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.

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.

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

Abstract

Cyclic codes over chain rings

In this paper, we use an approach of group rings to characterize cyclic codes over chain rings, their dual and some conditions on self-dual codes. It also featured free cyclic codes over chain rings and finally we show a formula for the weight of any cyclic code over chain rings.

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

Sumário

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 é um campo de pesquisa muito atual, tanto do ponto de vista científico quanto tecnológico. Pela junção da teoria e de suas aplicações, vem tornando cada vez mais próximo a matemática pura e aplicada.

Descobertas recentes de que bons códigos binários não lineares estão relacionados com códigos lineares sobre Z_4(veja em [5], [8], [14], [25]) têm motivado os estudos de códigos sobre anéis em geral.

Como uma extensão natural de Z_4, em [6], Carlderbank e Sloane determinaram a estrutura de códigos cíclicos sobre Z_{p^m}, depois, Kanwar e López-Permouth em [17] fizeram o mesmo, mas com diferentes demonstrações. Usando as mesmas técnicas que em [17], Wan em [32] estendeu os resultados de Kanwar e López-Permuth para códigos cíclicos sobre anéis de Galois. Em 1999, Norton e Sălăgean-Mandache em [23] estenderam os resultados de [6]

e [17] para códigos cíclicos sobre anéis de cadeia finito. Mais adiante, em 2004, Dinh e López-Permouth em [9], demonstraram os mesmos resultados de [23] de uma forma diferente.

O peso de um código é uma informação fundamental, juntamente com um método de decodificação. Se tratando de códigos cíclicos sobre anéis, tanto o peso, quanto um método de decodificação são difíceis de determinar e vem sendo alvo de estudos na atualidade. Em [7] Campello, Jorge e Costa desenvolveram um método de decodificação de códigos q-ários utilizando 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 algorítimo 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 [9]. Além disso, vamos determinar o peso de qualquer código cíclico sobre anéis de cadeia finito de comprimento p^n e $2p^n$, com algumas hipóteses adicionais.

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 Kanwar e López-Permuth (veja [9]) sobre códigos cíclicos sobre anéis de cadeia de comprimento m e caracterizamos o código dual a um dado código e também os códigos auto-duais.

No capítulo 3, consideremos o caso particular de códigos de comprimento p^n com algumas hipóteses sobre a relação entre q e p^n; 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 finito(ou uni-seriais), caracterizamos os códigos cíclicos livres sobre anéis de cadeia, exibindo duas bases 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, 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 apresentado a demonstração dos resultados.

No que segue, estaremos sempre considerando anéis comutativos com unidade. Portanto, não iremos fazer distinção entre ideais a direita e 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], [16], [18], [21], [26].

Proposição 1.1.1 *Seja R um anel de cadeia finito e comutativo com unidade, com ideal maximal $M =< a >$, e seja t o índice de nilpotência de a em R. Então:*

(a) *Para algum primo q e inteiros positivos k e l $(k \geq l)$, $\mid R \mid = q^k$, $\mid \overline{R} \mid = q^l$ e a característica de R e $\overline{R}$ são potências de q.*

(b) *para $i = 0, 1, 2, ..., t, \mid < a^i > \mid = \mid \overline{R} \mid^{t-i}$. Em particular, $\mid R \mid = \mid \overline{R} \mid^t$, isto é, $k = lt$.*

Definição 1.1.2 *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 $e_i \cdot e_j = 0$ e* ***central*** *se $e \cdot r = r \cdot e$ para todo $r \in R$. Um idempotente e é chamado de* ***primitivo*** *ou* ***minimal*** *se sempre que escrevermos $e = e_1 + e_2$, com e_1 e e_2 idempotentes e $e_1 \cdot e_2 = 0$, então $e_1 = 0$ ou $e_2 = 0$.*

Proposição 1.1.3 *Se $R = I_0 \oplus ... \oplus I_j$ para alguns ideais a direita $I_0, ..., I_j$, então existem idempotentes ortogonais $e_0, e_1, ..., e_j$, tal que $1 = e_0 + e_1 + ... + e_j$ e $e_k R = I_k$, para $k \in \{0, 1, ..., j\}$.*

Definição 1.1.4 *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 $\sum_{i=1}^{n} x_1 x_2 ... x_n$, com $x_i \in I, 1 \leq i \leq n$.*

Definição 1.1.5 *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 1.1.6 *Todo ideal nil de R esta 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 1.1.7 *[[16], Proposição 7.14] Seja R anel comutativo e N um nil ideal em R, e $\overline{e}_j = u + N$ um idempotente de $\overline{R} = \frac{R}{N}$. Então existe um único idempotente e em R tal que $\overline{e} = \overline{e}_j$.*

Definição 1.1.8 *Dois ideais I_1 e I_2 são chamados* ***coprimos****(ou* ***comaximais****) se $I_1 + I_2 =< 1 >$.*

Claramente dois ideais I_1 e I_2 são coprimos se, e somente se, existe $x \in I_1$ e $y \in I_2$ tal que $x + y = 1$.

Proposição 1.1.9 *Se I_1,...,I_n são ideais coprimos aos pares, então $I_1I_2...I_n = I_1 \cap I_2 \cap ... \cap I_n$.*

Teorema 1.1.10 (Teorema Chinês do Resto) *Se I_1,....,I_n são ideais coprimos aos pares de um anel R, então*

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

Definição 1.1.11 *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 1.1.12 *Um anel R é chamado **local** se possui um único ideal maximal.*

Definição 1.1.13 *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.*

Teorema 1.1.14 *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 de ideais principais local*

(iii) *R é um anel de cadeia.*

Definição 1.1.15 *Seja $\overline{R} = \frac{R}{M}$. Seja $^- : R[x] \to \overline{R}[x]$ que aplica r em $r+M$ e x em x. Um polinômio $f \in R[x]$ é chamado **básico irredutível** se $\overline{f}$ é irredutível em $\overline{R}[x]$ e **regular** se ele não é um divisor de zero.*

Proposição 1.1.16 *([18],Teorema $XIII.2(c)$) Seja $f = a_0 + a_1x + ... + a_nx^n \in R[x]$. Então são equivalentes:*

i) f é regular,

ii) $< a_0, ..., a_n >= R$,

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

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

O próximo teorema é chamado de **Lema de Hensel** e pode ser encontrado em [18], Teorema $XIII.4$

Lema 1.1.17 (Lema de Hensel) *Seja f um polinômio sobre R e assuma que $\overline{f} = g_1 g_2 ... g_r$, onde g_1, g_2,...,g_r são polinômios coprimos dois a dois sobre $\overline{R}$. Então existem polinômios f_1,f_2,...,f_r coprimos dois a dois sobre R, tal que $f = f_1 f_2 ... f_r$ e $\overline{f}_i = g_i$, para $i = 1, 2, ..., r$.*

Proposição 1.1.18 *([18], Teorema $XIII.7$) Seja f um polinômio regular. Se f é básico irredutível, então f é irredutível.*

Definição 1.1.19 *Seja G um grupo e R um anel. Um **anel de grupo** de G sobre R, denotado por RG é o conjunto de elemento 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.

No decorrer do texto, denotaremos por C_n, o grupo cíclico de ordem n.

Definição 1.1.20 *Dado um elemento $\alpha = \sum_{g \in G} a_g g \in RG$, definimos o **suporte** de α, denotado por $supp(\alpha)$ como sendo*

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

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

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 possui a estrutura de anel.

- $(\sum_{g\in G} a_g g) + (\sum_{g\in G} b_g g) = \sum_{g\in G}(a_g + b_g)g$;
- $\alpha \cdot \beta = \sum_{g,h\in G} a_g b_h gh$, 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 1.1.21 *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 $\triangle(G) = \{\sum_{g\in G} a_g(g-1) : g \in G, g \neq 1\}$ é chamado de* ***ideal de aumento*** *de RG.*

Proposição 1.1.22 *Se H é um subgrupo de G, então $\triangle(G:H) = \{\sum_{ht} \alpha_{ht} t(h-1) : h \in H, h \neq 1, t \in \tau\}$ é um ideal de RG, onde τ é uma transversal de H em G.*

Corolário 1.1.23 *Se H é um subgrupo normal de G, então*

$$\frac{RG}{\triangle(G:H)} \simeq R(\frac{G}{H}).$$

Proposição 1.1.24 *Se I é um ideal bilateral de um anel R e G um grupo comutativo, então $IG = \{\sum_{g\in G} a_g g \in RG : a_g \in I\}$ é um ideal bilateral de RG e $\frac{RG}{IG} \simeq (\frac{R}{I})G$.*

Proposição 1.1.25 *Seja $\{R_i\}_{i\in I}$ uma família de anéis e seja $R = \oplus_{i\in I} R_i$. Então para qualquer grupo G, $RG \simeq \sum_{i\in I} R_i G$.*

Teorema 1.1.26 (3) *[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 1.1.27 (3) *Sejam G um grupo finito e K um corpo. KG é semisimples se, e somente se, $car(K)$ não divide $|\,G\,|$.*

Corolário 1.1.28 (3) *Se G é um grupo abeliano finito e K um corpo tal que $car(K)$ não divide $|\,G\,|$, então KG é uma soma direta de corpos.*

Teorema 1.1.29 ([18], Teorema VII.8) *Seja e um idempotente não nulo de um anel R. As seguintes condições são equivalentes:*

(1) *e é minimal.*

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

(1) *e é minimal.*

(2) *RGe é um anel local.*

(3) *RGe é indecomponível.*

Teorema 1.1.31 *Seja R um anel com unidade e seja H um subgrupo de um grupo G. Se $|\,H\,|$ é inversível em R, então $e_H = \widehat{H}$ é um idempotente em RG, onde $\widehat{H} = \frac{1}{|H|}\sum_{h\in H} h$. Além disso, se $H \lhd G$, então e_H é central e*

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

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], [25].

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

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 $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n) \in A^n$, a* ***distância de Hamming*** *entre u e v é definida como*

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

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

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

$$d(C) := min\{d(x, y); u, v \in C \backslash \{0\}\},$$

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

Definição 1.2.7 *Dizemos que um código linear é livre se o posto livre é igual ao posto.*

Dentro da classe de códigos lineares, existe uma importante sub classe de códigos conhecida como classe dos códigos cíclicos, que será nosso principal interesse. Códigos cíclicos tem-se mostrado importante 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 [12], onde o alfabeto em questão é um corpo.

Definição 1.2.8 *Um código linear C é chamado* ***cíclico*** *se para toda palavra $\beta = (r_1, ..., r_n) \in C$, sua troca cíclica também esta em C, ou seja, a palavra $\beta' = (r_n, r_1, ..., r_{n-1}) \in C$.*

Definição 1.2.9 *Dado $\beta = (r_1, ..., r_n) \in R^n$, defini-se o* ***peso*** *de β como sendo o número inteiro*

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

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

Definição 1.2.10 *O peso de um código linear C é o inteiro*

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

Proposição 1.2.11 *Seja $C \subset R^n$ um código linear com distância d. Temos que*

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

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

Sejam $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n)$ elementos de R^n. Defini-se o **produto escalar** de u e v como sendo

$$u \cdot v = u_1 v_1 + ... + u_n v_n.$$

Essa operação 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, defini-se*

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

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} . O número de palavras em qualquer código linear de comprimento n sobre R é q^k , para algum inteiro $k \in \{0, ..., \beta n\}$. 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 apresentados adiante, podem ser encontrados em [20], [29].

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 dada por

$$\begin{array}{rcl} \psi : R^n & \to & RG \\ \beta = (r_0, ..., r_{n-1}) & \mapsto & r_0 + r_1 g + r_2 g^2 + ... + r_{n-1} g^{n-1} \end{array}.$$

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 homomorfismo, para todo $r \in R$ e $x \in C$, temos que $r \cdot \psi(x) = \psi(r \cdot x)$. Como C é um R-submódulo de R^n, temos que $r \cdot x \in C$ e portanto $r \cdot \psi(x) \in \psi(C)$. Para provarmos que $\psi(C)$ é um ideal em RG é suficiente provar que $g \cdot \psi(x) \in \psi(C)$, $\forall x \in C$. Seja $x = (x_0, ..., x_{n-1}) \in C$, $g \cdot \psi(x) = g \cdot (x_0 + x_1 g + ... + x_{n-1} g^{n-1}) = x_{n-1} + x_0 g + x_1 g^2 + ... + x_{n-2} g^{n-1}$. Como $x = (x_0, ..., x_{n-1}) \in C$ e C é cíclico, então $(x_{n-1}, x_0, ..., x_{n-2}) \in C$. Portanto,

$$\begin{array}{rcl} \psi((x_{n-1}, x_0, ..., x_{n-2})) & = & x_{n-1} + x_0 g + x_1 g^2 + ... + x_{n-2} g^{n-1} \\ & = & g \cdot \psi(x) \in \psi(C). \end{array}$$

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 $x = (x_0, ..., x_{n-1}) \in C$, então $(x_{n-1}, x_0, ..., x_{n-2}) \in C$. Como $x = (x_0, ..., x_{n-1}) \in C$, então $x_0 + x_1 g + ... + x_{n-1} g^{n-1} \in \psi(C)$. Como $\psi(C)$ é ideal, temos que $g \cdot \psi(x) \in C$. Logo $x_{n-1} + x_0 g + x_1 g^2 + ... + x_{n-2} g^{n-1} \in \psi(C)$. Assim, $(x_{n-1}, ..., x_{n-2}) \in C$.

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

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 $x^n - 1 = \overline{g}_0 ... \overline{g}_m$ a decomposição de $x^n - 1$ em polinômios irredutíveis coprimos dois a dois em $\overline{R}[x]$. Pelo lema de Hensel 1.1.17, sabemos que existem polinômios f_0,...,f_m, coprimos dois a dois em $R[x]$, tal que $x^n - 1 = f_0 ... f_m$. Como f_i é regular para $0 \leq i \leq m$, por 1.1.18, temos que f_i é irredutível.

