Luiza Helena Silva Vidigal Gonçalves

Códigos Abelianos Minimais

Universidade Federal de Minas Gerais

Agosto de 2012

Luiza Helena Silva Vidigal Gonçalves

Códigos Abelianos Minimais

Dissertação de mestrado apresentada como parte dos requisitos necessários para obtenção do título de Mestre pelo Departamento de Matemática do Instituto de Ciências Exatas, Universidade Federal de Minas Gerais.

Orientadores: Fabio Enrique Brochero Martínez e Carmen Rosa Giraldo Vergara

Universidade Federal de Minas Gerais

31 de Agosto de 2012

Agradecimentos

Agradeço primeiramente a Deus por ter me dado força e saúde.

Aos meus pais, Hélio e Ana, pelo amor, incentivo e confiança ao iniciar esta jornada. Ao meu marido, Júlio, pelo carinho, companheirismo e dedicação. Sem o apoio de vocês não teria alcançado este objetivo. Amo muito vocês!

À minha irmã, Aracy, pela compreensão diante das dificuldades que enfrentamos.

À minha família querida, pela torcida e pelas orações, em especial à Alaíde, minha madrinha.

Aos meus amigos por entenderem minha ausência.

Aos meus orientadores, Carmen e Fabio, pela paciência e pelos conhecimentos adquiridos.

Aos professores Osnel e Viviane pelas sugestões e comentários que contribuíram para a qualidade deste trabalho.

Aos professores e funcionários do Departamento de Matemática da UFMG pela presteza, em especial às professoras Ana e Viviane.

Aos colegas de pós-graduação que fizeram com que estes últimos três anos fossem mais suaves: Luciana Cadar, Rômulo, Ariana, Vitor, Luiz, Carlos, Luciana França, Natália, Willian, Leonel, entre outros. Em especial à Monique e à Sílvia, muito obrigada pela solidariedade!

Dedico esta dissertação ao meu pai, saudades eternas!

Resumo

O objetivo desse trabalho é estudar os artigos de Arora-Pruthi e Ferraz-Milies sobre Códigos Corretores de Erros dotados de certas estruturas algébricas. Em particular, estudamos Códigos Abelianos Minimais, vistos como ideais de uma álgebra de grupo FG, onde F é um corpo finito e G é um grupo abeliano finito. Sob tais condições, são encontrados os idempotentes primitivos da álgebra FG, caracterizando assim os códigos abelianos minimais desta álgebra. Além disso, são obtidos também a distância mínima, a dimensão, o peso e o polinômio gerador destes códigos minimais. Por fim, são calculados o número de componentes simples da álgebra de grupo semissimples e demonstrado que este número corresponde ao número de idempotentes primitivos desta álgebra de grupo.

Abstract

The purpose of this work is to study the articles of Arora-Pruthi and Ferraz-Milies about Error Correcting Codes endowed with certain algebraic structures. Precisely, we study the minimal abelian codes seen as ideals of a group algebra FG, where F is a finite field and G is a finite abelian group. Under these conditions, the primitive idempotents of the algebra FG, characterizing the minimal abelian codes of this algebra, are found. Furthermore, the minimum distance, the dimension, the weight and the generator polynomial of these minimal codes are also obtained. Finally, the number of simple components of the semisimple group algebra is calculated and it is shown that this number corresponds to the number of primitive idempotents of this group algebra.

Sumário

Introdução

A Teoria de Códigos Corretores de Erros teve sua origem no Laboratório Bell de Tecnologia em 1947, quando R. W. Hamming, depois de ter alguns problemas com a leitura de seus programas nos computadores da Bell, desenvolveu um código que conseguia detectar até dois erros e corrigir um erro, se ele fosse único. Em 1948, C. E. Shannon, também do laboratório Bell, publicou o primeiro artigo sobre Códigos Corretores de Erros, "A Mathematical Theory of Communication". Este artigo respondeu de forma indireta a seguinte questão, que em 1977 foi numa entrevista relembrada por Richard W. Hamming "... se as máquinas podem detectar um erro, porque não podemos localizar a posição do erro e corrigi-lo."[1] M. J. E. Golay conseguiu estender alguns resultados dados no artigo de Shannon, publicando em julho de 1949 no Proceedings of Institute of Radio Engineers seu trabalho, o qual foi intitulado "Notes on Digital Coding."

As ideias destes pesquisadores foram aprimoradas e, atualmente, temos diversas aplicabilidades desta teoria, tais como telefones celulares, gravadores, DVD, internet, rádio, comunicações via Satélite, entre outras.

Para a construção de Códigos Corretores de Erros precisa-se de alguns elementos básicos: de um conjunto finito A qualquer, chamado **alfabeto,** de uma sequência finita de n símbolos de A chamada **palavra de comprimento** n e de um **código de comprimento** n que é qualquer subconjunto próprio de A^n, para algum n natural.

Neste trabalho tratamos de códigos dotados de certa estrutura algébrica, para isso consideramos F_q um corpo de q elementos como sendo nosso alfabeto. Assim temos em F_q^n uma estrutura de espaço vetorial de dimensão n sobre F_q. Em particular, estudamos Códigos Abelianos Minimais, vistos como ideais de uma álgebra

[1] R.W. Hamming, Interview, fevereiro de 1977 [5].

de grupo F_qG, onde G é um p-grupo abeliano finito.

Inicialmente fizemos um breve estudo sobre anéis de grupo e sobre a teoria de códigos corretores de erros os quais compõem o capítulo 1 desta dissertação e no capítulo 2 estudamos os artigos: *"Minimal Codes of Prime-Power Length"* de S. K. Arora e Manju Pruthi e *"Idempotents in group algebras and minimal abelian codes"*, de Raul Antonio Ferraz e César Polcino Milies; os quais são a base deste trabalho.

No primeiro artigo, o qual foi publicado em 1997, foram encontrados os idempotentes primitivos da álgebra F_qG, em dois casos, primeiro quando $G = \langle g \rangle = C_n$ é um grupo cíclico finito de ordem n e F_q é um corpo com q elementos, tal que $q = n\Gamma + 1$ para algum inteiro $\Gamma > 0$, isto é, $q \equiv 1 \pmod{n}$, e depois quando $G = \langle g \rangle = C_{p^n}$ é um grupo cíclico de ordem p^n e F_q é um corpo de ordem potência prima q, onde a ordem de q módulo p^n é $\phi(p^n)$, sendo ϕ a função de Euler, caracterizando assim os códigos cíclicos minimais destas álgebras de grupo. Estes autores calcularam os idempotentes de F_qG com G e F_q nas hipóteses do segundo caso usando as classes q-ciclotômicas.

No artigo de Ferraz e Milies, publicado em 2007, são encontrados também os idempotentes de F_qG conforme as condições do segundo caso descrito acima, mas a abordagem feita por estes autores é mais prática. Estes idempotentes são também os códigos cíclicos minimais de comprimento p^n sobre F_q. Neste artigo é calculado o número de componentes simples da álgebra de grupo semissimples e, mostra-se que este número corresponde ao número de idempotentes primitivos desta álgebra de grupo. Além disso, se encontra também a distância mínima, a dimensão, o peso e o polinômio gerador destes códigos minimais.

O texto termina com algumas considerações onde apresentamos perspectivas de continuidade do tema estudado e trabalhos relacionados a esta área.

Capítulo 1

Preliminares

Neste primeiro capítulo apresentaremos algumas definições e resultados básicos de anéis de grupos, álgebras semissimples e da Teoria de Códigos Corretores de Erros, fundamentais no desenvolvimento deste trabalho.

1.1 Anéis de Grupos

Sejam R um anel com unidade e G um grupo, definimos RG como sendo o conjunto de todas as combinações lineares formais finitas:

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

onde $\alpha_g \neq 0$ para um número finito de $g \in G$.

Dados dois elementos α e β, definimos a soma, a multiplicação e a multiplicação por escalar da seguinte forma:

- $\sum\limits_{g \in G} \alpha_g g + \sum\limits_{g \in G} \beta_g g = \sum\limits_{g \in G} (\alpha_g + \beta_g) g$;
- $(\sum\limits_{g \in G} \alpha_g g)(\sum\limits_{h \in G} \beta_h h) = \sum\limits_{g,h \in G} \alpha_g \beta_h gh = \sum\limits_{j \in G} \gamma_j j$, sendo $\gamma_j = \sum\limits_{gh=j} \alpha_g \beta_h$;
- $\lambda(\sum\limits_{g \in G} \alpha_g g) = \sum\limits_{g \in G} (\lambda \alpha_g) g, \text{com } \lambda \in R.$

Note que se associamos $g \in G$ com $1 \cdot g \in RG$, podemos considerar G contido em RG, e assim os elementos de G formam uma base de RG como R-módulo. Observemos que $1 \in G$ é a unidade de RG.

O conjunto RG com as operações definidas acima é um anel, chamado o **anel de grupo de G sobre R.** Quando R é um anel comutativo, RG tem uma estrutura de álgebra sendo, portanto, chamado **álgebra de grupo de G sobre R.** No que segue, F representa um corpo.

Proposição 1.1 *([13], Proposição 1) Sejam A uma F-álgebra, G um grupo, $\mathcal{U}(A)$ o grupo das unidades de A e*

$$\eta : G \to \mathcal{U}(A)$$

um homomorfismo de grupo. Então, a aplicação

$$\zeta : FG \to A$$

definida por

$$\zeta\left(\sum_{g\in G} \alpha_g g\right) := \sum_{g\in G} \alpha_g \eta(g)$$

é um homomorfismo de F-álgebras.

Consideremos $H \triangleleft G$, então existe o homomorfismo de G em G/H, consequentemente de G no grupo das unidades da álgebra de grupo $F[G/H]$ e, pela proposição 1.1, existe um homomorfismo natural:

$$\epsilon : FG \to F[G/H]$$

definido por:

$$\epsilon\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g \bar{g},$$

onde $\bar{g}$ é a imagem de g em G/H.

Observemos que se $H = G$, então $G/H = \{1\}$ e $\bar{g} = 1$ para todo $g \in G$. Portanto, neste caso particular, o homomorfismo é dado por:

$$\epsilon\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g.$$

O núcleo desta aplicação, denotado por $\Delta(G)$, é chamado o **ideal de aumento** de FG, isto é,

$$Ker(\epsilon) = \Delta(G) = \left\{ \sum_{g \in G} \alpha_g g : \sum_{g \in G} \alpha_g = 0 \right\}.$$

Notemos que se um elemento $\alpha = \sum_{\alpha \in G} \alpha_g g \in \Delta(G)$, então podemos escrever α da seguinte forma

$$\alpha = \sum_{g \in G} \alpha_g (g-1) + \sum_{g \in G} \alpha_g = \sum_{g \in G} \alpha_g (g-1).$$

Assim concluímos facilmente que $\Delta(G)$ é um F-módulo livre com base $\{g-1 : 1 \neq g \in G\}$.

Um conceito fundamental na teoria de anéis de grupos é o conceito de semissimplicidade.

Dizemos que uma álgebra A é **simples** se $A \neq \{0\}$ e seus únicos ideais são (0) e A.

Definição 1.2 *Uma álgebra A é **semissimples,** se A é semissimples como A-módulo à esquerda, isto é, se A como A-módulo é soma direta de módulos simples.*

Uma pergunta natural é que condições tem que cumprir um anel R e um grupo G para que o anel FG seja semissimples. O Teorema de Maschke dá resposta a esta pergunta. Antes de enunciar este teorema, precisamos de algumas definições e resultados:

Dado $\alpha \in RG$, define-se o **suporte** de α como sendo o subconjunto de G, formado pelos elementos $g \in G$ com coeficiente não nulo em α, isto é:

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

Seja X um subconjunto de um anel de grupo RG, o **anulador à esquerda** de X é definido como:

$$Anl_e(X) = \{\alpha \in RG : \alpha X = 0\}.$$

De forma análoga, o **anulador à direita** é

$$Anl_d(X) = \{\alpha \in RG : X\alpha = 0\}.$$

Se $Anl_e(X) = Anl_d(X)$ denotamos por $Anl(X)$ **o anulador de** X.

Lema 1.3 *([9], Capítulo 3, Lema 3.4.3) Sejam H um subgrupo de um grupo G e R um anel. Então $Anl_d(\Delta(G,H)) \neq 0$ se, e somente se, H é finito. Neste caso temos que*

$$Anl_d(\Delta(G,H)) = \tilde{H} \cdot RG,$$

onde $\tilde{H} = \sum_{h\in H} h$. Além disso, se $H \lhd G$ então $\tilde{H}$ é central em RG e temos

$$Anl_d(\Delta(G,H)) = Anl_e(\Delta(G,H)) = RG \cdot \tilde{H}.$$

Corolário 1.4 *Se G é um grupo finito, então*

$$Anl_e(\Delta(G)) = Anl_d(\Delta(G)) = Anl(\Delta(G)) = \left\{ a\sum_{g\in G} g : a \in R \right\}.$$

Demonstração:

De fato, seja

$$\begin{aligned} Anl(\Delta(G)) &= \{\alpha \in RG : x\alpha = 0, \forall\ x \in \Delta(G)\} \\ &= \{\alpha \in RG : (g-1)\alpha = 0, \forall\ g \in G\}. \end{aligned}$$

Por outro lado, escrevendo $\alpha = \sum_{h\in G} \alpha_h h$, como $\alpha \in Anl(\Delta(G))$, então para todo $g \in G$ temos

$$\begin{aligned} 0 = (g-1)\alpha &= (g-1)\sum_{h\in G} \alpha_h h \\ &= \sum_{h\in G} \alpha_h gh - \sum_{h\in G} \alpha_h h \\ &= \sum_{g^{-1}m\in G} \alpha_{g^{-1}m} m - \sum_{m\in G} \alpha_m m, \end{aligned}$$

logo $\alpha_{g^{-1}m} = \alpha_m$ para todo $g \in G$, segue que $\sum_{m\in G} \alpha_m m = \beta \sum_{m\in G} m = \beta\tilde{G}$, onde $\beta \in R$, e $\tilde{G} = \sum_{m\in G} m$. Portanto,

$$Anl(\Delta(G)) \subset R\tilde{G}.$$

Tomemos agora $x \in \Delta(G)$ tal que $x = \sum_{j=1}^{t} a_j g_j$, temos que

$$x\tilde{G} = \sum_{j=1}^{t} a_j g_j \tilde{G} = \sum_{j=1}^{t} a_j \tilde{G} = 0,$$

pois $\sum_{j=1}^{t} a_j = 0$. Assim concluímos que

$$Anl(\Delta(G)) = R\tilde{G}.$$

□

Lema 1.5 *Seja $\Delta(G)$ o ideal de aumento de RG, onde G é um grupo finito. Se existe um ideal à esquerda J de RG tal que $RG = \Delta(G) \oplus J$ (como R-módulos à esquerda), então $J \subset Anl(\Delta(G))$.*

Demonstração:

Pelo lema anterior, basta provar que se $y \in J$ então $xy = 0$, para todo $x \in \Delta(G)$. Como J é um ideal à esquerda de RG, $xy \in J$, de forma análoga $xy \in \Delta(G)$, pois $\Delta(G)$ é o ideal de aumento de RG. Mas $J \cap \Delta(G) = \{0\}$, logo $xy = 0$, isto é, $y \in Anl(\Delta(G))$.

□

Teorema 1.6 (Teorema de Maschke) *Sejam G um grupo e R um anel com unidade. Então RG é semissimples se, e somente se, as seguintes condições valem:*

i) R é um anel semissimples;

ii) G é finito;

iii) $|G|$ é invertível em R.

Demonstração:

Suponhamos que RG é semissimples, assim o ideal de aumento:

$$\Delta(G) = \left\{ \sum_{g \in G} \alpha_g g \in RG : \sum_{g \in G} \alpha_g = 0 \right\}$$

é semissimples. Este ideal é gerado pelo conjunto $\{g - 1 : 1 \neq g \in G\}$. Consideremos agora

$$\begin{array}{rcl} \psi : RG & \to & R \\ \sum\limits_{g\in G} \alpha_g g & \mapsto & \sum\limits_{g\in G} \alpha_g \end{array} \tag{1.1}$$

Note que ψ é um epimorfismo de anéis, logo pelo Primeiro Teorema do Isomorfismo,

$$\frac{RG}{Ker(\psi)} \cong Im(\psi) = R.$$

Como $Ker(\psi) = \{\alpha \in RG : \psi(\alpha) = 0\} = \Delta(G)$, temos:

$$R \cong \frac{RG}{\Delta(G)}.$$

Portanto, R é semissimples, pois o quociente de anéis semissimples é semissimples.

Agora suponhamos, por absurdo, que G é infinito. Seja $\alpha \in Anl_d(\Delta(G))$, como $supp(\alpha) = \{g \in G : \alpha_g \neq 0\}$ é finito, temos que

$$\alpha = \sum_{g\in G} \alpha_g g = \sum_{i=1}^{t} a_i g_i, \quad \text{com} \quad a_i \neq 0.$$

Sendo G infinito, existe um elemento $h \in G$, tal que $g_i h \neq g_1$, com $1 \leq i \leq t$. Por outro lado, como $h - 1 \in \Delta(G)$, temos

$$0 = \alpha(h-1) = (\sum_{i=1}^{t} a_i g_i)(h-1) = \sum_{i=1}^{t} a_i g_i h - \sum_{i=1}^{t} a_i g_i.$$

Observemos que, na expressão acima, o coeficiente de g_1 é $a_1 \neq 0$. Mas isto é uma contradição já que G é uma base para RG. Logo G é finito.

