UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

MAURO RODRIGUES ROCHA JÚNIOR

Códigos diedrais e seus pesos

Campinas

2024

Mauro Rodrigues Rocha Júnior

Códigos diedrais e seus pesos

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática.

Orientador: Marcelo Firer

Coorientador: Fabio Enrique Brochero Martínez
Coorientadora: Beatriz Casulari da Motta Ribeiro

Este trabalho corresponde à versão final da Tese defendida pelo aluno Mauro Rodrigues Rocha Júnior e orientada pelo Prof. Dr. Marcelo Firer.

Campinas

2024

Ficha catalográfica
Universidade Estadual de Campinas (UNICAMP)
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

R582c

Rocha Júnior, Mauro Rodrigues, 1993-
Códigos diedrais e seus pesos / Mauro Rodrigues Rocha Júnior. – Campinas, SP : [s.n.], 2024.

Orientador: Marcelo Firer.
Coorientadores: Fabio Enrique Brochero Martínez e Beatriz Casulari da Motta Ribeiro.
Tese (doutorado) – Universidade Estadual de Campinas (UNICAMP), Instituto de Matemática, Estatística e Computação Científica.

1. Código diedral. 2. Traço (Álgebra linear). 3. Corpos finitos (Álgebra). I. Firer, Marcelo, 1961-. II. Brochero Martínez, Fabio Enrique. III. Ribeiro, Beatriz Casulari da Motta,1984-. IV. Universidade Estadual de Campinas (UNICAMP). Instituto de Matemática, Estatística e Computação Científica. V. Título.

Informações Complementares

Título em outro idioma: Dihedral codes and their weights
Palavras-chave em inglês:
Dihedral code
Trace (Linear algebra)
Finite fields (Algebra)
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Marcelo Firer [Orientador]
Saeed Tafazolian
Guilherme Chaud Tizziotti
Francisco Cesar Polcino Milies
Cícero Fernandes de Carvalho
Data de defesa: 29-04-2024
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0009-0009-9816-1382
- Currículo Lattes do autor: https://lattes.cnpq.br/4390983329407591

Tese de Doutorado defendida em 29 de abril de 2024 e aprovada

pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). MARCELO FIRER

Prof(a). Dr(a). SAEED TAFAZOLIAN

Prof(a). Dr(a). GUILHERME CHAUD TIZZIOTTI

Prof(a). Dr(a). FRANCISCO CESAR POLCINO MILIES

Prof(a). Dr(a). CÍCERO FERNANDES DE CARVALHO

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

Após uma longa caminhada, contando com o apoio de indivíduos extraordinários, alcancei esta grande conquista. Durante esse percurso, enfrentei desafios e momentos desafiadores; no entanto, graças ao suporte inabalável dessas pessoas, consegui superar e concluir meu objetivo. Numerosas pessoas me auxiliaram ao longo do caminho, no entanto, citarei apenas algumas delas.

Agradeço ao Professor Fábio Brochero, que foi uma das pessoas mais marcantes nesta jornada, pelo conhecimento que me transmitiu e pela paciência e disponibilidade que demonstrou comigo ao longo de todo o percurso. Para mim, você foi um verdadeiro mentor. Com ele tive a oportunidade de crescer profissionalmente e me aprofundar no universo dos códigos.

Agradeço profundamente aos meus familiares, com gratidão especial voltada para minha tia Marinede e meu tio Ismael. Eles foram fundamentais nos momentos difíceis, sempre me apoiando. Sou verdadeiramente privilegiado por contar com parentes tão dedicados e solidários em minha jornada.

Agradeço ao meu formal orientador nesta tese, Marcelo Firer, expresso minha profunda gratidão. Sempre disponível e atencioso, aceitou guiar-me em um período desafiador. Sua excelência na condução de seus trabalhos é verdadeiramente inspiradora.

Agradeço a minha orientadora de mestrado Beatriz Casulari, que me apresentou os códigos corretores de erros no mestrado e que sempre esteve a disposição pra me ajudar em todos os momentos que precisei.

Ao longo desta jornada, construí amizades valiosas que foram essenciais para mim. Em particular, Douglas e Ronaldo que foram de imensa ajuda e importância.

Agradeço ao pessoal da república onde morei e ao meu amigo Tiago, pelos momentos compartilhados e pela paciência que tiveram comigo. A minha namorada Ana Paula, pela sua compreensão e por sempre estar ao meu lado quando precisei.

