

**Códigos cíclicos
sobre anéis de cadeia**

Anderson Tiago da Silva

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 e do CNPq

São Paulo, 03 de fevereiro de 2012

Códigos cíclicos sobre anéis de cadeia

Esta tese trata-se da versão original
do aluno Anderson Tiago da Silva.

Códigos Cíclicos sobre Anéis de Cadeia

Esta tese/dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa realizada por Anderson Tiago da Silva em 05/03/2012.

O original encontra-se disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Banca Examinadora:

- Prof. Dr. Francisco César Polcino Milies (orientador) - IME-USP
- Prof. Dr. Raul Antonio Ferraz - IME-USP
- Prof. Dr. Thierry Corrêa Petit Lobão - UFBA
- Profa. Dra. Sueli Irene Rodrigues Costa - UNICAMP
- Profa. Dra. Marinês Guerreiro - UFV

Agradecimentos

Agradeço primeiramente a USP pela oportunidade e a CAPES e CNPq pelo suporte financeiro.

Aos membros da banca por aceitarem o convite, pelas dicas e correções.

A Deus, por ter me iluminado neste período da minha vida.

Aos meus pais, Marinalva e Rosino, pelo apoio nos momentos que mais precisei e por estarem sempre presentes, apesar da distância.

Aos meus irmãos, Alexsandro, Andreza e Andreia pela força.

Ao Robert pelo auxílio no programa MATLAB.

A minha mulher Daniela, pelos momentos felizes, pelo apoio, compreensão e pela paciência que teve comigo quando eu não estava bem.

Ao Prof. Dr. Francisco César Polcino Milies, que me orientou neste trabalho com paciência e me proporcionou grandes oportunidades acadêmicas durante o doutorado.

Aos professores do IME-USP, em especial ao prof. Dr. Raul Ferraz, por estar sempre disponível para me ouvir(sempre que eu descobria alguma coisa ia falar com ele antes de apresentar ao Polcino).

Aos amigos do IME, Alexander, John, Renata, Patricia, Fernanda, César e Ulisses, pelos momentos de descontração e pela companhia nos momentos de estudo.

A todos que contribuíram diretamente ou indiretamente com este trabalho.

Resumo

Códigos cíclicos sobre anéis de cadeia

Neste trabalho, usamos uma abordagem de anéis de grupo para caracterizar códigos cíclicos sobre anéis de cadeia, seus duais e algumas condições sobre códigos auto-duais. Caracterizamos também os códigos cíclicos livres sobre anéis de cadeia e por fim exibimos uma fórmula para o peso de qualquer código cíclico sobre anéis de cadeia de comprimento p^n e $2p^n$.

Palavras-chave: anéis de grupo, anéis de cadeia, códigos cíclicos, peso de códigos cíclicos.

Abstract

Cyclic codes over chain rings

In this thesis, we use an approach of group rings to characterize cyclic codes over chain rings, their duals and some conditions on self-dual codes. It also features free cyclic codes over chain rings and finally we show a formula for the weight of any cyclic code over chain rings of length p^n and $2p^n$.

Keywords: group rings, chain rings, cyclic codes, weight of cyclic codes.

Sumário

1	Conceitos Preliminares	7
1.1	Resultados sobre anéis e anéis de grupos	7
1.2	Códigos cíclicos	13
1.3	Códigos cíclicos como ideais de RG	16
1.4	Alguns Resultados sobre Resíduos Quadráticos	19
2	Caracterização de Códigos Cíclicos sobre Anéis de Cadeia	23
2.1	Códigos Cíclicos sobre Anéis de Cadeia	24
2.2	Códigos duais e auto duais	29
3	Códigos de Comprimento p^n sobre Anéis de Cadeia	37
3.1	Códigos que são livres como R -submódulos de RG	45
3.2	Códigos MDS de Comprimento p^n	50
3.3	Códigos MDS de Comprimento 2^n	54
3.3.1	Resultados Sobre Códigos MDS de comprimento p^n	55
4	Códigos sobre Anéis de Cadeia de Comprimento $2p^n$	57
4.1	Peso Mínimo de Códigos de Comprimento $2p^n$	58
4.2	Códigos Livres de Comprimento $2p^n$ Sobre Anéis de Cadeia	82
5	Conclusões Finais	85
	Referências Bibliográficas	89
	Bibliografia	91

Introdução

O avanço e a necessidade do uso de computadores e a utilização de qualquer aparelho ou atividade que envolve códigos tem levado ao crescente estudo de uma parte importante da Teoria da Informação, que é a Teoria dos Códigos Corretores de Erros, que lida com o problema geral da transmissão de mensagens de forma confiável. O marco inicial da teoria dos códigos corretores de erros é o trabalho de C.E. Shannon, “A Mathematical Theory of Communication”, publicado em 1948.

A Teoria dos Códigos Corretores de Erros é um campo de pesquisa muito atual, tanto do ponto de vista científico quanto tecnológico. A junção da teoria e de suas aplicações vem tornando cada vez mais próximas a Matemática Pura e a Aplicada.

Descobertas recentes de que bons códigos binários não lineares estão relacionados com códigos lineares sobre \mathbb{Z}_4 (veja em [5], [8], [16], [30]) têm motivado os estudos de códigos sobre anéis em geral. Pesquisas mais recentes podem ser vistas em [9], [11], [20], [25].

Como uma extensão natural de \mathbb{Z}_4 , em [6], Carlderbank e Sloane determinaram a estrutura de códigos cíclicos sobre \mathbb{Z}_p^m , depois, Kanwar e López-Permouth em [19] fizeram o mesmo, mas com diferentes demonstrações. Usando as mesmas técnicas que em [19], Wan em [37] estendeu os resultados de Kanwar e López-Permouth para códigos cíclicos sobre anéis de Galois. Em 1999, Norton e Sălăgean-Mandache em [28] estenderam os resultados

de [6] e [19] para códigos cíclicos sobre anéis de cadeia finitos. Mais adiante, em 2004, Dinh e López-Permouth em [10], demonstraram os mesmos resultados de [28] de uma forma diferente.

O peso de um código é uma informação fundamental, juntamente com um método de decodificação. Em se tratando de códigos cíclicos sobre anéis, tanto o peso, quanto um método de decodificação são difíceis de determinar e isto vem sendo alvo de estudos na atualidade. Em [7] Campello, Jorge e Costa desenvolveram um método de decodificação de códigos q-ários utilizando a métrica de Lee. Vale ressaltar que códigos q-ários são exemplos de códigos cíclicos sobre anéis de cadeia. Em [2], Babu e Zimmermann exibem um algoritmo para decodificação de códigos sobre anéis de Galois, que também são exemplos de anéis de cadeia.

O objetivo principal deste trabalho é utilizar uma abordagem via anéis de grupo para provar de diferente forma os resultados de Dinh e López-Permouth em [10], onde as demonstrações de todos os resultados são feitas de forma mais simples e diretas e em alguns resultados, de forma mais geral. Como contribuição original, vamos determinar o peso de qualquer código cíclico sobre anéis de cadeia finitos de comprimento p^n e $2p^n$, com algumas hipóteses adicionais e iremos caracterizar também os códigos cíclicos livres sobre anéis de cadeia, exibindo duas bases distintas para qualquer somando de um código cíclico livre.

O Capítulo 1 consiste de uma revisão de conceitos preliminares de anéis, anéis de grupo, códigos corretores de erros, códigos cíclicos e uma conexão entre o estudo de ideais em álgebras de grupo e códigos cíclicos.

No Capítulo 2, usando uma abordagem de anéis de grupo, provamos os resultados de Dinh e López-Permouth [10] sobre códigos cíclicos sobre anéis de cadeia de comprimento n e caracterizamos o código dual a um dado código e também os códigos auto-duais.

No Capítulo 3, consideramos o caso particular de códigos de comprimento p^n com algumas hipóteses sobre a relação entre q e p^n , onde $|R| = q^l$. Neste caso, a determinação dos códigos minimais depende unicamente da estrutura de subgrupos de C_{p^n} . Calculamos o peso de todos

os possíveis códigos cíclicos sobre anéis de cadeia finitos (ou uniseriais), caracterizamos os códigos cíclicos livres sobre anéis de cadeia, exibindo duas bases distintas para um dado código e por fim exibimos alguns resultados para códigos MDS.

No Capítulo 4, restringindo o comprimento para $2p^n$, calculamos o peso de todos os possíveis códigos cíclicos sobre anéis de cadeia e caracterizamos os códigos cíclicos livres sobre anéis de cadeia de forma análoga ao feito no Capítulo 3.

CAPÍTULO 1

Conceitos Preliminares

Neste capítulo apresentaremos os conceitos preliminares necessários para o entendimento e boa compreensão do texto. Não será apresentada a demonstração dos resultados.

No que segue, estaremos sempre considerando anéis comutativos com unidade e assim, não faremos distinção entre ideais a direita e a esquerda tanto em definições quanto nos resultados.

1.1 Resultados sobre anéis e anéis de grupos

Os resultados nesta seção podem ser encontrados em [1], [18], [21], [26], [31]. Admitimos conhecidos os conceitos básicos da teoria de Anéis e listamos alguns deles para estabelecer a notação do trabalho.

Definição 1.1.1 *Um anel R é chamado **anel de cadeia**, ou **uniserial**, se o conjunto de todos os ideais formam uma cadeia com a relação de inclusão.*

Definição 1.1.2 *Seja R um anel finito comutativo. Um ideal I de R é chamado **principal***

se ele é gerado por um único elemento. Um anel R é chamado **anel de ideais principais** se todo ideal de R é principal.

Definição 1.1.3 Um anel R é chamado **local** se possui um único ideal maximal.

Teorema 1.1.4 Para um anel comutativo R as seguintes condições são equivalentes:

- (i) R é um anel local e o ideal maximal M de R é principal.
- (ii) R é um anel local de ideais principais.
- (iii) R é um anel de cadeia.

Definição 1.1.5 Um anel R é chamado **anel serial**, se R é uma soma direta de anéis de cadeia.

Proposição 1.1.6 Sejam R um anel de cadeia finito e comutativo com unidade, com ideal maximal $M = \langle a \rangle$, t o índice de nilpotência de a em R e $\bar{R} = \frac{R}{M}$. Então:

- (a) Para algum primo q e inteiros positivos k e l ($k \geq l$), $|R| = q^k$, $|\bar{R}| = q^l$ e a característica de R e \bar{R} são potências de q .
- (b) Para $i = 0, 1, 2, \dots, t$, $|\langle a^i \rangle| = |\bar{R}|^{t-i}$. Em particular, $|R| = |\bar{R}|^t$, isto é, $k = lt$.

Definição 1.1.7 Um elemento e de um anel R é dito **idempotente** se $e^2 = e$. Dois idempotentes e_i e e_j são chamados **ortogonais** se $e_i \cdot e_j = 0$. Um idempotente e é **central** se $e \cdot r = r \cdot e$, para todo $r \in R$. Um idempotente e é chamado **primitivo** se sempre que escrevermos $e = e_1 + e_2$, com e_1 e e_2 idempotentes ortogonais, então ou $e_1 = 0$ ou $e_2 = 0$.

Proposição 1.1.8 Se $R = I_0 \oplus \dots \oplus I_j$ para alguns ideais I_0, \dots, I_j , então existem idempotentes ortogonais e_0, e_1, \dots, e_j tais que $1 = e_0 + e_1 + \dots + e_j$ e $e_k R = I_k$, para cada $k \in \{0, 1, \dots, j\}$.

Definição 1.1.9 Um ideal I de R é chamado **nil**, se para cada $x \in I$, existe um inteiro n , tal que $x^n = 0$.

Um ideal I de um anel R é chamado **nilpotente** se existe um inteiro positivo n , tal que $I^n = 0$, onde I^n é o conjunto de todas as somas finitas da forma $\sum_{i=1}^n x_1 x_2 \dots x_n$, com $x_i \in I, 1 \leq i \leq n$.

Definição 1.1.10 Seja R um anel. O **radical de Jacobson** de R , denotado por $J(R)$ é a intersecção de todos os ideais maximais de R .

Proposição 1.1.11 Seja R um anel. Todo ideal nil de R está contido em $J(R)$.

É claro que se um ideal I de R é nilpotente, então I é nil. Logo, todo ideal nilpotente esta contido em $J(R)$.

Proposição 1.1.12 ([18], Proposição 7.14) Seja R anel comutativo e N um nil ideal em R , e $\bar{f} = u + N$ um idempotente de $\bar{R} = \frac{R}{N}$. Então existe um único idempotente e em R tal que $\bar{e} = \bar{f}$.

Definição 1.1.13 Dois ideais I_1 e I_2 são chamados **coprímos** (ou **comaximais**) se $I_1 + I_2 = \langle 1 \rangle$.

Claramente dois ideais I_1 e I_2 são coprímos se, e somente se, existem $x \in I_1$ e $y \in I_2$ tais que $x + y = 1$.

Proposição 1.1.14 Se I_1, \dots, I_n são ideais coprímos aos pares, então

$$I_1 I_2 \dots I_n = I_1 \cap I_2 \cap \dots \cap I_n.$$

Teorema 1.1.15 (Teorema Chinês do Resto) Se I_1, \dots, I_n são ideais de um anel R coprímos dois a dois, então

$$\frac{R}{I_1 \dots I_n} \simeq \frac{R}{I_1} \times \dots \times \frac{R}{I_n}.$$

Definição 1.1.16 *Seja R um anel, M um ideal de R e $\bar{R} = \frac{R}{M}$. Considere a aplicação*

$$\begin{aligned} \bar{} : R[x] &\rightarrow \bar{R}[x] \\ f(x) = \sum_{i=0}^s r_i x^i &\mapsto \bar{f}(x) = \sum_{i=0}^s \bar{r}_i x^i, \end{aligned}$$

onde $\bar{r}_i = r_i + M$, para todo $r_i \in R$. Um polinômio $f \in R[x]$ é chamado **básico irreduzível** sobre R se \bar{f} é irreduzível em $\bar{R}[x]$ e **regular** sobre R se ele não é um divisor de zero.

Proposição 1.1.17 ([21], Teorema XIII.2(c)) *Seja $f = a_0 + a_1x + \dots + a_nx^n \in R[x]$.*

Então são equivalentes:

i) f é regular,

ii) $\langle a_0, \dots, a_n \rangle = R$,

iii) a_i é uma unidade para algum i , $0 \leq i \leq n$,

iv) $\bar{f} \neq 0$.

O próximo teorema é chamado de **Lema de Hensel** e pode ser encontrado em [21], Teorema XIII.4

Lema 1.1.18 (Lema de Hensel) *Seja f um polinômio sobre R e assumamos $\bar{f} = g_1g_2\dots g_r$, onde g_1, g_2, \dots, g_r são polinômios coprimos dois a dois sobre \bar{R} . Então existem polinômios f_1, f_2, \dots, f_r coprimos dois a dois sobre R tais que $f = f_1f_2\dots f_r$ e $\bar{f}_i = g_i$, para $i = 1, 2, \dots, r$.*

Proposição 1.1.19 ([21], Teorema XIII.7) *Seja f um polinômio regular sobre $R[x]$. Se f é básico irreduzível, então f é irreduzível.*

Definição 1.1.20 *Seja G um grupo e R um anel. O **anel de grupo** de G sobre R , denotado por RG , é o conjunto dos elementos da forma*

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

onde $x_g \in R$ e $x_g = 0$ quase sempre, ou seja, somente um número finito de coeficientes são diferentes de zero.

Definição 1.1.21 Dado um elemento $\alpha = \sum_{g \in G} a_g g \in RG$, definimos o **suporte** de α , denotado por $\text{supp}(\alpha)$ como sendo

$$\text{supp}(\alpha) = \{g \in G : a_g \neq 0\}.$$

Observe que, dados dois elementos $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g \in RG$, temos $\alpha = \beta$ se, e somente se, $a_g = b_g$, para todo $g \in G$.

Com as seguintes definições de soma e produto de dois elementos em RG e produto de um elemento de RG por um elemento $\lambda \in R$, o anel de grupo RG possui estrutura de anel e de R -módulo.

- $(\sum_{g \in G} a_g g) + (\sum_{g \in G} b_g g) = \sum_{g \in G} (a_g + b_g) g;$
- $\alpha \cdot \beta = \sum_{g, h \in G} a_g b_h gh$, onde $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{h \in G} b_h h;$
- $\lambda(\sum_{g \in G} a_g g) = \sum_{g \in G} \lambda a_g g.$

Definição 1.1.22 O homomorfismo

$$\begin{aligned} \xi : RG &\rightarrow R \\ (\sum_{g \in G} a_g g) &\mapsto \sum_{g \in G} a_g \end{aligned}$$

é chamado **aplicação de aumento** de RG e seu núcleo, denotado por

$$\Delta(G) = \left\{ \sum_{g \in G} a_g (g - 1) : g \in G, g \neq 1 \right\}, \text{ é chamado } \mathbf{ideal de aumento} \text{ de } RG.$$

Proposição 1.1.23 Se H é um subgrupo de um grupo G , então

$$\Delta(G : H) = \left\{ \sum_{ht} \alpha_{ht} t(h - 1) : h \in H, h \neq 1, t \in \tau \right\},$$

onde τ é um transversal de H em G , é um ideal de RG .

Corolário 1.1.24 *Se H é um subgrupo normal de um grupo G , então*

$$\frac{RG}{\Delta(G:H)} \simeq R\left(\frac{G}{H}\right).$$

Proposição 1.1.25 *Se I é um ideal bilateral de um anel R e G é um grupo comutativo, então $IG = \left\{ \sum_{g \in G} a_g g \in RG : a_g \in I \right\}$ é um ideal bilateral de RG e $\frac{RG}{IG} \simeq \left(\frac{R}{I}\right)G$.*

Proposição 1.1.26 *Seja $\{R_i\}_{i \in I}$ uma família de anéis e seja $R = \bigoplus_{i \in I} R_i$. Então para qualquer grupo G , $RG \simeq \sum_{i \in I} R_i G$.*

Teorema 1.1.27 (Teorema de Maschke) *Seja G um grupo. O anel de grupo RG é semisimples se, e somente se, as seguintes condições são satisfeitas:*

- (i) R é um anel semisimples.
- (ii) G é finito.
- (iii) $|G|$ é inversível em R .

Corolário 1.1.28 *Sejam G um grupo finito e K um corpo. A álgebra KG é semisimples se, e somente se, $\text{car}(K)$ não divide $|G|$.*

Corolário 1.1.29 *Se G é um grupo abeliano finito e K um corpo tal que $\text{car}(K)$ não divide $|G|$, então KG é uma soma direta de corpos.*

Teorema 1.1.30 ([21], Teorema VII.8) *Seja e um idempotente não nulo de um anel R . As seguintes condições são equivalentes:*

- (1) e é primitivo.
- (2) eRe é um anel local.

(3) Re é indecomponível.

Note que, no caso particular em que R e G são comutativos, temos o seguinte.

Corolário 1.1.31 *Seja e um idempotente não nulo de um anel RG . As seguintes condições são equivalentes:*

(1) e é primitivo.

(2) RGe é um anel local.

(3) RGe é indecomponível.

Teorema 1.1.32 *Sejam R um anel com unidade e H um subgrupo de um grupo G . Se $|H|$ é inversível em R , então $e_H = \hat{H}$ é um idempotente em RG , onde $\hat{H} = \frac{1}{|H|} \sum_{h \in H} h$. Além disso, se $H \triangleleft G$, então e_H é central e*

$$RGe_H \simeq R\left(\frac{G}{H}\right).$$

1.2 Códigos cíclicos

Nesta seção, abordaremos sem muitos detalhes conceitos de códigos corretores de erros. Os resultados e definições apresentados nesta seção podem ser encontrados em [6], [30].

Definição 1.2.1 *Um conjunto finito A será chamado de **alfabeto** e o número de elementos de A será denotado por $|A|$.*

Definição 1.2.2 *Um código corretor de erros é um subconjunto próprio qualquer de A^n , para algum número natural n . Os elementos de um código corretor de erros serão chamados de **palavras**.*

A fim de tornar possível medir a distância entre palavras de um dado código em A^n , definiremos a seguir a distância de Hamming.

Definição 1.2.3 Dados dois elementos $u = (u_1, \dots, u_n)$ e $v = (v_1, \dots, v_n) \in A^n$, a **distância de Hamming** entre u e v é definida por

$$d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|.$$

Observe que a distância de Hamming é simétrica, satisfaz a desigualdade triangular e $d(u, v) \geq 0$, para todo $u, v \in A^n$. Por isso, é também chamada de **métrica de Hamming**.

Definição 1.2.4 A **distância mínima** de um código C é o inteiro

$$d(C) := \min\{d(x, y); x, y \in C \text{ e } x \neq y\},$$

onde $d(x, y)$ é a distância de Hamming entre x e y .

Uma classe de códigos muito utilizada na prática é a chamada classe dos códigos lineares. Para definir esta classe de códigos, iremos considerar um anel finito R como sendo o alfabeto e R^n um conjunto de n -uplas de elementos de R como um módulo sobre R de maneira usual.

Definição 1.2.5 Um subconjunto $C \subset R^n$ é chamado um **código linear de comprimento n** sobre R , se C é um R -submódulo próprio de R^n .

Definição 1.2.6 Dado $\beta = (r_1, \dots, r_n) \in R^n$, defini-se o **peso** de β como sendo o número inteiro

$$w(\beta) = |\{i; r_i \neq 0\}|.$$

Observe que o peso de um elemento β é a distância de Hamming entre β e zero.

Definição 1.2.7 O **peso mínimo** de um código linear $C \subset R^n$ é o inteiro

$$w(C) := \min\{w(\beta); \beta \in C \setminus \{0\}\}.$$

Proposição 1.2.8 Seja $C \subset R^n$ um código linear com distância d . Então, temos:

(i) $d(\beta_1, \beta_2) = w(\beta_1 - \beta_2)$, para todo $\beta_1, \beta_2 \in R^n$.

(ii) $d(C) = w(C)$.

Definição 1.2.9 Para um código linear C de comprimento n sobre R , definimos o **posto** de C , denotado por $\text{posto}(C)$, como sendo o número mínimo de geradores de C . Definimos o **posto livre** de C , denotado por $\text{postolivre}(C)$, como sendo o máximo dos postos de R -submódulos livres de C .

Definição 1.2.10 Dizemos que um código linear $C \subset R^n$ é **livre** se $\text{postolivre}(C) = \text{posto}(C)$.

Dentro da classe dos códigos lineares, existe uma importante subclasse de códigos, conhecida como classe dos códigos cíclicos, que será nosso principal interesse. Códigos cíclicos são importantes na prática, devido aos eficientes métodos de codificação e decodificação existentes quando tomamos o anel como sendo um corpo. Não entraremos em detalhes sobre codificação e decodificação, mas estes podem ser estudados em [14], onde o alfabeto em questão é um corpo.

Definição 1.2.11 Um código linear C é dito **cíclico** se para toda palavra $\beta = (r_1, \dots, r_n) \in C$, sua troca cíclica também está em C , ou seja, a palavra $\beta' = (r_n, r_1, \dots, r_{n-1}) \in C$.

Sejam $u = (u_1, \dots, u_n)$ e $v = (v_1, \dots, v_n)$ elementos de R^n . Define-se o **produto escalar** de u e v por

$$u \cdot v = u_1v_1 + \dots + u_nv_n.$$

O produto escalar possui as propriedades usuais de um produto interno.

Definição 1.2.12 Sejam u e $v \in R^n$. Dizemos que u e v são **ortogonais** se $u \cdot v = 0$.

Definição 1.2.13 Seja $C \subset R^n$ um código linear, define-se

$$C^\perp = \{\beta \in R^n; \beta \cdot u = 0, \text{ para todo } u \in C\}.$$

Proposição 1.2.14 *Se $C \subset R^n$ é um código linear, então C^\perp é um R -submódulo de R^n .*

Definição 1.2.15 *Dado um código linear C , chamaremos de C^\perp de **código dual de C** .*

Lema 1.2.16 *Seja R um anel finito de ordem q^β , q primo. O número de palavras em qualquer código linear de comprimento n sobre R é q^k , para algum inteiro $k \in \{0, \dots, \beta n\}$. Além disso, o código dual C^\perp tem q^l palavras, onde $k + l = \beta n$.*

1.3 Códigos cíclicos como ideais de RG

Nesta seção exibiremos uma conexão entre códigos cíclicos e ideais em anéis de grupo. Os resultados aqui apresentados, podem ser encontrados em [24], [34].

Seja R um anel comutativo com unidade e G um grupo cíclico de ordem n gerado por g . Seja C um R -submódulo de R^n . Considere agora o homomorfismo de módulos ψ dado por

$$\begin{aligned} \psi : R^n &\rightarrow RG \\ \beta = (r_0, \dots, r_{n-1}) &\mapsto r_0 + r_1g + r_2g^2 + \dots + r_{n-1}g^{n-1}. \end{aligned}$$

Observe que C é um código cíclico em R^n se, e somente se, $\psi(C)$ é um ideal em RG . De fato, seja C um código cíclico em R^n . Como ψ é um R -homomorfismo, para todo $r \in R$ e $x \in C$, temos $r \cdot \psi(x) = \psi(r \cdot x)$. Como C é um R -submódulo de R^n , temos $r \cdot x \in C$ e portanto $r \cdot \psi(x) \in \psi(C)$. Para provarmos que $\psi(C)$ é um ideal em RG é suficiente provar que $g \cdot \psi(x) \in \psi(C)$, para todo $x \in C$. Seja $x = (x_0, \dots, x_{n-1}) \in C$, $g \cdot \psi(x) = g \cdot (x_0 + x_1g + \dots + x_{n-1}g^{n-1}) = x_{n-1} + x_0g + x_1g^2 + \dots + x_{n-2}g^{n-1}$. Como $x = (x_0, \dots, x_{n-1}) \in C$ e C é cíclico, então $(x_{n-1}, x_0, \dots, x_{n-2}) \in C$. Portanto,

$$\begin{aligned} \psi((x_{n-1}, x_0, \dots, x_{n-2})) &= x_{n-1} + x_0g + x_1g^2 + \dots + x_{n-2}g^{n-1} \\ &= g \cdot \psi(x) \in \psi(C). \end{aligned}$$

Agora suponhamos que $\psi(C)$ seja um ideal em RG . Devemos provar que C é um código

cíclico em R^n . Para isso, basta provar que se $x = (x_0, \dots, x_{n-1}) \in C$, então $(x_{n-1}, x_0, \dots, x_{n-2}) \in C$. Como $x = (x_0, \dots, x_{n-1}) \in C$, então $x_0 + x_1g + \dots + x_{n-1}g^{n-1} \in \psi(C)$. Como $\psi(C)$ é ideal, temos $g \cdot \psi(x) \in C$. Logo $x_{n-1} + x_0g + x_1g^2 + \dots + x_{n-2}g^{n-1} \in \psi(C)$. Assim, $(x_{n-1}, \dots, x_{n-2}) \in C$.

Definição 1.3.1 A palavra $(a_0, a_1, \dots, a_{n-1}) \in R^n$ é definida como **palavra associada** a $\alpha = a_0 + a_1g + \dots + a_{n-1}g^{n-1} \in RG$.

Uma outra abordagem muito utilizada no estudo de códigos é a de anéis polinomiais. É fácil ver que $RG \simeq \frac{R[x]}{(x^n-1)}$, onde G é um grupo cíclico de ordem n e R anel comutativo com unidade.

Seja $x^n - 1 = \bar{g}_0 \dots \bar{g}_m$ a decomposição de $x^n - 1$ em polinômios irredutíveis coprimos dois a dois em $\bar{R}[x]$. Pelo Lema de Hensel 1.1.18, sabemos que existem polinômios f_0, \dots, f_m , coprimos dois a dois em $R[x]$ tais que $x^n - 1 = f_0 \dots f_m$. Como f_i é regular, para $0 \leq i \leq m$, pela proposição 1.1.19, temos f_i irredutível.