Resta verificar que $|G|$ é invertível em R. Sabemos que $\Delta(G)$ é somando direto de RG, isto é,

$$RG = \Delta(G) \oplus J,$$

e que G é finito, então

$$J \subset Anl(\Delta(G)).$$

Como $1 \in RG$, podemos escrever $1 = c_1 + c_2$ em que $c_1 \in \Delta(G)$ e $c_2 \in J$. Seja ψ o epimorfismo dado em (1.1), página 6, tal que

$$1 = \psi(1) = \psi(c_1 + c_2) = \psi(c_1) + \psi(c_2).$$

Como $c_1 \in \Delta(G), \psi(c_1) = 0$, então temos que $\psi(c_2) = 1$. Como G é finito pelo corolário 1.4 temos $Anl_d(\Delta(G)) = Anl_e(\Delta(G)) = Anl(\Delta(G)) = R\tilde{G}$, onde $\tilde{G} =$

$\sum_{g\in G} g$. Disto segue que c_2 é da forma $a\tilde{G}$, com $a \in R$, logo $\psi(c_2) = 1 = \psi(a\tilde{G}) = a\psi(\tilde{G})$. Como

$$\begin{aligned}\psi(\tilde{G}) &= \psi(g_1 + g_2 + \cdots + g_t) \\ &= \psi(g_1) + \psi(g_2) + \cdots + \psi(g_t) \\ &= |G|\end{aligned}$$

então $1 = a\psi(\tilde{G}) = a|G|$, ou seja, $|G|$ é invertível em R.

Agora suponhamos que as três condições do teorema valem e seja M um RG-submódulo de RG, temos que provar que M é somando direto de RG. Observemos que M é um R-submódulo de RG. Por hipótese temos que R é semissimples, o que implica que RG é semissimples como um R-módulo. Então, existe um R-submódulo N de RG tal que $RG = M \oplus N$ (como R-módulos).

Seja $\pi : RG \to M$ a projeção canônica associada à soma direta dada acima, assim π é um R-homomorfismo, e seja $\pi^* : RG \to RG$ definido da seguinte forma:

$$\pi^*(\alpha) := \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(g\alpha), \quad \text{para todo } \alpha \in RG.$$

Note que $Im(\pi^*) \subset M$, já que $Im(\pi) \subset M$, e além disso M é um RG-módulo. Se provamos que π^* é um RG-homomorfismo tal que $(\pi^*)^2 = \pi^*$ e $Im(\pi^*) = M$, então $Ker(\pi^*)$ será um RG-submódulo tal que $RG = M \oplus Ker(\pi^*)$ e, desta forma, o teorema estará provado. Como π^* é um R-homomorfismo, então temos que mostrar que é também um RG-homomorfismo. Para isso, basta mostrar que $\pi^*(ha) = h\pi^*(a)$, para todo $h \in G$, para todo $a \in RG$. De fato,

$$\begin{aligned}\pi^*(ha) &= \tfrac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gha) \\ &= \tfrac{1}{|G|}h\sum_{g\in G}(gh)^{-1}\pi(gha).\end{aligned}$$

Fazendo $g' = gh$, obtemos que

$$\begin{aligned}\pi^*(ha) &= h\tfrac{1}{|G|}\sum_{g'\in G} g'^{-1}\pi(g'a) \\ &= h\pi^*(a).\end{aligned}$$

Além disso, temos que

$$\pi^*(a+b) = \pi^*(a) + \pi^*(b).$$

Mas π é uma projeção sobre M, então $\pi(m) = m$, para todo $m \in M$. Como M é um RG-módulo, então temos que $gm \in M$, para todo $g \in G$. Portanto:

$$\begin{aligned}
\pi^*(m) &= \tfrac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm) \\
&= \tfrac{1}{|G|} \sum_{g \in G} g^{-1}gm \\
&= \tfrac{1}{|G|} \sum_{g \in G} m \\
&= \tfrac{1}{|G|}|G|m \\
&= m.
\end{aligned}$$

Como $Im(\pi^*) \subset M$ obtemos $\pi^*(\pi^*(x)) = \pi^*(x)$, para todo $x \in RG$, o que nos leva a concluir que $(\pi^*)^2 = \pi^*$. O fato de $\pi^*(m) = m$, para todo $m \in M$ implica também que $M \subset Im(\pi^*)$, o que conclui a demonstração deste teorema. □

Corolário 1.7 *Sejam G um grupo finito e F um corpo, então FG é semissimples se, e somente se, $car(F)$ não divide $|G|$.*

Observação 1.8 *Se $G = \langle a : a^n = 1\rangle$ é um grupo cíclico de ordem n e F um corpo de característica k que não divide n, então a aplicação $\psi : F[x] \to FG$ dada por $f(x) \to f(a)$ é um epimorfismo de anéis, logo $FG \cong \dfrac{F[x]}{Ker(\psi)}$, onde $Ker(\psi) = \{f(x) \in F[x] : f(a) = 0\}$. Como $F[x]$ é um domínio de ideais principais, $Ker(\psi)$ é gerado pelo polinômio mônico de menor grau que é nulo em a. Se chamamos este polinômio de $f_a(x)$, o elemento a corresponde à classe $x + \langle f_a\rangle \in \dfrac{F[x]}{\langle f_a\rangle}$.*

Seja $x^n - 1 = p_1p_2\cdots p_m$ a decomposição de $x^n - 1$ em fatores irredutíveis em $F[x]$. Como $mdc(k, n) = 1$, $x^n - 1$ é separável sobre F, logo $p_i \neq p_j$ para $i \neq j$. Pelo Teorema Chinês dos Restos podemos escrever

$$FG \cong \frac{F[x]}{\langle p_1\rangle} \oplus \frac{F[x]}{\langle p_2\rangle} \oplus \cdots \oplus \frac{F[x]}{\langle p_m\rangle}.$$

Se ξ_i é uma raiz de p_i, $1 \leq i \leq m$ então $\frac{F[x]}{\langle p_i\rangle} \cong F(\xi_i)$ e, consequentemente,

$$FG \cong F(\xi_1) \oplus F(\xi_2) \oplus \cdots \oplus F(\xi_m),$$

assim FG é soma direta de extensões ciclotômicas de F.

Por outro lado, $x^n - 1 = \prod_{d|n} \Phi_d(x)$ *em* $F[x]$*, onde o polinômio*

$$\Phi_d(x) = \prod_{i=1}^{\phi(d)} (x - \alpha_i),$$

sendo α_i *as raízes d-ésimas primitivas da unidade,* Φ_d *o d-ésimo polinômio ciclotômico sobre* F *e* ϕ *a função de Euler, isto é,*

$$\phi(d) = |\{n \in \mathbb{Z} : 1 \leq n < d, mdc(n, d) = 1\}|.$$

Se prova indutivamente, usando a fórmula $\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}$*, que* $\Phi_n(x) \in F[x]$*.*

Agora, se $\Phi_d(x) = \prod_{i=1}^{a_d} P_{d_i}$ *é a decomposição de* Φ_d *como produto de irredutíveis em* $F[x]$*, então temos que*

$$FG \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \frac{F[x]}{\langle P_{d_i} \rangle} \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} F(\xi_{d_i}),$$

onde ξ_{d_i} *é uma raiz de* P_{d_i}*,* $1 \leq i \leq a_d$*, mais ainda* $FG \simeq \bigoplus_{d|n} a_d F(\xi_d)$ *onde* $a_d = \frac{\phi(d)}{[F(\xi_d):F]}$*.*

O teorema de Perlis e Walker estende o resultado anterior para grupos abelianos finitos, isto é, mostra que o número de componentes simples de uma álgebra de grupo de um grupo abeliano finito G *é igual ao número de subgrupos cíclicos de* G*.*

Teorema 1.9 (Perlis-Walker) *([9], Capítulo 3, Teorema 3.5.4)*

Sejam G *um grupo abeliano finito de ordem* n *e* F *um corpo tal que* $car(F)$ *não divide* $|G|$*. Então*

$$FG \simeq \bigoplus_{d|n} a_d F(\xi_d),$$

onde ξ_d *denota uma raiz d-ésima primitiva da unidade e* $a_d = \frac{n_d}{[F(\xi_d) : F]}$*. Nesta fórmula,* n_d *denota o número de elementos de ordem* d *de* G*.*

Em particular, para $F = \mathbb{Q}$ *temos o seguinte corolário:*

Corolário 1.10 *([9], capítulo 3, Corolário 3.5.5) Seja* G *um grupo abeliano finito de ordem* n*. Então*

$$\mathbb{Q}G \simeq \bigoplus_{d|n} a_d \mathbb{Q}(\xi_d),$$

onde ξ_d denota uma raiz d-ésima primitiva da unidade e a_d é o número de subgrupos cíclicos de ordem d em G.

Os elementos idempotentes são fundamentais no estudo da decomposição de álgebras semissimples. A seguir daremos alguns resultados sobre eles.

Definição 1.11 *Um elemento $e \neq 0$ numa álgebra A é dito* ***idempotente*** *se $e^2 = e$. Um idempotente e é dito* ***primitivo*** *se ele não pode ser escrito como $e = e' + e''$, onde e', e'' são idempotentes não nulos tais que $e' \cdot e'' = 0$. Uma família de idempotentes $e_1, \cdots, e_t$ satisfazendo as seguintes condições:*

i) $e_i \neq 0$ *para todo* $1 \leq i \leq t$;

ii) se $i \neq j$ *então* $e_i e_j = 0$;

iii) $1 = e_1 + \cdots + e_t$;

é chamada uma ***família completa de idempotentes ortogonais.***

Observemos que 1 é idempotente. Se e é um idempotente, $1 - e$ também é um idempotente, mais ainda, e e $1 - e$ são idempotentes ortogonais. De fato,

$$\begin{aligned} (1-e)^2 &= 1 - 2e + e^2 \\ &= 1 - 2e + e \\ &= 1 - e \end{aligned}$$

e

$$\begin{aligned} e \cdot (1-e) &= e - e^2 \\ &= e - e \\ &= 0. \end{aligned}$$

Observação 1.12 *Se H é um subgrupo finito de um grupo G, tal que $|H|$ é invertível em F, define-se $\hat{H} \in FG$ como*

$$\hat{H} = \frac{1}{|H|} \sum_{h \in H} h.$$

Temos que $\hat{H}$ é um idempotente de FG. De fato,

$$\begin{aligned}\hat{H}^2 &= \left(\tfrac{1}{|H|}\sum_{h\in H} h\right)\left(\tfrac{1}{|H|}\sum_{h'\in H} h'\right)\\ &= \tfrac{1}{|H|^2}\sum_{h\in H} h\sum_{h'\in H} h'\\ &= \tfrac{1}{|H|^2}|H|\sum_{h\in H} h\\ &= \tfrac{1}{|H|}\sum_{h\in H} h\\ &= \hat{H}.\end{aligned}$$

Observemos que se $\hat{H}$ é central em FG então $\hat{H} = g^{-1}\hat{H}g$, para todo $g \in G$, isto é,

$$\frac{1}{|H|}\sum_{h\in H} h = \frac{1}{|H|}\sum_{h\in H} g^{-1}hg,$$

assim

$$\sum_{h\in H} h = \sum_{h\in H} g^{-1}hg.$$

Logo todo elemento da forma $g^{-1}hg$ pertence a H, para todo $g \in G$ e $h \in H$, portanto, $H \triangleleft G$. Notemos também que se $H \triangleleft G$, então $\hat{H}$ é central em FG. Desta forma, $\hat{H}$ é central em FG se, e somente se, H é normal em G.

Proposição 1.13 *([13], Proposição 4) Se H é um subgrupo normal e finito de G com $|H| \neq 0$ em F, então*

$$FG \cdot \hat{H} \cong F[G/H].$$

Proposição 1.14 *([9] Proposição 3.6.7) Sejam R um anel, G um grupo e H um subgrupo normal de G. Se $|H|$ é invertível em R e $\hat{H} = \dfrac{1}{|H|}\displaystyle\sum_{h\in H} h$, então temos:*

$$RG = RG\hat{H} \oplus RG(1 - \hat{H})$$

onde $RG\hat{H} \simeq R[G/H]$ e $RG(1-\hat{H}) = \Delta(G, H)$ é o núcleo do homomorfismo natural de RG em $R[G/H]$.

Consideremos M e N R-módulos. Definimos o **produto tensorial** de M e N como um R-módulo $M \bigotimes N$ junto com uma aplicação bilinear $M \times N \to M \bigotimes N$, denotada por $(u, v) \mapsto u \otimes v$, tal que:

i) $M \bigotimes N$ é gerado como R-módulo por $\{u \otimes v : u \in M, v \in N\}$;

ii) Se $\Psi : M \times N \to P$ é uma aplicação bilinear de R-módulos (isto é, $\psi(u, *) : N \to P$ e $\psi(*, v) : M \to P$ são homomorfismos de R-módulos para todo $u \in M, v \in N$), então existe um homomorfismo $\psi : M \bigotimes N \to P$ tal que $\psi(u \otimes v) = \Psi(u, v)$ para todo $u \in M$ e $v \in N$.

Uma prova da existência e unicidade salvo isomorfismo do produto tensorial pode ser encontrada no livro de Pierce [11] cap. 9.

Se X e Y são F-álgebras, então são também F-módulos, e assim podemos formar o produto tensorial $X \bigotimes Y$. Logo no F-módulo $X \bigotimes Y$, define-se uma estrutura de F-álgebras com a seguinte multiplicação:

$$(x \otimes y)(x' \otimes y') = xx' \otimes yy' \quad \text{para} \quad x, x' \in X \quad \text{e} \quad y, y' \in Y.$$

Proposição 1.15 *([11], Capítulo 9, Proposição a) Sejam $M, M_1, M_2, N, N_1,$ e N_2 R-módulos, temos que $M \otimes (N_1 \oplus N_2) \cong (M \otimes N_1) \oplus (M \otimes N_2)$ é um isomorfismo que aplica $u \otimes (v_1, v_2)$ em $(u \otimes v_1, u \otimes v_2)$*

Proposição 1.16 *([13], Proposição 5) Seja S um subanel do anel comutativo R, então para qualquer grupo G, $R \bigotimes_S SG \cong RG$ como R-álgebras.*

Proposição 1.17 *Sejam G e H grupos e F um corpo, então*

$$F[G \times H] \cong FG \otimes FH.$$

Demonstração:

Observemos que $\{x \otimes y : x \in G, y \in H\}$ é uma F-base para $FG \otimes FH$ e que a aplicação :

$$\begin{aligned} \psi : G \times H &\to FG \otimes FH \\ (x, y) &\mapsto x \otimes y \end{aligned}$$

é um homomorfismo injetivo.

Pela injetividade e pelo fato de $FG \otimes FH$ ser gerado por $\psi(G \times H)$ como F-álgebra, temos que

$$F[G \times H] \cong FG \otimes FH.$$

□

A seguir daremos alguns resultados sobre teoria de caracter para grupos abelianos finitos.

Definição 1.18 *Seja G um grupo abeliano, G é chamado* ***grupo divisível*** *se para todo $x \in G$ e $n \geq 2$ existe $y \in G$ tal que $\underbrace{y + y + \cdots + y}_{n \text{ vezes}} = x$.*

Exemplos de grupos divisíveis são $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}^*, \cdot)$. Além disso, se G é um grupo divisível e $H < G$ então G/H também é divisível, assim por exemplo, $\mathbb{Q}/\mathbb{Z}$ é um grupo divisível. De igual forma como a aplicação

$$\begin{array}{ccc} (\mathbb{Q}/\mathbb{Z}, +) & \stackrel{\tau}{\to} & (\mathbb{C}^*, \cdot) \\ a & \mapsto & e^{2\pi i a} \end{array}$$

é um homomorfismo de grupos então $Im(\tau) = \{a \in \mathbb{C}^* : a^n = 1 \text{ para algum } n \in \mathbb{N}^*\}$ é um grupo divisível.

Teorema 1.19 (Propriedade Injetiva, Baer, 1940) *Seja D um grupo divisível e seja A um subgrupo de um grupo B. Se $f : A \to D$ é um homomorfismo de grupos, então f pode ser estendido a um homomorfismo de grupos $\psi : B \to D$, isto é, o seguinte diagrama comuta:*

$$\begin{array}{ccc} D & & \\ {\scriptstyle f}\uparrow & \nwarrow\ \searrow\ {\scriptstyle \psi} & \\ A & \xhookrightarrow[i]{} & B. \end{array}$$

Demonstração:

Consideremos o conjunto $\mathcal{L}$ de todos os pares (S, h), onde $A \leq S \leq B$ e $h : S \to D$ é um homomorfismo de grupos com $h\restriction_A = f$. Notemos que $\mathcal{L} \neq \emptyset$, pois $(A, f) \in \mathcal{L}$. Ordenamos parcialmente $\mathcal{L}$ da seguinte forma: $(S, h) \preceq (S', h')$ se $S \leq S'$ e h' estende h, isto é, $h'\restriction_S = h$. Se $\mathcal{J} = \{S_\alpha, h_\alpha\}$ é um subconjunto ordenado de $\mathcal{L}$, definimos $(\tilde{S}, \tilde{h})$ por $\tilde{S} = \bigcup_\alpha S_\alpha$ e $\tilde{h} = \bigcup_\alpha h_\alpha$. Assim, se $s \in \tilde{S}$, então $s \in S_\alpha$ para algum α, e $\tilde{h}(s) = h_\alpha(s)$ que independe do representante h_α. Logo $(\tilde{S}, \tilde{h}) \in \mathcal{L}$ e é uma cota superior de $\mathcal{J}$. Pelo lema de Zorn, existe um par maximal $(M, g) \in \mathcal{L}$. Para completar a prova, resta mostrar que $M = B$.

Suponhamos que existe $b \in B$, com $b \notin M$. Se $M' = \langle M, b\rangle$, então $M < M'$, e assim é suficiente definir $g' : M' \to D$ que estende g para chegar a uma contradição.

- Caso 1: $M \cap \langle b\rangle = \{0\}$.

Neste caso $M' = M \oplus \langle b\rangle$, e assim podemos definir g' como a função $m + kb \mapsto g(m)$, que é um homomorfismo de grupos bem definido porque cada elemento de $M + \langle b\rangle$ tem uma única representação na forma $m + kb$.