Sabemos que

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

onde G é um grupo cíclico de ordem n e $x^n - 1 = f_0.f_1...f_m$ é a decomposição de $x^n - 1$ como produto de polinômios irredutíveis coprimos dois a dois em $R[x]$. Pelo Teorema Chinês do Resto (1.1.10), temos que

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

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, onde

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

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

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

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 $C =< p(x) >$ se, e somente se, $p(x)|x^n - 1$.*

Teorema 1.3.3 *Seja $C_1 =< g_1(x) >$ e $C_2 =< g_2(x) >$ códigos cíclicos em R_n. Então, $C_1 \subset C_2$ se, e somente se, $g_2(x)|g_1(x)$.*

Considere a seguinte caracterização para idempotentes minimais e_k's que pode ser encontrada em [3]. Seja G um grupo abeliano de ordem n, tal que $G = S_1 \cup S_2 \cup ... \cup S_r$, onde $S_1 = \{1\}$, $S_2 = \{g_2, g_2^2, G_2^{2^2}, ..., g_2^{2^{k-1}}\}$, onde $g_2 \notin S_1$ e $g_2^{2^k} = g_2$, e continue assim até obter uma decomposição para G. Denotemos por G' o grupo dos caracteres irredutíveis de

G. Considere a seguinte decomposição de $G^{'}$:

$$G^{'} = \sum_{1} \cup \sum_{2} \cup, , , \cup \sum_{r},$$

onde

$$\sum_{i} = \{\mathcal{X}_g \in G^{'} : g \in S_i\},$$

onde $\mathcal{X}_g$ é o caracter correspondente para $g \in G$. Assim,

$$e_k = \sum_{g \in G} [\frac{1}{n} \sum_{\mathcal{X}_h \in \sum_k} \mathcal{X}_h(g^{-1})]g.$$

Uma caracterização semelhante para o idempotente primitivo descrito acima, pode ser encontrado em [29].

Considere a aplicação

$$\begin{array}{rcl} ^* : RG & \to & RG \\ \alpha = a_0 + a_1 g + ... + a_{n-1} g^{n-1} & \mapsto & \alpha^* = a_0 + a_1 g^{-1} + a_2 g^{-2} + ... a_{n-1} g^1 \end{array}.$$

* esta bem definida e é chamada **involução clássica de** RG. Vejamos algumas propriedades de *. Sejam $\alpha = a_0 + a_1 g + ... + a_{n-1} g^{n-1}$, $\beta = b_0 + b_1 g + ... + b_{n-1} g^{n-1} \in RG$ e $r \in R$. Temos que

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

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

Teorema 1.3.4 *Sejam* $\alpha = a_0 + a_1 g + ... + a_{n-1} g^{n-1}$ *e* $\beta = b_0 + b_1 g + ... + b_{n-1} g^{n-1}$. *Então,* $\alpha \cdot \beta = 0$ *em* RG *se, e somente se,* $(a_0, a_1, ..., a_{n-1})$ *é ortogonal em* R^n *a* $(b_{n-1}, b_{n-2}, ..., b_1, b_0)$ *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], [22], [28], [30], [31].

Definição 1.4.1 *Sejam* a *e* m *inteiros relativamente primos, isto é,* $mdc(a, m) = 1$. *Se a congruência quadrática* $x^2 \equiv a (mod m)$ *tem uma solução, então* a *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* $mdc(a, q) = 1$. *Então* a *é um resíduo quadrático ou não resíduo quadrático de* q *quando* $a^{\frac{q-1}{2}} \equiv 1 (mod q)$ *ou* $a^{\frac{q-1}{2}} \equiv -1 (mod q)$, *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* $mdc(a, q) = 1$. *O símbolo de Legendre* $(a|q)$ *é definido por:*

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

a e q são chamados ***numerador*** *e* ***denominador*** *do símbolo* $(a|q)$*, respectivamente.*

Observação 1.4.4 *Pelo critério 1.4.2 e pela definição do símbolo de Legendre 1.4.3, para um inteiro ímpar q e um inteiro a com* $mdc(a,q)=1$*, temos*

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

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* $a \equiv b(modq)$*, então* $(a|q)=(b|q)$*;*

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

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

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

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

Teorema 1.4.6 (Lema de Gauss) *Seja q um primo ímpar e* $mdc(a,q)=1$*. Se k denota o número de inteiros no conjunto* $S=\{a,2a,3a,...,\frac{q-1}{2}a\}$ *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*

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

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

$$(i)\text{-}\ (p|q)(q|p) = \begin{cases} 1, & se\ p \equiv 1(mod4)\ \ ou\ q \equiv 1(mod4) \\ -1 & se\ p \equiv q \equiv 3(mod4). \end{cases}$$

$$(ii)\text{-}\ (p|q) = \begin{cases} (q|p), & se\ p \equiv 1(mod4)\ \ ou\ q \equiv 1(mod4) \\ -(q|p) & se\ p \equiv q \equiv 3(mod4). \end{cases}$$

O lema de Gauss 1.4.6 e a lei da reciprocidade quadrática 1.4.7 nos permite 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:*

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

$$(ii)-\ (-1|q) = \begin{cases} 1, & se\ q \equiv 1(mod4) \\ -1 & se\ q \equiv 3(mod4). \end{cases}$$

$$(iii)-\ (2|q) = \begin{cases} 1, & se\ q \equiv 1(mod8)\ \ ou\ q \equiv 7(mod8) \\ -1 & se\ q \equiv 3(mod8)\ \ ou\ q \equiv 5(mod8). \end{cases}$$

$$(iv)-\ (-2|q) = \begin{cases} 1, & se\ q \equiv 1(mod8)\ \ ou\ q \equiv 3(mod8) \\ -1 & se\ q \equiv 5(mod8)\ \ ou\ q \equiv 7(mod8). \end{cases}$$

$$(v)-\ (5|q) = \begin{cases} 1, & se\ q \equiv 1,9,11,19(mod20) \\ -1 & se\ q \equiv 3,7,13,17(mod20). \end{cases}$$

$$(vi)-\ (6|q) = \begin{cases} 1, & se\ q \equiv 1,5,19,23(mod24) \\ -1 & se\ q \equiv 7,11,13,17(mod24). \end{cases}$$

$$(vii)-\ (7|q) = \begin{cases} 1, & se\ q \equiv 1,3,9,19,25,27(mod28) \\ -1 & se\ q \equiv 5,11,13,15,17,23(mod28). \end{cases}$$

$$(viii)-\ (11|q) = \begin{cases} 1, & se\ q \equiv 1,5,7,9,19,25,35,37,39,43(mod44) \\ -1 & se\ q \equiv 3,13,15,17,21,23,27,29,31,41(mod44). \end{cases}$$

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

$$(ix)-\ (3|q) = \begin{cases} 1, & se\ q \equiv 1(mod12)\ ou\ q \equiv 11(mod12) \\ -1 & se\ q \equiv 5(mod12)\ ou\ q \equiv 7(mod12). \end{cases}$$

$$(x)-\ (-3|q) = \begin{cases} 1, & se\ q \equiv 1(mod6) \\ -1 & se\ q \equiv 5(mod6). \end{cases}$$

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

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

$(i)-$ *para $i = 1,...,r$, $(a|p_i) = 1$;*

$$(ii)-\ a \equiv \begin{cases} 1(mod4), & se\ 4|m\ mas\ 8 \nmid m \\ 1(mod8), & se\ 8|m. \end{cases}$$

CAPÍTULO 2

Caracterização de Códigos Cíclicos sobre Anéis de Cadeia

Neste capítulo iremos identificar todos os possíveis códigos cíclicos C em anéis de grupo com R anel de cadeia finito, comutativo, com unidade, com $\mid R \mid = q^k$ 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 [9], 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; determinaram o número de elementos dos mesmo e exibiram 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 proximo capítulo apresentaremos resultados novos, utilizando a abordagem de anéis de grupo.

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 $\overline{R} = \frac{R}{M}$ é um corpo. Daqui em diante estaremos sempre nos referindo a anéis de cadeia onde $q \nmid | G |$.

Por 1.1.1, sabemos que, $| R | = q^k$, então $car(R)$ é uma potência de q.

A seguir, temos um teorema usado como ferramenta na caracterização dos códigos sobre anéis de cadeia.

Teorema 2.0.12 *Seja R anel de cadeia e M o ideal maximal de R. Então*

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

Prova: Trata-se de um caso particular de 1.1.24.

■

Como estamos considerando que $q \nmid n$, onde $| R | = q^k$ e $| G | = n$, por 1.1.1 temos que $car(\frac{R}{M}) \nmid | G |$. Agora, por 1.1.27, temos que $\left(\frac{R}{M}\right)G$ é semisimples e por 1.1.3, existem idempotentes primitivos ortogonais $\overline{e}_0, ..., \overline{e}_m$ tal que $\overline{R}G = \overline{R}G\overline{e}_0 \oplus ... \oplus \overline{R}G\overline{e}_m$. Por 2.0.12 e 1.1.7, existe uma única família de idempotentes ortogonais $\{e_0, ..., e_m\}$ em RG, tal que $RG = RGe_0 \oplus ... \oplus RGe_m$. Nosso objetivo agora é garantir que $\{e_0, ..., e_m\}$ é um conjunto de idempotentes primitivos ortogonais em RG.

Teorema 2.0.13 *Seja R é anel local com ideal maximal $M =< a >$, com $| R | = q^k$ e G é um grupo cíclico de ordem n, onde $q \nmid n$. Se $\{\overline{e}_o, ..., \overline{e}_m\}$ é o conjunto de idempotentes primitivos ortogonais em $\overline{R}G$, então $\{e_o, ..., e_m\}$ é o conjunto de idempotentes primitivos ortogonais em RG.*

Prova: Considere

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

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

Já sabemos, pelo corolário 1.1.30, que RGe_i é um anel local. No que segue, para simplificar notação, escreveremos os ideais da forma $(RG)ae_i$ como $< ae_i >$.

Teorema 2.0.14 *Seja R anel de cadeia finito, comutativo com unidade, com $\mid R \mid = q^k$, $M =< a >$ ideal maximal e t o índice de nilpotência de a em R. Seja $G =< g_0; g_0^n = 1 >$, onde $q \nmid n$. Se I é um ideal de RGe_i, então I é da forma $I =< a^{k_i}e_i >$ 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. Temos que $\zeta = xe_i$, com $x \in RG$. Como M é ideal maximal de R, temos que $\left(\frac{R}{M}\right)Ge_i$ 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 1.1.28, temos que $\frac{RGe_i}{MGe_i}$ é corpo. Assim, podemos concluir que MGe_i é ideal maximal de RGe_i. Pelo corolário 1.1.30, sabemos que RGe_i é anel local, onde, $\zeta \in MGe_i$. 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, $\zeta = \sum r_g a g e_i = (\sum r_g g)ae_i \in < ae_i >$ e $I \subset < ae_i >$.

Agora seja k o maior inteiro positivo tal que $I \subset < a^k e_i >$. Com isso, existe $\zeta \in I$ tal que ζ não pertence a $< a^{k+1}e_i >$. 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, temos que $\beta = a\beta'$, $\beta' \in RGe_i$ e assim, temos que $\zeta = a^k.a\beta' e_i \in < a^{k+1}e_i >$, contradição. Logo, existe $\gamma \in RGe_i$ tal que $\beta\gamma = e_i$. Portanto, $a^k e_i = a^k \beta\gamma e_i = a^k \beta e_i.\gamma e_i = (\zeta).\gamma e_i \in I$ e com isso concluímos que $I =< a^k e_i >$.

■

Corolário 2.0.15 *O ideal RGe_i é indecomponível em RG e o código gerado por $< a^{t-1}e_i >$ é minimal.*

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

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

Teorema 2.0.16 *Seja R anel de cadeia finito e comutativo, com ideal maximal $M =< a >$, t o índice de nilpotência de a em R, com $\mid R \mid = q^k$ e $G =< g_0; g_0^n = 1 >$, tal que $q \nmid n$. Se I é um ideal de RG, então I é da forma $I = I_0 \oplus ... \oplus I_m$, onde $I_i =< a^{k_i}e_i >$, com $0 \leq k_i \leq t$.*

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

$$\begin{array}{ccccc} \alpha_1 & = & \alpha_1 e_0 + \ldots + \alpha_1 e_j & & \\ \vdots & \vdots & & \vdots & . \\ \alpha_k & = & \alpha_k e_0 + \ldots + \alpha_k e_j & & \end{array}$$

Como RGe_0 é um anel de cadeia, existe $j_0 \in \{1, ..., k\}$ tal que $< \alpha_i e_0 > \subset < \alpha_{j_0} e_0 >$, $\forall i \in \{1, ..., k\}$. Pelo teorema anterior, existe k_0 tal que $< \alpha_{j_0} e_0 > =< a^{k_0} e_0 >$. De forma análoga, para cada índice ρ, $1 \leq \rho \leq m$, existe j_ρ tal que $< \alpha_i e_\rho > \subset < \alpha_{j_\rho} e_\rho >$. Novamente pelo teorema anterior, existe k_ρ tal que $< \alpha_{j_\rho} e_\rho > =< a^{k_\rho} e_\rho > = I_\rho$. Assim, dado $\alpha_i \in I$,

$$\alpha_i = \alpha_i e_0 + ... + \alpha_i e_m \in < a^{k_0} e_0 > + ... + < a^{k_m} e_m > = I_0 + ... + I_m.$$

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

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

Lema 2.0.17 *Seja R uma anel local com ideal maximal $M =< a >$ e t o índice de nilpotência de a. Então, $x \cdot a^{t-k} = 0$ se, e somente se, $x \in < a^k >$, onde $x \in R$ e $0 < k < t$.*

Prova:

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

Já vimos no capítulo anterior que

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

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

Teorema 2.0.18 *Seja C um código cíclico da forma $C =< a^{k_{i_1}} e_{i_1} > \oplus ... \oplus < a^{k_{i_r}} e_{i_r} >$. Então, o número de palavras de C é $\mid C \mid = \mid \overline{R} \mid^{\sum_{s=1}^{r}(t-k_{i_s})w_{i_s}}$.*

Prova: Como C é uma soma direta, temos que $\mid C \mid = \mid < a^{k_{i_1}} e_{i_1} > \mid ... \mid < a^{k_{i_l}} e_{i_l} > \mid$. Devemos então determinar $\mid < a^{k_i} e_i > \mid$.

Considere

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

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 2.0.17, temos que $\alpha a^k = 0$ se, e somente se, $\alpha \in < a^{t-k} > G$. Portanto,

$$RGa^k \simeq \frac{RG}{< a^{t-k} > G}.$$

Como $\frac{RG}{<a^{t-k}>G} \simeq (\frac{R}{<a^{t-k}>})G$, temos,

$$|RGa^{k_i}e_i| = \left|(\frac{R}{< a^{t-k_i} >})Ge_i\right| = \left|\frac{R}{< a^{t-k_i} >}\right|^{w_i} = \left(\frac{\mid R \mid}{|< a^{t-k_i} >|}\right)^{w_i} = \mid \overline{R} \mid^{(t-k_i)w_i}.$$

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

■

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

Teorema 2.0.19 *Sejam R anel de cadeia finito e comutativo, com ideal maximal $M =< a >$, t o índice de nilpotência de a, com $\mid R \mid = q^k$ e $G =< g_0; g_0^n = 1 >$, 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 $I =< a^{k_0}e_0 > +...+ < a^{k_m}e_m >$, com $0 \leq k_j \leq t$.

Suponhamos que $< a^k e_i > =< a^l e_i >$, 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 que $a^{k+t-l}e_i = 0$. Como $k < l$, temos que $k + t - l < t$ e portanto $a^{k+t-l} \neq 0$. Usando o lema 2.0.17, podemos concluir que $e_i \in MG$. Como MG é nilpotente, existe m tal que $e_i^m = 0$. Como $e_i^2 = e_i$, temos que $e_i = 0$, contradição. Logo, $k = l$. Assim, para cada índice k_j, teremos códigos diferentes, portanto o número de códigos será $(t+1)^{m+1}$.

■

Teorema 2.0.20 *Para RG nas mesmas condições do teorema anterior, temos que RG é um anel de ideais principais.*

Prova: Seja I um ideal de RG. Então $I =< a^{k_0}e_0 > +...+ < a^{k_m}e_m >$.

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

Assim, $< a^{k_j}e_i > \subset < a^{k_0}e_0 + ... + a^{k_j}e_j >$ e portanto,

$$< a^{k_0}e_0 > +...+ < a^{k_m}e_m > = < a^{k_0}e_0 + ... + a^{k_m}e_m > .$$

Logo RG é um ideal de anéis principais.

■

2.1 Códigos duais e auto duais

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

Sejam $\{e_0, e_1, ..., e_m\}$ um conjunto de idempotentes ortogonais, tal que

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

Sabemos que $\mid RGe_i \mid = \mid R \mid^{w_i}$. Lembremos que como * denota a involução clássica, então $\mid RGe_i \mid = \mid RGe_i^* \mid$.

Proposição 2.1.1 *Sejam $\alpha = a_0 + a_1g + ... + a_{n-1}g^{n-1}$ e $\beta = b_0 + b_1g + ... + b_{n-1}g^{n-1} \in RG$. Se $\alpha \cdot \beta^* = 0$, então α é ortogonal a β.*

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

■ O resultado a seguir será necessário nos próximos teoremas.

Proposição 2.1.2 *Seja $\{e_0, ..., e_m\}$ o conjunto de idempotentes ortogonais, primitivos de RG. Então, $\{e_0{}^*, ..., e_m{}^*\}$ é também o conjunto de idempotentes ortogonais primitivos de RG.*

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

$(i)-$ $e_i{}^* \cdot e_i{}^* = e_i{}^*$.

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

$(iii)-$ $1 = e_0^* + ... + e_m^*$.

$(iv)-$ Cada e_i^* é primitivo.

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

■

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

Teorema 2.1.3 *Se um código cíclico C é da forma $C =< a^{k_0}e_0 > \oplus ... \oplus < a^{k_m}e_m >$, então o código dual a C é da forma $C^{\perp} = \oplus \sum_{r=0}^{m} < a^{t-k_r}e_r{}^* >$.*

Prova: Seja

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

Assim,

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

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 $C =< a^{k_0}e_0 > \oplus ... \oplus < a^{k_m}e_m >$, temos que

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

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

Por 1.2.16, temos que $| C^{\perp} |= q^l$, onde

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

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

Definição 2.1.4 *Um Código cíclico C é chamado de* ***código auto-dual*** *se $C = C^{\perp}$.*

Pelo teorema 2.1.3 é fácil ver que um código C é auto-dual se

$$C =< a^{k_0}e_0 > \oplus ... \oplus < a^{k_j}e_m >,$$

onde $k_i < t$, para $0 \leq i \leq m$.

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

Agora seja $C =< a^{k_0}e_0 > \oplus ... \oplus < a^{k_m}e_m >$.

Reordenando se necessário, podemos escrever C na forma

$$C =< a^{r_0}e_{k_{01}} > \oplus ... \oplus < a^{r_0}e_{k_{0s_0}} > \oplus ... \oplus < a^{r_l}e_{k_{l1}} > \oplus ... \oplus < a^{r_l}e_{k_{ls_l}} >,$$

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

Sejam

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

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

$$C =< a^{r_0}f_0 > \oplus ... \oplus < a^{r_l}f_l > .$$

Usando o teorema 2.1.3 para

$$C =< a^{r_0}e_{k_{01}} > \oplus ... \oplus < a^{r_0}e_{k_{0s_0}} > \oplus ... \oplus < a^{r_l}e_{k_{l1}} > \oplus ... \oplus < a^{r_l}e_{k_{ls_l}} >,$$

temos que

$$C^{\perp} =< a^{t-r_l}f_l^* > \oplus ... \oplus < a^{t-r_0}f_0^* > .$$

Definição 2.1.5 *Para um anel de cadeia R, com ideal maximal $M =< a >$, onde t o índice de nilpotência de a é par, o código $C =< a^{\frac{t}{2}} >$ é chamado* ***código auto-dual trivial****.*

Proposição 2.1.6 *Seja $C =< a^{r_0}f_0 > \oplus ... \oplus < a^{r_l}f_l >$ um código cíclico. Então C é auto-dual se, e somente se, para cada par de índices i, j tais que $i + j \equiv 0(modl)$ tem-se que $r_i + r_j = t$ e $f_i = f_j^*$.*

Prova: Sabemos que

$$C^{\perp} =< a^{t-r_l}f_l^* > \oplus ... \oplus < a^{t-r_0}f_0^* > .$$

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 $i + j \equiv 0(modl)$, 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 2.1.7 *Em [9], a notação usada por Kanwar e López-Permouth exclui vários casos de códigos cíclicos auto-duais, pois denotam o código C na forma $C =< \widehat{F}_1, a\widehat{F}_2, ..., a^{t-1}\widehat{F}_t >$, onde $x^n - 1 = F_0F_1...F_t$. Aqui, enunciamos e provamos os teoremas para C da forma $< a^{r_0}f_0 > \oplus ... \oplus < a^{r_l}f_l >$, onde a única imposição sobre os expoentes r_i's de a é que $0 \leq r_0 < r_1 < ... < r_l < t$, i.e., para todos os possíveis ideais.*

Teorema 2.1.8 *Suponha que t é um inteiro par. Então códigos 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

$$C =< a^{r_0}f_0 > \oplus ... \oplus < a^{r_l}f_l >=< a^{t-r_0}f_0^* > \oplus ... \oplus < a^{t-r_l}f_l^* >=< a^{t-r_0}f_0 > \oplus ... \oplus < a^{t-r_l}f_l > .$$

Logo, $r_i = t - r_i$, $\forall 0 \leq i \leq l$ e assim, $r_i = \frac{t}{2}$.

Portanto, $C =< a^{\frac{t}{2}}(f_0 + ... + f_l) >=< a^{\frac{t}{2}} >$, contradição.

Reciprocamente, seja $e \in RG$, tal que $e \neq e^*$. Então e^* é também um idempotente primitivo e podemos escrever $1 = e + e^* + e_2 + ... + e_m$. Denotemos $\beta = e_2 + ... + e_m$. Assim, $1 = e + e^* + \beta$. Por outro lado, $1 = (e + e^* + \beta)^* = e^* + e + \beta^*$. Logo, $\beta = \beta^*$.

Considere

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

Por 2.1.3 $C^{\perp} =< a^{(t-(\frac{t}{2}+1))}e^* > \oplus < a^{t-(\frac{t}{2}-1)}e^{**} > \oplus < a^{\frac{t}{2}}\beta^* >= C$.

■

Teorema 2.1.9 *Sejam R anel de cadeia finito com ideal maximal $< a >$, $\mid R \mid = q^{lt}$, onde $\mid \overline{R} \mid = q^l$ 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, $q^i \not\equiv -1(modn)$ para todo inteiro positivo i.*

Prova: Sabemos por [3] que um idempotente primitivo é da forma

$$e_k = \sum_{j=1}^{n} [\frac{1}{n} \sum_{\mathcal{X}_h \in \sum_k} \mathcal{X}_h(g^{-j})] g^j.$$

Assim,

$$e_k^* = \sum_{j=1}^{n} [\frac{1}{n} \sum_{\mathcal{X}_h \in \sum_k} \mathcal{X}_h(g^{n-j})] g^{n-j} = \sum_{j=1}^{n} [\frac{1}{n} \sum_{\mathcal{X}_h \in \sum_{n-k}} \mathcal{X}_h(g^{-j})] g^j, .$$

Pelo teorema2.1.8, sabemos que códigos auto-duais não triviais existem se, e somente se, existe um idempotente e_k, tal que $e_k \neq e_k^*$. Temos que para todo idempotente e_k, $e_k = e_k^*$ se, e somente se, $S_k = S_{n-k}$. Portanto, para todo $0 \leq k \leq m$, $\Omega_k = \Omega_{n-k}$, onde Ω_k denota a q classe ciclotômica contendo k. Isto acontece se, e somente se, existe i tal que $q^i k \equiv (n-k)(modn)$ para todo $0 \leq k \leq m$, ou equivalentemente $q^i \equiv -1 mod(n)$. ■

Corolário 2.1.10 *Se n é um número primo, então códigos cíclicos auto-duais de comprimento n não existem nos seguintes casos:*

- $p = 2$, $n \equiv 3, 5(mod 8)$;
- $p = 3$, $n \equiv 5, 7(mod 12)$;
- $p = 5$, $n \equiv 3, 7, 13, 17(mod 20)$;
- $p = 7$, $n \equiv 5, 11, 13, 15, 17, 23(mod 28)$;
- $p = 11$, $n \equiv 3, 13, 15, 17, 21, 23, 27, 29, 31, 41(mod 44)$

Prova: Segue do teorema2.1.9, observação1.4.4 e proposição1.4.9. ■

Corolário 2.1.11 *Seja n um primo ímpar diferente de p, e p um não resíduo quadrático de n^k, onde $k \geq 1$. Então códigos cíclicos auto-duais de comprimento n não existe.*

Prova: Segue do teorema2.1.9, observação1.4.4 e proposição1.4.10. ■

Corolário 2.1.12 *Se n é um primo ímpar, então códigos cíclicos auto-duais de comprimento n não existem nos seguintes casos:*

- $p \equiv 1(mod 4)$, *e existe um inteiro k tal que $mdc(p, 4n^k) = 1$ e p é um não resíduo quadrático de $4n^k$;*
- $p \equiv 1(mod 8)$, *e existem inteiros positivos i, j tal que $i > 2$, $mdc(p, 2^i n^j) = 1$ e p é um não resíduo quadrático de $n^i n^j$.*

Prova: Segue do teorema2.1.9, observação1.4.4 e proposição1.4.11. ■

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 $M =< a >$, tal que $\mid R/ < a > \mid = q$, tal que $o(q) = \phi(p^n)$ em $U(Z_{p^n})$ e $q \nmid p^n$. Neste caso, Ferraz e Polcino Milies em [13] 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:

$$G = G_o \supset G_1 \supset ... \supset G_n = 1.$$

Neste caso, os elementos

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

formam um conjunto de idempotentes ortogonais tal que

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

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

Teorema 3.0.13 *([13], Teorema 3.1)*

Seja F um corpo com q elementos e G um grupo cíclico de ordem p^n tal que $o(q) = \varphi(p^n)$ em $U(Z_{p^n})$. Seja

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

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

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

Daqui em diante, iremos sempre considerar R anel de cadeia comutativo, finito, com unidade, *com* $\mid R \mid = q^k =$, e G nas condições do teorema acima.

Assim por 3.0.13 temos que $\overline{e_0} = \widehat{G}$, $\overline{e_i} = \widehat{G_i} - \widehat{G_{i-1}}$ formam um conjunto de idempotentes primitivos ortogonais de $(\frac{R}{<a>})G$.

Para este conjunto de idempotentes primitivos, o próximo teorema exibi uma fórmula do número de elementos dos códigos da forma $I =< a^{k_0}e_0 > \oplus ... \oplus < a^{k_n}e_n >$.

Teorema 3.0.14 *Se I é um ideal de RG da forma $I =< a^{k_0}e_0 > \oplus ... \oplus < a^{k_m}e_m >$, com $0 \leq k_i \leq t$, então*

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

Prova: Como C é uma soma direta, temos que $\mid C \mid = \mid < a^{k_0}e_0 > \mid ... \mid < a^{k_m}e_m > \mid$. Devemos então determinar $\mid < a^{k_i}e_i > \mid$. 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 $e_i.\widehat{G}_{i-1} = (\widehat{G}_i - \widehat{G}_{i-1}).\widehat{G}_{i-1} = 0$. Logo

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

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

Considere

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

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 2.0.17, temos que $\alpha a^{k_i} = 0$ se, e somente se, $\alpha \in < a^{t-k_i} > G$. Portanto,

$$RGa^{k_i} \simeq \frac{RG}{< a^{t-k_i} > G}.$$

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

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

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

Sabemos que $\overline{R}_k G\widehat{G}_i \simeq \overline{R}_{k_i}(\frac{G}{G_i})$. Portanto, $\mid \overline{R}_{k_i}GG_i \mid = \mid \overline{R}_{k_i} \mid^{\frac{|G|}{|G_i|}} = \mid \overline{R}_{k_i} \mid^{p^i}$. De forma análoga, $\mid RGa^{k_i}\widehat{G}_{i-1} \mid = \mid \overline{R}_{k_i} \mid^{p^{i-1}}$.

Logo,

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

Para finalizar, temos que calcular $|< a^{k_0}e_0 >|$. Pelo lema 3.1, temos que

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

Logo,

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

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

■

Tão importante quanto descrever todos os possíveis códigos cíclicos é saber o seu peso. Nos teoremas que seguem, determinaremos os pesos para todos códigos cíclicos nas condições das hipóteses anteriores. Os resultados seguintes são uma generalização de resultados semelhantes obtidos por F. Mello [19] para corpos, à situação que estamos considerando.

No teorema seguinte iremos considerar G um grupo cíclico de ordem p^n com gerador b e $G_i =< b^{p^i} >$ os subgrupos de G.

Teorema 3.0.15 *Sejam G_i e G_{i-1} subgrupos normais de G tais que $G_i \subset G_{i-1}$ e $e_i = \widehat{G_i} - \widehat{G_{i-1}}$. Então $w((RG)a^k e_i) = 2 \mid G_i \mid$, para $i \neq 0$ e $w((RG)a^k e_0)) = \mid G \mid$, para $0 \leq k \leq t-1$.*

Prova:

Para $i \neq 0$, temos que $e_i\widehat{G_i} = (\widehat{G_i} - \widehat{G_{i-1}})\widehat{G_i} = \widehat{G_i} - \widehat{G_{i-1}} = e_i$. Logo, $(RG)e_i \subset (RG)\widehat{G_i}$. Seja Γ uma transversal de G_i em G. Um elemento arbitrário $\alpha \in RG$ pode ser escrito da 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 então uma palavra de $(RG)a^k e_i$. Se apenas um coeficiente $x_h a^k$ desta palavra é diferentes de 0, para algum $h \in \Gamma$, teríamos que $x_h a^k h\widehat{G_i} \in (RG)e_i$. Assim, existe $\beta \in RG$ tal que $x_h a^k h\widehat{G_i} = \beta a^k e_i$. Portanto $x_h a^k h\widehat{G_i}.\widehat{G_{i-1}} = \beta a^k e_i.\widehat{G_{i-1}}$. 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, $x_h a^k h\widehat{G_i} = 0$, contradição. Portanto, $w((RG)a^k e_i) \geq 2 \mid G_i \mid$.

Agora, considere $\alpha \in G_{i-1} \setminus G_i$. Temos que $(1-\alpha)a^k e_i \in (RG)a^k e_i$. Como $(1-\alpha)a^k e_i = (1-\alpha)a^k(\widehat{G_i} - \widehat{G_{i-1}}) = (1-\alpha)a^k\widehat{G_i} - (1-\alpha)a^k\widehat{G_{i-1}} = (1-\alpha)a^k\widehat{G_i}$ e $supp(a^k\widehat{G_i}) \cap supp(a^k\alpha\widehat{G_i}) = \emptyset$, temos que $w((RG)a^k e_i) \leq 2 \mid G_i \mid$. Portanto, $w((RG)a^k e_i) = 2 \mid G_i \mid$, para $i \neq 0$.

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

$$\begin{aligned} RGa^k e_0 &= (Ra^k)(G\widehat{G}) \\ &= (Ra^k)\widehat{G} \\ &= \{ra^k(1 + g_0 + ... + g_0^{p^n-1}) | r \in R\} \end{aligned} \quad .$$

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

■

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

Teorema 3.0.16 *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, $w(I_i \oplus I_j) = 2 \mid G_j \mid$.*

Prova: Consideremos inicialmente o caso em que $i \neq 0$. Temos que $G_j \subset G_i$. 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 α_1, $\alpha_2 \in RG$. Portanto, $\alpha.\widehat{G_j} = \alpha_i a^{k_1}(\widehat{G_i} - \widehat{G_{i-1}})\widehat{G_j} + \alpha_j a^{k_2}(\widehat{G_j} - \widehat{G_{j-1}})\widehat{G_j} = \alpha$. Logo, $\alpha \in (RG)\widehat{G_j}$. Considere agora Γ_j uma transversal de G_j em G. Assim, $\alpha = (\sum_{h\in\Gamma} x_h h)\widehat{G_j}$, onde $x_h \in R$. Suponhamos que apenas um coeficiente $x_h \neq 0$. Assim, $\alpha = x_h h\widehat{G_j}$. Como $e_i.\widehat{G_{i-1}} = e_j.\widehat{G_{i-1}} = 0$, temos que $\alpha.\widehat{G_{i_1}} = x_h h\widehat{G_j}.\widehat{G_{i-1}}$. Logo, $x_h h\widehat{G_{i-1}} = 0$ e com isso, temos que $x_h = 0$, 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 α_1, $\alpha_2 \in RG$. Assim, $\alpha.\widehat{G_j} = \alpha$ e portanto, $I_0 + I_j \subset (RG)\widehat{G_j}$.

Seja Γ uma transversal de G_j em G. Assim, podemos escrever α como sendo $\alpha = (\sum_{h\in\Gamma} x_h h)\widehat{G_j}$.

Suponhamos que apenas um coeficiente x_h é 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 $\widehat{G}_j.\widehat{G}_{j-1} = \widehat{G}_{j-1}$. Assim, $x_h h\widehat{G_j}.\widehat{G}_{j-1} = \alpha_1 a^{k_1}\widehat{G}\widehat{G}_{j-1} + \alpha_2 a^{k_2}(\widehat{G_j} - \widehat{G_{j-1}})\widehat{G}_{j-1}$, 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 ultima 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.

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

■

Teorema 3.0.17 *Sejam $I_j = (RG)a^{k_j}e_j$, com $0 \leq k_j \leq t-1$. Seja $I = I_0 \oplus ... \oplus I_j$, com $0 \leq j \leq n-1$. Então, $w(I_0 \oplus I_1 \oplus ... \oplus I_j) =\mid G_j \mid$.*

Prova: Seja $\alpha \in I$. Como $I = I_0 \oplus ... \oplus I_j$, existem β_0,..., $\beta_j \in RG$ tal que $\alpha = \beta_0 a^{k_0}\widehat{G} + ... + \beta_j a^{k_j}(\widehat{G}_j - \widehat{G}_{j-1})$. 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 $w(I) \geq w((RG)\widehat{G}_j) =\mid G_j \mid$.

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

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

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

■

Teorema 3.0.18 *Sejam $I_j = (RG)a^{k_j}e_j$, com $0 \leq k_j \leq t-1$. Se $I = I_{j_1} \oplus ... \oplus I_{j_l}$, $j_r < j_{r+1}$, para $1 \leq r \leq l$ com $\{j_1, ..., j_l\} \subsetneqq \{0, 1, ..., j_l\}$, então, $w(I) = 2 \mid G_{j_l} \mid$.*

Prova: Consideremos inicialmente

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

Seja $\alpha \in I$. Como $I = I_{j_1} \oplus ... \oplus I_{j_l}$, existem β_{j_1},..., β_{j_l}, tal que

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

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

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

Como, $\widehat{G}_{j_i} \subset \widehat{G}_{j_1-1}$, para $1 \leq i \leq l$, temos que $\widehat{G}_{j_i}.\widehat{G}_{j_1-1} = \widehat{G}_{j_1-1}$, para $1 \leq i \leq l$. Logo, $\widehat{G}_{j_1-1} \cdot e_{j_i} = 0$, para $1 \leq i \leq l$. Multiplicando ambos os lados da igualdade por $\widehat{G}_{j_1-1}$, temos que $x_{h_0}h_0\widehat{G}_{j_1-1} = 0$. A partir daí, temos que $x_{h_0} = 0$, o que contradiz nossa escolha inicial de $x_{h_0} \neq 0$. Portanto, $w(I) \geq 2 \mid G_{j_l} \mid$.

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

Agora, considere

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

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

Seja $\alpha \in I$. Como $I = I_0 \oplus I_{j_1} \oplus ... \oplus I_{j_l}$, existem β_0,β_{j_1},..., $\beta_{j_l} \in RG$, tal que $\alpha = \beta_0 a^{k_0}\widehat{G} + \beta_{j_1} a^{k_{j_1}}(\widehat{G}_{j_1} - \widehat{G}_{j_1-1}) + ... + \beta_{j_l} a^{k_{j_l}}(\widehat{G}_{j_l} - \widehat{G}_{j_{l-1}})$. Assim, $\alpha \cdot \widehat{G}_{j_l} = \alpha$. Logo, $I \subset (RG)\widehat{G}_{j_l}$.

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

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

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

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

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

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

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

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

■

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

Teorema 3.1.2 ([16], 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 portanto qualquer módulo que for um somando de um módulo livre é projetivo e portanto livre.

O proximo teorema é semelhante ao provado por Dutra, Ferraz e Polcino Milies em [11] 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 *Seja G um grupo cíclico de ordem p^n e R um anel de cadeia, com $\mid R \mid = q^k$, onde $q \nmid \mid G \mid$. Seja $e_i = \widehat{G}_i - \widehat{G}_{i-1}$. Seja γ uma transversal de G_{i-1} em G e τ uma transversal de G_i em G_{i-1}. Então*

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

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 que $(1-h)\widehat{G}_{i-1} = 0$, pois $h.\widehat{G}_{i-1} = \widehat{G}_{i-1}$.

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

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

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

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 $h \in \tau \setminus \{1\}$ que é uma transversal de G_i em G_{i-1}, temos que $\widehat{G}_i$ e $h\widehat{G}_i$ tem suportes disjuntos. Como $c \in \gamma$ que é uma transversal de G_{i-1} em G, 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 uma transversal de G_i em G, temos que $c_jh_j\widehat{G}_i$ e $c_kh_k\widehat{G}_i$ 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 β pertence a RGe_i. Provemos agora que os dois conjuntos têm o mesmo número de elementos. Sabemos pelo teorema 4.1.15 que $\mid RGe_i \mid = \mid \overline{R} \mid^{t(p^i-p^{i-1})} = \mid R \mid^{(p^i-p^{i-1})}$. Por outro lado, temos que o número de elementos gerado pelo módulo livre sobre R cuja base é β é dado por $\mid R \mid^{|\gamma|(|\tau|-1)} = \mid R \mid^{|\frac{G}{G_{i-1}}|(|\frac{G_{i-1}}{G_i}|-1)} = \mid R \mid^{p^i-p^{i-1}}$. Portanto, RGe_i e 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^ke_i não pode ser livre, pois $(a^{t-k}\alpha) \cdot (a^ke_i) = 0$, para qualquer $\alpha \in RGe_i$.

Por 3.1.1 e 3.1.2, e o teorema acima, temos o seguinte corolário.

Corolário 3.1.5 *Seja G um grupo cíclico de ordem p^n e R um anel de cadeia com $\mid R \mid = q^k$, 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*

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

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

Sabemos que $posto(RGe_i) = p^i - p^{i-1}$. Iremos adiante exibir outra base para RGe_i, Antes porém será necessária a seguinte proposição.

Proposição 3.1.7 ([16], 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 $G =< g_0 | g_0^{p^n} = 1 >$ e o conjunto $\mathcal{B} = \{e_i, ge_i, g^2e_i, ..., g^{p^i - p^{i-1}-1}e_i\}$ é uma base de RGe_i, onde g é um gerador do grupo G.*

Prova: Como o número de elementos de $\mathcal{B}$ é $p^i - p^{i-1}$, usando 3.1.7 basta provar que $\mathcal{B}$ gera RGe_i.

Temos que um elemento de RGe_i é dado por $r_0e_i + r_1ge_i + ... + r_{p^n-1}g^{p^n-1}e_i$. Devemos provar então que os elementos da forma $r_l g^l e_i$ onde $p^i - p^{i-1} \leq l \leq p^n$ são combinação linear 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 combinação linear 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 combinação linear dos elementos de $\mathcal{B}$.

Note que

$$\begin{aligned} e_i \;=\; & \tfrac{1}{p^{n-i+1}}\Big((p-1) - g^{p^{i-1}} - g^{2p^{i-1}} - ... + (p-1)g^{p.p^{i-1}} - g^{(p+1)p^{i-1}} - g^{(p+2)p^{i-1}} - ... \\ & ... + (p-1)g^{2p.p^{i-1}} - .... - g^{(p^{n-i+1}-(p-1))p^{i-1}} - g^{(p^{n-i+1}-1)p^{i-1}}\Big). \end{aligned}$$

Logo,

$$\begin{aligned} g^{(p-1)p^{i-1}+k}e_i &= \tfrac{1}{p^{n-i+1}}\Big((p-1)g^{(p-1)p^{i-1}+k} - g^{p.p^{i-1}+k} - g^{(p+1)p^{i-1}+k} - ... - g^{(2p-2).p^{i-1}+k} + \\ &\quad +(p-1)g^{(2p-1)p^{i-1}+k} - g^{(2p)p^{i-1}+k} - g^{(2p+1)p^{i-1}+k} - ... + \\ &\quad +(p-1)g^{(p^{n-i+1}).p^{i-1}+k} - g^{k} - g^{p^{i-1}+k} - g^{2p^{i-1}+k} + ... - g^{(p-2)p^{i-1}+k}\Big). \end{aligned}$$

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

$$\begin{aligned} g^{k}e_i &= \tfrac{1}{p^{n-i+1}}\Big((p-1)g^{k} - g^{p^{i-1}+k} - g^{2p^{i-1}+k} - ... - g^{(p-1)p^{i-1}+k} + (p-1)g^{p.p^{i-1}+k} - \\ &\quad -g^{(p+1)p^{i-1}+k} - ... + (p-1)g^{(2p).p^{i-1}+k} - ... - (p-1)g^{(p^{n-i+1}-p)p^{i-1}+k} - \\ &\quad -g^{(p^{n-i+1}-(p-1))p^{i-1}+k} - g^{(p^{n-i+1}-(p-2))p^{i-1}+k} - ... - g^{(p^{n-i+1}-1)p^{i-1}+k}\Big). \end{aligned}$$

$$\begin{aligned} g^{(p^{i-1}+k)}e_i &= \tfrac{1}{p^{n-i+1}}\Big((p-1)g^{p^{i-1}+k} - g^{2p^{i-1}+k} - g^{3p^{i-1}+k} - ... - g^{p.p^{i-1}+k} + \\ &\quad +(p-1)g^{(p+1)p^{i-1}+k} - g^{(p+2)p^{i-1}+k} - g^{(p+3)p^{i-1}+k} - ... + (p-1)g^{(2p+1)p^{i-1}+k} - \\ &\quad ... + (p-1)g^{(p^{n-i+1}-(p-1))p^{i-1}+k} - g^{(p^{n-i+1}-(p-2))p^{i-1}+k} - .... - g^{k}\Big). \end{aligned}$$

$$\begin{aligned} g^{(2p^{i-1}+k)}e_i &= \tfrac{1}{p^{n-i+1}}((p-1)g^{2p^{i-1}+k} - g^{3p^{i-1}+k} - g^{4p^{i-1}+k} - ... - g^{(p+1).p^{i-1}+k} + \\ &\quad +(p-1)g^{(p+2)p^{i-1}+k} - g^{(p+3)p^{i-1}+k} - g^{(p+4)p^{i-1}+k} - ... + (p-1)g^{(2p+2)p^{i-1}+k} - \\ &\quad ... + (p-1)g^{(p^{n-i+1}-(p-2))p^{i-1}+k} - g^{(p^{n-i+1}-(p-3))p^{i-1}+k} - .... - g^{k} - g^{p^{i-1}+k}) \end{aligned}$$

$$\vdots$$

$$\begin{aligned} g^{(p-2)p^{i-1}+k}e_i &= \tfrac{1}{p^{n-i+1}}\Big((p-1)g^{(p-2)p^{i-1}+k} - g^{(p-1)p^{i-1}+k} - ... - g^{(2p-3)p^{i-1}+k} \\ &\quad +(p-1)g^{(2p-2)p^{i-1}+k} - g^{(2p-1)p^{i-1}+k} - ... + (p-1)g^{(3p-2)p^{i-1}+k} - ... \\ &\quad +(p-1)g^{(p^{n-i+1}-2)p^{i-1}+k} - g^{(p^{n-i+1}-1)p^{i-1}+k} - g^{k} - g^{p^{i-1}+k} - ... \\ &\quad -g^{(p-3)p^{i-1}+k}\Big). \end{aligned}$$

Agora, pode se verificar diretamente que

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

Como $\mathcal{B}' \subset \mathcal{B}$, segue que $\{e_i, ge_i, ...g^{(p-1)p^{i-1}-1}e_i\}$ 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 $\mathcal{B} = \{e_2, ge^2, ..., g^{19}e_2\}$ é uma base para $< e_2 >$. Note que os elementos da forma $g^k e_2$, com $20 \leq k \leq 24$ são dados pelas seguintes combinações dos elementos de $\mathcal{B}$.

$$g^{20}e_2 = -e_2 - g^5e_2 - g^{10}e_2 - g^{15}e_2$$
$$g^{21}e_2 = -ge_2 - g^6e_2 - g^{11}e_2 - g^{16}e_2$$
$$g^{22}e_2 = -g^2e_3 - g^7e_2 - g^{12}e_2 - g^{17}e_2$$
$$g^{23}e_2 = -g^3e_2 - g^8e_2 - g^{13}e_2 - g^{18}e_2$$
$$g^{24}e_2 = g^4e_2 - g^9e_2 - g^{14}e_2 - g^{19}e_2$$

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

$$d_H(C) \leq n - \log_m(\mid C \mid) + 1.$$

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*

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

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 $R = Z_{2^4}$ 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 $e_3 = \widehat{G}_3 - \widehat{G}_2$.*

Seja $C = RGe_1 \oplus RGe_2$.

Temos que

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

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

Sabemos que $d_H(C) \leq n - \log_m(\mid C \mid) + 1$, onde m é o tamanho do alfabeto, n é o comprimento do código. Portanto, pela desigualdade, sabemos que para $C = < e_1 > \oplus < e_2 >$,

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

Neste exemplo o peso está muito distante do seu limitante superior

Exemplo 3.2.3 *Considere agora G um grupo cíclico de ordem 9 e o anel $R = Z_4$.*

Observe que $U(Z_9) = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$ e $< \overline{2} >= U(z_9)$. Como $\frac{|Z_4|}{|<2>|} = 2$, 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 $e_2 = \widehat{G}_2 - \widehat{G}_1$.

Tomemos $C =< e_1 >$. Assim,

$$w(C) = 2 \mid G_1 \mid = 2.3 = 6$$

e

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

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 proxima da distância máxima do limitante.

Tomemos agora G grupo cíclico de ordem 4, R anel de cadeia, tal que $\mid \overline{R} \mid = q$, onde $q \equiv 3(mod4)$ e o código gerado por $C =< e_1 >$, onde $e_1 = \widehat{G}_1 - \widehat{G}_0$.

Temos que

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

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

e

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

Observe que para qualquer $q \equiv 3(mod4)$, 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 $< \overline{q} >= U(Z_4)$, temos que $\{e_0, e_1, e_2\}$ formam um conjunto de idempotentes primitivos ortogonais em RG.

Exemplo 3.2.4 *Sejam G um grupo cíclico de ordem 4, R o anel Z_{11^7} e o código C_1 gerado por*
$e_1 = \widehat{G}_1 - \widehat{G}_0$. *Temos que* $\frac{|Z_{11^7}|}{|<\overline{11}>|} = 11$. *Como* $\overline{11} = \overline{3}$ *em* Z_4, *temos que* $< \overline{11} >= U(Z_4)$. *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 $C_2 =< e_2 >$ não é um código MDS. De fato,

$$w(RGe_2) = 2.2^{2-2} = 2 \text{ e } d_H(RGe_2) \leq 4 - 2^2 - 2^1 + 1 = 3.$$

Agora, observe que o código $C_3 = RGe_0 \oplus RGe_1$ 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, $w(C_4) = 2. \mid G_2 \mid = 2.2^{(2-2)} = 2$. *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,* $w(C_5) = 2$. $\mid G_2 \mid = 2.2^{(2-2)} = 2$. *O limitante de Hamming é dado por*

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

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

Quando tomamos $\mid \overline{R} \mid = q$, e $\overline{q}$ gera $U(Z_{p^n})$, para códigos de comprimento p^n, sabemos que $\{e_0, ..., e_n\}$ formam um conjunto de idempotentes primitivos ortogonais em RG. Quando tomamos $\mid G \mid = 2^n$, temos um problema, pois o grupo das unidade de Z_{2^m}, para $m \geq 2$ não é cíclico e assim, para qualquer $\mid \overline{R} \mid = q$, 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 3.2.5 *Se* G *é um grupo de ordem* $\mid G \mid = 2^n$ *e* R *é um anel de cadeia, tal que* $\mid R \mid$ *não divide* 2 *então* $e_1 = \widehat{G}_1 - \widehat{G}_0$ *é um idempotente primitivo.*

Prova: Temos que $e_1 = \widehat{G}_1 - \widehat{G}_0$. Assim, $\widehat{G}_1 = e_1 + \widehat{G}_0$. Como $e_1 \cdot \widehat{G}_0 = (\widehat{G}_1 - \widehat{G}_0) \cdot \widehat{G}_0 = \widehat{G}_0 - \widehat{G}_0 = 0$, temos que, $RG\widehat{G}_1 = RGe_1 \oplus RG\widehat{G}_0$ e com isso, temos que

$$\mid RG\widehat{G}_1 \mid = \mid RGe_1 \mid \cdot \mid RG\widehat{G}_0 \mid .$$

Assim,

$$\mid RGe_1 \mid = \frac{\mid RG\widehat{G}_1 \mid}{\mid RG\widehat{G}_0 \mid} = \frac{\mid R \mid^{\frac{|G|}{|G_1|}}}{\mid R \mid^{\frac{|G|}{|G|}}} = \frac{\mid R \mid^{2^1}}{\mid R \mid} = \mid R \mid .$$

Como $\mid RGe_1 \mid = \mid R \mid$, temos que e_1 é idempotente primitivo, como queríamos demonstrar.

■

Temos que $w(RGe_1) = 2 \cdot 2^{n-1} = 2^n$ e pelo resultado anterior, temos que $\mid RGe_1 \mid = \mid R \mid$. Como o comprimento do código já é 2^n, temos que o código gerado por e_1 tem distância de Hamming máxima.

3.2.1 Resultados de Códigos MDS de comprimento p^n

Consideremos agora G um grupo cíclico de ordem p^n com $p > 2$ e $\mid R \mid = g^k$, com $q \nmid \mid G \mid$, tal que $o(q) = \phi(p^n)$ em $U(Z_{p^n})$. Iremos agora apresentar alguns dois resultados sobre códigos MDS.

Teorema 3.2.6 *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 $p^{(-n+2i-1)} > 2$. Reescrevendo a desigualdade anterior, temos que $p^{i-1} > 2p^{n-i}$. Como $p^n \geq p^i$, temos que $p^n + p^{i-1} > p^i + 2p^{n-i}$. Portanto, $p^n - p^i + p^{i-1} - 2p^{n-i} > 0$ 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 3.2.7 *Se $C = RGe_0 \oplus RGe_1 \oplus RGe_2 \oplus ... \oplus RGe_k$, então C não é um código MDS.*

Prova: Se $C = RGe_0 \oplus RGe_1 \oplus RGe_2 \oplus ... \oplus RGe_k$, então, $w(C) = 2 \mid G_k \mid = 2p^{n-k}$. Calculando o limitante, temos que

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

Calculando a desigualdade acima, temos que

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

Como $p^k \geq 2$, temos que $p^k(p^{n-k}+1)+1 \geq 2p^{n-k}$. 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 e R anel de cadeia? Esta pergunta ainda não possui uma resposta concreta, mas devidos a alguns resultados encontrados, 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 anterior, calculamos o peso de todos os códigos cíclicos de comprimento p^n sobre anéis de cadeia. Neste capítulo iremos calcular o peso de todos os possíveis códigos cíclicos de sobre anéis de cadeia de comprimento $2p^n$ e caracterizar todos os códigos livres de comprimento $2p^n$, exibindo uma base para estes códigos.

No decorrer deste capítulo estaremos considerando sempre $p > 2$. Iremos sempre considerar também R anel de cadeia finito, comutativo, com unidade, com ideal maximal $M =< a >$, t o índice de nilpotência de a e $\mid R/ < a > \mid = q$, tal que $o(q) = \phi(p^n)$ em $U(Z_{p^n})$ e $q \nmid 2p^n$.

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

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

Em [13], Ferraz e Polcino Milies provaram o seguinte teorema:

Teorema 4.1.1 ([13], Teorema 3.2) *Sejam K um corpo com q elementos e G 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 G de Sylow e $B = \{1, d\}$ é um 2-subgrupo de Sylow. Se e_i, $0 \leq i \leq n$, denota o idempotente primitivo de KG, então os idempotentes primitivos de KA são*

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

Fazendo o levantamento, temos que

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

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

Em [13], Ferraz e Polcino Milies provaram que o peso do código $KA\Big(\frac{1\pm d}{2}e_i\Big)$ é dado por

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

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

Teorema 4.1.2 *Seja $C = RA(a^k(\frac{1\pm d}{2})e_i)$, com $0 \leq k < t$. Então*

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

Prova: Temos que $e_i = \widehat{G}_i - \widehat{G}_{i-1}$, para $i \neq 0$. Seja $\Gamma = \{\tau_1, ..., \tau_n\}$ uma transversal de G_i em G. Como $\Big(a^k(\frac{1\pm d}{2})e_i\Big) \cdot \widehat{G}_i = \Big(a^k(\frac{1\pm d}{2})e_i\Big)$, temos que $C \subset \Big(a^k(\frac{1\pm d}{2})\widehat{G}_i\Big)$. Seja $\alpha \neq 0 \in C$,

logo α pode ser escrito como

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

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

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

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 que $(x_i\tau_i)\Big(a^k(\frac{1\pm d}{2})\widehat{G}_{i-1}\Big) = 0$. Observe que $(x_i a^k\tau_i)\cdot\widehat{G}_{i-1}$ e $(x_i a^k\tau_i)\cdot t\widehat{G}_{i-1}$ 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

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

pois $(1 - g_0)\cdot\widehat{G}_{i-1} = 0$. Logo, $\alpha = (1 - g_0)(a^k\frac{1\pm d}{2})\widehat{G}_i \in C$ 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 que $C =< a^k\Big(\frac{1\pm d}{2}e_0\Big) >$. Provemos que $w(< a^k(\frac{1\pm d}{2}e_0) >) =\mid A \mid$. Seja $\alpha \neq 0 \in C$. Temos que $\alpha = \sum_{g\in G} x_g t^{\zeta_g} g(a^k(\frac{1 \pm d}{2})e_0)$, onde $\zeta_g = 0$ ou 1, $x_g \in R$. Como $g \cdot e_o = e_0 = \widehat{G}$ e $d \cdot (\frac{1\pm d}{2}) = \pm(\frac{1\pm d}{2})$, temos que $\alpha = (\sum a^k x_g')(\frac{1\pm d}{2}e_0)$. Portanto $w(C) = 2 \mid G \mid =\mid A \mid$. ■

Agora iremos calcular os pesos de todos os possíveis códigos cíclicos de comprimento $2p^n$ sobre um anel de cadeia R, onde $q \not| \mid G \mid$. Iremos calcular os resultados de acordo com a soma dos geradores dos códigos. Nos teoremas que seguem iremos considerar apenas o caso

de somas de idempotentes da forma $a^{k_i}(\frac{1+d}{2})e_i$, sendo que a demonstração é análoga no caso $a^{k_i}(\frac{1-d}{2})e_i$.

Teorema 4.1.3 *Se o código C é da forma $C =< a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} > \oplus ... \oplus < a^{k_{i_l}}(\frac{1+d}{2})e_{i_l} >$, onde $0 \leq k_{i_j} < t$, $1 \leq j \leq l$ e $0 < i_1 < i_2 < ... < i_l$, 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 que $\widehat{G}_{i_l}.e_j = e_j$. Logo, $C \subset< a^k(\frac{1+d}{2})\widehat{G}_{i_l} >$, onde $k = min\{k_{i_1}, ..., k_{i_l}\}$. Seja $\Gamma = \{\tau_1, ..., \tau_n\}$ uma transversal de G_{i_l} em G e $\alpha \in C$. Então podemos escrever

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

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 $C =< a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} > \oplus ... \oplus < a^{k_{i_l}}(\frac{1+d}{2})e_{i_l} >$, existem $\beta_1, ..., \beta_l \in RA$, tal que

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

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

■

Teorema 4.1.4 *Se o código C é da forma $C =< a^{k_0}(\frac{1+d}{2})e_0 > \oplus < a^{k_1}(\frac{1+d}{2})e_1 > \oplus ... \oplus \oplus < a^{k_l}(\frac{1+d}{2})e_l >$, onde $0 \leq k_j, < t$, $0 \leq j \leq l$, então $w(C) = 2 \mid G_l \mid$.*

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

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

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

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

Portanto,

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

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

Teorema 4.1.5 *Se o código C é da forma $C =< a^{k_0}(\frac{1+d}{2})e_0 > \oplus < a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} > \oplus ... \oplus \oplus < a^{k_{i_l}}(\frac{1+d}{2})e_{i_l} >$, onde $0 \leq k_{i_j}, k_0 < t$, $1 \leq j \leq l$ e $\{i_1, ..., i_l\} \subsetneqq \{1, ..., i_l\}$, 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 que $\widehat{G}_{i_l}.e_j = e_j$. Logo, $C \subset < a^k(\frac{1+d}{2})\widehat{G}_{i_l} >$, onde $k = max\{k_{i_1}, ..., k_{i_l}\}$. Seja $\Gamma = \{\tau_1, ..., \tau_n\}$ uma transversal de G_{i_l} em G e $\alpha \in C$. Então podemos escrever $\alpha = (x_1\tau_1 + ... + x_n\tau_n)(a^k(\frac{1+d}{2})\widehat{G}_{i_l})$, 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

$$C =< a^{k_0}(\frac{1+d}{2})e_0 > \oplus < a^{k_{i_1}}(\frac{1+d}{2})e_{i_1} > \oplus ... \oplus < a^{k_{i_l}}(\frac{1+d}{2})e_{i_l} >,$$

existem $\beta_0, \beta_1, ..., \beta_l$, tal que

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

Como $\{i_1, ..., i_l\} \subsetneqq \{1, ..., i_l\}$, existe pelo menos um $i_r \in \{1, ..., i_l\}$, 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 $\{i_1, ..., i_l\}$ e está em $\{1, ..., i_l\}$. Multiplicando ambos os lados da igualdade por $\widehat{G}_{i_r}$, temos que

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

Como o peso do ideal $< a^{k_0}(\frac{1+d}{2})e_0 > \oplus < a^{k_1}(\frac{1+d}{2})e_{i_1} > \oplus < a^{k_2}(\frac{1+d}{2})e_{i_2} > \oplus ... \oplus \oplus < a^{k_{i_r-1}}(\frac{1+d}{2})e_{i_r-1} >$ 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 que $w(C) \geq 4 \mid G_{i_l} \mid$ e assim, $w(C) = 4 \mid G_{i_l} \mid$. ■

Agora iremos calcular o peso dos códigos que sejam somas de ideais $< (a^{k_i}(\frac{1+d}{2})e_i) >$ e $< (a^{k_j}(\frac{1-d}{2})e_j) >$. Como o cálculo destes códigos envolvem varias técnicas diferentes para os diferentes tipos de somas, iremos calcular inicialmente os pesos de códigos que sejam somas de dois ideais apenas e depois iremos generalizar estes cálculos para uma soma finita destes ideais.

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

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

Temos que $\widehat{G}_j.e_i = e_i$ e $\widehat{G}_j.e_j = e_j$. Logo,

$$C \subset < a^k(\frac{1+d}{2})\widehat{G}_j > \oplus < a^k(\frac{1-d}{2})\widehat{G}_j > = < a^k\widehat{G}_j >,$$

onde $k = min\{k_i, k_j\}$. Seja $\Gamma = \{\tau_1, ..., \tau_n\}$ uma transversal de G_j em G e $\alpha \neq 0 \in C$. Podemos escrever α como $\alpha = (x_1\tau_1 + ... + x_n\tau_n + x_1^{'}d\tau_1 + ... + x_n^{'}d\tau_n)a^k\widehat{G}_j$, 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 $\beta_i, \beta_j \in RA$, tal que

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

Multiplicando ambos os lados da igualdade por $\widehat{G}_{i-1}$, temos que

$$(ya^kd^{\zeta_\tau}\tau)\widehat{G}_{i-1} = 0.$$

Logo, $ya^k = 0$, contradição.

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

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

onde $\zeta_\tau, \zeta_{\tau'} = 0$ ou 1 e τ e $\tau^{'} \in \Gamma$. Suponhamos agora que $\zeta_\tau \neq \zeta_{\tau'}$. 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 suporte disjunto. 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,

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

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

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

Desenvolvendo os termos da igualdade acima, temos que

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

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

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

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

$$w(\alpha) = 2 \mid G_j \mid \quad e \quad w(< a^{k_j}(\frac{1-d}{2})e_j >) = 4 \mid G_j \mid,$$

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

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

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

onde $\zeta_\tau, \zeta_{\tau'}, \zeta^{\tau^{''}} = 0$ ou 1 e $\tau, \tau^{'}$ e $\tau^{''} \in \Gamma$. Suponhamos que $\zeta_1 = \zeta_2 \neq \zeta_3$. Multiplicando a

equação acima por $\widehat{G}_{i-1}$, temos que

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

Como $(y_1 d^{\zeta_\tau}\tau + y_2 d^{\zeta_{\tau'}}\tau')a^k G_{j-1}$ e $(y_3 d^{\zeta_{\tau'}}\tau')a^k\widehat{G}_{i-1}$ têm suportes disjuntos, temos que $y_3 a^k = 0$, o que contradiz nossa hipótese inicial. Suponhamos então sem perda de generalidade que $\zeta_\tau = \zeta_{\tau'} = \zeta_{\tau''} = 0$. Assim,

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

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

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

Desenvolvendo os termos da igualdade acima, temos que

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

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

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

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

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

$$w(\alpha) = 3 \mid G_j \mid \quad e \quad w(< a^{k_j}(\frac{1-d}{2})e_j >) = 4 \mid G_j \mid,$$

o que contradiz a minimalidade do peso de $< a^{k_j}(\frac{1-d}{2})e_j >$.

Portanto, $w(C) \geq 4 \mid G_j \mid$ e assim, podemos concluir que $w(C) = 4 \mid G_j \mid$.

■

Teorema 4.1.7 *Se o código C é da forma $C =< a^{k_0}(\frac{1+d}{2})e_0 > \oplus < a^{k_j}(\frac{1-d}{2})e_j >$, onde $1 < j \leq n$, $0 \leq k_0, k_j < t$, então $w(C) = 4 \mid G_j \mid$.*

Prova: Primeiramente, temos que $w(C) \leq w(< a^{k_j}(\frac{1-d}{2})e_j >) = 4 \mid G_j \mid$.

Observe que $C \subset < a^k \widehat{G}_j >$, onde $k = min\{k_0, k_j\}$. Seja $\Gamma = \{\tau_1, ..., \tau_n\}$ uma transversal de G_j em G e $\alpha \neq 0 \in C$. Assim, $\alpha = (x_1\tau_1 + ... + x_n^{'}\tau_n + x_1^{'}d\tau_1 + ... + x_n^{'}d\tau_n)a^k\widehat{G}_j$.

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 $\alpha_1, \alpha_2 \in RA$ tal que

$$(yd^{\zeta_\tau}\tau)a^k\widehat{G}_j = \alpha_1 a^{k_0}(\frac{1+d}{2})e_0 + \alpha_2 a^{k_j}(\frac{1-d}{2})e_j.$$

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

$$(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{j-1} = \alpha_1 a^{k_0}(\frac{1+d}{2})e_0.$$

Daí, $(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{j-1} = 0$, pois independente do valor de ζ_τ, teríamos $\alpha_1 a^{k_0}\widehat{G} = 0$ ou $\alpha_1 a^{k_0} d\widehat{G} = 0$ da igualdade e portanto $ya^k = 0$.

Suponhamos agora que existam apenas dois coeficientes y_1, y_2 de α, tal que $y_1a^k \neq 0$, $y_2a^k \neq 0$. Logo, existem α_1, $\alpha_2 \in RA$, tal que

$$\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau^{'})a^k\widehat{G}_j = \alpha_1 a^{k_0}(\frac{1+d}{2})e_0 + \alpha_2 a^{k_j}(\frac{1-d}{2})e_j,$$

onde $\zeta_\tau, \zeta_{\tau'} = 0$ ou 1 e τ e $\tau^{'} \in \Gamma$. Temos que $\alpha_1 = \sum_{g\in G} x_g d^{\zeta_g} g$, onde $\zeta_g = 0$ ou 1. Logo,

$\alpha_1.(a^{k_0}\frac{1+d}{2})e_0) = (\sum x_g)a^{k_0}(\frac{1+d}{2})e_0 = (\sum x_g)a^{k_0}(\frac{1+d}{2})\widehat{G}$. Assim,

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

Suponhamos sem perda de generalidade que $\zeta_\tau \neq \zeta_{\tau'}$ e que $\zeta_\tau = 0$. Como $\mid \tau G_{j-1} \mid = \mid \tau' G_{j-1} \mid = \mid G_{j-1} \mid < \mid G \mid$, pois $j > 1$, temos que $(\sum x_g a^{k_0}) = 0$, 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 que $\zeta_\tau = \zeta_{\tau'} = 0$. Assim,

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

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

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

Novamente, podemos escrever $\alpha_1.a^{k_0}(\frac{1+d}{2})e_0 = (\sum x_g)a^{k_0}(\frac{1+d}{2})e_0 = (\sum x_g)a^{k_0}(\frac{1+d}{2})\widehat{G}$, 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 $\alpha = \alpha_2 a^{k_j}(\frac{1-d}{2})e_j$, ou seja, $\alpha \in < a^{k_j}(\frac{1-d}{2})e_j >$, porém, $w(\alpha) = 2 \mid G_j \mid$ e $w(< a^{k_j}(\frac{1-d}{2})e_j >) = 4 \mid G_j \mid$, o que é um absurdo.

Suponhamos agora que existam apenas três coeficientes y_1, y_2 e y_3 de α, tal que $y_1 a^k \neq 0$, $y_2 a^k \neq 0$ e $y_3 a^k \neq 0$. Logo, existem α_1, $\alpha_2 \in RA$, tal que

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

onde $\zeta_\tau, \zeta_{\tau'}, \zeta_{\tau''} = 0$ ou 1 e τ, τ' e $\tau'' \in \Gamma$. Temos que $\alpha_1 = \sum_{g\in G} x_g d^{\zeta_g} g$, onde $\zeta_g = 0$ ou 1.

Logo, $\alpha_1.(a^{k_0}\frac{1+d}{2})e_0) = (\sum x_g)a^{k_0}(\frac{1+d}{2})e_0 = (\sum x_g)a^{k_0}(\frac{1+d}{2})\widehat{G}$. Assim,

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

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 $\mid \tau_3 G_{j-1} \mid = \mid G_{j-1} \mid < \mid G \mid$.

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

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

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

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

■

No próximo teorema, vamos considerar $p > 3$.

Teorema 4.1.8 *Se o código C é da forma $C =< a^{k_0}(\frac{1+d}{2})e_0 > \oplus < a^{k_1}(\frac{1-d}{2})e_1 >$, onde $1 < j \leq n$, $0 \leq k_0, k_1 < t$, então $w(C) = 4 \mid G_1 \mid$.*

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

Observe que $C \subset < a^k\widehat{G}_1 >$, onde $k = min\{k_0, k_1\}$. Sejam $\Gamma = \{\tau_1, ..., \tau_p\}$ uma 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 $\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_1 = \alpha_0 a^{k_0}(\frac{1+d}{2})e_0 + \alpha_1 a^{k_1}(\frac{1-d}{2})e_1$, onde $\zeta_\tau = 1$ ou 0 e $\tau \in \Gamma$.

multiplicando a igualdade acima por $(\frac{1-d}{2})\widehat{G}$, temos que

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

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

Suponhamos que exista apenas dois coeficiente y_1, y_2 de α, tal que $y_1a^k \neq 0$ e $y_2a^k \neq 0$. Então, existem α_0 e $\alpha_1 \in RA$, tal que

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

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

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

$$(y_1\tau + y_2\tau')a^k\widehat{G} = \alpha_0a^{k_0}(\frac{1+d}{2})e_0.$$

Como $\alpha_0 \in RA$, então $\alpha_0 = \sum_{g\in G} x_g d^{\zeta_g} g$, e assim, $\alpha_0a^{k_0}(\frac{1+d}{2})e_0 = (\sum x_g)a^{k_0}(\frac{1+d}{2})\widehat{G}$. Portanto, $(\sum x_g)a^{k_0}t\widehat{G} = 0$ e assim, $(\sum x_g)a^{k_0} = 0$. Assim, $\alpha \in < a^{k_1}(\frac{1-d}{2})e_1 >$, mas $w(\alpha) = 2 \mid G_1 \mid$ e $w(< a^{k_1}(\frac{1-d}{2})e_1 >) = 4 \mid G_1 \mid$, o que é um absurdo.

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

$$\alpha = (y_1\tau + y_2d\tau')a^k\widehat{G}_1 = \alpha_0a^{k_0}(\frac{1+d}{2})e_0 + \alpha_1a^{k_1}(\frac{1-d}{2})e_1.$$

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

$$(y_1\tau + y_2d\tau')(\frac{1+d}{2})a^k\widehat{G}_1 = (\sum x_g)a^{k_0}(\frac{1+d}{2})\widehat{G}.$$

Desenvolvendo e igualando termo a termo, termos que

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

Como estamos considerando $p \neq 2$, temos que $\mid G \mid \neq \mid \tau_1G_1 \mid + \mid \tau_2G_1 \mid = 2 \mid G_1 \mid$. Logo,

$(\sum x_g)a^{k_0} = 0$ e assim, $\alpha \in < a^{k_1}(\frac{1-d}{2})e_1 >$, mas $w(\alpha) = 2 \mid G_1 \mid$ e $w(< a^{k_1}(\frac{1-d}{2})e_1 >) = 4 \mid G_1 \mid$, o que é um absurdo.