Sabemos que

$$RG \simeq \frac{R[x]}{(x^n - 1)},$$

onde G é um grupo cíclico de ordem n e $x^n - 1 = f_0 \cdot f_1 \dots f_m$ é a decomposição de $x^n - 1$ como produto de polinômios irredutíveis coprimos dois a dois em $R[x]$. Pelo Teorema Chinês do Resto (1.1.15), temos

$$\frac{R[x]}{(x^n - 1)} \simeq \frac{R[x]}{(f_0)} \oplus \dots \oplus \frac{R[x]}{(f_m)}.$$

Assim, informações importantes sobre os códigos cíclicos sobre R podem ser obtidas através dos anéis $\frac{R[x]}{(f_i)}$. Observe também que devido ao isomorfismo podemos afirmar que existe um conjunto de idempotentes primitivos ortogonais com exatamente $m + 1$ elementos, tal que

$$RG = RGe_0 \oplus \dots \oplus RGe_m,$$

onde, reordenando as parcelas se preciso, temos $RGe_r \simeq \frac{R[x]}{(f_r)}$ e assim,

$$| RGe_r | = | R |^{w_r}, \text{ onde } w_r = \text{grau}(f_r).$$

A fim de simplificar a notação, denotaremos $\frac{R[x]}{(x^n-1)}$ por R_n .

Teorema 1.3.2 *Um polinômio mônico $p(x)$ em R_n é um **polinômio gerador para um código cíclico** C , isto é, $C = \langle p(x) \rangle$ se, e somente se, $p(x)$ divide $x^n - 1$.*

Teorema 1.3.3 *Sejam $C_1 = \langle g_1(x) \rangle$ e $C_2 = \langle g_2(x) \rangle$ códigos cíclicos em R_n . Então, $C_1 \subset C_2$ se, e somente se, $g_2(x)$ divide $g_1(x)$.*

Consideremos a seguinte caracterização para os idempotentes primitivos e_s 's que pode ser encontrada em [34] ou [22]. Seja C_s a classe ciclotômica módulo n que contém s e α uma raiz n -ésima primitiva da unidade. Então,

$$e_s = \frac{1}{n} \sum_{i=0}^{n-1} \sum_{j \in C_s} \alpha^{-ij} g^i. \quad (1.1)$$

Considere a aplicação

$$\begin{aligned} * : RG & \rightarrow RG \\ \alpha = a_0 + a_1g + \dots + a_{n-1}g^{n-1} & \mapsto \alpha^* = a_0 + a_1g^{-1} + a_2g^{-2} + \dots + a_{n-1}g^1, \end{aligned}$$

chamada **involução clássica de RG** . Vejamos algumas propriedades de $*$. Sejam $\alpha, \beta \in RG$ e $r \in R$. Temos

- $(\alpha + \beta)^* = \alpha^* + \beta^*$.
- $(r \cdot \alpha)^* = r(\alpha)^*$.
- $(\alpha\beta)^* = \beta^*\alpha^* = \alpha^*\beta^*$, pois RG é comutativo.

É fácil ver que $*$ é um isomorfismo de anéis. Observe também que $*$: $RGe_i \rightarrow RGe_i^*$ é isomorfismo de anéis. Portanto, $|RGe_i| = |RGe_i^*|$.

Teorema 1.3.4 *Sejam $\alpha = a_0 + a_1g + \dots + a_{n-1}g^{n-1}$ e $\beta = b_0 + b_1g + \dots + b_{n-1}g^{n-1}$. Então, $\alpha \cdot \beta = 0$ em RG se, e somente se, $(a_0, a_1, \dots, a_{n-1})$ é ortogonal em R^n a $(b_{n-1}, b_{n-2}, \dots, b_1, b_0)$ e todas as suas trocas cíclicas.*

Definição 1.3.5 *Dizemos que duas palavras α e $\beta \in RG$ são **ortogonais** se suas palavras associadas em R^n são ortogonais.*

1.4 Alguns Resultados sobre Resíduos Quadráticos

Nesta seção, apresentaremos alguns resultados sobre resíduos quadráticos, que serão necessários em resultados no próximo capítulo sobre códigos auto-duais. O conteúdo desta seção pode ser encontrado em [4], [27], [33], [35], [36].

Definição 1.4.1 *Sejam a e m inteiros relativamente primos, isto é, $\text{mdc}(a, m) = 1$. Se a congruência quadrática $x^2 \equiv a \pmod{m}$ tem uma solução, então a é dito ser um **resíduo quadrático** de m , caso contrário a é chamado de **não resíduo quadrático** de m .*

Euler deu um critério simples para saber quando um inteiro a é um resíduo quadrático de um dado primo q .

Teorema 1.4.2 *Seja q um primo ímpar e $\text{mdc}(a, q) = 1$. Então a é um resíduo quadrático ou não resíduo quadrático de q quando $a^{\frac{q-1}{2}} \equiv 1 \pmod{q}$ ou $a^{\frac{q-1}{2}} \equiv -1 \pmod{q}$, respectivamente.*

Para simplificar a notação, definiremos a seguir o símbolo de Legendre, introduzido pelo matemático Adrien Marie Legendre(1752-1833), em 1798.

Definição 1.4.3 *Seja q um primo ímpar e $\text{mdc}(a, q) = 1$. O símbolo de Legendre $(a|q)$ é definido por:*

$$(a|q) = \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático de } q. \\ -1, & \text{se } a \text{ é um não resíduo quadrático de } q. \end{cases}$$

No símbolo de Legendre $(a|q)$, a e q são chamados **numerador** e **denominador**, respectivamente.

Observação 1.4.4 *Pelo Teorema 1.4.2 e pela definição do símbolo de Legendre, para um inteiro ímpar q e um inteiro a com $\text{mdc}(a, q) = 1$, temos*

$$(a|q) = \begin{cases} 1, & \text{se e somente se, } a^{\frac{q-1}{2}} \equiv 1 \pmod{q}. \\ -1, & \text{se e somente se, } a^{\frac{q-1}{2}} \equiv -1 \pmod{q}. \end{cases}$$

A seguir, exibiremos algumas propriedades elementares do símbolo de Legendre.

Proposição 1.4.5 *Sejam q um primo ímpar, a e b inteiros relativamente primos com q , Então:*

(i) *Se $a \equiv b \pmod{q}$, então $(a|q) = (b|q)$;*

(ii) *$(a|q) \equiv a^{\frac{q-1}{2}} \pmod{q}$;*

(iii) *$(ab|q) = (a|q)(b|q)$;*

(iv) *$(a^2|q) = 1$;*

(v) *$(ab^2|q) = (a|q)(b^2|q) = (a|q)$.*

Teorema 1.4.6 (Lema de Gauss) *Seja q um primo ímpar e $\text{mdc}(a, q) = 1$. Se k denota o número de inteiros no conjunto $S = \{a, 2a, 3a, \dots, \frac{q-1}{2}a\}$ cujo resto da divisão por q excede $\frac{q}{2}$, então $(a|q) = (-1)^k$.*

Teorema 1.4.7 (Lei da Reciprocidade Quadrática) *Se p e q são primos ímpares distintos, então*

$$(p|q)(q|p) = -1^{\left(\frac{p-1}{2} \frac{q-1}{2}\right)}.$$

Teorema 1.4.8 *Se p e q são primos ímpares distintos, então*

$$(i) \quad (p|q)(q|p) = \begin{cases} 1, & \text{se } p \equiv 1(\text{mod}4) \text{ ou } q \equiv 1(\text{mod}4) \\ -1 & \text{se } p \equiv q \equiv 3(\text{mod}4). \end{cases}$$

$$(ii) \quad (p|q) = \begin{cases} (q|p), & \text{se } p \equiv 1(\text{mod}4) \text{ ou } q \equiv 1(\text{mod}4) \\ -(q|p) & \text{se } p \equiv q \equiv 3(\text{mod}4). \end{cases}$$

O Lema de Gauss 1.4.6 e a Lei da Reciprocidade Quadrática 1.4.7 nos permitem calcular $(a|q)$ para valores específicos de a . A proposição seguinte nos fornece uma lista de alguns destes cálculos.

Proposição 1.4.9 *Seja q um primo ímpar. Então:*

$$(i) \quad (1|q) = 1 \text{ e } (-1|q) = (-1)^{\frac{q-1}{2}};$$

$$(ii) \quad (-1|q) = \begin{cases} 1, & \text{se } q \equiv 1(\text{mod}4) \\ -1 & \text{se } q \equiv 3(\text{mod}4). \end{cases}$$

$$(iii) \quad (2|q) = \begin{cases} 1, & \text{se } q \equiv 1(\text{mod}8) \text{ ou } q \equiv 7(\text{mod}8) \\ -1 & \text{se } q \equiv 3(\text{mod}8) \text{ ou } q \equiv 5(\text{mod}8). \end{cases}$$

$$(iv) \quad (-2|q) = \begin{cases} 1, & \text{se } q \equiv 1(\text{mod}8) \text{ ou } q \equiv 3(\text{mod}8) \\ -1 & \text{se } q \equiv 5(\text{mod}8) \text{ ou } q \equiv 7(\text{mod}8). \end{cases}$$

$$(v) \quad (5|q) = \begin{cases} 1, & \text{se } q \equiv 1, 9, 11, 19(\text{mod}20) \\ -1 & \text{se } q \equiv 3, 7, 13, 17(\text{mod}20). \end{cases}$$

$$(vi) \quad (6|q) = \begin{cases} 1, & \text{se } q \equiv 1, 5, 19, 23(\text{mod}24) \\ -1 & \text{se } q \equiv 7, 11, 13, 17(\text{mod}24). \end{cases}$$

$$(vii) \quad (7|q) = \begin{cases} 1, & \text{se } q \equiv 1, 3, 9, 19, 25, 27(\text{mod}28) \\ -1 & \text{se } q \equiv 5, 11, 13, 15, 17, 23(\text{mod}28). \end{cases}$$

$$(viii) \quad (11|q) = \begin{cases} 1, & \text{se } q \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43(\text{mod}44) \\ -1 & \text{se } q \equiv 3, 13, 15, 17, 21, 23, 27, 29, 31, 41(\text{mod}44). \end{cases}$$

Se além disso o primo ímpar q é > 3 , então,

$$(ix) \quad (3|q) = \begin{cases} 1, & \text{se } q \equiv 1(\text{mod}12) \text{ ou } q \equiv 11(\text{mod}12) \\ -1 & \text{se } q \equiv 5(\text{mod}12) \text{ ou } q \equiv 7(\text{mod}12). \end{cases}$$

$$(x) \quad (-3|q) = \begin{cases} 1, & \text{se } q \equiv 1(\text{mod}6) \\ -1 & \text{se } q \equiv 5(\text{mod}6). \end{cases}$$

Proposição 1.4.10 *Seja q um primo ímpar, k um inteiro positivo e $\text{mdc}(a, q) = 1$. Então a é um resíduo quadrático de q^k se, e somente se, $(a|q) = 1$.*

Teorema 1.4.11 *Seja $m = 2^{k_0} p_1^{k_1} \dots p_r^{k_r}$ a fatorização de m , com p_i primo e $\text{mdc}(a, m) = 1$. Então a é um resíduo quadrático de m se, e somente se,*

(i) *para $i = 1, \dots, r$, $(a|p_i) = 1$;*

$$(ii) \quad a \equiv \begin{cases} 1(\text{mod}4), & \text{se } 4|m \text{ mas } 8 \nmid m \\ 1(\text{mod}8), & \text{se } 8|m. \end{cases}$$

CAPÍTULO 2

Caracterização de Códigos Cíclicos sobre Anéis de Cadeia

Neste capítulo iremos identificar todos os possíveis códigos cíclicos C em anéis de grupo sobre um anel de cadeia finito R , comutativo com unidade, com $|R| = q^k$ com q primo e G um grupo cíclico finito de ordem n , onde q não divide n . Determinaremos o número de códigos existentes sobre um dado anel, provaremos que RG é um anel de ideais principal e para finalizar, iremos caracterizar o código dual a um dado código C e também alguns resultados sobre códigos auto-duais.

Em [10], López-Permouth e Dinh caracterizam códigos sobre anéis de cadeia para um comprimento n onde a característica do anel R é q^m e q não divide n ; determinam o número de elementos dos mesmo e exibem o dual de um dado código utilizando linguagem de anéis polinomiais. Aqui, faremos o mesmo utilizando uma abordagem de anéis de grupo, porém, de maneira mais simples. No próximo capítulo apresentaremos resultados novos, utilizando a abordagem de anéis de grupo.

2.1 Códigos Cíclicos sobre Anéis de Cadeia

A seguir exibiremos alguns resultados para o desenvolvimento da teoria.

Observe que se R é anel de cadeia comutativo com unidade e M é o ideal maximal de R , então $\bar{R} = \frac{R}{M}$ é um corpo. Daqui em diante estaremos sempre nos referindo a anéis de cadeia onde $q \nmid |G|$.

Pela Proposição 1.1.6, sabemos que, $|R| = q^k$, então $\text{car}(R)$ é uma potência de q .

A seguir, temos um teorema usado como ferramenta na caracterização dos códigos sobre anéis de cadeia, que é um caso particular da Proposição 1.1.25.

Teorema 2.1.1 *Seja R anel de cadeia e M o ideal maximal de R . Então*

$$\frac{RG}{MG} \cong \left(\frac{R}{M} \right) G.$$

Como estamos considerando que $q \nmid n$, onde $|R| = q^k$ e $|G| = n$, pela Proposição 1.1.6, $\text{car}\left(\frac{R}{M}\right) \nmid |G|$. Agora, pelo Corolário 1.1.28, $\left(\frac{R}{M}\right)G$ é semisimples e, pela Proposição 1.1.8, existem idempotentes primitivos ortogonais $\bar{e}_0, \dots, \bar{e}_m$ tais que $\bar{R}G = \bar{R}G\bar{e}_0 \oplus \dots \oplus \bar{R}G\bar{e}_m$. Pelo Teorema 2.1.1 e pela Proposição 1.1.12, existe uma única família de idempotentes ortogonais $\{e_0, \dots, e_m\}$ em RG tal que $RG = RGe_0 \oplus \dots \oplus RGe_m$. Nosso objetivo agora é garantir que $\{e_0, \dots, e_m\}$ é um conjunto de idempotentes primitivos ortogonais em RG .

Teorema 2.1.2 *Sejam R um anel local com ideal maximal $M = \langle a \rangle$, com $|R| = q^k$ e G um grupo cíclico de ordem n , onde $q \nmid n$. Se $\{\bar{e}_0, \dots, \bar{e}_m\}$ é o conjunto de idempotentes primitivos ortogonais em $\bar{R}G$, então $\{e_0, \dots, e_m\}$ é o conjunto de idempotentes primitivos ortogonais em RG .*

Prova: Considere

$$\begin{aligned} \phi: RGe_k &\rightarrow \frac{RG}{MG}\bar{e}_k \\ \sum_{i=0}^n r_i g^i e_k &\mapsto \sum_{i=0}^n \bar{r}_i g^i \bar{e}_k. \end{aligned}$$

Suponhamos $e_k = b_k + c_k$, onde b_k e c_k são idempotentes ortogonais. Então $\bar{e}_k = \bar{b}_k + \bar{c}_k$. Como \bar{e}_k é um idempotente primitivo, temos $\bar{b}_k = 0$ ou $\bar{c}_k = 0$. Logo, $b_k \in MG$ ou $c_k \in MG$. Como MG é nilpotente, temos $b_k = 0$ ou $c_k = 0$. Portanto, e_k é idempotente primitivo. ■

No teorema a seguir, iremos caracterizar todos os códigos cíclicos de comprimento n sobre RGe_i , onde R é um anel de cadeia e e_i é um idempotente primitivo ortogonal.

Sabemos pelo Corolário 1.1.31, que RGe_i é um anel local. No que segue, para simplificar a notação, escreveremos os ideais da forma $(RG)a^j e_i$ como $\langle a^j e_i \rangle$.

Teorema 2.1.3 *Seja R um anel de cadeia finito, comutativo com unidade, com $|R| = q^k$, $M = \langle a \rangle$ ideal maximal de R e t o índice de nilpotência de a em R . Seja $G = C_n$, onde $q \nmid n$. Se I é um ideal de RGe_i , então I é da forma $I = \langle a^{k_i} e_i \rangle$, com $0 \leq k_i \leq t$.*

Prova: Seja I um ideal não nulo de RGe_i , com $I \neq (RG)e_i$. Seja $\zeta \neq 0$ um elemento de I , logo $\zeta = xe_i$, com $x \in RG$. Como M é ideal maximal de R , $\left(\frac{R}{M}\right)Ge_i$ é corpo e, como $\left(\frac{R}{M}\right)Ge_i \simeq \frac{RGe_i}{MGe_i}$ e $\left(\frac{R}{M}\right)Ge_i$ é uma componente simples de $\left(\frac{R}{M}\right)G$, pelo Corolário 1.1.29, $\frac{RGe_i}{MGe_i}$ é um corpo. Assim, concluímos que MGe_i é ideal maximal de RGe_i . Pelo Corolário 1.1.31, sabemos que RGe_i é anel local. Como $\zeta \in MGe_i$, podemos escrever $\zeta = \sum \alpha_g g e_i$, com $\alpha_g \in M$. Então $\alpha_g = r_g a$, $r_g \in R$. Assim, $\zeta = \sum r_g a g e_i = (\sum r_g g) a e_i \in \langle a e_i \rangle$ e, portanto, $I \subset \langle a e_i \rangle$.

Agora seja k o maior inteiro positivo tal que $I \subset \langle a^k e_i \rangle$. Com isso, existe $\zeta \in I$ tal que ζ não pertence a $\langle a^{k+1} e_i \rangle$. Provemos que $\zeta = a^k \beta e_i$, com $\beta \in RGe_i$ inversível. De fato, suponhamos que β não seja inversível. Como $\left(\frac{R}{M}\right)Ge_i$ é corpo, temos que $\beta \in MGe_i$; com isso, $\beta = a\beta'$, $\beta' \in RGe_i$ e assim temos $\zeta = a^k \cdot a\beta' e_i \in \langle a^{k+1} e_i \rangle$, o que é uma contradição. Logo, existe $\gamma \in RGe_i$ tal que $\beta\gamma = e_i$. Portanto, $a^k e_i = a^k \beta\gamma e_i = a^k \beta e_i \cdot \gamma e_i = (\zeta) \cdot \gamma e_i \in I$ e com isso concluímos que $I = \langle a^k e_i \rangle$.

■

Corolário 2.1.4 *Com as mesmas hipóteses do Teorema anterior, o ideal RGe_i é indecomponível em RG e o código gerado por $\langle a^{t-1}e_i \rangle$ é minimal.*

Observe que como qualquer ideal I de RGe_i é da forma $I = \langle a^{k_i}e_i \rangle$, então RGe_i é anel de cadeia.

Seja $\{e_0, \dots, e_m\}$ o conjunto dos idempotentes primitivos de RG . No teorema a seguir iremos caracterizar todos os códigos cíclicos de comprimento n sobre anéis de cadeia.

Teorema 2.1.5 *Seja R um anel de cadeia finito e comutativo, com ideal maximal $M = \langle a \rangle$, t o índice de nilpotência de a em R , com $|R| = q^k$ e $G = \langle g_0; g_0^n = 1 \rangle$ tal que $q \nmid n$. Se I é um ideal de RG , então I é da forma $I = I_0 \oplus \dots \oplus I_m$, onde $I_i = \langle a^{k_i}e_i \rangle$, com $0 \leq k_i \leq t$.*

Prova: Escrevemos $RG = RGe_0 \oplus \dots \oplus RGe_m$. Do Teorema 2.1.3, RGe_i é um anel de cadeia. Falta provar apenas que se I é um ideal de RG , então existem ideais I_0, \dots, I_m de RGe_0, \dots, RGe_m respectivamente, tais que $I = I_0 + \dots + I_m$. De fato, seja I um ideal próprio não nulo de RG . Como RG é finito, então I é finito. Podemos listar os elementos de I na forma $I = \{\alpha_1, \dots, \alpha_k\}$. Como $\{e_0, \dots, e_m\}$ é um conjunto de idempotentes ortogonais primitivos, com $1 = e_0 + \dots + e_m$, temos :

$$\begin{aligned} \alpha_1 &= \alpha_{10}e_0 + \dots + \alpha_{1m}e_m \\ &\vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \\ \alpha_k &= \alpha_{k0}e_0 + \dots + \alpha_{km}e_m \end{aligned}$$

Como RGe_0 é um anel de cadeia, existe $j_0 \in \{1, \dots, k\}$ tal que $\langle \alpha_{i0}e_0 \rangle \subset \langle \alpha_{j_0 0}e_0 \rangle$, para todo $i \in \{1, \dots, k\}$. Pelo Teorema 2.1.3, existe k_0 tal que $\langle \alpha_{j_0 0}e_0 \rangle = \langle a^{k_0}e_0 \rangle$. De forma análoga, para cada índice ρ , $1 \leq \rho \leq m$, existe j_ρ tal que $\langle \alpha_{i\rho}e_\rho \rangle \subset \langle \alpha_{j_\rho \rho}e_\rho \rangle$. Novamente pelo Teorema 2.1.3, existe k_ρ tal que $\langle \alpha_{j_\rho \rho}e_\rho \rangle = \langle a^{k_\rho}e_\rho \rangle = I_\rho$. Assim, dado $\alpha_i \in I$,

$$\alpha_i = \alpha_{i0}e_0 + \dots + \alpha_{im}e_m \in \langle a^{k_0}e_0 \rangle \oplus \dots \oplus \langle a^{k_m}e_m \rangle = I_0 \oplus \dots \oplus I_m.$$

Portanto $I \subset I_0 \oplus \dots \oplus I_m$. Segue imediatamente que $I_0 \oplus \dots \oplus I_j \subset I$. ■

A seguir, iremos demonstrar um resultado que será necessário mais adiante.

Lema 2.1.6 *Seja R um anel local com ideal maximal $M = \langle a \rangle$ e t o índice de nilpotência de a . Então $x \cdot a^{t-k} = 0$ se, e somente se, $x \in \langle a^k \rangle$, onde $x \in R$ e $0 < k < t$.*

Prova:

Como x não é inversível, temos que $x \in \langle a \rangle$. Seja $r < k$ o maior índice tal que $x \in \langle a^r \rangle$. Assim, $x = x_1 \cdot a^r$. Mostremos que x_1 é inversível. De fato, se x_1 não é inversível, então $x_1 \in \langle a \rangle$ e assim, $x \in \langle a^{r+1} \rangle$, o que é uma contradição. Como $x \cdot a^{t-k} = 0$, temos que $x_1 \cdot a^{t-k+r} = 0$, onde $t - k + r < t$. Como x_1 é inversível, temos que $a^{t-k+r} = 0$, o que contradiz o índice de nilpotência de a . Portanto, $x \in \langle a^k \rangle$. ■

Já vimos no capítulo anterior que

$$RG = RGe_0 \oplus \dots \oplus RGe_m \simeq \frac{R[x]}{(x^n - 1)} \simeq \frac{R[x]}{(f_0)} \oplus \dots \oplus \frac{R[x]}{(f_m)},$$

onde, reordenando as parcelas se necessário, temos $RGe_i \simeq \frac{R[x]}{(f_i)}$. Portanto, $|RGe_i| = |R|^{w_i}$, onde $w_i = \text{grau}(f_i)$.

Teorema 2.1.7 *Seja C um código cíclico da forma $C = \langle a^{k_{i_1}} e_{i_1} \rangle \oplus \dots \oplus \langle a^{k_{i_r}} e_{i_r} \rangle$. Então, o*

número de palavras de C é $|C| = |\overline{R}| \sum_{s=1}^r (t - k_{i_s}) w_{i_s}$.

Prova: Como C é uma soma direta, temos $|C| = |\langle a^{k_{i_1}} e_{i_1} \rangle| \dots |\langle a^{k_{i_r}} e_{i_r} \rangle|$. Devemos então determinar $|\langle a^{k_i} e_i \rangle|$.

Considere

$$\begin{aligned} \psi : RG &\rightarrow RGa^k. \\ \alpha &\mapsto \alpha a^k \end{aligned} \tag{2.1}$$

Claramente ψ é um epimorfismo de grupos aditivos. O núcleo de ψ é dado por

$$\ker(\psi) = \{\alpha \in RG; \alpha a^k = 0\}.$$

Pelo Lema 2.1.6, temos $\alpha a^k = 0$ se, e somente se, $\alpha \in \langle a^{t-k} \rangle G$. Portanto,

$$RGa^k \simeq \frac{RG}{\langle a^{t-k} \rangle G}.$$

Como $\frac{RG}{\langle a^{t-k} \rangle G} \simeq \left(\frac{R}{\langle a^{t-k} \rangle} \right) G$, temos,

$$|RGa^{k_i} e_i| = \left| \left(\frac{R}{\langle a^{t-k_i} \rangle} \right) G e_i \right| = \left| \frac{R}{\langle a^{t-k_i} \rangle} \right|^{w_i} = \left(\frac{|R|}{|\langle a^{t-k_i} \rangle|} \right)^{w_i} = |\bar{R}|^{(t-k_i)w_i}.$$

$$\text{Logo, } |C| = |\bar{R}|^{\sum_{s=1}^r (t - k_{i_s}) w_{i_s}}.$$

■

Seja $\{e_0, \dots, e_m\}$ o conjunto dos idempotentes primitivos de RG . No teorema a seguir, iremos calcular o número de todos os códigos cíclicos possíveis sobre um anel de cadeia.

Teorema 2.1.8 *Sejam R um anel de cadeia finito e comutativo, com ideal maximal $M = \langle a \rangle$, t o índice de nilpotência de a , com $|R| = q^k$ e $G = \langle g_0; g_0^n = 1 \rangle$, onde $q \nmid n$. Então o número de códigos cíclicos de comprimento n sobre R é $(t+1)^{m+1}$.*

Prova: Sabemos, do teorema anterior, que se I é um ideal de RG , então I é da forma $I = \langle a^{k_0} e_0 \rangle \oplus \dots \oplus \langle a^{k_m} e_m \rangle$, com $0 \leq k_j \leq t$.

Suponhamos $\langle a^k e_i \rangle = \langle a^l e_i \rangle$, com $k < l$. Assim, existe $\zeta \in RG$ tal que $a^k e_i = a^l e_i \zeta$. Multiplicando por a^{t-l} em ambos os lados temos $a^{k+t-l} e_i = 0$. Como $k < l$, temos que $k + t - l < t$ e, portanto, $a^{k+t-l} \neq 0$. Pelo Lema 2.1.6, $e_i \in MG$. Como MG é nilpotente, existe m tal que $e_i^m = 0$. Como $e_i^2 = e_i$, temos $e_i = 0$, o que é uma contradição. Logo, $k = l$. Assim, para cada par de índice diferentes, teremos códigos diferentes, portanto o número de

códigos será $(t + 1)^{m+1}$.

■

Teorema 2.1.9 *Para RG nas mesmas condições do Teorema 2.1.8, temos que RG é um anel de ideais principais.*

Prova: Seja I um ideal de RG . Então, pelo Teorema 2.1.5, $I = \langle a^{k_0} e_0 \rangle + \dots + \langle a^{k_m} e_m \rangle$.

É claro que $\langle a^{k_0} e_0 + \dots + a^{k_m} e_m \rangle \subset \langle a^{k_0} e_0 \rangle + \dots + \langle a^{k_m} e_m \rangle$. Provemos então que $\langle a^{k_i} e_i \rangle \subset \langle a^{k_0} e_0 + \dots + a^{k_m} e_m \rangle$. Seja $x \in \langle a^{k_i} e_i \rangle$, temos então que $x = \alpha a^{k_i} e_i$, onde $\alpha \in RG$. Como $e_i \cdot e_k = 0$, para $i \neq k$ e $e_i^2 = e_i$, temos $x = \alpha a^{k_i} e_i = \alpha e_i (a^{k_0} e_0 + \dots + a^{k_m} e_m)$.

