Sobre códigos cíclicos e abelianos

Fernanda Diniz de Melo

Tese apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Doutor em Ciências

Programa: Matemática

Orientador: Prof. Dr. Francisco César Polcino Milies

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES

São Paulo, fevereiro de 2012

Sobre códigos cíclicos e abelianos

Esta versão da tese contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 19/03/2012. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Prof. Dr. Francisco César Polcino Milies - IME-USP
- Profª. Drª. Alegria Gladys Chalom - IME-USP
- Prof. Dr. Raul Antonio Ferraz - IME-USP
- Profª. Drª. Marinês Guerreiro - UFV
- Profª. Drª. Rosali Brusamarello - UEM

RESUMO

Neste trabalho calculamos o peso e a dimensão de todos os códigos cíclicos de comprimento p^n na álgebra de grupo $\mathbb{F}_q C_{p^n}$, onde p é um número primo e $\mathbb{F}_q$ é um corpo finito de característica q. Também calculamos o peso do código dado pela soma de dois códigos abelianos minimais em $\mathbb{F}_q(C_p \times C_p)$, dessa forma foi possível fazer uma breve comparação entre códigos cíclicos e abelianos não cíclicos de comprimento p^2.

Palavras chave: anéis de grupo, código abeliano, código cíclico, peso de códigos lineares

ABSTRACT

In this work we compute the weight and the dimension of all cyclic codes of length p^n in the group algebra $\mathbb{F}_q C_{p^n}$, where p is a prime number and $\mathbb{F}_q$ is a finite field of characteristic q. Furthermore, we compute the weight of codes which are given by the sum of two minimal abelian codes in $\mathbb{F}_q(C_p \times C_p)$. In this way, it was possible to compare briefly cyclic codes and non-cyclic abelian codes of length p^2.

Keywords group ring, abelian code, cyclic code, weight linear code.

SUMÁRIO

Introdução **1**

1 Conceitos Básicos **5**

1.1 Anéis de Grupo 6

1.2 Códigos Lineares 9

2 Códigos Cíclicos **13**

2.1 Códigos Cíclicos Minimais 14

2.2 Soma de Ideais Minimais 15

2.3 Distribuição de Pesos 20

3 Códigos Abelianos **25**

3.1 Códigos Abelianos Minimais 26

3.2 Soma de Ideais Minimais 27

3.2.1 Caso $p > 3$ 29

3.2.2 Caso p=2 35

3.2.3 Caso p=3 36

3.3 Exemplos 38

3.4 Código Fonte 40

4 Conclusões **47**

4.1 Introdução 47

4.2 Comparação de códigos 49

4.2.1 Códigos Minimais 49

4.2.2 Soma de ideais minimais 51

Referências Bibliográficas **53**

INTRODUÇÃO

No fim da década de 40 do século XX teve ínicio, com Richard W. Hamming, o estudo de códigos corretores de erros. Um código é um conjunto $\mathcal{C}$ de palavras que são sequências $(a_0, a_1, ...a_{n-1})$ de comprimento n, de dígitos tomados em um conjunto finito $\mathcal{A}$ com q elementos chamado alfabeto. O objetivo de Hamming era criar um código que fosse capaz de detectar e corrigir um erro.

Nessa época Hamming trabalhava no *Bell Telephone Laboratories*, ali os computadores eram muito lentos e capazes apenas de detectar o erro, não de corrigi-lo. Quando isso acontecia o computador parava de processar o programa que executava e passava para outro e então muitos trabalhos eram perdidos.

Em 1950 foi publicado o estudo de Hamming no *Bell System Thechnical Journal* [8], onde ele descreve um código capaz de detectar até dois erros e corrigir um, se ele for o único. Querendo construir um código ainda mais eficiente Hamming perguntou se seria possível construir um código capaz de detectar e corrigir um erro em uma palavra com quatro dígitos de informação e três de verificação. A resposta veio no artigo *"A Mathematical Theory of Communication"* [17], de um colega de trabalho, chamado Claude Shannon em 1948. Nesse artigo Shannon atribuiu o código encontrado ao próprio Hamming.

O artigo de Shannon é considerado hoje como o responsável pela origem de duas

teorias: a **Teoria de Códigos Corretores de Erros** e a **Teoria da Informação**.

Pouco tempo depois Marcel Golay, que trabalhava no *Signal Corps Enginneering Laboratories at Fort Monmouth*, em Nova Jersey, inspirado no trabalho de Shannon publicou o artigo *"Notes on Digital Coding "* [7], de uma única página, onde descreve alguns códigos que estão entre os melhores utilizados até hoje.

Desde então, a Teoria de Códigos Corretores de Erros é um amplo campo de pesquisa que vem despertando o interesse de matemáticos, engenheiros elétricos e cientistas da computação.

A fim de se obter uma teoria matemática dos códigos é necessário introduzir alguma estrutura algébrica, para isso consideraremos o alfabeto sendo um corpo finito $\mathbb{F}$ com q elementos e o código $\mathcal{C}$ será um subespaço vetorial do espaço $\mathbb{F}^n$ de dimensão n sobre $\mathbb{F}$. Dessa forma $\mathcal{C}$ é dito código linear q-ário de comprimento n.

Uma importante classe de códigos lineares são os códigos cíclicos que possuem a seguinte propriedade

$$(c_0, c_1, ..., c_{n-1}) \in \mathcal{C} \Rightarrow (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in \mathcal{C}.$$

Os exemplos mais importantes dessa classe são os códigos de Hamming e Golay.

É fácil verificar que o espaço vetorial $\mathbb{F}^n$ é isomorfo a álgebra de grupo $\mathbb{F}C_n$, onde C_n é o grupo cíclico de ordem n, em particular os códigos cíclicos de $\mathbb{F}^n$ são identificados com ideais da álgebra $\mathbb{F}C_n$. Assim podemos afirmar que um código cíclico pode ser realizado como um ideal de uma álgebra de grupo de um grupo cíclico.

De modo geral, dizemos que um ideal de uma álgebra de grupo finita $\mathbb{F}G$ é um código de grupo.

No caso em que a característica do corpo $\mathbb{F}$ não divide a ordem do grupo G, a álgebra $\mathbb{F}G$ é semisimples e assim todo ideal é gerado por elementos idempotentes. Logo todos os códigos em $\mathbb{F}G$ são somas diretas de ideais minimais e daí, uma lista de códigos de $\mathbb{F}G$ pode ser dada determinando os idempotentes centrais primitivos, os quais gerarão os ideais minimais. Determinar esses idempotentes não é um problema fácil, porém existe bastante literatura a respeito, veja [1], [3], [9], [13] e [16]

Entre os anos 1997 e 1999, S.K. Arora e M. Pruthi [13] e [1] caracterizaram códigos cíclicos mínimais de comprimento p^n e $2p^n$ sob certas hipóteses e usando o ponto de vista polinomial, eles construíram os idempotentes centrais primitivos.

A partir da Teoria de Anéis de Grupo, em 2005 R. Ferraz e C.Polcino Milies [5] estenderam esses resultados descrevendo todos os códigos minimais abelianos de comprimento p^n e $2p^n$ em um certo corpo finito $\mathbb{F}$, usando os subgrupos do grupo dado. Eles também calcularam as dimensões e as distâncias mínimas dos códigos abelianos mínimais utilizando resultados gerais de anéis de grupo. Esses dois últimos parâmetros são muito importantes na Teoria de Códigos Corretores de Erro, pois estão diretamente relacionados com a capacidade de um código detectar e corrigir erros.

Neste trabalho vamos estudar os códigos cíclicos e abelianos que são somas dos códigos minimais obtidos por Ferraz e Polcino Milies. O objetivo é determinar a dimensão e a distância mínima desses códigos, além de fazer uma breve comparação entre eles. Essa tese está dividida em quatro capítulos.

No primeiro capítulo introduziremos os conceitos básicos necessários para o entendimento desse trabalho, tais como: a definição de anéis de grupos, códigos lineares e dos seus parâmetros. Apresentaremos resultados sobre a semisimplicidade de um anel de grupo e ideais de anéis de grupo como códigos lineares.

Introduzimos os códigos cíclicos minimais de comprimento p^n no Capítulo 2, como pode ser visto no Lema 2.1 e Corolário 2.1. Na segunda seção calculamos a distância mínima dos códigos em $\mathbb{F}C_n$, que são somas dos códigos cíclicos minimais no Teorema 2.2.1 e por último fazemos a distribuição de peso de alguns desses códigos.

No terceiro capítulo encontram-se, na primeira seção, os códigos abelianos minimais, (veja Lema 3.1 e o Teorema 3.1.1), na segunda seção, temos o cálculo da distância da soma de dois códigos minimais. Finalizamos esse capítulo com exemplos feitos usando o programa GAP para calcular a distância mínima de todos os possíveis códigos na álgebra de grupo abeliano.

No quarto capítulo fazemos algumas comparações entre os códigos obtidos nos capítulos anteriores a partir das distâncias mínima e dimensões calculadas.

CAPÍTULO 1

CONCEITOS BÁSICOS

Neste capítulo, afim de proporcionar um melhor entendimento dos próximos capítulos, apresentamos os conceitos básicos da Teoria de Anéis de Grupo, considerando que o leitor tenha conhecimento da Teoria de Anéis. Também apresentamos alguns conceitos da Teoria de Códigos Corretores de Erros.

Na primeira seção introduzimos o conceito de anéis de grupo e damos uma condição para que tenha estrutura de álgebra. Também estudamos a semisimplicidade do anel de grupo; aqui destacamos o Teorema de Maschke 1.1.1, e a estrutura de anéis de grupo semisimples, destacando o Teorema de Wedderburn-Artin 1.1.2 para o caso de álgebra de grupo.

Já na segunda seção encontra-se a definição de um código e formalizamos a ideia de distância entre palavras do códigos. Em particular, estudamos os códigos lineares e em específico os códigos cíclicos, destacamos que os códigos cíclicos podem ser realizados como ideais em uma álgebra de grupo, e damos uma definição geral para códigos de grupo.

Aqui optamos por apenas citar as fontes onde se encontram as demonstrações dos resultados apresentados.

1.1 Anéis de Grupo

Seja R um anel com unidade e G um grupo, denotamos por RG o conjunto formado pelas somas formais do tipo

$$\alpha = \sum_{g \in G} \alpha_g g,$$

onde $\alpha_g \in R$ e $\alpha_g = 0$, exceto para um número finito de elementos $g \in G$. Note que dado dois elementos $\alpha = \sum_{g \in G} \alpha_g g$ e $\beta = \sum_{g \in G} \beta_g g$ em RG temos $\alpha = \beta$ se, e somente se, $\alpha_g = \beta_g$, para todo $g \in G$.

Definimos o *suporte* do elemento α em RG como o subconjunto dos elementos de G para os quais seus coeficientes são não nulos em α, isto é,

$$supp(\alpha) = \{g \in G / \, \alpha_g \neq 0\}.$$

Para dois elementos em RG definimos as seguintes operações:

$$\alpha + \beta = \sum_{g \in G} (\alpha_g g + \beta_g) g$$

$$\alpha\beta = \sum_{g,h \in G} \alpha_g \beta_h gh.$$

Observe que, com essas operações, RG é um anel com unidade dada pelo elemento $1 = \sum_{g \in G} u_g g$, onde o coeficiente correspondente ao elemento unidade do grupo é igual a 1 e $u_g = 0$, para todo outro $g \in G$. Dessa forma RG é dito *anel de grupo*.

Podemos ainda definir a multiplicação por escalar da seguinte maneira, seja $\lambda \in R$ então

$$\lambda(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} (\lambda \alpha_g) g,$$

assim RG é um R-módulo. Se R for um corpo, então RG será uma álgebra sobre R.

Podemos dizer que G é uma base de RG sobre R fazendo a identificação $i : G \to RG$, sendo $i(x) = \sum_{g \in G} \alpha_g g$ onde $\alpha_x = 1$ e $\alpha_g = 0$ se $g \neq x$. Assim se G é finito, podemos afirmar que o posto de RG sobre R é precisamente $|G|$.

Observe que temos também um homomorfismo de anéis entre o anel de grupo RG e o anel R da seguinte forma: $\varepsilon : RG \to R$ dado por $\varepsilon(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \alpha_g$, essa função é dita *função de aumento* de RG e seu núcleo denotado por $\Delta(G)$ é chamado *ideal de aumento* de RG.

Sobre a semisimplicidade do anel de grupo RG temos o seguinte teorema

Teorema 1.1.1 (Teorema de Maschke)**.** *([11], Teo. 3.4.7) Seja G um grupo, então o anel de grupo RG é semisimples se, e somente se, as seguintes condições são válidas*

i) R é um anel semisimples

ii) G é finito

iii) $|G|$ é invertível em R.

Para o caso em que $R = \mathbb{K}$ é um corpo, temos que $\mathbb{K}$ é sempre semisimples e para o grupo G finito, $|G|$ é invertível em $\mathbb{K}$ se, e somente se, a característica do corpo $\mathbb{K}$ não divide $|G|$. Assim, como consequência direta do teorema acima temos:

Corolário 1.1. *Seja G um grupo finito e $\mathbb{K}$ um corpo. Então $\mathbb{K}G$ é semisimples se, e somente se, $char(\mathbb{K}) \nmid |G|$.*

O conhecido Teorema de Wedderburn-Artin, para anéis semisimples, no contexto de anéis de grupo nos dará informações sobre a estrutura de uma álgebra de grupo.

Teorema 1.1.2. *([11]) Seja G um grupo finito e seja $\mathbb{K}$ um corpo tal que $char(\mathbb{K}) \nmid |G|$. Então:*

i) $\mathbb{K}G$ é soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$, chamadas componentes simples de $\mathbb{K}G$. Cada B_i é um anel simples.

ii) Qualquer ideal bilateral de $\mathbb{K}G$ é a soma direta de algum dos membros da família $\{B_i\}_{1\leq i\leq r}$.

iii) Cada componente simples B_i é isomorfa a um anel de matrizes do tipo $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia isomórfica de $\mathbb{K}$ em seu centro, e o isomorfismo $\mathbb{K}G \simeq \oplus_{i=1}^{r} M_{n_i}(D_i)$ é um isomorfismo de $\mathbb{K}$-algebras.

iv) Em cada anel de matrizes $M_{n_i}(D_i)$, o conjunto

$$I_i = \left\{ \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ & & \cdots & \\ x_{n_i} & 0 & \cdots & 0 \end{pmatrix}, \ x_1, x_2, ..., x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

é um ideal minimal à esquerda.