- Caso 2: $M \cap \langle b\rangle \neq \{0\}$.

Neste caso existe $k \in \mathbb{Z}^*$ tal que $kb \in M \cap \langle b\rangle$. Como a interseção é um grupo então o inverso $-kb$ também pertence a $M \cap \langle b\rangle$, assim existe um inteiro positivo $\tilde{k}$ tal que $\tilde{k}b \in M \cap \langle b\rangle$. Seja k o menor inteiro positivo tal que $kb \in M$. Como $M \cap \langle b\rangle$ tem um único gerador, concluímos que $M \cap \langle b\rangle = \langle kb\rangle$. Assim cada $y \in M'$ tem uma única expressão na forma $y = m + tb$, onde $0 \leq t < k$. De fato se $y = m_1 + t_1 b = m_2 + t_2 b$, são duas representações com $k > t_1 > t_2 \geq 0$, então $m_2 - m_1 = (t_1 - t_2)b$, logo $(t_1 - t_2)b \in M$ e $0 < t_1 - t_2 < k$ o que contradiz a minimalidade de k. Como $g(kb) \in D$ e D é divisível, então existe $c_b \in D$ tal que $kc_b = g(kb)$. Considerando cada elemento de M' escrito de maneira única na forma $m + tb$ com $0 \leq t < k$, definimos

$$\begin{aligned} g' : M' &\to D \\ m + tb &\mapsto g(m) + tc_b. \end{aligned}$$

Temos que g' é um homomorfismo de grupos. De fato, se $0 \leq t_i < k$, e $m_i \in M$, então existem $n \in \mathbb{N}$ e $0 \leq t < k$ tais que $t_1 + t_2 = kn + t$. Logo

$$\begin{aligned} g'\left((m_1 + t_1 b) + (m_2 + t_2 b)\right) &= g'\left((m_1 + m_2) + (t_1 + t_2)b\right) \\ &= g'\left(m_1 + m_2 + (kn + t)b\right) \\ &= g'\left((m_1 + m_2 + knb) + tb\right) \\ &= g(m_1 + m_2 + knb) + tc_b \\ &= g(m_1) + g(m_2) + g(knb) + tc_b \\ &= g(m_1) + g(m_2) + nkc_b + tc_b \\ &= g(m_1) + g(m_2) + (t_1 + t_2)c_b \\ &= g(m_1) + g(m_2) + t_1 c_b + t_2 c_b \\ &= g'(m_1 + t_1 b) + g'(m_2 + t_2 b). \end{aligned}$$

□

Definição 1.20 *Seja G um grupo, o* ***grupo de caracteres de*** *G é definido como*

$$G^* = Hom(G, \mathbb{Q}/\mathbb{Z}),$$

isto é, um caracter de G é um homomorfismo $\chi : G \to \mathbb{Q}/\mathbb{Z}$.

Quando G é finito, temos os seguintes resultados:

Lema 1.21 *Se G é abeliano e finito, então $G^* \cong Hom(G, \mathbb{C}^*)$.*

Demonstração:
Temos que $\mathbb{C}^* \cong \mathbb{Q}/\mathbb{Z} \oplus D$, onde $\mathbb{Q}/\mathbb{Z}$ é um grupo de torção e D é um grupo divisível livre de torção. Então

$$\begin{aligned} Hom(G, \mathbb{C}^*) &\simeq Hom(G, \mathbb{Q}/\mathbb{Z} \oplus D) \\ &\simeq Hom(G, \mathbb{Q}/\mathbb{Z}) \otimes Hom(G, D) \quad \text{(conforme teorema 10.53 de [12])} \\ &\simeq Hom(G, \mathbb{Q}/\mathbb{Z}), \end{aligned}$$

pois como G é finito, $Hom(G, D) = 0$. □

Teorema 1.22 *Se G é abeliano e finito, então $G \cong G^*$.*

Demonstração:

No caso em que G é cíclico de ordem m, e $G = \langle \sigma \rangle$, então para todo $\chi \in G^*$ temos $[\chi(\sigma)]^m = \chi(\sigma^m) = 1$, isto é, $\chi(\sigma)$ é raiz m-ésima da unidade. Por outro lado, se $y \in \mathbb{C}^*$, com $y^m = 1$, temos que a aplicação $\sigma^n \mapsto y^n$ é um caracter. Disso segue que $|G^*| = m$.

No caso em que G não é cíclico, pelo teorema de representação de grupos abelianos finitos temos que $G \cong G_1 \oplus G_2 \oplus \cdots \oplus G_n$, onde cada G_i é cíclico de ordem m_i e gerador σ_i. Assim para aplicarmos o que foi usado no caso cíclico, devemos mostrar que $G^* \cong {G_1}^* \oplus \cdots \oplus {G_n}^*$. Se χ_i é caracter de G_i, $i = 1, 2$ então $(x_1, x_2) \mapsto \chi_1(x_1)\chi_2(x_2)$ é um caracter de $G_1 \oplus G_2$, onde $x_i \in G_i$, $i = 1, 2$. Reciprocamente, se χ é caracter de $G_1 \oplus G_2$ então $x_1 \mapsto \chi(x_1, e_2)$ é caracter de G_1 e

$x_2 \mapsto \chi(e_1, x_2)$ é caracter de G_2, onde $e_i \in G_i$ é a identidade do grupo G_i, $i = 1, 2$. Como as funções do tipo $(x_1, x_2) \mapsto \chi_1(x_1)\chi_2(x_2)$ são inversas às funções do tipo $x_1 \mapsto \chi(x_1, e_2); x_2 \mapsto \chi(e_1, x_2)$, segue-se o resultado, isto é, todo caracter pode-se escrever como produto de suas projeções. □

Lema 1.23 *Se G é um grupo abeliano finito e $H < G$, então G contém um subgrupo K tal que G/K é isomorfo a H.*

Demonstração:

Sabemos que $G \cong G^*$. Seja $H < G$, definimos o homomorfismo de grupos

$$\begin{array}{ccc} G^* = Hom(G, \mathbb{Q}/\mathbb{Z}) & \stackrel{\psi}{\to} & Hom(H, \mathbb{Q}/\mathbb{Z}) = H^* \\ \varphi & \mapsto & \varphi\restriction_H \end{array}$$

Afirmamos que ψ é sobrejetiva. Se $\eta \in Hom(H, \mathbb{Q}/\mathbb{Z})$, temos:

$$\begin{array}{ccc} & & \mathbb{Q}/\mathbb{Z} \\ & \nearrow^{\varphi} & \uparrow{\scriptstyle \eta} \\ H & \xrightarrow[i]{} & G, \end{array}$$

então pelo teorema 1.19 existe um φ que estende η. Logo o homomorfismo ψ é sobrejetivo e, portanto, pelo teorema do isomorfismo de grupos temos:

$$\frac{G^*}{Ker\psi} \cong H^* \cong H.$$

como queríamos demonstrar. □

Teorema 1.24 *Dado um grupo G abeliano finito, então a aplicação*

$$\begin{array}{ccc} \{\textit{subgrupos de } G\} & \stackrel{T}{\to} & \{\textit{subgrupos de } G^*\} \\ H & \longmapsto & \{\varphi \in G^* : \varphi\restriction_H \equiv 0\} \end{array}$$

está bem definida e é uma bijeção. Além disso, $\frac{G^*}{T(H)} \simeq H$ para todo $H < G$.

Demonstração:

Observemos que $\frac{G^*}{T(H)} \simeq H$ e que a aplicação T está bem definida seguem diretamente do lema 1.23. Falta mostrar que T é uma bijeção. Como G é abeliano finito, então $G \simeq G^*$ e assim os dois têm a mesma quantidade finita de subgrupos. Logo basta mostrar que T é injetiva. Sejam H_1, H_2 subgrupos distintos de G, assim podemos supor, sem perda de generalidade, que existe $h \in H_1 \backslash H_2$ e seja $k \geq 2$ o menor inteiro tal que $h^k \in H_2$. Note que este inteiro sempre existe já que $h^{o(h)} = 1 \in H_2$, onde $o(h)$ denota a ordem de h. Definimos o homomorfismo de grupos

$$\eta : \langle H_2, h \rangle \to \mathbb{Q}/\mathbb{Z}$$

tal que $\eta(h) = \frac{1}{k}$ e $\eta(g) = 0$ para todo $g \in H_2$. Observemos que todo elemento de $\langle H_2, h \rangle$ pode-se escrever de forma única da forma gh^j com $g \in H_2$ e $0 \leq j < k$ assim

$$\begin{aligned} \eta(gh^j) &= \eta(g) + j\eta(h) \\ &= \frac{j}{k} \end{aligned}$$

Como mostrado na prova do teorema 1.19, este homomorfismo está bem definido, isto é, independe do representante.

Pelo teorema 1.19, η pode-se estender a $\varphi \in G^*$ tal que $\varphi \restriction_{\langle H_2,h \rangle} = \eta$. Mas $\varphi \in T(H_2)$ e $\varphi \notin T(H_1)$ porque $\varphi(h) \neq 0$ logo $T(H_2) \neq T(H_1)$. Assim T é injetivo e portanto T é uma bijeção. □

1.2 Códigos Lineares

Nesta seção trataremos algumas definições e resultados básicos da Teoria de Códigos Corretores de Erros. Em particular, estudaremos códigos minimais vistos como ideais de uma álgebra de grupo FG, onde F é um corpo finito e G é um grupo cíclico finito. O ponto de partida da Teoria de Códigos é um conjunto finito A qualquer, chamado **alfabeto.** Uma sequência finita de n símbolos de A é chamada **palavra** de comprimento n. Um **código de comprimento** n é um subconjunto próprio de A^n, para algum n natural.

Estamos interessados em códigos dotados de certa estrutura algébrica, assim, tomando como alfabeto um corpo de q elementos, o qual denotaremos por F_q, temos

em F_q^n uma estrutura de espaço vetorial de dimensão n sobre F_q. Um **código linear** $\mathtt{C}$ sobre o alfabeto F_q é um subespaço vetorial de F_q^n.

Existem várias formas de descrever um código, uma delas é considerando, por exemplo, uma base $v_1, v_2, \cdots, v_k$ de $\mathtt{C}$. Assim, todo elemento de $\mathtt{C}$ se escreve, de forma única, da seguinte maneira:

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k,$$

onde os $\lambda_i \in F_q$ e $i = 1, \cdots, k$.

Observemos que a aplicação

$$\begin{array}{rcl} T : {F_q}^k & \rightarrow & {F_q}^n \\ \lambda = (\lambda_1, \lambda_2, \cdots, \lambda_k) & \mapsto & (\lambda_1, \lambda_2, \cdots, \lambda_k)M \end{array}$$

onde

$$M = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & & & \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}$$

é uma transformação linear injetiva tal que $Im(T) = \mathtt{C}$. Se $x = (\lambda_1, \lambda_2, \cdots, \lambda_k)$, então $T(x) = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$. A matriz M descreve a aplicação linear T e é chamada **matriz geradora do código.** Observemos que $\mathtt{C}$ consiste de q^k combinações lineares λM. Na teoria de códigos $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_k) \in {F_q}^k$ é chamada **sequência de informação ou mensagem,** $\mathtt{C}$ **código de canal** e T **um codificador.**

Como a base para um código linear $\mathtt{C}$ não é única, temos que a matriz geradora também não é única. Porém, dadas duas matrizes que gerem $\mathtt{C}$, uma pode ser obtida a partir da outra através das seguintes operações elementares de linhas:

- permutação de duas linhas;
- multiplicação de uma linha por um escalar não nulo;
- adição de um múltiplo escalar de uma linha a outra;

assim podemos escolher uma base para $\mathtt{C}$ tal que a matriz geradora seja da forma $M = (I_k|A)$, onde I_k é a matriz identidade $k \times k$ e A é uma matriz $k \times (n-k)$. Neste caso dizemos que M está na forma padrão.

Se M está na forma padrão, então dada uma palavra $c \in \mathtt{C}$, os primeiros k símbolos são os **símbolos de informação** e os restantes são os **símbolos de verificação.**

Esta forma de representar o código tem a vantagem de gerar todos os elementos de $\mathtt{C}$, mas em contrapartida, é "difícil" decidir se um dado elemento $x \in {F_q}^n$ pertence ou não a $\mathtt{C}$, pois para verificar isso é necessário resolver um sistema linear de n equações e k incógnitas, o que gera um custo computacional muito elevado.

Se $\mathtt{C} \subset {F_q}^n$ é um código linear então $\mathtt{C}^{\perp} = \{v \in {F_q}^n; \langle v, u\rangle = 0, \forall\ u \in \mathtt{C}\}$ também é um código linear, este código é chamado o **código dual a** $\mathtt{C}$.

Proposição 1.25 *([6], Capítulo 5, Proposição 4) Seja $\mathtt{C}$ um código linear sobre F_q e suponhamos que H seja uma matriz geradora de $\mathtt{C}^{\perp}$. Temos então que:*

$$v \in \mathtt{C} \Leftrightarrow Hv^t = 0.$$

A matriz geradora H de $\mathtt{C}^{\perp}$ é a **matriz teste de paridade de** $\mathtt{C}$.

Se $T : {F_q}^k \to {F_q}^n$ é um "codificador" para o código $\mathtt{C}$ com matriz geradora $M = [I_k|A]$, então $dim\ \mathtt{C}^{\perp} = n - k$ e a aplicação linear

$$h : {F_q}^n \to {F_q}^{n-k}$$

definida pela matriz $H_{(n-k)\times n}$

$$H = \left[-A^t|I_{n-k}\right]$$

satifaz as seguintes propriedades:

i) $Ker(h) = Im(T)$;

ii) $c \in \mathtt{C}$ se e somente se $Hc^t = 0$.

A matriz H associada à transformação linear h é chamada **matriz teste de paridade do código** $\mathtt{C}$.

Exemplo 1.26 *Consideremos F_2 um corpo com 2 elementos e seja T a transformação linear injetiva*

$$\begin{aligned} T : {F_2}^3 &\rightarrow {F_2}^4 \\ (\lambda_1, \lambda_2, \lambda_3) &\mapsto (\lambda_1, \lambda_2, \lambda_3, \lambda_2 + \lambda_3) \end{aligned}$$

Sejam $\{e_1, e_2, e_3\}$ e $\{f_1, f_2, f_3, f_4\}$, respectivamente, as bases canônicas de ${F_2}^3$ e ${F_2}^4$.

Vamos encontrar a matriz M a qual representa a transformação linear T. Assim,

$$T(e_1) = T(100) = 1f_1 + 0f_2 + 0f_3 + 0f_4$$

$$T(e_2) = T(010) = 0f_1 + 1f_2 + 0f_3 + 1f_4$$

$$T(e_3) = T(001) = 0f_1 + 0f_2 + 1f_3 + 1f_4.$$

Logo,

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

onde M está na forma padrão, $M = [I_3|A]$, sendo I_3 a matriz identidade 3×3 e A uma matriz 3×1.

Considere a aplicação linear $h : {F_2}^4 \rightarrow F_2$ definida pela matriz $H_{1\times 4}$, em que

$$H = [-A^t|I_1] = \begin{pmatrix} 0 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix}.$$

Dados $\alpha = (1, 0, 1, 1)$ e $\beta = (0, 1, 1, 1) \in {F_2}^4$, vamos verificar se estes vetores pertencem a $\mathcal{C}$. Para isto, basta verificar se $H \cdot \alpha^t = 0$ e se $H \cdot \beta^t = 0$.

$$H \cdot \alpha^t = \begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = (0)$$

e

$$H \cdot \beta^t = \begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = (1).$$

Logo $\alpha \in \mathcal{C}$ *e* $\beta \notin \mathcal{C}$.

Sabemos que $\alpha = (1,0,1,1) \in \mathcal{C}$ *e que* $M = [I_3|A]$. *Então as três primeiras coordenadas de* α *são os dígitos de informação, isto é, se recebemos a palavra* $\alpha = (1,0,1,1)$, *a mensagem enviada foi* $(1,0,1)$.

Uma das características principais dos códigos corretores de erros é transmitir ou armazenar dados de forma confiável. O procedimento é o seguinte: o remetente tem a mensagem inicial e deseja codificá-la para enviá-la ao destinatário, assim que o destinário a recebe, ele quer decodificar a mensagem, caso a mensagem chegue com erros, o destinatário tenta detectar e corrigir os erros, recuperando assim, a informação original. Para determinar se a mensagem chegou com erro é preciso ter em mãos um parâmetro que compare a palavra enviada com a recebida, é necessário então introduzir o conceito de distância entre palavras de um código.

Dados dois elementos $x = (x_1, x_2, \cdots, x_n)$ e $y = (y_1, y_2, \cdots, y_n) \in {F_q}^n$, definimos a **distância de Hamming** de x a y como

$$d(x,y) = |\{i : x_i \neq y_i, 1 \leq i \leq n\}|,$$

sendo que a **distância mínima** de um código $\mathtt{C} \subset {F_q}^n$ é

$$d := d(\mathtt{C}) = min\{d(x,y) : x, y \in \mathtt{C}, x \neq y\}.$$

Notemos que a distância definida acima satisfaz, para todos $u, v, w \in {F_q}^n$, as seguintes propriedades:

i) Positividade: $d(u,v) \geq 0$.

ii) Simetria: $d(u,v) = d(v,u)$.

iii) Desigualdade Triangular: $d(u,v) \leq d(u,w) + d(w,v)$.

Estas propriedades caracterizam também uma métrica, chamada **métrica de Hamming.**

Dizemos que dois códigos $\mathtt{C}$ e $\mathtt{C}'$ são códigos linearmente equivalentes se existe uma isometria linear $L : {F_q}^n \to {F_q}^n$ tal que $L(\mathtt{C}) = \mathtt{C}'$. Dado um código $\mathtt{C}$ sempre existe um código equivalente $\mathtt{C}'$ com matriz geradora na forma padrão. Além disso

$\mathtt{C}$ e $\mathtt{C}'$ são códigos linearmente equivalentes se $\mathtt{C}$ pode ser obtido de $\mathtt{C}'$ (ou $\mathtt{C}'$ de $\mathtt{C}$) por meio de uma sequência de operações, conforme itens abaixo:

- multiplicar por escalar, não nulo, os elementos de uma determinada posição fixa, em todas as palavras;
- permutar as posições de todas as palavras do código, esta permutação deve ser fixa de $\{1, 2, ..., n\}$.