Assim, $\langle a^{k_i} e_i \rangle \subset \langle a^{k_0} e_0 + \dots + a^{k_m} e_m \rangle$ e, portanto,

$$\langle a^{k_0} e_0 \rangle + \dots + \langle a^{k_m} e_m \rangle = \langle a^{k_0} e_0 + \dots + a^{k_m} e_m \rangle.$$

Logo RG é um anel de ideais principais.

■

2.2 Códigos duais e auto duais

Como vimos no capítulo anterior, os códigos duais de códigos cíclicos também são códigos cíclicos e nesta seção caracterizaremos os códigos duais de um dado código e os códigos auto duais.

Sejam $\{e_0, e_1, \dots, e_m\}$ o conjunto dos idempotentes primitivos ortogonais de RG tal que

$$RG = RGe_0 \oplus RGe_1 \oplus \dots \oplus RGe_m.$$

Pelo Teorema 2.1.7 temos que $|RGe_i| = |R|^{w_i}$. Como $*$ denota a involução clássica, temos $|RGe_i| = |RGe_i^*|$.

Proposição 2.2.1 *Sejam $\alpha = a_0 + a_1g + \dots + a_{n-1}g^{n-1}$ e $\beta = b_0 + b_1g + \dots + b_{n-1}g^{n-1} \in RG$. Se $\alpha \cdot \beta^* = 0$, então α é ortogonal a β .*

Prova: Temos que $\beta^* = b_0 + b_{n-1}g + b_{n-2}g^2 + \dots + b_2g^{n-2} + b_1g^{n-1}$. Como $\alpha \cdot \beta^* = 0$, por 1.3.4, $(a_0, a_1, \dots, a_{n-1})$ é ortogonal a $(b_1, b_2, \dots, b_{n-1}, b_0)$ em R^n e todas as suas trocas cíclicas. Portanto, $(a_0, a_1, \dots, a_{n-1})$ é ortogonal a $(b_0, b_1, \dots, b_{n-1})$ e assim α é ortogonal a β .

■ O resultado a seguir será necessário nos próximos teoremas.

Proposição 2.2.2 *Seja $\{e_0, \dots, e_m\}$ o conjunto dos idempotentes ortogonais, primitivos de RG . Então $\{e_0^*, \dots, e_m^*\}$ é também o conjunto dos idempotentes ortogonais primitivos de RG .*

Prova: Como $*$: $RG \rightarrow RG$ é um isomorfismo, segue que

$$(i) \quad e_i^* \cdot e_i^* = e_i^*.$$

$$(ii) \quad e_i^* \cdot e_k^* = 0, \text{ se } i \neq k.$$

$$(iii) \quad 1 = e_0^* + \dots + e_m^*.$$

(iv) Cada e_i^* é primitivo.

Conseqüentemente, $\{e_0^*, \dots, e_m^*\}$ é o conjunto dos idempotentes primitivos de RG .

■

No próximo teorema iremos caracterizar o código dual a um dado código cíclico.

Teorema 2.2.3 *Se um código cíclico C é da forma $C = \langle a^{k_0}e_0 \rangle \oplus \dots \oplus \langle a^{k_m}e_m \rangle$, onde $0 \leq k_i \leq t$, então o código dual a C é da forma $C^\perp = \oplus \sum_{r=0}^m \langle a^{t-k_r}e_r^* \rangle$.*

Prova: Seja

$$\beta = \oplus \sum_{r=0}^m \langle a^{t-k_r}e_r^* \rangle.$$

Assim,

$$|\beta| = |\overline{R}| \left(\sum_{l=0}^m k_l w_l \right).$$

Como

$$a^{k_r} e_r \cdot (a^{t-k_s} e_s^*)^* = 0, \quad \forall 0 \leq r, s \leq m,$$

temos que $\beta \subset C^\perp$. Como $C = \langle a^{k_0} e_0 \rangle \oplus \dots \oplus \langle a^{k_m} e_m \rangle$, temos que

$$|C| = |\bar{R}| \sum_{l=0}^m (t - k_l) w_l.$$

Suponha $|\bar{R}| = q^\alpha$. Assim, $|R| = q^{\alpha t}$.

Pelo Lema 1.2.16, temos $|C^\perp| = q^l$, onde

$$\begin{aligned} l &= \alpha t n - \alpha \left(\sum_{l=0}^m (t - k_l) w_l \right) \\ &= \alpha t n - \alpha \sum_{l=0}^m (t w_l) + \alpha \sum_{l=0}^m k_l w_l \\ &= \alpha t \left(n - \sum_{l=0}^m w_l \right) + \alpha \sum_{l=0}^m k_l w_l \\ &= \alpha \left(\sum_{l=0}^m k_l w_l \right). \end{aligned}$$

Portanto, $|C^\perp| = |\beta|$ e assim $C^\perp = \beta$. ■

Definição 2.2.4 Um código C é chamado **auto ortogonal** se $C \subset C^\perp$ e **auto-dual** se $C = C^\perp$.

Nos teoremas a seguir, abordaremos os códigos auto-duais.

Agora seja $C = \langle a^{k_0} e_0 \rangle \oplus \dots \oplus \langle a^{k_m} e_m \rangle$.

Reordenando as parcelas se necessário, podemos escrever C na forma

$$C = \langle a^{r_0} e_{k_{0s_0}} \rangle \oplus \dots \oplus \langle a^{r_0} e_{k_{0s_0}} \rangle \oplus \dots \oplus \langle a^{r_l} e_{k_{ls_1}} \rangle \oplus \dots \oplus \langle a^{r_l} e_{k_{ls_1}} \rangle, \quad (2.2)$$

com $0 \leq r_0 < r_1 < \dots < r_l \leq t$.

Sejam

$$\begin{aligned} f_0 &= e_{k_{01}} + \dots + e_{k_{0s_0}} \\ f_1 &= e_{k_{11}} + \dots + e_{k_{1s_1}} \\ &\vdots \\ f_l &= e_{k_{l1}} + \dots + e_{k_{ls_l}}. \end{aligned}$$

Temos $1 = f_0 + \dots + f_l$. Além disso, f_i e f_k são idempotentes ortogonais, para $i \neq k$. Assim,

$$C = \langle a^{r_0} f_0 \rangle \oplus \dots \oplus \langle a^{r_l} f_l \rangle.$$

Usando o Teorema 2.2.3 para o código descrito em 2.2, temos

$$C^\perp = \langle a^{t-r_l} f_l^* \rangle \oplus \dots \oplus \langle a^{t-r_0} f_0^* \rangle. \quad (2.3)$$

Definição 2.2.5 Para um anel de cadeia R , com ideal maximal $M = \langle a \rangle$, onde t o índice de nilpotência de a é par, o código $C = \langle a^{\frac{t}{2}} \rangle$ é chamado **código auto-dual trivial**.

Proposição 2.2.6 Seja $C = \langle a^{r_0} f_0 \rangle \oplus \dots \oplus \langle a^{r_l} f_l \rangle$ um código cíclico. Então C é auto-dual se, e somente se, para cada par de índices i, j tais que $i + j \equiv 0 \pmod{l}$ tem-se que $r_i + r_j = t$ e $f_i = f_j^*$.

Prova: Por 2.3, temos

$$C^\perp = \langle a^{t-r_l} f_l^* \rangle \oplus \dots \oplus \langle a^{t-r_0} f_0^* \rangle.$$

Note que o menor expoente de a em C^\perp é $t - r_l$. Assim, se $C = C^\perp$ temos que $r_0 = t - r_l$, donde $r_0 + r_l = t$ e $f_0 = f_l^*$.

Da mesma forma, se $i + j \equiv 0 \pmod{l}$, deve-se ter $r_i = t - r_j$, donde $r_i + r_j = t$ e $f_i = f_j^*$.

Reciprocamente, se valem estas condições, é fácil ver que $C = C^\perp$.

■

Observação 2.2.7 Em [10], a notação usada por Dinh e López-Permouth exclui vários casos de códigos cíclicos auto-duais, pois usam a notação $C = \langle \widehat{F}_1, a\widehat{F}_2, \dots, a^{t-1}\widehat{F}_t \rangle$ para o

código, onde $x^n - 1 = F_0 F_1 \dots F_l$. Aqui, enunciamos e provamos os teoremas para C da forma $\langle a^{r_0} f_0 \rangle \oplus \dots \oplus \langle a^{r_l} f_l \rangle$, onde a única imposição sobre os expoentes r_i 's de a é que $0 \leq r_0 < r_1 < \dots < r_l \leq t$, o que ocorre para todos os possíveis ideais. Entraremos em mais detalhes no Capítulo 5.

Teorema 2.2.8 *Suponha que t é um inteiro par. Então códigos cíclicos auto-duais diferentes do auto-dual trivial existem se, e somente se, existe um idempotente $e_i \in RG$, tal que $e_i \neq e_i^*$.*

Prova: Vamos supor que $C = C^\perp$ é não trivial e que $e_i = e_i^*$, para todo índice $0 \leq i \leq l$. Reordenando os idempotentes, temos

$$C = \langle a^{r_0} f_0 \rangle \oplus \dots \oplus \langle a^{r_l} f_l \rangle = \langle a^{t-r_0} f_0^* \rangle \oplus \dots \oplus \langle a^{t-r_l} f_l^* \rangle = \langle a^{t-r_0} f_0 \rangle \oplus \dots \oplus \langle a^{t-r_l} f_l \rangle .$$

Logo, $r_i = t - r_i$, para todo $0 \leq i \leq l$ e assim, $r_i = \frac{t}{2}$. Portanto, $C = \langle a^{\frac{t}{2}}(f_0 + \dots + f_l) \rangle = \langle a^{\frac{t}{2}} \rangle$, o que é uma contradição.

Reciprocamente, seja $e \in RG$ tal que $e \neq e^*$. Então e^* é também um idempotente primitivo e podemos escrever $1 = e + e^* + e_3 + \dots + e_m$. Denotemos $\beta = e_3 + \dots + e_m$. Assim, $1 = e + e^* + \beta$. Por outro lado, $1 = (e + e^* + \beta)^* = e^* + e + \beta^*$. Logo, $\beta = \beta^*$.

Considere

$$C = \langle a^{\frac{t}{2}+1} e \rangle \oplus \langle a^{\frac{t}{2}-1} e^* \rangle \oplus \langle a^{\frac{t}{2}} \beta \rangle .$$

Pelo Teorema 2.2.3 $C^\perp = \langle a^{t-(\frac{t}{2}+1)} e^* \rangle \oplus \langle a^{t-(\frac{t}{2}-1)} e^{**} \rangle \oplus \langle a^{\frac{t}{2}} \beta^* \rangle = C$.

■

Teorema 2.2.9 *Sejam R anel de cadeia finito com ideal maximal $\langle a \rangle$, $|R| = q^{lt}$, onde $|\overline{R}| = q^l$ e t o índice de nilpotência de a e seja G um grupo cíclico de ordem n , onde $q \nmid n$. Se t é par, então códigos cíclicos auto-duais não triviais sobre R existem se, e somente se, $q^i \not\equiv -1 \pmod{n}$ para todo inteiro positivo i .*

Prova: Sabemos por 1.1 que um idempotente primitivo é da forma

$$e_s = \frac{1}{n} \sum_{i=0}^{n-1} \sum_{j \in C_s} \alpha^{-ij} g^i.$$

Assim,

$$e_s^* = \frac{1}{n} \sum_{i=0}^{n-1} \sum_{j \in C_s} \alpha^{ij} g^i = \frac{1}{n} \sum_{i=0}^{n-1} \sum_{j \in C_{n-s}} \alpha^{-ij} g^i.$$

Pelo Teorema 2.2.8, códigos auto-duais não triviais existem se, e somente se, existe um idempotente e_k , tal que $e_k \neq e_k^*$. Agora, para todo idempotente e_k , $e_k = e_k^*$ se, e somente se, $C_s = C_{n-s}$. Portanto, para todo $0 \leq s \leq m$, $\Omega_s = \Omega_{n-s}$, onde Ω_s denota a q classe ciclotômica contendo s . Isto acontece se, e somente se, existe i tal que $q^i s \equiv (n-s) \pmod{n}$ para todo $0 \leq s \leq m$, ou equivalentemente $q^i \equiv -1 \pmod{n}$. ■

Corolário 2.2.10 *Se n é um número primo, então códigos cíclicos auto-duais de comprimento n não existem nos seguintes casos:*

- $q = 2, n \equiv 3, 5 \pmod{8}$;
- $q = 3, n \equiv 5, 7 \pmod{12}$;
- $q = 5, n \equiv 3, 7, 13, 17 \pmod{20}$;
- $q = 7, n \equiv 5, 11, 13, 15, 17, 23 \pmod{28}$;
- $q = 11, n \equiv 3, 13, 15, 17, 21, 23, 27, 29, 31, 41 \pmod{44}$

Prova: Segue do Teorema 2.2.9, Observação 1.4.4 e Proposição 1.4.9. ■

Corolário 2.2.11 *Seja n um primo ímpar diferente de q , e q um não resíduo quadrático de n^k , onde $k \geq 1$. Então códigos cíclicos auto-duais de comprimento n não existem.*

Prova: Segue dos Teorema 2.2.9, Observação 1.4.4 e Proposição 1.4.10. ■

Corolário 2.2.12 *Se n é um primo ímpar, então códigos cíclicos auto-duais de comprimento n não existem nos seguintes casos:*

- $q \equiv 1 \pmod{4}$ e existe um inteiro k tal que $\text{mdc}(q, 4n^k) = 1$ e q é um não resíduo quadrático de $4n^k$;
- $q \equiv 1 \pmod{8}$ e existem inteiros positivos i, j tais que $i > 2$, $\text{mdc}(q, 2^i n^j) = 1$ e q é um não resíduo quadrático de $2^i n^j$.

Prova: Segue do Teorema 2.2.9, Observação 1.4.4 e Proposição 1.4.11. ■

CAPÍTULO 3

Códigos de Comprimento p^n sobre Anéis de Cadeia

Neste capítulo vamos considerar o caso particular de códigos cíclicos de comprimento p^n , com p primo, sobre um anel de cadeia R , com ideal maximal $M = \langle a \rangle$ tal que $|\overline{R}| = q^l$, com $o(|\overline{R}|) = \phi(p^n)$ em $U(\mathbb{Z}_{p^n})$ e $q \nmid p^n$. Neste caso, Ferraz e Polcino Milies em [15] provaram que os idempotentes primitivos de $\overline{R}G$ dependem unicamente da estrutura de subgrupos de C_{p^n} e deram sua fórmula explícita.

Para um grupo cíclico G de ordem p^n , o reticulado de subgrupos de G formam uma cadeia:

$$G = G_0 \supset G_1 \supset \dots \supset G_n = 1.$$

Neste caso, os elementos

$$e_0 = \widehat{G} \quad \text{e} \quad e_i = \widehat{G}_i - \widehat{G}_{i-1}, \text{ para } 1 \leq i \leq n,$$

formam o conjunto dos idempotentes ortogonais tal que

$$e_0 + e_1 + \dots + e_n = 1.$$

Se $|\overline{R}| = q$ e $o(q) = \varphi(p^n)$ em $U(\mathbb{Z}_{p^n})$, onde ϕ denota a função de Euler, temos o seguinte.

Teorema 3.0.13 ([15], Teorema 3.1) *Seja F um corpo com q elementos e G um grupo cíclico de ordem p^n tal que $o(q) = \phi(p^n)$ em $U(\mathbb{Z}_{p^n})$. Seja*

$$G = G_0 \supset G_1 \supset \dots \supset G_n = \{1\}$$

a cadeia descendente de todos os subgrupos de G . Então o conjunto dos idempotentes primitivos de FG é dado por

$$\bar{e}_0 = \frac{1}{p^n} \left(\sum_{g \in G} g \right) \quad e \quad \bar{e}_i = \widehat{G}_i - \widehat{G}_{i-1}, \quad 1 \leq i \leq n.$$

A seguir, iremos estabelecer uma hipótese central que consideraremos ao longo do capítulo.

Hipótese A

Sejam R anel de cadeia finito, comutativo com unidade, tal que $|R| = q^k$, $M = \langle a \rangle$ o ideal maximal de R , $|\overline{R}| = q^l$, com $k = lt$, onde t é o índice de nilpotência de a e G um grupo cíclico de ordem p^n com gerador g_0 , tal que $o(|\overline{R}|) = \phi(p^n)$ em $U(\mathbb{Z}_{p^n})$, $G_i = \langle g_0^{p^i} \rangle$ e $e_i = \widehat{G}_i - \widehat{G}_{i-1}$.

Daqui em diante, estaremos sempre nas condições da *Hipótese A*.

Pelo Teorema 3.0.13, $\bar{e}_0 = \widehat{G}$, $\bar{e}_i = \widehat{G}_i - \widehat{G}_{i-1}$ formam o conjunto dos idempotentes primitivos ortogonais de $(\frac{R}{\langle a \rangle})G$. Pelo levantamento, $e_0 = \widehat{G}$ e $e_i = \widehat{G}_i - \widehat{G}_{i-1}$ formam o conjunto dos idempotentes primitivos ortogonais de RG .

Para este conjunto de idempotentes primitivos, o próximo teorema exibe uma fórmula do número de elementos nos códigos da forma $I = \langle a^{k_0} e_0 \rangle \oplus \dots \oplus \langle a^{k_n} e_n \rangle$.

Teorema 3.0.14 *Para R e G nas condições da Hipótese A, se I é um ideal de RG da forma $I = \langle a^{k_0} e_0 \rangle \oplus \dots \oplus \langle a^{k_m} e_m \rangle$, com $0 \leq k_i \leq t$, então*

$$|I| = |\overline{R}| \left[\sum_{j=1}^m (t - k_j)(p^j - p^{j-1}) + (t - k_0) \right].$$

Prova: Como C é uma soma direta, temos $|C| = |\langle a^{k_0} e_0 \rangle| \dots |\langle a^{k_m} e_m \rangle|$. Devemos então determinar $|\langle a^{k_i} e_i \rangle|$. Seja $i > 0$, temos que $a^{k_i} e_i = a^{k_i} \widehat{G}_i - a^{k_i} \widehat{G}_{i-1}$, com $e_i + \widehat{G}_{i-1} = \widehat{G}_i$ e $e_i \cdot \widehat{G}_{i-1} = (\widehat{G}_i - \widehat{G}_{i-1}) \cdot \widehat{G}_{i-1} = 0$. Logo

$$RGa^{k_i} \widehat{G}_i = RGa^{k_i} e_i \oplus RGa^{k_i} \widehat{G}_{i-1}.$$

$$\text{Assim, } |RGa^{k_i} e_i| = \frac{|RGa^{k_i} \widehat{G}_i|}{|RGa^{k_i} \widehat{G}_{i-1}|}.$$

Considere

$$\begin{aligned} \psi : RG &\rightarrow RGa^{k_i}. \\ \alpha &\mapsto \alpha a^{k_i} \end{aligned} \tag{3.1}$$

Claramente ψ é um epimorfismo de grupos aditivos. O núcleo de ψ é dado por

$$\ker(\psi) = \{\alpha \in RG; \alpha a^{k_i} = 0\}.$$

Pelo Lema 2.1.6, temos $\alpha a^{k_i} = 0$ se, e somente se, $\alpha \in \langle a^{t-k_i} \rangle G$. Portanto,

$$RGa^{k_i} \simeq \frac{RG}{\langle a^{t-k_i} \rangle G}.$$

Como $RG / \langle a^{t-k_i} \rangle G \simeq (R / \langle a^{t-k_i} \rangle)G$, temos

$$|RGa^{k_i}\widehat{G}_i| = \left| \left(\frac{R}{\langle a^{t-k_i} \rangle} \right) G\widehat{G}_i \right|.$$

Denotemos $R / \langle a^{t-k_i} \rangle$ por \overline{R}_{k_i} . Lembremos que $|\overline{R}_{k_i}| = \frac{|\overline{R}|^t}{|\overline{R}|^{k_i}}$.

Pelo Teorema 1.1.32, $\overline{R}_{k_i}G\widehat{G}_i \simeq \overline{R}_{k_i}(\frac{G}{G_i})$. Portanto, $|\overline{R}_{k_i}G\widehat{G}_i| = |\overline{R}_{k_i}|^{\frac{|G|}{|G_i|}} = |\overline{R}_{k_i}|^{p^i}$. De forma análoga, $|RGa^{k_i}\widehat{G}_{i-1}| = |\overline{R}_{k_i}|^{p^{i-1}}$. Logo,

$$|RGa^{k_i}e_i| = \left(\frac{|\overline{R}|^t}{|\overline{R}|^{k_i}} \right)^{p^i - p^{i-1}} = |\overline{R}|^{(t-k_i)(p^i - p^{i-1})}.$$

Para finalizar, calculemos $|\langle a^{k_0}e_0 \rangle|$. Pelo Lema 3.1, temos

$$|RGa^{k_0}e_0| = \left| \left(\frac{R}{\langle a^{t-k_0} \rangle} \right) G\widehat{G} \right|.$$

Logo,

$$|RGa^{k_0}e_0| = \left(\frac{|R|}{|\langle a^{t-k_0} \rangle|} \right)^{\frac{|G|}{|G|}} = \frac{|\overline{R}|^t}{|\overline{R}|^{k_0}} = |\overline{R}|^{(t-k_0)}.$$

Portanto, $|I| = |\overline{R}|^{\sum_{j=1}^m (t-k_j)(p^j - p^{j-1}) + (t-k_0)}$.

■

Tão importante quanto descrever todos os possíveis códigos cíclicos é saber o seu peso mínimo. Nos teoremas que seguem, determinaremos o peso mínimo de todos os códigos cíclicos nas condições das hipóteses anteriores. Os resultados seguintes são uma generalização de resultados semelhantes obtidos por F. Mello [23] para corpos, à situação que estamos considerando.

Teorema 3.0.15 *Considere R e G nas condições da Hipótese A. Então $w((RG)a^k e_i) = 2 |G_i|$, para $i \neq 0$ e $w((RG)a^k e_0) = |G|$, para $0 \leq k \leq t-1$.*

Prova:

Para $i \neq 0$, temos $e_i \widehat{G}_i = (\widehat{G}_i - \widehat{G}_{i-1})\widehat{G}_i = \widehat{G}_i - \widehat{G}_{i-1} = e_i$. Logo, $(RG)e_i \subset (RG)\widehat{G}_i$. Seja Γ um transversal de G_i em G . Um elemento arbitrário $\alpha \in RG$ pode ser escrito na forma $\alpha = (\sum_{h \in \Gamma} \alpha_h h)$, com $\alpha_h \in RG_i$. Portanto, qualquer palavra sobre $(RG)\widehat{G}_i$ é da forma $\alpha = (\sum_{h \in \Gamma} x_h h)\widehat{G}_i$, $x_h \in R$.

Como $(RG)a^k e_i \subset (RG)a^k \widehat{G}_i$ qualquer palavra de $(RG)a^k e_i$ também é da forma $\alpha = (\sum_{h \in \Gamma} x_h a^k h)\widehat{G}_i$, $x_h \in R$.

Analisemos assim uma palavra de $(RG)a^k e_i$. Se apenas um coeficiente $x_h a^k$ desta palavra é diferente de 0, para algum $h \in \Gamma$, teríamos $x_h a^k h \widehat{G}_i \in (RG)e_i$. Assim, existe $\beta \in RG$ tal que $x_h a^k h \widehat{G}_i = \beta a^k e_i$. Logo, $x_h a^k h \widehat{G}_i \widehat{G}_{i-1} = \beta a^k e_i \widehat{G}_{i-1}$. Como $e_i \widehat{G}_{i-1} = 0$, temos que $x_h a^k h \widehat{G}_{i-1} = 0$ e, assim, $x_h a^k = 0$. Logo, $x_h a^k h \widehat{G}_i = 0$, o que é uma contradição. Portanto, $w((RG)a^k e_i) \geq 2 | G_i |$.

Agora, considere $\alpha \in G_{i-1} \setminus G_i$. Temos $(1 - \alpha)a^k e_i \in (RG)a^k e_i$. Como

$$\begin{aligned} (1 - \alpha)a^k e_i &= (1 - \alpha)a^k(\widehat{G}_i - \widehat{G}_{i-1}) \\ &= (1 - \alpha)a^k \widehat{G}_i - (1 - \alpha)a^k \widehat{G}_{i-1} \\ &= (1 - \alpha)a^k \widehat{G}_i \end{aligned}$$

e $\text{supp}(a^k \widehat{G}_i) \cap \text{supp}(a^k \alpha \widehat{G}_i) = \emptyset$, temos que $w((RG)a^k e_i) \leq 2 | G_i |$. Portanto, $w((RG)a^k e_i) = 2 | G_i |$, para $i \neq 0$.

Consideremos agora o caso em que $i = 0$. Temos

$$\begin{aligned} R G a^k e_0 &= (R a^k)(G \widehat{G}) \\ &= (R a^k) \widehat{G} \\ &= \{r a^k (1 + g_0 + \dots + g_0^{p^n - 1}) | r \in R\} \end{aligned}$$

Assim, todos os elementos não nulos deste conjunto têm peso $p^n = | G |$.

■

O próximo teorema é um caso particular do resultado a seguir. Foi incluído apenas porque, nesta situação mais simples, é fácil ver a origem das ideias envolvidas.

Teorema 3.0.16 *Considere R e G nas condições da Hipótese A. Sejam $I_r = (RG)a^{k_r}e_r$, com $0 \leq k_r \leq t-1$. Considere $I_i \oplus I_j$, com $i < j$. Então $w(I_i \oplus I_j) = 2 \mid G_j \mid$ ou $\mid G_1 \mid$.*

Prova: Consideremos inicialmente o caso em que $i \neq 0$. Temos $G_j \subset G_i$. Seja $\alpha \in (I_i \oplus I_j)$. Assim, $\alpha = \alpha_i a^{k_1} e_i + \alpha_j a^{k_2} e_j$, onde $\alpha_i, \alpha_j \in RG$. Portanto,

$$\alpha \cdot \widehat{G}_j = \alpha_i a^{k_1} (\widehat{G}_i - \widehat{G}_{i-1}) \widehat{G}_j + \alpha_j a^{k_2} (\widehat{G}_j - \widehat{G}_{j-1}) \widehat{G}_j = \alpha.$$

Logo, $\alpha \in (RG)\widehat{G}_j$. Considere agora Γ_j um transversal de G_j em G . Assim, $\alpha = \left(\sum_{h \in \Gamma} x_h h \right) \widehat{G}_j$, onde $x_h \in R$. Suponhamos que apenas um coeficiente $x_h \neq 0$. Assim, $\alpha = x_h h \widehat{G}_j$. Como $e_i \cdot \widehat{G}_{i-1} = e_j \cdot \widehat{G}_{i-1} = 0$, temos que $\alpha \cdot \widehat{G}_{i-1} = x_h h \widehat{G}_j \cdot \widehat{G}_{i-1}$. Logo, $x_h h \widehat{G}_{i-1} = 0$ e, com isso, temos $x_h = 0$, o que é uma contradição. Portanto, $w(I_i \oplus I_j) \geq 2 \mid G_j \mid$. Como $w(I) \leq w(I_j) = 2 \mid G_j \mid$, temos que $w(I) = 2 \mid G_j \mid$.

Provemos agora, o caso em $i = 0$ e $1 < j$. Como $I_j \subset I_0 + I_j$, temos que $2 \mid G_j \mid = w(I_j) \geq w(I_0 + I_j)$.

Se $\alpha \in I_0 + I_j$, então $\alpha = \alpha_1 a^{k_1} \widehat{G} + \alpha_2 a^{k_2} (\widehat{G}_j - \widehat{G}_{j-1})$, onde $\alpha_1, \alpha_2 \in RG$. Assim, $\alpha \cdot \widehat{G}_j = \alpha$ e, portanto, $I_0 + I_j \subset (RG)\widehat{G}_j$.

Seja Γ um transversal de G_j em G . Assim, podemos escrever α como sendo $\alpha = \left(\sum_{h \in \Gamma} x_h h \right) \widehat{G}_j$. Suponhamos que apenas um coeficiente x_h seja diferente de zero. Assim, $\alpha = x_h h \widehat{G}_j = \alpha_1 a^{k_1} \widehat{G} + \alpha_2 a^{k_2} (\widehat{G}_j - \widehat{G}_{j-1})$.

Como $G_j \subset \widehat{G}_{j-1}$, temos que $\widehat{G}_j \cdot \widehat{G}_{j-1} = \widehat{G}_{j-1}$. Assim, $x_h h \widehat{G}_j \cdot \widehat{G}_{j-1} = \alpha_1 a^{k_1} \widehat{G} \widehat{G}_{j-1} + \alpha_2 a^{k_2} (\widehat{G}_j - \widehat{G}_{j-1}) \widehat{G}_{j-1}$, ou seja, $x_h h \widehat{G}_{j-1} = \alpha_1 a^{k_1} \widehat{G}$. Como $\alpha_1 = \sum r_g g$, podemos reescrever a última igualdade como $x_h h \widehat{G}_{j-1} = \sum r_g a^{k_1} \widehat{G}$. Desenvolvendo a equação anterior temos

$$\sum_{g \in \{hG_{j-1}\}} (x_h - \sum r_g a^{k_1}) g - \sum_{g \in \{G/hG_{j-1}\}} (\sum r_g a^{k_1}) g = 0.$$

Assim, $\sum r_g a^{k_1} = 0$ e daí $x_h = 0$, o que contradiz nossa hipótese inicial sobre x_h .

Concluimos assim que, para toda palavra $\alpha \in I_0 + I_j$, com $\alpha = (\sum_{h \in \Gamma} x_h h) \widehat{G}_j$, devem existir pelo menos dois coeficientes x_{h_0}, x_{h_1} , com $h_0, h_1 \in \Gamma$ diferentes de zero. Portanto, $w(I_0 + I_j) \geq 2 |G_j|$, e assim, $w(I_0 + I_j) = 2 |G_j|$.

Provemos agora o caso em que $i = 0$ e $j = 1$.

Seja $\alpha \in C$. Como $C = I_0 \oplus I_1$, existem $\beta_0, \beta_1 \in RG$, tais que $\alpha = \beta_0 a^{k_0} e_0 + \beta_1 a^{k_1} e_1$. Como $\alpha \cdot \widehat{G}_1 = \alpha$, temos $I \subset RG \widehat{G}_1$ e, assim, $w(I) \geq w(RG \widehat{G}_1) = |G_1|$.

Seja $k = \max\{k_0, k_1\}$. Temos

$$RG a^k \widehat{G}_1 = RG a^k \widehat{G} \oplus RG a^k (\widehat{G}_1 - \widehat{G}) \subset RG a^{k_0} e_0 \oplus RG a^{k_1} e_1 = I.$$

Logo $|G_1| = w(RG a^k \widehat{G}_1) \geq w(I)$. Portanto, $w(I) = |G_1|$.

■

Teorema 3.0.17 *Considere R e G nas condições da Hipótese A. Sejam $I_j = (RG) a^{k_j} e_j$, com $0 \leq k_j \leq t-1$ e $I = I_0 \oplus \dots \oplus I_j$, com $0 \leq j \leq n-1$. Então $w(I_0 \oplus I_1 \oplus \dots \oplus I_j) = |G_j|$.*

Prova: Seja $\alpha \in I$. Como $I = I_0 \oplus \dots \oplus I_j$, existem $\beta_0, \dots, \beta_j \in RG$ tais que $\alpha = \beta_0 a^{k_0} \widehat{G} + \dots + \beta_j a^{k_j} (\widehat{G}_j - \widehat{G}_{j-1})$. Como $G_j \subset G_i$, para $1 \leq i \leq j-1$, temos que $\widehat{G}_j \cdot e_i = e_i$, para $0 \leq i \leq j-1$ e assim, $\alpha \cdot \widehat{G}_j = \alpha$. Portanto, $I \subset (RG) \widehat{G}_j$ e $w(I) \geq w((RG) \widehat{G}_j) = |G_j|$.

Seja $k = \max\{k_0, \dots, k_j\}$. Logo,

$$(RG) a^k \widehat{G}_j \subset (RG) a^k \widehat{G} \oplus (RG) a^k (\widehat{G}_1 - \widehat{G}) \oplus \dots \oplus (RG) a^k (\widehat{G}_j - \widehat{G}_{j-1}) \subset I_0 \oplus I_1 \oplus \dots \oplus I_j.$$

Portanto, $|G_j| = w((RG) a^k \widehat{G}_j) \geq w(I)$. Logo, $w(I) = |G_j|$.

■

Teorema 3.0.18 *Considere R e G nas condições da Hipótese A. Sejam $I_j = (RG) a^{k_j} e_j$, com $0 \leq k_j \leq t-1$. Se $I = I_{j_1} \oplus \dots \oplus I_{j_l}$, $j_r < j_{r+1}$, para $1 \leq r \leq l$ com $\{j_1, \dots, j_l\} \subsetneq \{0, 1, \dots, j_l\}$, então $w(I) = 2 |G_{j_l}|$.*

Prova: Consideremos inicialmente

$$I = I_{j_1} \oplus \dots \oplus I_{j_l}, \text{ com } j_1 \neq 0 \text{ e } j_r < j_{r+1}, \text{ para } 1 \leq r \leq l.$$

Seja $\alpha \in I$. Como $I = I_{j_1} \oplus \dots \oplus I_{j_l}$, existem $\beta_{j_1}, \dots, \beta_{j_l}$, tais que

$$\alpha = \beta_{j_1} a^{k_{j_1}} (\widehat{G}_{j_1} - \widehat{G}_{j_1-1}) + \dots + \beta_{j_l} a^{k_{j_l}} (\widehat{G}_{j_l} - \widehat{G}_{j_l-1}).$$

Como $G_{j_i} \subset G_{j_i}$, para $1 \leq i \leq l-1$, temos $\widehat{G}_{j_i} \cdot e_{j_i} = e_{j_i}$, para $1 \leq i \leq l$. Assim, $\alpha G_{j_i} = \alpha$ e, portanto, $I \subset (RG)\widehat{G}_{j_i}$. Seja Γ um transversal de G_{j_i} em G . Assim, podemos escrever $\alpha = \left(\sum_{h \in \Gamma} x_h h \right) \widehat{G}_{j_i}$, $x_h \in R$. Suponhamos agora que apenas um x_{h_0} seja diferente de zero, para algum $h_0 \in \Gamma$. Assim,

$$\alpha = x_{h_0} h_0 \widehat{G}_{j_i} = \beta_{j_1} a^{k_{j_1}} (\widehat{G}_{j_1} - \widehat{G}_{j_1-1}) + \dots + \beta_{j_l} a^{k_{j_l}} (\widehat{G}_{j_l} - \widehat{G}_{j_l-1}).$$

Como $\widehat{G}_{j_i} \subset \widehat{G}_{j_i-1}$, para $1 \leq i \leq l$, temos que $\widehat{G}_{j_i} \cdot \widehat{G}_{j_i-1} = \widehat{G}_{j_i-1}$, para $1 \leq i \leq l$. Logo, $\widehat{G}_{j_i-1} \cdot e_{j_i} = 0$, para $1 \leq i \leq l$. Multiplicando ambos os lados da igualdade por \widehat{G}_{j_i-1} , temos $x_{h_0} h_0 \widehat{G}_{j_i-1} = 0$. A partir daí, temos $x_{h_0} = 0$, o que contradiz nossa escolha inicial de $x_{h_0} \neq 0$. Portanto, $w(I) \geq 2 |G_{j_i}|$.

Como $I_{j_i} \subset I$, temos $2 |G_{j_i}| = w(I_{j_i}) \geq w(I)$. Logo, $w(I) = 2 |G_{j_i}|$.

Agora considere

$$I = I_0 \oplus I_{j_1} \oplus \dots \oplus I_{j_l}, \text{ com } j_r < j_{r+1} \text{ para } 1 \leq r \leq l \text{ e } \{j_1, \dots, j_l\} \subsetneq \{1, \dots, j_l\}.$$

Como $I_{j_l} \subset I$, temos que $2 |G_{j_l}| = w(I_{j_l}) \geq w(I)$.

Seja $\alpha \in I$. Como $I = I_0 \oplus I_{j_1} \oplus \dots \oplus I_{j_l}$, existem $\beta_0, \beta_{j_1}, \dots, \beta_{j_l} \in RG$ tais que $\alpha = \beta_0 a^{k_0} \widehat{G} + \beta_{j_1} a^{k_{j_1}} (\widehat{G}_{j_1} - \widehat{G}_{j_1-1}) + \dots + \beta_{j_l} a^{k_{j_l}} (\widehat{G}_{j_l} - \widehat{G}_{j_l-1})$. Assim, $\alpha \cdot \widehat{G}_{j_l} = \alpha$. Logo, $I \subset (RG)\widehat{G}_{j_l}$.

Seja Γ um transversal de G_{j_i} em G . Assim, podemos escrever $\alpha = \left(\sum_{h \in \Gamma} x_h h\right) \widehat{G}_{j_i}$, onde $x_h \in R$. Suponha que exista apenas um $h_0 \in \Gamma$ tal que $x_{h_0} \neq 0$. Assim,

$$\alpha = x_{h_0} t_0 \widehat{G}_{j_i} = \beta_0 a^{k_0} \widehat{G} + \beta_{j_1} a^{k_{j_1}} (\widehat{G}_{j_1} - \widehat{G}_{j_1-1}) + \dots + \beta_{j_i} a^{k_{j_i}} (\widehat{G}_{j_i} - \widehat{G}_{j_i-1}).$$

Como $\{j_1, \dots, j_i\} \subsetneq \{1, \dots, j_i\}$, existe $r \in \{1, \dots, j_i\}$, tal que $r \notin \{j_1, \dots, j_i\}$. Tome r como sendo o menor índice pertencente à $\{1, \dots, j_i\}$ e que não pertence à $\{j_1, \dots, j_i\}$.

Multiplicando ambos os lados da igualdade acima por \widehat{G}_r , temos

$$x_{h_0} h_0 \widehat{G}_r = \beta_0 a^{k_0} \widehat{G} + \beta_1 a^{k_1} (e_1) + \dots + \beta_{r-1} a^{k_{r-1}} (e_{r-1}).$$

Portanto, $\alpha \widehat{G}_r$ pertence ao código C' gerado por

$$\langle a^{k_0} \widehat{G} \rangle \oplus \langle a^{k_1} (e_1) \rangle \oplus \dots \oplus \langle a^{k_{r-1}} (e_{r-1}) \rangle.$$

Mas o peso de $\alpha \widehat{G}_r$ é dado por $w(\alpha \widehat{G}_r) = |G_r|$ e peso de C' é $w(C') = |G_{r-1}|$. Como $G_r \subset G_{r-1}$, temos que $|G_r| < |G_{r-1}|$, o que é uma contradição. Logo, $w(C) \geq 2 |G_{j_i}|$ e assim $w(C) = 2 |G_{j_i}|$.

■

3.1 Códigos que são livres como R -submódulos de RG

Agora iremos caracterizar todos os códigos cíclicos de comprimento p^n que são R -submódulos livres de RG . Para isso, lembremos os seguintes resultados.

Teorema 3.1.1 ([18], Teorema 3.10) *Um módulo M é projetivo se, e somente se, M é um somando direto de um módulo livre.*

Teorema 3.1.2 ([18], Teorema 7.5) *Se R é um anel local, então todo módulo projetivo finitamente gerado sobre R é livre.*

Como estamos trabalhando com módulos finitos, eles são finitamente gerados e assim qualquer módulo que for um somando de um módulo livre é projetivo e, portanto, livre.

O próximo resultado é semelhante a Proposição 2.1 provado por Dutra, Ferraz e Polcino Milies em [13] para algebras de grupo sobre corpos. Exibiremos uma base para RGe_i , provando assim que RGe_i é um código livre. Mais adiante exibiremos outra base para RGe_i .

Teorema 3.1.3 *Considere R e G nas condições da Hipótese A. Seja γ um transversal de G_{i-1} em G e τ um transversal de G_i em G_{i-1} . Então*

$$\mathcal{B} = \{c(1-h)\widehat{G}_i \mid c \in \gamma, h \in \tau \setminus \{1\}\}$$

é uma base de RGe_i sobre R .

Prova: Primeiramente provaremos que os elementos de \mathcal{B} pertencem a RGe_i . Para isso, observe que:

1. Para $h \in \tau \setminus \{1\}$, temos $(1-h)\widehat{G}_{i-1} = 0$, pois $h\widehat{G}_{i-1} = \widehat{G}_{i-1}$.
2. Para $c \in \gamma$ e $h \in \tau \setminus \{1\}$, temos $c(1-h)\widehat{G}_i = c(1-h)\widehat{G}_i(\widehat{G}_i - \widehat{G}_{i-1}) = c(1-h)\widehat{G}_i e_i \in RGe_i$.

Mostremos agora que os elementos de \mathcal{B} são linearmente independentes. Sejam $x_{ch} \in R$ tais que $0 = \sum_{c,h} x_{ch}(c(1-h)\widehat{G}_i)$.

$$0 = \sum_{c,h} x_{ch}(c(1-h)\widehat{G}_i) = \sum_c \left(\sum_h x_{ch} \right) c\widehat{G}_i - \sum_{c,h} x_{ch} ch\widehat{G}_i.$$

Agora observe que, para c, h fixados, temos que o elemento $ch\widehat{G}_i$ tem suporte disjunto de qualquer outro elemento nesta combinação linear. De fato, como τ é um transversal de G_i em G_{i-1} e $h \in \tau \setminus \{1\}$, temos que \widehat{G}_i e $h\widehat{G}_i$ têm suportes disjuntos. Como γ é um transversal de G_{i-1} em G $c \in \gamma$, temos que $c\widehat{G}_i$ e $ch\widehat{G}_i$ também têm suportes disjuntos. É

claro que se $c_j \neq c_k \in \gamma$, então $c_j \widehat{G}_i$ e $c_k \widehat{G}_i$ têm suportes disjuntos. Como $\{ch, c \in \gamma \text{ e } h \in \tau\}$ formam um transversal de G_i em G , temos que $c_j h_j \widehat{G}_i$ e $c_k h_k \widehat{G}_i$ têm suporte disjuntos, para $c_j \neq c_k$ ou $h_j \neq h_k$. Portanto, $x_{ch} = 0$, para todo $c \in \gamma$ e $h \in \tau$. Devemos provar que o módulo livre sobre R gerado por \mathcal{B} é igual ao ideal gerado por e_i . Já provamos que todo elemento de \mathcal{B} pertence a RGe_i . Provemos agora que os dois conjuntos têm o mesmo número de elementos. Pelo Teorema 3.0.14, $|RGe_i| = |\overline{R}|^{t(p^i - p^{i-1})} = |R|^{(p^i - p^{i-1})}$. Por outro lado, o número de elementos gerado pelo módulo livre sobre R cuja base é \mathcal{B} é dado por $|R|^{|\gamma|(|\tau|-1)} = |R|^{\left|\frac{G}{G_{i-1}}\right| \left(\left|\frac{G_{i-1}}{G_i}\right|-1\right)} = |R|^{p^i - p^{i-1}}$. Portanto, RGe_i é livre e \mathcal{B} é uma base de RGe_i . ■

Corolário 3.1.4 *O posto do código livre RGe_i é $p^i - p^{i-1}$.*

Observe que o ideal gerado por $a^k e_i$ não pode ser livre, pois $(a^{t-k} \alpha) \cdot (a^k e_i) = 0$, para qualquer $\alpha \in RGe_i$.

Pelos Teoremas 3.1.1, 3.1.2 e 3.1.3, temos o seguinte corolário.

Corolário 3.1.5 *Seja G um grupo cíclico de ordem p^n e R um anel de cadeia com $|R| = q^k$, onde $q \nmid p^n$. Seja $e_i = \widehat{G}_i - \widehat{G}_{i-1}$. Então os possíveis códigos cíclicos livres de comprimento p^n são da forma*

$$C = RGe_{i_1} \oplus \dots \oplus RGe_{i_k}.$$

Corolário 3.1.6 *Seja G um grupo cíclico de ordem p^n e R um anel de cadeia com $|R| = q^k$, onde $q \nmid p^n$. O número de códigos cíclicos livres de comprimento p^n sobre um anel de cadeia R é 2^{n+1} .*

Pelo Corolário 3.1.4, $\text{posto}(RGe_i) = p^i - p^{i-1}$. Adiante exibiremos outra base para RGe_i , para a qual será necessária a seguinte proposição.

Proposição 3.1.7 ([18], Proposição 7.18) *Seja M um módulo livre sobre um anel comutativo de posto n . Então qualquer conjunto gerador de n elementos é uma base de M .*

Teorema 3.1.8 *Seja $G = \langle g | g^{p^n} = 1 \rangle$. O conjunto $\mathcal{B} = \{e_i, ge_i, g^2e_i, \dots, g^{p^i - p^{i-1} - 1}e_i\}$ é uma base de RGe_i .*

Prova: Como o número de elementos de \mathcal{B} é $p^i - p^{i-1}$, pela Proposição 3.1.7 basta provar que \mathcal{B} gera RGe_i . Como um elemento de RGe_i é dado por $r_0e_i + r_1ge_i + \dots + r_{p^n-1}g^{p^n-1}e_i$, devemos provar então que os elementos da forma $r_l g^l e_i$, onde $p^i - p^{i-1} \leq l \leq p^n - 1$, são combinações lineares de elementos de \mathcal{B} . Observe porém que $g^{p^i} \cdot e_i = e_i$, pois

$$g^{p^i} e_i = g^{p^i} \widehat{G}_i - g^{p^i} \widehat{G}_{i-1} = \widehat{G}_i - \widehat{G}_{i-1}.$$

Logo, $g^{p^i+k}e_i = g^k e_i$, $0 \leq k \leq p^n - p^i + p^{i+1} - 1$, donde um elemento $\alpha \in RGe_i$ é da forma $\alpha = \sum_{j=0}^{p^i} r g_0^j e_i$. Portanto, é suficiente provar que elementos da forma $g^j e_i$ com $p^i - p^{i-1} \leq j \leq p^i$ são combinações lineares dos elementos de \mathcal{B} .

Escrevendo de outra maneira, é suficiente provar que os elementos da forma $g^{(p-1)p^{i-1}+k}e_i$ onde $0 \leq k < p^{i-1}$ são combinações lineares dos elementos de \mathcal{B} .

Note que

$$e_i = \frac{1}{p^{n-i+1}} \left((p-1) - g^{p^{i-1}} - g^{2p^{i-1}} - \dots + (p-1)g^{p \cdot p^{i-1}} - g^{(p+1)p^{i-1}} - g^{(p+2)p^{i-1}} - \dots \right. \\ \left. \dots + (p-1)g^{2p \cdot p^{i-1}} - \dots - g^{(p^{n-i+1} - (p-1))p^{i-1}} - g^{(p^{n-i+1} - 1)p^{i-1}} \right).$$

Logo,

$$g^{(p-1)p^{i-1}+k}e_i = \frac{1}{p^{n-i+1}} \left((p-1)g^{(p-1)p^{i-1}+k} - g^{p \cdot p^{i-1}+k} - g^{(p+1)p^{i-1}+k} - \dots - g^{(2p-2)p^{i-1}+k} + \right. \\ \left. + (p-1)g^{(2p-1)p^{i-1}+k} - g^{(2p)p^{i-1}+k} - g^{(2p+1)p^{i-1}+k} - \dots + \right. \\ \left. + (p-1)g^{(p^{n-i+1}) \cdot p^{i-1}+k} - g^k - g^{p^{i-1}+k} - g^{2p^{i-1}+k} + \dots - g^{(p-2)p^{i-1}+k} \right).$$

Para cada índice k escrito acima, temos que $g^{(p-1)p^{i-1}+k}e_i$ é combinação linear do conjunto $\mathcal{B}' = \{g^k e_i, g^{p^{i-1}+k}e_i, \dots, g^{(p-2)p^{i-1}+k}e_i\}$. Para isso, escrevemos:

$$g^k e_i = \frac{1}{p^{n-i+1}} \left((p-1)g^k - g^{p^{i-1}+k} - g^{2p^{i-1}+k} - \dots - g^{(p-1)p^{i-1}+k} + (p-1)g^{p \cdot p^{i-1}+k} - \right. \\ \left. - g^{(p+1)p^{i-1}+k} - \dots + (p-1)g^{(2p) \cdot p^{i-1}+k} - \dots - (p-1)g^{(p^{n-i+1} - p)p^{i-1}+k} - \right. \\ \left. - g^{(p^{n-i+1} - (p-1))p^{i-1}+k} - g^{(p^{n-i+1} - (p-2))p^{i-1}+k} - \dots - g^{(p^{n-i+1} - 1)p^{i-1}+k} \right).$$

$$\begin{aligned}
 g^{(p^{i-1}+k)}e_i &= \frac{1}{p^{n-i+1}} \left((p-1)g^{p^{i-1}+k} - g^{2p^{i-1}+k} - g^{3p^{i-1}+k} - \dots - g^{p \cdot p^{i-1}+k} + \right. \\
 &\quad + (p-1)g^{(p+1)p^{i-1}+k} - g^{(p+2)p^{i-1}+k} - g^{(p+3)p^{i-1}+k} - \dots + (p-1)g^{(2p+1)p^{i-1}+k} - \\
 &\quad \left. \dots + (p-1)g^{(p^{n-i+1}-(p-1))p^{i-1}+k} - g^{(p^{n-i+1}-(p-2))p^{i-1}+k} - \dots - g^k \right). \\
 \\
 g^{(2p^{i-1}+k)}e_i &= \frac{1}{p^{n-i+1}} \left((p-1)g^{2p^{i-1}+k} - g^{3p^{i-1}+k} - g^{4p^{i-1}+k} - \dots - g^{(p+1) \cdot p^{i-1}+k} + \right. \\
 &\quad + (p-1)g^{(p+2)p^{i-1}+k} - g^{(p+3)p^{i-1}+k} - g^{(p+4)p^{i-1}+k} - \dots + (p-1)g^{(2p+2)p^{i-1}+k} - \\
 &\quad \left. \dots + (p-1)g^{(p^{n-i+1}-(p-2))p^{i-1}+k} - g^{(p^{n-i+1}-(p-3))p^{i-1}+k} - \dots - g^k - g^{p^{i-1}+k} \right) \\
 \\
 &\vdots \\
 \\
 g^{(p-2)p^{i-1}+k}e_i &= \frac{1}{p^{n-i+1}} \left((p-1)g^{(p-2)p^{i-1}+k} - g^{(p-1)p^{i-1}+k} - \dots - g^{(2p-3)p^{i-1}+k} \right. \\
 &\quad + (p-1)g^{(2p-2)p^{i-1}+k} - g^{(2p-1)p^{i-1}+k} - \dots + (p-1)g^{(3p-2)p^{i-1}+k} - \dots \\
 &\quad + (p-1)g^{(p^{n-i+1}-2)p^{i-1}+k} - g^{(p^{n-i+1}-1)p^{i-1}+k} - g^k - g^{p^{i-1}+k} - \dots \\
 &\quad \left. - g^{(p-3)p^{i-1}+k} \right).
 \end{aligned}$$

Agora, pode se verificar diretamente a igualdade

$$g^{(p-1)p^{i-1}+k}e_i = -(g^k e_i) - (g^{p^{i-1}+k} e_i) - (g^{2p^{i-1}+k} e_i) - \dots - (g^{(p-2)p^{i-1}+k} e_i).$$

Como $\mathcal{B}' \subset \mathcal{B}$, segue que $\{e_i, ge_i, \dots, g^{(p-1)p^{i-1}-1}e_i\}$ é um conjunto gerador de RGe_i . ■

Exemplo 3.1.9 *Seja G um grupo cíclico de ordem 25. Neste caso,*

$$e_2 = \frac{1}{5}(4 - g^5 - g^{10} - g^{15} - g^{20}).$$

Considere a seguinte tabela com todos elementos da forma $g^k e_2$, com $0 \leq k \leq 24$.

$e_2 = \frac{1}{5}(4 - g^5 - g^{10} - g^{15} - g^{20})$	$g^{13}e_2 = \frac{1}{5}(4g^{13} - g^{18} - g^{23} - g^3 - g^8)$
$ge_2 = \frac{1}{5}(4g - g^6 - g^{11} - g^{16} - g^{21})$	$g^{14}e_2 = \frac{1}{5}(4g^{14} - g^{19} - g^{24} - g^4 - g^9)$
$g^2e_2 = \frac{1}{5}(4g^2 - g^7 - g^{12} - g^{17} - g^{22})$	$g^{15}e_2 = \frac{1}{5}(4g^{15} - g^{20} - 1 - g^5 - g^{10})$
$g^3e_2 = \frac{1}{5}(4g^3 - g^8 - g^{13} - g^{18} - g^{23})$	$g^{16}e_2 = \frac{1}{5}(4g^{16} - g^{21} - g - g^6 - g^{11})$
$g^4e_2 = \frac{1}{5}(4g^4 - g^9 - g^{14} - g^{19} - g^{24})$	$g^{17}e_2 = \frac{1}{5}(4g^{17} - g^{22} - g^2 - g^7 - g^{12})$
$g^5e_2 = \frac{1}{5}(4g^5 - g^{10} - g^{15} - g^{20} - 1)$	$g^{18}e_2 = \frac{1}{5}(4g^{18} - g^{23} - g^3 - g^8 - g^{13})$
$g^6e_2 = \frac{1}{5}(4g^6 - g^{11} - g^{16} - g^{21} - g)$	$g^{19}e_2 = \frac{1}{5}(4g^{19} - g^{24} - g^4 - g^9 - g^{14})$
$g^7e_2 = \frac{1}{5}(4g^7 - g^{12} - g^{17} - g^{22} - g^2)$	$g^{20}e_2 = \frac{1}{5}(4g^{20} - 1 - g^5 - g^{10} - g^{15})$
$g^8e_2 = \frac{1}{5}(4g^8 - g^{13} - g^{18} - g^{23} - g^3)$	$g^{21}e_2 = \frac{1}{5}(4g^{21} - g - g^6 - g^{11} - g^{16})$
$g^9e_2 = \frac{1}{5}(4g^9 - g^{14} - g^{19} - g^{24} - g^4)$	$g^{22}e_2 = \frac{1}{5}(4g^{22} - g^2 - g^7 - g^{12} - g^{17})$
$g^{10}e_2 = \frac{1}{5}(4g^{10} - g^{15} - g^{20} - 1 - g^5)$	$g^{23}e_2 = \frac{1}{5}(4g^{23} - g^3 - g^8 - g^{13} - g^{18})$
$g^{11}e_2 = \frac{1}{5}(4g^{11} - g^{16} - g^{21} - g - g^6)$	$g^{24}e_2 = \frac{1}{5}(4g^{24} - g^4 - g^9 - g^{14} - g^{19})$
$g^{12}e_2 = \frac{1}{5}(4g^{12} - g^{17} - g^{22} - g^2 - g^7)$	

Temos que $\mathcal{B} = \{e_2, ge_2, \dots, g^{19}e_2\}$ é uma base para $\langle e_2 \rangle$. Note que os elementos da forma $g^k e_2$, com $20 \leq k \leq 24$ são dados pelas seguintes combinações dos elementos de \mathcal{B} .

$$\begin{aligned}
g^{20}e_2 &= -e_2 - g^5e_2 - g^{10}e_2 - g^{15}e_2 \\
g^{21}e_2 &= -ge_2 - g^6e_2 - g^{11}e_2 - g^{16}e_2 \\
g^{22}e_2 &= -g^2e_2 - g^7e_2 - g^{12}e_2 - g^{17}e_2 \\
g^{23}e_2 &= -g^3e_2 - g^8e_2 - g^{13}e_2 - g^{18}e_2 \\
g^{24}e_2 &= g^4e_2 - g^9e_2 - g^{14}e_2 - g^{19}e_2
\end{aligned}$$

3.2 Códigos MDS de Comprimento p^n

Já é conhecido que, para códigos C de comprimento n sobre qualquer alfabeto de tamanho m , vale a seguinte desigualdade

$$d_H(C) \leq n - \log_m(|C|) + 1. \quad (3.2)$$

Definição 3.2.1 Dizemos que um código C de comprimento n sobre um alfabeto de tamanho m é um **código Separável pela Distância Máxima**, ou **código MDS**, se

$$d_H(C) = n - \log_m(|C|) + 1.$$

Até aqui já caracterizamos os códigos de comprimento p^n sobre anéis de cadeia, seus pesos, tamanhos e alguns resultados sobre posto. Vejamos alguns exemplos de códigos e uma comparação com o limitante antes mencionado.