Dado $x \in \mathbb{K}G$, consideramos $\phi(x) = (\alpha_1, ..., \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ e defina o produto de x por um elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. Com essa definição I_i é um $\mathbb{K}G$-módulo simples.

v) $I_i \ncong I_j$ se $i \neq j$.

vi) Qualquer $\mathbb{K}G$-módulo simples é isomorfo a algum I_i, $1 \leq i \leq r$.

Também podemos decompor uma álgebra de grupo como a soma direta de ideais de uma família de idempotentes (veja [11]). Para tanto considere o conjunto $\{e_1, ..., e_n\}$ de elementos de $\mathbb{K}G$ tais que:

(i) e_i é um idempotente central em $\mathbb{K}G$, $1 \leq i \leq n$;

(ii) $e_i e_j = 0$, se $i \neq j$;

(iii) $1 = e_1 + \cdots + e_n$;

(iv) e_i não pode ser escrito como $e_i = e_i' + e_i''$, onde e_i', e_i'' satisfazem os itens anteriores.

Esses idempotentes $e_1, ..., e_n$ são ditos *idempotentes centrais primitivos* de $\mathbb{K}G$. E nesse caso a decomposição de Wedderburn de $\mathbb{K}G$ em soma de ideais bilaterais é dada por

$$\mathbb{K}G = (\mathbb{K}G)e_1 \oplus (\mathbb{K}G)e_2 \oplus \cdots \oplus (\mathbb{K}G)e_n.$$

1.2 Códigos Lineares

Considere $\mathcal{A}$ um conjunto finito qualquer com q elementos, que será chamado *alfabeto* e os elementos de $\mathcal{A}$ são ditos *letras* ou *dígitos*. Uma *palavra de comprimento* n é qualquer sequência com n elementos de $\mathcal{A}$.

Assim seja $\mathcal{A}^n$ o conjunto com todas as palavras de comprimento n, isto é, $\mathcal{A}^n = \{(a_1, a_2, ..., a_n) \,/\, a_i \in \mathcal{A}, 1 \leq i \leq n\}$.

Um *código* $\mathcal{C}$ *de comprimento* n é um subconjunto não trivial de $\mathcal{A}^n$, para algum número natural n. Também dizemos que o código $\mathcal{C} \subset \mathcal{A}^n$ é um *código de bloco q-ário*.

O objetivo da Teoria de Códigos Corretores de Erros é determinar quando uma palavra transmitida através de um canal é recebida com algum erro e, o mais importante, saber corrigir este erro.

Para fazer isso, vamos formalizar a noção de proximidade entre duas palavras dadas. Assim sejam $v = (v_1, v_2, ..., v_n)$ e $w = (w_1, w_2, ..., w_n)$ tais palavras de $\mathcal{A}^n$. Dizemos que a *distância de Hamming* entre elas é o número de coordenadas em que v e w diferem, ou seja,

$$d(v, w) = |\{i \,/\, v_i \neq w_i,\ 1 \leq i \leq n\}|.$$

A *distância mínima* de um código $\mathcal{C}$ é o número

$$d(\mathcal{C}) = min\{d(v, w) \,/\, v, w \in C,\ v \neq w\}.$$

Afim de trabalharmos em um conjunto munido de estrutura algébrica tomamos o alfabeto como sendo um corpo finito com q elementos, $\mathbb{F}_q$. O código $\mathcal{C}$ será um subespaço vetorial próprio de dimensão k do espaço vetorial $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$. Esse código é dito *código linear*. Assim temos um código de comprimento n e com q^k palavras; se d for a distância mínima de $\mathcal{C}$ diremos que $\mathcal{C}$ é um (n, q^k, d)-código linear.

Dada uma palavra $v = (v_1, v_2, ..., v_n) \in \mathbb{F}_q^n$, definimos o seu *peso* como o número inteiro positivo

$$\omega(v) = |\{i|\, v_i \neq 0,\ 1 \leq i \leq n\}|.$$

O *peso de um código* $\mathcal{C}$ é dado por

$$\omega(\mathcal{C}) = min\{\omega(v) | \, v \in \mathcal{C} \setminus \{0\}\}.$$

Dar a *distribuição de pesos* de um código é determinar a quantidade de palavras existentes no código para cada peso possível.

Para um código linear $\mathcal{C}$ temos o seguinte $\omega(v-u) = d(v,u)$, para todo $v, u \in \mathcal{C}$, consequentemente, $d(\mathcal{C}) = \omega(\mathcal{C})$.

Um código linear $\mathcal{C}$ é dito um *código cíclico* se, para toda palavra $v = (v_1, v_2, ..., v_n)$ em $\mathcal{C}$, a palavra $(v_n, v_1, ..., v_{n-1})$ obtida através de v pela troca cíclica de coordenadas $i \to i+1$, tomada módulo n, também está em $\mathcal{C}$. Essa é uma importante classe de códigos dentre os códigos lineares.

Agora seja C_n um grupo cíclico de ordem n e seja $\mathbb{F}_q C_n$ a álgebra de grupo. Consideremos o isomorfismo φ entre os espaços vetoriais $\mathbb{F}_q^n$ e $\mathbb{F}_q C_n$ dado por

$$\begin{array}{rcl} \varphi : \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q C_n \\ (\alpha_1, \alpha_2, ..., \alpha_n) & \mapsto & \displaystyle\sum_{i=1}^{n} \alpha_i a^i, \end{array}$$

onde a é um gerador do grupo cíclico C_n. Observamos que a troca cíclica em elementos de $\mathbb{F}_q^n$ é equivalente à multiplicação pelo gerador a em $\mathbb{F}_q C_n$, fato que garante que um subespaço vetorial $\mathcal{C}$ de $\mathbb{F}_q^n$ é um código cíclico se, e somente se, $\varphi(\mathcal{C})$ é um ideal de $\mathbb{F}_q C_n$. Logo podemos dizer que um código cíclico é um ideal de $\mathbb{F}_q C_n$. Note que, como $\mathbb{F}_q C_n$ é comutativo, todo ideal é bilateral.

Quando $mdc(q,n) = 1$, temos que a álgebra de grupo $\mathbb{F}_q C_n$ é semisimples, ou seja, se escreve como uma soma direta de ideais bilaterais minimais e todos os outros ideais desta álgebra são determinados como uma soma destes. Assim, dizemos que um *código cíclico minimal* é um ideal minimal da álgebra de grupo semisimples $\mathbb{F}_q C_n$. Como no caso dos ideais, todos os códigos cíclicos estarão determinados a partir dos códigos cíclicos minimais. Devido a essa identificação entre códigos e ideais, todas as definições feitas para códigos lineares de peso e distância minima podem ser atribuídas a ideais.

De forma geral podemos definir *código de grupo* como sendo um ideal em uma álgebra de grupo finita.

Ainda, para álgebras comutativas semisimples sabemos que os ideais minimais são gerados pelos idempotentes centrais primitivos da álgebra, logo um código cíclico minimal é do tipo $(\mathbb{F}_q C_n)e$, onde e é tal idempotente.

No próximo capítulo faremos a caracterização desses códigos.

CAPÍTULO 2

CÓDIGOS CÍCLICOS

Iniciamos este capítulo descrevendo os idempotentes primitivos que gerarão os códigos cíclicos minimais de comprimento p^n em uma álgebra de grupo semisimples $\mathbb{F}G$, onde G é um grupo cíclico de ordem p^n, tal como feito por Ferraz, Polcino e Dutra em [5] e [6], bem como o peso e a dimensão desses códigos. Esses resultados encontram-se no Lema 2.1, no Corolário 2.1 e no Lema 2.2.

Na segunda parte calculamos o peso, a dimensão e determinamos uma base de todos os códigos cíclicos em $\mathbb{F}G$, estendendo assim os resultados obtidos em [5]. Nesta seção destacamos os Lemas 2.6 e 2.7, onde podem ser encontrados os cálculos dos pesos dos códigos cíclicos mencionados.

Por último determinamos a distribuição de pesos do código com maior dimensão para um determinado peso fixado.

Optamos por não fazer as demonstrações na primeira seção já que essas são encontradas na bibliografia.

2.1 Códigos Cíclicos Minimais

Sejam $\mathbb{F}$ um corpo e G um grupo satisfazendo as seguintes hipóteses: $\mathbb{F}$ é finito, com q elementos; G é um grupo cíclico de ordem p^n, com gerador a, tal que $mdc(q, p^n) = 1$. Desta forma, $\mathbb{F}G$ é uma álgebra de grupo semisimples, logo pode ser escrita como soma de ideais minimais, os quais são gerados por idempotentes centrais primitivos de $\mathbb{F}G$. Como vimos no capítulo 1, esses ideais minimais serão os códigos cíclicos minimais de comprimento p^n em $\mathbb{F}G$.

Seja H um subgrupo de G. O elemento

$$\widehat{H} = \frac{1}{|H|} \sum_{g \in H} g,$$

de $\mathbb{F}G$ está bem definido e claramente é um idempotente de $\mathbb{F}G$.

Lema 2.1 ([5], Lema 3)**.** *Sejam $\mathbb{F}$ e G satisfazendo as hipóteses fixadas, e seja ainda*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$$

a cadeia descendente de todos os subgrupos de G. Então os elementos

$$\mathrm{e}_0 = \widehat{G} \ \text{ e } \ \mathrm{e}_i = \widehat{G_i} - \widehat{G_{i-1}}, \ i = 1, 2, ..., n, \tag{2.1}$$

formam um conjunto de idempotentes ortogonais de $\mathbb{F}G$ tal que $\mathrm{e}_0 + \mathrm{e}_1 + \cdots + \mathrm{e}_n = 1$.

Corolário 2.1 ([5], Corol. 4)**.** *Sejam $\mathbb{F}$ e G como na hipótese fixada. Então o conjunto de idempotentes dado em (2.1) é o conjunto de idempotentes centrais primitivos de $\mathbb{F}G$ se, e somente se, vale o seguinte:*

1. *$p = 2$ e ou $n = 1$ e q é ímpar ou $n = 2$ e $q \equiv 3 (\mathrm{mod}\ 4)$ ou*

2. *p é um primo ímpar e $< \bar{q} >= U(\mathbb{Z}_{p^n})$*

Nessas condições o ideal minimal $\mathcal{I}_i = (\mathbb{F}G)\mathrm{e}_i$, com $1 \leq i \leq n$ é um código cíclico minimal em $\mathbb{F}G$. Para calcular o peso e a dimensão desse código consideremos o

resultado já bem conhecido ([11], Prop. 3.6.7):

$$(\mathbb{F}G)\widehat{H} \simeq \mathbb{F}[G/H],$$

logo $dim_{\mathbb{F}}((\mathbb{F}G)\widehat{H}) = [G : H]$. Também é fácil ver que, se τ é um tranversal de H em G, então

$$\{t\widehat{H} / \, t \in \tau\}$$

é uma base de $(\mathbb{F}G)\widehat{H}$. Daí, um elemento α em tal ideal é da forma

$$\alpha = \sum_{t \in \tau} \alpha_t t\widehat{H}, \;\; \alpha_t \in \mathbb{F}.$$

Lema 2.2 ([6], Prop. 2.1)**.** *Seja $\mathcal{I}_i$, $1 \leq i \leq n$, um ideal minimal em $\mathbb{F}G$ então*

$$w(\mathcal{I}_i) = 2|G_i| = 2p^{n-i} \;\; \text{e} \;\; dim_{\mathbb{F}}(\mathcal{I}_i) = \phi(p^i) = p^i - p^{i-1},$$

e ainda uma base de $\mathcal{I}_i$ é dada por

$$\mathcal{B}_i = \{a(1-b)\widehat{G_i} \, / \, a \in A, \, 1 \neq b \in B\},$$

onde A é um transversal de G_{i-1} em G_i e B é um transversal de G_i em G.

Para o código mínimal $\mathcal{I}_0 = (\mathbb{F}G)\mathrm{e}_0$ temos:

$$w(\mathcal{I}_0) = p^n \;\; \text{e} \;\; dim_{\mathbb{F}}(\mathcal{I}_0) = 1.$$

2.2 Soma de Ideais Minimais

Sob as hipóteses fixadas para o corpo $\mathbb{F}$ e o grupo G na seção 2.1, os demais códigos cíclicos em $\mathbb{F}G$ são dados pela soma direta dos ideais minimais. Começamos calculando o peso da soma de dois ideais minimais e depois generalizamos para uma soma de t ideais minimais quaisquer e finalmente descrevemos completamente todos os códigos em $\mathbb{F}G$.

Seja agora $\mathcal{I} = \mathcal{I}_i \oplus \mathcal{I}_j$, com $0 < i < j$. A dimensão de $\mathcal{I}$ é a soma das dimensões de $\mathcal{I}_i$ e $\mathcal{I}_j$. Vamos calcular o peso desse código.

Observação 2.1. *Verifiquemos que* $\mathcal{I} \subset (\mathbb{F}G)\widehat{G_j}$.

Como $\mathcal{I} = \mathcal{I}_i \oplus \mathcal{I}_j$, dado $\gamma \in \mathcal{I}$ temos $\gamma = \alpha \mathrm{e}_i + \beta \mathrm{e}_j$, com $\alpha, \beta \in \mathbb{F}G$, então

$$\begin{aligned}
\gamma\widehat{G_j} &= \alpha \mathrm{e}_i\widehat{G_j} + \beta \mathrm{e}_j\widehat{G_j} \\
&= \alpha(\widehat{G_i} - \widehat{G_{i-1}})\widehat{G_j} + \beta(\widehat{G_j} - \widehat{G_{j-1}})\widehat{G_j} \\
&= \alpha(\widehat{G_i} - \widehat{G_{i-1}}) + \beta(\widehat{G_j} - \widehat{G_{j-1}}) \\
&= \gamma,
\end{aligned}$$

isto é, $\gamma \in (\mathbb{F}G)\widehat{G_j}$.