Suponhamos que existam apenas três coeficiente y_1, y_2 e y_3 de α, tal que $y_1a^k \neq 0$, $y_2a^k \neq 0$ e $y_3a^k \neq 0$. Então, existem α_0 e $\alpha_1 \in RA$, tal que

$$\alpha = (y_1 d^{\zeta_\tau}\tau + y_2 d^{\zeta_{\tau'}}\tau' + y_3 d^{\zeta_{\tau''}}\tau'')a^k\widehat{G}_1 = \alpha_0 a^{k_0}(\frac{1+d}{2})e_0 + \alpha_1 a^{k_1}(\frac{1-d}{2})e_1,$$

onde ζ_τ, $\zeta_{\tau'}$ 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

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

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

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

$$\alpha = (y_1\tau + y_2\tau' + y_3 d\tau'')a^k\widehat{G}_1 = \alpha_0 a^{k_0}(\frac{1+d}{2})e_0 + \alpha_1 a^{k_1}(\frac{1-d}{2})e_1.$$

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

$$(y_1\tau + y_2\tau' + y_3 d\tau'')a^k(\frac{1+d}{2})\widehat{G}_1 = \alpha_0 a^{k_0}(\frac{1+d}{2})e_0 = (\sum x_g)a^{k_0}(\frac{1+d}{2})\widehat{G}.$$

Da igualdade acima temos que $(y_1\tau + y_2\tau' + y_3\tau'')a^k\widehat{G}_1 = (\sum x_g)a^{k_0}\widehat{G}$. Como estamos considerando $p \neq 3$, temos que $\mid G \mid \neq \mid \tau G_1 \mid + \mid \tau' G_1 \mid + \mid \tau'' G_1 \mid = 3 \mid G_1 \mid$. Logo, $(\sum x_g)a^{k_0} = 0$ e assim, $\alpha \in < a^{k_1}(\frac{1-d}{2})e_1 >$, mas $w(\alpha) = 3 \mid G_1 \mid$ e $w(< a^{k_1}(\frac{1-d}{2})e_1 >) = 4 \mid G_1 \mid$, o que é um absurdo.

Portanto, $w(C) \geq 4 \mid G_1 \mid$ e então podemos concluir que $w(C) = 4 \mid G_1 \mid$.

■

Teorema 4.1.9 *Se o código C é da forma $C =< a^{k_i}(\frac{1+d}{2})e_i > \oplus < a^{k_j}(\frac{1-d}{2})e_i >$, 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 $C \subset < a^k(\frac{1+d}{2})e_i > \oplus < a^k(\frac{1-d}{2})e_i > \subset$ $\subset < a^k(\frac{1+d}{2})\widehat{G}_i > + < a^k(\frac{1-d}{2})\widehat{G}_i > \subset < a^k\widehat{G}_i >$.

Sejam $\Gamma = \{\tau_1, ..., \tau_n\}$ uma transversal de G_i em G e $\alpha \in C$. Podemos escrever α como $\alpha = (x_1\tau_1 + ... + x_n\tau_n + x_1^{'}d\tau_1 + ... + x_n^{'}d\tau_n)a^k\widehat{G}_i$, 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 $\beta_2 \in RA$, tal que

$$\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_i = \beta_1 a^{k_i}(\frac{1+d}{2})e_i + \beta_2 a^{k_j}(\frac{1-d}{2})e_i,$$

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

Multiplicando a igualdade acima por $\widehat{G}_{i-1}$, temos que $(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{i-1} = 0$. Assim, temos que $ya^k = 0$, 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 $\alpha = (1 - g_0)a^k e_i = (1 - g_0)a^k(\frac{1+d}{2})e_i + (1 - g_0)a^k(\frac{1-d}{2})e_i \in C$. Logo $w(C) \leq 2 \mid G_i \mid$ e portanto $w(C) = 2 \mid G_i \mid$. ■

Agora iremos generalizar estes casos e calcular outros possíveis casos onde possam ocorrer somas de idempotentes $(\frac{1+d}{2})e_0$ e $(\frac{1-d}{2})e_0$, $(\frac{1+d}{2})e_i$ e $(\frac{1-d}{2})e_i$.

Teorema 4.1.10 *Se o código C é da forma $C =< a^{k_{i_1}}(\frac{1\pm d}{2})e_{i_1} > \oplus ... \oplus < a^{k_{i_l}}(\frac{1\pm d}{2})e_{i_l} >$, onde $0 \leq k_{i_j} < t$, $1 \leq j \leq l$, $0 < i_1 \leq i_2 \leq ... \leq i_{l-1} < i_l$, e existe pelo menos um idempotente $(\frac{1+d}{2})e_i$ e $(\frac{1-d}{2})e_j$ como geradores dos ideais somando de C, então $w(C) = 4 \mid G_{i_l} \mid$.*

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

Temos que $C \subset < a^k\widehat{G}_{i_l} >$, onde $k = min\{k_{i_1}, ..., k_{i_l}\}$. Sejam $\Gamma = \{\tau_1, ..., \tau_n\}$ uma transversal de G_{i_l} em G e $\alpha \in C$. Podemos escrever α como $\alpha = (x_1\tau_1 + ... + x_n\tau_n + x_1^{'}d\tau_1 + ... + x_n^{'}d\tau_n)a^k\widehat{G}_{i_l}$, onde x_j e $x_j^{'} \in R$. Como $\alpha \in C$, existem $\beta_1, ..., \beta_l \in RA$, tal que

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

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

Multiplicando a igualdade acima por $\widehat{G}_{i_1-1}$, temos que

$$(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{i_l-1} = 0.$$

Assim, concluímos que $ya^k = 0$, o que contradiz nossa hipótese.

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

$$\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau^{'})a^k\widehat{G}_{i_l} = \beta_1 a^{k_{i_1}}(\frac{1 \pm d}{2})e_{i_1} + ... + \beta_l a^{k_{i_l}}(\frac{1 \pm d}{2})e_{i_l}, \tag{4.3}$$

onde ζ_τ, $\zeta_{\tau'} = 0$ ou 1 e τ,$\tau^{'} \in \Gamma$. 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 for feito abaixo para $(\frac{1-d}{2})e_{i_l}$.

Multiplicando a igualdade 4.3 por $(\frac{1-d}{2})$, temos

$$(y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau^{'})a^k(\frac{1 - d}{2})\widehat{G}_{i_l} = \beta_1 a^{k_{j_1}}(\frac{1 - d}{2})e_{j_1} + ... + \beta_l a^{k_{j_s}}(\frac{1 - d}{2})e_{j_s},$$

onde $j_s < i_l$. Assim, $\alpha(\frac{1-d}{2})$ pertence ao código $C^{'} = < a^{k_{j_1}}(\frac{1-d}{2})e_{j_1} > \oplus ... \oplus < a^{k_{j_s}}(\frac{1-d}{2})e_{j_s} >$. 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 tal que $y_1a^k \neq 0$,

$y_2a^k \neq 0$ e $y_3a^k \neq 0$. Assim, podemos escrever α como

$$\alpha = (y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau^{'} + y_3d^{\zeta_{\tau''}}\tau^{''})a^k\widehat{G}_{i_l} = \beta_1a^{k_{i_1}}(\frac{1 \pm d}{2})e_{i_1} + ... + \beta_la^{k_{i_l}}(\frac{1 \pm d}{2})e_{i_l}, \quad (4.4)$$

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

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

Multiplicando a igualdade 4.4 por $(\frac{1-d}{2})$, temos

$$(y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau^{'} + y_3d^{\zeta_{\tau''}}\tau^{''})a^k(\frac{1-d}{2})\widehat{G}_{i_l} = \beta_1a^{k_{j_1}}(\frac{1-d}{2})e_{j_1} + ... + \beta_la^{k_{j_s}}(\frac{1-d}{2})e_{j_s},$$

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

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

■

No próximo teorema, também estaremos considerando $p > 3$.

Teorema 4.1.11 *Se o código C é da forma $C =< a^{k_{00}}(\frac{1+d}{2})e_0 > \oplus < a^{k_{01}}(\frac{1-d}{2})e_0 > \oplus < a^{k_{10}}(\frac{1+d}{2})e_1 > \oplus < a^{k_{11}}(\frac{1-d}{2})e_1 > \oplus < a^{k_{20}}(\frac{1+d}{2})e_2 > \oplus < a^{k_{21}}(\frac{1-d}{2})e_2 > \oplus ... \oplus \oplus < a^{k_{(j-1)0}}(\frac{1+d}{2})e_{j-1} > \oplus < a^{k_{(j-1)1}}(\frac{1-d}{2})e_{j-1} > \oplus < a^{k_j}(\frac{1\pm d}{2})e_j >$, 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 $< a^{k_r}(\frac{1+d}{2})e_r >$ e $< a^{k_s}(\frac{1-d}{2})e_s >$ não nulos, então $w(C) = 4 \mid G_j \mid$.*

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

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

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

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

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

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

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

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

$$C^{'} =< a^{k_{00}}(\frac{1+d}{2})e_0 > \oplus < a^{k_{10}}(\frac{1+d}{2})e_1 > \oplus ... \oplus < a^{k_{r0}}(\frac{1+d}{2})e_r > .$$

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

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

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

$$(y_1d^{\zeta_\tau}\tau + y_2d^{\zeta_{\tau'}}\tau^{'})a^k(\frac{1+d}{2})\widehat{G}_j = \beta_{00}a^{k_{00}}(\frac{1+d}{2})e_0 + \beta_{10}a^{k_{10}}(\frac{1+d}{2})e_1 + ... + \beta_{j_l0}a^{k_{j_l0}}(\frac{1+d}{2})e_{j_l},$$

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

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

e o peso do código C' é

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

Como $p > 3$, temos que $4 \mid G_j \mid < 2 \mid G_r \mid < 4 \mid G_r \mid < \mid A \mid$. 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 que

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

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

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

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

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 $C' =< a^{k_{00}}(\frac{1+d}{2})e_0 > \oplus < a^{k_{10}}(\frac{1+d}{2})e_1 > +...+ < a^{k_{j_l 0}}(\frac{1+d}{2})e_{j_l} >$. Temos que

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

e o peso do código C' é

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

Como $p > 3$, temos que $6 \mid G_j \mid < 2 \mid G_r \mid < 4 \mid G_r \mid < \mid A \mid$. 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 que

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

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

Portanto $w(C) \geq 4 \mid G_j \mid$, e como tínhamos $w(C) \leq 4 \mid G_j \mid$, podemos concluir que $w(C) = 4 \mid G_j \mid$. ■

Nos teoremas anteriores, sempre consideramos o último ideal da soma do código 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 existe ambos os ideais, ou seja, o gerador do último ideal dos códigos em questão é $a^{k_{j0}}(\frac{1+d}{2})e_j$ e $a^{k_{j1}}(\frac{1-d}{2})e_j$, onde $k_{j0},\ k_{j1} < t$.

Teorema 4.1.12 *Se o código C é da forma $C =< a^{k_{i_1}}(\frac{1\pm d}{2})e_{i_1} > \oplus < a^{k_{i_2}}(\frac{1\pm d}{2})e_{i_2} > \oplus ... \oplus < a^{k_{i_{l_1}}}(\frac{1+d}{2})e_{i_l} > \oplus < a^{k_{i_{l_2}}}(\frac{1-d}{2})e_{i_l} >$, onde $0 \leq k_{i_j} < t$, $1 \leq j \leq l$, $0 < i_1 \leq i_2 \leq ... \leq i_{l-1} < i_l$, então $w(C) = 2 \mid G_{i_l} \mid$.*

Prova: Temos que $w(C) \leq w(< a^{k_{i_{l_1}}}(\frac{1+d}{2})e_{i_l} > \oplus < a^{k_{i_{l_2}}}(\frac{1-d}{2})e_{i_l} >) = 2 \mid G_{i_l} \mid$. Temos também que $C \subset < a^k \widehat{G}_{i_l} >$, onde $k = min\{k_{i_1}, k_{i_2}, ..., k_{i_{l_1}}, k_{i_{l_2}}\}$. Sejam $\Gamma = \{\tau_1, ..., \tau_n\}$ uma transversal de G_{i_l} em G e $\alpha \in C$.

Podemos escrever α como $\alpha = (x_1\tau_1 + ... + x_n\tau_n + x_1^{'}d\tau_1 + ... + x_n^{'}d\tau_n)a^k\widehat{G}_{j_l}$. Como $\alpha \in C =< a^{k_{i_1}}(\frac{1\pm d}{2})e_{i_1} > \oplus < a^{k_{i_2}}(\frac{1\pm d}{2})e_{i_2} > \oplus ... \oplus < a^{k_{i_{l_1}}}(\frac{1+d}{2})e_{i_l} > \oplus < a^{k_{i_{l_2}}}(\frac{1-d}{2})e_{i_l} >$, existem $\beta_1, ..., \beta_{l_1}, \beta_{l_2} \in RA$, tal que

$$\alpha = \beta_1 a^{k_{i_1}}(\frac{1 \pm d}{2})e_{i_1} + ... + \beta_{l_1}a^{k_{i_{l_1}}}(\frac{1+d}{2})e_{i_l} + \beta_{l_2}a^{k_{i_{l_2}}}(\frac{1-d}{2})e_{i_l}.$$

Vamos supor que exista apenas um coeficiente y de α, tal que $ya^k \neq 0$. Então $\alpha = (yd^{\zeta_\tau}\tau)a^k\widehat{G}_{j_l} = \beta_1 a^{k_{i_1}}(\frac{1\pm d}{2})e_{i_1} + ... + \beta_{l_1}a^{k_{i_{l_1}}}(\frac{1+d}{2})e_{i_l} + \beta_{l_2}a^{k_{i_{l_2}}}(\frac{1-d}{2})e_{i_l}$, onde $\zeta_\tau = 0$ ou 1 e $\tau \in \Gamma$.