Exemplo 3.2.2 Considere o anel RG , onde $R = \mathbb{Z}_{2^4}$ e $G = C_{5^3}$. Neste anel os idempotentes são $e_0 = \widehat{G}$, $e_1 = \widehat{G}_1 - \widehat{G}$, $e_2 = \widehat{G}_2 - \widehat{G}_1$ e $e_3 = \widehat{G}_3 - \widehat{G}_2$, onde $G_i = \langle g^{5^i} \rangle$.

Seja $C = RGe_1 \oplus RGe_2$. Temos que

$$w(C) = 2 |G_2| = 2 \cdot 5^{3-2} = 10,$$

$$|C| = 2^{4(5^1-5^0)+4(5^2-5^1)} = 2^{96}.$$

Pela desigualdade 3.2, para o código $C = \langle e_1 \rangle \oplus \langle e_2 \rangle$, temos:

$$d_H(C) \leq 125 - \log_{2^4}(2^{96}) + 1 = 102.$$

Neste exemplo o peso está muito distante do seu limitante superior

Exemplo 3.2.3 Considere agora $G = \langle g \rangle$ um grupo cíclico de ordem 9 e o anel $R = \mathbb{Z}_4$.

Observe que $U(\mathbb{Z}_9) = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ e $\langle \bar{2} \rangle = U(\mathbb{Z}_9)$. Como $\frac{|\mathbb{Z}_4|}{|\langle \bar{2} \rangle|} = 2$, temos que e_0, e_1 e e_2 são idempotentes primitivos ortogonais, onde $e_0 = \widehat{G}$, $e_1 = \widehat{G}_1 - \widehat{G}_0$ e $e_2 = \widehat{G}_2 - \widehat{G}_1$, onde $G_i = \langle g^{3^i} \rangle$.

Tomemos $C = \langle e_1 \rangle$. Assim,

$$w(C) = 2 |G_1| = 2 \cdot 3 = 6$$

e

$$|C| = 2^{2(3-1)} = 2^4.$$

O limitante para C é dado por

$$d_H(C) \leq 9 - \log_4(2^4) + 1 = 8.$$

Neste caso, a distância do código está próxima da distância máxima do limitante.

Tomemos agora G um grupo cíclico de ordem 4, R um anel de cadeia tal que $|\overline{R}| = q$, onde $q \equiv 3 \pmod{4}$ e o código gerado por $C = \langle e_1 \rangle$, onde $e_1 = \widehat{G}_1 - \widehat{G}_0$. Temos que

$$W(C) = 2 |G_1| = 2 \cdot 2 = 4,$$

$$|C| = |\overline{R}|^{t(2^1 - 2^{1-1})} = q^t.$$

e

$$d_H(C) \leq 4 - \log_{|\overline{R}|}(|\overline{R}|^t) + 1 = 4 - \log_{q^t}(q^t) = 4 = w(C).$$

Observe que, para qualquer $q \equiv 3 \pmod{4}$, estes códigos tem a maior distância de Hamming possível, além disso, é possível aumentar o número de palavras do código aumentando q . Sendo assim, qualquer outro código de comprimento 4, com q^t elementos possui distância de Hamming menor ou igual a deste código. Além disso, como $\langle \overline{q} \rangle = U(\mathbb{Z}_4)$, temos que $\{e_0, e_1, e_2\}$ é o conjunto dos idempotentes primitivos ortogonais em RG .

Exemplo 3.2.4 *Sejam G um grupo cíclico de ordem 4, $R = \mathbb{Z}_{11^7}$ um anel de cadeia e o código C_1 gerado por $e_1 = \widehat{G}_1 - \widehat{G}_0$. Temos que $\frac{|\mathbb{Z}_{11^7}|}{|\langle \overline{11} \rangle|} = 11$. Como $\overline{11} = \overline{3}$ em \mathbb{Z}_4 , temos*

que $\langle \overline{11} \rangle = U(\mathbb{Z}_4)$. Logo,

$$w(C_1) = 2 \mid G_1 \mid = 4$$

e

$$\mid C_1 \mid = 11^7.$$

O limitante da distância de Hamming é dado por

$$d_H(C_1) \leq 4 - \log_{11^7}(11^7) + 1 = 4 = w(C).$$

Observe que $C_2 = \langle e_2 \rangle$ não é um código MDS. De fato,

$$w(RGe_2) = 2 \cdot 2^{2-2} = 2 \text{ e } d_H(RGe_2) \leq 4 - 2^2 - 2^1 + 1 = 3.$$

Observe que o código $C_3 = RGe_0 \oplus RGe_1$ também não é MDS. De fato, $w(C_3) = \mid G_1 \mid = 2^{2-1} = 2$. O limitante de Hamming neste caso é dado por

$$d_H(C_3) \leq 4 - \log_{|R|}(\mid \overline{R} \mid)^{(t(2-1)+t)} + 1 = 5 - 2 = 3.$$

Agora, porém, o código $C_4 = RGe_0 \oplus RGe_2$ é um código MDS. De fato, $w(C_4) = 2 \cdot \mid G_2 \mid = 2 \cdot 2^{(2-2)} = 2$. O limitante de Hamming é dado por

$$d_H(C_4) = 5 - \log_{|R|}(\mid \overline{R} \mid)^{t(2^2-2^1)+t} = 5 - 3 = 2.$$

Novamente, o código $C_5 = RGe_1 \oplus RGe_2$ é um código MDS. De fato, $w(C_5) = 2 \cdot \mid G_2 \mid = 2 \cdot 2^{(2-2)} = 2$. O limitante de Hamming é dado por

$$d_H(C_5) \leq 5 - \log_{|R|}(\mid \overline{R} \mid)^{t(2^1-2^0)+t(2^2-2^1)} = 5 - 3 = 2.$$

3.3 Códigos MDS de Comprimento 2^n

Análogo ao que foi feito anteriormente, iremos analisar códigos de comprimento 2^n .

Quando tomamos $| \bar{R} | = q$, onde \bar{q} gera $U(\mathbb{Z}_{p^n})$, para códigos de comprimento p^n , sabemos que $\{e_0, \dots, e_n\}$ é o conjunto de idempotentes primitivos ortogonais em RG . Quando tomamos $| G | = 2^n$, temos um problema, pois o grupo das unidade de Z_{2^n} , para $m \geq 2$ não é cíclico e, assim, para qualquer $| \bar{R} | = q$, não teríamos a condição necessária dita anteriormente.

Agora, estamos interessados na construção de códigos que possuam distância de Hamming máxima. Para isso, tomaremos o comprimento 2^n e iremos focar nos códigos gerados pelo idempotente e_1 .

No teorema a seguir provaremos que e_1 é um idempotente primitivo.

Teorema 3.3.1 *Se $G = \langle g \rangle$ é um grupo cíclico de ordem $| G | = 2^n$, R é um anel de cadeia tal que $| R |$ não divide 2, então $e_1 = \hat{G}_1 - \hat{G}_0$ é um idempotente primitivo.*

Prova: Como $e_1 = \hat{G}_1 - \hat{G}_0$, temos $\hat{G}_1 = e_1 + \hat{G}_0$ e daí $e_1 \cdot \hat{G}_0 = (\hat{G}_1 - \hat{G}_0) \cdot \hat{G}_0 = \hat{G}_0 - \hat{G}_0 = 0$. Logo, $RG\hat{G}_1 = RGe_1 \oplus RG\hat{G}_0$ e, com isso, temos

$$| RG\hat{G}_1 | = | RGe_1 | \cdot | RG\hat{G}_0 |.$$

Assim,

$$| RGe_1 | = \frac{| RG\hat{G}_1 |}{| RG\hat{G}_0 |} = \frac{| R |^{\frac{|G|}{|\hat{G}_1|}}}{| R |^{\frac{|G|}{|\hat{G}_0|}}} = \frac{| R |^{2^1}}{| R |} = | R |.$$

Como $| RGe_1 | = | R |$, então $RGe_1 \cong R$. Como R é anel local, temos que R é indecomponível. Assim, e_1 é um idempotente primitivo, como queríamos demonstrar. ■

Neste caso, como $| G | = 2^n$, que é o comprimento do código e $w(RGe_1) = 2 \cdot 2^{n-1} = 2^n$, e pelo Teorema 3.3.1, $| RGe_1 | = | R |$, o código gerado por e_1 têm distância de Hamming máxima.

3.3.1 Resultados Sobre Códigos MDS de comprimento p^n

Consideremos agora G um grupo cíclico de ordem p^n com $p > 2$ e $|R| = q^k$, com $q \nmid |G|$ tal que $o(|\overline{R}|) = \phi(p^n)$ em $U(\mathbb{Z}_{p^n})$. Apresentaremos agora dois resultados sobre códigos MDS.

Teorema 3.3.2 *Considere R e G nas condições da Hipótese A. O código gerado por RGe_i onde $i > \frac{n+1}{2}$ não é MDS.*

Prova: Como $i > \frac{n+1}{2}$, temos que $-n + 2i - 1 > 0$. Como $p > 2$, então $p^{(-n+2i-1)} > 2$, e daí $p^{i-1} > 2p^{n-i}$. Como $p^n \geq p^i$, temos $p^n + p^{i-1} > p^i + 2p^{n-i}$, logo,

$$p^n - p^i + p^{i-1} - 2p^{n-i} > 0$$

e, assim, $p^n - p^i + p^{i-1} - 2p^{n-i} + 1 > 0$ o que resulta

$$p^n - p^i + p^{i-1} + 1 > 2p^{n-i},$$

onde $2.p^{n-i} = w(RGe_i)$. ■

Teorema 3.3.3 *Se $C = RGe_0 \oplus RGe_1 \oplus RGe_2 \oplus \dots \oplus RGe_k$, então C não é um código MDS.*

Prova: Se $C = RGe_0 \oplus RGe_1 \oplus RGe_2 \oplus \dots \oplus RGe_k$, então $w(C) = 2 |G_k| = 2p^{n-k}$.

Calculando o limitante 3.2, temos que

$$d_H(C) \leq p^n + \log_{|R|}(|\overline{R}|)^{t((p^1-p^0)+(p^2-p^1)+(p^3-p^2)+\dots+(p^k-p^{k-1})+1)} + 1.$$

Desenvolvendo a desigualdade acima, temos

$$d_H(C) \leq p^n - p^k + 1 = p^k(p^{n-k} + 1) + 1.$$

Como $p^k > 2$, temos $p^k(p^{n-k} + 1) + 1 > 2p^{n-k}$. Portanto, C não é MDS. ■

Uma pergunta interessante é: existem códigos MDS da forma RGe_i , onde G é um grupo cíclico de ordem p^n (p primo ímpar) e R um anel de cadeia? Esta pergunta ainda não possui uma resposta concreta, mas devido a algumas simulações computacionais, suspeitamos que os únicos códigos MDS da forma RGe_i onde G é um grupo cíclico de ordem p^n sejam os triviais.

CAPÍTULO 4

Códigos sobre Anéis de Cadeia de Comprimento $2p^n$

No Capítulo 3 calculamos o peso de todos os códigos cíclicos de comprimento p^n sobre anéis de cadeia. Neste capítulo, calcularemos o peso de todos os possíveis códigos cíclicos sobre anéis de cadeia de comprimento $2p^n$ e caracterizaremos todos os códigos livres de comprimento $2p^n$, exibindo uma base para estes códigos.

A seguir, descreveremos uma hipótese central que será utilizada ao longo deste capítulo.

Hipótese B

Sejam R um anel de cadeia finito, comutativo com unidade, tal que $|R| = q^k$, $M = \langle a \rangle$ o ideal maximal de R , $|\overline{R}| = q^l$, com $k = lt$, onde t é o índice de nilpotência de a e G um grupo cíclico com gerador g_0 , de ordem $2p^n$, com p primo ímpar, tal que $o(|\overline{R}|) = \phi(p^n)$ em $U(\mathbb{Z}_{2p^n})$, onde $q \nmid 2p^n$, $G_i = \langle g_0^{p^i} \rangle$ e $e_i = \widehat{G}_i - \widehat{G}_{i-1}$.

4.1 Peso Mínimo de Códigos de Comprimento $2p^n$

Nesta seção, calcularemos o peso de todos os códigos cíclicos de comprimento $2p^n$ sobre anéis de cadeia.

Em [15], Ferraz e Polcino Milies provaram o seguinte teorema:

Teorema 4.1.1 ([15], Teorema 3.2) *Sejam K um corpo com q elementos e A um grupo cíclico de ordem $2p^n$, p um primo ímpar tal que $o(q) = \phi(p^n)$ em $U(Z_{2p^n})$. Escreva $A = B \times G$ onde G é um p -subgrupo de Sylow e $B = \{1, d\}$ é um 2-subgrupo de Sylow. Se e_i , $0 \leq i \leq n$, denota um idempotente primitivo de KG , então os idempotentes primitivos de KA são*

$$\frac{1+d}{2}e_i \quad \text{e} \quad \frac{1-d}{2}e_i, \quad 0 \leq i \leq n.$$

Considere $K = \frac{R}{M}$. Fazendo o levantamento dos idempotentes de K para R , temos que

$$\left\{ \frac{1+d}{2}e_i \quad \text{e} \quad \frac{1-d}{2}e_i, \quad 0 \leq i \leq n \right\}$$

é um conjunto de idempotentes primitivos ortogonais em RA , onde R é um anel de cadeia, com $|R| = q^k$ e $q \nmid |A|$.

Em [15], Ferraz e Polcino Milies provaram que o peso do código $KA\left(\frac{1 \pm d}{2}e_i\right)$ é dado por

$$w(KA\left(\frac{1 \pm d}{2}e_i\right)) = \begin{cases} 4 |G_i|, & \text{se } 0 < i \leq n \\ |A|, & \text{se } i = 0 \end{cases}$$

Provaremos agora um resultado semelhante para $RA\left(\frac{1 \pm d}{2}e_i\right)$.

Teorema 4.1.2 *Considere R e G nas condições da Hipótese B. Seja $C = RA(a^k(\frac{1 \pm d}{2}e_i))$, com $0 \leq k < t$. Então*

$$w(C) = \begin{cases} 4 |G_i|, & \text{se } 0 < i \leq n \\ |A|, & \text{se } i = 0 \end{cases}$$

Prova: Temos que $e_i = \widehat{G}_i - \widehat{G}_{i-1}$, para $i \neq 0$. Seja $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_i em G . Como $\left(a^k\left(\frac{1\pm d}{2}\right)e_i\right) \cdot \widehat{G}_i = \left(a^k\left(\frac{1\pm d}{2}\right)e_i\right)$, temos $C \subset \left(a^k\left(\frac{1\pm d}{2}\right)\widehat{G}_i\right)$. Seja $\alpha \neq 0 \in C$, logo α pode ser escrito como

$$\alpha = (x_1\tau_1 + \dots + x_n\tau_n)\left(a^k\left(\frac{1\pm d}{2}\right)\widehat{G}_i\right).$$

Suponhamos que exista apenas um $x_i a^k \neq 0$ tal que $\alpha = (x_i\tau_i)\left(a^k\left(\frac{1\pm d}{2}\right)\widehat{G}_i\right)$. Então existe $\beta_i \in RA$ tal que

$$\alpha = (x_i\tau_i)\left(a^k\left(\frac{1\pm d}{2}\right)\widehat{G}_i\right) = \beta_i \cdot \left(a^k\left(\frac{1\pm d}{2}\right)e_i\right).$$

Como $\widehat{G}_{i-1} \cdot G_i = \widehat{G}_{i-1}$ e $e_i \cdot G_{i-1} = 0$, pois $G_i \subset G_{i-1}$, temos $(x_i\tau_i)\left(a^k\left(\frac{1\pm d}{2}\right)\widehat{G}_{i-1}\right) = 0$. Observe que $(x_i a^k \tau_i) \cdot \widehat{G}_{i-1}$ e $(x_i a^k \tau_i) \cdot d\widehat{G}_{i-1}$ têm suportes disjuntos. Logo, $(x_i a^k \tau_i) \cdot \widehat{G}_{i-1} = 0$ e, assim, $x_i a^k \widehat{G}_{i-1} = 0$. Portanto, $x_i a^k = 0$, o que contradiz nossa hipótese inicial. Logo existem pelo menos dois coeficientes diferentes de zero e, portanto, $w(C) \geq 4 \mid G_j \mid$.

Seja $g_0 \in G_{i-1}/G_i$. Temos que

$$\begin{aligned} \alpha &= (1 - g_0)\left(a^k\left(\frac{1\pm d}{2}\right)\widehat{G}_i\right) \\ &= (1 - g_0)\left(a^k\frac{1\pm d}{2}\right)(\widehat{G}_i - \widehat{G}_{i-1} + G_{i-1}) \\ &= (1 - g_0)\left(a^k\frac{1\pm d}{2}\right)(e_i + \widehat{G}_{i-1}) \\ &= (1 - g_0)\left(a^k\frac{1\pm d}{2}\right)e_i, \end{aligned}$$

pois $(1 - g_0) \cdot \widehat{G}_{i-1} = 0$. Logo $\alpha = (1 - g_0)\left(a^k\frac{1\pm d}{2}\right)\widehat{G}_i \in C$ e, como $w(\alpha) = 4 \mid G_i \mid$, temos que $w(C) \leq 4 \mid G_i \mid$. Portanto, $w(C) = 4 \mid G_i \mid$.

Vamos supor agora $C = \left\langle a^k\left(\frac{1\pm d}{2}\right)e_0 \right\rangle$. Provemos que $w(\langle a^k\left(\frac{1\pm d}{2}\right)e_0 \rangle) = \mid A \mid$. Seja $\alpha \neq 0 \in C$. Temos $\alpha = \sum_{g \in G} x_g d^{\zeta_g} g\left(a^k\left(\frac{1\pm d}{2}\right)e_0\right)$, onde $\zeta_g = 0$ ou 1 , $x_g \in R$. Como $g \cdot e_0 = e_0 = \widehat{G}$ e $d \cdot \left(\frac{1\pm d}{2}\right) = \pm\left(\frac{1\pm d}{2}\right)$, temos que $\alpha = \left(\sum a^k x'_g\right)\left(\frac{1\pm d}{2}\right)e_0$. Portanto, $w(C) = 2 \mid G \mid = \mid A \mid$. ■

Agora calcularemos os pesos de todos os possíveis códigos cíclicos de comprimento $2p^n$

sobre um anel de cadeia R , e um grupo G nas condições da *Hipótese B*. Iremos calcular os resultados de acordo com a soma dos geradores dos códigos. Nos teoremas que seguem consideraremos apenas o caso de somas de idempotentes da forma $a^{k_i(\frac{1+d}{2})}e_i$, sendo a demonstração análoga no caso $a^{k_i(\frac{1-d}{2})}e_i$.

Teorema 4.1.3 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_{i_1}(\frac{1+d}{2})}e_{i_1} \rangle \oplus \dots \oplus \langle a^{k_{i_l}(\frac{1+d}{2})}e_{i_l} \rangle$, onde $0 \leq k_{i_j} < t$, $1 \leq j \leq l$ e $0 < i_1 < i_2 < \dots < i_l$, então $w(C) = 4 \mid G_{i_l} \mid$.*

Prova:

Primeiramente, observe que $w(C) \leq w(\langle a^{k_{i_l}(\frac{1+d}{2})}e_{i_l} \rangle) = 4 \mid G_{i_l} \mid$.

Como $G_{i_l} \subset G_j$, para $j < i_l$, temos $\widehat{G}_{i_l}.e_j = e_j$. Logo $C \subset \langle a^k(\frac{1+d}{2})\widehat{G}_{i_l} \rangle$, onde $k = \min\{k_{i_1}, \dots, k_{i_l}\}$. Seja $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_{i_l} em G e $\alpha \in C$. Então podemos escrever

$$\alpha = (x_1\tau_1 + \dots + x_n\tau_n)(a^k(\frac{1+d}{2})\widehat{G}_{i_l}),$$

onde $x_i \in R$. Suponhamos agora que exista apenas um coeficiente x , tal que $xa^k \neq 0$. Então, podemos escrever α como

$$\alpha = x\tau(a^k(\frac{1+d}{2})\widehat{G}_{i_l}),$$

onde $\tau \in \Gamma$. Como $C = \langle a^{k_{i_1}(\frac{1+d}{2})}e_{i_1} \rangle \oplus \dots \oplus \langle a^{k_{i_l}(\frac{1+d}{2})}e_{i_l} \rangle$, existem $\beta_1, \dots, \beta_l \in RA$ tais que

$$\alpha = \beta_1 a^{k_{i_1}(\frac{1+d}{2})}e_{i_1} + \dots + \beta_l a^{k_{i_l}(\frac{1+d}{2})}e_{i_l} = x_1\tau_1(a^k(\frac{1+d}{2})\widehat{G}_{i_l}).$$

Como $G_{i_{l-1}} \supset G_j$, para $i_1 \leq j \leq i_l$, temos $\widehat{G}_{i_{l-1}}.e_j = 0$. Logo, $x\tau(a^k(\frac{1+d}{2})\widehat{G}_{i_{l-1}}) = 0$. Como $x\tau(a^k\widehat{G}_{i_{l-1}})$ e $x\tau(a^kd\widehat{G}_{i_{l-1}})$ têm suportes disjuntos, temos que $x\tau(a^k\widehat{G}_{i_{l-1}}) = 0$ e daí, $xa^k = 0$, o que contradiz nossa hipótese original. Logo $w(\alpha) \geq 4 \mid G_{i_l} \mid$ e, portanto, $w(C) \geq 4 \mid G_{i_l} \mid$.

Com isso, temos $w(C) = 4 \mid G_{i_l} \mid$.

■

Teorema 4.1.4 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_0}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_1}(\frac{1+d}{2})e_1 \rangle \oplus \dots \oplus \langle a^{k_l}(\frac{1+d}{2})e_l \rangle$, onde $0 \leq k_j < t$, $0 \leq j \leq l$, então $w(C) = 2 \mid G_l \mid$.*

Prova: Como $(a^{k_i}(\frac{1+d}{2})e_i) \cdot (\frac{1+d}{2})\widehat{G}_l = (a^k(\frac{1+d}{2})e_i)$, para $0 \leq i \leq l$, temos $C \subset \langle a^{k_i}(\frac{1+d}{2})\widehat{G}_l \rangle$, logo

$$w(C) \geq w(\langle a^{k_i}(\frac{1+d}{2})\widehat{G}_l \rangle) = 2 \mid G_l \mid.$$

Agora seja $k = \max\{k_0, \dots, k_l\}$. Observe que

$$\begin{aligned} a^k(\frac{1+d}{2})\widehat{G}_l &= a^k(\frac{1+d}{2})((\widehat{G}_l - \widehat{G}_{l-1}) + (\widehat{G}_{l-1} + \widehat{G}_{l-2}) + \dots + (\widehat{G}_1 - \widehat{G}_0) + \widehat{G}_0) \\ &= a^k(\frac{1+d}{2})e_l + a^k(\frac{1+d}{2})e_{l-1} + \dots + a^k(\frac{1+d}{2})e_2 + a^k(\frac{1+d}{2})e_1 + a^k(\frac{1+d}{2})e_0. \end{aligned}$$

Portanto,

$$\begin{aligned} \langle (a^k(\frac{1+d}{2})\widehat{G}_l) \rangle &\subset \langle a^k(\frac{1+d}{2})e_0 \rangle \oplus \langle a^k(\frac{1+d}{2})e_1 \rangle \oplus \dots \oplus \langle a^k(\frac{1+d}{2})e_l \rangle \\ &\subset \langle a^{k_0}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_1}(\frac{1+d}{2})e_1 \rangle \oplus \dots \oplus \langle a^{k_l}(\frac{1+d}{2})e_l \rangle = C. \end{aligned}$$

Logo $2 \mid G_l \mid = w(\langle (a^k(\frac{1+d}{2})\widehat{G}_l) \rangle) \geq w(C)$. Portanto, $w(C) = 2 \mid G_l \mid$. ■

Teorema 4.1.5 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_0}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} \rangle \oplus \dots \oplus \langle a^{k_{i_l}}(\frac{1+d}{2})e_{i_l} \rangle$, onde $0 \leq k_j, k_0 < t$, $1 \leq j \leq l$ e $\{i_1, \dots, i_l\} \subsetneq \{1, \dots, i_l\}$, então $w(C) = 4 \mid G_{i_l} \mid$.*

Prova: Primeiramente observe que $w(C) \leq w(a^{k_{i_l}}(\frac{1+d}{2})e_{i_l}) = 4 \mid G_{i_l} \mid$.

Como $G_{i_l} \subset G_j$, para $j < i_l$, temos $\widehat{G}_{i_l} \cdot e_j = e_j$. Logo $C \subset \langle a^k(\frac{1+d}{2})\widehat{G}_{i_l} \rangle$, onde $k = \max\{k_{i_1}, \dots, k_{i_l}\}$. Seja $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_{i_l} em G e $\alpha \in C$. Então

podemos escrever $\alpha = (x_1\tau_1 + \dots + x_n\tau_n)(a^k(\frac{1+d}{2})\widehat{G}_{i_l})$, onde $x_i \in R$. Suponhamos agora que exista apenas um coeficiente x de α tal que $xa^k \neq 0$. Então podemos escrever α como $\alpha = x\tau(a^k(\frac{1+d}{2})\widehat{G}_{i_l})$, onde $\tau \in \Gamma$. Como

$$C = \langle a^{k_0}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} \rangle \oplus \dots \oplus \langle a^{k_{i_l}}(\frac{1+d}{2})e_{i_l} \rangle,$$

existem $\beta_0, \beta_1, \dots, \beta_l$, tais que

$$\alpha = x\tau(a^k(\frac{1+d}{2})\widehat{G}_{i_l}) = \beta_0 a^{k_0}(\frac{1+d}{2})e_0 + \beta_1 a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} + \dots + \beta_l a^{k_{i_l}}(\frac{1+d}{2})e_{i_l}.$$

Como $\{i_1, \dots, i_l\} \subsetneq \{1, \dots, i_l\}$, existe pelo menos um $i_r \in \{1, \dots, i_l\}$ tal que o idempotente $(\frac{1+d}{2})e_{i_r}$ não está na soma inicial. Considere i_r o menor número que não está em $\{i_1, \dots, i_l\}$ e está em $\{1, \dots, i_l\}$. Multiplicando ambos os lados da igualdade por \widehat{G}_{i_r} , temos

$$\alpha = x\tau(a^k(\frac{1+d}{2})\widehat{G}_{i_r}) = \beta_0 a^{k_0}(\frac{1+d}{2})e_0 + \beta_1 a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} + \dots + \beta_l a^{k_{i_r-1}}(\frac{1+d}{2})e_{i_r-1}.$$

Como o peso do ideal $\langle a^{k_0}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_1}(\frac{1+d}{2})e_{i_1} \rangle \oplus \langle a^{k_2}(\frac{1+d}{2})e_{i_2} \rangle \oplus \dots \oplus \langle a^{k_{i_r-1}}(\frac{1+d}{2})e_{i_r-1} \rangle$ é $2 \mid G_{i_r-1} \mid = 2p^{n-i_r+1}$ e $w(\alpha\widehat{G}_{i_r}) = 2 \mid G_{i_r} \mid = 2p^{n-i_r}$ temos uma contradição. Com isso, temos $w(C) \geq 4 \mid G_{i_l} \mid$ e assim, $w(C) = 4 \mid G_{i_l} \mid$. ■

Agora iremos calcular o peso mínimo dos códigos que sejam somas de ideais do tipo $\langle (a^{k_i}(\frac{1+d}{2})e_i) \rangle$ e $\langle (a^{k_j}(\frac{1-d}{2})e_j) \rangle$. Como o cálculo para estes códigos envolvem várias técnicas diferentes para os diferentes tipos de somas, calcularemos inicialmente o peso mínimo dos códigos que sejam somas de dois ideais apenas e depois generalizaremos estes cálculos para uma soma finita destes ideais.