Então $\gamma \in \mathcal{I}$ pode ser escrito na forma

$$\gamma = \left(\sum_{t \in \tau_j} \alpha_t t \right) \widehat{G_j}, \tag{2.2}$$

onde τ_j é um transversal de G_j em G.

Lema 2.3. *Se* $0 < i < j$, *então* $w(\mathcal{I}_i \oplus \mathcal{I}_j) = 2|G_j| = 2p^{n-j}$.

Demonstração:

Suponha que, na expressão 2.2, exista apenas um coeficiente α_t não nulo. Então $\gamma = \alpha_t t\widehat{G_j}$, donde $\widehat{G_j} = \alpha_t^{-1} t^{-1} \gamma \in \mathcal{I}$. Isto é uma contradição, pois como $\mathrm{e}_i + \mathrm{e}_j$ é o elemento identidade de $\mathcal{I}$, deveríamos ter $\widehat{G_j}(\mathrm{e}_i + \mathrm{e}_j) = \widehat{G_j}$, mas

$$\widehat{G_j}(\widehat{G_i} - \widehat{G_{i-1}} + \widehat{G_j} - \widehat{G_{j-1}}) = \mathrm{e}_i + \mathrm{e}_j \neq \widehat{G_j}.$$

Logo $w(\gamma) \geq 2|G_j|$.

Seja $g \in G_{j-1} \setminus G_j$, então $g \in G_i$ e $g \in G_{i-1}$ e $\gamma = (1-g)(\mathrm{e}_i + \mathrm{e}_j) \in \mathcal{I}$ e temos que:

$$\begin{aligned}
\gamma &= (1-g)(\widehat{G_i} - \widehat{G_{i-1}}) + (1-g)(\widehat{G_j} - \widehat{G_{j-1}}) \\
&= (1-g)(\widehat{G_j} - \widehat{G_{j-1}}) \\
&= (1-g)(\widehat{G_j}).
\end{aligned}$$

Logo $w(\gamma) = 2|G_j|$, donde $w(\mathcal{I}) = 2|G_j| = 2p^{n-j}$. ■

Lema 2.4. *Se* $1 < j$ *então* $w(\mathcal{I}_0 + \mathcal{I}_j) = 2|G_j| = 2p^{n-j}$

Demonstração:

Como antes, é fácil ver que $\widehat{G_j}(\mathrm{e}_0 + \mathrm{e}_j) = \mathrm{e}_0 + \mathrm{e}_j$, donde $\mathcal{I}_0 + \mathcal{I}_j \subset (\mathbb{F}G)\widehat{G_j}$.

Novamente, $\gamma \in \mathcal{I}$ pode-se escrever na forma

$$\gamma = \left(\sum_{t \in \tau_j} \alpha_t t \right) \widehat{G_j},$$

e se houvesse γ com um único coeficiente α_t não nulo, teríamos $\widehat{G_j} = \alpha_t^{-1} t^{-1} \gamma \in \mathcal{I}$. Logo,

$$\widehat{G_j} = \widehat{G_j}(\mathrm{e}_0 + \mathrm{e}_j) = \mathrm{e}_0 + \mathrm{e}_j = \widehat{G_0} + \widehat{G_j} - \widehat{G_{j-1}}$$

e daí teríamos $\widehat{G_0} = \widehat{G_{j-1}}$ o que implicaria $j = 1$, absurdo.

Consequentemente, $w(\mathcal{I}) \geq 2|G_j|$ e tomando $\gamma = (1 - g)(\mathrm{e}_0 + \mathrm{e}_j)$ com $g \in G \setminus G_j$, como no lema anterior, temos $w(\gamma) = 2|G_j|$, logo $w(\mathcal{I}) = 2|G_j|$. ■

Lema 2.5. *Se* $\mathcal{I} = \mathcal{I}_0 + \mathcal{I}_1$, *então* $w(\mathcal{I}) = |G_1| = p^{n-1}$.

Demonstração:

Basta observar que $\mathrm{e}_0 + \mathrm{e}_1 = \widehat{G_0} + \widehat{G_1} - \widehat{G_0} = \widehat{G_1}$ daí se conclui que $\mathcal{I} = (\mathbb{F}G)\widehat{G_1}$. Como $\widehat{G_1} \in \mathcal{I}$ segue facilmente que $w(\mathcal{I}) = w(\widehat{G_1}) = |G_1| = p^{n-1}$. ■

Agora generalizaremos o cálculo do peso da soma direta de t ideais minimais. Essa generalização será feita em duas partes: primeiro consideraremos uma soma de ideais minimais consecutivos e depois uma soma de ideais minimais arbitrários.

Lema 2.6. *Seja* $\mathcal{I} = (\mathbb{F}G)\mathrm{e}_0 \oplus (\mathbb{F}G)\mathrm{e}_1 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_t$, *então* $\mathcal{I} = (\mathbb{F}G)\widehat{G_t}$ *e* $w(\mathcal{I}) = |G_t| = p^{n-t}$.

Demonstração:

Primeiro verifiquemos que $\bigoplus_{i=0}^{t} \mathbb{F}G\mathrm{e}_i = \mathbb{F}G(\mathrm{e}_0 + \cdots + \mathrm{e}_t)$

- É fácil ver que $\mathbb{F}G(\mathrm{e}_0 + \cdots + \mathrm{e}_t) \subset \bigoplus_{i=0}^{t} (\mathbb{F}G)\mathrm{e}_i$

- $\bigoplus_{i=0}^{t}(\mathbb{F}G)\mathrm{e}_i \subset \mathbb{F}G(\mathrm{e}_0+\mathrm{e}_1+\cdots+\mathrm{e}_t)$ pois, como os elementos e_i, $0 \leq i \leq t$ são dois a dois ortogonais então:

$$\mathrm{e}_i = \mathrm{e}_i(\mathrm{e}_0+\cdots+\mathrm{e}_t), \ \ \forall i = 0, 1, ..., t.$$

  Consequentemente $\bigoplus_{i=0}^{t}(\mathbb{F}G)\mathrm{e}_i \subset \mathbb{F}G(\mathrm{e}_0+\mathrm{e}_1+\cdots+\mathrm{e}_t)$.

Portanto, $\bigoplus_{i=0}^{t}(\mathbb{F}G)\mathrm{e}_i = \mathbb{F}G(\mathrm{e}_0+\mathrm{e}_1+\cdots+\mathrm{e}_t)$.

Agora basta observar que

$$\mathrm{e}_0+\mathrm{e}_1+\cdots+\mathrm{e}_t = \widehat{G_0} + (\widehat{G_1}-\widehat{G_0}) + \cdots + (\widehat{G_t}-\widehat{G_{t-1}}) = \widehat{G_t}.$$

Então $\mathcal{I} = (\mathbb{F}G)\widehat{G_t}$ e $w(\mathcal{I}) = |G_t| = p^{n-t}$. ■

No próximo Lema consideraremos uma soma de ideais minimais não consecutivos, ou seja, excluímos um, ou mais ideais minimais da soma $(\mathbb{F}G)\mathrm{e}_0 \oplus (\mathbb{F}G)\mathrm{e}_1 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_t$.

Lema 2.7. *Se* $\mathcal{I} = \bigoplus_{k=1}^{t}(\mathbb{F}G)\mathrm{e}_{i_k}$, *com* $0 \leq i_1 < i_2 < \cdots < i_t$ *e* $\mathrm{e}_{i_1}+\mathrm{e}_{i_2}+\cdots+e_{i_t} \neq \mathrm{e}_0+\mathrm{e}_1+\cdots+\mathrm{e}_t$, *então* $w(\mathcal{I}) = 2|G_{i_t}| = 2p^{n-i_t}$.

Demonstração:

Como $(\mathrm{e}_{i_1}+\mathrm{e}_{i_2}+\cdots+e_{i_t})$ é a identidade de $\bigoplus_{k=1}^{t}(\mathbb{F}G)\mathrm{e}_{i_k}$, devemos ter

$$(\mathrm{e}_{i_1}+\mathrm{e}_{i_2}+\cdots+e_{i_t})\widehat{G_{i_t}} = (\mathrm{e}_{i_1}+\mathrm{e}_{i_2}+\cdots+e_{i_t}),$$

donde $\mathcal{I} \subset (\mathbb{F}G)\widehat{G_{i_t}}$.

Seja τ um transversal de G_{i_t} em G. Escrevendo $\gamma = \left(\sum_{t\in\tau}\alpha_t t\right)\widehat{G_{i_t}}$, se existisse $\gamma \in \mathcal{I}$ com um único α_t não nulo teríamos, como antes, que $\widehat{G_{i_t}} \in \mathcal{I}$ e, multiplicando pela identidade deste ideal, teríamos:

$$\widehat{G_{i_t}} = \widehat{G_{i_t}}(\mathrm{e}_{i_1}+\mathrm{e}_{i_2}+\cdots+e_{i_t}) = (\mathrm{e}_{i_1}+\mathrm{e}_{i_2}+\cdots+e_{i_t}). \tag{2.3}$$

Se $(\mathrm{e}_{i_1}+\mathrm{e}_{i_2}+\cdots+e_{i_t}) \neq \mathrm{e}_0+\mathrm{e}_1+\cdots+\mathrm{e}_t$, existe um idempotente e_l, com $0 \leq l \leq t-1$ que não aparece na soma a esquerda. Multiplicando (2.3) por esse idempotente temos:

$$\widehat{G_{i_t}}\mathrm{e}_l = (\mathrm{e}_{i_1} + \mathrm{e}_{i_2} + \cdots + e_{i_t})\mathrm{e}_l = 0$$

logo, $0 = \widehat{G_{i_t}}(\widehat{G_l} - \widehat{G_{l-1}}) = \widehat{G_l} - \widehat{G_{l-1}}$, absurdo.

Assim, para todo $\gamma \in \mathcal{I}$, temos $w(\gamma) \geq 2|G_{i_t}|$, donde $w(\mathcal{I}) \geq 2|G_{i_t}|$ e tomando $g \in G_{i_{t-1}} \setminus G_{i_t}$, como antes temos

$$\gamma = (1-g)(\mathrm{e}_{i_1} + \mathrm{e}_{i_2} + \cdots + \mathrm{e}_{i_t}) = (1-g)\widehat{G_{i_t}},$$

donde $w(\mathcal{I}) = w(\gamma) = 2|G_{i_t}| = 2p^{n-i_t}$. ■

Pelos lemas anteriores concluímos que há dois tipos de somas de ideias minimais em $\mathbb{F}_q C_{p^n}$; um quando somamos ideais minimais consecutivos, como no Lema 2.6, resultando em um ideal de peso p^{n-t} e o outro caso, como no Lema 2.7, onde não consideramos a soma consecutiva de ideais minimais, resultando em um ideal de peso $2p^{n-t}$. Assim, podemos determinar o código cíclico com maior dimensão para um determinado peso.

Teorema 2.2.1. *Para cada inteiro j, com $0 \leq j \leq n$, o código cíclico de maior dimensão com peso p^{n-j} é*

$$\mathcal{I} = (\mathbb{F}G)\mathrm{e}_0 \oplus (\mathbb{F}G)\mathrm{e}_1 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j.$$

Neste caso $dim\mathcal{I} = p^j$.

O código cíclico com peso $2p^{n-j}$ de maior dimensão é

$$\mathcal{I} = (\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j$$

com $dim\mathcal{I} = p^j - 1$.

Demonstração:

Para obtermos um ideal com peso p^{n-j} segue imediatamente do Lema 2.6 que, o único ideal com tal peso dever ser uma soma do tipo $\mathcal{I} = (\mathbb{F}G)\mathrm{e}_0 \oplus (\mathbb{F}G)\mathrm{e}_1 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j$. E a dimensão desse ideal é dada por $dim\mathcal{I} = 1+(p-1)+(p^2-p)+\cdots+(p^j-p^{j-1}) = p^j$

Já para termos um ideal de peso $2p^{n-j}$, segue do Lema 2.7, que esse ideal é uma soma de ideais minimais não consecutivos, então da soma $\mathcal{I} = (\mathbb{F}G)\mathrm{e}_0 \oplus (\mathbb{F}G)\mathrm{e}_1 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j$ devemos eliminar algum somando. Como queremos o ideal de maior dimensão e a dimensão do ideal $\mathcal{I}$ é dada pela soma das dimensões de cada ideal minimal então eliminamos o de menor dimensão e esse é o ideal $(\mathbb{F}G)\mathrm{e}_0$. Assim obtemos o ideal

$$\mathcal{I} = (\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j$$

e sua dimensão é $dim\mathcal{I} = (p-1) + (p^2 - p) + \cdots + (p^j - p^{j-1}) = p^j - 1$. ■

Observação 2.2. *No final desse trabalho faremos uma breve comparação entre códigos cíclicos e códigos abelianos não cíclicos de comprimento p^2.*

Assim observe que em $\mathbb{F}C_{p^2}$ existem apenas três idempotentes minimais, a saber:

$$e_0 = \widehat{G}, \;\; e_1 = \widehat{G_1} - \widehat{G} \;\text{ e }\; e_2 = \widehat{G_2} - \widehat{G_1}$$

logo há apenas ideais somas com dois ideais minimais que nos dão ideais não trivias. De acordo com o Teorema 2.2.1 os ideais com maior dimensão para cada peso possível são

$$\mathcal{I} = \mathcal{I}_0 \oplus \mathcal{I}_1 \;\text{ e }\; J = \mathcal{I}_1 \oplus \mathcal{I}_2$$

com $dim(\mathcal{I}) = p$, $w(\mathcal{I}) = p$ e $dim(J) = p^2 - 1$, $w(J) = 2$.

2.3 Distribuição de Pesos

A distribuição de pesos de um código determina para cada peso possível, a quantidade de palavras do código que tem esse peso. Faremos a distribuição de peso dos códigos citados no Teorema 2.2.1.

1. Consideraremos primeiro o código $\mathcal{I} = (\mathbb{F}G)\mathrm{e}_0 \oplus (\mathbb{F}G)\mathrm{e}_1 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j$, para $0 \leq j \leq n$.

Neste caso temos $\mathcal{I} = (\mathbb{F}G)\widehat{G_j}$, logo se $\alpha \in \mathcal{I}$ então $\alpha = \left(\sum_{i=0}^{p^j-1} \alpha_i a^i\right)\widehat{G_j}$.

Observe que, como $|G_j| = p^{n-j}$, então toda palavra em $\mathcal{I}$ tem peso igual a lp^{n-j}, com $l \in \mathbb{N}$.

(a) Existe apenas uma palavra de peso 0: essa é a palavra nula.

(b) Com peso igual a p^{n-j} temos $\begin{pmatrix} p^j \\ 1 \end{pmatrix}(q-1)$ palavras, pois apenas o coeficiente correspondente a um elemento do transversal é não nulo. Temos p^j elementos no transversal e, para cada uma deles, há $(q-1)$ coeficientes possíveis.

(c) Da mesma forma, com peso $2p^{n-j}$ temos $\begin{pmatrix} p^j \\ 2 \end{pmatrix}(q-1)^2$ palavras, pois temos que escolher dois elementos do transversal entre p^j possibilidades e para cada posição há $(q-1)$ coeficientes possíveis.

Generalizando, há $\begin{pmatrix} p^j \\ l \end{pmatrix}(q-1)^l$ palavras com peso lp^{n-j}.

2. Agora consideremos o código $\mathcal{I} = (\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j$.

Afirmamos que $\mathcal{I} = (\mathbb{F}G)(\widehat{G_j} - \widehat{G})$ e que $\alpha \in \mathcal{I}$ se, e somente se, $\alpha \in (\mathbb{F}G)\widehat{G_j}$ e tem aumento zero.

De fato, $\mathcal{I} = (\mathbb{F}G)(\widehat{G_j} - \widehat{G})$ pois, vimos no Lema 2.7, que

$$(\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j = \mathbb{F}G(e_1 + \cdots + e_j)$$

e, como $e_1 + \cdots + e_j = \widehat{G_j} - \widehat{G}$, temos $\mathcal{I} = (\mathbb{F}G)(\widehat{G_j} - \widehat{G})$.

Agora suponha $\alpha \in \mathcal{I}$ e provemos a segunda parte.

Primeiro observe que $(\mathbb{F}G)\widehat{G_j} = (\mathbb{F}G)(\widehat{G_j} - \widehat{G}) \oplus (\mathbb{F}G)\widehat{G}$, logo $(\mathbb{F}G)(\widehat{G_j} - \widehat{G}) \subset (\mathbb{F}G)\widehat{G_j}$.

Logo, se $\alpha \in \mathcal{I}$ então $\alpha \in (\mathbb{F}G)\widehat{G_j}$. Como

$$\{(1-a^k)\widehat{G_j}, \quad k = 1, 2, \cdots p^j - 1\}$$

é base de $(\mathbb{F}G)(\widehat{G_j} - \widehat{G})$ então

$$\alpha = \sum_{k=1}^{p^j-1} \alpha_k (1-a^k)\widehat{G_j}$$

e claramente α tem aumento zero.

Por outro lado, suponha $\alpha \in (\mathbb{F}G)\widehat{G_j}$ com aumento zero. Então α pode ser escrito na forma $\alpha = \sum_{i=0}^{p^j-1} \alpha_i a^i \widehat{G_j}$, com $\alpha_i \in \mathbb{F}$, $0 \leq i \leq p^j - 1$.

Logo $\varepsilon(\alpha) = \sum_{i=0}^{p^j-1} (\alpha_i)\,|G_j|$. Como α tem aumento nulo, temos $\sum_{i=0}^{p^j-1} \alpha_i = 0$.

Ainda, podemos escrever $\alpha = \alpha_1 + \alpha_2$ com $\alpha_1 \in (\mathbb{F}G)(\widehat{G_j} - \widehat{G})$ e $\alpha_2 \in (\mathbb{F}G)\widehat{G}$. Multiplicando α por $\widehat{G}$ temos

$$\alpha\widehat{G} = \alpha_1\widehat{G} + \alpha_2\widehat{G} = \alpha_2,$$

pois $(\widehat{G_j} - \widehat{G})\widehat{G} = 0$. Logo:

$$\alpha\widehat{G} = \sum_{i=1}^{p^j-1} \alpha_i a^i \widehat{G_j}\widehat{G} = \alpha_2 \Rightarrow \sum_{i=1}^{p^j-1} \alpha_i a^i \widehat{G} = \alpha_2,$$

donde $\left(\sum_{i=1}^{p^j-1} \alpha_i\right)\widehat{G} = \alpha_2$ e, como $\sum_{i=1}^{p^j-1} \alpha_i = 0$, temos $\alpha_2 = 0$. Assim $\alpha = \alpha_1 \in (\mathbb{F}G)(\widehat{G_j} - \widehat{G})$. Portanto, se $\alpha \in \mathcal{I}$ então $\alpha = \sum_{i=1}^{p^j-1} \alpha_i a^i \widehat{G_j}$ e $\sum_{i=1}^{p^j-1} \alpha_i = 0$.

Agora podemos determinar a distribuição de pesos desse código. Observe que também nesse caso o peso de toda palavra é da forma lp^{n-j}.

(a) Existe apenas uma palavra de peso 0; essa é a palavra nula.

(b) Não existem palavras de peso $1p^{n-j}$, pois essas palavras não tem aumento zero, logo não pertencem a $\mathcal{I}$.

(c) Com peso $2p^{n-j}$ temos $\begin{pmatrix} p^j \\ 2 \end{pmatrix} \underbrace{(q-1)\cdot 1}_{t_2}$, palavras, pois devemos escolher 2 posições entre p^j possíveis elementos do transversal e, para a primeira posição há $(q-1)$ coeficientes possíveis. O segundo coeficiente está fixado pela hipótese de aumento zero.

(d) Com peso $3p^{n-j}$ são $\begin{pmatrix} p^j \\ 3 \end{pmatrix} \underbrace{((q-1)^2 - t_2)\cdot 1}_{t_3}$ palavras, pois temos que escolher 3 posições entre p^j posições. Para as duas primeiras posições não podemos ter aumento zero, caso contrário α não teria aumento zero já que na terceira posição temos um elemento não nulo. Note que há $t_2 = (q-1)$ maneiras de ter o aumento nulo nas duas primeiras posições. Então para as duas primeiras posições temos um total de $(q-1)^2 - t_2$ possibilidades. A última posição está fixada pela hipótese.

(e) Analogamente, com peso $4p^{n-j}$, temos $\begin{pmatrix} p^j \\ 4 \end{pmatrix} \underbrace{((q-1)^3 - t_3)\cdot 1}_{t_4}$ palavras.

Generalizando, se indicamos por t_{l-1} o número de maneiras de obter $l-1$ coeficientes escolhidos em $\mathbb{F}$, cuja soma é zero; então existem $\begin{pmatrix} p^j \\ l \end{pmatrix} \underbrace{((q-1)^{l-1} - t_{l-1})\cdot 1}_{t_l}$ palavras com peso lp^{n-j}.

Reunindo os resultados acima, nesta seção provamos o seguinte:

Teorema 2.3.1. *Seja $\mathcal{I} = (\mathbb{F}G)\mathrm{e}_0 \oplus (\mathbb{F}G)\mathrm{e}_1 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j$ um código, então toda palavra em $\mathcal{I}$ tem peso igual a lp^{n-j}, com $l \in \mathbb{N}$ e há $\begin{pmatrix} p^j \\ l \end{pmatrix} (q-1)^l$ palavras para cada possível peso.*

Agora seja o código $\mathcal{I} = (\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{e}_j$, então toda palavra nesse código tem peso lp^{n-j}, com $l \in \mathbb{N}$ e $l \neq 1$. E há $\begin{pmatrix} p^j \\ l \end{pmatrix} \underbrace{((q-1)^{l-1} - t_{l-1})\cdot 1}_{t_l}$ palavras com peso lp^{n-j}, onde t_{l-1} indica o número de maneiras de obter $l-1$ coeficientes escolhidos em $\mathbb{F}$, cuja soma é zero.

CAPÍTULO 3

CÓDIGOS ABELIANOS

Seguindo o caminho de construção de idempotentes em uma álgebra de grupo a partir de um subgrupo do grupo dado; na primeira seção deste capítulo descrevemos os idempotentes primitivos da álgebra de grupo $\mathbb{F}G$, onde G é um p-grupo abeliano finito com p primo e $\mathbb{F}$ um corpo finito de característica q, com mdc(q,p) = 1, como pode ser visto no Lema 3.1 e no Teorema 3.1.1. Esses idempotentes geram os códigos abelianos minimais em $\mathbb{F}G$. Em particular, apresentamos os códigos abelianos minimais de comprimento p^n e calculamos o peso e a dimensão desses códigos.

Na segunda seção estudamos os códigos abelianos de comprimento p^2 que são soma de dois códigos abelianos minimais desse comprimento, calculando o peso e a dimensão desse código. Os resultados obtidos com esse estudo estende os resultados em [5] e [6].

Na última seção apresentamos alguns exemplos de códigos abelianos de comprimento p^2 e o peso desses códigos, o qual foi possível calcular com o uso do software Groups, Algorithm, Programming - GAP.

As demonstrações da primeira seção são omitidas, pois podem ser encontradas na bibliografia.

3.1 Códigos Abelianos Minimais

Seja $\mathbb{F}$ um corpo finito com q elementos e G um p-grupo abeliano. Para cada subgrupo H de G tal que $G/H \neq \{1\}$ é cíclico, vamos construir um idempotente de $\mathbb{F}G$. Observemos que, como G/H é um grupo cíclico de ordem potência de p, existe somente um subgrupo H^* de G contendo H, tal que $|H^*/H| = p$. Definimos $\mathrm{e}_H = \widehat{H} - \widehat{H^*}$. Claramente $\mathrm{e}_H \neq 0$ e temos o seguinte:

Lema 3.1. *([5], Lema 5) Os elementos* e_H*, definidos acima, juntos com* $\mathrm{e}_G = \widehat{G}$ *formam um conjunto de idempotentes dois a dois ortogonais de* $\mathbb{F}G$ *cuja soma é igual a* 1.

Teorema 3.1.1. *([5], Teorema 4.1) Seja* p *um primo e seja* G *um* p*-grupo abeliano de expoente* p^r*. Então, o conjunto de idempotentes acima é o conjunto de idempotentes primitivos de* $\mathbb{F}G$ *se, e somente se, vale uma das seguintes afirmações:*

(i) $p^r = 2$ *e* q *é ímpar;*

(ii) $p^r = 4$ *e* $q \equiv 3 (mod\ 4)$*;*

(iii) p *é um primo ímpar e* $< \bar{q} >= U(\mathbb{Z}_{p^r})$.

No que segue, vamos considerar códigos abelianos não cíclicos de comprimento p^2; isto é, ideais da álgebra de grupo $\mathbb{F}(C_p \times C_p)$. Nosso objetivo é verificar se existe alguma vantagem em passar de códigos cíclicos a códigos abelianos não cíclicos.

Vamos considerar inicialmente $G \simeq \underbrace{C_p \times \cdots \times C_p}_{n}$. De acordo com os teoremas anteriores, para escrever os idempotentes primitivos da álgebra de grupo $\mathbb{F}G$, precisamos encontrar os subgrupos H de G tal que G/H é um grupo cíclico. Neste caso, tal propriedade ocorre para os subgrupos de ordem p^{n-1}. De fato, considere o homomorfismo canônico

$$\begin{aligned} \pi : \quad G &\to \quad G/H \\ g &\mapsto \quad gH \end{aligned}$$

temos que $o(\pi(g)) = o(gH))$ divide $o(g)$, e como todos os elementos $1 \neq g \in G$ tem ordem p, então $o(gH) = p$. Assim se G/H é cíclico então $|G/H| = p$, daí $|H| = p^{n-1}$.

Dessa forma os idempotentes centrais primitivos de $\mathbb{F}G$ devem ser

$$e_G = \widehat{G} \quad \text{e} \quad e_H = \widehat{H} - \widehat{G},$$

onde H é um subgrupo de G de ordem p^{n-1}. Como consequência, temos o seguintes resultado sobre o peso, a dimensão e a base desses códigos abelianos minimais:

Proposição 3.1. *[6] Sejam G, $\mathbb{F}$, H como antes. E também $e = \widehat{H} - \widehat{G}$, então*

$$dim((\mathbb{F}G)e) = |G/H| - |G/G| = p - 1 \ \text{ e } \ w((\mathbb{F}G)e) = 2|H| = 2p^{n-1}.$$

Proposição 3.2. *Seja τ um transversal de H em G. Então uma base de $(\mathbb{F}G)e_H$ sobre $\mathbb{F}$ é:*

$$\mathcal{B} = \{(1-t)\widehat{H} / \, t \in \tau \setminus \{1\}\}$$

3.2 Soma de Ideais Minimais

Nesta seção consideraremos o caso particular do p-grupo abeliano $G = C_p \times C_p = < a > \times < b >$, para esse caso temos que os idempotentes da álgebra $\mathbb{F}G$ são:

$$\mathrm{e}_0 = \widehat{G}, \ \mathrm{e}_1 = \widehat{< a >} - \widehat{G}, \ \mathrm{e}_2 = \widehat{< b >} - \widehat{G}, \ f_i = \widehat{< ab^i >} - \widehat{G}, 1 \leq i \leq p-1.$$

Aqui determinaremos o peso e a dimensão dos códigos abelianos obtidos como a soma de dois códigos abelianos minimais. Veremos no último capítulo que, sob certo ponto de vista, esses códigos são melhores que os códigos cíclicos de comprimento p^2, já mencionados na observação 2.2. Completando assim o objetivo dessa tese.

Observe que se H, K são dois subgrupos quaisquer dentre os subgrupos $< a >$, $< b >$ e $< ab^i >$, $1 \leq i \leq p-1$, então $G = H \times K$.

Escrevendo $H =< h >$ e $K =< k >$, os idempotentes centrais associados a estes grupos são $e = \widehat{H} - \widehat{G}$, $f = \widehat{K} - \widehat{G}$. Seja

$$\mathcal{I} = (\mathbb{F}G)e \oplus (\mathbb{F}G)f,$$

então $\mathcal{B} = \{(1-k^i)\widehat{H} \ / \ 1 \leq i \leq p-1\} \bigcup \{(1-h^j)\widehat{K} \ / \ 1 \leq j \leq p-1\}$ é uma base de $\mathcal{I}$.

Logo todo elemento $\alpha \in \mathcal{I}$ pode ser escrito na forma:

$$\alpha = \sum_{i=1}^{p-1} x_i(1-k^i)\widehat{H} + \sum_{j=1}^{p-1} y_j(1-h^j)\widehat{K}$$

com $x_i, y_j \in \mathbb{F}$. Daí

$$\begin{aligned}
\alpha &= \sum_{i=1}^{p-1} x_i\widehat{H} - \sum_{i=1}^{p-1} x_i h^i \widehat{H} + \sum_{j=1}^{p-1} y_j \widehat{K} - \sum_{j=1}^{p-1} y_j h^j \widehat{K} \\
\alpha &= \underbrace{\left(\sum_{i=1}^{p-1} x_i + \sum_{j=1}^{p-1} y_j\right) 1}_{\alpha_1} + \underbrace{\sum_{i=1}^{p-1}\left(-x_i + \sum_{j=1}^{p-1} y_j\right) k^i}_{\alpha_2} + \\
&\quad \underbrace{\sum_{j=1}^{p-1}\left(-y_j + \sum_{i=1}^{p-1} x_i\right) h^j}_{\alpha_3} - \underbrace{\sum_{i,j=1}^{p-1}(x_i+y_j)k^i h^j}_{\alpha_4} \\
\alpha &= \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \qquad (3.1)
\end{aligned}$$

Como os respectivos suportes de α_1, α_2, α_3 e α_4 são disjuntos temos

$$w(\alpha) = w(\alpha_1) + w(\alpha_2) + w(\alpha_3) + w(\alpha_4)$$

e $w(\alpha_1) \leq 1$, $w(\alpha_2), w(\alpha_3) \leq p-1$, $w(\alpha_4) \leq (p-1)^2$.

No caso particular em que $x_1 = x_2 = \cdots = x_{p-1} = -y_1 = -y_2 = \cdots = -y_{p-1}$, temos $w(\alpha) = 2p-2$, pois claramente

$$w(\alpha_1) = w(\alpha_4) = 0$$

e

$$w(\alpha_2) = w(\alpha_3) = p-1,$$

já que se em α_2 o coeficiente de k^i, para algum i, fosse zero, então

$$\begin{aligned}
x_i &= \sum_{j=1}^{p-1} y_j \\
-y_1 &= (p-1)y_1 \\
py_1 &= 0.
\end{aligned}$$

Isto é absurdo, pois $y_1 \in \mathbb{F}$ e a característica de $\mathbb{F}$ não divide p . De forma análoga segue o resultado para $w(\alpha_3)$.

Queremos provar agora que $w(\mathcal{I}) = 2p-2$, então precisamos provar que não existe $\beta \in \mathcal{I}$ tal que $w(\beta) < 2p-2$. Para isso suponha que existe tal elemento e seja β esse elemento; escrevemos $\beta = \beta_1+\beta_2+\beta_3+\beta_4$ como em (3.1). Observe que se $w(\beta) < 2p-2$ então devemos ter $w(\beta_4) < 2p-2$.

Apartir de agora vamos estudar o peso de β_4, mais especificamente quando $w(\beta_4) = 2p-k$, $k = 3, 4, \cdots, 2p-1$.

Vamos dispor os coeficientes de β_4 numa matriz:

$$\mathcal{A} = \begin{bmatrix} x_1+y_1 & x_1+y_2 & \cdots & x_1+y_{p-1} \\ x_2+y_1 & x_2+y_2 & \cdots & x_2+y_{p-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{p-1}+y_1 & x_{p-1}+y_2 & \cdots & x_{p-1}+y_{p-1} \end{bmatrix}$$

3.2.1 Caso $p > 3$

Vamos considerar inicialmente o caso em que $p > 3$, assim a matriz $\mathcal{A}$ tem pelo menos 4 linhas e 4 colunas.

Lema 3.2. *A matriz $\mathcal{A}$ não contém nenhuma submatriz 2×2 da forma:*

$$\mathcal{A}' = \begin{bmatrix} a_{ij} & a_{ik} \\ a_{hj} & a_{hk} \end{bmatrix}$$

com um elemento não nulo e os outros três elementos iguais a zero.

Demonstração:

Suponha $a_{ij} \neq 0$, os outros casos são análogos. Então temos:

$$\begin{aligned} x_i + y_k &= 0 \\ x_h + y_k &= 0 \\ x_h + y_j &= 0 \end{aligned}$$

logo $x_i = -y_k = x_h = -y_j$, portanto, $a_{ij} = x_i + y_j = 0$, contradição. ■

Lema 3.3. *Seja $w(\beta_4) = 2p - k$, para $k = 3, 4, \cdots, 2p - 1$. A matriz $\mathcal{A}$ só pode ter linhas cujos elementos sejam todos iguais a zero se, e somente se, $k = p + 1$.*

Demonstração:

Suponha que existe uma linha i_0 cujos elementos são todos nulos, então:

$$-x_{i_0} = y_1 = y_2 = \cdots = y_{p-1}.$$

Se existe algum outro elemento nulo na matriz, devem existir índices i, j tais que $-x_i = y_j$. Como vimos acima os elementos y_j, $1 \leq j \leq p - 1$, são todos iguais entre si, segue então que todos os elementos da linha i devem ser iguais a zero.

Como cada linha tem $p - 1$ elementos, o argumento acima mostra que o número total de elementos nulo na matriz é um múltiplo de $p - 1$.

Agora, se $w(\beta_4) = 2p - k$, β_4 deve ter exatamente $(p-1)^2 - (2p - k) = (p-1)^2 - 2(p-1) + k - 2$ coeficientes iguais a zero, portanto:

$$(p - 1) \mid [(p - 1)^2 + 2(p - 1) + k - 2],$$

logo $(p - 1) \mid [k - 2]$.

Mas $1 \leq k - 2 \leq 2p - 3$, então para $k - 2 = t(p - 1)$ deve-se ter $k = p + 1$.

Por outro lado, suponha agora que $k = p+1$, ou seja, $w(\beta_4) = p-1$. E suponha que a matriz $\mathcal{A}$ não tem nenhuma linha nula, ou seja, toda linha tem um único elementos não nulo. Se esses elementos não estão na mesma coluna temos, imediatamente, do Lema 3.2 uma contradição. Logo todos os elementos não nulos estão na mesma coluna ou equivalemente em uma mesma linha e as demais linhas da matriz são nulas

■

Vamos considerar o caso quando $k = p + 1$. Assim $w(\beta_4) = 2p - (p + 1) = p - 1$. Verifiquemos que nesse caso $w(\beta) \geq 2p - 2$.

Lema 3.4. *Se $w(\beta_4) = p - 1$ então $w(\beta_2) \geq p - 2$ e, caso $w(\beta_2) = p - 2$, então $w(\beta_1) = 1$.*

Demonstração:

Pelo Lema 3.3 se $w(\beta_4) = p-1$, então para algum i_0 os elementos da linha i_0 são todos não nulos, isto é, $-x_{i_o} \neq y_1 = y_2 = \cdots = y_{p-1}$ e, as demais linhas são nulas, $-x_i = y_1 = y_2 = \cdots = y_{p-1}$.

Suponha, em (3.1), que o coeficiente de k^i, com $i \neq i_0$, é zero. Assim:

$$x_i = \sum_{j=1}^{p-1} y_j \implies -y_1 = (p-1)y_1 \implies py_1 = 0,$$

o que é um absurdo. Portanto $w(\beta_2) \geq p-2$.

Se $w(\beta_2) = p-2$, então o coeficiente de k^{i_0} é zero, logo

$$x_{i_0} = \sum_{j=1}^{p-1} y_j \implies x_{i_0} = (p-1)y_1.$$

Nesse caso se $w(\beta_1) = 0$, então

$$\begin{aligned} \sum_{i=1}^{p-1} x_i &= -\sum_{j=1}^{p-1} y_j \\ x_{i_0} + \sum_{i \neq i_0} x_i &= -\sum_{j=1}^{p-1} y_j \\ (p-1)y_1 - (p-2)y_1 &= -(p-1)y_1 \\ py_1 &= 0 \end{aligned}$$

absurdo, portanto $w(\beta_1) = 1$. ■

Proposição 3.3. *Não existe $\beta \in \mathcal{I}$ com $w(\beta) \leq 2p-3$ e $w(\beta_4) = p-1$.*

Demonstração:

Pelo Lema 3.4 se $w(\beta_4) = p-1$, então ou $w(\beta_2) = p-1$ e daí

$$w(\beta) \geq w(\beta_2) + w(\beta_4) = p-1+p-1 = 2p-2,$$

ou $w(\beta_2) = p-2$ e $w(\beta_1) = 1$ e então:

$$w(\beta) \geq w(\beta_1) + w(\beta_2) + w(\beta_4) = 1+p-2+p-1 = 2p-2.$$

■

Agora consideramos o caso $w(\beta_4) = 2p - k$, $k = 3, 4, \cdots, 2p-1$ e $k \neq p+1$. Assim, de acordo com o Lema 3.3, toda linha da matriz $\mathcal{A}$ tem pelo menos um elemento não nulo.

Lema 3.5. *Se $\beta \in \mathcal{I}$ e $w(\beta_4) = 2p - k$, então existe pelo menos uma linha de $\mathcal{A}$ que tem um único elemento não nulo.*

Demonstração:

Suponha que toda linha de $\mathcal{A}$ tem pelo menos dois elementos não nulos. Como $\mathcal{A}$ tem $p-1$ linhas, há pelo menos $2(p-1)$ elementos não nulos. Consequentemente

$$w(\beta_4) \geq 2(p-1) > 2p - k,$$

uma contradição. ■

Lema 3.6. *Se $a_{i_0 j_0} = x_{i_0} + y_{j_0}$ é o único elemento não nulo de uma linha da matriz $\mathcal{A}$ e $a_{i_1 j_1} = x_{i_1} + y_{j_1}$ é o único elemento não nulo de outra linha (i.e., se $i_0 \neq i_1$), então $j_0 = j_1$.*

Demonstração:

Se $j_1 \neq j_0$ temos $a_{i_0 j_1} = 0$. Como a matriz contém pelo menos outra coluna j_2 diferente de j_0 e j_1, temos $a_{i_1 j_0} = a_{i_1 j_2} = 0$ e também $a_{i_0 j_2} = 0$. Ficamos com a seguinte submatriz:

$$\mathcal{A}' = \begin{bmatrix} a_{i_0 j_0} & a_{i_0 j_1} & a_{i_0 j_2} \\ a_{i_1 j_0} & a_{i_1 j_1} & a_{i_1 j_2} \end{bmatrix} = \begin{bmatrix} a_{i_0 j_0} & 0 & 0 \\ 0 & a_{i_1 j_1} & 0 \end{bmatrix}$$

Temos assim uma submatriz 2×2 com exatamente três elementos nulos, uma contradição conforme o Lema 3.2. Portanto, $j_0 = j_1$. ■

Lema 3.7. *Se $a_{i_0 j_0} \in \mathcal{A}$ é o único elemento não nulo de índice i_0 e outra linha, de índice i_1, tem pelo menos dois elementos não nulos, então vale uma das seguintes condições:*

(i) *A linha i_1 tem todos os seus elementos não nulos.*

(ii) *O elemento $a_{i_1 j_0}$ é nulo e os demais elementos desta linha são não nulos.*

Demonstração:

Suponha que $a_{i_1 j_0} \neq 0$. Veremos que todos os elementos da linha i_1 têm que ser não nulos. De fato, seja $a_{i_1 j_1}$ um outro elemento não nulo da mesma linha. Dado qualquer elemento $a_{i_1 j}$ desta linha com $j \neq j_0, j_1$ se $a_{i_1 j} = 0$ a submatriz

$$\begin{bmatrix} a_{i_1 j_1} & a_{i_1 j} \\ a_{i_0 j_1} & a_{i_0 j} \end{bmatrix} = \begin{bmatrix} a_{i_1 j_1} & 0 \\ 0 & 0 \end{bmatrix}$$

tem um elemento não nulo e três iguais a zero, uma contradição pelo Lema 3.2.

Assim, se $a_{i_1 j_0} \neq 0$ toda a linha i_1 é formada por elementos não nulos e vale (i).

Se $a_{i_1 j_0} = 0$ e existe outro elemento $a_{i_1 j} = 0$, então temos a seguinte submatriz

$$\begin{bmatrix} a_{i_1 j_0} & a_{i_1 j} \\ a_{i_0 j_0} & a_{i_0 j} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a_{i_0 j_0} & 0 \end{bmatrix}$$

e novamente temos uma contradição pelo Lema 3.2. Logo se $a_{i_1 j_0} = 0$ então vale (ii). ■

Observação 3.1. *Este lema mostra que se $\beta \in \mathcal{I}$ e $w(\beta) = 2p-3$, então $w(\beta_4) = 2p-3$ ou $w(\beta_4) = 2p-4$.*

De fato, se estamos na condição (i), na linha i_1 temos $(p-1)$ elementos não nulos e nas demais $(p-2)$ linhas devemos ter apenas um elemento não nulo para não ultrapassar o peso de β, então temos um total de $(p-1)+(p-2) = 2p-3$ elementos não nulos. Portanto $w(\beta_4) = 2p-3$.

E se estamos na condição (ii) na linha i_1 temos $(p-2)$ elementos não nulos, na linha i_0 e nas demais devemos ter novamente apenas um elemento não nulo dando um total de $(p-2)+(p-2) = 2p-4$. Portanto $w(\beta_4) = 2p-4$.

Pelo Lema 3.6, em todas as linhas que temos um único elemento não nulo, esses estão todos na mesma coluna. Dessa forma se $w(\beta_4) = 2p-3$ então, reordenando as

linhas e colunas se necessário, temos

$$\mathcal{A} = \begin{bmatrix} 0 & 0 & \cdots & x_1 + y_{p-1} \\ 0 & 0 & \cdots & x_2 + y_{p-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{p-1} + y_1 & x_{p-1} + y_2 & \cdots & x_{p-1} + y_{p-1} \end{bmatrix},$$

onde os elementos da última linha e coluna são todos não nulos. Isto implica

$$x_1 = x_2 = \cdots = x_{p-2} = -y_1 = -y_2 = \cdots = -y_{p-2},$$

e, em particular, $x_1 \neq x_{p-1}$ e $y_1 \neq y_{p-1}$.