Multiplicando a igualdade acima por $\widehat{G}_{i_1-1}$, temos que

$$(yd^{\zeta_\tau}\tau)a^k\widehat{G}_{i_1-1} = 0.$$

Logo, $ya^k = 0$, o que contradiz nossa hipótese, assim $w(C) \geq 2 \mid G_{i_l} \mid$. Portanto, $w(C) = 2 \mid G_{i_l} \mid$ ■

Teorema 4.1.13 *Se o código C é da forma $C =< a^{k_{00}}(\frac{1+d}{2})e_0 > \oplus < a^{k_{01}}(\frac{1-d}{2})e_0 > \oplus \oplus < a^{k_{10}}(\frac{1+d}{2})e_1 > \oplus < a^{k_{11}}(\frac{1-d}{2})e_1 > \oplus < a^{k_{20}}(\frac{1+d}{2})e_2 > \oplus < a^{k_{21}}(\frac{1-t}{2})e_2 > \oplus ... \oplus \oplus < a^{k_{j_1}}(\frac{1+d}{2})e_j > \oplus < a^{k_{j_2}}(\frac{1-d}{2})e_j >$, onde $0 < j \leq n$, k_{00} ou $k_{01} \neq t$, e k_{j_1} e $k_{j_2} \neq t$ então $w(C) = 2 \mid G_j \mid$ ou $\mid G_j \mid$.*

Prova: Dividiremos a demonstração em duas partes. Vamos supor inicialmente que existe r tal que k_{r0} ou k_{r1} seja igual a t e provaremos que $w(C) = 2 \mid G_j \mid$ e depois iremos considerar

o caso em que k_{i0}, $k_{i1} < t$, para $0 \leq i \leq j-1$ e provaremos que $w(C) =\mid G_j \mid$.

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

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

Podemos escrever α como $\alpha = (x_1\tau_1 + ... + x_n\tau_n + x_1^{'}d\tau_1 + ... + x_n^{'}d\tau_n)a^k\widehat{G}_j$.

Como $\alpha \in C =< a^{k_{00}}(\frac{1+d}{2})e_0 > \oplus < a^{k_{01}}(\frac{1-d}{2})e_0 > \oplus \oplus < a^{k_{10}}(\frac{1+d}{2})e_1 > \oplus < a^{k_{11}}(\frac{1-d}{2})e_1 > \oplus < a^{k_{20}}(\frac{1+d}{2})e_2 > \oplus < a^{k_{21}}(\frac{1-d}{2})e_2 > \oplus ... \oplus \oplus < a^{k_{j_1}}(\frac{1+d}{2})e_j > \oplus < a^{k_{j_2}}(\frac{1-d}{2})e_j >$, existem $\beta_{00}, \beta_{01}, ..., \beta_{j_1}, \beta_{j_2} \in RA$, tal que $\alpha = \beta_{00}a^{k_{00}}(\frac{1+d}{2})e_0 + \beta_{01}a^{k_{01}}(\frac{1-d}{2})e_0 + ... + \beta_{j_1}(\frac{1+d}{2})a^{k_{j_1}}e_j + \beta_{j_2}(\frac{1-d}{2})a^{k_{j_2}}e_j$.

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

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

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:

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

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 $C^{'} =< a^{k_{00}}(\frac{1+d}{2})e_0 > \oplus \oplus < a^{k_{10}}(\frac{1+d}{2})e_1 > \oplus ... \oplus < a^{k_{i-10}}(\frac{1+d}{2})e_{i-1} >$. 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 $p \neq 2$. Assim, temos uma contradição. Portanto, $w(C) \geq 2 \mid G_j \mid$.

Suponhamos agora que k_{i0}, $k_{i1} < t$, para $0 \leq i \leq j-1$.

Temos que $C \subset < \widehat{G}_j >$. Portanto, $w(C) \geq w(< \widehat{G}_j >) =\mid G_j \mid$.

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

$< a^k\widehat{G}_j >=< a^k((\widehat{G}_j - \widehat{G}_{j-1}) + (\widehat{G}_{j-1} - \widehat{G}_{j-2}) + ... + (\widehat{G}_1 - \widehat{G}_0) + \widehat{G}_0) >$

$=< a^k(e_j + e_{j-1} + ... + e_1 + e_0) >$

$=< a^k(\frac{1+d}{2})e_0 + a^k(\frac{1-d}{2})e_0 + ... + a^k(\frac{1+d}{2})e_j + a^k(\frac{1-d}{2})e_j) >$

$\subset< a^{k_{00}}(\frac{1+d}{2})e_0 > \oplus < a^{k_{01}}(\frac{1-d}{2})e_0 > \oplus < a^{k_{10}}(\frac{1+d}{2})e_1 > \oplus < a^{k_{11}}(\frac{1-d}{2})e_1 > \oplus ... \oplus$
$\oplus < a^{k_{j_1}}(\frac{1+d}{2})e_j > \oplus < a^{k_{j_2}}(\frac{1-d}{2})e_j >= C.$

Logo, $\mid G_j \mid = w(< a^k\widehat{G}_j >) \geq w(C)$. 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 $< a^k(\frac{1+d}{2})e_i >$.

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

Prova: Observe que se $i > 0$, então

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

Logo,

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

Como

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

temos que

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

Assim,

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

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

Considere

$$\begin{array}{rcl} \psi : RA & \rightarrow & RAa^k. \\ \alpha & \mapsto & \alpha a^k \end{array} \tag{4.5}$$

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 2.0.17, temos que $\alpha a^k = 0$ se, e somente se, $\alpha \in < a^{t-k} > A$. Portanto,

$$RAa^k \simeq \frac{RA}{< a^{t-k} > A}.$$

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

$$\mid RAa^k(\frac{1+d}{2})\widehat{G}_i \mid = \mid \left(\frac{R}{< a^{t-k} >}\right)A(\frac{1+d}{2})\widehat{G}_i \mid .$$

Agora considere $R^{'} = \left(\frac{R}{<a^{t-k}>}\right)$ 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

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

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 que $\alpha_1 = \beta_1$ e assim, $\Phi(\alpha) = \Phi(\beta)$.

Claramente Φ é um isomorfismo de anéis. Portanto

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

Logo,

$$\mid R^{'} A(\frac{1+d}{2})e_i \mid = \mid R^{'} \mid^{p^i - p^{i-1}} = \Big(\frac{\mid R \mid}{\mid < a^{t-k} > \mid}\Big)^{p^i - p^{i-1}} = \Big(\frac{\mid \overline{R} \mid^t}{\mid \overline{R} \mid^k}\Big)^{p^i - p^{i-1}} = \mid \overline{R} \mid^{(t-k)(p^i - p^{i-1})} .$$

Agora iremos calcular $\mid RAa^{k_0}(\frac{1+d}{2})e_0 \mid$. Por 4.5, temos que

$$\mid RAa^{k_0}(\frac{1+d}{2})e_0 \mid = \mid (\frac{R}{< a^{t-k_0} >})A(\frac{1+d}{2})e_0 \mid .$$

Denotemos $(\frac{R}{<a^{t-k_0}>})$ por $R^{'}$. Considere

$$\begin{array}{rcl} \Phi : RA(\frac{1+d}{2})\widehat{G} & \to & RG\widehat{G}. \\ (\sum\limits_{g\in G} x_g)(\frac{1+d}{2})\widehat{G} & \mapsto & (\sum\limits_{g\in G} x_g)\widehat{G} \end{array}$$

Claramente Φ é um isomorfismo de anéis entre $RA(\frac{1+d}{2})\widehat{G}$ e $RG\widehat{G}$.

$|< a^{k_0}\frac{1+d}{2}e_0 >| = \frac{|RG\widehat{G}|}{|<a^{t-k_0}>A(\frac{1+d}{2})\widehat{G}|}$. Como

$$\mid RG\widehat{G} \mid = \mid R \mid \text{ e } \mid < a^{t-k_0} > A(\frac{1+d}{2})\widehat{G} \mid = \mid < a^{t-k_0} > \mid,$$

segue que $|< a^{k_0}(\frac{1+d}{2})e_0 >| = \mid \overline{R} \mid^{t-k_0}$. ■

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

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

então

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

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

Nesta seção iremos caracterizar códigos livres de comprimento $2p^n$ sobre anéis de cadeia. Isto será feito de modo análogo ao 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 $mdc(| R |, | A |) = 1$, e os idempotentes primitivos ortogonais $(\frac{1\pm d}{2})e_i$, com $0 \leq i \leq n$.

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

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

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

Prova: Iremos fazer 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 que $(1-b)(\frac{1+d}{2})\widehat{G}_{i-1} = (\frac{1+d}{2})\widehat{G}_{i-1} - (\frac{1+d}{2})b\widehat{G}_{i-1} = 0$, 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 os elementos de $\mathcal{B} \in RA(\frac{1+d}{2})e_i$.

Agora iremos mostrar que os elementos de $\mathcal{B}$ são linearmente independentes.

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

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

Desenvolvendo a igualdade acima temos que

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

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

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

Provaremos então que os elementos do somatório $(\sum_{c\in\gamma}(\sum_{b\in\tau} x_{cb}c\widehat{G}_i) - \sum_{c\in\gamma}\sum_{b\in\tau} x_{cb}cb\widehat{G}_i)$ 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 $c_k\widehat{G}_i$ tem suportes disjuntos. Como τ é uma transversal de G_i em G_{i-1}, temos que para $b_j \neq b_k \in \tau$, $c_jb_j\widehat{G}_i$ e $c_kb_k\widehat{G}_i$ têm suportes disjuntos. Portanto, $x_{cb} = 0$, $\forall c \in \gamma$ e $b \in \tau$.

Sabemos pelo teorema 4.1.14 que o número de elementos do código $RA(\frac{1+d}{2})e_i$ é dado por

$$\mid \overline{R} \mid^{t(p^i-p^{i-1})} = \mid R \mid^{(p^i-p^{i-1})}.$$

O número de elementos do código gerado por $\mathcal{B}$ sobre R é dado por $\mid R \mid^{(\mid\gamma\mid\cdot(\mid\tau\mid-1))}$.

$$(\mid \gamma \mid \cdot(\mid \tau \mid -1)) = \frac{\mid G \mid}{\mid G_{i-1} \mid} \cdot (\frac{\mid G_{i-1} \mid}{\mid G_i \mid} - 1) = (p^i - p^{i-1}).$$

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 $\alpha \cdot a^{t-k}. \cdot a^k(\frac{1+d}{2})e_i = 0,\ \forall \alpha \in RA$.

Referências Bibliográficas

[1] M. F. Atiyah and I. G. macdonald, *Introduction to Commutative Algebra*, Westview Press, Massachusetts, 1969. 7

[2] N. S. Babu and K. H. Zimmermann, *Decoding of Linear Codes over Galois Rings*, IEE Transactions on Informations Theory, Vol 47,(2001) 1599-1603. 4

[3] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*, Academic Press, Inc, New York, 1975. 17, 34

[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, and P. Solé, *A Linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math., vol.29,(1993) 218-222. 3

[6] A. R. Calderbank, and, N. J. A. Sloane, *Modular and p-adic codes*Des., Codes Cryptogr., vol. 6, (1995)21-35. 3, 13

[7] A. C. A. Campello Jr., G. C. Jorge and S. I. R. Costa, *Decoding q-ary lattices in the Lee metric*, IEEE Information theory workshop, (2011) 220-224. 4

[8] J. H. Conway and 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 and S. R. López-Permouth, *Cyclic and Negacyclic Codes Over Finite Chain Rings*, IEEE Transactions on Information Theory, Vol. **50**, No. 8 (2004) 1728-1744. 4, 23, 33

[10] Y. A. Drodz and V. V. Kirichenko, *Finite Dimensional Algebras*, Springer-Verlag, Berlin, 1991.

[11] F. Dutra, R. Ferraz and C. Polcino Milies, *Semisimple group codes and dihedral codes*, Algebra and Discrete Mathematics , number **3**, (2009) 28-48. 45

[12] A. Hefez, M. L. T. Villela, *Códigos Corretores de Erros*, Instituto Nacional de Matemática Pura e Aplicada-IMPA- Série de Computação e Matemática, Rio de Janeiro, 2008. 14

[13] R.A. Ferraz and 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

[14] A. R. Hammons Jr., P.V. Kumar, A.R.Calderbank, N.J.A. Sloane, P. Sole, *The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Transactions on Information Theory, vol 40, (1994) 301-319. 3

[15] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003. 3, 13

[16] N. Jacobson, *Basic Algebra*, W.H.Freeman and Company, San Francisco, 1980. 7, 8, 45, 47

[17] P. Kanwar and S. R. López-Permouth, *Cyclic codes over the interger modulo p^m*, Finite Fields Appl. vol3, (1997) 334-352. 3, 4

[18] B. R. MacDonald, *Finite Rings With Identity*, Pure abd Applied Nathematics, A Series of Monographs and Textbooks, New York, 1974. 7, 9, 10, 12

[19] F. Melo, *Sobre Códigos Cíclicos e Abelianos*, Tese de doutorado a ser apresentada ao Instituto de Matemática e Estatística, USP, São Paulo, 2012. 40

[20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 10th Ed. , The Netherlands:North-Holland, Amsterdam, 1998. 15

[21] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, New York, 1986. 7

[22] 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

[23] G. Norton and A. Sălăgean-Mandache, *On the structure of linear cyclic codes over finite chain rings*, Appl. Algebra Eng. Commun. Comput., vol 10, (2000)486-506. 3, 4

[24] G. T .Peterson, *Lifting idempotents in near rings*; Arch. Math., Vol 51,(1988)208-212.

[25] V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over* Z_4, IEEE Transactions on Information Theory, vol. 42, (1996)1594-1600. 3, 13

[26] C. Polcino Milies and S. K. Sehgal, *An introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, Netherlands, 2002. 7

[27] G. Puninski; *Serial Rings*; Kluwer Academic Publishers, Dordrecht, Boston, London, 2001.

[28] D. Redmond, *Number Theory: An Introduction*, ser. Monographs and Textbooks in Pure and Applied Mathematics. New York, 1996. 19

[29] S. Roman, *Coding and Information Theory*, Kluwer Academic Publishers, Graduate Texts in Mathematics, Springer, New York, 1992. 15, 18

[30] J. P. O. Santos, *Introdução à Teoria dos Números*, Associoação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2003. 19

[31] C. Vanden Eynden, *Elementary Number Theory*, McGraw-Hill, 2nd ed. New York, 2001. 19

[32] Z. Wan, *cyclic codes over Galois rings*, Alg. Colloq., vol. 6, (1999)291-304. 3