Teorema 4.1.6 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_i}(\frac{1+d}{2})e_i \rangle \oplus \langle a^{k_j}(\frac{1-d}{2})e_j \rangle$, onde $0 < i < j \leq n$, $0 \leq k_i, k_j < t$, então $w(C) = 4 \mid G_j \mid$.*

Prova: Como $\langle a^{k_j}(\frac{1-d}{2})e_j \rangle \subset C$, temos $w(C) \leq w(\langle a^{k_j}(\frac{1-d}{2})e_j \rangle) = 4 \mid G_j \mid$. Além

disso, $\widehat{G}_j \cdot e_i = e_i$ e $\widehat{G}_j \cdot e_j = e_j$. Logo

$$C \subset \langle a^k \left(\frac{1+d}{2}\right) \widehat{G}_j \rangle \oplus \langle a^k \left(\frac{1-d}{2}\right) \widehat{G}_j \rangle = \langle a^k \widehat{G}_j \rangle,$$

onde $k = \min\{k_i, k_j\}$. Seja $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_j em G e $\alpha \neq 0 \in C$. Podemos escrever $\alpha = (x_1\tau_1 + \dots + x_n\tau_n + x'_1d\tau_1 + \dots + x'_nd\tau_n)a^k\widehat{G}_j$, onde x_l e $x'_l \in R$. Suponha que exista apenas um coeficiente y de α tal que $ya^k \neq 0$. Então α é da forma $\alpha = (ya^kd^{\zeta_\tau}\tau)\widehat{G}_j$, onde $\zeta_\tau = 0$ ou 1 e $\tau \in \Gamma$. Logo existem $\beta_i, \beta_j \in RA$ tais que

$$\alpha = (ya^kd^{\zeta_\tau}\tau)\widehat{G}_j = \beta_i a^{k_i} \left(\frac{1+d}{2}\right) e_i + \beta_j a^{k_j} \left(\frac{1-d}{2}\right) e_j.$$

Multiplicando ambos os lados da igualdade por \widehat{G}_{i-1} , temos $(ya^kd^{\zeta_\tau}\tau)\widehat{G}_{i-1} = 0$. Logo, $ya^k = 0$, o que é uma contradição.

Suponhamos agora que existam apenas dois coeficientes y_1, y_2 de α tais que $y_1a^k \neq 0$ e $y_2a^k \neq 0$. Assim, podemos escrever

$$\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_j = \beta_i a^{k_i} \left(\frac{1+d}{2}\right) e_i + \beta_j a^{k_j} \left(\frac{1-d}{2}\right) e_j,$$

onde $\zeta_\tau, \zeta_{\tau'} = 0$ ou 1 e τ e $\tau' \in \Gamma$. Suponhamos agora $\zeta_\tau \neq \zeta_{\tau'}$. Multiplicando ambos os lados por \widehat{G}_{i-1} , temos $(y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_{i-1} = 0$. Como $\zeta_\tau \neq \zeta_{\tau'}$, então as palavras $(y_1d^{\zeta_\tau}\tau)a^k\widehat{G}_{i-1}$ e $(y_2d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_{i-1}$, têm suportes disjuntos. Portanto,

$$(y_1d^{\zeta_\tau}\tau)a^k\widehat{G}_{i-1} = (y_2d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_{i-1} = 0$$

e assim, $y_1 = y_2 = 0$, o que contradiz nossa hipótese. Suponhamos agora sem perda de generalidade que $\zeta_\tau = \zeta_{\tau'} = 0$. Assim,

$$\alpha = (y_1\tau + y_2\tau')a^k\widehat{G}_j = \beta_i a^{k_i} \left(\frac{1+d}{2}\right) e_i + \beta_j a^{k_j} \left(\frac{1-d}{2}\right) e_j. \quad (4.1)$$

Multiplicando ambos os lados da igualdade 4.1 por $(\frac{1-d}{2})\widehat{G}_{j-1}$, temos

$$(y_1\tau + y_2\tau')a^k(\frac{1-d}{2})\widehat{G}_{j-1} = 0.$$

Desenvolvendo os termos da igualdade acima, temos

$$(y_1\tau + y_2\tau')a^k\widehat{G}_{j-1} - (y_1d\tau_1 + y_2d\tau_2)a^k\widehat{G}_{j-1} = 0.$$

Como as palavras $(y_1\tau + y_2\tau')a^k\widehat{G}_{j-1}$ e $(y_1d\tau + y_2d\tau')a^k\widehat{G}_{j-1}$ têm suportes disjuntos, temos $(y_1\tau + y_2\tau')a^k\widehat{G}_{j-1} = 0$. Agora, multiplicando a equação 4.1 por \widehat{G}_{j-1} , temos

$$0 = (y_1\tau + y_2\tau')a^k\widehat{G}_{j-1} = \beta_i a^{k_i}(\frac{1+d}{2})e_i.$$

Portanto, $\alpha \in \langle a^{k_j}(\frac{1-d}{2})e_j \rangle$. Mas o peso de α é

$$w(\alpha) = 2 |G_j| \quad e \quad w(\langle a^{k_j}(\frac{1-d}{2})e_j \rangle) = 4 |G_j|,$$

o que é um absurdo, pois contradiz a condição da minimalidade do peso de $\langle a^{k_j}(\frac{1-d}{2})e_j \rangle$.

Suponhamos agora que existam apenas três coeficientes y_1, y_2, y_3 de α , tais que $y_1a^k \neq 0, y_2a^k \neq 0, y_3a^k \neq 0$. Então, podemos escrever

$$\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau' + y_3d^{\zeta_{\tau''}}\tau'')a^k\widehat{G}_j = \beta_i a^{k_i}(\frac{1+d}{2})e_i + \beta_j a^{k_j}(\frac{1-d}{2})e_j,$$

onde $\zeta_\tau, \zeta_{\tau'}, \zeta_{\tau''} = 0$ ou 1 e τ, τ' e $\tau'' \in \Gamma$. Suponhamos que $\zeta_\tau = \zeta_{\tau'} \neq \zeta_{\tau''}$. Multiplicando a equação acima por \widehat{G}_{i-1} , temos

$$(y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau' + y_3d^{\zeta_{\tau''}}\tau'')a^k\widehat{G}_{i-1} = 0.$$

Como $(y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_{i-1}$ e $(y_3d^{\zeta_{\tau''}}\tau'')a^k\widehat{G}_{i-1}$ têm suportes disjuntos, temos

$y_3 a^k = 0$, o que contradiz nossa hipótese inicial. Suponhamos então, sem perda de generalidade, que $\zeta_\tau = \zeta_{\tau'} = \zeta_{\tau''} = 0$. Assim,

$$\alpha = (y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \widehat{G}_j = \beta_i a^{k_i} \left(\frac{1+d}{2}\right) e_i + \beta_j a^{k_j} \left(\frac{1-d}{2}\right) e_j. \quad (4.2)$$

Multiplicando ambos os lados da equação acima por $\left(\frac{1-d}{2}\right) \widehat{G}_{j-1}$, temos

$$(y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \left(\frac{1-d}{2}\right) \widehat{G}_{j-1} = 0.$$

Desenvolvendo os termos da igualdade acima, temos

$$(y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \widehat{G}_{j-1} - (y_1 \tau + y_2 \tau' + y_3 \tau'') a^k d \widehat{G}_{j-1} = 0.$$

Como as palavras $(y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \widehat{G}_{j-1}$ e $(y_1 \tau + y_2 \tau' + y_3 \tau'') a^k d \widehat{G}_{j-1}$ têm suportes disjuntos, temos $(y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \widehat{G}_{j-1} = 0$.

Multiplicando a equação 4.2 por \widehat{G}_{j-1} , temos

$$0 = (y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \widehat{G}_{j-1} = \beta_i a^{k_i} \left(\frac{1+d}{2}\right) e_i = 0.$$

Portanto, $\alpha \in \langle a^{k_j} \left(\frac{1-d}{2}\right) e_j \rangle$. Mas o peso de α é

$$w(\alpha) = 3 |G_j| \quad e \quad w(\langle a^{k_j} \left(\frac{1-d}{2}\right) e_j \rangle) = 4 |G_j|,$$

o que contradiz a minimalidade do peso de $\langle a^{k_j} \left(\frac{1-d}{2}\right) e_j \rangle$.

Portanto, $w(C) \geq 4 |G_j|$ e, assim, temos $w(C) = 4 |G_j|$.

■

Teorema 4.1.7 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_0} \left(\frac{1+d}{2}\right) e_0 \rangle \oplus \langle a^{k_j} \left(\frac{1-d}{2}\right) e_j \rangle$, onde $1 < j \leq n$, $0 \leq k_0, k_j < t$, então $w(C) = 4 |G_j|$.*

Prova: Primeiramente, temos $w(C) \leq w(\langle a^{k_j}(\frac{1-d}{2})e_j \rangle) = 4 |G_j|$.

Observe que $C \subset \langle a^k \widehat{G}_j \rangle$, onde $k = \min\{k_0, k_j\}$. Seja $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_j em G e $0 \neq \alpha \in C$. Assim, $\alpha = (x_1\tau_1 + \dots + x'_n\tau_n + x'_1d\tau_1 + \dots + x'_nd\tau_n)a^k\widehat{G}_j$.

Suponhamos que exista apenas um coeficiente y de α tal que $ya^k \neq 0$. Assim, podemos escrever α como

$$\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_j,$$

onde $\zeta_\tau = 0$ ou 1 . Logo, existem $\alpha_1, \alpha_2 \in RA$ tais que

$$(yd^{\zeta_\tau}\tau)a^k\widehat{G}_j = \alpha_1a^{k_0}\left(\frac{1+d}{2}\right)e_0 + \alpha_2a^{k_j}\left(\frac{1-d}{2}\right)e_j.$$

Multiplicando a igualdade acima por \widehat{G}_{j-1} , temos

$$(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{j-1} = \alpha_1a^{k_0}\left(\frac{1+d}{2}\right)e_0. \quad (4.3)$$

Daí, $(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{j-1} = 0$, pois independente do valor de ζ_τ na igualdade 4.3, teríamos $\alpha_1a^{k_0}\widehat{G} = 0$ ou $\alpha_1a^{k_0}d\widehat{G} = 0$ e portanto $ya^k = 0$.

Suponhamos agora que existam apenas dois coeficientes y_1, y_2 de α tais que $y_1a^k \neq 0$, $y_2a^k \neq 0$. Logo existem $\alpha_1, \alpha_2 \in RA$ tais que

$$\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_j = \alpha_1a^{k_0}\left(\frac{1+d}{2}\right)e_0 + \alpha_2a^{k_j}\left(\frac{1-d}{2}\right)e_j,$$

onde $\zeta_\tau, \zeta_{\tau'} = 0$ ou 1 e τ e $\tau' \in \Gamma$. Temos $\alpha_1 = \sum_{g \in G} x_g d^{\zeta_g} g$, onde $\zeta_g = 0$ ou 1 . Logo $\alpha_1 \cdot (a^{k_0} \frac{1+d}{2} e_0) = (\sum x_g) a^{k_0} (\frac{1+d}{2}) e_0 = (\sum x_g) a^{k_0} (\frac{1+d}{2}) \widehat{G}$. Assim,

$$\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_{j-1} = (\sum x_g) a^{k_0} \left(\frac{1+d}{2}\right) \widehat{G}.$$

Suponhamos, sem perda de generalidade, $\zeta_\tau \neq \zeta_{\tau'}$ e $\zeta_\tau = 0$. Como

$|\tau G_{j-1}| = |\tau' G_{j-1}| = |G_{j-1}| < |G|$, pois $j > 1$, temos $(\sum x_g a^{k_0}) = 0$, pois

$$y_1 \tau a^k G_{j-1} = \frac{1}{2} (\sum x_g a^{k_0}) \widehat{G} \text{ e } y_2 d \tau' a^k G_{j-1} = \frac{1}{2} (\sum x_g a^{k_0}) d \widehat{G}.$$

Assim, $y_1 a^k = y_2 a^k = 0$, o que contradiz nossa hipótese.

Suponhamos agora $\zeta_\tau = \zeta_{\tau'} = 0$. Assim,

$$\alpha = (y_1 \tau + y_2 \tau') a^k \widehat{G}_j = \alpha_1 a^{k_0} \left(\frac{1+d}{2}\right) e_0 + \alpha_2 a^{k_j} \left(\frac{1-d}{2}\right) e_j.$$

Multiplicando a igualdade acima por \widehat{G}_{j-1} , temos

$$(y_1 \tau + y_2 \tau') a^k \widehat{G}_{j-1} = \alpha_1 a^{k_0} \left(\frac{1+d}{2}\right) e_0.$$

Novamente, podemos escrever $\alpha_1 a^{k_0} \left(\frac{1+d}{2}\right) e_0 = (\sum x_g) a^{k_0} \left(\frac{1+d}{2}\right) e_0 = (\sum x_g) a^{k_0} \left(\frac{1+d}{2}\right) \widehat{G}$ e, novamente, teríamos $\frac{1}{2} (\sum x_g) a^{k_0} d \widehat{G} = 0$ e assim, $(\sum x_g) a^{k_0} = 0$. Portanto, teríamos $\alpha = \alpha_2 a^{k_j} \left(\frac{1-d}{2}\right) e_j$, ou seja, $\alpha \in \langle a^{k_j} \left(\frac{1-d}{2}\right) e_j \rangle$, porém, $w(\alpha) = 2 \mid |G_j|$ e $w(\langle a^{k_j} \left(\frac{1-d}{2}\right) e_j \rangle) = 4 \mid |G_j|$, o que é um absurdo.

Suponhamos agora que existam apenas três coeficientes y_1, y_2 e y_3 de α tais que $y_1 a^k \neq 0$, $y_2 a^k \neq 0$ e $y_3 a^k \neq 0$. Logo existem $\alpha_1, \alpha_2 \in RA$ tais que

$$\alpha = (y_1 d^{\zeta_\tau} \tau_1 + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k \widehat{G}_j = \alpha_1 a^{k_0} \left(\frac{1+d}{2}\right) e_0 + \alpha_2 a^{k_j} \left(\frac{1-d}{2}\right) e_j,$$

onde $\zeta_\tau, \zeta_{\tau'}, \zeta_{\tau''} = 0$ ou 1 e τ, τ' e $\tau'' \in \Gamma$. Temos $\alpha_1 = \sum_{g \in G} x_g d^{\zeta_g} g$, onde $\zeta_g = 0$ ou 1. Logo $\alpha_1 \cdot (a^{k_0} \frac{1+d}{2} e_0) = (\sum x_g) a^{k_0} \left(\frac{1+d}{2}\right) e_0 = (\sum x_g) a^{k_0} \left(\frac{1+d}{2}\right) \widehat{G}$. Assim,

$$(y_1 d^{\zeta_\tau} \tau_1 + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k \widehat{G}_{j-1} = (\sum x_g) a^{k_0} \left(\frac{1+d}{2}\right) \widehat{G}.$$

Se $\zeta_\tau = \zeta_{\tau'} \neq \zeta_{\tau''}$, teríamos $y_3 a^k = 0$, pois se $\zeta_{\tau''} = 0$ (ou 1), então $y_3 \zeta_{\tau''} a^k \widehat{G}_{j-1} = \frac{1}{2} (\sum x_g) \widehat{G}$, onde $|\tau_3 G_{j-1}| = |G_{j-1}| < |G|$.

Vamos considerar agora, sem perda de generalidade, $\zeta_\tau = \zeta_{\tau'} = \zeta_{\tau''} = 0$. Assim,

$$(y_1\tau + y_2\tau' + y_3\tau'')a^k\widehat{G}_{j-1} = \left(\sum x_g\right)a^{k_0}\left(\frac{1+d}{2}\right)\widehat{G}.$$

Daí, $(\sum x_g)a^{k_0}\left(\frac{1}{2}\right)d\widehat{G} = 0$ e assim, $(\sum x_g)a^{k_0} = 0$. Logo $\alpha \in \langle a^{k_j}\left(\frac{1-d}{2}\right)e_j \rangle$, mas $w(\alpha) = 3 \mid G_j \mid$ e $w(\langle a^{k_j}\left(\frac{1-d}{2}\right)e_j \rangle) = 4 \mid G_j \mid$, o que é um absurdo.

Assim, $w(C) \geq 4 \mid G_j \mid$ e portanto, $w(C) = 4 \mid G_j \mid$.

■

Teorema 4.1.8 *Considere R e G nas condições da Hipótese B, onde $p > 3$. Se o código C é da forma $C = \langle a^{k_0}\left(\frac{1+d}{2}\right)e_0 \rangle \oplus \langle a^{k_1}\left(\frac{1-d}{2}\right)e_1 \rangle$, onde $1 < j \leq n$, $0 \leq k_0, k_1 < t$, então $w(C) = 4 \mid G_1 \mid$.*

Prova: Temos $w(C) \leq w(\langle a^{k_1}\left(\frac{1-d}{2}\right)e_1 \rangle) = 4 \mid G_1 \mid$. Provemos agora que $w(C) \geq 4 \mid G_1 \mid$.

Observe que $C \subset \langle a^k\widehat{G}_1 \rangle$, onde $k = \min\{k_0, k_1\}$. Sejam $\Gamma = \{\tau_1, \dots, \tau_p\}$ um transversal de G_1 em G e $\alpha \neq 0 \in C$.

Suponhamos que exista apenas um coeficiente y de α tal que $ya^k \neq 0$. Então existem α_0 e $\alpha_1 \in RA$, tal que $\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_1 = \alpha_0a^{k_0}\left(\frac{1+d}{2}\right)e_0 + \alpha_1a^{k_1}\left(\frac{1-d}{2}\right)e_1$, onde $\zeta_\tau = 1$ ou 0 e $\tau \in \Gamma$.

Multiplicando a igualdade acima por $\left(\frac{1-d}{2}\right)\widehat{G}$, temos

$$(yd^{\zeta_\tau}\tau)a^k\left(\frac{1-d}{2}\right)\widehat{G} = 0.$$

Desenvolvendo, temos $(yd^{\zeta_\tau}\tau)a^k\widehat{G} - (yd^{\zeta_\tau}\tau)a^kd\widehat{G} = 0$. Como as palavras $(yd^{\zeta_\tau}\tau)a^k\widehat{G}$ e $(yd^{\zeta_\tau}\tau)a^kd\widehat{G}$ têm suportes disjuntos, temos $(yd^{\zeta_\tau}\tau)a^k\widehat{G} = 0$ e, portanto, $ya^k = 0$, o que contradiz nossa hipótese inicial.

Suponhamos que existam apenas dois coeficiente y_1, y_2 de α tais que $y_1a^k \neq 0$ e $y_2a^k \neq 0$.

Então existem α_0 e $\alpha_1 \in RA$, tais que

$$\alpha = (y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau') a^k \widehat{G}_1 = \alpha_0 a^{k_0} \left(\frac{1+d}{2}\right) e_0 + \alpha_1 a^{k_1} \left(\frac{1-d}{2}\right) e_1,$$

onde $\zeta_\tau, \zeta_{\tau'} = 0$ ou 1 e τ e $\tau' \in \Gamma$.

Se $\zeta_\tau = \zeta_{\tau'}$, multiplicando a igualdade acima por \widehat{G} , temos

$$(y_1 \tau + y_2 \tau') a^k \widehat{G} = \alpha_0 a^{k_0} \left(\frac{1+d}{2}\right) e_0.$$

Como $\alpha_0 \in RA$, então $\alpha_0 = \sum_{g \in G} x_g d^{\zeta_g} g$ e, assim, $\alpha_0 a^{k_0} \left(\frac{1+d}{2}\right) e_0 = (\sum x_g) a^{k_0} \left(\frac{1+d}{2}\right) \widehat{G}$. Portanto, $(\sum x_g) a^{k_0} \widehat{G} = 0$ e assim $(\sum x_g) a^{k_0} = 0$. Logo $\alpha \in \langle a^{k_1} \left(\frac{1-d}{2}\right) e_1 \rangle$, mas $w(\alpha) = 2 \mid G_1 \mid$ e $w(\langle a^{k_1} \left(\frac{1-d}{2}\right) e_1 \rangle) = 4 \mid G_1 \mid$, o que é um absurdo.

Se $\zeta_\tau = 0 \neq \zeta_{\tau'}$, então

$$\alpha = (y_1 \tau + y_2 d \tau') a^k \widehat{G}_1 = \alpha_0 a^{k_0} \left(\frac{1+d}{2}\right) e_0 + \alpha_1 a^{k_1} \left(\frac{1-d}{2}\right) e_1.$$

Multiplicando a igualdade acima por $\left(\frac{1+d}{2}\right)$, temos

$$(y_1 \tau + y_2 d \tau') \left(\frac{1+d}{2}\right) a^k \widehat{G}_1 = \left(\sum x_g\right) a^{k_0} \left(\frac{1+d}{2}\right) \widehat{G}.$$

Desenvolvendo e igualando termo a termo, temos

$$(y_1 \tau + y_2 \tau') a^k \widehat{G}_1 = \left(\sum x_g\right) a^{k_0} \widehat{G}.$$

Como estamos considerando $p \neq 3$, temos $\mid G \mid \neq \mid \tau_1 G_1 \mid + \mid \tau_2 G_1 \mid = 2 \mid G_1 \mid$. Logo $(\sum x_g) a^{k_0} = 0$ e, assim, $\alpha \in \langle a^{k_1} \left(\frac{1-d}{2}\right) e_1 \rangle$, mas $w(\alpha) = 2 \mid G_1 \mid$ e $w(\langle a^{k_1} \left(\frac{1-d}{2}\right) e_1 \rangle) = 4 \mid G_1 \mid$, o que é um absurdo.

Suponhamos que existam apenas três coeficiente y_1, y_2 e y_3 de α tais que $y_1 a^k \neq 0$,

$y_2a^k \neq 0$ e $y_3a^k \neq 0$. Então existem α_0 e $\alpha_1 \in RA$ tais que

$$\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau' + y_3d^{\zeta_{\tau''}}\tau'')a^k\widehat{G}_1 = \alpha_0a^{k_0}\left(\frac{1+d}{2}\right)e_0 + \alpha_1a^{k_1}\left(\frac{1-d}{2}\right)e_1,$$

onde $\zeta_\tau, \zeta_{\tau'}$ e $\zeta_{\tau''} = 0$ ou 1 e τ, τ' e $\tau'' \in \Gamma$.

Se $\zeta_\tau = \zeta_{\tau'} = \zeta_{\tau''} = 0$, multiplicando a igualdade acima por \widehat{G} , temos

$$(y_1\tau + y_2\tau' + y_3\tau'')a^k\widehat{G} = \left(\sum x_g\right)a^{k_0}\left(\frac{1+d}{2}\right)\widehat{G}.$$

Portanto, $(\sum x_g)a^{k_0}d\widehat{G} = 0$ e, assim, $(\sum x_g)a^{k_0} = 0$. Logo, $\alpha \in \langle a^{k_1}\left(\frac{1-d}{2}\right)e_1 \rangle$, mas $w(\alpha) = 3 \mid G_1 \mid$ e $w(\langle a^{k_1}\left(\frac{1-d}{2}\right)e_1 \rangle) = 4 \mid G_1 \mid$ e daí temos $\alpha = 0$.

Agora vamos supor $\zeta_\tau = \zeta_{\tau'} = 0$ e que $\zeta_{\tau''} = 1$. Assim, α é dado por

$$\alpha = (y_1\tau + y_2\tau' + y_3d\tau'')a^k\widehat{G}_1 = \alpha_0a^{k_0}\left(\frac{1+d}{2}\right)e_0 + \alpha_1a^{k_1}\left(\frac{1-d}{2}\right)e_1.$$

Multiplicando a igualdade por $\left(\frac{1+d}{2}\right)$, temos

$$(y_1\tau + y_2\tau' + y_3d\tau'')a^k\left(\frac{1+d}{2}\right)\widehat{G}_1 = \alpha_0a^{k_0}\left(\frac{1+d}{2}\right)e_0 = \left(\sum x_g\right)a^{k_0}\left(\frac{1+d}{2}\right)\widehat{G}. \quad (4.4)$$

Da igualdade 4.4 temos $(y_1\tau + y_2\tau' + y_3d\tau'')a^k\widehat{G}_1 = (\sum x_g)a^{k_0}\widehat{G}$. Como estamos considerando $p > 3$, temos $\mid G \mid \neq \mid \tau G_1 \mid + \mid \tau' G_1 \mid + \mid \tau'' G_1 \mid = 3 \mid G_1 \mid$. Logo $(\sum x_g)a^{k_0} = 0$ e assim, $\alpha \in \langle a^{k_1}\left(\frac{1-d}{2}\right)e_1 \rangle$, mas $w(\alpha) = 3 \mid G_1 \mid$ e $w(\langle a^{k_1}\left(\frac{1-d}{2}\right)e_1 \rangle) = 4 \mid G_1 \mid$, o que é um absurdo.

Portanto, $w(C) \geq 4 \mid G_1 \mid$ e assim temos $w(C) = 4 \mid G_1 \mid$.

■

Teorema 4.1.9 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_i}\left(\frac{1+d}{2}\right)e_i \rangle \oplus \langle a^{k_j}\left(\frac{1-d}{2}\right)e_i \rangle$, onde $0 < i < j \leq n$, $0 \leq k_i, k_j < t$, então $w(C) = 2 \mid G_j \mid$.*

Prova: Seja $k = \min\{k_i, k_j\}$. Então

$$C \subset \langle a^k \left(\frac{1+d}{2}\right) e_i \rangle \oplus \langle a^k \left(\frac{1-d}{2}\right) e_i \rangle \subset \langle a^k \left(\frac{1+d}{2}\right) \widehat{G}_i \rangle + \langle a^k \left(\frac{1-d}{2}\right) \widehat{G}_i \rangle \subset \langle a^k \widehat{G}_i \rangle .$$

Sejam $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_i em G e $\alpha \in C$. Podemos escrever α como $\alpha = (x_1\tau_1 + \dots + x_n\tau_n + x'_1d\tau_1 + \dots + x'_nd\tau_n)a^k\widehat{G}_i$, onde x_j e $x'_j \in R$.

Suponhamos que exista apenas um coeficiente y de α tal que $ya^k \neq 0$. Então existem β_1 e $\beta_2 \in RA$ tais que

$$\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_i = \beta_1a^{k_i}\left(\frac{1+d}{2}\right)e_i + \beta_2a^{k_j}\left(\frac{1-d}{2}\right)e_i,$$

onde $\zeta_\tau = 0$ ou 1 e $\tau \in \Gamma$.

Multiplicando a igualdade acima por \widehat{G}_{i-1} , temos $(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{i-1} = 0$. Assim, $ya^k = 0$, o que contradiz nossa hipótese inicial. Portanto $w(C) \geq 2 \mid G_i \mid$.