Lema 3.8. *Se $w(\beta_4) = 2p - 3$, então $w(\beta_2) \geq 1$ e $w(\beta_3) \geq 1$.*

Demonstração:

Temos $\beta_2 = \sum_{i=1}^{p-1} \left(-x_i + \sum_{j=1}^{p-1} y_j \right) k^i$.

Se o coeficiente de k^{p-1} é diferente de zero, então $w(\beta_2) \geq 1$.

Se o coeficiente de k^{p-1} é zero, então $x_{p-1} = \sum_{j=1}^{p-1} y_j$ e como $x_1 \neq x_{p-1}$ segue que o coeficiente de k é não nulo. Portanto $w(\beta_2) \geq 1$.

O caso $w(\beta_3) \geq 1$ é análogo. ■

Proposição 3.4. *Não existe $\beta \in \mathcal{I}$ tal que $w(\beta) \leq 2p - 3$ e $w(\beta_4) = 2p - 3$.*

Demonstração:

Se $w(\beta_4) = 2p - 3$ então, pelo Lema 3.8, $w(\beta_2) \geq 1$ e $w(\beta_3) \geq 1$ daí $w(\beta) \geq 2p - 2$.

■

Agora se $w(\beta_4) = 2p - 4$ então, reordenando as linhas e colunas se necessário,

$$\mathcal{A} = \begin{bmatrix} 0 & 0 & \cdots & x_1 + y_{p-1} \\ 0 & 0 & \cdots & x_2 + y_{p-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{p-1} + y_1 & x_{p-1} + y_2 & \cdots & 0 \end{bmatrix}$$

Isto implica $x_1 = x_2 = \cdots = x_{p-2} = -y_1 = -y_2 = \cdots = -y_{p-2}$ e, em particular, $x_1 \neq x_{p-1}$, $y_1 \neq y_{p-1}$ e $x_{p-1} = y_{p-1}$.

Proposição 3.5. *Não existe um elemento $\beta \in \mathcal{I}$ com $w(\beta) \leq 2p-3$ e $w(\beta_4) = 2p-4$.*

Demonstração:

Afirmamos que $w(\beta_2) \geq 1$.

De fato, como $\beta_2 = \sum_{i=1}^{p-1} \left(-x_i + \sum_{j=1}^{p-1} y_j \right) k^i$, se $x_1 = \sum_{j=1}^{p-1} y_j$ então certamente $x_{p-1} \neq \sum_{j=1}^{p-1} y_j$ donde $w(\beta_2) \geq 1$, da mesma forma $w(\beta_3) \geq 1$. Portanto,

$$w(\beta) \geq w(\beta_2) + w(\beta_3) + w(\beta_4) \geq 1 + 1 + 2p - 4 = 2p - 2.$$

■

Como provamos que $\mathcal{I}$ contém um elemento α de peso $2p-2$ e pelos lemas anteriores todo elemento de $\mathcal{I}$ tem peso maior ou igual a $2p-2$, temos o seguinte:

Teorema 3.2.1. *O peso do ideal $\mathcal{I}$ é $w(\mathcal{I}) = 2p-2$ e a dimensão é $dim(\mathcal{I}) = 2p-2$.*

3.2.2 Caso p=2

Agora consideremos $p = 2$. Como antes, sejam H e K dois subgrupos quaisquer dentre os subgrupos $< a >$, $< b >$ e $< ab >$, então $G = H \times K$.

Escrevendo $H =< h >$ e $K =< k >$ sejam e $= \widehat{H} - \widehat{G}$, f $= \widehat{K} - \widehat{G}$ e

$$\mathcal{I} = (\mathbb{F}G)\mathrm{e} \oplus (\mathbb{F}G)\mathrm{f}$$

então $\mathcal{B} = \{(1-k)\widehat{H}, (1-h)\widehat{K}\}$ é uma base de $\mathcal{I}$.

Assim todo elemento $\alpha \in \mathcal{I}$ é escrito da seguinte forma

$$\begin{aligned} \alpha &= x(1-k)\widehat{H} + y(1-h)\widehat{K} \\ &= (x+y)1 + (x-y)h + (y-x)k - (x+y)hk \end{aligned}$$

Se tomamos $x = -y$, claramente $w(\alpha) = 2$. É fácil ver que não existe um elemento $\alpha \in \mathcal{I}$ tal que $w(\alpha) = 1$, logo $w(\mathcal{I}) = 2 = 2p-2$.

3.2.3 Caso p=3

Seja agora $G = C_3 \times C_3$. Nesse caso, os idempotentes são $\mathrm{e}_0 = \widehat{G}$, $\mathrm{e}_1 = \widehat{< a >} - \widehat{G}$, $\mathrm{e}_2 = \widehat{< b >} - \widehat{G}$, $\mathrm{f}_1 = \widehat{< ab >} - \widehat{G}$, $\mathrm{f}_2 = \widehat{< ab^2 >} - \widehat{G}$.

Novamente considere H e K dois subgrupos quaisquer dentre os subgrupos $< a >$, $< b >$ e $< ab^i >$ para $i = 1, 2$. Seja $\mathcal{I} = (\mathbb{F}G)\mathrm{e} \oplus (\mathbb{F}G)\mathrm{f}$, onde $\mathrm{e} = \widehat{H} - \widehat{G}$ e $\mathrm{f} = \widehat{K} - \widehat{G}$. Se $\alpha \in \mathcal{I}$ então

$$\begin{aligned} \alpha \quad = \quad & \underbrace{\left(\sum_{i=1}^{2} x_i + \sum_{i=1}^{2} y_j\right) 1}_{\alpha_1} + \underbrace{\sum_{i=1}^{2} \left(-x_i + \sum_{j=1}^{2} y_j\right) k^i}_{\alpha_2} + \\ & \underbrace{\sum_{j=1}^{2} \left(-y_j + \sum_{i=1}^{2} x_i\right) h^j}_{\alpha_3} - \underbrace{\sum_{i,j=1}^{2} (x_i + y_j) k^i h^j}_{\alpha_4} . \end{aligned}$$

Se $x_1 = x_2 = -y_1 = -y_2$, então o peso de α, $w(\alpha) = 4 = 2p - 2$. Provemos que o peso do código $\mathcal{I}$ é exatamente 4.

Para isso verifiquemos que não existe uma palavra $\beta \in \mathcal{I}$ tal que $w(\beta) < 4$. Caso uma tal palavra exista, escrevemos $\beta = \beta_1 + \beta_2 + \beta_3 + \beta_4$ e observamos que se $w(\beta) < 4$, então devemos ter $w(\beta_4) < 4$. Devemos assim estudar o peso de β_4.

Novamente dispomos os coeficientes de β_4 em uma matriz 2×2, como segue

$$\mathcal{A} = (a_{ij}) = \begin{pmatrix} x_1 + y_1 & x_1 + y_2 \\ x_2 + y_1 & x_2 + y_1 \end{pmatrix} .$$

Observe que, pelo Lema 3.2, β_4 não assume peso igual a 1. Assim devemos estudar o peso de β_4 igual a 3 ou 2.

Lema 3.9. *Se $w(\beta_4) = 3$, então $w(\beta_1) = 1$.*

Demonstração:

Se $w(\beta_4) = 3$, então β_4 deve ter $4 - 3 = 1$ coeficiente nulo e temos a seguinte matriz:

$$\mathcal{A} = \begin{pmatrix} 0 & a_{12} \\ a_{21} & a_{22} \end{pmatrix} ,$$

onde a_{12}, a_{21} e a_{22} são não nulos. Quando trocamos o elemento nulo de posição na matriz temos uma situação completamente análoga a essa. Nessa situação temos: $x_1 = -y_1$, $x_1 \neq -y_2$, $x_2 \neq -y_1$ e $x_2 \neq -y_2$.

Assim o coeficiente de β_1, $x_1 + x_2 + y_1 + y_2 = x_2 + y_2 \neq 0$, logo $w(\beta_1) = 1$. ■

Proposição 3.6. *Não existe $\beta \in \mathcal{I}$, tal que $w(\beta) < 4$ e $w(\beta_4) = 3$*

Demonstração:

Pelo Lema 3.9 se $w(\beta_4) = 3$, então $w(\beta_1) = 1$. Assim

$$w(\beta) \geq w(\beta_1) + w(\beta_4) = 4.$$

■

Proposição 3.7. *Não existe $\beta \in \mathcal{I}$ tal que $w(\beta) < 4$ e $w(\beta_4) = 2$.*

Demonstração:

Se $w(\beta_4) = 2$, então β_4 tem $4-2 = 2$ coeficientes nulos, logo a matriz dos coeficientes tem seis formas diferentes porém é necessário analisar apenas três formas as demais são provadas de forma análoga.

(i) Considere a seguinte matriz dos coeficientes:

$$\mathcal{A} = \begin{pmatrix} 0 & 0 \\ x_2 + y_1 & x_2 + y_2 \end{pmatrix},$$

onde $x_1 = -y_1 = -y_2$ e $x_2 \neq x_1$.

Nesse caso o $w(\beta_2) \geq 1$, pois se o coeficiente de k for nulo então:

$$x_1 = y_1 + y_2 \Longrightarrow 3y_1 = 0,$$

o que é um absurdo, portanto $w(\beta_2) \geq 1$.

E também $w(\beta_1) = 1$, pois $x_1 + x_2 + y_1 + y_2 = x_2 + y_2 \neq 0$.

Assim $w(\beta) \geq w(\beta_1) + w(\beta_2) + w(\beta_4) \geq 4$

(ii) Agora temos a seguinte matriz

$$\mathcal{A} = \begin{pmatrix} 0 & x_1 + y_2 \\ x_2 + y_1 & 0 \end{pmatrix}$$

Novamente, $w(\beta_2) \geq 1$, pois se o coeficiente de k for nulo então o coeficiente de k^2 é não nulo já que $x_1 \neq x_2$. Analogamente, $w(\beta_3) \geq 1$.

Logo $w(\beta) \geq w(\beta_2) + w(\beta_3) + w(\beta_4) \geq 4$.

(iii) Por último, seja

$$\mathcal{A} = \begin{pmatrix} 0 & x_1 + y_2 \\ 0 & x_2 + y_2 \end{pmatrix}.$$

Como antes $w(\beta_3) \geq 1$, pois $y_1 \neq y_2$.

E $w(\beta_1) = 1$, pois $x_1 + x_2 + y_1 + y_2 = x_2 + y_2 \neq 0$

Assim $w(\beta) \geq w(\beta_1) + w(\beta_3) + w(\beta_4) \geq 4$.

■

Como provamos que $\mathcal{I}$ contém um elemento α de peso 4 e todo elemento de $\mathcal{I}$ tem peso maior ou igual a 4, temos o seguinte:

Teorema 3.2.2. *O peso do ideal $\mathcal{I}$ é $w(\mathcal{I}) = 2p - 2 = 4$. E a dimensão é $dim\mathcal{I} = 2p - 2 = 4$.*

3.3 Exemplos

Com o auxílio do conhecido programa **Groups Algorithms Programming - GAP**, apresentaremos aqui o cálculo do peso de todos os possíveis códigos de comprimento p^2 em uma certa álgebra de grupo abeliano. Na próxima seção encontra-se o código fonte.

Primeiramente observe que os códigos da álgebra de grupo $\mathbb{F}(C_p \times C_p)$ podem ser descritos na seguinte cadeia:

$$\underbrace{(\mathbb{F}G)\mathrm{e}_1}_{\mathcal{I}_1} \subset \underbrace{(\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2}_{\mathcal{I}_2} \subset \underbrace{(\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus (\mathbb{F}G)\mathrm{f}_1}_{\mathcal{J}_1} \subset \cdots \subset$$

$$\underbrace{(\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus (\mathbb{F}G)\mathrm{f}_1 \oplus (\mathbb{F}G)\mathrm{f}_2 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{f}_{p-2}}_{\mathcal{J}_{p-2}} \subset$$

$$\underbrace{(\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus (\mathbb{F}G)\mathrm{f}_1 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{f}_{p-1}}_{\mathcal{J}_{p-1}},$$

onde $G = C_p \times C_p$, e os idempotentes e_1, e_2, f_j $j = 1, ..., p-1$ foram definidos no início da Seção 3.2. Nesta seção provamos que o peso do ideal $\mathcal{I}_2$ é $2p-2$ e também vimos que o peso do código minimal $\mathcal{I}_1$ é $2p$.

Observe ainda que o peso dos ideais $\mathcal{J}_{p-2}$ e $\mathcal{J}_{p-1}$ é igual a 2, pois temos

$$\mathcal{J}_{p-2} = (\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus (\mathbb{F}G)\mathrm{f}_1 \oplus (\mathbb{F}G)\mathrm{f}_2 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{f}_{p-2} =$$

$$(\mathbb{F}G)(\mathrm{e}_1 + \cdots + \mathrm{f}_{p-2}) = (\mathbb{F}G)(1 - \widehat{< ab^{p-1} >})$$

e

$$\mathcal{J}_{p-1} = (\mathbb{F}G)\mathrm{e}_1 \oplus (\mathbb{F}G)\mathrm{e}_2 \oplus (\mathbb{F}G)\mathrm{f}_1 \oplus (\mathbb{F}G)\mathrm{f}_2 \oplus \cdots \oplus (\mathbb{F}G)\mathrm{f}_{p-1} =$$

$$(\mathbb{F}G)(\mathrm{e}_1 + \cdots + \mathrm{f}_{p-2}) = (\mathbb{F}G)(1 - \widehat{G}),$$

nos dois casos segue imediatamente da Proposição 3.1 que o peso desses ideais é 2.

Assim usaremos o GAP para calcular o peso dos demais ideais no nosso exemplo.

- Considere a álgebra $\mathbb{F}_2(C_3 \times C_3)$

  Os idempotentes centrais primitivos nessa álgebra são: $\mathrm{e}_1 = \widehat{< a >} - \widehat{G}$, $\mathrm{e}_2 = \widehat{< b >} - \widehat{G}$, $\mathrm{f}_1 = \widehat{< ab >} - \widehat{G}$ e $\mathrm{f}_2 = \widehat{< ab^2 >}$.