Finalmente, agradeço à minha família pelo apoio e amor incondicionais. Em especial, à minha mãe, Joana, e ao meu pai, Mauro, que são pessoas à frente de seu tempo; sem eles, não teria chegado até aqui. Dedico-lhes esta conquista. Sou profundamente grato por tudo que fizeram por mim. Amo vocês e serei eternamente grato por tudo.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

Neste trabalho, abordamos as principais propriedades de códigos diedrais sobre corpos finitos. O principal objetivo é apresentar um forma diferente de construção de códigos diedrais e mostrar alguns resultados, principalmente os resultados relacionados ao peso das palavras. Fizemos uma construção de códigos diedrais sobre corpos finitos utilizando traço, baseada em códigos cíclicos e a partir dos resultados do cálculo de peso de códigos cíclicos irredutíveis, fizemos uma adaptação para códigos diedrais.

Palavras-chave: Código diedral. Traço. Peso. Corpos finitos.

Abstract

In this work, we address the main properties of dieral codes over finite fields. The main objective is to present a different way of constructing dieral codes and to show some results, mainly the results related to the weight of the words. We made a construction of diedral codes over finite fields using trace, based on cyclic codes and from the results of the calculated weight of irreducible cyclic codes, making an adaptation for diedral codes.

Keywords: Diedral codes. trace. Weight. finite fields.

Sumário

Introdução

A teoria dos códigos corretores de erros teve início na década de 40 do século XX. De lá pra cá ela vem sendo bastante estudada e desenvolvida, fazendo com que esteja presente no nosso dia a dia, como por exemplo na transmissão de dados por meios eletromagnéticos como é feita a comunicação em internet, assim como o armazenamento de dados em HDs, SSDs etc. Dentro da teoria de códigos corretores de erros, os mais importantes são os códigos lineares, pelo uso da estrutura algébrica dos mesmos para determinar se uma palavra pertence ao código ou não. Dentre estes, os códigos cíclicos são um tipo interessante de código, pois determinar se um certo elemento faz parte do código é computacionalmente mais fácil do que para códigos lineares em geral. Este tipo de código é amplamente usado em sistemas onde a quantidade de erros é pequena, mas é importante determinar de forma rápida qual seria a correção do erro, como acontece por exemplo na leitura de CDs e DVDs.

Um dos códigos cíclicos mais famosos é o código de Golay que foi usado nas missãos Mariner Jupiter-Saturn dos anos 1979, 1980 e 1981. Este código corrigia três erros, e foi usado para a transmissão de milhares de fotos destes planetas, transmitindo três fotos em branco e preto (0 ou 1 por pixel), que representavam a intensidade de luz nas cores vermelho, verde a azul (consultar https://blogs.ams.org/visualinsight/2015/12/01/golay-code/ para mais informações).

No código de Golay é usado para cada pixel, um vetor de 0's e 1's que tem uma estrutura natural de espaço vetorial sobre o corpo com dois elementos $\mathbb{F}_2$. Para estes mesmos vetores é possível adicionar uma estrutura de corpos finitos que será uma extensão do corpo $\mathbb{F}_2$.

Em geral, dado um corpo finito $\mathbb{F}_q$, e um código cíclico de comprimento n, existe uma extensão $\mathbb{F}_{q^s}$ do corpo $\mathbb{F}_q$ e uma transformação linear $\mathbb{F}_{q^s} \to \mathbb{F}_q^n$, que é definida coordenada a coordenada, a partir da função traço da extensão e que tem como imagem um subespaço vetorial que é exatamente o código dado, como veremos na Seção 1.3 do Capítulo 1. Baseados nessas mesmas ideias, nesta tese pretendemos desenvolver uma teoria equivalente para os códigos diedrais, que são essencialmente ideais a esquerda (ou à direita) de uma álgebra finita sobre um grupo diedral. Os códigos diedrais são objetos bastante estudados nos últimos anos, porém o cálculo da distribuição de pesos é algo pouco desenvolvido.

No primeiro capítulo, fundamentado nas referências [4, 10, 14], desenvolveremos uma introdução de conceitos básicos sobre corpos finitos e códigos lineares, além de teoria de caracteres e somas de Gauss, cujas referências fundamentais foram [1, 11]. