relacionam estas classes de códigos com a classe dos códigos **G**-lineares e consequentemente com a classe dos códigos geometricamente uniformes. Apresentamos os códigos propelineares m-ários. Mostramos que não é possível obter códigos propelineares m-ários invariantes por translação sobre $\mathbb{Z}_m$ para $m \geq 3$. Em outras palavras não existem subgrupos do produto-semidireto de $\mathbb{Z}_m$ por $\mathbf{S}_n$ cuja ação sobre $\mathbb{Z}_m^n$ seja preservada pela distância de Hamming.

Abstract

In this dissertation we consider the class of propelinear codes as well as the subclass of translation invariant propelinear codes. From the algebraic point of view these classes of codes are shown to be subgroups of the semidirect product of $\mathbb{Z}_m^n$ by $\mathbf{S}_n$ whereas from the geometric point of view they are shown to be codes over isometry groups of a given alphabet. In this direction, we show how these classes of codes are related to the **G**-linear codes, and consequently to the class of geometrically uniform codes. We also present the m-ary propelinear codes. We show that it is not possible to obtain translation invariant m-ary propelinear codes over $\mathbb{Z}_m$, $m \geq 3$. Equivalently, there are no subgruops of the semidirect product of $\mathbb{Z}_m^n$ by $\mathbf{S}_m$ whose action on $\mathbb{Z}_m^n$ is preserved by the Hamming distance.

Lista de Símbolos

- $\mathbf{G} \times \mathbf{G}$: Produto cartesiano.
- $(\mathbf{G}, *)$: Grupo.
- x^{-1} : Elemento inverso
- $|\mathbf{G}|$: Ordem do grupo $\mathbf{G}$.
- $\mathbf{H} \leq \mathbf{G}$: $\mathbf{H}$ subgrupo do grupo $\mathbf{G}$.
- $\mathbf{S}_X$: Grupo smétrico sobre o conjunto X.
- $\mathbf{S}_n$: Grupo smétrico de gru n.
- $g * \mathbf{H}$: Classe lateral à esquerda de $\mathbf{H}$ em $\mathbf{G}$.
- $[\mathbf{H} : \mathbf{G}]$: Índice de $\mathbf{H}$ em $\mathbf{G}$.
- $\langle \mathbf{A} \rangle$: O menor subgrupo de $\mathbf{G}$ que contém $\mathbf{A}$.
- $\langle \mathbf{A} \rangle = \langle a \rangle$: Subgrupo cíclico gerado por a.
- $\mathbb{D}_n$: Grupo diedral.
- $\mathbb{QD}_8$: Grupo quasidiedral.

- $\mathbf{H} \lhd \mathbf{G}$: $\mathbf{H}$ subgrupo normal de $\mathbf{G}$.
- $\mathbb{Q}_8$: Grupo dos quatérnios.
- $\mathbf{H}/\mathbf{G}$: Grupo quociente.
- $\mathrm{Aut}\,(\mathbf{G})$: Grupo dos automorfismos do grupo $\mathbf{G}$.
- $(R, +\cdot)$: Anel.
- $(\mathbb{Z}_m, \oplus, \otimes)$: Anel dos inteiros módulo m.
- $(\mathcal{M}, +, \cdot)$ Módulo sobre R
- $\mathbb{Z}_m^n$: $\mathbb{Z}_m$-módulo livre.
- $\mathrm{Orb}_{\mathbf{G}}\,(x)$: Órbita de x em $\mathbf{G}$.
- $\mathrm{Stab}_{\mathbf{G}}\,(x)$: Estabilizador de x em $\mathbf{G}$.
- $\mathbf{G} = \mathbf{N} \rtimes \mathbf{H}$: $\mathbf{G}$ é produto semi-direto de $\mathbf{N}$ por $\mathbf{H}$.
- d_M : Métrica sobre o conjunto M
- d_{01} : Métrica zero-um.
- $\mathrm{Isom}\,(M)$: Grupo das isometrias.
- $\Gamma\,(S)$: Grupo das simetriais de um conjunto S.
- $\mathbb{R}^n$: Espaço vetorial real de dimensão n.
- $\langle \mathbf{x}, \mathbf{y} \rangle$: Produto interno de $\mathbf{x}$ por $\mathbf{y}$.
- $||\mathbf{x}||$: Norma de um vetor $\mathbf{x} \in \mathbb{R}^n$.
- $\mathbb{E}^n$: Espaço Euclidiano n-dimensional.
- d_E : Distância Euclidiana.

- $\mathbf{T}(\mathbb{E}^n)$: Translações de $\mathbb{E}^n$.
- $\mathbf{O}(\mathbb{E}^n) = \mathbf{O}(n, \mathbb{R})$: Matrizes ortogonais $n \times n$.
- $\mathrm{Isom}_o(\mathbb{E}^n)$: Grupo das isometrias de $\mathbb{E}^n$ que fixa a origem.
- d_H : Distância de Hamming.
- $\mathbf{C}$: Código sobre um alfabeto $\mathcal{A}$.
- $d_H(\mathbf{C})$: Distância mínima de Hamming.
- $\mathbb{F}_q = \mathbf{GF}(q)$: Corpo de Galois.
- $wt_H(\mathbf{x})$: Peso de Hamming de um vetor $x \in \mathbb{F}_q^n$.
- $\mathbf{G}(S)$: Grupo gerador de S.
- m-**PSK**: Conjunto de m sinais do tipo chaveamento por deslocamento de fase.
- ϕ_4 : Isomorfismo de $\mathbb{Z}_4$ em $\mathbb{F}_2$.
- ϕ_8 : Isomorfismo de $\mathbb{Q}_8$ em $\mathbf{C} = \langle a, b \rangle$.

Sumário

Lista de Tabelas

Capítulo 1

Introdução

1.1 Histórico

Em 1989 Rifá et al. [30], definiram códigos propelineares e apresentaram algumas de suas propriedades. A idéia geral, consiste em definir um mapeamento sobrejetivo do espaço de Hamming $(\mathbb{Z}_2^n, d_H)$ num grafo $\Delta(X, A)$, onde X é um conjunto de vértices e A um conjunto de arestas de modo que cada aresta seja um subconjunto de X com cardinalidade dois. A imagem inversa de cada vértice do grafo é um código. Em outras palavras, isso é chamado de recobrimento de um conjunto de pontos pelo espaço de Hamming. Ainda em [30], mostra-se que através desse procedimento obtem-se uma nova classe de códigos, a classe dos códigos propelineares.

Em 1994, Hammons et al.[19], introduziram os códigos $\mathbb{Z}_4$-lineares . A $\mathbb{Z}_4$-linearidade foi uma descoberta significativa para o desenvolvimento da teoria da codificação, pois possibilita tratar famílias bem conhecidas de códigos binários não-lineares, como códigos lineares sobre $\mathbb{Z}_4$. Dessa forma, a complexidade do processo de decodificação dos códigos não-lineares é bastante reduzida.

Em 1997, Rifá e Pujol [31] voltaram a falar sobre a classe dos códigos propelineares, desta vez com mais detalhes, mostrando algumas propriedades algébricas e combinatóriais. Apresentaram a subclasse dos códigos propelineares cujas palavras-

códigos são invariantes sob a métrica induzida pelo espaço métrico $(\mathbb{Z}_2^n, d_H)$. Esses códigos foram chamados de códigos propelineares invariantes por translação. Temos como exemplo importante destes códigos, os códigos $\mathbb{Z}_4$-lineares.

O conceito de códigos geometricamente uniformes, ou seja, códigos gerados por códigos de grupo sobre um grupo de isometrias Γ, foram introduzidos por Forney em [12]. Esses códigos generalizam os conjuntos de sinais tipo Slepian (código de Slepian) descritos em [40], onde o grupo de isometriais é dado pelo grupo das tranformações ortogonais. Em [23] Loeliger estabeleceu as condições para que um conjunto de sinais S esteja *casado* e *efetivamente casado* a um grupo $\mathbf{G}$. Também mostrou que o casamento efetivo de um grupo $\mathbf{G}$ a um conjunto S resulta da ação transitiva de $\mathbf{G}$ sobre S. Em particular, a ação transitiva de $\mathbf{G}$ sobre S é equivalente ao casamento de $\mathbf{G}$ a S, ou seja, isto corresponde a definição de códigos geometricamente uniformes. A uniformidade geométrica também generaliza outras classes importante de códigos, conhecidos como códigos do tipo Ungerboeck, ver por exemplo [43] e [13]. Entretanto, um dos fatos relevantes é que os códigos $\mathbb{Z}_4$-lineares também são geometricamente uniformes.

Em [17], foi apresentada a $\mathbf{G}$-linearidade como uma extensão da $\mathbb{Z}_4$-linearidade, onde $\mathbf{G}$ é um grupo finito qualquer. Essa técnica consiste em determinar um subgrupo do grupo de simetrias do espaço de sinais em questão, digamos um espaço métrico (M,d_M), tal que sua ação sobre o conjunto M seja *fortemente transitiva*. Em outras palavras, a busca incessante da uniformidade geométrica.

Por outro lado, é até retórico falar sobre a beleza da construção dos códigos $\mathbf{G}$-lineares, entretanto a obtenção efetiva destes códigos continua um problema a ser resolvido. Procuramos abrandar um pouco mais essa questão, buscando relações algébricas entre os códigos propelineares, propelineares invariantes por translação e os códigos $\mathbf{G}$-lineares. Para isso, exploramos sistematicamente o produto semi-direto de grupos, o qual é uma excelente ferramenta algébrica utilizada na construção de códigos.

1.2 Descrição do Trabalho

No Capítulo 2, fazemos uma revisão sobre alguns tópicos da teoria de grupos e da teoria da codificação, os quais julgamos necessários para o desenvolvimento deste trabalho.

No Capítulo 3, primeiro tratamos da propelinearidade, onde procuramos acrescentar alguns esclarecimentos à visão original. Definimos códigos $\mathbb{Z}_4$-lineares e **G**-lineares. Apresentamos algumas propriedades que relacionam essas classes de códigos, ou seja, estabelecemos resultados que fazem parte da contribuição deste trabalho, tais como a classificação dos códigos **G**-lineares binários como propelineares, classificação de uma subclasse dos códigos propelineares invariantes por translação binários como códigos **G**-lineares binários. Além disso, visto que estes códigos estão muito bem determinados como subgrupos de $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times \mathbb{Q}_8^{k_3}$, onde $\times$ denota o produto direto, temos consequentemente, uma técnica de construção de códigos **G**-lineares binários. Finalmente, através do subgrupo estabilizador, apresentamos um critério que permite afirmar se um código é **G**-linear binário.

No Capítulo 4, consideramos os espaços de Hamming $(\mathbb{Z}_m^n, d_H)$. Apresentamos os códigos propelineares m-ários, ou seja, vimos que é possível fazer o produto semi-direto $\mathbb{Z}_m^n$ por $\mathbf{S}_n$. Logo, podemos falar em subgrupos de $\mathbb{Z}_m^n \rtimes \mathbf{S}_n$, produto semi-direto de $\mathbb{Z}_m^n$ por $\mathbf{S}_n$. Em seguida, derivamos alguns resultados provenientes do caso binário. Observamos ainda, que geralmente o produto semi-direto é definido pela ação do grupo sobre um conjunto, dessa forma é possível induzir neste conjunto propriedades algébricas herdadas do grupo e relacioná-las com a métrica do conjunto. Desta maneira, vemos que a invariância da métrica depende desta ação. Isto posto, podemos especular sobre o que significa códigos propelineares m-ários serem invariantes por translação. Mostramos que dentro deste contexto de propelinearidade não existem subgrupos de $\mathbb{Z}_m^n \rtimes \mathbf{S}_n$ cuja ação sobre $\mathbb{Z}_m^n$ é deixe invariante a distância de Hamming. Mais precisamente, não existe códigos propelineares m-ários invariantes por translação.

No Capítulo 5, apresentamos as conclusões e contribuições deste trabalho, bem como

algumas sugestões para novos trabalhos.

Capítulo 2

Revisão dos Conceitos sobre Grupos e Códigos

Neste capítulo apresentaremos definições e resultados básicos da teoria dos grupos e dos códigos, necessários para o desenvolvimenteo deste trabalho.

Nas Seções 2.1, 2.2 e 2.3 apresentaremos uma simples introdução, relativa aos seguintes tópicos: grupos e módulos, ações de grupos e produtos de grupos, e grupos de isometrias (simetrias). Na Seção 2.4, faremos uma breve revisão sobre a teoria de códigos, bem como de alguns resultados apresentados em [12] e [23]. Os resultados relativos às seções anteriores, podem ser encontrados nas referências bibliográficas [8], [18], [3], [36], [33] e [45]

2.1 Grupos

Uma **operação binária** num conjunto não vazio $\mathbf{G}$ é uma função $\mu : \mathbf{G} \times \mathbf{G} \longrightarrow \mathbf{G}$ que a cada par ordenado (a, b) de elementos de $\mathbf{G}$ associa um elemento $\mu(a, b)$ de $\mathbf{G}$, chamado o *produto* de a e b, o qual indicamos por $a * b$ ou por justaposição ab.

Definição 2.1.1 *Um* ***grupo*** *consiste de um conjunto não vazio* $\mathbf{G}$ *munido de uma operação binária* $(*)$*, que satisfaz as seguintes propriedades:*

($G1$.) Associativa: $(a * b) * c = a * (b * c)$, $\forall a, b, c \in \mathbf{G}$;

($G2$.) Elemento neutro (ou identidade): Existe $e \in \mathbf{G}$ tal que $e * a = a * e$, $\forall a \in \mathbf{G}$;

($G3$.) Existência de inverso: Para todo $a \in \mathbf{G}$, existe $a' \in \mathbf{G}$ tal que $a * a' = a' * a = e$.

Em um grupo temos um único elemento identidade e um único inverso a', o qual indicamos por a^{-1}. Diremos que um grupo $(\mathbf{G},*)$ é **comutativo** ou **abeliano**, se a operação $*$ é comutativa, ou seja, $a * b = b * a$ para todo a e b em $\mathbf{G}$. Um grupo $(\mathbf{G},*)$ é **finito** se o número de elementos de $\mathbf{G}$ é finito. Também chamamos o número de elementos de um grupo $(\mathbf{G},*)$, de **cardinalidade** do grupo ou **ordem** do grupo e indicamos isto por $|\mathbf{G}|$.

Definição 2.1.2 *Sejam* $(\mathbf{G},*)$ *um grupo e* $\mathbf{H}$ *um subconjunto não vazio de* $\mathbf{G}$. *Diremos que* $\mathbf{H}$ *é um subgrupo de* $\mathbf{G}$, *se as seguintes condições são satisfeitas*:

(i) $\forall x, y \in \mathbf{H}$, então $x * y \in \mathbf{H}$;

(ii) $\forall x \in \mathbf{H}$, então $x^{-1} \in \mathbf{H}$.

Em outras palavras, $\mathbf{H}$ é um grupo com a operação herdada de $\mathbf{G}$. Usaremos a notação $\mathbf{H} \leq \mathbf{G}$, para indicar que $\mathbf{H}$ é um subgrupo de $\mathbf{G}$.

Exemplo 2.1.1 *Seja* X *um conjunto não vazio, uma* ***permutação*** *de* X *é uma bijeção de* X *em* X. *O conjunto das permutações de* X, *indicado por* $\mathbf{S}_X$, *é um grupo com a operação de composição de funções. Chamamos* $\mathbf{S}_X$ *de* ***grupo simétrico*** *sobre o conjunto* X. *Quando* $X = \{1, 2, ..., n\}$, *chamamos* $\mathbf{S}_X$ *de* ***grupo simétrico de grau*** n *e o indicamos por* $\mathbf{S}_n$. *Note que* $|\mathbf{S}_n| = n!$.

Definição 2.1.3 *Sejam* $(\mathbf{G},*)$ *um grupo,* $\mathbf{H} \leq \mathbf{G}$ *e* $g \in \mathbf{G}$. *O conjunto*

$$g * \mathbf{H} = \{g * h \mid h \in \mathbf{H}\}$$

é chamado de ***classe lateral*** *(à esquerda) de* $\mathbf{H}$ *em* $\mathbf{G}$. *Analogamente definimos uma classe lateral à direita de* $\mathbf{H}$ *em* $\mathbf{G}$.

Observação 2.1.1 *Seja* $\mathbf{H}$ *um subgrupo do grupo* $\mathbf{G}$. *Então:*

1. *Todo elemento de* $\mathbf{G}$ *pertence a alguma classe lateral de* $\mathbf{H}$ *em* $\mathbf{G}$;

2. *Duas classes laterais distintas não possuem elementos em comum;*

3. *Duas classes laterais quaisquer possuem a mesma cardinalidade:*

4. *Dois elementos* $x, y \in \mathbf{G}$ *estão na mesma classe lateral de* $\mathbf{H}$ *em* $\mathbf{G}$ *se, e somente se,* $x * y^{-1} \in \mathbf{H}$;

5. *O grupo* $(\mathbf{G},*)$ *é particionado numa união disjunta de classes laterais de* $\mathbf{H}$ *em* $\mathbf{G}$.

Quando $\mathbf{H}$ é um subgrupo do grupo $\mathbf{G}$, indicamos o conjunto das classes laterais de $\mathbf{H}$ em $\mathbf{G}$, por $\mathbf{G}/\mathbf{H}$. O número de classe laterais de $\mathbf{H}$ em $\mathbf{G}$ é chamado índice de $\mathbf{H}$ em $\mathbf{G}$, que indicamos por $[\mathbf{G} : \mathbf{H}]$, que pelo item 3.é bem definido.

Teorema 2.1.1 ***(Lagrange)*** *Se* $\mathbf{G}$ *é um grupo e* $\mathbf{H}$ *um subgrupo de* $\mathbf{G}$, *então*

$$|\mathbf{G}| = |\mathbf{H}| \ \ [\mathbf{G} : \mathbf{H}] .$$

Definição 2.1.4 *Se* A *é um subconjunto não vazio de um grupo* $\mathbf{G}$ *e*

$$\mathcal{F} = \{\mathbf{H} : \mathbf{H} \leq \mathbf{G} \ e \ A \subseteq \mathbf{H}\},$$

o ***subgrupo gerado por*** A, *que indicamos por* $\langle A \rangle$, *é dado por*

$$\langle A \rangle = \bigcap_{\mathbf{H} \in \mathcal{F}} \mathbf{H} .$$

Em outras palavras, $\langle A \rangle$ *é o menor subgrupo de* $\mathbf{G}$ *que contém* A. *Em particular, para* $A = \{a\}$ *diremos que* $\langle A \rangle = \langle a \rangle$ *é o* ***subgrupo cíclico gerado por*** a.

Definição 2.1.5 *Seja um grupo* $(\mathbf{G},*)$. *Se existir um* $g \in \mathbf{G}$ *tal que* $\mathbf{G} = \langle g \rangle$, *diremos que* $\mathbf{G}$ *é um grupo cíclico e que* g *é um gerador de* $\mathbf{G}$.

Exemplo 2.1.2 *Sejam $m \geq 2$ um inteiro e $\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}$. Consideremos $(\mathbb{Z}_m, \oplus)$, onde $\oplus$ é a operação binária definida do seguinte modo: dados $x, y \in \mathbb{Z}_m$, $x \oplus y$ é igual ao resto da divisão de $x + y$ por m, onde $+$ é a operação usual de adição. Esta operação $\oplus$ é chamada de* **adição módulo** *m. O conjunto $\mathbb{Z}_m$ com essa operação é um grupo cíclico.*

Exemplo 2.1.3 (Grupos Diedrais) *Consideremos $n \geq 3$ um inteiro positivo. O grupo*

$$\mathbb{D}_n = \left\langle r, s \mid r^n = s^2 = e\,,\; sr = r^{n-1}s \right\rangle,$$

onde $|\mathbb{D}_n| = 2n$, é chamado de grupo diedral de ordem $2n$. *Esse grupo é isomorfo ao grupo das simetrias no plano de um polígono regular com n-lados. Estas simetriais (ou isometrias) são: as n rotações em torno do centro através de $\frac{2k\pi}{n}$ radianos, $0 \leq k \leq n-1$ e as n reflexões (n par temos $\frac{n}{2}$ reflexões nas diagonais e $\frac{n}{2}$ reflexões através das retas que passam pelos pontos médios dos lados opostos; para n ímpar temos as n reflexões através da reta que passa por cada vértice e pelo ponto médio do seu lado oposto).*

Exemplo 2.1.4 (Quasidiedral) *O grupo*

$$\mathbb{QD}_8 = \left\langle x, y \mid x^8 = y^2 = e, xy = yx^3 \right\rangle,$$

é chamado grupo quasidiedral (*ou* semi-diedral) *de ordem* 16.

Proposição 2.1.1 *Seja $\mathbf{H}$ um subgrupo de $\mathbf{G}$. As seguintes afirmações são equivalentes:*

1. $g * \mathbf{H} = \mathbf{H} * g$, *para todo* $g \in \mathbf{G}$;
2. $g * \mathbf{H} * g^{-1} = \mathbf{H}$, *para todo* $g \in \mathbf{G}$;
3. $g * \mathbf{H} * g^{-1} \subset \mathbf{H}$, *para todo* $g \in \mathbf{G}$.

Definição 2.1.6 *Seja $\mathbf{H}$ um subgrupo de $\mathbf{G}$. Diremos que $\mathbf{H}$ é um* **subgrupo normal** *de $\mathbf{G}$, e indicamos por $\mathbf{H} \lhd \mathbf{G}$, se pelo menos uma das condições da Proposição 2.1.1 é satisfeita.*

Exemplo 2.1.5 (Quatérnio) *O grupo*

$$\mathbb{Q}_8 = \left\langle a, b \mid a^4 = e, b^2 = a^2, bab^{-1} = b^{-1} \right\rangle$$

dos ***quatérnios,*** *é um grupo não abeliano de ordem* 8, *cujos subgrupos são todos normais.*

Proposição 2.1.2 *Se* $\mathbf{H} \lhd \mathbf{G}$, *então o conjunto das classes laterais* $\mathbf{G}/\mathbf{H}$ *com a operação induzida de* $\mathbf{G}$ *é um grupo, chamado de* ***grupo quociente.***

Definição 2.1.7 *Sejam* $(\mathbf{G}, *)$ *e* $(\mathbf{H}, \diamond)$ *grupos e* $f : \mathbf{G} \longrightarrow \mathbf{H}$ *uma função. Diremos que* f *é um homomorfismo se*

$$f(a * b) = f(a) \diamond f(b) \ , \forall a, b \in \mathbf{G}.$$

Se, além disso, f *é uma bijeção, diremos que* f *é um isomorfismo e escrevemos* $\mathbf{G} \cong \mathbf{H}$. *Um isomorfismo de* $\mathbf{G}$ *em* $\mathbf{G}$ *é chamado de* ***automorfismo*** *de* $\mathbf{G}$.

Observação 2.1.2 *O conjunto dos automorfismos de um grupo* $\mathbf{G}$, *com a operação de composição de funções forma um grupo, o qual indicamos por* $\mathrm{Aut}(\mathbf{G})$.

Definição 2.1.8 *Considere um conjunto munido com duas operações binárias,* $(R, +, \cdot)$. *Diremos que* R *é um* ***anel comutativo com unidade*** *se as seguintes propriedade são satisfeitas:*

1. $(R, +)$ *é um grupo abeliano;*
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall x, y, z \in R$;
3. $x \cdot (y + z) = x \cdot y + x \cdot z$ *e* $(x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in R$;
4. $\mathbf{1} \cdot x = x, \forall x \in R$ ($\mathbf{1}$ *é o elemento identidade de* R);
5. $x \cdot y = y \cdot x, \forall x, y \in R$.

Definição 2.1.9 *Seja R um anel com unidade. Diremos que R é um anel* ***comutativo com unidade*** *se $(x \cdot y) = (y \cdot x)$ para todo $x, y \in R$.*

Exemplo 2.1.6 *$(\mathbb{Z}_m, \oplus, \otimes)$ o anel dos inteiros módulo m, onde a operação $\oplus$ é a soma módulo m e $\otimes$ é o produto módulo m, definido de modo semelhante à soma módulo m.*

Definição 2.1.10 *Seja K. um anel comutativo com unidade. Diremos que K é um* ***corpo*** *se para todo elemento não nulo $r \in K$ existe $r^{-1} \in K$ tal que $r \cdot r^{-1} = r^{-1} \cdot r = \mathbf{1}$.*

Seja $\mathcal{M}$ um conjunto não vazio e R um anel com unidade. Diremos que $(\mathcal{M}, +, \cdot)$ é um **módulo** sobre R (ou um R-**módulo**), se $(\mathcal{M}, +)$ é um grupo abeliano e se existir uma funçaõ $\mu : R \times \mathcal{M} \longrightarrow \mathcal{M}$ definida por $\mu(r, m) = rm$, chamada **multiplicação por escalar**, satisfazendo as condições: para quaisquer $r, r_1, r_2 \in R$ e $m, m_1, m_2 \in \mathcal{M}$,

M1. $r(m_1 + m_2) = rm_1 + rm_2$;

M2. $(r_1 + r_2)\, m = r_1 m + r_2 m$;

M3. $(r_1 r_2)\, m = r_1 (r_2 m)$;

M4. $\mathbf{1}m = m$.

Exemplo 2.1.7 *Todo anel R é um R-módulo. Em particular, o anel $\mathbb{Z}_m$ é um $\mathbb{Z}_m$-módulo.*

Exemplo 2.1.8 *Todo grupo abeliano é um $\mathbb{Z}$-módulo, onde $\mathbb{Z}$ é o anel dos inteiros.*

Um R-módulo é uma generalização de um espaço vetorial, onde os escalares pertencem a um anel, em vez de pertencerem a um corpo. Em outras palavras, se R é um corpo o R-módulo é um espaço vetorial sobre R. A idéia de um conjunto de geradores para um R-módulo também é uma generalização natural de um conjunto de geradores para um espaço vetorial. Assim, diremos que um R-módulo $\mathcal{M}$ é **finitamente gerado** se ele pode ser gerado por um conjunto finito $\mathcal{S} = \{\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_n\} \subset \mathcal{M}$, ou seja, todo

elemento $m \in \mathcal{M}$ pode ser escrito na forma $m = \sum r_i \mathbf{u}_i$, onde $r_i \in R$, e $i = 1, 2, ..., n$ .Nesse caso, escrevemos $\langle \mathcal{S} \rangle = \mathcal{M}$ para indicar que $\mathcal{M}$ é finitamente gerado

Uma **base** para um R-módulo $\mathcal{M}$ é um conjunto $\mathcal{S} = \{\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_n\} \subset \mathcal{M}$ tal que $\langle \mathcal{S} \rangle = \mathcal{M}$ e a representação $m = \sum r_i \mathbf{u}_i$ é única para cada $m \in \mathcal{M}$ Um módulo que possui uma base, é chamado de **módulo livre**.