Agora, tomemos $g_0 \in G_{i-1}/G_i$ e considere o elemento $\alpha = (1 - g_0)a^k\widehat{G}_i$, onde $k = \max\{k_i, k_j\}$. Temos que $w(\alpha) = 2 \mid G_i \mid$. Podemos reescrever α como:

$$\alpha = (1 - g_0)a^k\widehat{G}_i = (1 - g_0)a^k(\widehat{G}_{i-1} - \widehat{G}_i + \widehat{G}_{i-1}) = (1 - g_0)a^k(e_i + \widehat{G}_{i-1}).$$

Como $(1 - g_0)\widehat{G}_{i-1} = 0$, pois $g_0 \in G_{i-1}$, então

$$\alpha = (1 - g_0)a^k e_i = (1 - g_0)a^k \left(\frac{1+d}{2}\right) e_i + (1 - g_0)a^k \left(\frac{1-d}{2}\right) e_i \in C.$$

Logo $w(C) \leq 2 \mid G_i \mid$ e, portanto, $w(C) = 2 \mid G_i \mid$. ■

Agora generalizaremos estes casos e calcularemos outros possíveis casos onde possam ocorrer somas dos idempotentes $\left(\frac{1+d}{2}\right)e_0$ e $\left(\frac{1-d}{2}\right)e_0$, $\left(\frac{1+d}{2}\right)e_i$ e $\left(\frac{1-d}{2}\right)e_i$.

Teorema 4.1.10 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_{i_1}} \left(\frac{1\pm d}{2}\right) e_{i_1} \rangle \oplus \dots \oplus \langle a^{k_{i_l}} \left(\frac{1\pm d}{2}\right) e_{i_l} \rangle$, onde $0 \leq k_{i_j} < t$, $1 \leq j \leq l$, $0 < i_1 \leq i_2 \leq \dots \leq$*

$i_{l-1} < i_l$, e existe pelo menos um idempotente $(\frac{1+d}{2})e_i$ e $(\frac{1-d}{2})e_j$ como geradores dos ideais somandos de C , então $w(C) = 4 \mid G_{i_l} \mid$.

Prova: Observe que $w(C) \leq w(\langle a^{k_{i_l}}(\frac{1+d}{2})e_{i_l} \rangle) = 4 \mid G_{i_l} \mid$.

Temos $C \subset \langle a^k \widehat{G}_{i_l} \rangle$, onde $k = \min\{k_{i_1}, \dots, k_{i_l}\}$. Sejam $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_{i_l} em G e $\alpha \in C$. Podemos escrever $\alpha = (x_1\tau_1 + \dots + x_n\tau_n + x'_1d\tau_1 + \dots + x'_nd\tau_n)a^k \widehat{G}_{i_l}$, onde x_j e $x'_j \in R$. Como $\alpha \in C$, existem $\beta_1, \dots, \beta_l \in RA$ tais que

$$\alpha = \beta_1 a^{k_{i_1}} \left(\frac{1 \pm d}{2}\right) e_{i_1} + \dots + \beta_l a^{k_{i_l}} \left(\frac{1 \pm d}{2}\right) e_{i_l}.$$

Suponhamos que exista apenas um coeficiente y de α tal que $ya^k \neq 0$. Então $\alpha = (yd^{\zeta_\tau}\tau)a^k \widehat{G}_{i_l} = \beta_1 a^{k_{i_1}} \left(\frac{1 \pm d}{2}\right) e_{i_1} + \dots + \beta_l a^{k_{i_l}} \left(\frac{1 \pm d}{2}\right) e_{i_l}$, onde $\tau \in \Gamma$.

Multiplicando a igualdade acima por $\widehat{G}_{i_{l-1}}$, temos $(yd^{\zeta_\tau}\tau)a^k \widehat{G}_{i_{l-1}} = 0$. Assim, $ya^k = 0$, o que contradiz nossa hipótese.

Suponhamos agora que existam apenas dois coeficientes y_1, y_2 de α tais que $y_1 a^k \neq 0$ e $y_2 a^k \neq 0$. Assim, podemos escrever α como

$$\alpha = (y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau') a^k \widehat{G}_{i_l} = \beta_1 a^{k_{i_1}} \left(\frac{1 \pm d}{2}\right) e_{i_1} + \dots + \beta_l a^{k_{i_l}} \left(\frac{1 \pm d}{2}\right) e_{i_l}, \quad (4.5)$$

onde $\zeta_\tau, \zeta_{\tau'} = 0$ ou 1 e $\tau, \tau' \in \Gamma$. Suponhamos que o idempotente gerador do último ideal somando de C seja $(\frac{1+d}{2})e_{i_l}$, caso contrário, refaça o mesmo que foi feito abaixo para $(\frac{1-d}{2})e_{i_l}$.

Multiplicando a igualdade (4.5) por $(\frac{1-d}{2})$, temos

$$(y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau') a^k \left(\frac{1-d}{2}\right) \widehat{G}_{i_l} = \beta_1 a^{k_{j_1}} \left(\frac{1-d}{2}\right) e_{j_1} + \dots + \beta_l a^{k_{j_s}} \left(\frac{1-d}{2}\right) e_{j_s},$$

onde $j_s < i_l$. Assim, $\alpha(\frac{1-d}{2})$ pertence ao código $C' = \langle a^{k_{j_1}}(\frac{1-d}{2})e_{j_1} \rangle \oplus \dots \oplus \langle a^{k_{j_s}}(\frac{1-d}{2})e_{j_s} \rangle$. Mas $w(\alpha(\frac{1-d}{2})) = 4 \mid G_{i_l} \mid$ e $w(C') = 4 \mid G_{j_s} \mid$. Como $\mid G_{i_l} \mid < \mid G_{j_s} \mid$, temos uma contradição.

Suponhamos agora que existam apenas três coeficientes y_1, y_2 e y_3 de α tais que $y_1 a^k \neq 0$,

$y_2 a^k \neq 0$ e $y_3 a^k \neq 0$. Assim, podemos escrever α como

$$\alpha = (y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k \widehat{G}_{i_l} = \beta_1 a^{k_{i_1}} \left(\frac{1 \pm d}{2}\right) e_{i_1} + \dots + \beta_l a^{k_{i_l}} \left(\frac{1 \pm d}{2}\right) e_{i_l}, \quad (4.6)$$

onde $\zeta_\tau, \zeta_{\tau'}, \zeta_{\tau''} = 1$ ou 0 e $\tau, \tau', \tau'' \in \Gamma$.

Suponhamos que o idempotente gerador do ultimo ideal somando de C seja $\left(\frac{1+d}{2}\right)e_{i_l}$, caso contrário, refaça o mesmo que for feito abaixo para $\left(\frac{1-d}{2}\right)e_{i_l}$.

Multiplicando a igualdade (4.6) por $\left(\frac{1-d}{2}\right)$, temos

$$(y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k \left(\frac{1-d}{2}\right) \widehat{G}_{i_l} = \beta_1 a^{k_{j_1}} \left(\frac{1-d}{2}\right) e_{j_1} + \dots + \beta_l a^{k_{j_s}} \left(\frac{1-d}{2}\right) e_{j_s},$$

onde $j_s < i_l$. Assim, $\alpha \left(\frac{1-d}{2}\right)$ pertence ao código $C' = \langle a^{k_{j_1}} \left(\frac{1-d}{2}\right) e_{j_1} \rangle \oplus \dots \oplus \langle a^{k_{j_s}} \left(\frac{1-d}{2}\right) e_{j_s} \rangle$. Mas $w(\alpha \left(\frac{1-d}{2}\right)) = 6 |G_{i_l}|$ e $w(C') = 4 |G_{j_s}|$. Como $4 |G_{j_s}| = 4p^{n-i_l} (p^{i_l-j_s})$ e $j_s < i_l$, temos $(p^{i_l-j_s}) > 3$, logo $6 |G_{i_l}| < 4 |G_{j_s}|$, o que é uma contradição.

Assim, $w(C) \geq 4 |G_{i_l}|$ e, portando, $w(C) = 4 |G_{i_l}|$

■

Teorema 4.1.11 *Considere R e G nas condições da Hipótese B, com $p > 3$. Se o código C é da forma $C = \langle a^{k_{00}} \left(\frac{1+d}{2}\right) e_0 \rangle \oplus \langle a^{k_{01}} \left(\frac{1-d}{2}\right) e_0 \rangle \oplus \langle a^{k_{10}} \left(\frac{1+d}{2}\right) e_1 \rangle \oplus \langle a^{k_{11}} \left(\frac{1-d}{2}\right) e_1 \rangle \oplus \langle a^{k_{20}} \left(\frac{1+d}{2}\right) e_2 \rangle \oplus \langle a^{k_{21}} \left(\frac{1-d}{2}\right) e_2 \rangle \oplus \dots \oplus \langle a^{k_{(j-1)0}} \left(\frac{1+d}{2}\right) e_{j-1} \rangle \oplus \langle a^{k_{(j-1)1}} \left(\frac{1-d}{2}\right) e_{j-1} \rangle \oplus \langle a^{k_j} \left(\frac{1+d}{2}\right) e_j \rangle$, onde $0 < j \leq n$, $0 \leq k_{i0}, k_{i1} \leq t$, para $0 < i \leq j$, $k_j < t$ e k_{00} ou $k_{01} < t$, e existem pelo menos dois ideais da forma $\langle a^{k_r} \left(\frac{1+d}{2}\right) e_r \rangle$ e $\langle a^{k_s} \left(\frac{1-d}{2}\right) e_s \rangle$ não nulos, então $w(C) = 4 |G_j|$.*

Prova: Temos $w(C) \leq 4 |G_j|$ e $C \subset a^k \widehat{G}_j$, onde $k = \min\{k_0, k_1, k_{20}, k_{21}, \dots, k_{(j-1)0}, k_{(j-1)1}, k_j\}$. Sejam $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de

G_j em G e $\alpha \in C$. Então podemos escrever

$$\begin{aligned}\alpha &= (x_1\tau_1 + \dots + x_n\tau_n + x'_1d\tau_1 + \dots + x'_nd\tau_n)a^k\widehat{G}_j \\ &= \beta_{00}a^{k_{00}}\left(\frac{1+d}{2}\right)e_0 + \beta_{01}a^{k_{01}}\left(\frac{1-d}{2}\right)e_0 + \beta_{10}a^{k_{10}}\left(\frac{1+d}{2}\right)e_1 + \beta_{11}a^{k_{11}}\left(\frac{1-d}{2}\right)e_1 + \\ &\quad + \beta_{20}a^{k_{20}}\left(\frac{1+d}{2}\right)e_2 + \beta_{21}a^{k_{21}}\left(\frac{1-d}{2}\right)e_2 + \dots + \beta_j a^{k_j}\left(\frac{1+d}{2}\right)e_j,\end{aligned}$$

onde $\beta_{00}, \beta_{01}, \beta_{10}, \beta_{11}, \dots, \beta_j \in RA$.

Vamos supor que o último ideal é da forma $\langle a^{k_j}\left(\frac{1-d}{2}\right)e_j \rangle$, sendo o cálculo análogo para $\langle a^{k_j}\left(\frac{1+d}{2}\right)e_j \rangle$.

Suponhamos que exista apenas um coeficiente y de α tal que $ya^k \neq 0$. Então $\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_j = \beta_{00}a^{k_{00}}\left(\frac{1+d}{2}\right)e_0 + \beta_{01}a^{k_{01}}\left(\frac{1-d}{2}\right)e_0 + \beta_{10}a^{k_{10}}\left(\frac{1+d}{2}\right)e_1 + \beta_{11}a^{k_{11}}\left(\frac{1-d}{2}\right)e_1 + \beta_{20}a^{k_{20}}\left(\frac{1+d}{2}\right)e_2 + \beta_{21}a^{k_{21}}\left(\frac{1-d}{2}\right)e_2 + \dots + \beta_j a^{k_j}\left(\frac{1-d}{2}\right)e_j$, onde $\tau \in \Gamma$.

Multiplicando a igualdade acima por $\left(\frac{1+d}{2}\right)$, temos $(yd^{\zeta_\tau}\tau)a^k\left(\frac{1+d}{2}\right)\widehat{G}_j = \beta_{00}a^{k_{00}}\left(\frac{1+d}{2}\right)e_0 + \beta_{10}a^{k_{10}}\left(\frac{1+d}{2}\right)e_1 + \dots + \beta_{r0}a^{k_{r0}}\left(\frac{1+d}{2}\right)e_r$, onde $r < j$.

Logo a palavra $(yd^{\zeta_\tau}\tau)a^k\left(\frac{1+d}{2}\right)\widehat{G}_j$ pertence ao código

$$C' = \langle a^{k_{00}}\left(\frac{1+d}{2}\right)e_0 \rangle \oplus \langle a^{k_{10}}\left(\frac{1+d}{2}\right)e_1 \rangle \oplus \dots \oplus \langle a^{k_{r0}}\left(\frac{1+d}{2}\right)e_r \rangle.$$

Temos $w((yd^{\zeta_\tau}\tau)a^k\left(\frac{1+d}{2}\right)\widehat{G}_j) = 2 \mid G_j \mid$ e $w(C') \in \{2 \mid G_r \mid, 4 \mid G_r \mid \text{ ou } \mid A \mid\}$. Como $p > 3$, temos $2 \mid G_j \mid < 2 \mid G_r \mid < 4 \mid G_r \mid < \mid A \mid$. Assim, a palavra $(yd^{\zeta_\tau}\tau)a^k\left(\frac{1+d}{2}\right)\widehat{G}_j = 0$, logo $ya^k = 0$, o que contradiz nossa hipótese inicial.

Suponhamos agora que existam apenas dois coeficientes y_1, y_2 de α tais que $y_1a^k \neq 0$ e $y_2a^k \neq 0$. Então $\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_j = \beta_{00}a^{k_{00}}\left(\frac{1+d}{2}\right)e_0 + \beta_{01}a^{k_{01}}\left(\frac{1-d}{2}\right)e_0 + \beta_{10}a^{k_{10}}\left(\frac{1+d}{2}\right)e_1 + \beta_{11}a^{k_{11}}\left(\frac{1-d}{2}\right)e_1 + \beta_{20}a^{k_{20}}\left(\frac{1+d}{2}\right)e_2 + \beta_{21}a^{k_{21}}\left(\frac{1-d}{2}\right)e_2 + \dots + \beta_j a^{k_j}\left(\frac{1-d}{2}\right)e_j$, onde τ e $\tau' \in \Gamma$ e ζ_τ e $\zeta_{\tau'} = 0$ ou 1 .

Multiplicando a igualdade acima por $\left(\frac{1+d}{2}\right)$, temos

$$(y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau')a^k\left(\frac{1+d}{2}\right)\widehat{G}_j = \beta_{00}a^{k_{00}}\left(\frac{1+d}{2}\right)e_0 + \beta_{10}a^{k_{10}}\left(\frac{1+d}{2}\right)e_1 + \dots + \beta_{j0}a^{k_{j0}}\left(\frac{1+d}{2}\right)e_j,$$

onde $j_l < j$. Logo a palavra $(y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau') a^k (\frac{1+d}{2}) \widehat{G}_j$ pertence ao código $C' = \langle a^{k_{00}} (\frac{1+d}{2}) e_0 \rangle \oplus \langle a^{k_{10}} (\frac{1+d}{2}) e_1 \rangle \oplus \dots \oplus \langle a^{k_{j_l 0}} (\frac{1+d}{2}) e_{j_l} \rangle$. Assim,

$$w((y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau') a^k (\frac{1+d}{2}) \widehat{G}_j) = 4 \mid G_j \mid$$

e

$$w(C') \in \{2 \mid G_{j_l} \mid, 4 \mid G_{j_l} \mid \text{ ou } \mid A \mid\}.$$

Como $p > 3$, temos $4 \mid G_j \mid < 2 \mid G_{j_l} \mid < 4 \mid G_{j_l} \mid < \mid A \mid$. Assim,

$$(y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau') a^k (\frac{1+d}{2}) \widehat{G}_j = 0.$$

Desenvolvendo a igualdade acima, temos $\frac{1}{2}((y_1 \tau + y_2 \tau') a^k \widehat{G}_j + (y_1 \tau + y_2 \tau') a^k d \widehat{G}_j) = 0$.

Como $(y_1 \tau + y_2 \tau') a^k \widehat{G}_j$ e $(y_1 \tau + y_2 \tau') a^k d \widehat{G}_j$ têm suportes disjuntos, temos

$$(y_1 \tau + y_2 \tau') a^k \widehat{G}_j = 0,$$

assim $y_1 a^k = y_2 a^k = 0$, o que contradiz nossa hipótese inicial.

Suponhamos agora que existam apenas três coeficientes y_1, y_2 e y_3 de α tais que $y_1 a^k \neq 0$, $y_2 a^k \neq 0$ e $y_3 a^k \neq 0$. Então $\alpha = (y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k \widehat{G}_j = \beta_{00} a^{k_{00}} (\frac{1+d}{2}) e_0 + \beta_{01} a^{k_{01}} (\frac{1-d}{2}) e_0 + \beta_{10} a^{k_{10}} (\frac{1+d}{2}) e_1 + \beta_{11} a^{k_{11}} (\frac{1-d}{2}) e_1 + \beta_{20} a^{k_{20}} (\frac{1+d}{2}) e_2 + \beta_{21} a^{k_{21}} (\frac{1-d}{2}) e_2 + \dots + \beta_j a^{k_j} (\frac{1-d}{2}) e_j$, onde τ, τ' e $\tau'' \in \Gamma$.

Multiplicando a igualdade acima por $(\frac{1+d}{2})$, temos

$$(y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k (\frac{1+d}{2}) \widehat{G}_j = \beta_{00} a^{k_{00}} (\frac{1+d}{2}) e_0 + \beta_{10} a^{k_{10}} (\frac{1+d}{2}) e_1 + \dots + \beta_{j_l 0} a^{k_{j_l 0}} (\frac{1+d}{2}) e_{j_l},$$

onde $j_l < j$.

Logo a palavra $(y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k (\frac{1+d}{2}) \widehat{G}_j$ pertence ao código

$C' = \langle a^{k_{00}}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_{10}}(\frac{1+d}{2})e_1 \rangle + \dots + \langle a^{k_{j_1 0}}(\frac{1+d}{2})e_{j_1} \rangle$. Assim,

$$w((y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k (\frac{1+d}{2}) \widehat{G}_j) = 6 |G_j|$$

e

$$w(C') \in \{2 |G_{j_i}|, 4 |G_{j_i}| \text{ ou } |A|\}.$$

Como $p > 3$, temos $6 |G_j| < 2 |G_{j_i}| < 4 |G_{j_i}| < |A|$. Assim,

$$(y_1 d^{\zeta_\tau} \tau + y_2 d^{\zeta_{\tau'}} \tau' + y_3 d^{\zeta_{\tau''}} \tau'') a^k (\frac{1+d}{2}) \widehat{G}_j = 0.$$

Desenvolvendo a igualdade acima, temos $\frac{1}{2}((y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \widehat{G}_j + (y_1 \tau + y_2 \tau' + y_3 \tau'') a^k d \widehat{G}_j) = 0$. Como $(y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \widehat{G}_j$ e $(y_1 \tau + y_2 \tau' + y_3 \tau'') a^k d \widehat{G}_j$ têm suportes disjuntos, temos

$$(y_1 \tau + y_2 \tau' + y_3 \tau'') a^k \widehat{G}_j = 0,$$

assim $y_1 a^k = y_2 a^k = y_3 a^k = 0$, o que contradiz nossa hipótese inicial.

Portanto $w(C) \geq 4 |G_j|$ e, como tínhamos $w(C) \leq 4 |G_j|$, obtemos $w(C) = 4 |G_j|$.

■

Nos teoremas anteriores, sempre consideramos o último ideal somando dos códigos como sendo ou $a^{k_1}(\frac{1+d}{2})e_j$ ou $a^{k_2}(\frac{1-d}{2})e_j$. Agora iremos considerar o caso em que existem ambos ideais, ou seja, os geradores do dois últimos ideais dos códigos em questão são $a^{k_{j_0}}(\frac{1+d}{2})e_j$ e $a^{k_{j_1}}(\frac{1-d}{2})e_j$, onde $k_{j_0}, k_{j_1} < t$.

Teorema 4.1.12 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} \rangle \oplus \langle a^{k_{i_2}}(\frac{1+d}{2})e_{i_2} \rangle \oplus \dots \oplus \langle a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} \rangle \oplus \langle a^{k_{i_2}}(\frac{1-d}{2})e_{i_2} \rangle$, onde $0 \leq k_{i_j} < t$, $1 \leq j \leq l$, $0 < i_1 \leq i_2 \leq \dots \leq i_{l-1} < i_l$, então $w(C) = 2 |G_{i_l}|$.*

Prova: Temos $w(C) \leq w(\langle a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} \rangle \oplus \langle a^{k_{i_2}}(\frac{1-d}{2})e_{i_2} \rangle) = 2 |G_{i_l}|$ e $C \subset \langle a^k \widehat{G}_{i_l} \rangle$, onde $k = \min\{k_{i_1}, k_{i_2}, \dots, k_{i_{l-1}}, k_{i_l}\}$. Sejam $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_{i_l} em G e

$\alpha \in C$.

Podemos escrever $\alpha = (x_1\tau_1 + \dots + x_n\tau_n + x'_1d\tau_1 + \dots + x'_nd\tau_n)a^k\widehat{G}_{j_l}$. Como $\alpha \in C = \langle a^{k_{i_1}}(\frac{1\pm d}{2})e_{i_1} \rangle \oplus \langle a^{k_{i_2}}(\frac{1\pm d}{2})e_{i_2} \rangle \oplus \dots \oplus \langle a^{k_{i_1}}(\frac{1\pm d}{2})e_{i_1} \rangle \oplus \langle a^{k_{i_2}}(\frac{1-d}{2})e_{i_2} \rangle$, existem $\beta_1, \dots, \beta_{i_1}, \beta_{i_2} \in RA$ tais que

$$\alpha = \beta_1 a^{k_{i_1}} \left(\frac{1 \pm d}{2} \right) e_{i_1} + \dots + \beta_{i_1} a^{k_{i_1}} \left(\frac{1 + d}{2} \right) e_{i_1} + \beta_{i_2} a^{k_{i_2}} \left(\frac{1 - d}{2} \right) e_{i_2}.$$

Vamos supor que exista apenas um coeficiente y de α , tal que $ya^k \neq 0$. Então $\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_{j_l} = \beta_1 a^{k_{i_1}} \left(\frac{1\pm d}{2} \right) e_{i_1} + \dots + \beta_{i_1} a^{k_{i_1}} \left(\frac{1+d}{2} \right) e_{i_1} + \beta_{i_2} a^{k_{i_2}} \left(\frac{1-d}{2} \right) e_{i_2}$, onde $\zeta_\tau = 0$ ou 1 e $\tau \in \Gamma$.

Multiplicando a igualdade acima por \widehat{G}_{i_1-1} , temos $(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{i_1-1} = 0$. Logo $ya^k = 0$, o que contradiz nossa hipótese, assim $w(C) \geq 2 |G_{i_1}|$. Portanto, $w(C) = 2 |G_{i_1}|$ ■

Teorema 4.1.13 *Considere R e G nas condições da Hipótese B. Se o código C é da forma $C = \langle a^{k_{00}}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_{01}}(\frac{1-d}{2})e_0 \rangle \oplus \langle a^{k_{10}}(\frac{1+d}{2})e_1 \rangle \oplus \langle a^{k_{11}}(\frac{1-d}{2})e_1 \rangle \oplus \langle a^{k_{20}}(\frac{1+d}{2})e_2 \rangle \oplus \langle a^{k_{21}}(\frac{1-d}{2})e_2 \rangle \oplus \dots \oplus \langle a^{k_{j_1}}(\frac{1+d}{2})e_j \rangle \oplus \langle a^{k_{j_2}}(\frac{1-d}{2})e_j \rangle$, onde $0 < j \leq n$, k_{00} ou $k_{01} < t$, e k_{j_1} e $k_{j_2} < t$ então $w(C) = 2 |G_j|$ ou $|G_j|$.*

Prova: Dividiremos a demonstração em duas partes. Vamos supor inicialmente que exista r tal que k_{r_0} ou k_{r_1} seja igual a t e provaremos que $w(C) = 2 |G_j|$ e depois consideraremos o caso em que $k_{i_0}, k_{i_1} < t$, para $0 \leq i \leq j-1$ e provaremos que $w(C) = |G_j|$.

Observe que $w(C) \leq w(\langle a^{k_{j_1}}(\frac{1+d}{2})e_j \rangle \oplus \langle a^{k_{j_2}}(\frac{1-d}{2})e_j \rangle) = 2 |G_j|$. Falta provar que $w(C) \geq 2 |G_j|$.

Temos $C \subset \langle a^k\widehat{G}_j \rangle$, onde $k = \min\{k_{00}, k_{01}, k_{10}, k_{11}, \dots, k_j\}$. Sejam $\Gamma = \{\tau_1, \dots, \tau_n\}$ um transversal de G_j em G e $\alpha \in C$.

Podemos escrever $\alpha = (x_1\tau_1 + \dots + x_n\tau_n + x'_1d\tau_1 + \dots + x'_nd\tau_n)a^k\widehat{G}_j$.

Como $\alpha \in C = \langle a^{k_{00}}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_{01}}(\frac{1-d}{2})e_0 \rangle \oplus \langle a^{k_{10}}(\frac{1+d}{2})e_1 \rangle \oplus \langle a^{k_{11}}(\frac{1-d}{2})e_1 \rangle \oplus \langle a^{k_{20}}(\frac{1+d}{2})e_2 \rangle \oplus \langle a^{k_{21}}(\frac{1-d}{2})e_2 \rangle \oplus \dots \oplus \langle a^{k_{j_1}}(\frac{1+d}{2})e_j \rangle \oplus \langle a^{k_{j_2}}(\frac{1-d}{2})e_j \rangle$, existem

$\beta_{00}, \beta_{01}, \dots, \beta_{j_1}, \beta_{j_2} \in RA$, tal que $\alpha = \beta_{00}a^{k_{00}}(\frac{1+d}{2})e_0 + \beta_{01}a^{k_{01}}(\frac{1-d}{2})e_0 + \dots + \beta_{j_1}(\frac{1+d}{2})a^{k_{j_1}}e_j + \beta_{j_2}(\frac{1-d}{2})a^{k_{j_2}}e_j$.

Vamos supor que exista apenas um coeficiente y de α tal que $ya^k \neq 0$. Então

$$\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_j = \beta_{00}a^{k_{00}}(\frac{1+d}{2})e_0 + \beta_{01}a^{k_{01}}(\frac{1-d}{2})e_0 + \dots + \beta_{j_1}(\frac{1+d}{2})a^{k_{j_1}}e_j + \beta_{j_2}(\frac{1-d}{2})a^{k_{j_2}}e_j,$$

onde $\tau \in \Gamma$. Agora vamos supor, sem perda de generalidade, que i é o menor índice tal que $k_{i0} = t$ e, assim, $a^{k_{i0}} = 0$. Multiplicando a igualdade acima por $\frac{1+d}{2}\widehat{G}_i$, temos:

$$(yd^{\zeta_\tau}\tau)a^k(\frac{1+d}{2})\widehat{G}_i = \beta_{00}a^{k_{00}}(\frac{1+d}{2})e_0 + \beta_{10}a^{k_{10}}(\frac{1+d}{2})e_1 + \dots + \beta_{i-1}a^{k_{i-10}}(\frac{1+d}{2})e_{i-1}.$$

Se $i = 0$, então $(yd^{\zeta_\tau}\tau)a^k(\frac{1+d}{2})\widehat{G}_i = 0$ e assim $ya^k = 0$, o que contradiz nossa hipótese.