  Mantendo a notação anterior, o programa obteve a seguinte relação de pesos para os códigos nessa álgebra:

$$w(\mathcal{I}_1) = 6,\ w(\mathcal{I}_2) = 4,\ w(\mathcal{J}_1) = 2,\ w(\mathcal{J}_2) = 2$$

- Considere a álgebra $\mathbb{F}_2(C_5 \times C_5)$

  Os idempotentes centrais primitivos nessa álgebra são: $\mathrm{e}_1 = \widehat{< a >} - \widehat{G}$, $\mathrm{e}_2 = \widehat{< b >} - \widehat{G}$, $\mathrm{f}_1 = \widehat{< ab >} - \widehat{G}$, $\mathrm{f}_2 = \widehat{< ab^2 >}$, $\mathrm{f}_3 = \widehat{< ab^3 >} - \widehat{G}$, $\mathrm{f}_4 = \widehat{< ab^4 >} - \widehat{G}$.

  Mantendo a notação anterior, o programa obteve a seguinte relação de pesos para os códigos nessa álgebra:

$$w(\mathcal{I}_1) = 10,\ w(\mathcal{I}_2) = 8,\ w(\mathcal{J}_1) = 6,\ w(\mathcal{J}_2) = 4,\ w(\mathcal{J}_3) = 2,\ w(\mathcal{J}_4) = 2$$

- $\mathbb{F}_3(C_5 \times C_5)$

  Os idempotentes são dados pelos mesmos subgrupos e obtivemos exatamente os mesmos pesos que em 3.3.

Esses três exemplos sugerem que a lista de pesos de códigos, naquela cadeia descrita no início da seção, vai diminuindo de dois em dois.

3.4 Código Fonte

Segue o código fonte utilizado no GAP para calcular o peso dos códigos abelianos nas seguintes álgebras $\mathbb{F}_2(C_3 \times C_3)$, $\mathbb{F}_2(C_5 \times C_5)$, $\mathbb{F}_3(C_5 \times C_5)$.

```
LoadPackage("wedderga");
-------------------------------------------------------------------------------
Loading  Wedderga 4.3.3 (Wedderga)
by Osnel Broche Cristo (osnel@ufla.br),
   Alexander Konovalov (http://www.cs.st-andrews.ac.uk/~alexk/),
   Gabriela Olteanu (golteanu@um.es, olteanu@math.ubbcluj.ro),
   Aurora Olivieri (olivieri@usb.ve), and
   Angel del Rio (http://www.um.es/adelrio).
-------------------------------------------------------------------------------
true
K:=GF(2);
GF(2)
C:=DirectProduct(CyclicGroup(3),CyclicGroup(3));
<pc group of size 9 with 2 generators>
KC:=GroupRing(K,C);
<algebra-with-one over GF(2), with 2 generators>
Está definida a álgebra de grupo F_2(C_3 X C_3)
MinimalGeneratingSet( C );
[ f1, f2 ]
 l := List(MinimalGeneratingSet( C ) , g -> g^Embedding( C, KC ) );
[ (Z(2)^0)*f1, (Z(2)^0)*f2 ]
a:=l[1];b:=l[2];
(Z(2)^0)*f1
(Z(2)^0)*f2
H1:=Subgroup(C,[C.1]);
Group([ f1 ])
H2:=Subgroup(C,[C.2]);
Group([ f2 ])
H3:=Subgroup(C,[C.1*C.2]);
Group([ f1*f2 ])
H4:=Subgroup(C,[C.1*C.2^2]);
Group([ f1*f2^2 ])
Está definido os subgrupos para o cálculo do idempotentes
S:=AverageSum(KC,C);
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f2+(Z(2)^0)*f1^2+(Z(2)^
0)*f1*f2+(Z(2)^0)*f2^2+(Z(2)^0)*f1^2*f2+(Z(2)^0)*f1*f2^2+(Z(2)^0)*f1^2*f2^2
S1:=AverageSum(KC,H1);
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f1^2
S2:=AverageSum(KC,H2);;
S3:=AverageSum(KC,H3);;
S4:=AverageSum(KC,H4);;
e1:=S1-S;
(Z(2)^0)*f2+(Z(2)^0)*f1*f2+(Z(2)^0)*f2^2+(Z(2)^0)*f1^2*f2+(Z(2)^0)*f1*f2^2+(
Z(2)^0)*f1^2*f2^2
e2:=S2-S;;
e3:=S3-S;;
e4:=S4-S;;
Esses são os idempotentes centrais primitivos
I1:=Ideal(KC,[e1]);
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (1 generators)>
I2:=Ideal(KC,[e2]);
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (1 generators)>
I3:=Ideal(KC,[e3]);
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (1 generators)>
I4:=Ideal(KC,[e4]);
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (1 generators)>
Os ideais minimais
J2:= I1 + I2;
```

```
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (2 generators)>
Soma de dois ideais minimais
Size(J2);
16
Quantidade de palavras em J2
P:=[]; for x in Elements(J2) do
Add(P, Size(Support(x)));
od;
[  ]
P;;
EnumeratorSorted(P);
[ 0, 4, 6 ]
Aqui temos o peso de J2 igual a 4
J3:= J2 + I3;
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (3 generators)>
Soma de tres ideais minimais
Size(J3);
64
Quantidade de palavras em J3
P3:=[];
[  ]
for x in Elements(J3) do
Add(P3, Size(Support(x)));
od;
P3;;
EnumeratorSorted(P3);
[ 0, 2, 4, 6 ]
Aqui temos o peso de J3 igual a 2
J4:=J3 + I4;
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (4 generators)>
Soma de quatro ideais minimais
Size(J4);
256
Quantidade de palavras em J4
P4:=[];
[  ]
for x in Elements(J4) do
Add(P4, Size(Support(x)));
od;
P4;;
EnumeratorSorted(P4);
[ 0, 2, 4, 6, 8 ]
Aqui temos o peso de J4 igual a 2
```

```
LoadPackage("wedderga");
-------------------------------------------------------------------------------
Loading  Wedderga 4.3.3 (Wedderga)
by Osnel Broche Cristo (osnel@ufla.br),
   Alexander Konovalov (http://www.cs.st-andrews.ac.uk/~alexk/),
   Gabriela Olteanu (golteanu@um.es, olteanu@math.ubbcluj.ro),
   Aurora Olivieri (olivieri@usb.ve), and
   Angel del Rio (http://www.um.es/adelrio).
-------------------------------------------------------------------------------
true
K:=GF(2);
GF(2)
C:=DirectProduct(CyclicGroup(5),CyclicGroup(5));
<pc group of size 25 with 2 generators>
KC:=GroupRing(K,C);
<algebra-with-one over GF(2), with 2 generators>
Está definida a álgebra F_2(C_5 X C_5)
MinimalGeneratingSet( C );
[ f1, f2 ]
 l := List(MinimalGeneratingSet( C ) , g -> g^Embedding( C, KC ) );
[ (Z(2)^0)*f1, (Z(2)^0)*f2 ]
a:=l[1];b:=l[2];
(Z(2)^0)*f1
(Z(2)^0)*f2
H1:=Subgroup(C,[C.1]);
Group([ f1 ])
H2:=Subgroup(C,[C.2]);
Group([ f2 ])
H3:=Subgroup(C,[C.1*C.2]);
Group([ f1*f2 ])
H4:=Subgroup(C,[C.1*C.2^2]);
Group([ f1*f2^2 ])
Esses são os subgrupos para o cálculo dos idempotentes
S:=AverageSum(KC,C);
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f2+(Z(2)^0)*f1^2+(Z(2)^
0)*f1*f2+(Z(2)^0)*f2^2+(Z(2)^0)*f1^3+(Z(2)^0)*f1^2*f2+(Z(2)^0)*f1*f2^2+(Z(2)^
0)*f2^3+(Z(2)^0)*f1^4+(Z(2)^0)*f1^3*f2+(Z(2)^0)*f1^2*f2^2+(Z(2)^0)*f1*f2^3+(
Z(2)^0)*f2^4+(Z(2)^0)*f1^4*f2+(Z(2)^0)*f1^3*f2^2+(Z(2)^0)*f1^2*f2^3+(Z(2)^
0)*f1*f2^4+(Z(2)^0)*f1^4*f2^2+(Z(2)^0)*f1^3*f2^3+(Z(2)^0)*f1^2*f2^4+(Z(2)^
0)*f1^4*f2^3+(Z(2)^0)*f1^3*f2^4+(Z(2)^0)*f1^4*f2^4
S1:=AverageSum(KC,H1);
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f1^2+(Z(2)^0)*f1^3+(Z(2)^
0)*f1^4
S2:=AverageSum(KC,H2);;
S3:=AverageSum(KC,H3);;
S4:=AverageSum(KC,H4);;
e1:=S1-S;;
e2:=S2-S;;
e3:=S3-S;;
e4:=S4-S;;
Esses são os idempotentes centrais primitivos
I1:=Ideal(KC,[e1]);
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (1 generators)>
I2:=Ideal(KC,[e2]);
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (1 generators)>
I3:=Ideal(KC,[e3]);
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (1 generators)>
I4:=Ideal(KC,[e4]);
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
```

```
  (1 generators)>
Esses os ideais minimais
I:=I1+I2;
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (2 generators)>
M:=I+I3;
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (3 generators)>
Ideal dado pela soma de tres minimais
Size(M);
4096
Quantidade de palavras em M
P:=[];
[  ]
for x in Elements(M) do
 Add(P,Size(Support(x)));
od;
P;;
EnumeratorSorted(P);
[ 0, 6, 8, 10, 12, 14, 16, 18, 20 ]
Aqui temos o peso de M igual a 6
J:=I3+I4;
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (2 generators)>
L:=I+J;
<two-sided ideal in <algebra-with-one over GF(2), with 2 generators>,
  (4 generators)>
Ideal dado pela soma de 4 ideais miniamis
Size(L);
65536
Quantidade de palavras em L
P:=[];
[  ]
for x in Elements(L) do
  Add(P,Size(Support(x)));
od;
P;;
EnumeratorSorted(P);
[ 0, 4, 6, 8, 10, 12, 14, 16, 18, 20 ]
O peso de L é 4
```

```
LoadPackage("wedderga");
-------------------------------------------------------------------------------
Loading  Wedderga 4.3.3 (Wedderga)
by Osnel Broche Cristo (osnel@ufla.br),
   Alexander Konovalov (http://www.cs.st-andrews.ac.uk/~alexk/),
   Gabriela Olteanu (golteanu@um.es, olteanu@math.ubbcluj.ro),
   Aurora Olivieri (olivieri@usb.ve), and
   Angel del Rio (http://www.um.es/adelrio).
-------------------------------------------------------------------------------
true
K:=GF(3);
GF(3)
C:=DirectProduct(CyclicGroup(5),CyclicGroup(5));
<pc group of size 25 with 2 generators>
KC:=GroupRing(K,C);
<algebra-with-one over GF(3), with 2 generators>
Está definida a álgebra de grupo F_3(C_5 X C_5)
MinimalGeneratingSet( C );
[ f1, f2 ]
l := List(MinimalGeneratingSet( C ) , g -> g^Embedding( C, KC ) );
[ (Z(3)^0)*f1, (Z(3)^0)*f2 ]
a:=l[1];b:=l[2];
(Z(3)^0)*f1
(Z(3)^0)*f2
H1:=Subgroup(C,[C.1]);
Group([ f1 ])
H2:=Subgroup(C,[C.2]);
Group([ f2 ])
H3:=Subgroup(C,[C.1*C.2]);
Group([ f1*f2 ])
H4:=Subgroup(C,[C.1*C.2^2]);
Group([ f1*f2^2 ])
Está definido os subgrupos para o cálculo do idempotentes
S:=AverageSum(KC,C);
(Z(3)^0)*<identity> of ...+(Z(3)^0)*f1+(Z(3)^0)*f2+(Z(3)^0)*f1^2+(Z(3)^
0)*f1*f2+(Z(3)^0)*f2^2+(Z(3)^0)*f1^3+(Z(3)^0)*f1^2*f2+(Z(3)^0)*f1*f2^2+(Z(3)^
0)*f2^3+(Z(3)^0)*f1^4+(Z(3)^0)*f1^3*f2+(Z(3)^0)*f1^2*f2^2+(Z(3)^0)*f1*f2^3+(
Z(3)^0)*f2^4+(Z(3)^0)*f1^4*f2+(Z(3)^0)*f1^3*f2^2+(Z(3)^0)*f1^2*f2^3+(Z(3)^
0)*f1*f2^4+(Z(3)^0)*f1^4*f2^2+(Z(3)^0)*f1^3*f2^3+(Z(3)^0)*f1^2*f2^4+(Z(3)^
0)*f1^4*f2^3+(Z(3)^0)*f1^3*f2^4+(Z(3)^0)*f1^4*f2^4
S1:=AverageSum(KC,H1);
(Z(3))*<identity> of ...+(Z(3))*f1+(Z(3))*f1^2+(Z(3))*f1^3+(Z(3))*f1^4
S2:=AverageSum(KC,H2);;
S3:=AverageSum(KC,H3);;
S4:=AverageSum(KC,H4);;
e1:=S1-S;;
e2:=S2-S;;
e3:=S3-S;;
e4:=S4-S;;
Esses são os idempotentes centrais primitivos
I1:=Ideal(KC,[e1]);
<two-sided ideal in <algebra-with-one over GF(3), with 2 generators>,
  (1 generators)>
I2:=Ideal(KC,[e2]);
<two-sided ideal in <algebra-with-one over GF(3), with 2 generators>,
  (1 generators)>
I3:=Ideal(KC,[e3]);
<two-sided ideal in <algebra-with-one over GF(3), with 2 generators>,
  (1 generators)>
I4:=Ideal(KC,[e4]);
<two-sided ideal in <algebra-with-one over GF(3), with 2 generators>,
  (1 generators)>
```

```
I:=I1+I2;
<two-sided ideal in <algebra-with-one over GF(3), with 2 generators>,
  (2 generators)>
E1:=Elements(I);;
J:=I3+I4;
<two-sided ideal in <algebra-with-one over GF(3), with 2 generators>,
  (2 generators)>
M:=I+I3;
<two-sided ideal in <algebra-with-one over GF(3), with 2 generators>,
  (3 generators)>
Esse é o ideal dado pelo soma de tres minimais
E2:=Elements(M);;
Size(E2);
531441
Essa é a quantidade de palavras em M
P:=[];
for x in E2 do
  Add(P,Size(Support(x)));
od;
[  ]
Esse conjunto lista o suporte de todas as palavras em M
P;;
EnumeratorSorted(P);
[ 0, 6, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25 ]
Aqui temos que o peso de M é 6
L:=I+J;
<two-sided ideal in <algebra-with-one over GF(3), with 2 generators>,
  (4 generators)>
L é o ideal dado pela soma de quatro ideais minimais
Size(L);
43046721
Quantidade de palavras em L
E3:=Elements(J);;
P:=[];
for x in E1 do for y in E3 do
  Add(P,Size(Support(x+y)));
od; od;
P;;
EnumeratorSorted(P);
[ 0, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23,
  24, 25 ]
Temos o peso do ideal L igual a 4
```

CAPÍTULO 4

CONCLUSÕES

O objetivo nesse capítulo é comparar os códigos estudados anteriormente. Isto será feito utilizando peso e dimensão dos códigos.