Exemplo 2.1.9 *O anel $\mathbb{Z}_m$ é um $\mathbb{Z}$-módulo que não possui uma base. Com efeito, para todo $x \in \mathbb{Z}_m$ temos que $mx = 0$, quer dizer $B = \{x\}$ é linearmente dependente. Portanto, $\mathbb{Z}_m$ não é um $\mathbb{Z}$-módulo livre.*

Exemplo 2.1.10 *Sejam m, n inteiros positivos e*

$$\mathbb{Z}_m^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{Z}_m, i = 1, 2, \ldots, n\}.$$

Então o anel $\mathbb{Z}_m^n$ é um $\mathbb{Z}_m$-módulo livre e

$$\mathcal{B} = \{\mathbf{e}_1 = (1, 0, \ldots, 0), \mathbf{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \mathbf{e}_n = (0, 0, \ldots, 1)\}$$

*é uma base de $\mathbb{Z}_m^n$. Geralmente, chamamos essa base de **base canônica**.*

2.2 Ações e Produtos de Grupos

Definição 2.2.1 *Sejam $(\mathbf{G}, *)$ um grupo e X um conjunto não vazio. Uma **ação** de $\mathbf{G}$ sobre o conjunto X é uma função $\psi : \mathbf{G} \times X \longrightarrow X$ satisfazendo as seguintes propriedades:*

1. *$\psi(a, \psi(b, x)) = \psi(a * b, x)$, para todos $a, b \in \mathbf{G}$ e $x \in X$;*
2. *$\psi(e, x) = x$, para todo $x \in X$.*

Para simplificar a notação, escrevemos $\psi(a, x) = a \cdot x$ e $a * b = ab$. Chamamos essa ação, de ação à esquerda de $\mathbf{G}$ em X. De modo análogo, definimos ação à direita de $\mathbf{G}$ em X. Com essa notação podemos escrever $a \cdot (b \cdot x) = (ab) \cdot x$, $e \cdot x = x$.

Exemplo 2.2.1 *Sejam* $\mathbf{G} = (\mathbb{Z}, +)$ *e* $X = \mathbb{R}$. *Então a função* $\cdot : \mathbf{G} \times X \longrightarrow X$ *dada por* $a \cdot x = x + a$ *é uma ação de* $\mathbf{G}$ *em* X. *Também a função* $\cdot : \mathbf{G} \times X \longrightarrow X$ *dada por* $a \cdot x = (-1)^a x$ *é uma ação de* $\mathbf{G}$ *em* X.

Proposição 2.2.1 *Seja* $\mathbf{G}$ *um grupo que atua sobre um conjunto* X. *Para cada* $g \in \mathbf{G}$ *a função* $\sigma_g : X \longrightarrow X$ *definida por* $\sigma_g(x) = g \cdot x$ *é uma permutação de* X. *Além disso, a função* $\Phi : \mathbf{G} \longrightarrow \mathbf{S}_X$ *definida por* $\Phi(g) = \sigma_g$ *é um homomorfismo com a propriedade de que* $\Phi(g)(x) = g \cdot x$.

Desse modo, segue-se que existe uma correspondência biunívoca entre ações de um grupo sobre um conjunto X e os homomorfismos de $\mathbf{G}$ em $\mathbf{S}_X$. Quer dizer, temos essencialmente a mesma noção expressa em diferentes terminologias. Em particular, quando $|X| = n$ denotaremos $\mathbf{S}_X$ por $\mathbf{S}_n$.

Definição 2.2.2 *Seja* $\mathbf{G}$ *um grupo atuando sobre um conjunto* X *e* $x \in X$. *Chamamos de* ***órbita*** *de* x *em* $\mathbf{G}$, *ao subconjunto de* X, *indicado por*

$$\text{Orb}_{\mathbf{G}}(x) = \{ g \cdot x : g \in \mathbf{G} \}.$$

Dados $x, y \in X$, diremos que x está relacionado com y, quando: $y = g \cdot x$ para algum $g \in \mathbf{G}$, isto define uma relação de equivalência em X, cujas classes de equivalência são as órbitas. Assim, as órbitas de X formam uma partição de X, isto é,

1. $X = \bigcup_{x \in X} \text{Orb}_{\mathbf{G}}(x)$;

2. Se $x, y \in X$, então $\text{Orb}_{\mathbf{G}}(x) \cap \text{Orb}_{\mathbf{G}}(y) = \emptyset$ ou $\text{Orb}_{\mathbf{G}}(x) = \text{Orb}_{\mathbf{G}}(y)$.

Definição 2.2.3 *Seja* $\mathbf{G}$ *é um grupo atuando sobre um conjunto* X *e* $x \in X$. *Chamaremos de* ***estabilizador*** *de* x *em* $\mathbf{G}$ *ao subgrupo de* $\mathbf{G}$, *indicado por*

$$\text{Stab}_{\mathbf{G}}(x) = \{ g \in \mathbf{G} : g \cdot x = x \}.$$

Teorema 2.2.1 *Se* $\mathbf{G}$ *é um grupo atuando sobre um conjunto* X, *então*

$$|\text{Orb}_{\mathbf{G}}(x)| = [\mathbf{G} : \text{Stab}_{\mathbf{G}}(x)].$$

Definição 2.2.4 *A ação de um grupo* $\mathbf{G}$ *sobre um conjunto* X *é* ***transitiva****, se para todos* $x, y \in X$ *existir* $g \in \mathbf{G}$ *tal que* $y = g \cdot x$*, ou seja,* $\mathrm{Orb}_{\mathbf{G}}(x) = X$, $\forall x \in X$*. Diremos que a ação de* $\mathbf{G}$ *sobre* X *é* ***fortemente transitiva****, se para todos* $x, y \in X$ *existir um único* $g \in \mathbf{G}$ *tal que* $y = g \cdot x$ *(nesse caso* $|\mathbf{G}| = |X|$ *).*

Agora faremos uma revisão do *produto semi-direto* de grupos. Esta técnica nos permite construir um grupo $\mathbf{G}$ a partir dos grupos $\mathbf{N}$ e $\mathbf{H}$, de modo que $\mathbf{G}$ contenha subgrupos isomorfos a $\mathbf{N}$ e $\mathbf{H}$ tais que $|\mathbf{G}| = |\mathbf{N}|\,|\mathbf{H}|$.

Definição 2.2.5 *Se* $\mathbf{N}$ *e* $\mathbf{H}$ *são subgrupos de um grupo* $\mathbf{G}$ *tais que*

$$\mathbf{N} \lhd \mathbf{G},\ \mathbf{N} \cap \mathbf{H} = \{e\} \ \ e \ \ \mathbf{G} = \mathbf{N}\mathbf{H}$$

então diremos que $\mathbf{G}$ *é o* ***produto semi-direto*** *de* $\mathbf{N}$ *por* $\mathbf{H}$*, que indicamos por* $\mathbf{G} = \mathbf{N} \rtimes \mathbf{H}$.

Exemplo 2.2.2 *O grupo* $\mathbb{D}_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$*. De fato:*

1. $\mathbb{Z}_n \cong \langle r \rangle \lhd \mathbb{D}_n$, $\mathbb{Z}_2 \cong \langle s \rangle$
2. $\langle r \rangle \cap \langle s \rangle = \{e\}$
3. $\mathbb{D}_n = \langle r \rangle \langle s \rangle$.

Proposição 2.2.2 *Seja* $\mathbf{G}$ *o produto semi-direto de* $\mathbf{N}$ *por* $\mathbf{H}$*. Para cada* $h \in \mathbf{H}$ *a aplicação* $\varphi_h : \mathbf{N} \longrightarrow \mathbf{N}$ *definida por* $\varphi_h(n) = hnh^{-1}$ *é um automorfismo de* $\mathbf{N}$*. A aplicação* $\varphi : \mathbf{H} \longrightarrow \mathrm{Aut}(\mathbf{N})$ *definida por* $\varphi(h) = \varphi_h$ *é um homomorfismo.*

Nesse caso, visto que $\mathbf{N} \lhd \mathbf{G}$, podemos falar na ação de $\mathbf{H}$ sobre $\mathbf{N}$ por conjugação, ou seja, $h \cdot n = hnh^{-1}$. Além disso, $\mathrm{Aut}(\mathbf{N})$ é um subgrupo de $\mathbf{S}_{\mathbf{N}}$, logo essa ação pode ser vista como o homomorfismo $\varphi : \mathbf{H} \longrightarrow \mathrm{Aut}(\mathbf{N})$.

Proposição 2.2.3 *Consideremos dois grupos quaisquer* $\mathbf{N}$, $\mathbf{H}$ *e* $\varphi : \mathbf{H} \longrightarrow \mathrm{Aut}(\mathbf{N})$ *um homomorfismo tal que* $\varphi(h) = \varphi_h$*. Seja o conjunto*

$$\mathbf{G} = \{(n, h) : n \in \mathbf{N}, h \in \mathbf{H}\}$$

de pares ordenados. Então, $\mathbf{G}$ *é um grupo com a operação*

$$(n_1, h_1)(n_2, h_2) = \left(n_1 \varphi_{h_1}(n_2), h_1 h_2\right).$$

Os conjuntos $\mathbf{N}_0 = \{(n, e_{\mathbf{H}}) : n \in \mathbf{N}, e_{\mathbf{H}} \in \mathbf{H}\}$ *e* $\mathbf{H}_0 = \{(e_{\mathbf{N}}, h) : e_{\mathbf{N}} \in \mathbf{N}, h \in \mathbf{H}\}$, *são subgrupos de* $\mathbf{G}$ *tais que* $\mathbf{N}_0 \cong \mathbf{N}$, $\mathbf{H}_0 \cong \mathbf{H}$ *e* $\mathbf{G}$ *é o produto semi-direto de* $\mathbf{N}_0$ *por* $\mathbf{H}_0$.

Exemplo 2.2.3 *Construção do produto semi-direto* $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_2 \cong \mathbb{D}_4$. *Consideremos o homomorfismo* $\varphi : \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_2^2)$ *definido por* $\varphi(0) = Id_{\mathbb{Z}_2^2} \in \mathrm{Aut}(\mathbb{Z}_2^2)$ *e* $\varphi(1) \in \mathrm{Aut}(\mathbb{Z}_2^2)$ *dado por:*

$$\begin{aligned} \varphi(1)(00) &= 00 \\ \varphi(1)(01) &= 10 \\ \varphi(1)(10) &= 01 \\ \varphi(1)(11) &= 11. \end{aligned}$$

Note que $a = (10, 1)$ *e* $b = (00, 1)$ *satisfaz* $a^4 = b^2 = (00, 0)$ *e* $ba = a^3 b = (01, 0)$. *Assim, identificando* r *com* a *e* s *com* b, *temos que* $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_2 \cong \mathbb{D}_4$.

2.3 Isometrias

Uma **métrica** sobre um conjunto M é uma função $d_M : M \times M \longrightarrow \mathbb{R}$, tal que o número real $d_M(x, y)$ chamado de **distância** de x a y, satisfaça as seguintes condições para quaisquer $x, y, z \in M$:

d_1. $d_M(x, x) = 0$;

d_2. Se $x \neq y$, então $d_M(x, y) > 0$;

d_3. $d_M(x, y) = d_M(y, x)$;

d_4. $d_M(x, z) \leq d_M(x, y) + d_M(y, z)$.

Definição 2.3.1 *Um espaço métrico é um par* $(\mathrm{M}, d_{\mathrm{M}})$, *onde* M *é um conjunto e* d_{M} *é um métrica sobre* M.

Exemplo 2.3.1 *O par* $(\mathbb{R}, d)$ *é um espaço métrico, onde* $\mathbb{R}$ *é o conjunto dos números reais e* $d : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ *dada por* $d(x, y) = |x - y|$ *é uma métrica.*

Exemplo 2.3.2 *O par* (M, d_{01}) *é um espaço métrico, onde* M *é um conjunto qualquer e* $d_{01} : \mathrm{M} \times \mathrm{M} \longrightarrow \mathbb{R}$ *definida por*

$$d_{01} = \begin{cases} 1 & se\ x \neq y \\ 0 & se\ x = y, \end{cases}$$

para todos $x, y \in$M *é um métrica sobre* M. *Essa métrica é chamada de* ***métrica zero-um*** *(ou* ***distância de Hamming*** d_H*).*

Definição 2.3.2 *Sejam* $(\mathrm{M}, d_{\mathrm{M}})$ *e* $(\mathrm{N}, d_{\mathrm{N}})$ *espaços métricos. Uma* ***isometria*** *é uma bijeção* $\phi : \mathrm{M} \longrightarrow \mathrm{N}$ *tal que*

$$d_{\mathrm{M}}(x, y) = d_{\mathrm{N}}(\phi(x), \phi(y)),$$

para todos $x, y \in \mathrm{M}$.

Exemplo 2.3.3 *O conjunto das isometrias de um espaço métrico* $(\mathrm{M}, d_{\mathrm{M}})$, *que indicamos por* $\mathrm{Isom}(\mathrm{M})$, *forma um grupo com a operação de composição. Mais precisamente,* $\mathrm{Isom}(\mathrm{M}) \leq \mathbf{S}_{\mathrm{M}}$.

Definição 2.3.3 *Seja* S *um subconjunto do espaço métrico* M. *As isometrias* ϕ *que deixam* S *invariante, isto é,* $\phi(\mathrm{S}) = \mathrm{S}$, *formam um grupo que é chamado* ***grupo das simetrias*** *de* S, *indicado por* $\Gamma(\mathrm{S})$.

Teorema 2.3.1 *[17] O grupo de simetrias* $\Gamma(\mathbb{Z}_2^n)$ *do espaço de Hamming n-dimensional* $(\mathbb{Z}_2^n, d_H)$ *é dado por* $\Gamma(\mathbb{Z}_2^n) = \mathbb{Z}_2^n \rtimes \mathbf{S}_n$.

Vamos indicar por $\mathbb{R}^n$ o espaço vetorial real de dimensão n. Um ponto em $\mathbb{R}^n$ é uma n-upla $(x_1, x_2, ..., x_n)$ de números reais. Para falar de geometria, precisamos equipar esse espaço com as noções de comprimento e ângulo. Podemos fazer isso de modo eficiente usando a noção de produto interno entre dois vetores $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

Se $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, definimos o **produto interno** como sendo o número real

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i.$$

Agora, podemos definir o **comprimento** (ou **norma**) de um vetor $\mathbf{x} \in \mathbb{R}^n$ por

$$||\mathbf{x}|| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2},$$

o **ângulo** entre dois vetores não nulos $\mathbf{x}$ e $\mathbf{x}$ por

$$\theta = \arccos\left(\frac{\langle \mathbf{x}, \mathbf{y} \rangle}{||\mathbf{x}||\ ||\mathbf{y}||}\right)$$

e a **distância** entre x e y por

$$d_E(\mathbf{x}, \mathbf{y}) = ||\mathbf{x} - \mathbf{y}||\ .$$

Definição 2.3.4 *O espaço $\mathbb{R}^n$ munido desse produto interno é usualmente chamado de* ***espaço Euclidiano n-dimensional****, que indicamos por $\mathbb{E}^n$.*

Observação 2.3.1 *Observamos que as isometrias $\sigma \in \mathrm{Isom}(\mathbb{E}^n)$ são funções que preservam distância, visto que σ é necessariamente bijetiva. O grupo $(\mathrm{Isom}(\mathbb{E}^n), \circ)$ é chamado* ***grupo Euclidiano****.*

Seja v um vetor em $\mathbb{E}^n$ e

$$\mathbf{T}(\mathbb{E}^n) = \{t_{\mathbf{v}} : \mathbb{E}^n \longrightarrow \mathbb{E}^n : t_{\mathbf{v}}(\mathbf{x}) = \mathbf{x} + \mathbf{v}, \forall \mathbf{x} \in \mathbb{E}^n\}$$

o conjunto das **translações** de $\mathbb{E}^n$. O conjunto $\mathbf{T}(\mathbb{E}^n)$ é um subgrupo de $\mathrm{Isom}(\mathbb{E}^n)$. O conjunto $\mathbf{O}(\mathbb{E}^n) = \mathbf{O}(n, \mathbb{R})$ das matrizes $n \times n$ ortogonais reais, ou seja, das transformações lineares de $\mathbb{E}^n$ que preservam produto interno, também é um subgrupo de $\mathrm{Isom}(\mathbb{E}^n)$, chamado de **grupo ortogonal**.

Proposição 2.3.1 *[18] O grupo* $\mathrm{Isom_0}(\mathbb{E}^n) = \{\sigma \in \mathrm{Isom}(\mathbb{E}^n) \mid \sigma(\mathbf{0}) = \mathbf{0}\}$, *das isometrias de* $\mathbb{E}^n$ *que fixa a origem é isomorfo a* $\mathbf{O}(\mathbb{E}^n)$.

Teorema 2.3.2 *[18] Toda isometria* $\sigma \in \mathrm{Isom}(\mathbb{E}^n)$ *pode ser escrita de modo único como* $\sigma = t_{\mathbf{v}} \circ \phi$, *onde* $t_{\mathbf{v}} \in \mathbf{T}(\mathbb{E}^n)$ *e* $\phi \in \mathbf{O}(\mathbb{E}^n)$.

Observação 2.3.2 *Seja*

$$\mathbf{G} = \{(\mathbf{v}, \phi) : \phi \in \mathbf{O}(\mathbb{E}^n) \ \ e \ \mathbf{v} \in \mathbb{E}^n\}.$$

Então $\mathbf{G}$ *munido com a operação binária*

$$(\mathbf{v}, \phi)(\mathbf{v}', \phi') = (\mathbf{v} + \phi(\mathbf{v}'), \phi \circ \phi')$$

é um grupo isomorfo a $\mathrm{Isom}(\mathbb{E}^n)$, *com elemento identidade* $(\mathbf{0}, id)$ *e elemento inverso* $(\mathbf{v}, \phi)^{-1} = \left(-\phi^{-1}(\mathbf{v}), \phi^{-1}\right)$. *Além disso,*

$$\mathbf{N} = \{(\mathbf{v}, id) : \mathbf{v} \in \mathbb{E}^n\}$$

é um subgrupo normal de $\mathbf{G}$ *e*

$$\mathbf{H} = \{(\mathbf{0}, \phi) : \phi \in \mathbf{O}(\mathbb{E}^n)\}$$

é um subgrupo de $\mathbf{G}$. *Portanto, pela Proposição 2.2.3,* $\mathbf{G} = \mathbf{N} \rtimes \mathbf{H}$, *onde* $\varphi : \mathbf{H} \longrightarrow \mathrm{Aut}(\mathbf{N})$ *é a inclusão natural. Como* $\mathbf{N} \cong \mathbf{T}(\mathbb{E}^n)$ *e* $\mathbf{H} \cong \mathbf{O}(\mathbb{E}^n)$, *temos que* $\mathrm{Isom}(\mathbb{E}^n) = \mathbf{T}(\mathbb{E}^n) \rtimes \mathbf{O}(\mathbb{E}^n) \cong \mathbb{R}^n \rtimes \mathbf{O}(\mathbb{E}^n)$. *Portanto, temos uma classe importante de exemplos de grupos de simetrias que podem ser classificados através de produtos semi-diretos.*

2.4 Códigos

Consideremos um espaço métrico $(\mathcal{A}, d_{\mathcal{A}})$ e $I \subseteq \mathbb{Z}$ um subconjunto de índices. Chamamos de **espaço de sequências** $\mathcal{A}^I$ sobre o alfabeto $\mathcal{A}$, ao conjunto de todas

as sequências $\mathbf{a} = (a_i)_{i \in I}$ tal que cada $a_i \in \mathcal{A}$. Quando $I = \{i : 1 \leq i \leq n\}$, indicamos $\mathcal{A}^{\mathrm{I}}$ por $\mathcal{A}^n$. A **cardinalidade** do alfabeto $\mathcal{A}$, será indicada por $|\mathcal{A}|$.

Um **código C** sobre o alfabeto $\mathcal{A}$ é qualquer subconjunto não vazio de $\mathcal{A}^I$. Um **código de bloco C** de comprimento n sobre o alfabeto $\mathcal{A}$ é qualquer subconjunto não vazio de $\mathcal{A}^n$. Chamamos cada n-upla $\mathbf{a} = (a_i)_{i=1}^n$ de **palavra-código**. A **dimensão** de um código $\mathbf{C}$ é o número $k = \log_{|\mathcal{A}|} |\mathbf{C}|$. Um código de bloco $\mathbf{C}$ de comprimento n e dimensão k é chamado de um $[n, k]$-código e sua **taxa** é definida por $r = \frac{k}{n}$ símbolos por bloco. Quando k for inteiro diremos que a palavra-código contém k dígitos de informação. Se $I = \{i : 1 \leq i \leq n\}$, diremos que a palavra código contém $(n - k)$ dígitos de redundância.

A **distância de Hamming** entre $\mathbf{x} = (x_1, x_2, \ldots, x_n), \mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathcal{A}^n$ é definida por

$$d_H(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} d_{01}(x_i, y_i).$$

Em outras palavras, o número de componentes em que $\mathbf{x}$ e $\mathbf{y}$ diferem. A **distância mínima de Hamming** de um código $\mathbf{C}$ tal que $|\mathbf{C}| \geq 2$, é definida por

$$d_H(\mathbf{C}) = \min\{d_H(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathbf{C}, \mathbf{x} \neq \mathbf{y}\}.$$

Um código de bloco $\mathbf{C}$ de comprimento n, dimensão k e distância mínima $d = d_H(\mathbf{C})$, é chamado de um $[n, k, d]$-código. Note que $1 \leq d_H(\mathbf{C}) \leq n$.

Sabemos que o interessante é obter códigos sobre espaços métricos que possuam estruturas algébricas bem definidas tais como: grupos, anéis ou corpos. A seguir, daremos algumas definições relacionadas com essas estruturas.

Quando o alfabeto $\mathcal{A}$ é um grupo finito, dizemos que o código de bloco $\mathbf{C}$ de comprimento n é um **código de grupo** sobre o grupo $\mathcal{A}$ se $\mathbf{C}$ for um subgrupo de $\mathcal{A}^I$. Quando $\mathcal{A}$ é um anel comutativo com unidade, um código $\mathbf{C}$ de comprimento n sobre $\mathcal{A}$ é linear, se $\mathbf{C}$ for um submódulo do $\mathcal{A}$-módulo livre $\mathcal{A}^n$. Sendo o alfabeto $\mathcal{A}$ o corpo de Galois $\mathbb{F}_q = \mathbf{GF}(q)$ com $q = p^s$ uma potência do número primo p, um código

$\mathbf{C}$ sobre $\mathbb{F}_q$ é linear se $\mathbf{C}$ for subespaço do espaço vetorial de $\mathbb{F}_q^n$. O **peso de Hamming** de um vetor $\mathbf{x} \in \mathbb{F}_q^n$, indicado por $\mathbf{w}t_H(\mathbf{x})$, é o número de componentes não nulas de $\mathbf{x}$.

2.4.1 Conjuntos Geometricamente Uniformes

O motivo do nosso interesse em códigos sobre grupos de isometrias do espaço euclidiano $\mathbb{E}^n$, vem do estudo de conjuntos de sinais geometricamente uniformes, apresentados por Forney em [12] e de modo semelhante por Loeliger em [23]. Estes resultados podem ser aplicados a qualquer espaço de dimensão finita ou infinita tais que tenham grupos de isometriais bem definidos.

Definição 2.4.1 *[12] Um conjunto de sinais $\mathcal{S} \subset \mathbb{E}^n$ é* geometricamente uniforme (*ou $\mathcal{S}$ é um código geometricamente uniforme*), *se a ação de seu grupo de simetrias $\Gamma(\mathcal{S})$ sobre $\mathcal{S}$ é transitiva.*

A ordem de $\Gamma(\mathcal{S})$ pode ser maior que a cardinalidade do conjunto $\mathcal{S}$, ou seja, o grupo $\Gamma(\mathcal{S})$ é maior do que o necessário para gerar $\mathcal{S}$. Assim, o interessante será obter um subgrupo $\mathbf{G}(\mathcal{S})$ de $\Gamma(\mathcal{S})$ de ordem mínima, porém com a mesma cardinalidade de $\mathcal{S}$, tal que sua ação sobre $\mathcal{S}$ seja *fortemente transitiva.* O grupo $\mathbf{G}(\mathcal{S})$, normalmente é chamado de **grupo gerador** de $\mathcal{S}$. Quando $\mathcal{S}$ for geometricamente uniforme e possuir um grupo gerador $\mathbf{G}(\mathcal{S})$, ou seja, $Orb_{\mathbf{G}(\mathcal{S})}(s_0) = \mathcal{S}$ para todo $s_0 \in \mathcal{S}$, então o mapeamento $\eta : \mathbf{G}(\mathcal{S}) \longrightarrow \mathcal{S}$ definido por $\eta(\sigma) = \sigma(s_0)$ é bijetivo e preserva a estrutura do grupo $\mathbf{G}(\mathcal{S})$ em $\mathcal{S}$. Em outras palavras, para todo $\sigma_1, \sigma_2 \in \mathbf{G}(\mathcal{S})$, segue que $\eta(\sigma_1\sigma_2) = (\sigma_1\sigma_2)(s_0) = \sigma_1(\eta(\sigma_2))$. Veremos na próxima subseção, que isto significa casamento de um grupo a um conjunto de sinais.

Exemplo 2.4.1 *O espaço de Hamming $\mathbb{Z}_2^2$ é um conjunto de sinais geometricamente uniforme. Seu grupo de simetrias é dado por $\Gamma(\mathbb{Z}_2^2) = \mathbb{Z}_2^2 \times \mathbb{Z}_2 \cong \mathbb{D}_4$, o grupo das simetrias do quadrado. Em $\Gamma(\mathbb{Z}_2^2)$ existem dois grupos de ordem quatro $\{e, r, r^2, r^3\} \cong \mathbb{Z}_4$ e $\{e, r^2, rs, r^3s\} \cong \mathbb{Z}_2^2$ tais que suas ações em $\mathbb{Z}_2^2$ são fortemente transitivas.*

$$\{e, r, r^2, r^3\} \cong \mathbb{Z}_4 \ \ e \ \ \{e, r^2, rs, r^3s\} \cong \mathbb{Z}_2^2.$$

Exemplo 2.4.2 *O conjunto de sinais m-**PSK** é geometricamente uniforme. Seu grupo de simetrias é o grupo diedral*

$$\mathbb{D}_m = \left\langle r, s \mid r^m = s^2 = e\,,\ sr = r^{m-1}s \right\rangle$$

e um grupo gerador é o grupo das rotações $\langle r \rangle \cong \mathbb{Z}_m$.

Exemplo 2.4.3 *Um conjunto de sinais pode não ter um grupo gerador. Em Slepian [41], foi representado matricialmente o* $\mathbf{S}_5$, *para construir um conjunto de sinais geometricamente uniforme* $\mathcal{S}$ *com* 10 *pontos em* $\mathbb{R}^5$, *cujo grupo de simetrias não contém subgrupos cuja ação sobre* $\mathcal{S}$ *seja* fortemente transitiva.