Em códigos equivalentes $\mathtt{C}$ e $\mathtt{C}'$ é permitido fazer as seguintes operações:

- permutação de duas colunas;
- multiplicação de uma coluna por um escalar não nulo,

para que a partir da matriz geradora de $\mathtt{C}$ se obtenha a matriz geradora de $\mathtt{C}'$.

Além do comprimento e da distância mínima, estão associados a um código outros parâmetros tais como peso, dimensão, os quais são necessários na construção de algoritmos para a decodificação e correção de erros.

Considere $x \in {F_q}^n$, definimos o **peso de** x como sendo

$$w(x) = d(x, 0).$$

O **peso de um código linear** $\mathtt{C}$ é o número inteiro

$$w(\mathtt{C}) := min\{w(x); x \in \mathtt{C}, x \neq 0\}.$$

Notemos que

$$\begin{aligned} d(x, y) &= |\{i : x_i \neq y_i, 1 \leq i \leq n\}| \\ &= |\{i : x_i - y_i \neq 0, 1 \leq i \leq n\}| \\ &= d(x - y, 0) \\ &= w(x - y) \end{aligned}$$

isto é, que $d(\mathtt{C}) = w(\mathtt{C})$.

Em um código linear definimos $[n, k, d]$ como os parâmetros deste código $\mathtt{C}$, sendo que n é o **comprimento de** $\mathtt{C}$, k é a **dimensão de** $\mathtt{C}$ **sobre** F_q, e d é a **distância mínima de** $\mathtt{C}$.

Dado um elemento $x \in {F_q}^n$ e um inteiro positivo r, temos que a **bola de centro em x e raio r** é o conjunto

$$B(x,r) = \{u \in {F_q}^n : d(u,x) \leq r\}$$

e a **esfera de centro em x e raio r** é o conjunto:

$$S(x,r) = \{u \in {F_q}^n : d(u,x) = r\}.$$

Na teoria de Códigos, a distância mínima desempenha um papel fundamental, como vemos a seguir.

Teorema 1.27 *Seja $\mathtt{C}$ um código, o qual possui distância mínima d e seja*

$$k = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

então $\mathtt{C}$ pode detectar até $d-1$ erros e corrigir até k erros.

Demonstração:

Se, ao transmitirmos uma palavra, um elemento $x \in \mathtt{C}$ for recebido com t erros, onde $t \leq d-1$, então este número de erros cometidos é justo a distância de Hamming entre x e a palavra recebida y, logo $d(x,y) \leq d-1 < d$. Conclui-se desta forma que $y \notin \mathtt{C}$, o que garante que o erro será detectado.

Agora temos que verificar se é possível corrigir este erro, suponhamos que o número de erros cometidos seja $t < k$. Consideremos a bola $B(y,k)$, assim $d(x,y) = t \leq k$, o que implica que $x \in B(y,k)$. Notemos que x é o único elemento de $\mathtt{C}$ contido nesta bola. De fato, se existisse outro elemento $x' \in \mathtt{C}$ em $B(y,k)$, teríamos que $d(x,x') \leq d(x,y) + d(y,x') \leq 2k < d$, o que é um absurdo, já que d é a distância mínima de $\mathtt{C}$. Portanto, x é o elemento de $\mathtt{C}$ mais próximo de y, o que garante que podemos corrigir o erro. □

Exemplo 1.28 *Seja $\mathcal{L} = F^n$ um espaço vetorial de dimensão n e $\xi = \langle v \rangle$ onde $v = (v_1, \cdots, v_n)$ com $v_j \neq 0$ para todo j. Então todo elemento de ξ é da forma $cv = (cv_1, \cdots, cv_n)$ com $c \in F$. Assim a distância de Hamming entre elementos de ξ é n, pois*

$$c_1 v_j = c_2 v_j \Leftrightarrow c_1 = c_2.$$

Neste exemplo a distância mínima do código gerado por ξ é a máxima possível.

1.3 Códigos Cíclicos

Entre os códigos lineares existe uma classe chamada Códigos Cíclicos que admitem uma representação em termos de polinômios sobre F_q. Este tipo de código linear é muito útil, pois tem bons algoritmos de codificação e decodificação.

Definição 1.29 *Um código linear* $\mathtt{C}$ *de* ${F_q}^n$ *é chamado* ***código cíclico,*** *se* $\mathtt{C}$ *é invariante com respeito a permutações cíclicas de coordenadas, isto é, se para todo* $c = (c_0, \cdots, c_{n-1}) \in \mathtt{C}$ *temos que* $(c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathtt{C}$.

Se consideramos a transformação linear:

$$\begin{array}{rcl} T : \mathtt{C} & \to & {F_q}^n \\ (c_0, \cdots, c_{n-1}) & \mapsto & (c_{n-1}, c_0, \cdots, c_{n-2}) \end{array} \tag{1.2}$$

temos que $\mathtt{C}$ é cíclico se $T(\mathtt{C}) = \mathtt{C}$.

Definimos R_n como sendo o **anel das classes residuais em** $F_q[x]$ **módulo** $x^n - 1$:

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

Um elemento de R_n é da forma:

$$[g(x)] = \{g(x) + f(x)(x^n - 1) : f(x) \in F_q[x]\}.$$

Em R_n, a adição, a multiplicação e a multiplicação por escalar $\lambda \in F_q$ são definidas como:

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$

$$[f(x)][g(x)] = [f(x)g(x)]$$

$$\lambda[f(x)] = [\lambda f(x)].$$

Com a soma e a multiplicação por escalar definidas acima R_n é um F_q-espaço vetorial com base $[1], [x], \cdots, [x^{n-1}]$ isomorfo a ${F_q}^n$, mediante a transformação linear:

$$\begin{array}{rcl} \psi : {F_q}^n & \to & R_n \\ (a_0, a_1, \cdots, a_{n-1}) & \mapsto & [a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}]. \end{array}$$

A vantagem de considerarmos este isomorfismo é que R_n tem, além da estrutura de espaço vetorial, uma estrutura de anel; e a imagem por meio de ψ de um código cíclico de ${F_q}^n$ é um ideal de R_n.

A seguir apresentaremos alguns aspectos dos códigos cíclicos necessários para o desenvolvimento de nosso trabalho.

Lema 1.30 *Seja V um subespaço vetorial de R_n. Então V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $[x]$.*

Demonstração:

Suponhamos que V é um ideal de R_n, então $[x][f(x)] \in V$, para todo $[f(x)] \in V$.

Reciprocamente, sejam $[f(x)] \in V$ e $[g(x)] = [a_0 + a_1x + \cdots + a_{n-1}x^{n-1}] \in R_n$, temos que mostrar que $[g(x)][f(x)] \in V$. Como V é um subespaço de R_n, então V é fechado para adição e multiplicação por escalar. Por hipótese V é fechado pela multiplicação por $[x]$, isto é,

$$[xf(x)] = [x][f(x)] \in V.$$

De forma análoga,

$$[x^2f(x)] = [x][xf(x)] \in V.$$

De forma indutiva, temos,

$$[x^mf(x)] = [x^m][f(x)] \in V, \text{para todo } m \in \mathbb{N}.$$

Assim

$$\begin{aligned}
[g(x)][f(x)] &= [g(x)f(x)] \\
&= [(a_0 + a_1x + \cdots + a_{n-1}x^{n-1})f(x)] \\
&= a_0[f(x)] + a_1[x][f(x)] + \cdots + a_{n-1}[x^{n-1}][f(x)] \in V
\end{aligned}$$

logo V é um ideal de R_n, como queríamos mostrar. □

Teorema 1.31 *Um subespaço $\mathcal{C} \subset {F_q}^n$ é um código cíclico se, e somente se, $\psi(\mathcal{C})$ é um ideal de R_n.*

Demonstração: Consideremos $T : \mathtt{C} \to {F_q}^n$ definida em (1.2), página 24:

Se $\mathtt{C}$ é cíclico então $c' = T(c) \in \mathtt{C}$, para todo $c \in \mathtt{C}$, logo $\psi(c') \in \psi(\mathtt{C})$, para todo $c' \in \mathtt{C}$. Notemos que se $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathtt{C}$,

$$\begin{aligned} \psi(\mathtt{C}) \ni \psi\left(T(c)\right) &= \psi(c_{n-1}, c_0, \cdots, c_{n-2}) \\ &= [c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-1}] \\ &= [x][c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}] \\ &= [x]\psi(c). \end{aligned}$$

Logo $\psi(\mathtt{C})$ é fechado pela multiplicação de $[x]$ e, pelo lema 1.30, $\psi(\mathtt{C})$ é um ideal de R_n.

Para mostrar a volta, suponha que $\psi(\mathtt{C})$ seja um ideal de R_n e considere $c = (c_0, \cdots, c_{n-1}) \in \mathtt{C}$. Temos então que $\psi(c) \in \psi(\mathtt{C})$ e $[x]\psi(c) \in \psi(\mathtt{C})$, assim

$$\begin{aligned} \psi^{-1}\left([x]\psi(c)\right) &= \psi^{-1}([x][c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}]) \\ &= \psi^{-1}(c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-1}) \\ &= (c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathtt{C}. \end{aligned}$$

Portanto $T(c) = (c_{n-1}, c_0, \cdots, c_{n-2}) \in T(\mathtt{C})$, o que implica $\mathtt{C}$ é um código cíclico.

□

Acabamos de ver que se $\mathtt{C}$ é um código cíclico, então $\psi(\mathtt{C})$ é um ideal de R_n, mas os ideais de R_n são principais, logo são da forma $\langle [F(x)] \rangle$ onde $F(x)$ é um divisor de $x^n - 1$, que podemos supor mônico.

Consideremos F_q um corpo de característica p, e sejam m e p primos entre si com $n = mp^s$, então

$$x^n - 1 = (x^m - 1)^{p^s}.$$

A derivada de $(x^m - 1)$ é $mx^{m-1} \neq 0$. O $mdc\left(x^m - 1, mx^{m-1}\right) = 1$, isto é, o polinômio $x^m - 1$ não tem fator não constante em comum com sua derivada. Desta forma, temos que

$$x^m - 1 = f_1 \cdots f_l,$$

onde os f_i são polinômios mônicos irredutíveis em F_q, distintos dois a dois. Assim

$$x^n - 1 = f_1^{p^s} \cdots f_l^{p^s}.$$

Desta forma o polinômio $x^n - 1$ tem $(p^s + 1)^l$ divisores mônicos. Logo R_n possui $(p^s + 1)^l$ ideais. Notemos que se p e n são primos entre si então R_n tem 2^l ideais.

Observemos que, dado um ideal I de R_n, existe um único polinômio mônico $g(x) \in F_q[x]$, divisor de $x^n - 1$, tal que $[g(x)]$ gera I. O polinômio $g(x)$ é chamado **polinômio gerador de** $\mathtt{C}$ e

$$h(x) = \frac{x^n - 1}{g(x)}$$

é chamado **polinômio teste de** $\mathtt{C}$. Assim $\psi^{-1}[c(x)] \in \mathtt{C}$ se, e somente se, $h(x)c(x) \equiv 0 \pmod{x^n - 1}$.

Teorema 1.32 *Seja $I = \langle [g(x)] \rangle$, onde $g(x)$ é um divisor de $x^n - 1$ de grau s. Temos que $[g(x)], [xg(x)], \cdots, [x^{n-s-1}g(x)]$ é uma base de I como espaço vetorial sobre F_q.*

Demonstração:

Afirmação 1: $[g(x)], [xg(x)], \cdots, [x^{n-s-1}g(x)]$ são linearmente independentes. De fato, suponhamos que existem $a_0, a_1, \cdots, a_{n-s-1} \in F_q$ tais que

$$a_0[g(x)] + a_1[xg(x)] + \cdots + a_{n-s-1}[x^{n-s-1}g(x)] = [0].$$

Disso segue que

$$[g(x)][a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1}] = [0].$$

Assim para algum $d(x) \in F_q[x]$, temos

$$g(x)\left(a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1}\right) = d(x) \cdot (x^n - 1),$$

isto é,

$$a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} = d(x) \cdot h(x).$$

O grau de $h(x)$ é $n - s$, então $a_0 + a_1x + \cdots + a_{n-s-1}x^{n-s-1} \equiv 0$, logo

$$a_0 = a_1 = \cdots = a_{n-s-1} = 0.$$

Afirmação 2: $[g(x)], [xg(x)], \cdots, [x^{n-s-1}g(x)]$ geram I sobre F_q. De fato, se $[f(x)] \in I$, então

$$f(x) = d(x)g(x) + t(x)(x^n - 1)$$

para algum $t(x) \in F_q[x]$. Pelo algoritmo da divisão existem polinômios $q(x)$ e $r(x)$ tais que

$$d(x) = h(x) \cdot q(x) + r(x)$$

onde $r(x) = 0$ ou $\partial r(x) < n - s$.

Logo,

$$\begin{aligned} f(x) &= [h(x) \cdot q(x) + r(x)]\, g(x) + t(x)(x^n - 1) \\ &= (x^n - 1)q(x) + r(x)g(x) + t(x)(x^n - 1) \\ &= (x^n - 1)[q(x) + t(x)] + r(x)g(x), \end{aligned}$$

ou seja, $[f(x)] = [r(x)][g(x)]$. Agora escrevendo $r(x) = b_0 + b_1 x + \cdots + b_{n-s-1}x^{n-s-1}$, temos

$$[f(x)] = b_0[g(x)] + b_1[xg(x)] + \cdots + b_{n-s-1}[x^{n-s-1}g(x)],$$

como queríamos demonstrar. □

Observação 1.33 *([6], Capítulo 6, Corolário 1) Dado um código cíclico $\mathtt{C}$, existe $v \in \mathtt{C}$ tal que $\mathtt{C} = \langle v \rangle$.*

Se $I = \langle [g(x)] \rangle$ com $g(x) = g_0 + g_1 x + \cdots g_s x^s$ vimos que $[g(x)], [xg(x)], \cdots, [x^{n-s-1}g(x)]$ é uma base de I como espaço vetorial sobre F_q, assim a dimensão de I sobre F_q é $n - s$, além disso, $\mathtt{C} = \psi^{-1}(I)$ tem como matriz geradora a matriz:

$$M = \begin{pmatrix} \psi^{-1}[g(x)] \\ \psi^{-1}[xg(x)] \\ \vdots \\ \psi^{-1}[x^{n-s-1}g(x)] \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_s & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_s \end{pmatrix}$$

Por outro lado, como $v \in \mathtt{C}$ se e somente se $Hv^t = 0$, então pode-se mostrar que

$$H = \begin{pmatrix} 0 & \cdots & 0 & h_{n-s} & \cdots & h_1 & h_0 \\ 0 & \cdots & h_{n-s} & h_{n-s-1} & \cdots & h_0 & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ h_{n-s} & \cdots & h_0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

é uma matriz teste de paridade de $\mathtt{C}$, onde

$$h(x) = \frac{x^n - 1}{g(x)} = \sum_{i=0}^{n-s} h_i x^i.$$

Como já foi dito anteriormente, o fato dos códigos cíclicos admitirem uma representação em termos de polinômios sobre F_q permite descrever algoritmos de codificação e decodificação de forma simples e eficiente, mas a tarefa de determinar a distância mínima desses códigos é um problema difícil de resolver, neste caso o procedimento a seguir é construir famílias de códigos (em particular códigos BCH) cujas distâncias mínimas tenham cotas inferiores predeterminadas.

Os códigos BCH podem ser obtidos a partir da construção de um código cíclico com um conjunto conveniente de raízes n-ésimas da unidade, obtendo desta maneira uma cota inferior para a sua distância mínima. Definimos uma **raiz n-ésima da unidade** α num corpo F_q como sendo a raiz em F_q do polinômio $x^n - 1$. Esta raiz é dita primitiva se não existe $0 < m < n$ tal que $\alpha^m = 1$.

Seja $\bar{F}_q$ o fecho algébrico de F_q e considere $\alpha \in \bar{F}_q$ uma raiz n-ésima primitiva da unidade e seja $g^{(i)}(x)$ o polinômio minimal de α^i sobre F_q, isto é, o polinômio mônico não nulo de menor grau com coeficientes em F_q que tem α^i como raiz. O **código BCH (Bose-Chaudhuri-Hocquenghem)** de "distância designada" δ é o código cíclico $\mathtt{C}$ de comprimento n sobre F_q com polinômio gerador

$$g(x) = mmc\left(g^{(1)}, g^{(2)}, \cdots, g^{(\delta-1)}\right).$$

Se $n = q^m - 1$, isto é, se α é um elemento primitivo de F_{q^m}, então o código BCH é chamado primitivo. Definimos **elemento primitivo** de um corpo F_q como um gerador do grupo multiplicativo deste corpo. A distância mínima de um código BCH com distância designada δ é pelo menos δ. (Ver em [7] página 91).

Os **códigos RS (Reed-Solomon)** são códigos BCH primitivos de comprimento $n = q-1$ sobre F_q. O polinômio gerador de tal código tem a forma $g(x) = \prod_{i=1}^{\delta-1}(x-\alpha^i)$, onde α é primitivo em F_q. Os códigos RS são um dos mais simples exemplos de códigos BCH.

Capítulo 2

Códigos Abelianos Minimais

Como vimos no capítulo 1, existe um isomorfismo entre ${F_q}^n$ e $F_qC_n \simeq \frac{F_q[x]}{\langle x^n-1\rangle}$ onde F_q é um corpo finito com q elementos e C_n um grupo cíclico de ordem n, que estabelece uma correspondência entre os códigos cíclicos de ${F_q}^n$ com os ideais de F_qC_n. Esta correspondência é fundamental pois os ideais nas álgebras de grupos são "gerados" por elementos idempotentes primitivos que podem ser calculados de várias formas, e a partir deles podem ser listados os códigos minimais. Neste capítulo mostraremos os resultados de Arora e Pruthi [1] e de Ferraz e Milies [3], que apresentam expressões para os idempotentes geradores de códigos cíclicos abelianos minimais, quando G é um grupo cíclico de ordem p^n e F_q um corpo com q elementos tal que q tem ordem $\phi(p^n)$ módulo p^n.

Um código abeliano sobre um corpo F_q é um ideal da álgebra de grupo F_qG de um grupo abeliano finito G. Um código minimal é um ideal minimal I no conjunto de todos os ideais de F_qG. Lembrando que a distância de Hamming entre dois elementos de F_qG, $\alpha = \sum_{g\in G} \alpha_g g$ e $\beta = \sum_{g\in G} \beta_g g$, é o número de elementos de G no qual os respectivos coeficientes em α e β diferem, isto é,

$$d(\alpha,\beta) = |\{g : \alpha_g \neq \beta_g, g \in G\}|.$$

O peso ou distância mínima do ideal I é dado por:

$$w(I) = min\{d(\alpha,\beta) : \alpha \neq \beta, \quad \alpha,\beta \in F_qG\}.$$

2.1 Componentes Simples de F_qG e classes q-ciclotômicas de G

Esta seção é baseada no artigo de Ferraz e Milies [9].

Sejam F_q um corpo com q elementos e G um grupo abeliano finito, tal que $mdc(q, |G|) = 1$. Pelo Teorema de Maschke, F_qG é semissimples, e se $\{e_1, \cdots, e_k\}$ é uma família completa de idempotentes ortogonais primitivos de F_qG, então:

$$F_qG = \bigoplus_{i=1}^{k} (F_qG)e_i \simeq \bigoplus_{i=1}^{k} F_{q_i},$$

onde $F_{q_i} \simeq (F_qG)e_i$, $1 \leq i \leq k$ são corpos, os quais são extensões finitas de F_q. Definamos

$$\mathcal{G} := \bigoplus_{i=1}^{k} F_q e_i. \tag{2.1}$$

Observemos que $F_q e_i \simeq F_q$ como corpos e assim a dimensão de $\mathcal{G}$ como espaço vetorial sobre F_q é k. Além disso, $\mathcal{G}$ é uma F_q-álgebra com o produto herdado de F_qG.

Lema 2.1 *Se a é um elemento de F_qG, então $a \in \mathcal{G}$ se, e somente se, $a^q = a$.*

Demonstração:

Seja $a = a_1e_1 + \cdots + a_ke_k \in \mathcal{G}$ com $a_j \in F_q, j = 1, \cdots, k$. Queremos mostrar que $a^q = a$. Temos

$$a^q = (a_1e_1 + a_2e_2 + \cdots + a_ke_k)^q = {a_1}^q {e_1}^q + {a_2}^q {e_2}^q + \cdots + {a_k}^q {e_k}^q,$$

já que $\{e_1, \cdots, e_k\}$ é uma família completa de idempotentes ortogonais primitivos. Além disso,

$${a_1}^q {e_1}^q + {a_2}^q {e_2}^q + \cdots + {a_k}^q {e_k}^q = a_1 {e_1}^q + a_2 {e_2}^q + \cdots + a_k {e_k}^q,$$

pois $a_j \in F_q$, para todo $1 \leq j \leq k$, e

$$a_1 {e_1}^q + a_2 {e_2}^q + \cdots + a_k {e_k}^q = a_1e_1 + a_2e_2 + \cdots + a_ke_k = a,$$

pois ${e_j}^i = e_j$, para $i = 2, 3, \cdots, q$. O que mostra uma das implicações.

Para mostrar a volta, suponhamos que $a \in F_qG$ é tal que $a^q = a$. Queremos mostrar que $a \in \mathcal{G}$. Do fato que $e_1 + e_2 + \cdots + e_k = 1$ podemos escrever:

$$a = a_1 + a_2 + \cdots + a_k,$$

com $a_j \in (F_qG)e_j$, assim

$$a^2 = (a_1 + \cdots + a_k)^2 = {a_1}^2 + \cdots + {a_k}^2,$$

já que $a_i a_j = 0$ para todo $i \neq j$. De igual forma se tem indutivamente que

$$a^l = {a_1}^l + \cdots + {a_k}^l,$$

para todo $l \in \mathbb{N}$, em particular

$$a^q = {a_1}^q + \cdots + {a_k}^q.$$

Como $a^q = a$, então multiplicando à direita por e_j obtemos

$${a_j}^q = a_j.$$

Como $a_j \in F_{q_j}$ é deixado fixo pela aplicação $x \mapsto x^q$, então a_j pertence ao corpo base $F_q e_j \simeq F_q$. Portanto $a \in \mathcal{G}$. □

Seja g um elemento do grupo abeliano finito G. A **classe q-ciclotômica de g** é definida como o conjunto

$$S_g := \{g^{q^j} : 0 \leq j \leq t_g - 1\},$$

onde t_g é o menor inteiro positivo tal que

$$q^{t_g} \equiv 1 \pmod{o(g)}.$$

Note que como $mdc(q, o(g)) = 1$, então $q^{\phi(o(g))} \equiv 1 \pmod{o(g)}$, portanto existe m tal que $q^m \equiv 1 \pmod{o(g)}$, logo existe um menor inteiro positivo t_g. Se $S_g \neq S_h$, então $S_g \cap S_h = \varnothing$, pois no caso que $f \in S_g \cap S_h$ temos:

- $S_f \subset S_g \cap S_h$,

- $f = g^{q^i}$,
- $f = h^{q^j}$,

para alguns i, j. Assim $f^{q^{t_g - i}} = g^{q^{t_g}} = g$ e $f^{q^{t_h - j}} = h^{q^{t_h}} = h$. Segue que $g \in S_f$ e $h \in S_f$, logo $S_g = S_f = S_h$. Se $T = \{g_1, g_2, \cdots, g_l\}$ é um conjunto de representantes destas classes, temos que G é a união das classes q-ciclotômicas $S_{g_1}, S_{g_2}, \cdots, S_{g_l}$, isto é,

$$G = \{g_1, {g_1}^q, \cdots, {g_1}^{q^{t_1 - 1}}\} \cup \{g_2, {g_2}^q, \cdots, {g_2}^{q^{t_2 - 1}}\} \cup \cdots \cup \{g_l, {g_l}^q, \cdots, {g_l}^{q^{t_l - 1}}\}.$$

Teorema 2.2 *Sejam F_q um corpo finito com q elementos e G um grupo abeliano finito tal que $mdc(q, |G|) = 1$. Então, o número de componentes simples de F_qG é igual ao número de classes q-ciclotômicas de G.*

Demonstração:

Como vimos na expressão (2.1), página 31, o número de componentes simples de F_qG é igual a dimensão de $\mathcal{G}$ sobre F_q, isto é, k. Assim basta exibir uma base desta subálgebra com l elementos, onde l é o número de classes q-ciclotômicas. Dada uma classe q-ciclotômica S_{g_j} definimos $\eta_j = \sum_{g \in S_{g_j}} g \in F_qG$.

Afirmação: $\mathcal{B} = \{\eta_1, \cdots, \eta_l\}$ é uma base para $\mathcal{G}$. A prova da afirmação será dividida em três passos:

- $\eta_j \in \mathcal{G}$.

Seja $\eta_j = g_j + {g_j}^q + {g_j}^{q^2} + \cdots + {g_j}^{q^{t_j - 1}}$, onde ${g_j}^{q^{t_j}} = g_j$. Observemos que

$$\begin{aligned} {\eta_j}^q &= ({g_j} + {g_j}^q + {g_j}^{q^2} + \cdots + {g_j}^{q^{t_j - 2}} + {g_j}^{q^{t_j - 1}})^q \\ &= {g_j}^q + {g_j}^{q^2} + {g_j}^{q^3} + \cdots + {g_j}^{q^{t_j - 1}} + {g_j}^{q^{t_j}} \\ &= {g_j}^q + {g_j}^{q^2} + {g_j}^{q^3} \cdots + g_j^{q^{t_j - 1}} + g_j = \eta_j. \end{aligned}$$

Assim, pelo lema 2.1, temos que $\eta_j \in \mathcal{G}$.

- $\mathcal{B}$ é F_q-linearmente independente.

Suponhamos que existem $a_1, a_2, \cdots, a_l \in F_q$ tais que

$$a_1\eta_1 + a_2\eta_2 + \cdots + a_l\eta_l = 0.$$

Como $\eta_j = \sum_{g \in S_{g_j}} g \in F_qG$, a equação anterior pode ser reescrita

$$a_1(g_1+{g_1}^q+\cdots+{g_1}^{q^{t_1-1}})+a_2(g_2+{g_2}^q+\cdots+{g_2}^{q^{t_2-1}})+\cdots+a_l(g_l+{g_l}^q+\cdots+{g_l}^{q^{t_l-1}}) = 0$$

$$a_1g_1+a_1{g_1}^q+\cdots+a_1{g_1}^{q^{t_1-1}}+a_2g_2+a_2{g_2}^q+\cdots+a_2{g_2}^{q^{t_2-1}}+\cdots+a_lg_l+\cdots+a_l{g_l}^{q^{t_l-1}} = 0.$$

Mas $\mathcal{L} = \{g_1, {g_1}^q, \cdots, {g_1}^{q^{t_1-1}}, g_2, {g_2}^q, \cdots, {g_2}^{q^{t_2-1}}, \cdots, g_l, {g_l}^q, \cdots, {g_l}^{q^{t_l-1}}\}$ é uma base para F_qG, então é linearmente independente sobre F_q. Em particular, $a_1 = a_2 = a_3 = \cdots = a_l = 0$.

- $\{\eta_j\}$ geram $\mathcal{G}$.

Notemos que ${\eta_j}^q = \eta_j$, para $1 \leq j \leq l$, então $\mathcal{B} \subset \mathcal{G}$. Seja $a \in \mathcal{G} = \bigoplus_{i=1}^{k} F_qe_i$. Como $\mathcal{L}$ é base de F_qG,

$a = a_{11}g_1 + a_{12}{g_1}^q + a_{13}{g_1}^{q^2} + \cdots + a_{1t_1}{g_1}^{q^{t_1-1}} + a_{21}g_2 + a_{22}{g_2}^q + \cdots + a_{2t_2}{g_2}^{q^{t_2-1}} + \cdots + a_{l1}g_l + a_{l2}{g_l}^q + \cdots + a_{lt_l}{g_l}^{q^{t_l-1}}$,

onde $a_{ij} \in F_q$, e

$a^q = a_{11}{g_1}^q + a_{12}{g_1}^{q^2} + a_{13}{g_1}^{q^3} + \cdots + a_{1t_1}g_1 + a_{21}{g_2}^q + a_{22}{g_2}^{q2} + \cdots + a_{2t_2}g_2 + \cdots + a_{l1}{g_l}^q + a_{l2}{g_l}^{q2} + \cdots + a_{lt_l}g_l$.

Pelo lema 2.1, $a^q = a$, e igualando coeficiente a coeficiente, obtemos que:

$$a_{11} = a_{12} = a_{13} = \cdots = a_{1t_1} =: a_1$$

$$a_{21} = a_{22} = a_{23} = \cdots = a_{2t_2} =: a_2$$

$$\vdots$$

$$a_{l1} = a_{l2} = a_{l3} = \cdots = a_{lt_l} =: a_l.$$

Logo,

$a = a_1(g_1 + {g_1}^q + {g_1}^{q2} + \cdots + {g_1}^{q^{t_1-1}}) + a_2(g_2 + {g_2}^q + {g_2}^{q2} + \cdots + {g_2}^{q^{t_2-1}}) + \cdots + a_l(g_l + {g_l}^q + {g_l}^{q2} + \cdots + {g_l}^{q^{t_l-1}}) = a_1\eta_1 + a_2\eta_2 + \cdots + a_l\eta_l$.

Portanto os $\{\eta_j\}$ geram $\mathcal{G}$.

Concluímos então que $l = k$.

□

Notemos que todo elemento pertencente a S_g gera o mesmo subgrupo cíclico que g. Então cada q-classe ciclotômica S_g é um subconjunto do conjunto A_g de todos os geradores do grupo cíclico gerado por g. Assim, o número de subgrupos cíclicos de G é uma cota inferior para o número de componentes simples de F_qG e, esta cota é atingida se, e somente se, $S_g = A_g$, para todo $g \in G$.

Para inteiros positivos r e m, denotaremos por $\bar{r} \in \mathbb{Z}_m$ a classe dos inteiros congruentes com r módulo m. Definimos:

$$A_g := \{g^r : mdc(r, o(g)) = 1\} = \{g^r : \bar{r} \in \mathcal{U}(\mathbb{Z}_{o(g)})\}.$$

Teorema 2.3 *Sejam F_q um corpo finito com q elementos e G um grupo abeliano finito de expoente e, tais que $mdc(q, |G|) = 1$. Então $S_g = A_g$ para todo $g \in G$ se, e somente se, $\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico gerado por $\bar{q} \in \mathbb{Z}_e$.*

Demonstração:

Suponhamos que $\mathcal{U}(\mathbb{Z}_e)$ é um grupo cíclico gerado por $\bar{q}$. Para um elemento $g \in G$, temos que $o(g)$ divide e, logo $\bar{q} \in \mathbb{Z}_{o(g)}$ é um gerador de $\mathcal{U}(\mathbb{Z}_{o(g)})$. Para todo elemento $h \in A_g$, temos que $h = g^r$, com r um inteiro positivo, tal que $\bar{r} \in \mathcal{U}(\mathbb{Z}_{o(g)})$, então $\bar{r} = \bar{q}^j$, para algum inteiro j e $h = g^{q^j} \in S_g$. E temos assim que $S_g = A_g$.

Agora suponhamos que $A_g = S_g$ para todo $g \in G$. Como G é um grupo abeliano finito de expoente e, então existe um elemento $g_0 \in G$ de ordem e, de fato, se $e = {p_1}^{\alpha_1} \cdots {p_m}^{\alpha_m}$, então para cada $1 \leq j \leq m$, existe g_j com $o(g_j) = {p_j}^{\alpha_j}$, desta forma basta pegar $g_0 = g_1 g_2 \cdots g_m$, $o(g_0) = e$. Em particular, $A_{g_0} = S_{g_0}$. Assim, para cada inteiro r, tal que $\bar{r} \in \mathcal{U}(\mathbb{Z}_e)$, temos que ${g_0}^r \in S_{g_0}$, logo existe um inteiro j tal que $\bar{r} = \bar{q}^j$. Portanto $\bar{q}$ gera $\mathcal{U}(\mathbb{Z}_e)$. □

Exemplo 2.4 *Sejam F_q um corpo, onde $|F_q| = q = 2$ e $G = \mathbb{Z}_3 \times \mathbb{Z}_9$ o grupo abeliano finito aditivo, de expoente 9. Temos que:*

i) $mdc(q, |G|) = mdc(2, 27) = 1$;

ii) $\mathcal{U}(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$;

iii) $\bar{q} = 2 \in \mathbb{Z}_9$ *e* 2 *gera* $\mathcal{U}(\mathbb{Z}_9)$, *pois a ordem de* 2 *módulo* 9 *é* 6 : *de fato,* $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16 \equiv 7 \pmod 9, 2^5 = 32 \equiv 5 \pmod 9, 2^6 = 64 \equiv 1 \pmod 9$.

Seja $g = (2, 8) \in G$, *então*

$$S_g = \{g, g^2, g^{2^2}, g^{2^3}, g^{2^4}, g^{2^5}\} = \{(2, 8), (1, 7), (2, 5), (1, 4), (2, 2), (1, 1)\}$$

e

$$A_g = \{(1, 7), (2, 5), (1, 4), (2, 2), (1, 1), (2, 8)\}.$$

Portanto, $S_g = A_g$.

Exemplo 2.5 *O seguinte exemplo mostra que, como* $\mathcal{U}(\mathbb{Z}_{25})$ *não é gerado por* $\bar{7} \in \mathbb{Z}_{25}$ *então* $S_g \neq A_g$ *em* F_qG, *para alguns elementos* $g \in G$, *sendo* F_q *um corpo finito, com* $|F_q| = q = 7$ *e* $G = \mathbb{Z}_5 \times \mathbb{Z}_{25}$ *um grupo abeliano finito aditivo de expoente* 25. *Observemos que:*

i) $mdc(q, |G|) = mdc(7, 125) = 1$;

ii) $\bar{q} = 7 \in \mathbb{Z}_{25}$, *mas* 7 *não gera* $\mathcal{U}(\mathbb{Z}_{25})$, *pois a ordem de* 7 *módulo* 25 *é* 4 : *de fato,* $7^1 = 7, 7^2 = 49 \equiv 24 \pmod{25}, 7^3 = 343 \equiv 18 \pmod{25}, 7^4 = 2401 \equiv 1 \pmod{25}$.

Seja $g = (2, 6) \in G$, *então*

$$S_g = \{g, g^7, g^{7^2}, g^{7^3}\} = \{(2, 6), (4, 12), (1, 18), (3, 24)\}$$

e

$$A_g = \left\{ \begin{array}{c} (2, 6), (4, 12), (1, 18), (3, 24), (2, 11), (4, 17), (1, 23), (3, 4), (2, 16), (4, 22), \\ (1, 3), (3, 9), (2, 21), (4, 2), (1, 8), (3, 14), (2, 1), (4, 7), (1, 13), (3, 19) \end{array} \right\}.$$

Portanto $S_g \subsetneq A_g$.

Teorema 2.6 *([8], Capítulo 1, Teorema 1.7.1)* $\mathcal{U}(\mathbb{Z}_e)$ *é cíclico se, e somente se,* $e = 2, 4, p^n$ *ou* $2p^n$, *onde* p *é um primo ímpar e* n *é um inteiro positivo.*

Corolário 2.7 *Sejam* F_q *um corpo finito com* $|F_q| = q$ *e* G *um grupo abeliano finito de expoente* e. *Então* $S_g = A_g$ *para todo* $g \in G$ *se, e somente se, alguma das afirmações valem:*

i) $e = 2$ *e* q *é ímpar;*

ii) $e = 4$ *e* $q \equiv 3 \pmod 4$;

iii) $e = p^n$, $o(q) = \phi(p^n)$ *em* $\mathcal{U}(\mathbb{Z}_{p^n})$ *e* p *é primo ímpar;*

iv) $e = 2p^n$, $o(q) = \phi(p^n)$ *em* $\mathcal{U}(\mathbb{Z}_{2p^n})$ *e* p *é primo ímpar.*

2.2 Idempotentes primitivos em F_qC_n com $q = n\Gamma + 1$

Esta seção é baseada no artigo de Arora e Pruthi [1].

Sejam $G = \langle g \rangle = C_n$ um grupo cíclico finito de ordem n e F_q um corpo com q elementos tal que $q = n\Gamma + 1$ para algum inteiro $\Gamma > 0$. Com esta escolha de q e n, o corpo F_q possui raízes n-ésima primitivas da unidade. De fato, F_q^* é grupo multiplicativo cíclico com $q-1$ elementos, isto é, $|F_q^*| = n\Gamma$, assim $F_q^* = \langle \theta \rangle$, onde $o(\theta) = n\Gamma$. Definindo $\alpha = \theta^\Gamma$, temos que $o(\alpha) = n$, isto é, $\alpha^n = 1$. O seguinte resultado mostra que F_qC_n tem n idempotentes.

Teorema 2.8 *Se* $q = n\Gamma + 1$, *então* F_qC_n *tem* n *idempotentes primitivos dados por*

$$e_i = \frac{1}{n} \sum_{j=0}^{n-1} \alpha^{ij} g^j, \quad 0 \leq i \leq n-1,$$

onde α *é uma raiz* n*-ésima primitiva da unidade em* F_q.

Demonstração:

Observemos que para todo $h \in C_n$ se tem que $h^q = h^{n\Gamma+1} = h$. Logo todas as classes q-ciclotômicas tem um elemento. Assim temos n classes q-ciclotômicas distintas, o que implica F_qC_n tem n idempotentes primitivos.

Afirmamos que $e_i = \frac{1}{n} \sum\limits_{j=0}^{n-1} \alpha^{ij} g^j$, para $0 \leq i \leq n-1$, são n idempotentes primitivos em F_qC_n. Claramente temos que $e_0 = \frac{1}{n} \sum\limits_{j=0}^{n-1} g^j$ é um idempotente. Consideremos e_0, e_i, $1 \leq i \leq n-1$:

$$\begin{aligned} e_0 \cdot e_i &= \left(\tfrac{1}{n} \sum_{k=0}^{n-1} g^k \right) \left(\tfrac{1}{n} \sum_{l=0}^{n-1} \alpha^{il} g^l \right) \\ &= \tfrac{1}{n^2} \left(\sum_{k=0}^{n-1} g^k \right) \left(\sum_{l=0}^{n-1} \alpha^{il} g^l \right) \\ &= \tfrac{1}{n^2} \sum_{s=0}^{n-1} \left(\sum_{l=0}^{n-1} \alpha^{il} \right) g^s. \end{aligned}$$

Como $\sum_{l=0}^{n-1} \alpha^{il} = \frac{\alpha^{ni}-1}{\alpha^i-1} = 0$, pois α é uma raiz n-ésima primitiva da unidade, concluímos

$$e_0 \cdot e_i = 0.$$

Agora consideremos e_i, e_j para $1 \leq i \leq j \leq n-1$.

$$\begin{aligned} e_i \cdot e_j &= \tfrac{1}{n^2} \left(\sum_{k=0}^{n-1} \alpha^{ik} g^k \right) \left(\sum_{l=0}^{n-1} \alpha^{jl} g^l \right) \\ &= \tfrac{1}{n^2} \sum_{s=0}^{n-1} \left(\sum_{k+l \equiv s \pmod n} \alpha^{ik+jl} \right) g^s, \end{aligned}$$

como $k = nt - l + s$, para algum t inteiro que depende de k e l, temos

$$\begin{aligned} e_i \cdot e_j &= \tfrac{1}{n^2} \sum_{s=0}^{n-1} \left(\sum_{l=0}^{n-1} \alpha^{i(nt-l)+jl} \right) \alpha^{is} g^s \\ &= \tfrac{1}{n^2} \sum_{s=0}^{n-1} \left(\sum_{l=0}^{n-1} \alpha^{l(j-i)} \right) \alpha^{is} g^s. \end{aligned}$$

Quando $i = j$,

$$\begin{aligned} {e_i}^2 &= \tfrac{1}{n^2} \sum_{s=0}^{n-1} \underbrace{(1+1+\cdots+1)}_{n \text{ vezes}} \alpha^{is} g^s \\ &= \tfrac{1}{n^2} \sum_{s=0}^{n-1} n \alpha^{is} g^s \\ &= \tfrac{1}{n} \sum_{s=0}^{n-1} \alpha^{is} g^s \\ &= e_i. \end{aligned}$$

Como α é a n-ésima raiz primitiva da unidade,

$$\sum_{l=0}^{n-1} \alpha^{l(j-i)} = \frac{\alpha^{n(j-i)} - 1}{\alpha^{(j-i)} - 1} = 0,$$

então quando $i \neq j$,

$$e_i \cdot e_j = 0.$$

Assim os n idempotentes e_i, $0 \leq i \leq n-1$ em $F_q C_n$ são ortogonais.

□

Exemplo 2.9 *Consideremos F_q um corpo com $q = 3\Gamma + 1$ elementos e $G = C_3$ o grupo cíclico de ordem 3. Vamos exibir os idempotentes de F_qG e ver que o número destes idempotentes corresponde ao número de classes q-ciclotômicas de G.*

Temos que $C_3 = \{1, g, g^2\}$ e $g^q = g^{3\Gamma+1} = (g^3)^\Gamma g^1 = g$.

Pelo teorema 2.8, *os idempotentes primitivos são:*

$$\begin{aligned} e_0 &= \tfrac{1}{3}(1+g+g^2), \\ e_1 &= \tfrac{1}{3}(1+\alpha g+\alpha^2 g^2), \\ e_2 &= \tfrac{1}{3}(1+\alpha^2 g+\alpha g^2), \end{aligned}$$

sendo α *a raiz cúbica primitiva da unidade em* F_q. *Observemos que* $3\cdot(2\Gamma+1) = 2(3\Gamma+1)+1 = 2q+1 \equiv 1 \pmod{q}$. *Logo* $2\Gamma+1$ *é o inverso de* 3 *módulo* q. *Isto implica que:*

$$\begin{aligned} e_0 &= (2\Gamma+1)(1+g+g^2), \\ e_1 &= (2\Gamma+1)(1+\alpha g+\alpha^2 g^2), \\ e_2 &= (2\Gamma+1)(1+\alpha^2 g+\alpha g^2). \end{aligned}$$

Como C_3 *é um grupo cíclico finito, então as classes q-ciclotômicas de* C_3 *são:*

$$\{1\}, \quad \{g\}, \quad \{g^2\}.$$

Portanto temos 3 *idempotentes em* F_qC_3 *e* 3 *classes q-ciclotômicas em* C_3.

No caso particular $F_q = \mathbb{Z}_7$, $q = 7$ *e* $\Gamma = 2$, *temos que* $\alpha = 2$, *é raiz cúbica primitiva da unidade em* $\mathbb{Z}_7$. *Os idempotentes são:*

$$\begin{aligned} e_0 &= 5(1+g+g^2), \\ e_1 &= 5(1+2g+4g^2), \\ e_2 &= 5(1+4g+2g^2). \end{aligned}$$

Exemplo 2.10 *Conforme teorema* 2.8, *os idempotentes da álgebra de grupo* $F_qG = \mathbb{Z}_7C_6$, *são:*

$$\begin{aligned} e_0 &= \tfrac{1}{6}(1+g+g^2+g^3+g^4+g^5) \\ e_1 &= \tfrac{1}{6}(1+3g+2g^2+6g^3+4g^4+5g^5) \\ e_2 &= \tfrac{1}{6}(1+2g+4g^2+g^3+2g^4+4g^5) \\ e_3 &= \tfrac{1}{6}(1+6g+g^2+6g^3+g^4+6g^5) \\ e_4 &= \tfrac{1}{6}(1+4g+2g^2+g^3+4g^4+2g^5) \\ e_5 &= \tfrac{1}{6}(1+5g+4g^2+6g^3+2g^4+3g^5). \end{aligned}$$

Para a álgebra de grupo $\mathbb{Z}_7C_6$ *e* $\alpha = 3$, *os polinômios testes são, conforme [1], página 110:*

$$
\begin{aligned}
h_0(x) &= x - \alpha^0 = x - 1 \pmod 7 \\
h_1(x) &= x - \alpha^5 = x - 5 \pmod 7 \\
h_2(x) &= x - \alpha^{2\cdot 5} = x - 4 \pmod 7 \\
h_3(x) &= x - \alpha^{3\cdot 5} = x - 6 \pmod 7 \\
h_4(x) &= x - \alpha^{4\cdot 5} = x - 2 \pmod 7 \\
h_5(x) &= x - \alpha^{5\cdot 5} = x - 3 \pmod 7
\end{aligned}
$$

Lembrando que os códigos RS são um caso particular dos códigos BCH, vamos calcular, de acordo com [1], página 110, os idempotentes do código RS sobre $\mathbb{Z}_7$, *com parâmetros* $[6, 2, 5]$, *e os polinômios geradores correspondentes:*

Idempotentes	*Polinômio gerador* $g_i(x)$
$e'_0 = e_0 + e_1$	$x^4 + 6x^3 + 3x^2 + 2x + 4$
$e'_1 = e_1 + e_2$	$x^4 + 2x^3 + 5x^2 + 5x + 1$
$e'_2 = e_2 + e_3$	$x^4 + 3x^3 + 6x^2 + 2x + 2$
$e'_3 = e_3 + e_4$	$x^4 + x^3 + 3x^2 + 5x + 4$
$e'_4 = e_4 + e_5$	$x^4 + 5x^3 + 5x^2 + 2x + 1$

2.3 Idempotentes primitivos em $F_qC_{p^n}$ com p primo

Nesta seção iremos abordar um teorema demonstrado primeiramente por Arora e Pruthi [1], em que calcula-se os idempotentes primitivos de $F_qC_{p^n}$ por meio das classes q-ciclotômicas e, mais tarde, demonstrado de forma mais prática por Ferraz e Milies [9]. Vejamos primeiramente a demonstração de Ferraz e Milies [9].

Sejam H um subgrupo de um grupo G e F_q um corpo com q elementos. Se $mdc(q, |H|) = 1$, temos que

$$\hat{H} = \frac{1}{|H|} \sum_{h \in H} h$$

está bem definido e, conforme já demonstramos na observação 1.12, é um idempotente da álgebra de grupo F_qG.

Lema 2.11 *Sejam* F_q *um corpo finito com* q *elementos,* p *um primo e* $G = C_{p^n}$ *um grupo cíclico de ordem* p^n, $n \geq 1$. *Considere*

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

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

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

formam um conjunto de idempotentes ortogonais de F_qG tais que $e_0+e_1+\cdots+e_n = 1$.

Demonstração:

Sabemos que ${e_0}^2 = e_0$. Observemos que, em geral, se $j \leq i$, então $G_j \supset G_i$ e

$$\begin{aligned}
\hat{G}_i\hat{G}_j &= \tfrac{1}{|G_i|}\tfrac{1}{|G_j|}\sum_{b\in G_i}\sum_{d\in G_j} bd \\
&= \tfrac{1}{|G_i|}\tfrac{1}{|G_j|}\sum_{b\in G_i}\sum_{d\in G_j} d \\
&= \tfrac{1}{|G_i|}\tfrac{1}{|G_j|}|G_i|\sum_{d\in G_j} d \\
&= \tfrac{1}{|G_j|}\sum_{d\in G_j} d \\
&= \hat{G}_j.
\end{aligned}$$

Vejamos que ${e_i}^2 = e_i$, para $i = 1, \cdots, n$. De fato,

$$\begin{aligned}
e_i \cdot e_i &= (\hat{G}_i - \hat{G}_{i-1})(\hat{G}_i - \hat{G}_{i-1}) \\
&= (\hat{G}_i)^2 - 2\hat{G}_i \cdot \hat{G}_{i-1} + (\hat{G}_{i-1})^2 \\
&= \hat{G}_i - 2\hat{G}_{i-1} + \hat{G}_{i-1} \\
&= \hat{G}_i - \hat{G}_{i-1} \\
&= e_i.
\end{aligned}$$

Resta verificar se estes idempotentes são ortogonais:

$$e_0 \cdot e_i = \hat{G}_0(\hat{G}_i - \hat{G}_{i-1}) = \hat{G}_0 \cdot \hat{G}_i - \hat{G}_0 \cdot \hat{G}_{i-1} = \hat{G}_0 - \hat{G}_0 = 0.$$

E para $0 < i < j$ temos

$$\begin{aligned}
e_i \cdot e_j &= (\hat{G}_i - \hat{G}_{i-1})(\hat{G}_j - \hat{G}_{j-1}) \\
&= \hat{G}_i \cdot \hat{G}_j - \hat{G}_i \cdot \hat{G}_{j-1} - \hat{G}_{i-1} \cdot \hat{G}_j + \hat{G}_{i-1} \cdot \hat{G}_{j-1} \\
&= \hat{G}_i - \hat{G}_i - \hat{G}_{i-1} + \hat{G}_{i-1} \\
&= 0.
\end{aligned}$$

Assim temos que $e_0, e_1, \cdots, e_n$ são $n+1$ idempotentes distintos ortogonais dois a dois, formando assim uma família completa de idempotentes ortogonais. Além

disso, claramente $e_0 + e_1 + \cdots + e_n = 1$. □

Em geral os idempotentes não são necessariamente primitivos. O seguinte corolário garante quando a família de idempotentes $e_0, e_1, \cdots, e_n$, mostrado anteriormente, é uma família completa de idempotentes ortogonais primitivos.

Corolário 2.12 *Sejam F_q um corpo finito com q elementos e G um grupo cíclico de ordem p^n, p primo. Então o conjunto de idempotentes dados no lema 2.11 é um conjunto de idempotentes primitivos de F_qG se, e somente se, uma das seguintes afirmativas valem:*

i) $p = 2$ e, ou $n = 1$ e q é ímpar, ou $n = 2$ e $q \equiv 3 \pmod 4$;

ii) p é ímpar e $o(q) = \phi(p^n)$ em $\mathcal{U}(\mathbb{Z}_{p^n})$.

Demonstração:

Conforme teorema 1.9, de Perlis-Walker, $F_qG \simeq \bigoplus_{d|p^n} a_d F_q(\xi_d)$, isto é, a álgebra de grupo F_qG contém exatamente $n+1$ idempotentes primitivos e pelo corolário 2.7 podemos demonstrar que uma das afirmativas sempre valem. □

Como consequência direta do lema 2.11 e corolário 2.12 temos o teorema 3.1 de Ferraz e Milies [3].

Teorema 2.13 (Ferraz-Milies) *Sejam F_q um corpo finito com q elementos e G um grupo cíclico de ordem p^n tal que $o(q) = \phi(p^n)$ em $\mathcal{U}(Z_{p^n})$ com p primo ímpar. Seja*

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

***uma** cadeia descendente de **todos** os subgrupos de G. Então, um conjunto de idempotentes primitivos de F_qG, é dado por:*

$$e_0 = \frac{1}{p^n}\left(\sum_{g \in G} g\right) \quad e \quad e_i = \hat{G}_i - \hat{G}_{i-1}, \quad 1 \leq i \leq n.$$

Estes idempotentes determinam o conjunto de ideais minimais em F_qG, e portanto os códigos cíclicos minimais de comprimento p^n sobre F_q. Em um artigo anterior ao de Ferraz e Milies, Arora e Pruthi [1] mostram no teorema 3.5 expressões

explícitas para os $n+1$ idempotentes primitivos de $F_qC_{p^n}$ sendo F_q um corpo de ordem potência prima q, onde a ordem de q módulo p^n é $\phi(p^n)$. Em particular, Arora e Pruthi definem os conjuntos:

$$\Omega_i := \{p^{i-1}, p^{i-1}q, \cdots, p^{i-1}q^{\phi(p^{n-i+1})-1}\} \tag{2.2}$$

para $i = 1, 2, \cdots, n$, e

$$\bar{C}_i := \sum_{s\in\Omega_i} g^s \in F_qC_{p^n}$$

onde q é um primo com ordem $\phi(p^n)$ módulo p^n e g é o gerador de C_{p^n}.

Teorema 2.14 (Arora-Pruthi) *$F_qC_{p^n}$ tem $n+1$ idempotentes primitivos dados por*

$$e_0 = \frac{1}{p^n}\left(1 + \sum_{i=1}^{n} \bar{C}_i\right),$$

e

$$e_i = \frac{1}{p^{n-i+1}}[(p-1)(1 + \bar{C}_{i+1} + \cdots + \bar{C}_n) - \bar{C}_i], \quad \textit{para} \quad 1 \leq i \leq n.$$

Ao invés de escrevermos a demonstração de Arora e Pruthi, responderemos aqui uma pergunta natural e interessante: São os idempotentes encontrados por Arora e Pruthi os mesmos que os encontrados por Ferraz e Milies?

Observação 2.15 *Os idempotentes encontrados por Arora e Pruthi são os mesmos que os encontrados por Ferraz e Milies.*

De fato, definindo $\Lambda_i = \bigcup_{j=i}^{n} \Omega_i \cup \{0\}$ temos que

$$G_i = \{g^k : k \in \Lambda_i\}$$

é o subgrupo de $G = \langle g \rangle$ gerado por $g^{p^{i-1}}$, já que todo elemento de Λ_i é da forma p^lq^s, com $l \geq i-1$, assim

$$g^{p^lq^s} = (g^{p^{i-1}})^{p^{l-i+1}q^s} \in \langle g^{p^{i-1}} \rangle = G_i,$$

e

$$p^{n-i+1}\hat{G}_i = \sum_{k\in\Lambda_i} g^k = 1 + \sum_{j=i}^{n}\sum_{k\in\Omega_j} g^k = 1 + \sum_{j=i}^{n} \bar{C}_j,$$

donde $e_0 = \hat{G}_0$ e

$$\begin{aligned}
\hat{G}_{i+1} - \hat{G}_i &= \tfrac{1}{p^{n-i}}\left(1 + \sum_{j=i+1}^{n} \bar{C}_j\right) - \tfrac{1}{p^{n-i+1}}\left(1 + \sum_{j=i}^{n} \bar{C}_j\right) \\
&= \frac{1}{p^{n-i+1}}\left(p + p\sum_{j=i+1}^{n} \bar{C}_j - 1 - \sum_{j=i}^{n} \bar{C}_j\right) \\
&= \frac{1}{p^{n-i+1}}\left[(p-1)\left(1 + \sum_{j=i+1}^{n} \bar{C}_j\right) - \bar{C}_i\right],
\end{aligned}$$

o que responde à pegunta.

Exemplo 2.16 *Sejam $G = \langle g \rangle$ um grupo cíclico de ordem $5^3 = 125$, e F_q um corpo de ordem potência prima q, onde q tem ordem $\phi(5^3) \equiv 100 \pmod{125}$. Notemos que $q = 127 \equiv 2 \pmod{125}$ satisfaz esses critérios. Por* (2.2), *página* 43, *as classes q-ciclotômicas módulo* 125 *são:*

$$\begin{aligned}
\Omega_1 &= \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 14, 16, \cdots, 121, 122, 123, 124\} \\
\Omega_2 &= \{5, 10, 15, 20, 30, 35, 40, 45, 55, 60, 65, 70, 80, 85, 90, 95, 105, 110, 115, 120\} \\
\Omega_3 &= \{25, 50, 75, 100\},
\end{aligned}$$

e pelo teorema 2.14, *os idempotentes são:*

$$\begin{aligned}
e_0 &= \tfrac{1}{5^3}[1 + \bar{C}_1 + \bar{C}_2 + \bar{C}_3] \\
e_1 &= \tfrac{1}{5^3}[4(1 + \bar{C}_2 + \bar{C}_3) - \bar{C}_1] \\
e_2 &= \tfrac{1}{5^2}[4(1 + \bar{C}_3) - \bar{C}_2] \\
e_3 &= \tfrac{1}{5}[3\bar{C}_3].
\end{aligned}$$

As próximas seções são baseadas no artigo de Ferraz e Milies [9].

2.4 Polinômios geradores de $I_i = (F_qG)(\hat{G}_i - \hat{G}_{i-1})$ sendo G grupo cíclico de ordem p^n

Consideremos F_q um corpo com q elementos e G um grupo cíclico de ordem p^n. Então os polinômios geradores de $I_i = (F_qG)(\hat{G}_i - \hat{G}_{i-1})$ podem ser computados conforme mostraremos abaixo. Se $e_i(x) \in F_q[x]$ é um polinômio qualquer tal que $e_i(g) = e_i$, então o polinômio gerador de I_i é dado por:

$$g_i(x) = mdc\left(e_i(x), x^{p^n} - 1\right), \quad 0 \leq i \leq n.$$

Tomando $e_i = \hat{G}_i - \hat{G}_{i-1}$, podemos considerar

$$\begin{aligned} e_i(x) &= \frac{1}{p^{n-i}} \sum_{j=0}^{p^{n-i}-1} x^{jp^i} - \frac{1}{p^{n-i+1}} \sum_{j=0}^{p^{n-i+1}-1} x^{jp^{i-1}} \\ &= \frac{1}{p^{n-i}} \left(\frac{x^{p^n}-1}{x^{p^i}-1} \right) - \frac{1}{p^{n-i+1}} \left(\frac{x^{p^n}-1}{x^{p^{i-1}}-1} \right) \\ &= \frac{x^{p^n}-1}{p^{n-i+1}} \left(\frac{p}{x^{p^i}-1} - \frac{1}{x^{p^{i-1}}-1} \right). \end{aligned}$$

Observemos que

$$\begin{aligned} (x^{p^i}-1) &= (x^{p^{i-1}})^p - 1 \\ &= (x^{p^{i-1}}-1)[(x^{p^{i-1}(p-1)}) + (x^{p^{i-1}(p-2)}) + \cdots + (x^{p^{i-1}}) + 1], \end{aligned}$$

assim,

$$\begin{aligned} e_i(x) &= \tfrac{1}{p^{n-i+1}} \left(\tfrac{x^{p^n}-1}{x^{p^i}-1} \right) (p - x^{p^{i-1}(p-1)} - x^{p^{i-1}(p-2)} - \cdots - x^{p^{i-1}} - 1) \\ &= \tfrac{1}{p^{n-i+1}} \left(\tfrac{x^{p^n}-1}{x^{p^i}-1} \right) M(x), \end{aligned}$$

onde $M(x) = (p - x^{p^{i-1}(p-1)} - x^{p^{i-1}(p-2)} - \cdots - x^{p^{i-1}} - 1)$.

Desta forma,

$$mdc\left(e_i(x)\ ,\ x^{p^n}-1\right) = \frac{x^{p^n}-1}{x^{p^i}-1} mdc\left(M(x)\ ,\ x^{p^i}-1\right),$$

com

$$mdc\left(M(x)\ ,\ x^{p^i}-1\right) \ = \ mdc\left(M(x)\ ,\ (x^{p^{i-1}}-1)(R(x))\right),$$

onde $R(x) = x^{p^{i-1}(p-1)} + x^{p^{i-1}(p-2)} + \cdots + x^{p^{i-1}} + 1$.

Sabemos que $x^{p^{i-1}} \equiv 1 \pmod{x^{p^{i-1}}-1}$. Então $x^{p^{i-1}k} \equiv 1^k \equiv 1 \pmod{x^{p^{i-1}}-1}$, para todo $k \in \mathbb{N}$, assim $R(x) \equiv p \pmod{x^{p^{i-1}}-1}$. Portanto $x^{p^{i-1}}-1$ divide $p - R(x) = M(x)$. Temos então que

$$mdc\left(M(x)\ ,\ (x^{p^{i-1}}-1)\,(R(x))\right) = (x^{p^{i-1}}-1) mdc\left(\frac{M(x)}{(x^{p^{i-1}}-1)}\ ,\ R(x)\right).$$

Como $mdc\left(\frac{M(x)}{(x^{p^{i-1}}-1)}\ ,\ R(x)\right)$ divide $mdc\,(M(x), R(x))$ e

$$mdc\,(M(x), R(x)) = mdc\,(p, R(x)) = 1,$$

então $mdc\left(\frac{M(x)}{(x^{p^{i-1}}-1)}\ ,\ R(x)\right)=1$.
Logo

$$\begin{aligned} g_i(x) &= mdc\left(e_i(x), x^{p^n}-1\right) \\ &= \frac{x^{p^n}-1}{x^{p^i}-1}\left(x^{p^{i-1}}-1\right) \\ &= \left(x^{p^i(p^{n-i}-1)}+x^{p^i(p^{n-i}-2)}+\cdots+x^{p^i}+1\right)\left(x^{p^{i-1}}-1\right). \end{aligned} \tag{2.3}$$

Como $\partial\left(g_i(x)\right)=p^i(p^{n-i}-1)+p^{i-1}$, obtemos que

$$dim(I_i)=p^n-\partial\left(g_i(x)\right)=p^i-p^{i-1}=\phi(p^i).$$

Exemplo 2.17 *Continuando o exemplo 2.16, e considerando E_0, E_1, E_2, E_3 códigos cíclicos de comprimento* 125, *temos os seguintes parâmetros:*

Código	*Dimensão*	*Distância*	*Polinômio Gerador $g_i(x)$*
E_0	1	125	$g_0(x)=1+x+x^2+\cdots+x^{124}$
E_1	4	50	$g_1(x)=(x-1)(1+x^5+x^{10}+\cdots+x^{120})$
E_2	20	10	$g_2(x)=(x^5-1)(1+x^{25}+x^{50}+x^{75}+x^{100})$
E_3	100	2	$g_3(x)=x^{25}-1$,

onde a dimensão é o grau do polinômio $h_i(x)=\frac{x^{125}-1}{g_i(x)}$, a distância é o número de somandos distintos de $g_i(x)$, por exemplo, em E_3, $g_3(x)=x^{25}-1$ tem dois somandos distintos, x^{25} e 1, *e o polinômio gerador é calculado por* (2.3), *página* 46.

2.5 Estendendo resultados para p-grupos abelianos finitos

Consideremos G um p-grupo abeliano, F_q um corpo com q elementos, sendo $mdc(q,|G|)=1$. Para cada subgrupo H de G tal que $G/H\neq\{1\}$ é cíclico, podemos construir um idempotente de F_qG. Como G/H é um grupo cíclico de ordem potência de p, então existe somente um subgrupo H^* de G contendo H, tal que $|H^*/H|=p$. Definamos $e_H=\hat{H}-\hat{H}^*$, observemos que $e_H\neq 0$, e:

Lema 2.18 *Os elementos e_H definidos acima junto com $e_G=\hat{G}$ formam um conjunto de idempotentes ortogonais dois a dois de F_qG cuja soma é igual a* 1.

Demonstração:

Como já mostramos no lema 2.11, estes elementos são idempotentes. Sejam H e K subgrupos diferentes de G tais que G/H e G/K são cíclicos, diferentes de $\{1\}$, e sejam H^* e K^* subgrupos contendo H e K respectivamente, tais que H^*/H e K^*/K são cíclicos de ordem p. Primeiro vamos considerar o caso em que $H \subsetneq K$, neste caso $H^* \subseteq K$. Assim:

$$\begin{aligned} e_H e_K &= (\hat{H} - \hat{H^*})(\hat{K} - \hat{K^*}) \\ &= \hat{H}\hat{K} - \hat{H}\hat{K^*} - \hat{H^*}\hat{K} + \hat{H^*}\hat{K^*} \\ &= \hat{K} - \hat{K^*} - \hat{K} + \hat{K^*} \\ &= 0. \end{aligned}$$

Consideremos agora o caso em que nenhum desses subgrupos está contido no outro. Então H e K estão propriamente contidos em HK, mas H^* e K^* estão também contidos em HK, então $H^*K^* \subset HK$ e $HK \subset H^*K^*$, portanto $H^*K^* = HK$. Como $HK \subset HK^* \subset H^*K^*$, segue que $HK^* = HK$, analogamente $H^*K = HK$. Assim, como

$$\begin{aligned} e_H e_K &= (\hat{H} - \hat{H^*})(\hat{K} - \hat{K^*}) \\ &= \hat{H}\hat{K} - \hat{H}\hat{K^*} - \hat{H^*}\hat{K} + \hat{H^*}\hat{K^*}, \end{aligned}$$

para mostrar que $e_H e_K = 0$, basta provarmos que $\hat{H}\hat{K} = \widehat{HK}$. Provemos agora que $\hat{H}\hat{K} = \widehat{HK}$. Como $H \triangleleft HK$ e $K \triangleleft HK$, pelo 2^o teorema do isomorfismo $\frac{HK}{H} \simeq \frac{K}{H \cap K}$. Logo

$$|HK||H \cap K| = |K||H|.$$

Observemos que $\frac{HK}{H} = \{\bar{x_1}, \bar{x_2}, \cdots, \bar{x_l}\}$, com $x_i \in K$, $i = 1, \cdots, l$ e $l = \frac{|K|}{|H \cap K|}$.

$$\begin{aligned} \widehat{HK} &= \frac{1}{|HK|} \sum_{g \in HK} g \\ &= \frac{1}{|HK|} \sum_{j=1}^{l} \sum_{h \in H} x_j h \\ &= \frac{1}{|HK|} \sum_{j=1}^{l} x_j \sum_{h \in H} h \\ &= \frac{1}{|HK|} \sum_{j=1}^{l} x_j |H| \hat{H}. \end{aligned}$$

Por outro lado,

$$\begin{aligned}\sum_{g\in H\cap K} g\sum_{j=1}^{l} x_j &= \sum_{g\in H\cap K}\sum_{j=1}^{l} gx_j \\ &= \sum_{k\in K} k = |K|\hat{K}\end{aligned}$$

e

$$\sum_{g\in H\cap K} g = |H\cap K|\widehat{H\cap K}.$$

Multiplicando $\widehat{HK} = \frac{1}{|HK|}\sum_{j=1}^{l} x_j|H|\hat{H}$ por $\widehat{H\cap K}$, temos:

$$\widehat{H\cap K}\,\widehat{HK} = \frac{1}{|HK|}\widehat{H\cap K}\sum_{j=1}^{l} x_j|H|\hat{H}.$$

Como $\widehat{H\cap K}\,\widehat{HK} = \widehat{HK}$,

$$\widehat{HK} = \frac{1}{|HK|}\hat{K}\frac{|K|}{|H\cap K|}|H|\hat{H} = \hat{H}\hat{K}.$$

Mostramos então que os e_H são idempotentes ortogonais dois a dois. O resultado segue, de forma análoga, se um dos idempotentes é e_G. Resta mostrar que a soma desses idempotentes é igual a 1. Para cada subgrupo cíclico C de G denotamos por $\mathcal{L}(C)$ o conjunto de todos elementos de C que geram este subgrupo, isto é:

$$\mathcal{L}(C) = \{c \in C : o(c) = |C|\}.$$

Se $\mathcal{F}$ denota a família de todos os subgrupos cíclicos de G, então $|G| = \sum_{C\in\mathcal{F}} |\mathcal{L}(C)|$, pois cada elemento de G gera um único grupo cíclico. Como G é um p-grupo, $|\mathcal{L}(C)| = |C| - |C|/p$. De fato, seja $C = \langle g\rangle$ em que $g^{p^i} = 1$, isto é, $o(g) = |C| = p^i$. Então $C = \{g^k : k = 1, \cdots, p^i\}$, $o(g^k) = \dfrac{o(g)}{mdc(o(g),k)} = \dfrac{p^i}{mdc(p^i,k)} = p^i$ se, e somente se, $mdc(p^i, k) = 1$, assim $|\mathcal{L}(C)| = \phi(p^i) = p^i - p^{i-1} = |C| - |C|/p$.

Seja S o conjunto de todos os subgrupos H de G tais que o quociente G/H é cíclico, e seja $e = \sum_{H\in S} e_H$. Queremos mostrar que $e = 1$. Então basta provar que $(F_qG)e = F_qG$. Como já mostramos que esses idempotentes são ortogonais dois a dois, temos que:

$$(F_qG)e = \bigoplus_{H\in S}(F_qG)e_H,$$

então

$$dim_{F_q}((F_qG)e) = \sum_{H\in S} dim_{F_q}((F_qG)e_H).$$

Dado que $\hat{H} = \hat{H^*} + e_H$, e $\hat{H^*}e_H = 0$, temos que:

$$(F_qG)\hat{H} = (F_qG)\hat{H^*} \oplus (F_qG)e_H.$$

Logo

$$dim_{F_q}((F_qG)e_H) = dim_{F_q}(F_qG)\hat{H} - dim_{F_q}(F_qG)\hat{H^*}$$

e conforme proposição 1.14,

$$dim_{F_q}((F_qG)e_H) = dim_{F_q}F_q[G/H] - dim_{F_q}F_q[G/H^*], \tag{2.4}$$

segue que

$$dim_{F_q}F_q[G/H] = |G/H| \quad \text{e} \quad dim_{F_q}F_q[G/H^*] = |G/H^*|.$$

Sabemos que existe uma bijeção $\psi : \mathcal{F} \to S$, tal que para todo $C \in \mathcal{F}$, $|C| = |G/\psi(C)|$. Isto é uma consequência da teoria de caracter para grupos abelianos finitos, conforme vimos no lema 1.23 e teorema 1.24. Consideremos $C \in \mathcal{F}$ o subgrupo tal que $\psi(C) = H$, como

$$dim_{F_q}F_q[G/H] = |G/H| = |G/\psi(C)| = |C|$$

e

$$dim_{F_q}F_q[G/H^*] = |G/H^*| = |G/H|/|H^*/H| = |C|/p,$$

então

$$dim_{F_q}\left((F_qG)e_H\right) = |C| - |C|/p = |\mathcal{L}(C)|.$$

Assim

$$dim_{F_q}\left((F_qG)e\right) = \sum_{H\in S} dim_{F_q}\left((F_qG)e_H\right) = \sum_{C\in\mathcal{F}_{\text{II}}} |\mathcal{L}(C)| = |G|.$$

□

Como consequência imediata do lema temos os teoremas 2.19 e 2.21.

Teorema 2.19 *Sejam p um primo e G um p-grupo abeliano de ordem p^n e de expoente p^r. Então, o conjunto de idempotentes dados acima é o conjunto de idempotentes primitivos de F_qG se, e somente se, valem alguma das seguintes afirmações:*

i) $p^r = 2$ *e* q *é ímpar.*

ii) $p^r = 4$ *e* $q \equiv 3 \pmod 4$.

iii) p *é um primo ímpar e* $o(q) = \phi(p^r)$ *em* $\mathcal{U}(\mathbb{Z}_{p^r})$.