Na primeira seção explicamos porque escolhemos esses dois parâmetros para comparar e em seguida, na segunda seção, fazemos a comparação propriamente dita.

4.1 Introdução

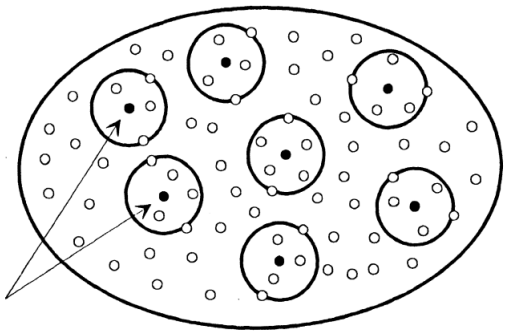
É natural buscarmos por códigos que tenham o maior número possível de palavras para poder transmitir a maior quantidade de informação possível. No caso dos códigos lineares, o número de palavras depende da dimensão do código, logo estamos interessados nos códigos que tenham dimensão maior possível.

Para entendermos porque estudar o peso do código, consideremos o método de decodificação de um vetor. Seja v o vetor recebido, se e representa o vetor erro, então $e = v - c$, onde c é uma palavra código. Se escolhemos um vetor erro e de menor peso e decodificamos v em $c = v - e$, então c será um vetor do código $\mathcal{C}$ mais próximo de v.

Geometricamente essa situação é descrita da seguinte forma. Defina a *esfera de raio r e centro $v \in \mathbb{F}_q^n$* como:

$$S(v,r) = \{v \in \mathbb{F}_q^n / \, d(v,w) \leq r\},$$

podemos representar a decodificação pela figura



As bolas sólidas são as palavras do código e as demais são vetores do espaço. Os vetores que estão dentro de uma esfera são decodificados nos vetores do centro da esfera.

O próximo teorema relaciona o peso do código, com o raio da esfera e com a capacidade de corrigir erros.

Teorema 4.1.1. *([12], Teo 2) Se w é o peso de um código $\mathcal{C}$, então $\mathcal{C}$ pode detectar $w-1$ erros e corrigir no máximo $r = \lfloor \frac{w-1}{2} \rfloor$ erros.*

Segue imediatamente do teorema acima que quanto maior o peso do código maior a capacidade de correção de erros.

Assim estamos interessados em códigos com dimensão grande para que um grande número de mensagens possam ser codificadas, e peso também grande para que muitos erros possam ser corrigidos. Porém esses objetivos são contraditórios.

Formulando matematicamente esse problema, podemos considerar fixado o comprimento n e o peso ω e então determinar o maior número possível de palavras para que exista um (n,ω)-código q-ário. Na bibliografia esse número é denotado por $A_q(n,d)$ e determiná-lo tornou-se *o problema principal da Teoria de Códigos* ([15], sec. 4.5).

Há vários estudos para determinar esse número, mas a maioria dos resultados obtidos apresentam apenas cotas superiores para $A_q(n, d)$. Podemos citar, por exemplo, a cota de Singleton:

$$A_q(n, \omega) \leq q^{n-\omega+1}.$$

Quando existe um código linear para o qual é válida a igualdade em 4.1 este é dito *maximum distance separable code* (código separável pela distância máxima) ou simplesmente código MDS, já que ele possui o maior peso possível para um código com dado comprimento e dimensão.

Reformulando o problema sobre o peso e dimensão de um código, podemos considerar fixado o comprimento n e a dimensão k. Nesse caso queremos determinar o maior peso possível para que exista um código com esses parâmetros ([15], sec. 5.3).

A fim de compararmos os códigos cíclicos e abelianos não cíclicos, obtidos nesse trabalho, vamos considerar que, para um comprimento fixado, queremos um código que transmita um grande número de mensagens e que também corrija um grande número de erros. Nesse sentido definimos a *conveniência* de um código como sendo o seguinte produto:

$$conv(\mathcal{C}) = \omega \cdot k,$$

onde ω denota o peso e k a dimensão de um código linear.

Assim parece natural considerar que um código $\mathcal{C}_\infty$ é melhor que outro $\mathcal{C}_\in$ se $\mathcal{C}_\infty$possui uma conveniência maior que $\mathcal{C}_\in$.

4.2 Comparação de códigos

4.2.1 Códigos Minimais

Aqui consideraremos códigos minimais de comprimento p^n.

1. **Códigos cíclicos**

Seja $\mathbb{F}$ o corpo finito com q elementos e $G = C_{p^n}$ o grupo cíclico de ordem p^n. De acordo com a Seção 2.1, os idempotentes centrais primitivos da álgebra de grupo $\mathbb{F}G$ são:

$$e_0 = \widehat{G} \text{ e } e_i = \widehat{G_i} - \widehat{G_{i-1}},$$

onde G_i é um subgrupo de G de ordem p^{n-i}, para $1 \leq i \leq n$.

Os códigos cíclicos minimais $\mathcal{I}_i = (\mathbb{F}G)e_i$ tem dimensão $d = p^i - p^{i-1}$ e peso $w = 2|G_i| = 2p^{n-i}$, para $1 \leq i \leq n$ e o código minimal $\mathcal{I}_0 = (\mathbb{F}G)e_0$ tem dimensão igual a 1 e peso igual a p^n.

Para o ideal $\mathcal{I}_i$, $1 \leq i \leq n$, temos

$$conv(\mathcal{I}_i) = 2p^{n-i}(p^i - p^{i-1}) = 2p^{n-1}(p-1).$$

Já o ideal $\mathcal{I}_0$ tem conveniência $conv(\mathcal{I}_0) = p^n$.

2. **Códigos abelianos**

Considere novamente o corpo $\mathbb{F}$ com q elementos e também o p-grupo abeliano $G \simeq \underbrace{C_p \times \cdots \times C_p}_{n}$, onde $mdc\{p, q\} = 1$. Pela Seção 3.1 os idempotentes centrais primitivos da álgebra $\mathbb{F}G$ são dados por:

$$e_0 = \widehat{G} \text{ e } e_H = \widehat{H} - \widehat{G},$$

onde H é um subgrupo de ordem p^{n-1}.

A dimensão e o peso do código abeliano minimal $\mathcal{I}_H = (\mathbb{F}G)e_H$ são $p-1$ e $2p^{n-1}$, respectivamente. Assim a conveniência é

$$conv(\mathcal{I}_H) = 2p^{n-1}(p-1),$$

e para o ideal $\mathcal{I}_0 = (\mathbb{F}G)e_0$ a conveniência é p^n.

Comparando os códigos minimais cíclicos e abelianos não cíclicos, a conveniência é a mesma. Note que, no caso abeliano, peso e dimensão são os mesmos para todo código minimal e, no caso cíclico, quando a dimensão aumenta o peso diminui.

4.2.2 Soma de ideais minimais

Aqui consideraremos os códigos cíclicos e abelianos não cíclicos de comprimento p^2.

1. **Soma de códigos cíclicos**

   Considere a álgebra de grupo $\mathbb{F}C_{p^2}$, então pela Observação 2.2 há apenas três ideais minimais nessa álgebra, logo os ideais somas são:

   - Se $\mathcal{I} = \mathcal{I}_0 \oplus \mathcal{I}_1$, então $dim(\mathcal{I}) = p$ e $w(\mathcal{I}) = p$, logo $conv(\mathcal{I}) = p^2$.
   - Se $\mathcal{J} = \mathcal{I}_1 \oplus \mathcal{I}_2$, então $dim(\mathcal{J}) = p^2 - 1$ e $w(\mathcal{J}) = 2$, logo $conv(\mathcal{J}) = 2(p^2 - 1)$.

2. **Soma de códigos abelianos não cíclicos**

   Seja $\mathcal{L} = (\mathbb{F}G)e \oplus (\mathbb{F}G)f$, como feito na Seção 3.2, então $dim(\mathcal{L}) = 2(p-1)$ e $w(\mathcal{L}) = 2(p-1)$, logo $conv(\mathcal{L}) = 4(p-1)^2$.

Comparando a conveniência entre o código cíclico $\mathcal{I}$ e um código abeliano $\mathcal{L}$ dados acima encontramos que $conv(\mathcal{L}) > conv(\mathcal{I})$, quando $p > 2$ e, para $p = 2$ temos $conv(\mathcal{L}) = conv(\mathcal{I})$.

Agora comparamos o código cíclico $\mathcal{J}$ com o código abeliano $\mathcal{L}$. Para $p = 2$, temos $conv(\mathcal{L}) < conv(\mathcal{J})$, para $p = 3$, temos $conv(\mathcal{L}) = conv(\mathcal{J})$ e, para $p > 3$ temos $conv(\mathcal{L}) > conv(\mathcal{J})$.

Desse ponto de vista os códigos abelianos de comprimentos p^2 são melhores que os códigos cíclicos de mesmo comprimento.

Observação 4.1. *1. Considerando a cota de Singleton, o código cíclico de comprimento p^2, $\mathcal{J} = \mathcal{I}_1 \oplus \mathcal{I}_2$, é um código MDS, pois nesse caso devemos ter*

$$A_q(p^2, 2) \leq q^{p^2-2+1} = q^{p^2-1}$$

e, como visto, a dimensão desse código é exatamente $p^2 - 1$. Logo o ideal $\mathcal{J}$ possui q^{p^2-1} palavras, o que caracteriza ser um código MDS. Veja que $\mathcal{J}$ é um $(p^2, p^2-1, 2)$-código, esse caso em particular é chamado código MDS trivial.

Apesar de atingir a cota de Singleton, do ponto de vista de correção de erros esse não é um bom código já que corrige apenas um erro.

2. *Observe também que quando consideramos comprimentos diferentes para os ideais* $\mathcal{J}$ *e* $\mathcal{L}$ *conseguimos que eles tenham a mesma dimensão, porém o código* $\mathcal{L}$ *corrigi mais erros que* $\mathcal{J}$*. Por exemplo, considere o ideal* $\mathcal{J}$ *com comprimento* 3^2*, então* $dim(\mathcal{J}) = 3^2 - 1 = 8$ *e* $w(\mathcal{J}) = 2$ *e tome o ideal* $\mathcal{L}$ *com comprimento* 5^2 *e então* $dim(\mathcal{L}) = 2(5-1) = 8$ *e* $w(\mathcal{L}) = 2(5-1) = 8$*.*

   Como podemos perceber os dois códigos possuem a mesma quantidade de palavras mas o código $\mathcal{J}$ *corrigi apenas 1 erro enquanto o código* $\mathcal{L}$ *corrigi 3 erros, confirmando a vantagem de trabalhar com códigos abelianos.*

REFERÊNCIAS BIBLIOGRÁFICAS

[1] S.K. Arora and M. Pruthi, *Minimal cyclic codes of length* $2p^n$, Finite Field and Appl., **5** (1999) 177-187.

[2] S.D.Berman, *On the theory of group codes*, Kibernetika (Kiev), **1** (1967) 31-39 (Russian).

[3] S.D. Berman, *Semi simple cyclic and abelian code II*, Cybernetics, **3** (3) (1967), 17-23.

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

[5] R. Ferraz and C. Polcino Milies, *Idempotents in Group Algebra and Minimal Abelian Codes*, Finite Fields and Appl., **13** (2007) 382-393.

[6] R. Ferraz, F. Dutra e C. Polcino Milies, *Semisimple Group Codes and Dihedral Codes*, Algebra and Discrete Math, vol. **3** (2009), 28-48.

[7] M. Golay, *Notes on digital coding*, Proc. I.R.E. (IEEE), vol. **37** (1949) 657.

[8] R.W. Hamming, *Error Detecting and Error Correcting Codes*, The Bell Sustem Tech. J., vol. 29 n.2, (1950) 147-160.

[9] A.V. Keralev and P. Solé, *Error-correcting codes as ideals in group rings*, Contemp. Math., vol. 273, American Mathematical Society, Rhode Island, (2001), 11-18.

[10] F.J. MacWilliams, *Binary codes which are ideals in the group algebra of an abelian group*, Bell System Tech. J., **49** (1970) 987-1011

[11] C. Polcino Milies, S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic, Dordrecht, 2002.

[12] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, A Wiley-Interscience publication, New York, 1998.

[13] M.Pruthi and S.K. Arora, *Minimal codes of prime power length*, Finite Field Appl., **3** (1997) 99-113.

[14] M. Pruthi, *Cyclic codes of length* 2^n, Proc. Indian Acad. Sci. **111** (2001) 371-379.

[15] S. Roman, *Coding and Information Theory*, Grad. Texts in Math., vol. 134, Springer-Verlag, New York, 1992.

[16] R.E. Sabin, *On Determining All Codes in Semi-simple Group Rings*, Lect. Notes in Comp. Sci., vol. **673** (1993) 279-290.

[17] C.E. Shannon, *A Mathematical Theory of Communication*, The Bell System Tech. J., **27** (1948) 379-423, 623-656.