Teorema 2.4.1 *[12] O produto cartesiano de conjuntos de sinais geometricamente uniformes é um conjunto de sinais geometricamente uniforme.*

2.4.2 Conjuntos de Sinais Casados a Grupos

Em [23], foi definido o conceito de conjunto de sinais casados a grupos. A idéia básica é a de introduzir alguma linearidade no conjunto de sinais, linearidade esta induzida por um rotulamento isométrico, obtido de um grupo de rótulos isomorfo ao grupo gerador mínimo. Usando a terminologia de Loeliger, temos os seguintes resultados:

Definição 2.4.2 *[23] Um conjunto de sinais finito* $\mathcal{S} \subset \mathbb{E}^n$ *está casado a um grupo* $\mathbf{G}$, *se existir um mapeamento* $\mu : \mathbf{G} \longrightarrow \mathcal{S}$ *sobrejetor tal que para todo* $g, h \in \mathbf{G}$

$$d_E\left(\mu\left(g\right), \mu\left(h\right)\right) = d_E\left(\mu\left(g^{-1}h\right), \mu\left(e\right)\right)\ ,$$

onde o elemento identidade de $\mathbf{G}$ *é indicado por* e *e* $\mu(e) = s_e$. *O mapeamento* μ *é chamado de **mapeamento casado**. Quando* μ *for injetivo, dizemos que* μ *é um **rotulamento casado**. Se* $\mathbf{G}$ *é isomorfo a um grupo gerador* $\mathbf{G}(\mathcal{S}) \subset \mathrm{Isom}(\mathcal{S})$, *então* μ *é um rotulamento isométrico.*

Exemplo 2.4.4 *O conjunto de sinais m-**PSK** é um subconjunto de* $\mathbb{E}^n$ *que está casado ao grupo* $(\mathbb{Z}_m, \oplus)$. *Para isso, basta considerar*

$$\mu : \mathbb{Z}_m \longrightarrow \mathbb{E}^n, \mu(k) = \left(r\cos\left(\frac{2k\pi}{m}\right), r\,\mathrm{sen}\left(\frac{2k\pi}{m}\right)\right) = re^{\frac{i2k\pi}{m}}.$$

Portanto,

$$\begin{aligned} d_E(\mu(a), \mu(b)) &= \left|\left|e^{\frac{i2a\pi}{m}}\right|\right| \left|\left|r - re^{\frac{i2(b-a)\pi}{m}}\right|\right| \\ &= \left|\left|re^{\frac{i2(b-a)\pi}{m}} - r\right|\right| \\ &= d_E(\mu(b-a), \mu(b)). \end{aligned}$$

Como μ é bijetiva, temos um rotulamento casado.

Teorema 2.4.2 *Se o conjunto $\mathcal{S} \subset \mathbb{E}^n$ é um conjunto de sinais casado a um grupo $\mathbf{G}$ e $f \in \mathrm{Isom}(\mathbb{E}^n)$, então $f(\mathcal{S})$ também está casado a $\mathbf{G}$.*

Consideremos um mapeamento casado $\mu : \mathbf{G} \longrightarrow \mathcal{S}$ e n um inteiro positivo. Quando falamos em mapeamento estendido (ou numa extensão do mapeamento μ), estamos nos referindo ao mapeamento $\mu^n : \mathbf{G}^n \longrightarrow \mathcal{S}^n$ o qual é definido componente a componente, ou seja, $\mu^n(g_1, g_2, ..., g_n) = (\mu(g_1), \mu(g_2), ..., \mu(g_n))$.

Teorema 2.4.3 *Sejam $\mu : \mathbf{G} \longrightarrow \mathcal{S}$ um mapeamento casado e $\mathbf{C}$ um código linear sobre $\mathbf{G}$ (um código de grupo sobre $\mathbf{G}$). Então, $\mu^n : \mathbf{C} \longrightarrow \mu^n(\mathbf{C})$ é um mapeamento casado.*

Isto siginifica que podemos construir conjuntos de sinais geometricamente uniformes (códigos geometricamente uniformes) $\mu^n(\mathbf{C})$. Isto pode ficar mais interessante quando o grupo $\mathbf{G}$ for isomorfo, por exemplo, a $\mathbb{Z}_m$.

Lema 2.4.1 *Seja $\mu : \mathbf{G} \longrightarrow \mathcal{S}$ um mapeamento casado. Se $\mu(e) = s_e$ e $\mathbf{H} = \mu^{-1}(s_e)$. Então $\mathbf{H} \leq \mathbf{G}$ e*

$$\mu(g) = \mu(g') \Longleftrightarrow g\mathbf{H} = g'\mathbf{H},$$

ou seja, g e g' estão na mesma classe lateral à esquerda de $\mathbf{H}$ em $\mathbf{G}$.

Definição 2.4.3 *Um mapeamento casado* $\mu : \mathbf{G} \rightarrow \mathcal{S}$ *tal que* $\mathbf{H} = \mu^{-1}(s_e)$ *e*

$$\bigcap_{g \in \mathbf{G}} g\mathbf{H}g^{-1} = \{e\}$$

é chamado de ***mapeamento efetivamente casado****. Também dizemos que* $\mathcal{S}$ *está* ***efetivamente casado*** *a* $\mathbf{G}$*.*

Teorema 2.4.4 *Se* Θ *é um grupo transitivo de isometrias de um conjunto de sinais* $\mathcal{S}$ $(\Theta \leq \Gamma(\mathcal{S}))$*, então* $\mathcal{S}$ *é casado a* Θ *e para todo* $s \in \mathcal{S}$ *o mapeamento* $\mu_s : \Theta \longrightarrow \mathcal{S}$ *definido por* $\mu_s(f) = f(s)$ *é um mapeamento casado. Reciprocamente, se o conjunto de sinais* $\mathcal{S}$ *está casado a um grupo* $\mathbf{G}$*, então existe um homomorfismo de* $\mathbf{G}$ *sobre um subgrupo transitivo de* $\Gamma(\mathcal{S})$*.*

Corolário 2.4.1 *Se um conjunto de sinais* $\mathcal{S}$ *está efetivamente casado a um grupo* $\mathbf{G}$*, então* $\mathbf{G}$ *é isomorfo a um subgrupo transitivo de* $\Gamma(\mathcal{S})$*.*

Capítulo 3

Códigos Propelineares e G-Lineares

O objetivo deste capítulo é apresentar os códigos propelineares e **G**-lineares, bem como algumas propriedades que relacionam esses dois conceitos.

Na Seção 3.1 apresentaremos os principais resultados sobre códigos propelineares e códigos propelineares invariantes por translação, introduzidos em Rifà [31], refazemos algumas demonstrações para uma melhor compreensão desses resultados. Na Seção 3.2, definiremos códigos **G**-lineares e, conforme nosso propósito, enfatizaremos algumas de suas propriedades. Na Seção 3.3, apresentaremos uma definição equivalente para códigos propelineares. Faremos alguns comentários que visam melhorar a compreensão de alguns resultados estabelecidos em [31]. Investigaremos estes códigos de forma a relacioná-los com os códigos **G**-lineares, pelo fato destes formarem uma subclasse da classe dos códigos geometricamente uniformes. Tendo estes argumentos como motivação, veremos que todo código **G**-linear é propelinear. Na Seção 3.4, estabeleceremos novos resultados que caracterizam os códigos **G**-lineares a partir dos códigos propelineares invariantes por translação, como também servem de ferramenta na construção destes códigos. Com isso, daremos um critério que nos permite identificar quando um código é ou não **G**-linear. Finalmente, na Seção 3.5 construiremos algumas tabelas destes códigos.

3.1 Códigos Propelineares

Definição 3.1.1 [31] *Seja* $\mathbf{C}$ *um subconjunto de* $\mathbb{Z}_2^n$ *tal que* $\mathbf{0} \in \mathbf{C}$. *Diremos que* $\mathbf{C}$ *é um código* ***propelinear*** *binário de comprimento* n *se existir um subconjunto*

$$\Pi = \{\pi_{\mathbf{v}} \in \mathbf{S}_n : \mathbf{v} \in \mathbf{C}\}$$

tal que as seguintes condições são satisfeitas

1. *Para todo* $\mathbf{v} \in \mathbf{C}$, $\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{s}) \in \mathbf{C} \iff \mathbf{s} \in \mathbf{C}$;

2. *Para todo* $\pi_{\mathbf{u}}$, $\pi_{\mathbf{v}} \in \Pi$, $\pi_{\mathbf{u}} \circ \pi_{\mathbf{v}} = \pi_{\mathbf{w}} \in \Pi$, *onde* $\mathbf{w} = \mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v})$.

Exemplo 3.1.1 *Seja* $\mathbf{C} \subset \mathbb{Z}_2^4$ *um código binário, dado por*

$$\mathbf{C} = \{\mathbf{u} = 0000, \mathbf{v} = 1100, \mathbf{r} = 0110, \mathbf{s} = 0101\}$$

e

$$\Pi = \{\pi_{\mathbf{u}} = id, \pi_{\mathbf{v}} = (12)(34), \pi_{\mathbf{r}} = (23)(14), \pi_{\mathbf{s}} = (13)(24)\}$$

subgrupo de $\mathbf{S}_4$. *Então* $\mathbf{C}$ *é um código propelinear binário de comprimento* 4. *Dessa forma, vemos que a propelinearidade induz uma estrutura linear a uma não linear.*

Proposição 3.1.1 [31] *Seja* $(\mathbf{C},\Pi)$ *um código propelinear binário de comprimento* n. *Então:*

1. $((\mathbf{C},\Pi), \star)$ *é um grupo, onde* $\mathbf{u} \star \mathbf{v} = \mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v})$, $\forall \mathbf{u}, \mathbf{v} \in \mathbf{C}$;

2. $(\Pi, \circ)$ *é um subgrupo do grupo das isometrias de* $\mathbb{Z}_2^n$;

3. $\mathbf{C}$ *é linear se, e somente se,* Π *é um subgrupo de* $\mathrm{Aut}(\mathbf{C})$;

4. *A operação* $\star$ *define uma ação de* $\mathbf{C}$ *sobre* $\mathbb{Z}_2^n$.

Prova.

1. (a) *Associatividade*: Para todo $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbf{C}$ e $\pi_{\mathbf{u}}, \pi_{\mathbf{v}}, \pi_{\mathbf{w}} \in \Pi$ temos

$$\begin{aligned}(\mathbf{u} \star \mathbf{v}) \star \mathbf{w} &= (\mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v})) \star \mathbf{w} \\ &= \mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v}) \oplus \pi_{\mathbf{u}+\pi_{\mathbf{u}}(\mathbf{v})}(\mathbf{w}) \\ &= \mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v}) \oplus (\pi_{\mathbf{u}} \circ \pi_{\mathbf{v}})(\mathbf{w}) \\ &= \mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{w})) \\ &= \mathbf{u} \star (\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{w})) \\ &= \mathbf{u} \star (\mathbf{v} \star \mathbf{w}).\end{aligned}$$

(b) *Elemento Identidade* $(\mathbf{0})$*:* $\forall\, \mathbf{v} \in \mathbf{C}$ existe $\mathbf{0} \in \mathbf{C}$, tal que

$$\mathbf{0} * \mathbf{v} = \mathbf{0} \oplus \pi_{\mathbf{0}}(\mathbf{v}) = \mathbf{0} \oplus \mathbf{v} = \mathbf{v}$$

e

$$\mathbf{v} \star \mathbf{0} = \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{0}) = \mathbf{v} \oplus \mathbf{0} = \mathbf{v}.$$

(c) *Elemento Inverso* $(\mathbf{s})$*:* $\forall\, \mathbf{v} \in \mathbf{C}$ existe $\mathbf{s} \in \mathbf{C}$ tal que $\mathbf{v} \star \mathbf{s} = \mathbf{s} \star \mathbf{v} = \mathbf{0}$. Tomando $\mathbf{s} = \pi_{\mathbf{v}}^{-1}(-\mathbf{v})$, segue que

$$\mathbf{v} \oplus \pi_{\mathbf{v}}\left(\pi_{\mathbf{v}}^{-1}(-\mathbf{v})\right) = \mathbf{v} \oplus (-\mathbf{v}) = \mathbf{0} \in \mathbb{C} \Longleftrightarrow \pi_{\mathbf{v}}^{-1}(-\mathbf{v}) \in \mathbb{C},$$

ou seja,

$$\mathbf{v} \star \pi_{\mathbf{v}}^{-1}(-\mathbf{v}) = \mathbf{v} \star \mathbf{s} = \mathbf{0}.$$

A permutação associada a palavra código $\mathbf{v} \star \mathbf{s} = \mathbf{0}$ é

$$\pi_{\mathbf{v}\star\mathbf{s}} = \pi_{\mathbf{v}} \circ \pi_{\mathbf{s}} = \pi_{\mathbf{0}} \Longleftrightarrow \pi_{\mathbf{s}} \circ \pi_{\mathbf{v}} = \pi_{\mathbf{0}} = \pi_{\mathbf{s}\star\mathbf{v}}.$$

Além disso, temos que

$$\begin{aligned}\mathbf{s} \star \mathbf{v} &= \mathbf{s} \oplus \pi_{\mathbf{s}}(\mathbf{v}) \\ &= \mathbf{s} \oplus \pi_{\mathbf{s}}(-\pi_{\mathbf{v}}(\mathbf{s})) \\ &= \mathbf{s} \oplus (-(\pi_{\mathbf{s}} \circ \pi_{\mathbf{v}})(\mathbf{s})) \\ &= \mathbf{s} \oplus (-\pi_{\mathbf{0}}(s)) \\ &= \mathbf{s} \oplus (-\mathbf{s}) = \mathbf{0}.\end{aligned}$$

Portanto, $((\mathbb{C}, \Pi), \star)$ é um grupo.

2. Basta mostrar que $(\Pi, \circ)$ é um subgrupo de $\mathbf{S}_n$. De fato:

   (a) É claro $\pi_{\mathbf{0}} \in \Pi$, pois $\mathbf{0} \in \mathbf{C}$ e

   $$\pi_{\mathbf{0}} \circ \pi_{\mathbf{0}} = \pi_{\mathbf{0} \oplus \pi_{\mathbf{0}}(\mathbf{0})} = \pi_{\mathbf{0} \oplus \mathbf{0}} = \pi_{\mathbf{0}}.$$

   Logo, $\pi_{\mathbf{0}} = id \in \mathbf{S}_n$.

   (b) Para todos $\pi_{\mathbf{u}}, \pi_{\mathbf{v}} \in \Pi$ temos que,

   $$\pi_{\mathbf{u}} \circ \pi_{\mathbf{v}} = \pi_{\mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v})} \in \Pi.$$

   (c) Para todo $\pi_{\mathbf{u}} \in \Pi$, temos que existe $\pi_{\mathbf{u}}^{-1} \in \mathbf{S}_n$, tal que

   $$\pi_{\mathbf{u}} \circ \pi_{\mathbf{u}}^{-1} = \pi_{\mathbf{u}}^{-1} \circ \pi_{\mathbf{u}} = id = \pi_{\mathbf{0}},$$

   por *a.* e *b.* segue que $\pi_{\mathbf{u}}^{-1} \in \Pi$.

3. Suponha que $\mathbf{C} \subset \mathbb{Z}_2^n$ seja linear. Então para todo $\mathbf{v} \in \mathbf{C}$, tem-se $\mathbf{v} \oplus \mathbf{C} = \mathbf{C}$ o que implica em $\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{C}) = \mathbf{C}$, ou ainda, $\pi_{\mathbf{v}}(\mathbf{C}) = \mathbf{C} \oplus (-\mathbf{v}) = \mathbf{C}$. Portanto, Π é um subgrupo de Aut $(\mathbf{C})$. Reciprocamente, se Π é um subgrupo de Aut $(\mathbf{C})$, então para cada $\mathbf{v} \in \mathbf{C}$ existe $\mathbf{s} \in \mathbf{C}$ tal que $\pi_{\mathbf{u}}(\mathbf{s}) = \mathbf{v}$. Logo,

   $$\mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{s}) = \mathbf{u} \star \mathbf{s} \in \mathbf{C},$$

   isto é, $\mathbf{C}$ é linear.

4. Basta notar que a função $\cdot : \mathbf{C} \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ definida por $\mathbf{v} \cdot \mathbf{x} = \mathbf{v} \star \mathbf{x}$ para todo $\mathbf{v} \in \mathbf{C}$ e $\mathbf{x} \in \mathbb{Z}_2^n$ é uma ação de $\mathbf{C}$ sobre $\mathbb{Z}_2^n$.

■

Definição 3.1.2 *Seja* $\mathbf{C}$ *um código binário. Diremos que* $\mathbf{C}$ *é um código* ***invariante por distância****, se a distribuição de peso de Hamming de suas classes laterais são iguais.*

Definição 3.1.3 *[31] Seja* $\mathbf{C}$ *um código propelinear. Diremos que* $\mathbf{C}$ *é um código* ***propelinear invariante por translação*** *se para todos* $\mathbf{u}, \mathbf{v} \in \mathbf{C}$ *e* $\mathbf{x} \in \mathbb{Z}_2^n$ *temos que*

$$\begin{aligned} d_H(\mathbf{u}, \mathbf{v}) &= d_H(\mathbf{u} \star \mathbf{x}, \mathbf{v} \star \mathbf{x}) \\ &= d_H(\mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{x}), \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x})). \end{aligned}$$

Proposição 3.1.2 *[31] Seja* $(\mathbf{C},\Pi)$ *um código propelinear binário de comprimento* n. *Então:*

1. *Se* $\mathbf{C}$ *é um código que corrige* e*-erros* $(\mathrm{e} \geq 1)$, *então todos os vetores de peso menor ou igual a* e *estão em classes laterais diferentes;*

2. $\mathbf{C}$ *é um código invariante por distância, mas não é necessariamente invariante por translação;*

3. *Para todos* $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$ *e* $\mathbf{v} \in \mathbf{C}$, *tem-se* $d_H(\mathbf{x}, \mathbf{y}) = d_H(\mathbf{v} \star \mathbf{x}, \mathbf{v} \star \mathbf{y})$.

   Prova.

   1. *Suponha que existam* $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$ *tais que* $wt_H(\mathbf{x}) \leq \mathrm{e}$, $wt_H(\mathbf{y}) \leq \mathrm{e}$ *e* $\mathbf{x} \in \mathbf{C} \star \mathbf{y}$ *ou, equivalentemente,* $wt_H(\mathbf{x}) \leq \mathrm{e}$, $wt_H(\mathbf{y}) \leq \mathrm{e}$ *e* $\mathbf{x} = \mathbf{v} \star \mathbf{y} = \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{y})$, *para algum* $\mathbf{v} \in \mathbf{C}$. *Como* $(\mathbf{C},\Pi)$ *é um código propelinear, ou seja* $((\mathbf{C},\Pi), \star)$ *é um grupo, existe* $(\mathbf{w}, \pi_{\mathbf{w}}) \in ((\mathbf{C},\Pi), \star)$ *tal que*

   $$(\mathbf{w}, \pi_{\mathbf{w}}) \star (\mathbf{v}, \pi_{\mathbf{v}}) = (\mathbf{w} \star \mathbf{v}, \pi_{\mathbf{w}\star\mathbf{v}}) = (\mathbf{0}, id),$$

   ou ainda,

   $$(\mathbf{w} + \pi_{\mathbf{w}}(\mathbf{v}), \pi_{\mathbf{w}} \circ \pi_{\mathbf{v}}) = (\mathbf{0}, id),$$

   dessa equação segue que $\pi_{\mathbf{w}}(\mathbf{v}) = -\mathbf{w} = \mathbf{w}$ *e* $\pi_{\mathbf{w}} \circ \pi_{\mathbf{v}} = id$. *Como*

   $$\begin{aligned} \pi_{\mathbf{w}}(\mathbf{x}) &= \pi_{\mathbf{w}}(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{y})) \\ &= \pi_{\mathbf{w}}(\mathbf{v}) \ominus (\pi_{\mathbf{w}} \circ \pi_{\mathbf{v}})(\mathbf{y}) \\ &= \mathbf{w} \oplus \mathbf{y}, \end{aligned}$$

temos que $\mathbf{w} = \mathbf{y} \oplus \pi_{\mathbf{w}}(\mathbf{x}) \in \mathbf{C}$, *pois* $\mathbf{w} \in \mathbf{C}$. *Por hipótese,*

$$wt_H(\mathbf{w}) = wt_H(\mathbf{y} \oplus \pi_{\mathbf{w}}(\mathbf{x})) \geq 2\mathrm{e} + 1.$$

Por outro lado,

$$wt_H(\mathbf{w}) \leq wt_H(\mathbf{y}) + wt_H(\pi_{\mathbf{w}}(\mathbf{x})) = wt_H(\mathbf{y}) + wt_H(\mathbf{x}) = 2\mathrm{e},$$

o que é uma contradição.

2. *Para cada* $\mathbf{y} \in \mathbf{C} \star \mathbf{x}$ *temos que existe* $\mathbf{v} \in \mathbf{C}$ *tal que* $\mathbf{y} = \mathbf{v} \star \mathbf{x} = \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x})$, *ou seja,*

$$\mathbf{C} \oplus \mathbf{y} = \mathbf{C} \oplus \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}).$$

Pelo item anterior, podemos afirmar que $\pi_{\mathbf{w}}(\mathbf{v}) = \mathbf{w}$ *e* $\pi_{\mathbf{w}} \circ \pi_{\mathbf{v}} = \pi_{\mathbf{0}} = id$. *Mas*

$$\begin{aligned}
\pi_{\mathbf{w}}(\mathbf{C} \oplus \mathbf{y}) &= \pi_{\mathbf{w}}(\mathbf{C} \oplus \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x})) \\
&= \pi_{\mathbf{w}}(\mathbf{C}) \oplus \pi_{\mathbf{w}}(\mathbf{v}) \oplus (\pi_{\mathbf{w}} \circ \pi_{\mathbf{v}})(\mathbf{x}) \\
&= \pi_{\mathbf{w}}(\mathbf{C}) \oplus \mathbf{w} \oplus \mathbf{x} \\
&= (\mathbf{w} \star \mathbf{C}) \oplus \mathbf{x} \\
&= \mathbf{C} \oplus \mathbf{x}
\end{aligned}$$

implica que

$$\begin{aligned}
wt_H(\mathbf{C} \oplus \mathbf{y}) &= wt_H(\pi_{\mathbf{w}}(\mathbf{C} \oplus \mathbf{y})) \\
&= wt_H(\mathbf{C} \oplus \mathbf{x}).
\end{aligned}$$

Portanto, $(\mathbf{C} \oplus \mathbf{x})$ *e* $(\mathbf{C} \oplus \mathbf{y})$ *tem a mesma distribuição de pesos. Para concluirmos que* $\mathbf{C}$ *não é necessariamente invariante por translação, precisamos apenas observar as equações:*

$$\begin{aligned}
d_H(\mathbf{u} \star \mathbf{x}, \mathbf{v} \star \mathbf{x}) &= d_H(\mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{x}), \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x})) \\
&= wt_H(\mathbf{v} \oplus \mathbf{u} \oplus \pi_{\mathbf{v}}(\mathbf{x}) \oplus \pi_{\mathbf{u}}(\mathbf{x})) \\
&\leq wt_H(\mathbf{v} \oplus \mathbf{u}) + wt_H(\pi_{\mathbf{v}}(\mathbf{x}) \oplus \pi_{\mathbf{u}}(\mathbf{x})) \\
&= d_H(\mathbf{u}, \mathbf{v}) + d_H(\pi_{\mathbf{v}}(\mathbf{x}) \oplus \pi_{\mathbf{u}}(\mathbf{x}), \mathbf{0}).
\end{aligned}$$

3. De fato: Para todo $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$ *e* $\mathbf{v} \in \mathbf{C}$, *tem-se*

$$\begin{aligned} d_H(\mathbf{v} \star \mathbf{x}, \mathbf{v} \star \mathbf{y}) &= d_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}), \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{y})) \\ &= wt_H(\pi_{\mathbf{v}}(\mathbf{y} \oplus \mathbf{x})) \\ &= wt_H(\mathbf{y} \oplus \mathbf{x}) \\ &= d_H(\mathbf{x}, \mathbf{y}). \end{aligned}$$

■

Lema 3.1.1 [31] *Seja* (C,Π) *um código propelinear. Então* $\mathbf{C}$ *é invariante por translação se, e somente se,*

$$wt_H(\mathbf{v}) = d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x}) \ , \forall \mathbf{x} \in \mathbb{Z}_2^n \ e \ \forall \mathbf{v} \in \mathbf{C}.$$

Prova. Por conveniência, denotamos o elemento inverso de $\mathbf{v} \in \mathbf{C}$ por $\mathbf{s} = \mathbf{v}^{-1}$. Suponha que $\mathbf{C}$ seja um código propelinear invariante por translação. Então

$$\begin{aligned} wt_H(\mathbf{v}) &= d_H(\mathbf{0}, \mathbf{v}) \\ &= d_H(\mathbf{0} \star \mathbf{x}, \mathbf{v} \star \mathbf{x}) \\ &= d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x}), \end{aligned}$$

para todo $\mathbf{x} \in \mathbb{Z}_2^n$. Reciprocamente, para quaisquer $\mathbf{u}, \mathbf{v} \in \mathbf{C}$ temos que

$$\begin{aligned} d_H(\mathbf{u}, \mathbf{v}) &= d_H\left(\mathbf{u}^{-1} \star \mathbf{u}, \mathbf{u}^{-1} \star \mathbf{v}\right) \\ &= d_H\left(\mathbf{0}, \mathbf{u}^{-1} \star \mathbf{v}\right) \\ &= wt_H\left(\mathbf{u}^{-1} \star \mathbf{v}\right) \\ &= d_H\left(\mathbf{x}, \left(\mathbf{u}^{-1} \star \mathbf{v}\right) \star \mathbf{x}\right) \\ &= d_H\left(\mathbf{x}, \mathbf{u}^{-1} \star (\mathbf{v} \star \mathbf{x})\right) \\ &= d_H\left(\mathbf{u} \star \mathbf{x}, \mathbf{u} \star \mathbf{u}^{-1} \star (\mathbf{v} \star \mathbf{x})\right) \\ &= d_H(\mathbf{u} \star \mathbf{x}, \mathbf{v} \star \mathbf{x}). \end{aligned}$$

■

Corolário 3.1.1 *Se* $\mathbf{G} = (\mathbf{C},\Pi)$ *é um código propelinear invariante por translação, então* $\mathrm{Stab}_{\mathbf{G}}(\mathbf{x}) = \{(0, id)\}$.

Corolário 3.1.2 [31] *Se* $\mathbf{C}$ *é um código propelinear invariante por translação de comprimento* n, *então* $|\mathbf{C}| = 2^k$ *para* $k \leq n$.

Prova. Considerando $\mathbf{g} \in (\mathbf{C}, *) = \mathbf{G}$, sabemos que existe sempre um mapeamento bijetivo

$$F : \mathrm{Orb}_{\mathbf{G}}(\mathbf{x}) \rightarrow G/\mathrm{Stab}_{\mathbf{G}}(\mathbf{x})$$

definido por $F(\mathbf{gx}) = \mathbf{g}Stab_{\mathbf{G}}(\mathbf{x})$, para todo $\mathbf{x} \in \mathbb{Z}_2^n$, e como

$$\begin{aligned} |\mathbf{G}| &= |\mathrm{Stab}_{\mathbf{G}}(\mathbf{x})| \ [\mathbf{G} : \mathrm{Stab}_{\mathbf{G}}(\mathbf{x})] \\ &= |\mathrm{Stab}_{\mathbf{G}}(\mathbf{x})| \ |\mathrm{Orb}_{\mathbf{G}}(\mathbf{x})| \\ &= |\mathrm{Orb}_{\mathbf{G}}(\mathbf{x})| . \end{aligned}$$

Isto acarreta que todas as classes laterais tem a mesma cardinalidade. Logo, $|G|$ divide $|\mathbb{Z}_2^n|$ e, assim, $|\mathbf{C}| = 2^k$, para algum $k \leq n$. ■

Pela Proposição 3.1.1 um código propelinear é um grupo. Indicaremos com o par $(\mathbf{G}(\mathbf{C}), \phi_{\mathbf{C}})$ o grupo associado a $\mathbf{C}$ juntamente com um isomorfismo $\phi_{\mathbf{C}}$ de $\mathbf{G}(\mathbf{C})$ em $\mathbf{C}$. Nesse caso, diremos também que o código propelinear $\mathbf{C}$ é do tipo $(\mathbf{G}(\mathbf{C}), \phi_{\mathbf{C}})$.