Se $i > 0$, a palavra $(yd^{\zeta_\tau}\tau)a^k(\frac{1+d}{2})\widehat{G}_i$ pertence ao código $C' = \langle a^{k_{00}}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_{10}}(\frac{1+d}{2})e_1 \rangle \oplus \dots \oplus \langle a^{k_{i-10}}(\frac{1+d}{2})e_{i-1} \rangle$. O menor peso possível para C' é $2 \mid G_{i-1} \mid$, mas o peso de $(yd^{\zeta_\tau}\tau)a^k(\frac{1+d}{2})\widehat{G}_i$ é $4 \mid G_i \mid$ que é menor que $2 \mid G_{i-1} \mid$, pois $p > 2$. Assim, temos uma contradição. Portanto, $w(C) \geq 2 \mid G_j \mid$.

Suponhamos agora $k_{i0}, k_{i1} < t$, para $0 \leq i \leq j-1$. Temos $C \subset \langle \widehat{G}_j \rangle$. Portanto, $w(C) \geq w(\langle \widehat{G}_j \rangle) = \mid G_j \mid$.

Agora, seja $k = \max\{k_{00}, k_{01}, \dots, k_{j-10}, k_{j-11}, k_j\}$. Assim,

$$\begin{aligned} \langle a^k\widehat{G}_j \rangle &= \langle a^k((\widehat{G}_j - \widehat{G}_{j-1}) + (\widehat{G}_{j-1} - \widehat{G}_{j-2}) + \dots + (\widehat{G}_1 - \widehat{G}_0) + \widehat{G}_0) \rangle \\ &= \langle a^k(e_j + e_{j-1} + \dots + e_1 + e_0) \rangle \\ &= \langle a^k(\frac{1+d}{2})e_0 + a^k(\frac{1-d}{2})e_0 + \dots + a^k(\frac{1+d}{2})e_j + a^k(\frac{1-d}{2})e_j \rangle \\ &\subset \langle a^{k_{00}}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_{01}}(\frac{1-d}{2})e_0 \rangle \oplus \langle a^{k_{10}}(\frac{1+d}{2})e_1 \rangle \oplus \langle a^{k_{11}}(\frac{1-d}{2})e_1 \rangle \oplus \dots \oplus \\ &\quad \oplus \langle a^{k_{j_1}}(\frac{1+d}{2})e_j \rangle \oplus \langle a^{k_{j_2}}(\frac{1-d}{2})e_j \rangle \\ &= C. \end{aligned}$$

Logo $\mid G_j \mid = w(\langle a^k\widehat{G}_j \rangle) \geq w(C)$. Portanto, $w(C) = \mid G_j \mid$. ■

Agora estamos interessados em calcular o número de palavras de um dado código. Iniciaremos então o cálculo para os ideais $\langle a^k(\frac{1+d}{2})e_i \rangle$.

Teorema 4.1.14 *Se o código C é da forma $C = \langle a^k(\frac{1+d}{2})e_i \rangle$, então o número de palavras de C é $|\langle a^k(\frac{1+d}{2})e_i \rangle| = |\overline{R}|^{(t-k)(p^i-p^{i-1})}$, se $i > 0$ e $|\langle a^k(\frac{1+d}{2})e_0 \rangle| = |\overline{R}|^{t-k}$.*

Prova: Observe que se $i > 0$, então

$$a^k\left(\frac{1+d}{2}\right)e_i = a^k\left(\frac{1+d}{2}\right)(\widehat{G}_i - \widehat{G}_{i-1}).$$

Logo

$$a^k\left(\frac{1+d}{2}\right)\widehat{G}_i = a^k\left(\frac{1+d}{2}\right)e_i + a^k\left(\frac{1+d}{2}\right)\widehat{G}_{i-1}.$$

Como

$$a^k\left(\frac{1+d}{2}\right)e_i \cdot a^k\left(\frac{1+d}{2}\right)\widehat{G}_{i-1} = 0,$$

temos que

$$RAa^k\left(\frac{1+d}{2}\right)\widehat{G}_i = RAa^k\left(\frac{1+d}{2}\right)e_i \oplus RAa^k\left(\frac{1+d}{2}\right)\widehat{G}_{i-1}.$$

Assim,

$$|RAa^k\left(\frac{1+d}{2}\right)e_i| = \frac{|RAa^k\left(\frac{1+d}{2}\right)\widehat{G}_i|}{|RAa^k\left(\frac{1+d}{2}\right)\widehat{G}_{i-1}|}.$$

Agora iremos calcular $|RAa^k\left(\frac{1+d}{2}\right)\widehat{G}_i|$.

Considere

$$\begin{aligned} \psi : RA &\rightarrow RAa^k. \\ \alpha &\mapsto \alpha a^k \end{aligned} \tag{4.7}$$

Claramente ψ é um epimorfismo de grupos aditivos. O núcleo de ψ é dado por

$$\ker(\psi) = \{\alpha \in RA; \alpha a^k = 0\}.$$

Pelo Lema 2.1.6, temos que $\alpha a^k = 0$ se, e somente se, $\alpha \in \langle a^{t-k} \rangle A$. Portanto,

$$RAa^k \simeq \frac{RA}{\langle a^{t-k} \rangle A}.$$

Como $\frac{RA}{\langle a^{t-k} \rangle A} \simeq (\frac{R}{\langle a^{t-k} \rangle})A$, temos,

$$|RAa^k(\frac{1+d}{2})\widehat{G}_i| = |(\frac{R}{\langle a^{t-k} \rangle})A(\frac{1+d}{2})\widehat{G}_i|.$$

Agora considere $R' = (\frac{R}{\langle a^{t-k} \rangle})$ e observe que

$$R'A(\frac{1+d}{2})\widehat{G}_i = \{(\sum_{g \in G} x_g g + \sum_{h \in G} y_h dh)(\frac{1+d}{2})\widehat{G}_i; x_g, y_h \in R', g \in G, d \in B\}.$$

Como $d \cdot \frac{1+d}{2} = \frac{1+d}{2}$, podemos escrever $R'A(\frac{1+d}{2})\widehat{G}_i$ como

$$R'A(\frac{1+d}{2})\widehat{G}_i = \{(\sum_{g \in G} x_g g)(\frac{1+d}{2})\widehat{G}_i; x_g \in R', g \in G, d \in B\}.$$

Considere

$$\begin{aligned} \Phi : R'A(\frac{1+d}{2})\widehat{G}_i &\rightarrow R'G\widehat{G}_i. \\ (\sum_{g \in G} x_g g)(\frac{1+d}{2})\widehat{G}_i &\mapsto (\sum_{g \in G} x_g g)\widehat{G}_i \end{aligned}$$

A aplicação Φ esta bem definida. De fato, se consideramos $\alpha = \alpha_1 \cdot (\frac{1+d}{2}) = \beta_1 \cdot (\frac{1+d}{2}) = \beta$, onde $\alpha_1, \beta_1 \in R'A\widehat{G}_i$, temos $\alpha_1 = \beta_1$ e, assim, $\Phi(\alpha) = \Phi(\beta)$.

Claramente Φ é um isomorfismo de anéis. Portanto,

$$|R'A(\frac{1+d}{2})\widehat{G}_i| = |R'G\widehat{G}_i| = |R'(G/G_i)| = |R'|_{\frac{|G|}{|G_i|}} = |R'|^{p^i}.$$

Logo

$$|R'A(\frac{1+d}{2})e_i| = |R'|^{p^i - p^{i-1}} = \left(\frac{|R|}{|\langle a^{t-k} \rangle|}\right)^{p^i - p^{i-1}} = \left(\frac{|\bar{R}|^t}{|\bar{R}|^k}\right)^{p^i - p^{i-1}} = |\bar{R}|^{(t-k)(p^i - p^{i-1})}.$$

Agora iremos calcular $|RAa^{k_0}(\frac{1+d}{2})e_0|$. Por (4.7), temos

$$|RAa^{k_0}(\frac{1+d}{2})e_0| = \left|\left(\frac{R}{\langle a^{t-k_0} \rangle}\right)A(\frac{1+d}{2})e_0\right|.$$

Denotemos $\left(\frac{R}{\langle a^{t-k_0} \rangle}\right)$ por R' . Considere

$$\begin{aligned} \Phi : R'A(\frac{1+d}{2})\widehat{G} &\rightarrow R'G\widehat{G}. \\ \left(\sum_{g \in G} x_g\right)\left(\frac{1+d}{2}\right)\widehat{G} &\mapsto \left(\sum_{g \in G} x_g\right)\widehat{G} \end{aligned}$$

Claramente Φ é um isomorfismo entre os anéis $R'A(\frac{1+d}{2})\widehat{G}$ e $R'G\widehat{G}$. Logo,

$|RAa^{k_0}(\frac{1+d}{2})e_0| = \left|\left(\frac{R}{\langle a^{t-k_0} \rangle}\right)A(\frac{1+d}{2})e_0\right| = |R'G\widehat{G}|$. Como

$$|R'G\widehat{G}| = |R'| \text{ e } |R'| = |\bar{R}|^{t-k_0},$$

segue que $|\langle a^{k_0}(\frac{1+d}{2})e_0 \rangle| = |\bar{R}|^{t-k_0}$. ■

Corolário 4.1.15 *Se I é um ideal de RG da forma*

$$I = \langle a^{k_{00}}(\frac{1+d}{2})e_0 \rangle \oplus \langle a^{k_{01}}(\frac{1-d}{2})e_0 \rangle \oplus \dots \oplus \langle a^{k_{m0}}(\frac{1+d}{2})e_m \rangle \oplus \langle a^{k_{m1}}(\frac{1-d}{2})e_m \rangle,$$

então

$$|I| = |\bar{R}|^{\left[\sum_{j=1}^m (2t - k_{j0} - k_{j1})(p^j - p^{j-1}) + (2t - k_{00} - k_{01})\right]}.$$

Exemplo 4.1.16 *Neste exemplo vamos considerar $p = 3$, $n = 2$ e $R = \mathbb{Z}_{25}$. Com isso, temos*

$G = \langle g_0; g_0^{18} = 1 \rangle$ e $|\bar{R}| = 5$. Como $o(5) = \phi(9)$ em $U(\mathbb{Z}_{18})$, segue-se que

$e_i = \left(\frac{1 \pm d}{2}\right) e_i$, com $e_i = \widehat{G}_1 - \widehat{G}_{i-1}$, para $i = 0, 1, 2$ são os idempotentes primitivos de $\mathbb{Z}_{25}G$, onde

$$G_i = \langle g_0^{3^i} \rangle.$$

Vamos analisar o peso de alguns códigos e o valor dos seus limitantes.

<i>Código</i>	<i>Peso</i>	<i>Limitante do Peso</i>
$C_1 = \left(\frac{1 \pm d}{2}\right) e_1$	$4 \mid G_1 = 12$	17
$C_2 = \left(\frac{1 \pm d}{2}\right) e_2$	$4 \mid G_2 = 4$	13
$C_3 = \left(\frac{1+d}{2}\right) e_0 \oplus \left(\frac{1-d}{2}\right) e_1$	$4 \mid G_1 = 12$	16
$C_4 = \left(\frac{1 \pm d}{2}\right) e_0 \oplus \left(\frac{1 \pm d}{2}\right) e_2$	$4 \mid G_2 = 4$	12
$C_5 = \left(\frac{1 \pm d}{2}\right) e_1 \oplus \left(\frac{1 \pm d}{2}\right) e_2$	$4 \mid g_2 = 4$	11

4.2 Códigos Livres de Comprimento $2p^n$ Sobre Anéis de Cadeia

Nesta seção caracterizaremos códigos livres de comprimento $2p^n$ sobre anéis de cadeia. Isto será feito de modo análogo aos códigos livres de comprimento p^n sobre anéis de cadeia. Iremos considerar A um grupo cíclico de ordem $2p^n$, R anel de cadeia com $\text{mdc}(|R|, |A|) = 1$ e os idempotentes primitivos ortogonais $\left(\frac{1 \pm d}{2}\right) e_i$, com $0 \leq i \leq n$.

Teorema 4.2.1 *Seja γ um transversal de G_{i-1} em G e τ um transversal de G_i em G_{i-1} . Então $RA\left(\frac{1 \pm d}{2}\right) e_i$ é um código livre com base*

$$\mathcal{B} = \left\{ c(1-b) \left(\frac{1 \pm d}{2}\right) \widehat{G}_i \mid c \in \gamma, b \in \tau \setminus \{1\} \right\}$$

sobre R , onde o sinal positivo nos elementos da base é referente ao ideal $RA\left(\frac{1+d}{2}\right) e_i$ e o sinal negativo é referente ao ideal $RA\left(\frac{1-d}{2}\right) e_i$.

Prova: Faremos a demonstração de que o código $RA(\frac{1+d}{2})e_i$ é livre. A demonstração de que $RA(\frac{1-d}{2})e_i$ é livre é análoga. Primeiramente vamos provar que os elementos de \mathcal{B} pertencem ao código.

- 1) Para $b \in \tau \setminus \{1\}$, temos $(1-b)(\frac{1+d}{2})\widehat{G}_{i-1} = (\frac{1+d}{2})\widehat{G}_{i-1} - (\frac{1+d}{2})b\widehat{G}_{i-1} = 0$, pois $b \cdot \widehat{G}_{i-1} = \widehat{G}_{i-1}$.
- 2) $c(1-b)(\frac{1+d}{2})\widehat{G}_i = c(1-b)(\frac{1+d}{2})(\widehat{G}_i - \widehat{G}_{i-1} + \widehat{G}_{i-1}) = c(1-b)(\frac{1+d}{2})e_i + c(1-b)(\frac{1+d}{2})\widehat{G}_{i-1} = c(1-b)(\frac{1+d}{2})e_i$. Portanto, $\mathcal{B} \subset RA(\frac{1+d}{2})e_i$.

Agora, mostraremos que os elementos de \mathcal{B} são linearmente independentes.

Sejam $x_{cb} \in R$, onde $c \in \gamma$ e $b \in \tau \setminus \{1\}$ são tais que

$$\sum_{c \in \gamma} \sum_{b \in \tau \setminus \{1\}} x_{cb} c(1-b) \left(\frac{1+d}{2}\right) \widehat{G}_i = 0.$$

Desenvolvendo a igualdade acima temos

$$\begin{aligned} 0 &= \sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} c(1-b) \left(\frac{1+d}{2}\right) \widehat{G}_i \right) \\ &= \sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} c \left(\frac{1+d}{2}\right) \widehat{G}_i \right) - \sum_{c \in \gamma} \sum_{b \in \tau} x_{cb} cb \left(\frac{1+d}{2}\right) \widehat{G}_i \\ &= \frac{1}{2} \left(\sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} c \widehat{G}_i \right) - \sum_{c \in \gamma} \sum_{b \in \tau} x_{cb} cb \widehat{G}_i \right) + \frac{1}{2} \left(\sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} dc \widehat{G}_i \right) - \sum_{c \in \gamma} \sum_{b \in \tau} x_{cb} dcb \widehat{G}_i \right). \end{aligned}$$

O que faremos agora será analisar cada elemento deste somatório. É claro que os elementos do somatório $\left(\sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} c \widehat{G}_i \right) - \sum_{c \in \gamma} \sum_{b \in \tau} x_{cb} cb \widehat{G}_i \right)$ têm suporte disjunto com os elementos do somatório $\left(\sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} dc \widehat{G}_i \right) - \sum_{c \in \gamma} \sum_{b \in \tau} x_{cb} dcb \widehat{G}_i \right)$. Assim,

$$\left(\sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} c \widehat{G}_i \right) - \sum_{c \in \gamma} \sum_{b \in \tau} x_{cb} cb \widehat{G}_i \right) = \left(\sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} dc \widehat{G}_i \right) - \sum_{c \in \gamma} \sum_{b \in \tau} x_{cb} dcb \widehat{G}_i \right) = 0.$$

Provaremos que os elementos do somatório $\left(\sum_{c \in \gamma} \left(\sum_{b \in \tau} x_{cb} c \widehat{G}_i \right) - \sum_{c \in \gamma} \sum_{b \in \tau} x_{cb} cb \widehat{G}_i \right)$ têm suporte disjunto. Para isso, provaremos que, para cada c, b fixos, o elemento $cb \widehat{G}_i$ tem suporte

disjunto de qualquer outro elemento nesta combinação linear. Como $b \in \tau$, então \widehat{G}_i e $b\widehat{G}_i$ têm suportes disjuntos. Logo $c\widehat{G}_i$ e $cb\widehat{G}_i$ têm suporte disjunto. É claro que se $c_j \neq c_k$, então $c_j\widehat{G}_i$ e $c_k\widehat{G}_i$ têm suportes disjuntos. Como τ é um transversal de G_i em G_{i-1} , temos que para $b_j \neq b_k \in \tau$, $c_j b_j \widehat{G}_i$ e $c_k b_k \widehat{G}_i$ têm suportes disjuntos. Portanto, $x_{cb} = 0$, $\forall c \in \gamma$ e $b \in \tau$.

Pelo Teorema 4.1.14, o número de elementos do código $RA(\frac{1+d}{2})e_i$ é dado por

$$|\overline{R}|^{t(p^i - p^{i-1})} = |R|^{(p^i - p^{i-1})}.$$

O número de elementos do código gerado por \mathcal{B} sobre R é dado por $|R|^{(|\gamma| \cdot (|\tau| - 1))}$.

$$(|\gamma| \cdot (|\tau| - 1)) = \frac{|G|}{|G_{i-1}|} \cdot \left(\frac{|G_{i-1}|}{|G_i|} - 1 \right) = (p^i - p^{i-1}).$$

Como o código gerado por \mathcal{B} está contido em $RA(\frac{1+d}{2})e_i$ e possuem o mesmo número de elementos, eles são iguais. Assim $RA(\frac{1+d}{2})e_i$ é um código livre com base \mathcal{B} .

■

É claro que se o código C é da forma $C = RAa^k(\frac{1+d}{2})e_i$, onde $0 < k < t$, então C não é livre, pois $\alpha \cdot a^{t-k} \cdot a^k(\frac{1+d}{2})e_i = 0$, para todo $\alpha \in RA$.

CAPÍTULO 5

Conclusões Finais

Em [10], Dinh e López-Permouth caracterizaram todos os códigos cíclicos de comprimento n sobre anéis de cadeia R , onde $|R| = q^k$ e $q \nmid n$ da seguinte forma:

Seja $x^n - 1 = f_0 \dots f_m$ a representação de $x^n - 1$ como produto de polinômios básico irreduzíveis coprimos dois a dois. Então qualquer ideal em $\frac{R[x]}{\langle x^n - 1 \rangle}$ é da forma $\langle a^j \widehat{f}_i + \langle x^n - 1 \rangle \rangle$, onde $0 \leq j \leq t$ e $0 \leq i \leq m$.

A seguir, vamos enunciar um teorema que foi muito utilizado no artigo [10].

Teorema 5.0.2 (Teorema 3.4) *Seja C um código cíclicos de comprimento n sobre um anel de cadeia finito R (R têm ideal maximal $\langle a \rangle$, com t o índice de nilpotência de a). Então existe uma única família de polinômios $F_0, F_1, \dots, F_t \in R[x]$, mônicos e coprimos dois a dois tais que $F_0 F_1 \dots F_t = x^n - 1$ e $C = \langle \widehat{F}_1, a\widehat{F}_2, \dots, a^{t-1}\widehat{F}_t \rangle$.*

Para demonstrar tal teorema, Dinh e López-Permouth assumiram que poderiam escrever o código C da seguinte forma:

$$\begin{aligned}
C = & \langle \widehat{f}_{k_1+1} \rangle \oplus \dots \oplus \langle \widehat{f}_{k_1+k_2} \rangle \oplus \langle a\widehat{f}_{k_1+k_2+1} \rangle \oplus \dots \oplus \langle a\widehat{f}_{k_1+k_2+k_3} \rangle \oplus \dots \oplus \\
& \oplus \langle a^{t-1}\widehat{f}_{k_1+\dots+k_t+1} \rangle \oplus \dots \oplus \langle a^{t-1}\widehat{f}_m \rangle,
\end{aligned} \tag{5.1}$$

onde $k_1, \dots, k_t \geq 0$ e $k_1 + \dots + k_t + 1 \leq m$.

Depois, foram definidos os polinômios F_i 's da seguinte forma:

Sejam $k_0 = 0$ e k_{t+1} um inteiro não negativo, tais que $k_1 + \dots + k_{t+1} = m$. Para $i = 0, \dots, t$ defina

$$F_i = f_{k_0+\dots+k_i+1} \dots f_{k_0+\dots+k_{i+1}}.$$

Observe porém que um código cíclico qualquer não necessariamente é da forma que foi descrito em 5.1. Por exemplo, $C = \langle \widehat{f}_{k_1+1} \rangle$ (mesma notação que foi utilizada em 5.1) é um código cíclico e desta forma não existiriam F_0, \dots, F_t funções como foi enunciado no teorema. Outro caso em que o código não poderia ser descrito como no Teorema 5.0.2 é quando $t > m$.

Quando provamos todos os resultados de Dinh e López-Permouth [10] referentes à códigos cíclicos, duais e auto-duais, corrigimos este erro dito acima e, além disso, através da abordagem via anéis de grupo, foi possível demonstrar todos os resultados de uma forma mais simples e direta. Conseguimos também resultados novos (Capítulo 3 e 4) que são de grande relevância para a Teoria dos Códigos Corretores de Erros, que são os cálculos dos pesos mínimos de todos os códigos cíclicos sobre anéis de cadeia de comprimento p^n e $2p^n$ e também a caracterização dos códigos cíclicos livres de comprimento p^n e $2p^n$, sendo que quando o comprimento do código é p^n estamos sob as condições da hipótese A e quando o comprimento do código é $2p^n$ estamos sob as condições da hipótese B. Exibimos também bases para ideais que são somando direto de códigos livres.

Neste trabalho, abordamos dois assuntos dentre os três assuntos principais da Teoria dos Códigos Corretores de Erros que são:

- Caracterização de códigos;

- Calculo dos pesos minimais;
- Descrição de algoritmos de decodificação.

Como perspectivas futuras, pretendemos desenvolver um algoritmo de decodificação para códigos cíclicos sobre anéis de cadeia, caracterizar e calcular os pesos mínimos de códigos cíclicos sobre anéis seriais e obter resultados sobre códigos cíclicos duais, auto-ortogonais e auto-duais sobre anéis seriais.

Referências Bibliográficas

- [1] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Westview Press, Massachusetts, 1969. [7](#)
- [2] N. S. Babu, K. H. Zimmermann, *Decoding of linear codes over Galois rings*, IEEE Transactions on Informations Theory, Vol **47** (2001) 1599-1603. [4](#)
- [3] I. F. Blake, R. C. Mullin, *The Mathematical Theory of Coding*, Academic Press, Inc, New York, 1975.
- [4] D. M. Burton, *Elementary Number Theory*, Series in Pure and Applied Mathematics, 4th ed, New York, 1998. [19](#)
- [5] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane, P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math., Vol **29** (1993) 218-222. [3](#)
- [6] A. R. Calderbank, N. J. A. Sloane, *Modular and p -adic codes*, Designs, Codes and Cryptography, Vol **6** (1995) 21-35. [3](#), [4](#), [13](#)
- [7] A. C. A. Campello Jr., G. C. Jorge, S. I. R. Costa, *Decoding q -ary lattices in the Lee metric*, IEEE Information Theory Workshop, (2011) 220-224. [4](#)
- [8] J. H. Conway, N. J. A. Sloane, *Self-dual codes over the integers modulo 4*, J. Combin. Theory Ser. A, Vol **62** (1993) 30-45. [3](#)
- [9] H. Q. Dinh, *Complete distances of all negacyclic codes of length 2^s over \mathbb{Z}_{2^a}* , IEEE transaction on Information Theory, Vol **53** (2007) 147-161. [3](#)

- [10] H. Q. Dinh, S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Transactions on Information Theory, Vol. **50** (2004) 1728-1744. [4](#), [23](#), [32](#), [85](#), [86](#)
- [11] S. T. Dougherty, J. Kim, H. Liu, *Construction of self-dual codes over finite commutative chain rings*, Int. Journal on Information and Coding Theory, (2010). [3](#)
- [12] Y. A. Drodz, V. V. Kirichenko, *Finite Dimensional Algebras*, Springer-Verlag, Berlin, 1991.
- [13] F. Dutra, R. Ferraz, C. Polcino Milies, *Semisimple group codes and dihedral codes*, Algebra and Discrete Mathematics , Vol **3** (2009) 28-48. [46](#)
- [14] A. Hefez, M. L. T. Villela, *Códigos Corretores de Erros*, IMPA, Série de Computação e Matemática, Rio de Janeiro, 2008. [15](#)
- [15] R.A. Ferraz, C. Polcino Milies; *Idempotents in group algebras and minimal abelian codes*, ScienceDirect, Finite Fields and their Applications, Vol **13** (2007) 382-393. [37](#), [38](#), [58](#)
- [16] A. R. Hammons Jr., P.V. Kumar, A.R.Calderbank, N.J.A. Sloane, P. Solé, *The Z_4 -linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Transactions on Information Theory, Vol **40** (1994) 301-319. [3](#)
- [17] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003. [3](#), [13](#)
- [18] N. Jacobson, *Basic Algebra*, W.H.Freeman and Company, San Francisco, 1980. [7](#), [9](#), [45](#), [47](#)
- [19] P. Kanwar, S. R. López-Permouth, *Cyclic codes over the interger modulo p^m* , Finite Fields Appl. Vol **3** (1997) 334-352. [3](#), [4](#)
- [20] Z. H. Liu, *Notes on linear codes over finite chain rings*, Acta Mathematicae Applicatae Sinica, Vol **27** (2011) 141-148. [3](#)
- [21] B. R. MacDonald, *Finite Rings With Identity*, Pure and Applied Mathematics, A Series of Monographs and Textbooks, New York, 1974. [7](#), [10](#), [12](#)
- [22] F. J. MacWilliams, N. J. A. Sloane *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, New York, 1977. [18](#)
- [23] F. Melo, *Sobre Códigos Cíclicos e Abelianos*, Tese de doutorado a ser apresentada ao Instituto de Matemática e Estatística, USP, São Paulo, 2012. [40](#)

-
- [24] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, The Netherlands:North-Holland, Amsterdam, 1998. [16](#)
- [25] E. Martínez-Moro, I. F. Rúa, *On repeated-root multivariable codes over a finite chain ring*, Des. Codes Cryptogr., Vol **45** (2007) 219-227. [3](#)
- [26] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, New York, 1986. [7](#)
- [27] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of numbers*, John Wiley and Sons.Inc, New York, 1991. [19](#)
- [28] G. Norton, A. Sălăgean-Mandache, *On the structure of linear cyclic codes over finite chain rings*, Appl. Algebra Eng. Commun. Comput., Vol **10** (2000) 489-506. [3](#), [4](#)
- [29] G. T .Peterson, *Lifting idempotents in near rings*; Arch. Math., Vol **51** (1988) 208-212.
- [30] V. Pless, Z. Qian, *Cyclic codes and quadratic residue codes over Z_4* , IEEE Transactions on Information Theory, Vol. **42** (1996) 1594-1600. [3](#), [13](#)
- [31] C. Polcino Milies, S. K. Sehgal, *An introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, Netherlands, 2002. [7](#)
- [32] G. Puninski, *Serial Rings*; Kluwer Academic Publishers, Dordrecht, Boston, London, 2001.
- [33] D. Redmond, *Number Theory: An Introduction*, ser. Monographs and Textbooks in Pure and Applied Mathematics. New York, 1996. [19](#)
- [34] S. Roman, *Coding and Information Theory*, Kluwer Academic Publishers, Graduate Texts in Mathematics, Springer, New York, 1992. [16](#), [18](#)
- [35] J. P. O. Santos, *Introdução à Teoria dos Números*, Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2003. [19](#)
- [36] C. Vanden Eynden, *Elementary Number Theory*, McGraw-Hill, 2nd ed. New York, 2001. [19](#)
- [37] Z. Wan, *cyclic codes over Galois rings*, Alg. Colloq., Vol. **6** (1999) 291-304. [3](#)