2.6 Idempotentes primitivos em F_qG onde G é um grupo abeliano de expoente $2p^r$

Consideremos primeiramente um grupo cíclico de ordem $2p^n$. Os idempotentes geradores de ideais minimais são dados pelo seguinte resultado:

Teorema 2.20 *Sejam F_q 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 $\mathcal{U}(\mathbb{Z}_{2p^n})$. Seja $G = C \times A$ onde A é o p-Sylow subgrupo de G e $C = \{1, t\}$ é seu 2-Sylow subgrupo. Denotemos por e_i, $0 \leq i \leq n$, os idempotentes primitivos de F_qA, então os idempotentes primitivos de F_qG são:*

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

Demonstração:

Observemos que $\frac{1+t}{2}$ e $\frac{1-t}{2}$ geram F_qC, pois

$$\left(\frac{1+t}{2}\right) + \left(\frac{1-t}{2}\right) = 1$$

e

$$\left(\frac{1+t}{2}\right) - \left(\frac{1-t}{2}\right) = t.$$

e são claramente linearmente independentes. Logo $\frac{1+t}{2}$ e $\frac{1-t}{2}$ formam uma base para F_qC.

Além disso, $\left(\frac{1+t}{2}\right)$ e $\left(\frac{1-t}{2}\right)$ são idempotentes ortogonais. De fato,

$$\left(\frac{1+t}{2}\right)^2 = \frac{1+2t+t^2}{4} = \frac{1+2t+1}{4} = \frac{2+2t}{4} = \frac{1+t}{2},$$

$$\left(\frac{1-t}{2}\right)^2 = \frac{1-2t+t^2}{4} = \frac{1-2t+1}{4} = \frac{2-2t}{4} = \frac{1-t}{2}$$

e

$$\left(\frac{1+t}{2}\right)\left(\frac{1-t}{2}\right) = \left(\frac{1-t^2}{4}\right) = 0.$$

Como $G = C \times A$,

$$\begin{aligned} F_qG &= F_q(C \times A) \\ &\cong F_qC \otimes F_qA \quad \text{(conforme proposição 1.17)} \\ &\cong [F_q\left(\tfrac{1+t}{2}\right) \oplus F_q\left(\tfrac{1-t}{2}\right)] \otimes F_qA \\ &\cong \left(F_q\left(\tfrac{1+t}{2}\right) \otimes F_qA\right) \oplus \left(F_q\left(\tfrac{1-t}{2}\right) \otimes F_qA\right) \quad \text{(conforme proposição 1.15)} \\ &\cong F_q\left(\tfrac{1+t}{2}\right) A \oplus F_q\left(\tfrac{1-t}{2}\right) A \\ &\cong \left(\tfrac{1+t}{2}\right) F_qA \oplus \left(\tfrac{1-t}{2}\right) F_qA. \end{aligned}$$

Por hipótese, e_i, $0 \leq i \leq n$, denotam os idempotentes de F_qA, isto é, $F_qA = F_qAe_0 + F_qAe_1 + \cdots + F_qAe_n$. Portanto,

$$\begin{aligned} F_qG &\cong \left(\tfrac{1+t}{2}\right)(F_qAe_0 \oplus \cdots \oplus F_qAe_n) \oplus \left(\tfrac{1-t}{2}\right)(F_qAe_0 \oplus \cdots \oplus F_qAe_n) \\ &\cong \left(\tfrac{1+t}{2}\right) F_qAe_0 \oplus \left(\tfrac{1+t}{2}\right) F_qAe_1 \oplus \cdots \oplus \left(\tfrac{1+t}{2}\right) F_qAe_n \oplus \\ &\qquad \oplus \left(\tfrac{1-t}{2}\right) F_qAe_0 \oplus \left(\tfrac{1-t}{2}\right) F_qAe_1 \oplus \cdots \oplus \left(\tfrac{1-t}{2}\right) F_qAe_n. \end{aligned}$$

Logo $\left(\frac{1+t}{2}\right) e_i$ e $\left(\frac{1-t}{2}\right) e_i$, com $i = 0, \cdots, n$ são os $2n+2$ idempotentes ortogonais de F_qG.

□

Seja o seguinte teorema, consequência do lema 2.18 :

Teorema 2.21 *Sejam p um primo ímpar, F_q um corpo com q elementos e G um grupo abeliano de expoente $2p^r$ tal que $o(q) = \phi(p^r)$ em $\mathcal{U}(\mathbb{Z}_{2p^r})$. Seja $G = E \times B$, onde E é um 2-grupo abeliano e B é um p-grupo. Então os idempotentes primitivos de F_qG são os produtos da forma $e \cdot f$, onde e é um idempotente primitivo de F_qE e f é um idempotente primitivo de F_qB.*

Observação 2.22 *Os idempotentes primitivos de F_qB foram dados pelo teorema 2.19 e escrevendo $E = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$, produto de grupos cíclicos de ordem 2, então os idempotentes primitivos de F_qE são todos os produtos da forma $e = e_1e_2 \cdots e_n$, onde*

$$e_i = \frac{1+g_i}{2} \quad ou \quad e_i = \frac{1-g_i}{2}, \quad 1 \leq i \leq n.$$

Vimos que se F_q é um corpo finito de q elementos e G um grupo abeliano finito de expoente e, então pelo corolário 2.7 temos que os teoremas 2.19 e 2.21 descrevem

os únicos casos onde os elementos idempotentes primitivos de álgebras de grupos finitos podem ser calculados por este caminho.

2.7 Cálculo da dimensão e da distância mínima dos ideais de F_qG

Vamos calcular agora a dimensão e a distância mínima destes códigos.

Consideremos p um primo ímpar, n um inteiro positivo, $m \geq 0$, $|G| = 2^m p^n$ e expoente p^r ou $2p^r$, onde G é um grupo abeliano e F_q um corpo com q elementos. Seja $G = E \times B$, onde E é um 2-grupo abeliano de ordem 2^m e B um p-grupo.

Já sabemos que os idempotentes primitivos de F_qE são todos os produtos da forma $e_E = e_1 e_2 \cdots e_m$, onde

$$e_i = \frac{1+g_i}{2} \quad \text{ou} \quad e_i = \frac{1-g_i}{2}, \quad 1 \leq i \leq m,$$

e os idempotentes primitivos de F_qG são produtos da forma $e_E \cdot e_B$, onde e_E são os idempotentes primitivos de F_qE e e_B os idempotentes primitivos de F_qB.

Sejam e_E um idempotente fixo de F_qE e y um elemento de E, desta forma podemos escrever $y = {g_1}^{\epsilon_1} \cdots {g_m}^{\epsilon_m}$, onde $\epsilon_i = 0$ ou 1, $1 \leq i \leq m$. Logo

$$ye_E = {g_1}^{\epsilon_1} \left(\frac{1 \pm g_1}{2}\right) \cdots {g_m}^{\epsilon_m} \left(\frac{1 \pm g_m}{2}\right) = \pm e_E = (-1)^{\epsilon_y} e_E, \tag{2.5}$$

onde $\epsilon_y = 0$ ou 1.

Vamos primeiro considerar os idempotentes da forma $e_E\hat{B}$. Um elemento de $(F_qG) \cdot e_E\hat{B}$ é da forma $\gamma \cdot e_E\hat{B}$, onde $\gamma = \sum_{y \in E, b \in B} x_{yb} yb$. Então:

$$\gamma \cdot e_E\hat{B} = \sum_{y \in E, b \in B} x_{yb} y e_E \cdot b\hat{B} = \left(\sum_{y \in E, b \in B} x_{yb}(-1)^{\epsilon_y}\right) e_E\hat{B} = C_\gamma e_E\hat{B}, \tag{2.6}$$

com $C_\gamma \in F_q$. Se $B^* \supset B$ temos de igual forma que $\gamma e_E\hat{B^*} = C_\gamma e_E\hat{B^*}$.

Se $I = (F_qG) \cdot e_E\hat{B}$, então

$$\begin{aligned} dim_{F_q}[F_qG \cdot e_E\hat{B}] &= dim_{F_q}[F_q[E \times B]e_E\hat{B}] \\ &= dim_{F_q}[((F_qE)B)\, e_E\hat{B}] \\ &= dim_{F_q}[(F_qE \cdot e_E)B\hat{B}] \\ &= 1. \end{aligned}$$

e que sua distância mínima é $d = |G|$, conforme exemplo 1.28.

Consideraremos agora os idempotentes da forma $e = e_E \cdot e_H$, sendo $e_E \in F_qE$ e $e_H = \hat{H} - \hat{H^*}$, onde H é um subgrupo de B tal que B/H é cíclico de ordem p^i, e H^* é o único subgrupo de B contendo H tal que $[H^* : H] = p$. Admitamos que $I_e = (F_qG)e$.

Seja $b \in B \backslash H$, tal que $\bar{b} \in B/H$ é um gerador, assim $B = \langle H, b\rangle$. Como $\langle \bar{b}^{p^{i-1}} \rangle \subseteq B/H$ é um grupo cíclico de ordem p então $\langle H, b^{p^{i-1}} \rangle$ tem índice p sobre H, logo $H^* = \langle H, b^{p^{i-1}} \rangle$ e

$$\begin{aligned} \hat{H^*} &= \frac{1}{|H^*|} \sum_{j=0}^{p-1} \sum_{h \in H} h(b^{p^{i-1}})^j \\ &= \frac{1}{p|H|} \sum_{j=0}^{p-1} (b^{p^{i-1}})^j \sum_{h \in H} h \\ &= \frac{1}{p} \sum_{j=0}^{p-1} b^{p^{i-1}j} \cdot \hat{H}. \end{aligned}$$

Multiplicando por $1 - b^{p^{i-1}}$ temos:

$$\begin{aligned} (1 - b^{p^{i-1}})\hat{H^*} &= \frac{1}{p}(1 - b^{p^{i-1}}) \sum_{j=0}^{p-1} b^{p^{i-1}j} \cdot \hat{H} \\ &= \frac{1}{p}(1 - b^{p^i}) \cdot \hat{H} \\ &= 0. \end{aligned}$$

Logo

$$(1 - b^{p^{i-1}})e_E\hat{H} = (1 - b^{p^{i-1}})e_E(\hat{H^*} + e_H) = (1 - b^{p^{i-1}})e_Ee_H \in I_e.$$

Como $b^{p^{i-1}} \notin H$, $supp\left((1 - b^{p^{i-1}})\hat{H}\right)$ é a união disjunta $H \cup b^{p^{i-1}}H$ e o peso deste elemento é $w\left((1 - b^{p^{i-1}})e_E\hat{H}\right) = 2|E||H|$, então se denotarmos por $d(I_e)$ a distância mínima de I_e, segue que $d(I_e) \leq 2^{m+1}|H|$.

Como B é a união disjunta $B = H \cup bH \cup \cdots \cup b^{p^i-1}H$ e $G = E \times B$, G é a união disjunta, $G = (E \times H) \cup b(E \times H) \cup \cdots \cup b^{p^i-1}(E \times H)$. Assim um elemento arbitrário de F_qG pode ser escrito de forma única como $\alpha = \sum_{j=0}^{p^i-1} \alpha_j b^j$, com $\alpha_j \in F_q[E \times H]$.

Dado que $B = \langle H, b\rangle$, então para todo $\beta \in B$ temos:

$$\beta = \sum_{j=0}^{p^i-1} \sum_{h \in H} \beta_{hj} hb^j = \sum_{j=0}^{p^i-1} \beta_j b^j$$

e $\beta_j e_E e_H = \left(\sum_{h\in H} \beta_{hj} h\right) e_E e_H$. De igual forma, se $\alpha \in F_qG = F_q[E \times B]$, então

$$\alpha = \sum_{j=0}^{p^i-1} \left(\sum_{h\in E\times H} \alpha_{hj} h\right) b^j = \sum_{j=0}^{p^i-1} \alpha_j b^j.$$

Usando (2.5), (2.6) página 52, e a expressão anterior, segue que $\alpha_j e_E e_H = k_j e_E e_H$ com $k_j \in F_q$.

Como para todo $\gamma \in (F_qG)$ temos que:

$$\begin{aligned} \gamma e_E e_H &= \gamma e_E(\hat{H} - \hat{H}^*) \\ &= \gamma e_E \left(\hat{H} - \frac{1}{p}\sum_{j=0}^{p-1} b^{p^{i-1}j} \cdot \hat{H}\right) \\ &= \gamma \left(1 - \frac{1}{p}\sum_{j=0}^{p-1} b^{p^{i-1}j}\right) e_E \hat{H}, \end{aligned}$$

assim

$$(F_qG)e_E e_H \subset (F_qG)e_E\hat{H}.$$

Seja $0 \neq \delta \in (F_qG)e_E e_H$, em particular $\delta \in (F_qG)e_E\hat{H}$, então $\delta = (k_0 + k_1 b + \cdots + k_{p^i-1} b^{p^i-1})e_E\hat{H}$. Como $\delta \neq 0$, temos que existe um coeficiente $k_j \neq 0$. Vejamos que existe mais de um coeficiente distinto de zero, pois no caso que $\delta = k_j b^j e_E\hat{H} \in (F_qG)e_E e_H$ temos que

$$b^{p^i-j}\delta = k_j b^{p^i} e_H\hat{H} = k_j e_E\hat{H} \in (F_qG)e_E e_H,$$

o que implica que $e_E\hat{H} = ce_E(\hat{H} - \hat{H}^*)$ com $c \in F_q$ ou equivalentemente $(1-c)e_E\hat{H} = -ce_E\hat{H}^*$, o que contradiz que os elementos de H^* sejam linearmente independentes sobre F_q. Então, no mínimo, dois coeficientes distintos $k_j, k_{j'}$ devem ser diferentes de zero para todo $\delta \in I_e$, assim $d(I_e) \geq 2^{m+1}|H|$. Logo

$$d(I_e) = 2^{m+1}|H|.$$

Finalmente vamos calcular a dimensão destes códigos abelianos minimais, isto é, a dimensão dos ideais da forma $F_qG \cdot e$, onde e é um idempotente primitivo de F_qG. Seja $e = e_E e_H$ um tal idempotente primitivo. Temos que:

$$F_qG \cdot e_E e_H = F_q[E \times B] \cdot e_E e_H = ((F_qE)B) \cdot e_E e_H = (F_qE \cdot e_E)B \cdot e_H.$$

Como $(F_qE)\cdot e_E \cong F_q$ para todos os idempotentes primitivos de F_qE, então

$$F_qG\cdot e_Ee_H \cong F_qB\cdot e_H,$$

logo por (2.4), página 49, temos que

$$dim_{F_q}[F_qG\cdot e_Ee_H] = \phi(p^i).$$

Considerações Finais

Após o desenvolvimento deste trabalho temos em mãos ferramentas que possibilitam calcular os idempotentes primitivos de F_qG, onde G é um grupo abeliano de ordem n, p^n, $2p^n$, 2^mp^n, com n um inteiro positivo e $m \geq 0$, tal que q é um gerador de $\mathcal{U}(\mathbb{Z}_e)$ com e expoente de G e F_q é um corpo finito de ordem q. Podemos calcular também a distância mínima, a dimensão, o peso e o polinômio gerador destes códigos minimais.

Há muitas perspectivas de continuidade do tema estudado. Continuando na mesma linha desta dissertação pode-se estudar os idempotentes primitivos de F_qG quando G é um grupo cíclico de ordem qp^n com p e q primos ímpares.

Outra opção seria tentar trabalhar com álgebras de grupos F_qG onde G é um grupo não-abeliano. Em [2] foi estudado códigos quatérnios e diedrais, ambos minimais. Nesta tese de doutorado foi calculado a distância mínima, a dimensão e exibido uma base tanto para os códigos quatérnios minimais quanto para os códigos diedrais minimais, mas para o caso dos quatérnios este trabalho se restringiu ao grupo que tem ordem potência de 2, portanto temos perspectivas de continuidade para completar os demais casos dos quatérnios.

Além disso, pode-se trabalhar com álgebras de grupo não-semissimples buscando determinar, se possível, os idempotentes primitivos.

Referências Bibliográficas

[1] ARORA, S. K., PRUTHI, M., *Minimal Codes of Prime-Power Length*, Finite Fields and Their Aplications 3 (1997), 99-113.

[2] DUTRA, F. S., *Sobre códigos diedrais e quatérnios*, Tese de Doutorado, UFMG, Belo Horizonte, 2006.

[3] FERRAZ, R. A.; MILIES, C. P., *Idempotents in Group Algebras and Minimal Abelian Codes*, Finite Fields and Their Aplications 13 (2007), 382-393.

[4] GOODAIRE, E. G.; JESPERS, E.; MILIES, C. P., *Alternative Loop Rings*, North- Holland Math. Stud., vol. 184, Elsevier, Amsterdam, 1996.

[5] HAMMING, R. W., Interview, February 3-4, 1977.

[6] HEFEZ, A., VILLELA, M. L. T., *Códigos Corretores de Erros*, Rio de Janeiro, IMPA, 2008.

[7] LINT, J. H. Van, *Introduction to Coding Theory*, Department of Mathematics, Eindhoven University of Technology, Springer, 1998.

[8] MARTINEZ, F. B.; MOREIRA, C. G.; et al., *Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro*, Rio de Janeiro, IMPA, 2011.

[9] MILIES, C. P.; SEHGAL, S. K., *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002.

[10] MILIES, C. P., *Introdução à Teoria dos Códigos Corretores de Erros*, Colóquio de Matemática da Região Centro-Oeste, Departamento de Matemática, UFMS, Campo Grande, 2009.

[11] PIERCE, R. S., *Associative algebras*, Springer-Verlag, New York, 1982.

[12] ROTMAN, J. J., *An Introduction to the Theory of Groups*, fourth ed., Grad. Texts in Math., vol. 148, Springer-Verlag, New York, 1995.

[13] VERGARA, C. R. G., *Álgebras de grupos racionais*, Dissertação de Mestrado, UFRJ, Rio de Janeiro, 1997.

[14] VOLOCH, J. F., *Códigos Corretores de Erros*, 16º Colóquio Brasileiro de Matemática, Rio de Janeiro, IMPA, 1987.