Exemplo 3.1.2 [31] *Seja* $\mathbf{C} \subset \mathbb{Z}_2^n$ *um código linear binário. Então* $\mathbf{C}$ *é propelinear, basta tomar* $\Pi = \{\pi_{\mathbf{v}} = id, \forall \mathbf{v} \in \mathbf{C}\}$. *Segue diretamente da Definição* 3.1.1 *que* $\mathbf{C}$ *é invariante por translação. Todos os códigos lineares são do tipo* $(\mathbb{Z}_2^n, id)$.

Exemplo 3.1.3 [31] *Os códigos* $\mathbb{Z}_4$***-lineares***, *apresentados em* [19], *são códigos lineares sobre* $\mathbb{Z}_4$. *Considerando* $\mathbb{Z}_2^2$ *e* $\Pi = \mathbf{S}_2$ *podemos definir a seguinte estrutura propelinear*

$$\begin{aligned} F^2 &= \left(\left(\mathbb{Z}_2^2, \Pi\right), \star\right) \\ &= \left\{\left(00, \pi_{00} = id\right), \left(01, \pi_{12} = (12)\right), \left(11, \pi_{00}\right), \left(10, \pi_{12}\right)\right\}. \end{aligned}$$

Como $F^2 = \langle(01, \pi_{12})\rangle$ *é cíclico de ordem* 4, *temos um isomorfismo* $\phi_4 : \mathbb{Z}_4 \to F^2$ *definido por* $\phi_4(1) = (01, \pi_{12})$. *Além disso, tanto o mapeamento Gray quanto o mapeamento Gray estendido componente a componente, são casos particulares do mapeamento* ϕ_4 *e do mapeamento* ϕ_4 *estendido componente a componete, ou seja,* $\phi_4^n : \mathbb{Z}_4^n \to F^{2n}$. *Portanto, todo código* $\mathbb{Z}_4$*-linear pode ser visto como um código propelinear invariante por translação em* F^{2n}, *do tipo* $(\mathbb{Z}_4^n, \phi_4^n)$.

Exemplo 3.1.4 [31] *Sejam* $a = (\mathbf{u}, \pi_{\mathbf{u}}) = (1010, \pi_{1010})$ *e* $b = (\mathbf{v}, \pi_{\mathbf{v}}) = (1001, \pi_{1001})$, *onde* $\pi_{1010} = (12)(34)$, $\pi_{1001} = (13)(24)$ *e* $\mathbf{Id} = (\mathbf{0}, id)$. *O código propelinear gerado por* a *e* b, *denotado por* $\mathbf{C} = \langle a, b\rangle$, *tem os seguintes elementos:*

$\mathbf{Id} = (\mathbf{0}, id)$	$b = (\mathbf{v}, \pi_{\mathbf{v}})$
$a = (\mathbf{u}, \pi_{\mathbf{u}})$	$a \star b = (\mathbf{u} \star \mathbf{v}, \pi_{\mathbf{u}\star\mathbf{v}})$
$a^2 = (\mathbf{u}^2, Id)$	$a^2 \star b = (\mathbf{u}^2 \star \mathbf{v}, \pi_{\mathbf{v}})$
$a^3 = (\mathbf{u}^3, \pi_{\mathbf{u}})$	$a^3 \star b = (\mathbf{u}^3 \star \mathbf{v}, \pi_{\mathbf{u}\star\mathbf{v}})$.

Tabela 3.1: $\mathbb{Q}_8$-cdigos

Satisfazendo as seguintes relações:

$$a^4 = \mathbf{Id}, a^2 = b^2 \text{ e } a \star b \star a = b.$$

Pelo Lema 3.1.1 *e pelas relações anteriores, podemos afirmar que este código é propelinear invariante por translação isomorfo ao grupo dos quatérnios* $\mathbb{Q}_8 = \langle i, j\rangle$, *isto é,* $\mathbf{C} = \langle a, b\rangle$ *é do tipo* $(\mathbb{Q}_8, \phi_8)$, *onde*

$$\phi_8 : \mathbb{Q}_8 \to \mathbf{C} = \langle a, b\rangle$$

é o isomorfismo definido por $\phi_8(i) = a$ *e* $\phi_8(j) = b$. *Logo, os códigos propelineares do tipo* $(\mathbb{Q}_8^k, \phi_8^k)$ *são códigos propelineares invariantes por translação. Também chamaremos estes códigos de* $\mathbb{Q}_8$*-códigos.*

Exemplo 3.1.5 [31] *Sejam* $a = (\mathbf{u}, \pi_{\mathbf{u}}) = (1010, \pi_{1010})$ *e* $b = (\mathbf{v}, \pi_{\mathbf{v}}) = (1100, \pi_{1100})$, *onde* $\pi_{1010} = (12)(34)$, $\pi_{1100} = (13)(24)$. *O código propelinear* $\mathbf{C} = \langle a, b\rangle$ *é um código*

propelinear abeliano com oito elementos, definido pelas relações

$$a^4 = \mathbf{Id}, a^2 = b^2 \ \ e \ \ a \star b = b \star a.$$

Porém $\mathbf{C}$ *não é invariante por translação, visto que*

$$wt_H(a \star b) = wt_H(0110) = 2,$$

enquanto

$$d_H(0100, a \star b \star 0100) = 0.$$

Esse código é do tipo $(\mathbb{Z}_2 \times \mathbb{Z}_4, \varphi)$*, onde*

$$\varphi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbf{C},$$

definido por $\varphi(0,1) = a$ *e* $\varphi(1,1) = b$ *é um isomorfismo. Note que* $\mathbf{C}$ *não é do tipo* $(\mathbb{Z}_2 \times \mathbb{Z}_4, (id, \phi_4))$.

Dos Exemplos 3.1.4 e 3.1.5, podemos observar que um mesmo conjunto pode ter mais de uma estrutura propelinear. Por isso, precisamos dar um melhor refinamento a esta estrutura. Veremos a seguir que os códigos propelineares binários invariantes por translação de comprimento n foram classificados como subgrupos de

$$\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times \mathbb{Q}_8^{k_3}$$

do tipo (k_1, k_2, k_3) onde $k_1 + 2k_2 + 4k_3 = n$.

Definição 3.1.4 *[31] Seja* $\mathbf{C} \subset \mathbb{Z}_2^n$ *um código binário de comprimento* n*. Diremos que* $\mathbf{C}$ *é um código do tipo* (k_1, k_2, k_3) *se* $\mathbf{C}$ *é um código propelinear invariante por translação do tipo*

$$\left(\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times \mathbb{Q}_8^{k_3}, (id, \phi_4, \phi_8)\right)$$

tal que $k_1 + 2k_2 + 4k_3 = n$ *e* (id, ϕ_4, ϕ_8) *são os mapeamentos definidos respectivamente nos Exemplos* 3.1.2, 3.1.3 *e* 3.1.4.

Nos próximos resultados, estamos supondo que (**C**,Π) seja um código propelinear invariante por translação. Além disso, para qualquer

$$\mathbf{v} = (\lambda_1, \lambda_2, \ldots, \lambda_n) = \sum_{i=1}^{n} \lambda_i \mathbf{e}_i \in \mathbb{Z}_2^n,$$

definimos o **suporte** de **v** por:

$$\mathrm{Supp}(\mathbf{v}) = \{i : 1 \leq i \leq n\,, \lambda_i \neq 0\}.$$

Nesse caso, $wt_H(\mathbf{v}) = |\mathrm{Supp}(\mathbf{v})|$.

Lema 3.1.2 *[31] Se* $\mathbf{v} \in \mathbf{C}$, *então* $\pi_{\mathbf{v}} = id$ *ou* $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$. *Quando* $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$, *para cada* $i, j \in I_n = \{1, 2, \ldots, n\}$ *tal que* $\pi_{\mathbf{v}}(\mathbf{e}_i) = \mathbf{e}_j \neq \mathbf{e}_i$ *temos:*

$$i \in \mathrm{Supp}(\mathbf{v}) \;\; \textit{se, e somente se,} \;\; j \notin \mathrm{Supp}(\mathbf{v})\,.$$

Prova. Como **C** é invariante por translação temos que

$$wt_H(\mathbf{v}) = d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x})\;, \forall \mathbf{v} \in \mathbf{C}, \mathbf{x} \in \mathbb{Z}_2^n.$$

Suponha que $\pi_{\mathbf{v}} \neq id$, então existem vetores coordenados $\mathbf{e}_i \neq \mathbf{e}_j$ tais que

$$\begin{aligned} wt_H(\mathbf{v}) &= d_H(\mathbf{e}_i, \mathbf{v} \star \mathbf{e}_i) \\ &= wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{e}_i) \oplus \mathbf{e}_i) \\ &= wt_H(\mathbf{v} \oplus \mathbf{e}_j \oplus \mathbf{e}_i)\,. \end{aligned} \tag{3.1}$$

Se $i \in \mathrm{Supp}(\mathbf{v})$, então $\lambda_i = 1$, isto é, $\lambda_i \oplus 1 = 0$. Por 3.1, temos que $\lambda_j \oplus 1 = 1$, ou seja, $\lambda_j = 0$, logo $j \notin \mathrm{Supp}(\mathbf{v})$. A recíproca basta trocar $\mathbf{e}_i$ por $\mathbf{e}_j$. ∎

Proposição 3.1.3 *[31] Se* $\mathbf{v} \in \mathbf{C}$, *então* $\pi_{\mathbf{v}}^2 = id$ *e* $\Pi = \{\pi_{\mathbf{v}} \in \mathbf{S}_n : \mathbf{v} \in \mathbf{C}\}$ *é um grupo abeliano.*

Prova. Como **C** é invariante por translação temos que

$$\begin{aligned} wt_H(\mathbf{v}) &= d_H(x, \mathbf{v} \star \mathbf{x}) \\ &= wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}) \oplus \mathbf{x})\,, \forall \mathbf{v} \in \mathbf{C}, \forall \mathbf{x} \in \mathbb{Z}_2^n. \end{aligned} \tag{3.2}$$

Se $\pi_{\mathbf{v}} = id$, então por 3.2 é verdadeira. Caso contrário, existe $\mathbf{x} \in \mathbb{Z}_2^n$ tal que $\pi_{\mathbf{v}}(\mathbf{x}) \neq \mathbf{x}$. Logo, existe um vetor de peso 1, digamos $\mathbf{e}_i$, tal que $\pi_{\mathbf{v}}(\mathbf{e}_i) \neq \mathbf{e}_i$, mais precisamente $\pi_{\mathbf{v}}(\mathbf{e}_i) = \mathbf{e}_j \neq \mathbf{e}_i$. Sem perda de generalidade podemos supor que $\pi_{\mathbf{v}}(\mathbf{e}_j) = \mathbf{e}_k$, com $\mathbf{e}_k \neq \mathbf{e}_j$, pois caso $\mathbf{e}_k$ seja igual a $\mathbf{e}_j$ teríamos $\pi_{\mathbf{v}} = id$. Pelo Lema 3.1.2, podemos escrever

$$i, k \in \mathrm{Supp}(\mathbf{v}) \text{ e } j \notin \mathrm{Supp}(\mathbf{v}) \text{ ou } i, k \notin \mathrm{Supp}(\mathbf{v}) \text{ e } j \in \mathrm{Supp}(\mathbf{v}).$$

Agora vamos supor que $\mathbf{e}_k \neq \mathbf{e}_i$. Então

$$\begin{aligned} wt_H((\mathbf{e}_i \oplus \mathbf{e}_j) \oplus \mathbf{v} \star (\mathbf{e}_i \oplus \mathbf{e}_j)) &= wt_H(\mathbf{e}_i \oplus \mathbf{e}_j \oplus \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{e}_i \oplus \mathbf{e}_j)) \\ &= wt_H(\mathbf{e}_i \oplus \mathbf{v} \oplus \mathbf{e}_k) \\ &< wt_H(\mathbf{v}). \end{aligned}$$

pois

$$\mathbf{e}_i \oplus \mathbf{v} \oplus \mathbf{e}_k = (\lambda_1, \ldots, \lambda_{i-1}, 0, \lambda_{i+1}, \ldots, \lambda_{k-1}, 0, \lambda_{k+1}, \ldots, \lambda_n).$$

Isto contradiz o fato de $\mathbf{C}$ ser invariante por translação. Portanto, $\pi_{\mathbf{v}}^2 = id$. Como todos os elementos de Π são idempotentes temos que Π é um grupo abeliano. ■

Observação 3.1.1 *Pela Proposição* 3.1.3 *temos que para cada* $\mathbf{v} \in \mathbf{C}$, $\pi_{\mathbf{v}} = id$ *ou* $\pi_{\mathbf{v}}$ *é um produto de transposições, ou seja,*

$$\pi_{\mathbf{v}} = \prod_{i \in \mathrm{Supp}(\mathbf{v})} \pi_i, \quad \textit{onde } \pi_i = id \textit{ ou } \pi_i = (ij) = \pi_j.$$

Corolário 3.1.3 *[31] Se* $\mathbf{v} \in \mathbf{C}$, *então* $\mathbf{v}^4 = \mathbf{0}$.

Prova.

$$\begin{aligned} \mathbf{v}^4 &= \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{v}) \oplus \pi_{\mathbf{v}}^2(\mathbf{v}) \oplus \pi_{\mathbf{v}}^3(\mathbf{v}) \\ &= \mathbf{v}^2 \oplus \mathbf{v}^2 = \mathbf{0}. \end{aligned}$$

■

Proposição 3.1.4 *[31] Sejam* $i,j,k,l \in I_n = \{1,2,\ldots,n\}$. *Se* $\mathbf{u},\mathbf{v} \in \mathbf{C}$ *e* $\pi_{\mathbf{u}}(\mathbf{e}_i) = \mathbf{e}_j$, $\pi_{\mathbf{v}}(\mathbf{e}_i) = \mathbf{e}_k$ *com* $j \neq k, j \neq i$ *e* $k \neq j$, *então*

1. $\pi_{\mathbf{u}}(\mathbf{e}_k) = \pi_{\mathbf{v}}(\mathbf{e}_j) = \mathbf{e}_l$, *com* $l \neq i, l \neq j$ *e* $l \neq k$;

2. *Seja* Π' *a restrição de* Π *ao conjunto de coordenadas* $\{i,j,k,l\}$. *Então* $\pi'_{\mathbf{u}} = (i,j)(k,l)$, $\pi'_{\mathbf{v}} = (i,k)(j,l)$ *e* $\pi'_{\mathbf{u}\star\mathbf{v}} = \pi'_{\mathbf{v}\star\mathbf{u}} = (i,l)(j,k)$.

Prova.

1.

$$\begin{aligned}\pi_{\mathbf{u}}(\mathbf{e}_k) &= \pi_{\mathbf{u}}(\pi_{\mathbf{v}}(\mathbf{e}_i)) \\ &= \pi_{\mathbf{v}}(\pi_{\mathbf{u}}(\mathbf{e}_i)) \\ &= \pi_{\mathbf{v}}(\mathbf{e}_j) = \mathbf{e}_l,\end{aligned}$$

para $l \neq j$, $l \neq i$ e $l \neq k$.

2. Sejam $\hat{I}_1 = \{i,j,k,l\} \subset I_n$ e

$$\Pi' = \Pi|_{\hat{I}_1} = \{\pi'_{\mathbf{w}} : \mathbf{w} \in \mathbf{C}\},$$

a restrição do conjunto das permutacões de Π a $\hat{I}_1$. Então pela Proposição 3.1.3 temos que $\pi'_{\mathbf{w}} = id$ ou $\pi'_{\mathbf{w}}$ é o produto de transposições. Pela hipótese e o item 1. temos que

$$\left\{\begin{array}{l} i \in \mathrm{Supp}(\mathbf{u}) \Leftrightarrow j \notin \mathrm{Supp}(\mathbf{u}) \\ i \in \mathrm{Supp}(\mathbf{v}) \Leftrightarrow k \notin \mathrm{Supp}(\mathbf{v}) \end{array}\right\} \quad \text{e} \quad \left\{\begin{array}{l} k \in \mathrm{Supp}(\mathbf{u}) \Leftrightarrow l \notin \mathrm{Supp}(\mathbf{u}) \\ j \in \mathrm{Supp}(\mathbf{v}) \Leftrightarrow l \notin \mathrm{Supp}(\mathbf{v}). \end{array}\right\}$$

Então pela Observação 3.1.1, temos que

$$\pi'_{\mathbf{u}} = \pi_i \circ \pi_k = (ij)(kl) \quad \text{e} \quad \pi'_{\mathbf{v}} = \pi_i \circ \pi_j = (ik)(jl)$$

e

$$\pi'_{\mathbf{u}\star\mathbf{v}} = \pi'_{\mathbf{u}} \circ \pi'_{\mathbf{v}} = \pi'_{\mathbf{v}} \circ \pi'_{\mathbf{u}} = \pi'_{\mathbf{v}\star\mathbf{u}} = (il)(jk).$$

■

Lema 3.1.3 *[31] Sejam $a, b, c \in \mathbf{C}$ três palavras código tais que os subcódigos $\mathbf{C}_1 = \langle a, b\rangle$ e $\mathbf{C}_2 = \langle b, c\rangle$ sejam $\mathbb{Q}_8$-códigos distintos. Então o subcódigo $\mathbf{C}_3 = \langle a \star b, c\rangle$ não pode ser um $\mathbb{Q}_8$-código.*

Prova. Como $\mathbf{C}_1 = \langle a, b\rangle$ e $\mathbf{C}_2 = \langle b, c\rangle$ são $\mathbb{Q}_8$-códigos temos que

$$a^4 = \mathbf{0}, a^2 = b^2 \text{ e } a \star b \star a = b$$

e

$$b^4 = \mathbf{0}, a^2 = b^2 \text{ e } b \star c \star b = c.$$

Portanto,

$$\begin{aligned} b \star a &= a \star b \star a \star a = a \star b^3 \\ a \star b &= a \star a \star b \star a = b^3 \star a \\ c \star b &= b \star c^3 \\ b \star c &= c^3 \star b. \end{aligned}$$

Suponha que $\mathbf{C}_3 = \langle a \star b, c\rangle$ seja um $\mathbb{Q}_8$-código. Então

$$\begin{aligned} (a \star b) \star c \star (a \star b) &= a \star (b \star c) \star (a \star b) \\ &= a \star \left(c^3 \star b\right) \star (a \star b) \\ &= \left(a \star c^3\right) \star b \star (a \star b) \\ &= (c \star a) \star b \star (a \star b) \\ &= c \star (a \star b) \star (a \star b) \\ &= c \star (a \star b)^2 \\ &= c \star c^2 \\ &= c^3 \neq c. \end{aligned}$$

■

Teorema 3.1.1 *[31]Se* $\mathbf{C}$ *é um código propelinear invariante por translação de comprimento* n*, então* $\mathbf{C}$ *é do tipo* (k_1, k_2, k_3).

Prova. Provaremos que $\mathbf{C}$ pode ser visto como um subgrupo de $\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times \mathbb{Q}_8^{k_3}$, onde $k_1 + 2k_2 + 4k_3 = n$. Para isto, vamos particionar o conjunto $I_n = J_1 \cup J_2 \cup J_3$ tal que $|J_1| = k_1$, $|J_2| = 2k_2$, $|J_3| = 4k_3$. Assim, temos três casos há serem considerados:

1º Caso Seja $J_1 = \{i \in I_n : \pi_{\mathbf{u}}(\mathbf{e}_i) = \mathbf{e}_i, \forall \mathbf{u} \in \mathbf{C}\}$. Então $\pi_{\mathbf{u}} = id$ e $\mathbf{C}$ é linear do tipo $(k_1, 0, 0)$.

2º Caso Seja $J_2 = \{\{i, j\} : i, j \in J_1 \text{ e } i \neq j\}$. Então, para cada $\mathbf{u} \in \mathbf{C}$ temos que $\pi_{\mathbf{u}}(\mathbf{e}_i) = \mathbf{e}_j$ ou $\pi_{\mathbf{u}}(\mathbf{e}_i) = \mathbf{e}_i$ e $\pi_{\mathbf{u}}(\mathbf{e}_j) = \mathbf{e}_j$:

(a) Se $\pi_{\mathbf{u}}(\mathbf{e}_i) = \mathbf{e}_j$, então pela Proposição 3.1.3 temos que $\pi_{\mathbf{u}}(\mathbf{e}_j) = \pi_{\mathbf{u}}^2(\mathbf{e}_i) = \mathbf{e}_i$ e pelo Lema 3.1.2

$$i \in \text{Supp}(\mathbf{u}) \Leftrightarrow j \notin \text{Supp}(\mathbf{u}).$$

Assim, tomando a restrição de $\pi_{\mathbf{u}}$ ao conjunto J_2, e pela Observação 3.1.1 podemos escrever

$$\pi_{\mathbf{u}} = \prod_{i \in \text{Supp}(\mathbf{u})} \pi_i, \text{ onde } \pi_i = id \text{ ou } \pi_i = (ij) = \pi_j.$$

ou seja,

$$a = (\mathbf{u}, \pi_{\mathbf{u}}) = (10, \pi_{10} = (ij))$$

ou

$$a = (\mathbf{u}, \pi_{\mathbf{u}}) = (01, \pi_{01} = (ji)).$$

Em qualquer caso, obtemos um código $\mathbb{Z}_4$-linear conforme visto no Exemplo 3.1.3, ou seja, um código do tipo $(0, k_2, 0)$.

(b) Agora, se $\mathbf{v} \in \mathbf{C}$ tal que $\pi_{\mathbf{v}}(\mathbf{e}_i) = \mathbf{e}_i$ e $\pi_{\mathbf{v}}(\mathbf{e}_j) = \mathbf{e}_j$, então

$$i, j \in \mathrm{Supp}(\mathbf{v}) \text{ ou } i, j \notin \mathrm{Supp}(\mathbf{v}).$$

Pois caso contrário,

$$i, j \in \mathrm{Supp}(\mathbf{v} \star \mathbf{u}) \text{ ou } i, j \notin \mathrm{Supp}(\mathbf{v} \star \mathbf{u}).$$

E pelo Lema 3.1.1, temos a contradição:

$$\begin{aligned} wt_H(\mathbf{v} \star \mathbf{u}) &= d_H(\mathbf{e}_i, (\mathbf{v} \star \mathbf{u}) \star \mathbf{e}_i) \\ &= wt_H((\mathbf{v} \star \mathbf{u}) \star \mathbf{e}_i \oplus \mathbf{e}_i) \\ &= wt_H(\mathbf{v} \star \mathbf{u} \oplus \pi_{\mathbf{v}\star\mathbf{u}}(\mathbf{e}_i) \oplus \mathbf{e}_i) \\ &= wt_H(\mathbf{v} \star \mathbf{u} \oplus (\pi_{\mathbf{v}} \circ \pi_{\mathbf{u}})(\mathbf{e}_i) \oplus \mathbf{e}_i)) \\ &= wt_H(\mathbf{v} \star \mathbf{u} \oplus \pi_{\mathbf{v}}(\mathbf{e}_j) \oplus \mathbf{e}_i)) \\ &= wt_H(\mathbf{v} \star \mathbf{u} \oplus \mathbf{e}_j \oplus \mathbf{e}_i)) \\ &< wt_H(\mathbf{v} \star \mathbf{u}). \end{aligned}$$

Então a restrição de $\pi_{\mathbf{v}}$ ao conjunto de índices J_2 é novamente o mesmo código $\mathbb{Z}_4$-linear definido em $a.$ e portanto do tipo $(0, k_2, 0)$.

$3^{\underline{0}}$ Caso Seja $J_3 = I_n - (I_1 \cup I_2) \neq \emptyset$. Então existe $i \in J_3$ e $\mathbf{u}, \mathbf{v} \in \mathbf{C}$ tal que $\pi_{\mathbf{u}}(\mathbf{e}_i) = \mathbf{e}_j$ e $\pi_{\mathbf{v}}(\mathbf{e}_i) = \mathbf{e}_k$ com $j \neq k, j \neq i$ e $k \neq i$. Se Π' é a restrição de Π ao conjunto de coordenadas $\{i, j, k, l\} \subset J_3$, então pela Proposição 3.1.4, podemos afirmar que $\pi'_{\mathbf{u}} = (i, j)(k, l)$, $\pi'_{\mathbf{v}} = (i, k)(j, l)$ e $\pi'_{\mathbf{u}\star\mathbf{v}} = \pi'_{\mathbf{v}\star\mathbf{u}} = (i, l)(j, k)$. Desta forma, temos quatro possibilidades para a coordenada i :

a_1. $i \in \mathrm{Supp}(\mathbf{u})$ e $i \in \mathrm{Supp}(\mathbf{v})$, nesse caso $j \notin \mathrm{Supp}(\mathbf{u})$ e $k \notin \mathrm{Supp}(\mathbf{v})$;

a_2. $i \notin \mathrm{Supp}(\mathbf{u})$ e $i \in \mathrm{Supp}(\mathbf{v})$, nesse caso $j \in \mathrm{Supp}(\mathbf{u})$ e $k \notin \mathrm{Supp}(\mathbf{v})$;

a_3. $i \in \mathrm{Supp}(\mathbf{u})$ e $i \notin \mathrm{Supp}(\mathbf{v})$, nesse caso $j \notin \mathrm{Supp}(\mathbf{u})$ e $k \in \mathrm{Supp}(\mathbf{v})$;

a_4. $i \notin \mathrm{Supp}(\mathbf{u})$ e $i \notin \mathrm{Supp}(\mathbf{v})$, nesse caso $j \notin \mathrm{Supp}(\mathbf{u})$ e $k \in \mathrm{Supp}(\mathbf{v})$;

Note que

$$\begin{aligned} wt_H(\mathbf{u}+\mathbf{v}) &= d_H(\mathbf{u},\mathbf{v}) \\ &= d_H(\mathbf{u}\star\mathbf{e}_i, \mathbf{v}\star\mathbf{e}_i) \\ &= wt_H(\mathbf{u}\star\mathbf{e}_i \oplus \mathbf{v}\star\mathbf{e}_i) \\ &= wt_H(\mathbf{u}\oplus\pi_{\mathbf{u}}(\mathbf{e}_i)\oplus\mathbf{v}\oplus\pi_{\mathbf{v}}(\mathbf{e}_i)) \\ &= wt_H(\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{e}_j\oplus\mathbf{e}_k). \end{aligned}$$

Dessas equações, obtemos respectivamente, duas possibilidades para cada um dos quatro casos anteriores:

b_1. $j \notin \mathrm{Supp}(\mathbf{v})$ e $k \in \mathrm{Supp}(\mathbf{u})$ ou $j \in \mathrm{Supp}(\mathbf{v})$ e $k \notin \mathrm{Supp}(\mathbf{u})$;

b_2. $j \notin \mathrm{Supp}(\mathbf{v})$ e $k \notin \mathrm{Supp}(\mathbf{u})$ ou $j \in \mathrm{Supp}(\mathbf{v})$ e $k \in \mathrm{Supp}(\mathbf{u})$;

b_3. $j \notin \mathrm{Supp}(\mathbf{v})$ e $k \notin \mathrm{Supp}(\mathbf{u})$ ou $j \in \mathrm{Supp}(\mathbf{v})$ e $k \in \mathrm{Supp}(\mathbf{u})$;

b_4. $j \notin \mathrm{Supp}(\mathbf{v})$ e $k \in \mathrm{Supp}(\mathbf{u})$ ou $j \in \mathrm{Supp}(\mathbf{v})$ e $k \notin \mathrm{Supp}(\mathbf{u})$.

Combinando adequadamente essas situações, cada a_r. com seu respectivo b_r., $r = 1,2,3,4$, podemos ter:

i. Para $r = 1$, temos que

$$\begin{aligned} (\mathbf{u},\pi'_{\mathbf{u}}) &= (1010, \pi'_{1010} = \pi_1\pi_3 = (ij)(kl)) \\ (\mathbf{v},\pi'_{\mathbf{v}}) &= (1001, \pi'_{1010} = \pi_1\pi_4 = (ik)(jl)) \end{aligned}$$

ou

$$\begin{aligned} (\mathbf{u},\pi'_{\mathbf{u}}) &= (1001, \pi'_{1001} = \pi_1\pi_3 = (ij)(kl)) \\ (\mathbf{v},\pi'_{\mathbf{v}}) &= (1100, \pi'_{1010} = \pi_1\pi_4 = (ik)(jl)). \end{aligned}$$

Em ambos os casos, obtemos dois códigos propelineares invariante por translação isomorfos a $\mathbb{Q}_8$, conforme o Exemplo 3.1.4 De modo análogo, determinamos seis códigos propelineares invariantes por translação isomorfos a $\mathbb{Q}_8$, cujos geradores são os respectivos $(\mathbf{u},\pi'_{\mathbf{u}})$ e $(\mathbf{v},\pi'_{\mathbf{v}})$:

ii. Para $r = 2$ temos que

$$\begin{aligned}(\mathbf{u}, \pi'_{\mathbf{u}}) &= (0101, \pi'_{\mathbf{u}}), (\mathbf{v}, \pi'_{\mathbf{v}}) = (1001, \pi'_{\mathbf{v}}) \\ (\mathbf{u}, \pi'_{\mathbf{u}}) &= (0110, \pi'_{\mathbf{u}}), (\mathbf{v}, \pi'_{\mathbf{v}}) = (1100, \pi'_{\mathbf{v}}).\end{aligned}$$

iii. Para $r = 3$ temos que

$$\begin{aligned}(\mathbf{u}, \pi'_{\mathbf{u}}) &= (1001, \pi'_{\mathbf{u}}), (\mathbf{v}, \pi'_{\mathbf{v}}) = (0011, \pi'_{\mathbf{v}}) \\ (\mathbf{u}, \pi'_{\mathbf{u}}) &= (1010, \pi'_{\mathbf{u}}), (\mathbf{v}, \pi'_{\mathbf{v}}) = (0110, \pi'_{\mathbf{v}}).\end{aligned}$$

iv. Para $r = 4$ temos que

$$\begin{aligned}(\mathbf{u}, \pi'_{\mathbf{u}}) &= (0110, \pi'_{\mathbf{u}}), (\mathbf{v}, \pi'_{\mathbf{v}}) = (0011, \pi'_{\mathbf{v}}) \\ (\mathbf{u}, \pi'_{\mathbf{u}}) &= (0101, \pi'_{\mathbf{u}}), (\mathbf{v}, \pi'_{\mathbf{v}}) = (0110, \pi'_{\mathbf{v}}).\end{aligned}$$

Finalmente, para qualquer $\mathbf{w} \in \mathbf{C}$ tal que $\pi_{\mathbf{w}}(\mathbf{e}_i) = \mathbf{e}_m$, ou seja, $\pi_{\mathbf{w}} = (im)$, para $m \neq i, m \neq j, m \neq k$, temos duas possibilidades a considerar:

- Se $m = l$, então pela Proposição 3.1.4 $\pi'_{\mathbf{w}} = (il)(jk)$ e pela construção anterior podemos assegurar que $\mathbf{w} = \mathbf{u} \star \mathbf{v}$ ou $\mathbf{w} = \mathbf{v} \star \mathbf{u}$. Portanto, $\mathbf{w}$ pertence a um $\mathbb{Q}_8$-código gerado por $\mathbf{w}$ e $\mathbf{v}$.
- Se $m \neq l$, então podemos construir os $\mathbb{Q}_8$-códigos $\langle \mathbf{u}, \mathbf{v} \rangle$, $\langle \mathbf{v}, \mathbf{w} \rangle$ e $\langle \mathbf{u} \star \mathbf{v}, \mathbf{w} \rangle$, o que contradiz o Lema 3.1.3. Portanto, $\mathbf{u}, \mathbf{v}$ e $\mathbf{w}$ não podem pertencer a um mesmo código propelinear invariante por translação.

■

Observação 3.1.2 *Os códigos propelineares invariantes por translação são subgrupos de*

$$\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times \mathbb{Q}_8^{k_3},$$

os quais são imagens isomorfas de certos grupos abstratos pelos mapeamentos (id, ϕ_4, ϕ_8).

Exemplo 3.1.6 *Consideremos o código propelinear binário* $\mathbf{C} = \langle a, b, c\rangle$ *de comprimento* $n = 7$, *gerado por*

$$\begin{aligned} a &= (1001010, \pi_{1001010} = (45)(67)), \\ b &= (0101001, \pi_{0101001} = (46)(57)), \\ c &= (1111111, \pi_{1111111} = id). \end{aligned}$$

Esse é um código propelinear invariante por translação do tipo $(3, 0, 1)$, *ou seja, um subgrupo de* $(\mathbb{Z}_2^3 \times \mathbb{Q}_8, (id, \phi_8))$, *cujas palavras código são dadas por*

$(0000000, id)$	$(0100110, (46)(57))$
$(0001111, id)$	$(0101001, (46)(57))$
$(1110000, id)$	$(1010110, (46)(57))$
$(1111111, id)$	$(1011001, (46)(57))$
$(0110101, (45)(67))$	$(0010011, (47)(56))$
$(0111010, (45)(67))$	$(0011100, (47)(56))$
$(1000101, (45)(67))$	$(1100011, (47)(56))$
$(1001010, (45)(67))$	$(1101100, (47)(56))$.

Observamos ainda que $\mathbf{C} = \langle a, b, c\rangle$ *é isomorfo a* $\mathbb{Z}_2 \times \mathbb{Q}_8$.

Exemplo 3.1.7 *Considere o código propelinear binário* $\mathbf{C} = \langle a, b, c\rangle$ *de comprimento* 7, *gerado por*

$$\begin{aligned} a &= (1001010, \pi_{1001010} = (45)(67)), \\ b &= (0101001, \pi_{0101001} = (45)(67)), \\ c &= (1111111, \pi_{1111111} = id). \end{aligned}$$

Então, $\mathbf{C}$ *é um código propelinear invariante por translação do tipo* $(3, 2, 0)$, *ou seja, um subgrupo de* $(\mathbb{Z}_2^3 \times \mathbb{Z}_4^2, (id, \phi_4))$. *Nesse caso,* $\mathbf{C}$ *é formado pelas seguintes palavras código*

$(0000000, id)$	$(0100110, (45)\,(67))$
$(0001111, id)$	$(0101001, (45)\,(67))$
$(0010011, id)$	$(0110101, (45)\,(67))$
$(0011100, id)$	$(0111010, (45)\,(67))$
$(1100011, id)$	$(1000101, (45)\,(67))$
$(1101100, id)$	$(1001010, (45)\,(67))$
$(1110000, id)$	$(1010110, (45)\,(67))$
$(1111111, id)$	$(1011001, (45)\,(67))$.

Com isso, vemos que $\mathbf{C} = \langle a, b, c\rangle$ *é isomorfo a* $\mathbb{Z}_2^2 \times \mathbb{Z}_4$.

Exemplo 3.1.8 *Consideremos o código propelinear binário* $\mathbf{C} = \langle a, b, c\rangle$ *de comprimento* $n = 7$, *gerado por*

$$\begin{aligned} a &= (1101010, \pi_{1101010} = (23)\,(45)\,(67))\,, \\ b &= (0011001, \pi_{0011001} = (23)\,(46)\,(57))\,, \\ c &= (1111111, \pi_{1111111} = id)\,. \end{aligned}$$

Esse é um código propelinear invariante por translação do tipo $(1, 1, 1)$, *ou seja, um subgrupo de* $(\mathbb{Z}_2^1 \times \mathbb{Z}_4^1 \times \mathbb{Q}_8^1, (id, \phi_4, \phi_8))$. *Além disso, podemos ver ainda que ele é*

formado pelas seguintes palavras código

$(0000000, id)$	$(0010101, (23)\,(45)\,(67))$
$(0001111, id)$	$(0011010, (23)\,(45)\,(67))$
$(0110000, id)$	$(0100101, (23)\,(45)\,(67))$
$(0111111, id)$	$(0101010, (23)\,(45)\,(67))$
$(1000000, id)$	$(1010101, (23)\,(45)\,(67))$
$(1001111, id)$	$(1011010, (23)\,(45)\,(67))$
$(1110000, id)$	$(1100110, (23)\,(45)\,(67))$
$(1111111, id)$	$(1101001, (23)\,(45)\,(67))$
$(0000011, (47)\,(56))$	$(0010110, (23)\,(46)\,(57))$
$(0001100, (47)\,(56))$	$(0011001, (23)\,(46)\,(57))$
$(0110011, (47)\,(56))$	$(0100110, (23)\,(46)\,(57))$
$(0111100, (47)\,(56))$	$(0101001, (23)\,(46)\,(57))$
$(1000011, (47)\,(56))$	$(1010110, (23)\,(46)\,(57))$
$(1001100, (47)\,(56))$	$(1011001, (23)\,(46)\,(57))$
$(1110011, (47)\,(56))$	$(1100110, (23)\,(46)\,(57))$
$(1111100, (47)\,(56))$	$(1101001, (23)\,(46)\,(57))$.

Observação 3.1.3 *Esse código é isomorfo a* $[\mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_4).\mathbb{Z}_2]$, *para essa notação confira [28].*

3.2 Códigos G-Lineares

A $\mathbb{Z}_4$-linearidade, apresentada em [19], contribuiu de forma significativa para a Teoria da Codificação, haja visto a grande quantidade de trabalhos publicados nesta direção. Uma das principais propriedades da $\mathbb{Z}_4$-linearidade é a obtenção de códigos não-lineares binários a partir de códigos lineares sobre $\mathbb{Z}_4$ obtidos através do mapeamento Gray, o qual é uma isometria entre os espaços métricos $(\mathbb{Z}_4, d_L)$ e $(\mathbb{Z}_2^2, d_H)$. Em [19], também foram respondidas as seguintes questões: Quando um código binário é $\mathbb{Z}_4$-linear? Quando a

imagem binária sob o mapeamento Gray de um código linear sobre $\mathbb{Z}_4$ é um código linear?

Observando um pouco melhor estas colocações, vemos a princípio que o conjunto de sinais $\mathbb{Z}_2^2$ é geometricamente uniforme, ou seja, o grupo $\mathbb{Z}_4$ está efetivamente casado a $\mathbb{Z}_2^2$, segundo Loeliger [23]. Tendo como ponto de partida essas considerações, em [17] foram introduzidas as primeiras propriedades da **G**-linearidade onde **G** é um grupo qualquer, como uma extensão das propriedades da $\mathbb{Z}_4$-linearidade. Com a finalidade de generalizar esta extensão, basta considerarmos o código **C** sobre um alfabeto qualquer $\mathcal{A}$ com $(\mathcal{A}^k, d_{\mathcal{A}})$ sendo um espaço métrico. Na realidade, o que se busca na **G**-linearidade é uma certa uniformidade geométrica do seu alfabeto, ou seja, determinar um subgrupo $\mathcal{G}(\mathcal{A}^k)$ do grupo de simetrias $\Gamma(\mathcal{A}^k)$ que seja isomorfo ao grupo abstrato **G** e sua ação sobre $\mathcal{A}^k$ seja *fortemente transitiva*. Isto define um rotulamento isométrico ψ dos pontos de $\mathcal{A}^k$ pelos elementos de **G** induzido pelo isomorfismo entre **G** e $\mathcal{G}(\mathcal{A}^k)$. Portanto, códigos **G**-lineares em $\mathcal{A}^{kn}$ correspondem a subgrupos de $\mathbf{G}^n$ mapeados por ψ, estendido componente a componente.

O *mapeamento Gray* é usualmente indicado por $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ e definido por

$$\phi(0) = (0,0)\,,\ \phi(1) = (0,1)\,,\ \phi(2) = (1,1)\ \text{ e } \phi(3) = (1,0)\,.$$

Naturalmente este mapeamento pode ser estendido componente a componente, ou seja, $\phi_{Ex} : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$, e tem a vantagem de que quando uma palavra código sobre $\mathbb{Z}_4$ é transmitida através de um canal Gaussiano com ruído branco aditivo, os erros mais prováveis de ocorrerem são os causados pela decodificação errônea de um único bit de informação.

Um código binário **C** de comprimento $2n$ ($\mathbf{C} \subseteq \mathbb{Z}_2^{2n}$) é chamado $\mathbb{Z}_4$-linear se a menos de uma permutação de coordenadas, $\mathbf{C} = \phi(C)$ para algum subgrupo C de $\mathbb{Z}_4^n$.

Teorema 3.2.1 *[19] Um código binário* **C** *de comprimento* $2n$ *é chamado* $\mathbb{Z}_4$*-linear se, e somente se, após uma permutação de coordenadas*

$$(\mathbf{u} + \sigma(\mathbf{u})) \cdot (\mathbf{v} + \sigma(\mathbf{v})) \in \mathbf{C}\ ,\ \textit{para todo}\ \mathbf{u}, \mathbf{v} \in \mathbf{C}\ ,$$

onde $\cdot$ *é a multiplicação de vetores componente a componente e* σ *é a* ***função troca****, ou seja, a permutação* $(1, n+1)(2, n+2)(3, n+3)\cdots(n, 2n)$ *sobre o vetor de dimensão* $2n$, $\mathbf{x} = (x_1, x_2, \ldots, x_n, x_{n+1}, \ldots, x_{2n})$ *tal que* $\sigma(\mathbf{x}) = (x_{n+1}, \ldots, x_{2n}, x_1, x_2, \ldots, x_n)$.

Definição 3.2.1 *Sejam* $\mathbf{G}$ *um grupo,* $d_{\mathbf{G}}$ *uma métrica sobre* $\mathbf{G}$ *e* $\mathbf{C}$ *um código de comprimento* n *sobre um alfabeto qualquer* $\mathcal{A}$ *com* $(\mathcal{A}^k, d_{\mathcal{A}})$ *sendo um espaço métrico. Diremos que* $\mathbf{C}$ *é* $\mathbf{G}$*-linear, se a menos de uma permutação de coordenadas,* $\mathbf{C} = \psi(\widehat{\mathbf{C}})$ *para algum subgrupo* $\widehat{\mathbf{C}}$ *de* $\mathbf{G}^n$ *e* $\psi : \mathbf{G}^n \to \mathcal{A}^{kn}$ *é uma isometria para algum* $k \geq 2$.

Proposição 3.2.1 [17] *Todo código* $\mathbf{G}$*-linear é geometricamente uniforme.*

Exemplo 3.2.1 *Consideremos o grupo de simetrias de* $\mathbb{Z}_2^k$*, isto é,* $\Gamma(\mathbb{Z}_2^k) \cong \mathbb{Z}_2^k \rtimes \mathbf{S}_k$.

1. Quando $k = 2$, temos que $\Gamma(\mathbb{Z}_2^2) \cong \mathbb{Z}_2^2 \rtimes \mathbf{S}_2 \cong \mathbb{D}_4$. Como $\mathcal{G}(\mathbb{Z}_2^2) = \mathbb{Z}_4$ é um subgrupo de $\mathbb{D}_4$ cuja ação é *fortemente transitiva* sobre $\mathbb{Z}_2^2$, obtemos os códigos $\mathbb{Z}_4$-lineares ;

2. Quando $k = 3$, temos que $\Gamma(\mathbb{Z}_2^3) \cong \mathbb{Z}_2^3 \rtimes \mathbf{S}_3$. Como $\mathcal{G}(\mathbb{Z}_2^3) = \mathbb{Z}_2 \times \mathbb{Z}_4$ é um subgrupo de $\Gamma(\mathbb{Z}_2^3)$ cuja ação sobre $\mathbb{Z}_2^3$ é *fortemente transitiva* sobre $\mathbb{Z}_2^3$, obtemos os códigos $\mathbb{Z}_2 \times \mathbb{Z}_4$-lineares.

3.3 Relação entre os Códigos Propelineares e G-Lineares

Nesta seção, por conveniência, vamos considerar uma definição de código propelinear equivalente a Definição 3.1.1. Apresentaremos algumas contribuições que relacionam a classe dos códigos propelineares e propelineares invariantes por translação com a classe dos códigos G-lineares. Geralmente, esses códigos podem ser pensados como códigos sobre grupos de isometrias, mais precisamente códigos provenientes da ação do grupo de simetrias de um dado alfabeto. Nosso interesse nestes códigos é motivado pelo estudo de conjuntos de sinais geomericamente uniformes (GU), dados em [12].

Definição 3.3.1 *Sejam* $(\mathbb{Z}_2^n, d_H)$ *o espaço de Hamming n-dimensional e* $\mathbf{S}_n$ *o grupo simétrico de grau n. Diremos que um subconjunto* $\mathbf{C} \subseteq \mathbb{Z}_2^n$, *com* $\mathbf{0} \in \mathbf{C}$ *é um* ***código propelinear*** *de comprimento n, se existir uma função* $\pi : \mathbf{C} \to \mathbf{S}_n$, *definida por* $\pi(\mathbf{v}) = \pi_{\mathbf{v}}$, *tal que o gráfico*

$$\Omega(\pi) = \{(\mathbf{v}, \pi_{\mathbf{v}}) : \forall \mathbf{v} \in \mathbf{C}\}$$

seja um subgrupo de $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$.

Desta forma, observamos que quando um código $\mathbf{C}$ é propelinear existe uma identificação natural de $\mathbf{C}$ com o subgrupo $(\Omega(\pi), \star)$ de $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$. Esta identificação produz uma ação *fortemente transitiva* de $(\Omega(\pi), \star)$ sobre $\mathbf{C}$, definida pela função $f : \Omega(\pi) \times \mathbf{C} \to \mathbf{C}$ tal que

$$f((\mathbf{v}, \pi_{\mathbf{v}}), x) = (\mathbf{v}, \pi_{\mathbf{v}}) \star x = \mathbf{v} + \pi_{\mathbf{v}}(x) = \mathbf{v} \star x.$$

Neste momento, nosso objetivo é dar consistência à construção de códigos G-lineares binários. Por isso, particularizaremos a Definição 3.2.1.

Definição 3.3.2 *Sejam* $\mathbf{G}$ *um grupo,* $d_{\mathbf{G}}$ *uma métrica sobre* $\mathbf{G}$ *e* $\mathbf{C}$ *um código binário de comprimento n em* $(\mathbb{Z}_2^n, d_H)$. *Diremos que* $\mathbf{C}$ *é* $\mathbf{G}$*-linear, se a menos de uma permutação de coordenadas,* $\mathbf{C} = \psi(\widehat{\mathbf{C}})$ *para algum subgrupo* $\widehat{\mathbf{C}}$ *de* $\mathbf{G}^n$ *e* $\psi : \mathbf{G}^n \to \mathbb{Z}_2^{kn}$ *para* $k \geq 2$ *é uma isometria.*

Teorema 3.3.1 [2] *Um código binário* $\mathbf{C}$ *é propelinear se, e somente se, existir um subgrupo* $\mathbf{N}$ *de* $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$ *cuja ação sobre* $\mathbf{C}$ *é* fortemente transitiva.

Prova. Suponha que $\mathbf{C} \subseteq \mathbb{Z}_2^n$ seja um código propelinear. Por definição temos que $(\Omega(\pi), \star)$ é um subgrupo de $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$. A identificação natural de $(\Omega(\pi), \star)$ com $\mathbf{C}$, induz uma ação *fortemente transitiva* de $(\Omega(\pi), \star)$ sobre $\mathbf{C}$. A recíproca é evidente. ■

Corolário 3.3.1 [2] *Todo código* $\mathbf{G}$*-linear binário é um código propelinear binário.*

Prova. Basta ver que $\mathbf{G} \cong \mathcal{G}(\mathbb{Z}_2^n)$ é um subgrupo de $\Gamma(\mathbb{Z}_2^n) \cong \mathbb{Z}_2^n \rtimes \mathbf{S}_n$. ■

Exemplo 3.3.1 *Considere* $\pi : \mathbb{Z}_2^2 \to \mathbf{S}_2$, *tal que* $(\Omega(\pi), *)$ *seja um subgrupo de* $\mathbb{Z}_2^2 \rtimes \mathbf{S}_2$, *quer dizer, o código propelinear dado por:*

$\mathbf{v}$	$\pi_{\mathbf{v}}$
00	id
11	id
01	(12)
10	(12)

Note que $(\Omega(\pi), *)$ *é um subgrupo de* $\mathbb{Z}_2^2 \rtimes \mathbf{S}_2 \cong \Gamma(\mathbb{Z}_2^2) \cong \mathbb{D}_4$, *gerado por* $(\mathbf{v}, \pi_{\mathbf{v}}) = ((01), (12))$, *ou seja,* $(\Omega(\pi), *) = \langle 01, (12) \rangle \cong \mathbb{Z}_4$. *Como a ação de* $\mathbb{Z}_4$ *sobre* $\mathbb{Z}_2^2$ *é* fortemente transitiva, *obtemos os códigos* $\mathbb{Z}_4$*-lineares.*

Exemplo 3.3.2 *Considere* $\pi : \mathbb{Z}_2^3 \to \mathbf{S}_3$, *tal que* $(\Omega(\pi), *)$ *seja um subgrupo de* $\mathbb{Z}_2^3 \rtimes \mathbf{S}_3 \cong \Gamma(\mathbb{Z}_2^3)$, *quer dizer, o código propelinear dado por:*

$\mathbf{v}$	$\pi_{\mathbf{v}}$
000	id
011	id
100	id
111	id
001	(23)
010	(23)
101	(23)
110	(23)

Observe que o subgrupo$(\Omega(\pi), *) = \langle (100, id), (110, (23)) \rangle$, *é isomorfo ao produto direto* $\mathbb{Z}_2 \times \mathbb{Z}_4$. *Além disso, a ação de* $(\Omega(\pi), *)$ *é* fortemente transitiva *sobre* $\mathbb{Z}_2^3$. *Portanto, desse código propelinear obtemos códigos* $\mathbb{Z}_2 \times \mathbb{Z}_4$*-lineares.*

Exemplo 3.3.3 *Considere* $\pi : \mathbb{Z}_2^3 \to \mathbf{S}_3$, *tal que* $(\Omega(\pi), *)$ *seja um subgrupo de*

$\mathbb{Z}_2^3 \rtimes \mathbf{S}_3 \cong \Gamma(\mathbb{Z}_2^3)$, *quer dizer, o código propelinear dado por:*

$\mathbf{v}$	$\pi_{\mathbf{v}}$
000	id
011	id
101	id
110	id
001	(23)
010	(23)
100	(23)
111	(23)

Note que $(\Omega(\pi), *) = \langle (110, id), (100, (23)) \rangle \cong \mathbb{D}_4$. *Vemos que a ação de* $(\Omega(\pi), *)$ *é* fortemente transitiva *sobre* $\mathbb{Z}_2^3$. *Portanto, desse código propelinear obtemos códigos* $\mathbb{D}_4$*-lineares.*

Exemplo 3.3.4 *A recíproca do Corolário* 3.3.1 *não é verdadeira. Com efeito, considere* $\pi : \mathbb{Z}_2^4 \to \mathbf{S}_4$, *tal que* $(\Omega(\pi), *)$ *seja o subgrupo de* $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4 \cong \Gamma(\mathbb{Z}_2^4)$, *quer dizer, o código propelinear dado por:*

$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id
1111	id
0101	(12)(34)
1010	(12)(34)
0110	(13)(24)
1001	(13)(24)
0011	(14)(23)
1100	(14)(23)

Neste caso, vemos que $(\Omega(\pi), *) \cong \mathbb{Q}_8$ *e como não existe uma ação* fortemente transitiva *de* $\mathbb{Q}_8$ *sobre* $\mathbb{Z}_2^4$, *não podemos obter códigos* $\mathbb{Q}_8$*-lineares.*

Exemplo 3.3.5 *Considere o subgrupo de* $\Gamma(\mathbb{Z}_2^4)$ *dado por*

$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id	0010	(24)
0001	id	0011	(24)
0100	id	0110	(24)
0101	id	0111	(24)
1010	id	1000	(24)
1011	id	1001	(24)
1110	id	1100	(24)
1111	id	1101	(24)

Esse código propelinear é isomorfo a $\mathbb{D}_4 \times \mathbb{Z}_2$ *e sua ação sobre* $\mathbb{Z}_2^4$ *é* fortemente transitiva. *Portanto, desse código podemos obter códigos* $\mathbb{D}_4 \times \mathbb{Z}_2$*-lineares.*

Exemplo 3.3.6 *Considere o subgrupo de* $\Gamma(\mathbb{Z}_2^4)$ *dado por*

$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id	0011	(13) (24)
0110	id	0101	(13) (24)
1001	id	1010	(13) (24)
1111	id	1100	(13) (24)
0011	(12) (34)	0000	(14) (23)
0101	(12) (34)	0110	(14) (23)
1010	(12) (34)	1001	(14) (23)
1100	(12) (34)	1111	(14) (23)

Esse código propelinear é isomorfo a $\mathbb{D}_4 \times \mathbb{Z}_2$ *, mas sua ação sobre* $\mathbb{Z}_2^4$ *não é* fortemente transitiva, *pois*

$$\text{Orb}_{\mathbb{D}_4 \times \mathbb{Z}_2}(0000) = \{0000, 0110, 1001, 1111, 0011, 0101, 1010, 1100\} \neq \mathbb{Z}_2^4.$$

Logo, não podemos obter códigos $\mathbb{D}_4 \times \mathbb{Z}_2$ *-lineares.*

Exemplo 3.3.7 *Considere o subgrupo de* $\Gamma(\mathbb{Z}_2^4)$ *dado por*

$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id	0000	(12)
0011	id	0011	(12)
1100	id	1100	(12)
1111	id	1111	(12)
0001	(34)	0001	(12) (34)
0010	(34)	0010	(12) (34)
1101	(34)	1101	(12) (34)
1110	(34)	1110	(12) (34)

Esse código propelinear é isomorfo a $\mathbb{Z}_2^2 \times \mathbb{Z}_4$ *, mas sua ação sobre* $\mathbb{Z}_2^4$ *não é* fortemente transitiva, *pois*

$$\text{Orb}_{\mathbb{Z}_2^2 \times \mathbb{Z}_4}(0000) = \{0000, 0011, 1100, 1111, 0001, 0010, 1101, 1110\} \neq \mathbb{Z}_2^4.$$

Logo, não podemos obter códigos $\mathbb{Z}_2^2 \times \mathbb{Z}_4$*-lineares.*

Exemplo 3.3.8 *Em [32], foi demonstrado que a estrutura linear é a única estrutura propelinear que possuem os códigos binários de Golay* G_{23} *e de Golay estendido* G_{24} *com parâmetros* $(23, 12, 7)$ *e* $(24, 12.8)$*, respectivamente. Pelo Corolário* 3.3.1*, podemos afirmar que os códigos* G_{23} *e* G_{24} *não são* **G***-lineares.*

3.4 Relação entre os Códigos Propelineares Invariantes por Translação e G-Lineares

Já vimos que os códigos propelineares e G-lineares binários fazem parte da mesma decomposição do grupo de simetrias $\Gamma(\mathbb{Z}_2^n)$. Os códigos propelineares invariantes por translação são códigos propelineares cuja ação sobre $\mathbb{Z}_2^n$ preserva a distância de Hamming. Como a ação de um grupo sobre um conjunto é uma ligeira generalização

do grupo de simetrias desse conjunto, isto nos leva a procura de códigos propelineares invariantes por translação em conjunto de sinais que sejam geometricamente uniformes. Explorando estas noções trataremos de dar uma caracterização mais abrangente dos códigos G-lineares.

Proposição 3.4.1 *Seja* $\mathbf{C} \subseteq \mathbb{Z}_2^n$ *um código propelinear de comprimento* n. *Se* $\mathbf{C}$ *for invariante por translação, então o estabilizador* $\mathrm{Stab}_{\mathbf{C}}(\mathbf{x}) = \{(\mathbf{0}, id)\}$, *para todo* $\mathbf{x} \in \mathbb{Z}_2^n$.

Prova. Pela identificação natural de $\mathbf{C}$ com $(\Omega(\pi), *)$ temos que

$$\mathrm{Stab}_{\Omega(\pi)}(\mathbf{x}) = \{(\mathbf{v}, \pi_{\mathbf{v}}) \in (\Omega(\pi), *) : (\mathbf{v}, \pi_{\mathbf{v}})(\mathbf{x}) = \mathbf{v} * \mathbf{x} = \mathbf{x}\}.$$

Como $\mathbf{C}$ é invariante por translação,

$$\mathbf{v} * \mathbf{x} = \mathbf{x} \Rightarrow 0 = d_H(\mathbf{x}, \mathbf{v} * \mathbf{x}) = \mathbf{w}_H(\mathbf{v}),$$

isto implica que $\mathbf{v} = 0, \forall \mathbf{x} \in \mathbb{Z}_2^n$, ou seja, $(\mathbf{v}, \pi_{\mathbf{v}}) = (\mathbf{0}, id)$. ∎

Exemplo 3.4.1 *Os códigos dos Exemplos* 3.1.2 *e* 3.1.3 *são códigos propelineares invariantes por translação. Logo,* $\mathrm{Stab}_{\mathbf{C}}(\mathbf{x}) = \{(\mathbf{0}, id)\}$.

Exemplo 3.4.2 *A recíproca da Proposição* 3.4.1 *não é verdadeira, pois basta considerar o código propelinear*

$\mathbf{v}$	$\pi_{\mathbf{v}}$
000	id
001	id
100	id
101	id
010	(13)
011	(13)
110	(13)
111	(13)

Para todo $\mathbf{x} \in \mathbb{Z}_2^3$ *temos que* $\mathrm{Stab}_{\mathbf{C}}(\mathbf{x}) = \{(\mathbf{0}, id)\}$. *Esse código não é invariante por translação, visto que* $wt_H(010) = 1$, *enquanto* $d_H(011, 010 \star 011) = 3$.

Exemplo 3.4.3 *Consideremos os seguintes códigos de comprimento $n = 4$:*

$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id
1111	id
0110	(12) (34)
1001	(12) (34)
0011	(13) (24)
1100	(13) (24)
0101	(14) (23)
1010	(14) (23)

$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id
0011	id
1100	id
1111	id
0101	(12) (34)
0110	(12) (34)
1001	(12) (34)
1010	(12) (34)

Estes são códigos propelineares invariantes por translação isomorfos a $\mathbb{Q}_8$ e a $\mathbb{Z}_2 \times \mathbb{Z}_4$, respectivamente. Portanto, seus estabilizadores são dados por

$$\mathrm{Stab}_{\mathbb{Q}_8}(\mathbf{x}) = \mathrm{Stab}_{\mathbb{Z}_2 \times \mathbb{Z}_4}(\mathbf{x}) = \{(\mathbf{0}, id)\}.$$

Exemplo 3.4.4 *Sejam os códigos de comprimento $n = 4$:*

$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id
1111	id
0011	(12) (34)
1100	(12) (34)
0110	(13) (24)
1001	(13) (24)
0101	(14) (23)
1010	(14) (23)

$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id
0100	id
1000	id
1100	id
0010	(12)
0110	(12)
1010	(12)
1110	(12)

O primeiro código propelinear é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$, com

$$\mathrm{Stab}_{\mathbb{Z}_2 \times \mathbb{Z}_4}(0111) = \{(\mathbf{0}, id), (1100, (12)(34))\} \neq \{(\mathbf{0}, id)\}.$$

Escolhendo $\mathbf{v} = 0011$ *e* $\mathbf{x} = 0111$, *vemos que esse código não é invariante por translação. O segundo código propelinear é isomorfo a* $\mathbb{D}_4$ *e tem* $\mathrm{Stab}_{\mathbb{Z}_2 \times \mathbb{Z}_4}(\mathbf{x}) = \{(\mathbf{0}, id)\}$, *para todo* $\mathbf{x}$ *em* $\mathbb{Z}_2^4$. *Tomando* $(\mathbf{v}, \pi_{\mathbf{v}}) = (1110, (12))$ *e* $\mathbf{x} = 0110$, *vemos que o mesmo também não é invariante por translação, pois* $wt_H(\mathbf{v}) \neq d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x})$.

Exemplo 3.4.5 *Considere o código de comprimento* $n = 5$

$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$
00000	id	00110	(24) (35)
01111	id	01001	(24) (35)
10000	id	10110	(24) (35)
11111	id	11001	(24) (35)
00101	(23) (45)	10011	(25) (34)
01010	(23) (45)	01100	(25) (34)
10101	(23) (45)	10011	(25) (34)
11010	(23) (45)	11100	(25) (34)

Este é um código propelinear invariante por translação isomorfo a $\mathbb{Z}_2 \times \mathbb{Q}_8$ *do tipo* $(1, 0, 1)$. *Logo,* $\mathrm{Stab}_{\mathbb{Z}_2 \times \mathbb{Q}_8}(\mathbf{x}) = \{(\mathbf{0}, id)\}$, *para todo* $\mathbf{x} \in \mathbb{Z}_2^5$.

Teorema 3.4.1 *Seja* $\mathbf{C}$ *um código propelinear invariante por translação de comprimento* n, *com* $|\mathbf{C}| = 2^n$, *para* $n \geq 2$, *então* $\mathbf{C}$ *é um código* $\mathbf{G}$*-linear.*

Prova. Como $\mathbf{C}$ é propelinear invariante por translação, isto implica que podemos identificar $\mathbf{C}$ com um subgrupo $\mathbf{G} = (\Omega(\pi), *)$ de $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$. Dessa identificação obtemos uma ação *fortemente transitiva* de $\mathbf{G}$ sobre $\mathbf{C}$. Pela Proposição 3.4.1, podemos afirmar que $|\mathbf{G}| = |\mathbf{C}| = 2^n$. ∎

Corolário 3.4.1 *Não existe códigos propelineares cíclicos invariantes por translação de comprimento* n, *cuja ordem seja* 2^n *para* $n > 2$.

Prova. Suponha que exista códigos $\mathbb{Z}_{2^n}$-lineares. Isto equivale a dizer que $\mathbb{Z}_{2^n}$ é isomorfo a um subgrupo cíclico $\mathbf{G} = \langle(\mathbf{v}, \pi_{\mathbf{v}})\rangle$ de $\Gamma(\mathbb{Z}_2^n)$ tal que $(\mathbf{v}, \pi_{\mathbf{v}}) \in \Gamma(\mathbb{Z}_2^n)$ e cuja

ação é *fortemente transitiva* sobre $\mathbb{Z}_2^n$. Tendo que

$$(\mathbf{v}, \pi_{\mathbf{v}})^n = \left(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{v}) \oplus \pi_{\mathbf{v}}^2(\mathbf{v}) \oplus \pi_{\mathbf{v}}^3(\mathbf{v}) \oplus \cdots \oplus \pi_{\mathbf{v}}^{n-1}(\mathbf{v}), id\right) = (\mathbf{v}^n, id)$$

e como cada vetor de $\mathbf{v}^n$ é um deslocamento cíclico das coordenadas de $\mathbf{v}$, temos que $(\mathbf{v}, \pi_{\mathbf{v}})^n = (\mathbf{0}, id)$ ou $(\mathbf{v}, \pi_{\mathbf{v}})^n = (\mathbf{1}, id)$. Se $(\mathbf{v}, \pi_{\mathbf{v}})^n = (\mathbf{0}, id)$, então $|\mathbf{G}| = n = 2^n$, logo não existe inteiro n que verifique esta igualdade. Se $(\mathbf{v}, \pi_{\mathbf{v}})^n = (\mathbf{1}, id)$, isto significa que $(\mathbf{v}, \pi_{\mathbf{v}})^{2n} = (\mathbf{0}, id)$, então $|\mathbf{G}| = 2n = 2^n$, neste caso temos $n = 1$ ou $n = 2$, como possíveis valores de n. ■

Teorema 3.4.2 *Sejam* $\mathbf{G}$ *um grupo,* $d_{\mathbf{G}}$ *uma métrica sobre* $\mathbf{G}$ *e* $\mathbf{C}$ *um código binário de comprimento* n *em* $(\mathbb{Z}_2^n, d_H)$. *O código* $\mathbf{C}$ *é* $\mathbf{G}$*-linear se, e somente se,* $\mathrm{Stab}_{\mathbf{G}}(\mathbf{x}) = \mathbf{Id}$, *para todo* $\mathbf{x} \in \mathbb{Z}_2^n$.

Prova. Seja $\mathbf{C}$ um código $\mathbf{G}$-linear, isto é equivalente a dizer que $\mathbf{G}$ é isomorfo a um subgrupo de $\Gamma(\mathbb{Z}_2^n)$, tal que $\mathrm{Orb}_{\mathbf{G}}(x) = \mathbb{Z}_2^n$ e $|\mathbf{G}| = |\mathbb{Z}_2^n|$, para todo $\mathbf{x} \in \mathbb{Z}_2^n$, $n \geq 2$. Equivalentemente, de

$$|\mathbf{G}| = |\mathrm{Stab}_{\mathbf{G}}(\mathbf{x})| \, |\mathrm{Orb}_{\mathbf{G}}(\mathbf{x})|,$$

obtemos que $|\mathrm{Stab}_{\mathbf{G}}(\mathbf{x})| = 1$, ou seja, $\mathrm{Stab}_{\mathbf{G}}(\mathbf{x}) = \mathbf{Id}$. ■

Exemplo 3.4.6 *Considere* $\pi : \mathbb{Z}_2^n \to \mathbf{S}_n$, *tal que* $(\Omega(\pi), *)$ *seja um subgrupo de* $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$, *quer dizer um código propelinear, dado por.*

1. *Para* $n = 4$

$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id	0100	(12)
0001	id	0101	(12)
0010	id	0110	(12)
0011	id	0111	(12)
1100	id	1000	(12)
1101	id	1001	(12)
1110	id	1010	(12)
1111	id	1011	(12)

Temos que $(\Omega(\pi), *) \cong \mathbb{Z}_2^2 \times \mathbb{Z}_4$, *ou seja, um código* $\mathbb{Z}_2^2 \times \mathbb{Z}_4$*-linear o qual é propelinear invariante por translação.*

2. *Para* $n = 4$

$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$
0000	id	0001	(13)
1111	id	1110	(13)
0111	(24)	0011	(13)(24)
1000	(24)	1100	(13)(24)
0110	(12)(34)	0100	(1423)
1001	(12)(34)	1011	(1423)
0010	(1234)	0101	(14)(23)
1101	(1234)	1010	(14)(23)

Neste caso temos um código $\mathbb{Q}\mathbb{D}_8$*-linear, ou seja,* $(\Omega(\pi), *)$ *é isomorfo ao grupo* quasidiedral *de ordem 16. Tomando* $\mathbf{x} = 0001$ *e* $(\mathbf{v}, \pi_{\mathbf{v}}) = (1110, (13))$, *vemos que esse código propelinear não é invariante por translação, pois* $wt_H(\mathbf{v}) \neq d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x})$.

3. *Para* $n = 5$

$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$
00000	id	11000	id	01000	(12)	10000	(12)
00001	id	11001	id	01001	(12)	10001	(12)
00010	id	11010	id	01010	(12)	10010	(12)
00011	id	11011	id	01011	(12)	10011	(12)
00100	id	11100	id	01100	(12)	10100	(12)
00101	id	11101	id	01101	(12)	10101	(12)
00110	id	11110	id	01110	(12)	10110	(12)
00111	id	11111	id	01111	(12)	10111	(12)

Temos um código propelinear invariante por translação, onde $(\Omega(\pi), *) \cong \mathbb{Z}_2^3 \times \mathbb{Z}_4$ *e, portanto,* $\mathbb{Z}_2^3 \times \mathbb{Z}_4$*-linear.*

4. *Para* $n = 5$

$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$	$\mathbf{v}$	$\pi_{\mathbf{v}}$
00000	id	00001	(34)	01000	(12)	01001	(12)(34)
00011	id	00010	(34)	01011	(12)	01010	(12)(34)
00100	id	00101	(34)	01100	(12)	01101	(12)(34)
00111	id	00110	(34)	01111	(12)	01110	(12)(34)
11000	id	11001	(34)	10000	(12)	10001	(12)(34)
11011	id	11010	(34)	10011	(12)	10010	(12)(34)
11100	id	11101	(34)	10100	(12)	10101	(12)(34)
11111	id	11110	(34)	10111	(12)	10110	(12)(34)

Obtemos um código $\mathbb{Z}_2 \times \mathbb{Z}_4^2$*-linear. Esse código propelinear não é invariante por translação, pois para* $(\mathbf{v}, \pi_{\mathbf{v}}) = (01110, (12)(34))$ *e* $\mathbf{x} = 01010$ *temos que* $wt_H(\mathbf{v}) \neq d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x})$.

Observação 3.4.1 *O Teorema* 3.4.1 *é um resultado importante na classificação de códigos G-lineares, em virtude da ampla classificação dos códigos propelineares invariantes por translação como subgrupos de*

$$\mathbb{Z}_2^{k_1} \times \mathbb{Z}_4^{k_2} \times \mathbb{Q}_8^{k_3}.$$

Vemos também que podemos obter este teorema através de uma combinação da Proposição 3.4.1 *e do Teorema* 3.4.2.

3.5 Tabelas de Códigos

Dividiremos esta seção em três subseções, nas quais apresentaremos tabelas de códigos propelineares invariantes por translação, de códigos **G**-lineares e de códigos propelineares invariantes por translação do tipo (k_1, k_2, k_3), para alguns valores específicos de n. Estas tabelas são decorrentes dos procedimentos estabelecidos anteriormente. Representaremos tais códigos como subgrupos de $\mathbb{Z}_2^k \rtimes \mathbf{S}_k$ gerado por um ou mais elementos, e identificaremos cada um destes códigos como sendo um grupo de rótulos $\mathcal{R}$.

3.5.1 Tabelas de Códigos Propelineares Invariantes por Translação

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^2 \rtimes \mathbf{S}_2$**
$Id = \{(00, id)\}$	$\langle (00, id) \rangle$
$\mathbb{Z}_2$	$\langle (11, id) \rangle = \langle (01, id) \rangle = \langle (10, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (01, id), (10, id) \rangle$
$\mathbb{Z}_4$	$\langle (01, (12)) \rangle$

Tabela 3.2: Tabela de códigos em $\mathbb{Z}_2^2 \rtimes \mathbf{S}_2$

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de** $\mathbb{Z}_2^3 \rtimes \mathbf{S}_3$
$\mathbf{Id} = \{(000, id)\}$	$\langle (000, id) \rangle$
$\mathbb{Z}_2$	$\langle (111, id) \rangle = \langle (001, id) \rangle = \langle (010, id) \rangle = \langle (100, id) \rangle$
$\mathbb{Z}_2$	$\langle (011, id) \rangle = \langle (101, id) \rangle = \langle (110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (011, id), (110, id) \rangle = \langle (001, id), (011, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (001, id), (101, id) \rangle = \langle (010, id), (110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (001, id), (111, id) \rangle = \langle (010), (111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (011, id), (111, id) \rangle$
$\mathbb{Z}_4$	$\langle (001, (23)) \rangle = \langle (001, (13)) \rangle$
$\mathbb{Z}_4$	$\langle (010, (12)) \rangle = \langle (101, (23)) \rangle$
$\mathbb{Z}_4$	$\langle (011, (13)) \rangle = \langle (011, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (001, id), (010, id), (100, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (001, id), (100, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (010, id), (100, (13)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (100, id), (110, (23)) \rangle$

Tabela 3.3: Tabela de códigos em $\mathbb{Z}_2^3 \rtimes \mathbf{S}_3$

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$\mathbf{Id} = \{(0000, id)\}$	$\langle (0000, id) \rangle$
$\mathbb{Z}_2$	$\langle (1111, id) \rangle = \langle (0001, id) \rangle = \langle (0010, id) \rangle = \langle (0100, id) \rangle$
$\mathbb{Z}_2$	$\langle (1000, id) \rangle = \langle (0111, id) \rangle = \langle (1011, id) \rangle = \langle (1101, id) \rangle$
$\mathbb{Z}_2$	$\langle (1110, id) \rangle = \langle (0011, id) \rangle = \langle (0101, id) \rangle = \langle (0110, id) \rangle$
$\mathbb{Z}_2$	$\langle (1001, id) \rangle = \langle (1010, id) \rangle = \langle (1100, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0011, id), (1111, id) \rangle = \langle (0101, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0110, id), (1111, id) \rangle = \langle (0001, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0010, id), (1111, id) \rangle = \langle (0100, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0111, id), (1111, id) \rangle = \langle (0011, id), (0110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0011, id), (1010, id) \rangle = \langle (0101, id), (1100, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0110, id), (1100, id) \rangle = \langle (0001, id), (0011, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (0101, id) \rangle = \langle (0001, id), (1100, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0010, id), (0110, id) \rangle = \langle (0010, id), (1010, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0100, id), (1100, id) \rangle$
$\mathbb{Z}_4$	$\langle (1101, (34)) \rangle = \langle (1011, (24)) \rangle = \langle (1011, (23)) \rangle$
$\mathbb{Z}_4$	$\langle (0111, (14)) \rangle = \langle (1101, (13)) \rangle = \langle (1011, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0011, id), (1110, id) \rangle = \langle (0101, id), (1110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0110, id), (1101, id) \rangle = \langle (0111, id), (1110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0111, id), (1101, id) \rangle = \langle (0111, id), (1100, id) \rangle$
$\mathbb{Z}_4$	$\langle (0001, (24)) \rangle = \langle (0100, (23)) \rangle = \langle (0001, (14)) \rangle$
$\mathbb{Z}_4$	$\langle (0010, (13)) \rangle = \langle (0100, (12)) \rangle = \langle (0101, (12)(34)) \rangle$
$\mathbb{Z}_4$	$\langle (0110, (12)(34)) \rangle = \langle (0011, (13)(24)) \rangle$

Tabela 3.4: Tabela de códigos em $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$\mathbb{Z}_4$	$\langle (0110, (1,3)(2,4)) \rangle = \langle (0011, (1,4)(2,3)) \rangle$
$\mathbb{Z}_4$	$\langle (0101, (1,4)(2,3)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (0111, id) \rangle = \langle (0001, id), (1011, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (1101, id) \rangle = \langle (0010, id), (0111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0010, id), (1011, id) \rangle = \langle (0010, id), (1110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0011, id), (0111, id) \rangle = \langle (0011, id), (1011, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0100, id), (1101, id) \rangle = \langle (0100, id), (1110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0101, id), (1101, id) \rangle = \langle (0110, id), (1110, id) \rangle$
$\mathbb{Z}_4$	$\langle (0101, (34)) \rangle = \langle (1001, (34)) \rangle = \langle (0011, (24)) \rangle$
$\mathbb{Z}_4$	$\langle (1001, (24)) \rangle = \langle (0011, (23)) \rangle = \langle (1010, (23)) \rangle$
$\mathbb{Z}_4$	$\langle (0011, (14)) \rangle = \langle (0101, (14)) \rangle = \langle (0011, (13)) \rangle$
$\mathbb{Z}_4$	$\langle (0110, (13)) \rangle = \langle (0101, (12)) \rangle = \langle (0110, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0011, id), (1010, id), (1111, id) \rangle$
$\mathbb{Q}_8$	$\langle (1010, (12)(34)), (1001, (13)(24)) \rangle$
$\mathbb{Q}_8$	$\langle (1001, (12)(34)), (1010, (14)(23)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1001, (12)(34)), (1010, (12)(34)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1001, (13)(24)), (1100, (13)(24)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1010, (14)(23)), (1100, (14)(23)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (0101, id), (0111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (1001, id), (1011, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (1001, id), (1101, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0010, id), (1000, id), (1110, id) \rangle$

Tabela 3.5: Continuação da Tabela 3.4

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (1011, id), (1101, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0010, id), (1001, id), (1110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0011, id), (1001, id), (1110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0011, id), (1011, id), (1110, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0110, (34)), (1010, (34)) \rangle = \langle (0101, (12)), (1010, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0110, (24)), (1100, (24)) \rangle = \langle (0011, (13)), (1100, (13)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0101, (23)), (1100, (23)) \rangle = \langle (0011, (14)), (1100, (14)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (1101, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (1011, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0001, id), (1001, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0010, id), (1011, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0010, id), (1010, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (0011, id), (1011, id), (1111, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0010, (34)), (1110, (34)) \rangle = \langle (0100, (12)), (1011, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0100, (24)), (1110, (24)) \rangle = \langle (0010, (13)), (1101, (13)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0100, (23)), (1101, (23)) \rangle = \langle (0001, (14)), (1110, (14)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0111, id), (1100, (23)) \rangle = \langle (1011, id), (1100, (13)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1101, id), (1010, (12)) \rangle = \langle (0111, id), (1100, (24)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1011, id), (1100, (14)) \rangle = \langle (1110, id), (1001, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0111, id), (1101, (34)) \rangle = \langle (1011, id), (1101, (34)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1101, id), (1010, (14)) \rangle = \langle (1110, id), (1001, (13)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1101, id), (1011, (24)) \rangle = \langle (1110, id), (1011, (23)) \rangle$

Tabela 3.6: Continuação da Tabela 3.5

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0111, id), (1001, (34)) \rangle = \langle (1011, id), (1000, (13)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1101, id), (1000, (12)) \rangle = \langle (0111, id), (0100, (24)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1011, id), (1000, (14)) \rangle = \langle (1110, id), (1000, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (0111, id), (0101, (34)) \rangle = \langle (1011, id), (1001, (34)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1101, id), (1100, (14)) \rangle = \langle (1110, id), (1000, (13)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (1101, id), (1001, (24)) \rangle = \langle (1110, id), (1010, (23)) \rangle$
$\mathbb{Z}_2^4$	$\langle (0001, id), (0110, id), (1100, id), (1111, id) \rangle$
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\langle (0111, (12)), (1010, (12)(34)) \rangle$
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\langle (0111, (13)), (1100, (13)(24)) \rangle$
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\langle (0111, (14)), (1100, (1,4)(23)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0110, (12)), (1011, (12)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0110, (13)), (1101, (13)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0101, (23)), (1101, (23)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0101, (14)), (1110, (14)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0110, (24)), (1110, (24)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0110, (34)), (1110, (34)) \rangle$

Tabela 3.7: Continuação da Tabela 3.6

3.6 Tabelas de Códigos G-Lineares

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^2 \rtimes \mathbf{S}_2$**
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (01, id), (11, id) \rangle$
$\mathbb{Z}_4$	$\langle (01, (12)) \rangle$

Tabela 3.8: Tabela de códigos em $\mathbb{Z}_2^2 \rtimes \mathbf{S}_2$

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^3 \rtimes \mathbf{S}_3$**
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle (001, id), (010, id), (100, id) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (001, id), (100, (12)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (010, id), (100, (13)) \rangle$
$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\langle (100, id), (110, (23)) \rangle$
$\mathbb{D}_8$	$\langle (110, id), (100, (23)) \rangle$
$\mathbb{D}_8$	$\langle (101, id), (100, (12)) \rangle$
$\mathbb{D}_8$	$\langle (011, id), (100, (13)) \rangle$

Tabela 3.9: Tabela de códigos em $\mathbb{Z}_2^3 \rtimes \mathbf{S}_3$

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$\mathbb{Z}_2^4$	$\langle (0001, id), (0110, id), (1100, id), (1111, id) \rangle$
$\mathcal{H}_1$	$\langle (0011, id), (0100, (12)(34)), (1110, (12)(34)) \rangle$
$\mathcal{H}_2$	$\langle (0011, id), (0100, (13)(24)), (1110, (13)(24)) \rangle$
$\mathcal{H}_3$	$\langle (0011, id), (0010, (14)(23)), (1110, (14)(23)) \rangle$

Tabela 3.10: Tabela de códigos em $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$

3.7 Tabelas de Códigos Propelineares Invariantes por Translação por Tipo:

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\langle (0111, (12)), (1010, (12)(34)) \rangle$
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\langle (0111, (13)), (1100, (13)(24)) \rangle$
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\langle (0111, (14)), (1100, (14)(23)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0011, id), (0001, (12)), (1010, (12)(34)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0101, id), (0001, (13)), (1100, (13)(24)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0110, id), (0010, (14)), (110, (14)(23)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0110, (34)), (1010, (34)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0110, (24)), (1100, (24)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0011, (14)), (1100, (14)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0010, id), (0101, (23)), (1100, (23)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0010, id), (0011, (13)), (1100, (13)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0011, id), (0101\,(12)), (1101, (, 2)) \rangle$
$\mathcal{H}_4$	$\langle (0001, id), (0101, (12)(34)), (1011, (12)(34)) \rangle$
$\mathcal{H}_5$	$\langle (0001, id), (0011, (13)(24)), (1101, (13)(24)) \rangle$
$\mathcal{H}_6$	$\langle (0001, id), (0100, (14)(23)), (1101, (14)(23)) \rangle$
$\mathcal{H}_7$	$\langle (0010, id), (0101, (14)(23)), (1110, (14)(23)) \rangle$
$\mathcal{H}_8$	$\langle (0010, id), (0100, (13)(24)), (1110, (13)(24)) \rangle$
$\mathcal{H}_9$	$\langle (0011, id), (0101, (1,2)(3,4)), (1110, (1,2)(3,4)) \rangle$

Tabela 3.11: Continuação da Tabela 3.10

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$[(\mathbb{Z}_2 \times \mathbb{Z}_4) . \mathbb{Z}_2]$	$\langle (0011, id), (1110, (34)), (1000, (12)(34)) \rangle$
$[(\mathbb{Z}_2 \times \mathbb{Z}_4) . \mathbb{Z}_2]$	$\langle (0011, id), (1010, (34)), (1101, (12)(34)) \rangle$
$[(\mathbb{Z}_2 \times \mathbb{Z}_4) . \mathbb{Z}_2]$	$\langle (0101, id), (1110, (24)), (1000, (13)(24)) \rangle$
$[(\mathbb{Z}_2 \times \mathbb{Z}_4) . \mathbb{Z}_2]$	$\langle (0101, id), (1100, (24)), (1011, (13)(24)) \rangle$
$[(\mathbb{Z}_2 \times \mathbb{Z}_4) . \mathbb{Z}_2]$	$\langle (0110, id), (1101, (23)), (1000, (14)(23)) \rangle$
$[(\mathbb{Z}_2 \times \mathbb{Z}_4) . \mathbb{Z}_2]$	$\langle (0110, id), (1100, (23)), (1011, (14)(23)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0110, (12)), (1011, (12)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0110, (13)), (1101, (13)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0101, (23)), (1101, (23)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0101, (14)), (1110, (14)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0110, (24)), (1110, (24)) \rangle$
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\langle (1111, id), (0110, (34)), (1110, (34)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0101, id), (0001, (34)), (1110, (34)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0101, id), (0001, (23)), (1110, (23)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0110, id), (0001, (24)), (1101, (24)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0101, id), (0001, (12)), (1110, (12)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0101, id), (0001, (13)), (1110, (13)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0101, id), (0001, (1,4)), (1110, (1,4)) \rangle$
$\mathcal{J}_1$	$\langle (0011, id), (1101, (1324)), (1011, (1423)) \rangle$
$\mathcal{J}_2$	$\langle (0011, id), (1000, (1324)), (1110, (1423)) \rangle$
$\mathcal{J}_3$	$\langle (0101, id), (1001, (13)(24)), (1101, (1432)) \rangle$
$\mathcal{J}_4$	$\langle (0101, id), (1001, (13)(24)), (1110, (1432)) \rangle$

Tabela 3.12: Continuação da Tabela 3.11

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$\mathcal{K}_1$	$\langle (0110, id), (1011, (1342)), (1100, (14)(23)) \rangle$
$\mathcal{K}_2$	$\langle (0110, id), (1000, (1342)), (1100, (14)(23)) \rangle$
$\mathcal{K}_3$	$\langle (0011, id), (1010, (12)), (1110, (12)(34)) \rangle$
$\mathcal{K}_4$	$\langle (0011, id), (1110, (12)), (1011, (12)(34)) \rangle$
$\mathcal{K}_5$	$\langle (0101, id), (1001, (13)), (1110, (13)(24)) \rangle$
$\mathcal{K}_6$	$\langle (0101, id), (1011, (13)), (1101, (13)(24)) \rangle$
$\mathcal{K}_7$	$\langle (0110, id), (1010, (14)), (1101, (14)(23)) \rangle$
$\mathcal{K}_8$	$\langle (0110, id), (1011, (14)), (1110, (14)(23)) \rangle$
$\mathcal{K}_9$	$\langle (0110, id), (1010, (14)), (1101, (14)(23)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (1011, (34)), (1111, (34)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (1011, (23)), (1111, (23)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (1011, (24)), (1111, (24)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0111, (34)), (1111, (34)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0110, (13)), (1111, (13)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0110, (14)), (1111, (14)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0110, (24)), (1111, (24)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0110, (12)), (1111, (12)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0001, id), (0010, (14)), (1111, (14)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0010, id), (0101, (23)), (1111, (23)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0010, id), (0101, (12)), (1111, (12)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0010, id), (0011, (13)), (1111, (13)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (1010, id), (0100, (23)), (1111, (23)) \rangle$

Tabela 3.13: Continuação da Tabela 3.12

Grupo de rótulos: $\mathcal{R}$	**Subgrupos de $\mathbb{Z}_2^4 \rtimes \mathbf{S}_4$**
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (1010, id), (0100, (1,2)), (1111, (1,2)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (1010, id), (0101, (1,3)), (1111, (1,3)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0010, id), (0100, (2,4)), (1111, (2,4)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0010, id), (0100, (1,2)), (1111, (1,2)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0101, id), (0100, (1,4)), (1111, (1,4)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0111, id), (0001, (3,4)), (1100, (3,4)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0011, id), (0010, (1,3)), (1111, (1,3)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0011, id), (0010, (1,4)), (1111, (1,4)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0101, id), (0100, (3,4)), (1111, (3,4)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0011, id), (0100, (2,3)), (1111, (2,3)) \rangle$
$\mathbb{D}_4 \times \mathbb{Z}_2$	$\langle (0011, id), (0100, (2,4)), (1111, (2,4)) \rangle$
$\mathbb{QD}_8$	$\langle (1111, id), (1101, (1324)), (1010, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (1111, id), (1000, (1324)), (1100, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (1111, id), (1011, (1324)), (1100, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (1111, id), (1110, (1324)), (1010, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (0001, (23)), (1001, (13)(24)), (1100, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (0001, (23)), (1100, (13)(24)), (1010, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (0111, (23)), (1001, (13)(24)), (1100, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (0111, (23)), (1100, (13)(24)), (1010, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (0010, (24)), (1001, (13)(24)), (1100, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (0010, (24)), (1100, (13)(24)), (1010, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (0111, (24)), (1001, (13)(24)), (1100, (14)(23)) \rangle$
$\mathbb{QD}_8$	$\langle (0111, (24)), (1100, (13)(24)), (1010, (14)(23)) \rangle$

Tabela 3.14: Continuação da Tabela 3.13

Comprimento	**Tipo** (k_1, k_2, k_3)	**Subgrupo de**
$n = 4$	$(4, 0, 0)$	$\mathbb{Z}_2^4$
	$(2, 1, 0)$	$\mathbb{Z}_2^2 \times \mathbb{Z}_4$
	$(0, 0, 1)$	$\mathbb{Q}_8$

Tabela 3.15: Tabela de códigos para $k_1 + 2k_2 + 4k_3 = 4$

Comprimento	**Tipo** (k_1, k_2, k_3)	**Subgrupo de**
$n = 5$	$(5, 0, 0)$	$\mathbb{Z}_2^5$
	$(3, 1, 0)$	$\mathbb{Z}_2^3 \times \mathbb{Z}_4$
	$(1, 2, 0)$	$\mathbb{Z}_2 \times \mathbb{Z}_4^2$
	$(1, 0, 1)$	$\mathbb{Z}_2 \times \mathbb{Q}_8$

Tabela 3.16: Tabela de códigos para $k_1 + 2k_2 + 4k_3 = 5$

Comprimento	**Tipo** (k_1, k_2, k_3)	**Subgrupo de**
$n = 7$	$(7, 0, 0)$	$\mathbb{Z}_2^7$
	$(5, 1, 0)$	$\mathbb{Z}_2^5 \times \mathbb{Z}_4$
	$(3, 2, 0)$	$\mathbb{Z}_2^3 \times \mathbb{Z}_4^2$
	$(3, 0, 1)$	$\mathbb{Z}_2^3 \times \mathbb{Q}_8$
	$(1, 1, 1)$	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Q}_8$

Tabela 3.17: Tabela de códigos para $k_1 + 2k_2 + 4k_3 = 7$

Comprimento	**Tipo** (k_1, k_2, k_3)	**Subgrupo de**
$n = 8$	$(8, 0, 0)$	$\mathbb{Z}_2^8$
	$(6, 1, 0)$	$\mathbb{Z}_2^6 \times \mathbb{Z}_4$
	$(4, 2, 0)$	$\mathbb{Z}_2^4 \times \mathbb{Z}_4^2$
	$(4, 0, 1)$	$\mathbb{Z}_2^4 \times \mathbb{Q}_8$
	$(2, 3, 0)$	$\mathbb{Z}_2^2 \times \mathbb{Z}_4^3$
	$(2, 1, 1)$	$\mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Q}_8$
	$(0, 4, 0)$	$\mathbb{Z}_4^4$
	$(0, 2, 1)$	$\mathbb{Z}_4^2 \times \mathbb{Q}_8$
	$(0, 0, 2)$	$\mathbb{Q}_8^2$

Tabela 3.18: Tabela de códigos para $k_1 + 2k_2 + 4k_3 = 8$

Comprimento	**Tipo** (k_1, k_2, k_3)	**Subgrupo de**
$n = 11$	$(11, 0, 0)$	$\mathbb{Z}_2^{11}$
	$(9, 1, 0)$	$\mathbb{Z}_2^9 \times \mathbb{Z}_4$
	$(7, 2, 0)$	$\mathbb{Z}_2^7 \times \mathbb{Z}_4^2$
	$(7, 0, 1)$	$\mathbb{Z}_2^7 \times \mathbb{Q}_8$
	$(5, 3, 0)$	$\mathbb{Z}_2^5 \times \mathbb{Z}_4^3$
	$(5, 1, 1)$	$\mathbb{Z}_2^5 \times \mathbb{Z}_4 \times \mathbb{Q}_8$
	$(3, 4, 0)$	$\mathbb{Z}_2^3 \times \mathbb{Z}_4^4$
	$(3, 2, 1)$	$\mathbb{Z}_2^3 \times \mathbb{Z}_4^2 \times \mathbb{Q}_8$
	$(3, 0, 2)$	$\mathbb{Z}_2^3 \times \mathbb{Q}_8^2$
	$(1, 5, 0)$	$\mathbb{Z}_2 \times \mathbb{Z}_4^5$
	$(1, 3, 1)$	$\mathbb{Z}_2 \times \mathbb{Z}_4^3 \times \mathbb{Q}_8$
	$(1, 1, 2)$	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Q}_8^2$

Tabela 3.19: Tabela de códigos para $k_1 + 2k_2 + 4k_3 = 11$

Capítulo 4

Códigos Propelineares m-ários

A propelinearidade demonstrou ser uma técnica eficiente quando utilizada na construção de novos códigos sobre grupos, em face a sua forte ligação com a teoria da decomposição de certos grupos abstratos e de modo geral, com a teoria da extensão de grupos. Acreditamos que essa idéia, venha abrir novos horizontes dentro da teoria da codificação.

Vimos que os códigos propelineares binários contém os códigos lineares e os códigos $\mathbb{Z}_4$-lineares. Conforme [31] alguns códigos não-lineares importantes como por exemplo os códigos de Preparata estendido, Preparata e Delsart-Goethals, também são propelineares. Uma das propriedades mais relevantes da propelinearidade é a de transformar códigos não-lineares em lineares.

Na Seção 4.1 apresentaremos os códigos propelineares m-ários, sob a ótica de uma generalização do caso binário. Nada mais natural de que considerar o alfabeto do código básico como sendo $\mathbb{Z}_m$, o anel dos inteiros módulo m. Sabemos que $\mathbb{Z}_m^n$ munido da métrica de Hamming d_H é um espaço métrico e que um código $\mathbf{C}$ sobre o espaço métrico $(\mathbb{Z}_m^n, d_H)$ é simplesmente um subconjunto não vazio de $\mathbb{Z}_m^n$. Como $(\mathbb{Z}_m^n, +)$ é um grupo abeliano, a distância de Hamming é invariante por translação, isto é, $d_H(x, y) = d_H(x + z, y + z)$ para todo x, y e z em $\mathbb{Z}_m^n$. Geralmente, o que interessa de fato é quando podemos identificar esse código com um grupo e estudar a invariância da métrica sob

a ação do código sobre o espaço métrico $(\mathbb{Z}_m^n, d_H)$. Essa foi uma das principais idéias usadas na classificação dos códigos propelineares invariantes por translação binários. Na Seção 4.2 utilizaremos essa idéia para definir códigos propelineres m-ários invariantes por translação e apresentaremos algumas de suas principais propriedades. Mostraremos que não existem códigos propelineares m-ários invariantes por translação para qualquer inteiro positivo $m \geq 3$. Na Seção 4.3, apresentaremos tabelas de códigos m-ários para $2 \leq m \leq 6$.

4.1 Códigos Propelineares m-ários

Definição 4.1.1 *Seja* $\mathbf{C}$ *um subconjunto de* $\mathbb{Z}_m^n$ *tal que* $\mathbf{0} \in \mathbf{C}$. *Diremos que* $\mathbf{C}$ *é um código* ***propelinear*** m*-ário de comprimento* n *se existir um subconjunto*

$$\Pi = \{\pi_{\mathbf{v}} \in \mathbf{S}_n : \mathbf{v} \in \mathbf{C}\}$$

tal que as seguintes condições são satisfeitas

1. *Para todo* $\mathbf{v} \in \mathbf{C}$, $\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{s}) \in \mathbf{C} \iff \mathbf{s} \in \mathbf{C}$;

2. *Para todo* $\pi_{\mathbf{u}}$, $\pi_{\mathbf{v}} \in \Pi$, $\pi_{\mathbf{u}} \circ \pi_{\mathbf{v}} = \pi_{\mathbf{w}} \in \Pi$, *onde* $\mathbf{w} = \mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v})$.

Essa definição é uma extensão natural do caso binário, só que desta forma a estrutura algébrica na qual se encontra inserida não aparece. Por isso, precisamos estabelecer algumas propriedades que nos permita inseri-la dentro de um contexto algébrico.

Consideremos a função

$$f : \mathbf{S}_n \times \mathbb{Z}_m^n \to \mathbb{Z}_m^n$$

definida por $f(\pi, \mathbf{x}) = \pi(\mathbf{x})$ de modo que

$$\pi(\mathbf{x}) = \pi(x_1, x_2, \ldots, x_n) = \left(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}\right),$$

define uma ação à direita de $\mathbf{S}_n$ sobre o $\mathbb{Z}_m$-módulo $\mathbb{Z}_m^n$ que é a de permutar as coordenadas de qualquer $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_m^n$.

Propriedades Algébricas:

1ª Para cada $\sigma \in \mathbf{S}_n$ e $\mathbf{g} = (g_1, g_2, ..., g_n) \in \mathbb{Z}_m^n$ a aplicação $\phi_\sigma : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ definida por

$$\phi_\sigma(\mathbf{g}) = \sigma(\mathbf{g}) = \left(g_{\sigma^{-1}(1)}, g_{\sigma^{-1}(2)}, \ldots, g_{\sigma^{-1}(n)}\right)$$

é um automorfismo.do $\mathbb{Z}_m$-módulo $\mathbb{Z}_m^n$

De fato: Dados $\mathbf{g}, \mathbf{h} \in \mathbb{Z}_m^n$,

$$\begin{aligned}
\phi_\sigma(\mathbf{g}) &= \phi_\sigma(\mathbf{h}) \Rightarrow \left(g_{\sigma^{-1}(1)}, g_{\sigma^{-1}(2)}, \ldots, g_{\sigma^{-1}(n)}\right) = \left(h_{\sigma^{-1}(1)}, h_{\sigma^{-1}(2)}, \ldots, h_{\sigma^{-1}(n)}\right) \\
&\Rightarrow \quad g_{\sigma^{-1}(1)} = h_{\sigma^{-1}(1)},\ g_{\sigma^{-1}(2)} = h_{\sigma^{-1}(2)}, \ldots,\ g_{\sigma^{-1}(n)} = h_{\sigma^{-1}(n)} \\
&\Rightarrow \quad g_1 = h_1,\ g_2 = h_2, \ldots,\ g_n = h_n \\
&\Rightarrow \quad \mathbf{g} = \mathbf{h}.
\end{aligned}$$

Para qualquer $\mathbf{y} \in \mathbb{Z}_m^n$ existe $\mathbf{x} \in \mathbb{Z}_m^n$ tal que $\phi_\sigma(\mathbf{x}) = \mathbf{y}$, basta tomar

$$\mathbf{x} = \left(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)}\right).$$

Agora, temos que

$$\begin{aligned}
\phi_\sigma(\mathbf{g}) \oplus \phi_\sigma(\mathbf{h}) &= \left(g_{\sigma^{-1}(1)}, g_{\sigma^{-1}(2)}, \ldots, g_{\sigma^{-1}(n)}\right) \oplus \left(h_{\sigma^{-1}(1)}, h_{\sigma^{-1}(2)}, \ldots, h_{\sigma^{-1}(n)}\right) \\
&= \left(g_{\sigma^{-1}(1)} \oplus h_{\sigma^{-1}(1)},\ g_{\sigma^{-1}(2)} \oplus h_{\sigma^{-1}(2)}, \ldots,\ g_{\sigma^{-1}(n)} \oplus h_{\sigma^{-1}(n)}\right) \\
&= \left((g_1 \oplus h_1)_{\sigma^{-1}(1)},\ (g_2 \oplus h_2)_{\sigma^{-1}(2)}, \ldots,\ (g_n \oplus h_n)_{\sigma^{-1}(n)}\right) \\
&= \phi_\sigma\left((g_1 \oplus h_1),\ (g_2 \oplus h_2), \ldots,\ (g_n \oplus h_n)\right) \\
&= \phi_\sigma(\mathbf{g} \oplus \mathbf{h}).
\end{aligned}$$

Portanto, $\phi_\sigma \in \mathrm{Aut}(\mathbb{Z}_m^n)$.

2^{a} Para cada $\sigma \in \mathbf{S}_n$ e $\mathbf{g} = (g_1, g_2, ..., g_n) \in \mathbb{Z}_m^n$, segue-se que

$$\begin{aligned}
\phi_\sigma(-\mathbf{g}) &= \phi_\sigma(-g_1, -g_2, \ldots, -g_n) \\
&= \left(-g_{\sigma^{-1}(1)}, -g_{\sigma^{-1}(2)}, \ldots, -g_{\sigma^{-1}(n)}\right) \\
&= -\left(g_{\sigma^{-1}(1)}, g_{\sigma^{-1}(2)}, \ldots, g_{\sigma^{-1}(n)}\right) \\
&= -\phi_\sigma(g_1, g_2, \ldots, g_n) \\
&= -\phi_\sigma(\mathbf{g}).
\end{aligned}$$

Além disso, para todo $\alpha \in \mathbb{Z}_m$ temos que $\phi_\sigma(\alpha) = \sigma(\alpha) = \alpha$, ou seja, $\phi_\sigma = id$ é a permutação identidade. De qualquer modo, podemos estender essa propriedade: $\phi_\sigma(\alpha g) = \alpha\sigma(g)$.

3^{a} A aplicação $\phi : \mathbf{S}_n \longrightarrow \mathrm{Aut}(\mathbb{Z}_m^n)$ definida por $\phi(\sigma) = \phi_\sigma$, para qualquer $\sigma \in \mathbf{S}_n$ é um homomorfismo injetivo.

De fato: A injetividade de ϕ segue da 2^{a} propriedade. Para cada $\sigma, \pi \in \mathbf{S}_n$ e $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_m^n$, temos que

$$\begin{aligned}
(\phi_\sigma \circ \phi_\pi)(\mathbf{x}) &= \phi_\sigma\left(x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, \ldots, x_{\pi^{-1}(n)}\right) \\
&= \left(x_{\pi^{-1}(\sigma^{-1}(1))}, x_{\pi^{-1}(\sigma^{-1}(2))}, \ldots, x_{\pi^{-1}(\sigma^{-1}(n))}\right) \\
&= \left(x_{(\sigma\circ\pi)^{-1}(1)}, x_{(\sigma\circ\pi)^{-1}}, \ldots, x_{(\sigma\circ\pi)^{-1}(n)}\right) \\
&= \phi_{(\sigma\circ\pi)}(x_1, x_2, \ldots, x_n) \\
&= \phi_{(\sigma\circ\pi)}(\mathbf{x}).
\end{aligned}$$

Observamos que o homomorfismo ϕ é determinado por ϕ_σ e, além disso

$$\phi_\sigma \circ \phi_{\sigma^{-1}} = \phi_{\sigma\circ\sigma^{-1}} = \phi_{id} = Id_{\mathrm{Aut}(\mathbb{Z}_m^n)}, \text{ ou ainda, } \phi_{\sigma^{-1}} = \phi_\sigma^{-1}.$$

Das propriedades anteriores podemos definir o produto semi-direto de $\mathbb{Z}_m^n$ por $\mathbf{S}_n$ determinado por ϕ, que denotamos por $\mathbb{Z}_m^n \rtimes \mathbf{S}_n$, como sendo o conjunto dos pares ordenados

$$\mathbb{Z}_m^n \times \mathbf{S}_n = \{(\mathbf{x}, \pi) : \mathbf{x} \in \mathbb{Z}_m^n \text{ e } \pi \in \mathbf{S}_n\}$$

munido da operação:

$$(\mathbf{x},\pi)\star(\mathbf{y},\tau)=(\mathbf{x}\oplus\phi(\pi)(\mathbf{y}),\pi\circ\tau)=(\mathbf{x}\oplus\phi_{\pi}(\mathbf{y}),\pi\circ\tau).$$

Desta maneira, podemos afirmar que $(\mathbb{Z}_m^n\rtimes\mathbf{S}_n,\star)$ é um grupo. Com efeito :

i. Associatividade: Dados $(\mathbf{x},\sigma),(\mathbf{y},\pi)$ e $(\mathbf{z},\gamma)\in\mathbb{Z}_m^n\rtimes\mathbf{S}_n$, temos que

$$\begin{aligned}
[\ (\mathbf{x},\sigma)\star(\mathbf{y},\pi)]\star(\mathbf{z},\gamma) &= (\mathbf{x}\oplus\phi_{\sigma}(\mathbf{y}),\sigma\circ\pi)\star(\mathbf{z},\gamma)\\
&= (\mathbf{x}\oplus\phi_{\sigma}(\mathbf{y})\oplus\phi_{\sigma\circ\pi}(\mathbf{z}),(\sigma\circ\pi)\circ\gamma)\\
&= (\mathbf{x}\oplus\phi_{\sigma}(\mathbf{y})\oplus(\phi_{\sigma}\circ\phi_{\pi})(\mathbf{z}),\sigma\circ(\pi\circ\gamma))\\
&= (\mathbf{x}\oplus\phi_{\sigma}(\mathbf{y}\oplus\phi_{\pi}(\mathbf{z})),\sigma\circ(\pi\circ\gamma))\\
&= (\mathbf{x},\sigma)\star[\mathbf{y}\oplus\phi_{\pi}(\mathbf{z}),\pi\circ\gamma]\\
&= (\mathbf{x},\sigma)\star[(\mathbf{y},\pi)\star(\mathbf{z},\gamma)];
\end{aligned}$$

ii. Elemento Identidade: Para todo $(\mathbf{x},\sigma)\in\mathbb{Z}_m^n\rtimes\mathbf{S}_n$ existe $(\mathbf{0},id)$ tal que

$$(\mathbf{0},id)\star(\mathbf{x},\sigma)=(\mathbf{0}\oplus\phi_{id}(\mathbf{x}),id\circ\sigma)=(\mathbf{0}\oplus\mathbf{x},id\circ\sigma)=(\mathbf{x},\sigma)$$

e

$$(\mathbf{x},\sigma)\star(\mathbf{0},id)=(\mathbf{x}\oplus\phi_{\sigma}(\mathbf{0}),\sigma\circ id)=(\mathbf{x}\oplus\mathbf{0},\sigma\circ id)=(\mathbf{x},\sigma);$$

iii. Elemento Inverso: Para todo $(\mathbf{x},\sigma)\in\mathbb{Z}_m^n\rtimes\mathbf{S}_n$ existe $(\phi_{\sigma^{-1}}(-\mathbf{x}),\sigma^{-1})$ tal que

$$\begin{aligned}
(\mathbf{x},\sigma)\star\left(\phi_{\sigma^{-1}}(-\mathbf{x}),\sigma^{-1}\right) &= \left(\mathbf{x}\oplus\phi_{\sigma}\left(\phi_{\sigma^{-1}}(-\mathbf{x}),\sigma\circ\sigma^{-1}\right)\right)\\
&= \left(\mathbf{x}\oplus(\phi_{\sigma}\circ\phi_{\sigma^{-1}})(-\mathbf{x}),\sigma\circ\sigma^{-1}\right)\\
&= \left(\mathbf{x}\oplus\phi_{\sigma\circ\sigma^{-1}}(-\mathbf{x}),\sigma\circ\sigma^{-1}\right)\\
&= (\mathbf{x}\oplus\phi_{id}(-\mathbf{x}),id)=(\mathbf{x}\oplus(-x),id)\\
&= (\mathbf{0},id)
\end{aligned}$$

e

$$\begin{aligned}
\left(\phi_{\sigma^{-1}}(-\mathbf{x}),\sigma^{-1}\right)\star(\mathbf{x},\sigma) &= \left(\phi_{\sigma^{-1}}(-\mathbf{x})\oplus\phi_{\sigma^{-1}}(\mathbf{x}),\sigma^{-1}\circ\sigma\right)\\
&= (\phi_{\sigma^{-1}}(-\mathbf{x}\oplus\mathbf{x}),id)=(\phi_{\sigma^{-1}}(\mathbf{0}),id)\\
&= (\mathbf{0},id).
\end{aligned}$$

Estas considerações nos levam a pensar em uma definição um pouco mais consistente, que venha generalizar a propelinearidade binária, como também algumas de suas propriedades. Formularemos essas idéias de modo mais preciso.

Definição 4.1.2 *Sejam* $(\mathbb{Z}_m^n, d_H)$ *o espaço de Hamming n-dimensional e* $\mathbf{S}_n$ *o grupo simétrico de grau n. Diremos que um subconjunto* $\mathbf{C} \subseteq \mathbb{Z}_m^n$, *com* $\mathbf{0} \in \mathbf{C}$ *é um* ***código propelinear*** *m-ário de comprimento n, se existir uma função* $\pi : \mathbf{C} \to \mathbf{S}_n$, *definida por* $\pi(\mathbf{v}) = \pi_{\mathbf{v}}$, *tal que o gráfico*

$$\Omega(\pi) = \{(\mathbf{v}, \pi_{\mathbf{v}}) : \forall\, \mathbf{v} \in \mathbf{C}\}$$

seja um subgrupo de $\mathbb{Z}_m^n \rtimes \mathbf{S}_n$.

Desta definição, segue que o código propelinear m-ário $\mathbf{C} \subseteq \mathbb{Z}_m^n$ é identificado com o subgrupo $(\Omega(\pi), \star)$ de $(\mathbb{Z}_m^n \rtimes \mathbf{S}_n, \star)$, de modo que

$$\mathbf{u} \star \mathbf{v} = \mathbf{u} \oplus \pi_{\mathbf{u}}(\mathbf{v}), \forall \mathbf{u}, \mathbf{v} \in \mathbf{C}.$$

Por isso, nos referimos a $\mathbf{C}$ e $\Omega(\pi)$, indistintamente.

Proposição 4.1.1 *Seja* $\mathbf{C}$ *um código propelinear m-ário de comprimento n. Então:*

1. $(\Pi = \{\pi_{\mathbf{v}} \mid \mathbf{v} \in \mathbf{C}\}, \circ)$ *é um subgrupo do grupo das isometrias de* $\mathbb{Z}_m^n$;
2. $\mathbf{C}$ *é linear se, e somente se,* Π *é um subgrupo de* $\mathrm{Aut}(\mathbf{C})$;
3. *A operação* $\star$ *define uma ação de* $\mathbf{C}$ *sobre* $\mathbb{Z}_m^n$.

1. **Prova.** Análoga a da Proposição 3.1.1. ∎

Proposição 4.1.2 *Seja* $\mathbf{C}$ *um código propelinear m-ário de comprimento n. Então:*

1. *Se* $\mathbf{C}$ *é um código que corrige* e*-erros* $(\mathrm{e} \geq 1)$, *então todos os vetores de peso menor ou igual a* e *estão em classes laterais diferentes*;
2. *Para todo* $x, y \in \mathbb{Z}_m^n$ *e todo* $\mathbf{v} \in \mathbf{C}$, *tem-se* $d_H(x, y) = d_H(\mathbf{v} \star x, \mathbf{v} \star y)$.

Prova. Análoga a da Proposição 3.1.2. ∎

Como estamos identificando um código propelinear m-ário como um subgrupo do produto semi-direto, $\mathbb{Z}_m^n \rtimes \mathbf{S}_n$, faz sentido falarmos em *códigos propelineares cíclicos*, ou seja, faz sentido a seguinte definição.

Definição 4.1.3 *Seja* $(\mathbf{v}, \pi_{\mathbf{v}}) \in \mathbb{Z}_m^n \rtimes \mathbf{S}_n$. *Chamaremos o subgrupo* $\mathbf{C}$ *de* $\mathbb{Z}_m^n \rtimes \mathbf{S}_n$, *gerado por* $(\mathbf{v}, \pi_{\mathbf{v}})$ *e denotado por* $\mathbf{C} = \langle (\mathbf{v}, \pi_{\mathbf{v}}) \rangle$, *de código propelinear cíclico gerado por* $(\mathbf{v}, \pi_{\mathbf{v}})$.

Exemplo 4.1.1 *As Tabelas 4.1 e 4.2, apresentadas na Seção 4.3, são exemplos de códigos propelineares m-ários cíclicos e gerado por dois elementos para* $m = 2, 3, 4, 5$ *e* 6.

4.2 Códigos Propelineares m-ários Invariantes por Translação

A Proposição 4.1.2, nos assegura que ação de $\mathbf{C}$ sobre $\mathbb{Z}_m^n$ é sempre preservada pela distância de Hamming que faz de $\mathbb{Z}_m^n$ o espaço métrico $(\mathbb{Z}_m^n, d_H)$. Porém, isto não é suficiente para garantir que o código seja invariante por translação. Para obtermos a invariância por translação do código, precisamos assegurar que a Proposição 4.1.2 também seja válida no grupo $\mathbf{C}$. Mais precisamente:

Definição 4.2.1 *Seja* $\mathbf{C}$ *um código propelinear m-ário. Diremos que* $\mathbf{C}$ *é um código* ***propelinear invariante por translação*** *se para todo* $\mathbf{u}, \mathbf{v} \in \mathbf{C}$ *e* $x \in \mathbb{Z}_m^n$ *temos que*

$$d_H(\mathbf{u}, \mathbf{v}) = d_H(\mathbf{u} \star x, \mathbf{v} \star x).$$

Das considerações anteriores, temos :

Lema 4.2.1 *Seja* $\mathbf{C}$ *um código propelinear m-ário.* $\mathbf{C}$ *é invariante por translação se, e somente se,*

$$wt_H(\mathbf{v}) = d_H(x, \mathbf{v} \star x), \forall x \in \mathbb{Z}_m^n \text{ e } \mathbf{v} \in \mathbf{C}.$$

Prova. Análoga a do Lema 3.1.1. ■

Agora, vamos reunir um pouco mais de condições para investigar a existência ou não, de códigos propelineares m-ários. Por isso, faremos uma análise das tabelas 4.1 e 4.2, do ponto de vista do Lema 4.2.1:

1. Da tabela 4.1, vemos que para $m = 2$, temos o código do Exemplo 3.1.3, o qual é invariante por translação. Os demais códigos, não são invariantes por translação, pois o Lema 4.2.1 não se verifica para os seguintes pares $(\mathbf{v}, x)$:

   (a) para $m = 3$, $(\mathbf{v}, x) = (01, 12)$ e $(02, 10)$;

   (b) para $m = 4$, $(\mathbf{v}, x) = (01, 13)$, $(02, 12)$ e $(03, 13)$;

   (c) para $m = 5$, $(\mathbf{v}, x) = (01, 43)$, $(02, 43)$, $(03, 43)$ e $(04, 34)$;

   (d) para $m = 6$, $(\mathbf{v}, x) = (01, 54)$, $(02, 54)$, $(03, 54)$ e $(04, 54)$ e $(05, 45)$.

2. A Tabela 4.2, nos mostra que para $m = 2$, temos o código do Exemplo 3.1.4, o qual é invariante por translação. Os demais códigos não são invariantes por translação. Com efeito, basta considerar os seguintes pares $(\mathbf{v}, x)$:

   (a) para $m = 3$,

   $(\mathbf{v}, x) = (1010, 0102), (1020, 2102), (2010, 2102)\, e\, (2020, 2102)$;

   (b) para $m = 4$,

   $(\mathbf{v}, x) = (1010, 2103), (1020, 2103), (1030, 2130), (2020, 2130)$ $(2030, 2132)$ e $(3030, 1200)$;

   (c) para $m = 5$,

   $(\mathbf{v}, x) = (1010, 2340), (2020, 2340), (3030, 2340)$ e $(4040, 2341)$;

   (d) para $m = 6$,

   $(\mathbf{v}, x) = (1010, 0423), (2020, 0423), (3030, 0422), (4040, 4252)$ e $(5050, 4252)$.

Lema 4.2.2 *Seja* $\mathbf{C} \subset \mathbb{Z}_m^n$ *um código propelinear invariante por translação* $m \geq 2$. *Se* $\mathbf{v} \in \mathbf{C}$ *e* $\pi_{\mathbf{v}} \neq id$, *então* $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$.

Prova. Suponha que $\pi_{\mathbf{v}}(\mathbf{v}) = \mathbf{v}$, isto implica que existem vetores coordenados $\mathbf{e}_i \neq \mathbf{e}_j$ tal que $\pi_{\mathbf{v}}(\mathbf{e}_i) \neq \mathbf{e}_j$, ou seja, $i, j \notin \mathrm{Supp}(\mathbf{v})$. Logo,

$$\begin{aligned} wt_H(\mathbf{v}) &= d_H(\mathbf{e}_i, \mathbf{v} \star \mathbf{e}_i) \\ &= d_H(\mathbf{e}_i, \mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{e}_i)) \\ &= wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{e}_i) - \mathbf{e}_i) \\ &= wt_H(\mathbf{v} \oplus \mathbf{e}_j \oplus (-\mathbf{e}_i)) \\ &= wt_H(\mathbf{v}) + 2, \end{aligned}$$

o que contradiz o fato de $\mathbf{C}$ ser invariante por translação. ■

Observação 4.2.1 *O Lema 3.1.2, vale para qualquer código propelinear m-ário invariante por translação* $\mathbf{C} \subset \mathbb{Z}_m^n$ *com* $m \geq 2$. *Para isso, basta tomar* $\lambda_i \mathbf{e}_i$ *em lugar de* $\mathbf{e}_i$

Teorema 4.2.1 *Sejam* m, n *inteiros maiores do que* 1. *Não existem códigos propelineares m-ários invariantes por translação para* $m > 2$, *exceto para* $\mathbf{C} \subset \mathbb{Z}_m^n$ *linear e tal que* $\pi_{\mathbf{v}} = id$ *para todo* $\mathbf{v} \in \mathbf{C}$.

Prova. Se $\mathbf{C} \subset \mathbb{Z}_m^n$ é linear e tal que $\pi_{\mathbf{v}} = id$ para todo $\mathbf{v} \in \mathbf{C}$, então $\mathbf{C}$ é trivialmente invariante por translação. Agora, basta mostrar que existe $\mathbf{x} \in \mathbb{Z}_m^n$ tal que

$$wt_H(\mathbf{v}) \neq d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x}) = wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}) - \mathbf{x})$$

para algum $\mathbf{v} \in \mathbf{C}$. Consideremos os seguintes casos:

1. Pelo Lema 4.2.2 e 4.2.1,segue que para $\pi_{\mathbf{v}} \neq id$ temos $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$ e que existe um vetor de peso 1, digamos $\mathbf{e}_i$ tal que

   $$\pi_{\mathbf{v}}(\mathbf{e}_i) = \mathbf{e}_j \neq \mathbf{e}_i, \text{ ou seja } , i \in \mathrm{Supp}(\mathbf{v}) \text{ e } j \notin \mathrm{Supp}(\mathbf{v}).$$

   Portanto,$wt_H(\mathbf{v}) = d_H(\mathbf{x}, \mathbf{v} \star \mathbf{x}) = wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}) - \mathbf{x}) \leq wt_H(\mathbf{v}) + 2$.

2. Para $m \geq 3$, basta considerar $\pi_{\mathbf{v}}(\mathbf{v}) \neq \mathbf{v}$, pelo item 1., temos que

$$i \in \mathrm{Supp}(\mathbf{v}) \text{ e } j \notin \mathrm{Supp}(\mathbf{v}).$$

Escolhendo $\mathbf{x} = \lambda \mathbf{e}_i$ com $\lambda \neq 0$ e $\lambda \neq \lambda_i$, temos que

$$\begin{aligned} wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}) - \mathbf{x}) &= wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\lambda \mathbf{e}_i) - \lambda \mathbf{e}_i) \\ &= wt_H(\lambda_1, \lambda_2, \ldots, \lambda_i - \lambda, \ldots, \lambda + \lambda_j, \ldots, \lambda_n). \end{aligned}$$

Pela nossa escolha, $0 \neq \lambda_i \oplus (-\lambda) \in \mathrm{Supp}(\mathbf{v})$ e apesar de $\lambda_j = 0$, pois $j \notin \mathrm{Supp}(\mathbf{v})$ temos $0 \neq \lambda \oplus \lambda_j \notin \mathrm{Supp}(\mathbf{v})$. Poranto,

$$wt_H(\mathbf{v} \oplus \pi_{\mathbf{v}}(\mathbf{x}) - \mathbf{x}) = wt_H(\mathbf{v}) + 1,$$

o que contradiz o fato de $\mathbf{C}$ ser invariante por translação.

■

Comentário:

Pelo Teorema 4.2.1, podemos afirmar que não existem códigos propelineares invariantes por translação m-ários para um inteiro $m \geq 3$, ou seja, não existem subgrupos de $\mathbb{Z}_m^n \rtimes \mathbf{S}_n$ cuja ação sobre $\mathbb{Z}_m^n$ preserva a distância de Hamming. Por outro lado, sabemos que existem subgrupos de $\mathbb{Z}_m^n \rtimes \mathbf{S}_n$ tais que sua ação sobre $\mathbb{Z}_m^n$ é fortemente transitiva. Por exemplo, para $m = 3$ e $n = 3$ temos o grupo de rótulos $(\mathbb{Z}_9 : \mathbb{Z}_3)$ que é uma extensão que se decompõe de $\mathbb{Z}_9$ por $\mathbb{Z}_3$.

4.3 Tabelas de Códigos m-ários

m	**Subgrupo de $\mathbb{Z}_m^2 \rtimes \mathbf{S}_2$**	**Grupo de rótulos: $\mathcal{R}$**
2	$a = (01, (12))$	$\mathbb{Z}_4$
3	$a_1 = (01, (12))$	$\mathbb{Z}_6$
	$b_1 = (02, (12))$	$\mathbb{Z}_6$
4	$a_2 = (01, (1, 2))$	$\mathbb{Z}_8$
	$b_2 = (02, (12))$	$\mathbb{Z}_4$
	$c_2 = (03, (12))$	$\mathbb{Z}_8$
5	$a_3 = (01, (12))$	$\mathbb{Z}_{10}$
	$b_3 = (02, (12))$	$\mathbb{Z}_{10}$
	$c_3 = (03, (1, 2))$	$\mathbb{Z}_{10}$
	$d_3 = (04, (12))$	$\mathbb{Z}_{10}$
6	$a_4 = (01, (12))$	$\mathbb{Z}_{12}$
	$b_4 = (02, (12))$	$\mathbb{Z}_6$
	$c_4 = (03, (12))$	$\mathbb{Z}_4$
	$d_4 = (04, (12))$	$\mathbb{Z}_6$
	$e_4 = (05, (12))$	$\mathbb{Z}_{12}$

Tabela 4.1: Tabela de códigos cíclicos em $\mathbb{Z}_m^2 \rtimes \mathbf{S}_2$

m	**Subgrupo de $\mathbb{Z}_m^4 \rtimes \mathbf{S}_4$**	**Grupo de rótulos: $\mathcal{R}$**
2	$\langle (1010, (12)(34)), (1001, (13)(,4)) \rangle$	$\mathbb{Q}_8$
3	$\langle (1010, (12)(34)), (1001, (13)(24)) \rangle$	$\mathbb{Z}_6 \times \mathbf{S}_3$
	$\langle (1020, (12)(34)), (1002, (13)(24)) \rangle$	$\mathcal{G}_1$ $(\lvert\mathcal{G}_1\rvert = 108)$
	$\langle (2010, (12)(34)), (2001, (13)(24)) \rangle$	$\mathcal{G}_2$ $(\lvert\mathcal{G}_2\rvert = 108)$
	$\langle (2020, (12)(34)), (2002, (13)(24)) \rangle$	$\mathbb{Z}_6 \times \mathbf{S}_3$
4	$\langle (1010, (12)(34)), (1001, (13)(24)) \rangle$	$\mathbb{Q}_8$
	$\langle (1020, (12)(34)), (1002, (13)(24)) \rangle$	$\mathcal{G}_3$ $(\lvert\mathcal{G}_3\rvert = 256)$
	$\langle (1030, (12)(34)), (1003, (13)(24)) \rangle$	$\mathcal{G}_4$ $(\lvert\mathcal{G}_4\rvert = 256)$
	$\langle (2020, (12)(34)), (2002, (13)(24)) \rangle$	$\mathcal{G}_5$ $(\lvert\mathcal{G}_5\rvert = 32)$
	$\langle (2030, (12)(34)), (2003, (13)(24)) \rangle$	$\mathcal{G}_6$ $(\lvert\mathcal{G}_6\rvert = 64)$
	$\langle (3030, (12)(34)), (3003, (13)(24)) \rangle$	$\mathcal{G}_7$ $(\lvert\mathcal{G}_7\rvert = 32)$
5	$\langle (1010, (12)(34)), (1001, (13)(24)) \rangle$	$\mathcal{G}_8$ $(\lvert\mathcal{G}_8\rvert = 100)$
	$\langle (2020, (12)(34)), (2002, (13)(24)) \rangle$	$\mathcal{G}_9$ $(\lvert\mathcal{G}_9\rvert = 100)$
	$\langle (3030, (12)(34)), (3003, (13)(24)) \rangle$	$\mathcal{G}_{10}$ $(\lvert\mathcal{G}_{10}\rvert = 100)$
	$\langle (4040, (12)(34)), (4004, (13)(24)) \rangle$	$\mathcal{G}_{11}$ $(\lvert\mathcal{G}_{11}\rvert = 100)$
6	$\langle (1010, (12)(34)), (1001, (13)(24)) \rangle$	$\mathbb{Z}_6 \times \mathbf{S}_3$
	$\langle (2020, (12)(34)), (2002, (13)(24)) \rangle$	$\mathbb{Z}_6 \times \mathbf{S}_3$
	$\langle (3030, (12)(34)), (3003, (13)(24)) \rangle$	$\mathbb{Q}_8$
	$\langle (4040, (12)(34)), (4004, (13)(24)) \rangle$	$\mathbb{Z}_3 \times \mathbb{Q}_8 + \mathbf{S}_3$
	$\langle (5050, (12)(34)), (5005, (13)(24)) \rangle$	$\mathbb{Z}_3 \times \mathbb{Q}_8 + \mathbf{S}_3$

Tabela 4.2: Tabela de códigos em $\mathbb{Z}_m^4 \rtimes \mathbf{S}_4$

Capítulo 5

Conclusões

Neste trabalho exploramos a riqueza existente na teoria dos grupos, na proposta de construção de alguns tipos de códigos. Dentro desse contexto, utilizamos de forma efetiva os grupos de isometrias de um conjunto de sinais e o produto semi-direto de grupos. Aplicamos esses conceitos na construção de códigos propelineares, propelineares invariantes por translação e **G**-lineares.

Inspirado na $\mathbb{Z}_4$-linearidade e consequentemente na **G**-linearidade, fomos levados a pensar em uma possível generalização da propelinearidade. Ou seja, existem códigos propelineares cujo alfabeto não seja binário? E códigos propelineares invariantes por translação? Esses códigos pertencem a alguma classe de códigos já existentes? Ao tentar responder essas questões, acabamos encontrando alguns resultados que relacionam essas classes de códigos.

Nos Capítulos 1 e 2, apresentamos um histórico deste trabalho, bem como os requisitos básicos para o seu desenvolvimento e sua compreensão.

No Capítulo 3, revisamos os principais resultados sobre códigos propelineares e códigos propelineares invariantes por translação binários, como também algumas propriedades dos códigos **G**-lineares binários, as quais evidenciam sua uniformidade geométrica. Obtivemos resultados que relacionaram essas classes de códigos.

No Capítulo 4, tratamos dos códigos propelineares e dos códigos propelineares

invariantes por translação m-ários.

5.1 Contribuições

As contruibuições deste trabalho, foram apresentadas nos Capítulos 3 e 4. Entretanto, podemos resumi-las como segue:

No Capítulo 3, apresentamos uma condição necessária e suficiente para obter códigos propelineares binários. Como consequência, podemos afirmar que a classe dos códigos **G**-lineares binários é uma subclasse dos códigos propelineares. Relacionamos códigos propelineares invariantes por translação com o subgrupo estabilizador de $\Gamma(\mathbb{Z}_2^n)$, formado pelo elemento identidade de $\Gamma(\mathbb{Z}_2^n)$. Mostramos também, que a classe dos códigos propelineares invariantes por translação de comprimento $n \geq 2$, cuja cardinalidade é 2^n, está contida na classe dos códigos **G**-lineares binários. Uma consequência desse resultado, é de que não se deve procurar códigos propelineares cíclicos invariantes por translação de comprimento $n > 2$, cuja ordem seja 2^n. Novamente, através do subgrupo estabilizador estabelecemos uma condição necessária e suficiente para que um código seja **G**-linear. Finalmente, utilizando alguns programas computacionais implementados no sistema **GAP**, apresentamos algumas tabelas de códigos propelineares invariantes por translação e de códigos **G**-lineares.

No Capítulo 4, estendemos o conceito de código propelinear binário para m-ário, de modo que o alfabeto do código base é o anel dos inteiros módulo m, indicado por $(\mathbb{Z}_m, \oplus, \otimes)$. Mostramos que não existe códigos propelineares invariantes por translação em $\mathbb{Z}_m^n$ para $m > 2$. Isto significa que para relacionar códigos **G**-lineares com códigos propelineares, precisamos ampliar um pouco mais o conceito de propelinearidade, pelo menos em termos do produto semi-direto de dois grupos.

5.2 Sugestões para Novos Trabalhos

Nesta seção procuramos destacar alguns tópicos de pesquisa como decorrência do desenvolvimento da proposta original. Estes tópicos apresentam desafios tanto sob o ponto de vista teórico como de aplicação. São eles:

- É possível estender a idéia da propelinearidade quando o grupo $\mathbf{S}_n$ em $\mathbb{Z}_2^n \rtimes \mathbf{S}_n$ for substituido por um grupo $\mathbf{G} \neq \mathbf{S}_n$. Seria possível obter a invariância por translação para algum $\mathbf{G} \neq \mathbf{S}_n$?

- É possível estender a propelinearidade a outros tipos de produtos de grupos? Por exemplo, o produto amalgamado e o produto subdireto.

- Sabemos que os códigos de grupo são subgrupos do produto direto de um certo grupo $\mathbf{H}$. Para $\mathbf{H} = \mathbb{Z}_m^k \rtimes \mathbf{S}_k$, seria interessante estudar códigos de grupo sobre $\mathbf{H}^n = \left(\mathbb{Z}_m^k \rtimes \mathbf{S}_k\right)^n$.

- O produto de Schreier é uma técnica de construção de grupos a partir de grupos conhecidos, ou seja, é exatamente um problema de extensão de grupos. Esta técnica generaliza os produtos direto e semi-direto. Seria possível encontrarmos um classe de códigos propelineares nesse produto? E de códigos propelineares invariantes por translação?

- Estudar a existência ou não de códigos propelineares invariantes por translação sobre o espaço métrico $(\mathbb{Z}_m^n, d_L)$, onde d_L é a métrica de **Lee**. Caso se confirme a existência de tais códigos, como poderíamos relacioná-los com os códigos $\mathbf{G}$-lineares, onde $\mathbf{G}$ é um subgrupo do grupo de simetrias de $\mathbb{Z}_m^n$, dado por $\Gamma\left(\mathbb{Z}_m^n\right)$? Conforme [?], para $m \neq 2$ e $m \neq 4$, temos que

$$\Gamma\left(\mathbb{Z}_m^n\right) \cong \mathbb{Z}_m^n \rtimes_1 \left(\mathbb{Z}_m^n \rtimes \mathbf{S}_n\right).$$

Referências Bibliográficas

[1] M. M. S. Alves, *Códigos Geometricamente Uniformes em Espaço de Lee*, Tese de Mestrado, IMECC-UNICAMP, Março 1998.

[2] M. M. S. Alves, J. R. Gerônimo, R. Palazzo, Jr., S. I. R. Costa, J. C. Interlando and M. C. Araujo, "On Equivalence Between Binary Propelinear and Binary **G**-Linear Codes", *discrete Mathematics* (aceito para publicação), December 1998.

[3] M. A. Armstrong, *Groups and Symmetry.* New York: Springer-Verlag, 1988.

[4] E. R. Berlekamp, *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.

[5] A. E. Brouwer, A. M. Cohen, A. Neumaier, *distance-Regular Graphs.* Berlin: Springer-Verlag, 1989.

[6] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding.* New York: Academic Press, 1975.

[7] G. Care and E. Biglieri, "Linear Block Codes Over Cyclic Groups", *IEEE Trans. Inform. Theory*, vol. IT-41, n°. 5, pp. 1246-1256, September 1995.

[8] S. R. Costa, J. R. Gerônimo, R. Palazzo Jr., J. C. Interlando e M. S. Alves, "The Symmetry Group of $\mathbb{Z}_q^n$ in the Lee Space and the $\mathbb{Z}_{q^n}$-Linear Codes ", *Lectures Notes in Computer Science*, n°. 1225, pp. 67-77, New York: Springer-Verlag,1997.

[9] D. S. Dummit and R. M. Foot, *Abstract Algebra.* New Jersey: Prentice-Hall, 1991.

[10] J. R. Durbin, *Modern Algebra: An Introduction.* New York: John Wiley & Sons, Inc., 1992.

[11] M. Elia and E. Biglieri, "The Isometry Group of Geometrically Uniforme Spherical Signal Sets", in *IEEE International Symposium on Information Theory*, August 1991.

[12] G. D. Forney, Jr., "Geometrically Uniform Codes", *IEEE Trans. Inform. Theory*, vol. IT-37, n°. 5, pp. 1241-1260, September 1991.

[13] G. D. Forney, Jr., "Coset Codes - Part I: Introduction and Geometrical Classifictiaon", *IEEE Trans. Inform. Theory*, vol. IT-34, n°. 5, pp. 1123-1151, September 1988.

[14] G. D. Forney, Jr.,"On the Hamming Distance Properties", *IEEE Trans. Inform. Theory*, vol. IT-38, n°. 6, pp. 1997-1801, November 1992.

[15] G. D. Forney, Jr., N. J. A. Sloane, M. D. Trott, "The Nordstrom-Robinson Code is the Binary Image of the Octacode", in *Coding and Quantization:* DIMACS / IEEE Workshop October 19-21, 1992, Amer. Math. Soc., 1993, edited by R. Calderbank, G.D. Forney, Jr. and N. Moayeri, pp. 19-26.

[16] R. Garello and S. Benedetto, "Multilevel Construction of Block and Trellis Group Codes", *IEEE Trans. Inform. Theory*, vol. IT-41, n°. 5, pp. 1257-1264, September 1996.

[17] J. R. Gerônimo, *Extensão da Z_4-Linearidade Via Grupo de Simetrias*, Tese de Doutorado, DECOM-FEE-UNICAMP, Janeiro 1997.

[18] W. Gilbert, *Modern Algebra with Applications.* New York: John Wiley & Sons, 1976.

[19] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, "A $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes", *IEEE Trans. Inform. Theory*, vol. IT-40, n° 2, pp. 301-319, March 1994.

[20] J. F. Humphreys, *A Course in Group Theory*. New York: Oxford University Press Inc, 1997.

[21] E. L. Lima, *Espaços Métricos*. Rio de Janeiro: Projeto Euclides, 1977.

[22] R. C. Lyndon, *Groups and Geometry*. Cambridge: Cambridge University Press, 1987.

[23] H. A. Loeliger, "Signal Sets Matched To Groups", *IEEE Trans. Inform. Theory*, vol. IT-37, n°. 6, pp. 1675-1682, November 1991.

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

[25] T. Mittelholzer and J. Lahtonen, "Group Codes Generated by Finite Reflections Groups", *IEEE Trans. Inform. Theory*, vol. IT-42, n°. 2, pp. 519-528, March 1996.

[26] P. M. Neumann, "On the Structure of Standard Wreath Products of Groups", Math. Zeitschr. vol. 84, pp. 343-373, 1964.

[27] A. Neumaier, "Completely regular codes". *discrete Mathematics*, vol. 106/107, pp. 353-360, 1992.

[28] A. Niemeyer, M. Schöenert, et al..., *GAP- Groups, Algorithms and Programming*, Version 3. April, 1999.

[29] O. Pretzel, *Error-Correcting Codes and Finite Fields*. New York: Oxford University Press Inc, 1996.

[30] J. Rifá, J. M.Bassart e L. Huguet, "On Completely Regular Propelinear Codes", in Proc.6th Int. Conf., AAECC-6, *Lectures Notes in Computer Science*, n°. 357, pp. 341-355, New York: Springer-Verlag,1989.

[31] J. Rifá e J. Pujol, "Translation-Invariant Propelinear Codes", *IEEE Trans. Inform. Theory*, vol. IT-43, n°. 2, pp. 590-598, March 1997.

[32] J. Rifá, "On a Categorial Isomorphism between a class of Completely Regular Codes and a class of Distance Regular Graphs", in Proc. 8th Int. Conf., AAECC-8, *Lectures Notes in Computer Science*, n°. 508, pp. 164-179, New York: Springer-Verlag,1991.

[33] D. J. S. Robinson, *A Course in the Theory of Groups*. New York: Springer-Verlag, 1982.

[34] S. Roman, *Coding and Information Theory*. New York: Springer-Verlag, 1992.

[35] J. S. Rose, *A Course on Group Theory*. New York: Dover Publications, Inc., 1978.

[36] J. J. Rotman, *An Introduction to the Theory of Groups*. New York: Springer-Verlag, 1995.

[37] R. L. E. Schwarzenberger, *N-dimensional crystallography*. San Francisco: Pitman Advanced Publishing Program, 1980.

[38] L. W. Shapiro, "Finite Groups Acting On Sets With Applications", *Mathematics Magazine*. May-June, pp. 136-147, 1973.

[39] A. A. Silva, *Uma Contribuição À Classe dos Códigos Geometricamente Uniformes*, Tese de Doutorado, DECOM-FEE-UNICAMP, Maio 1996.

[40] D. Slepian, "Groups Codes for Gaussian Channel", *Bell Syst. Tech. J.*, vol. 47, pp.575-602, April 1967.

[41] D. Slepian, "On Neighbor Distances and Symmetry in Group Codes", *IEEE Trans. Inform. Theory*, vol. IT-17, n°. 5, pp. 630-6321, September 1971.

[42] P. Solé, "Completely Regular Codes and Completely Transitive Codes", *discrete Mathematics*, vol. 81, pp. 193-201, 1990.

[43] G. Ungerboeck, "Channel Coding with Multilevel/Phase Signals", *IEEE Trans. Inform. Theory*, vol. IT-28, n°. 1, pp. 56-67, January 1982.

[44] S. A. Vastone and P. C. van Oorschot, *An Introduction To Error Correcting Codes With Applications*. Boston: Kluwer Academic Publishers, 1992.

[45] P. B. Yale, *Geometry and Symmetry*. New York: Dover Publications, Inc., 1968.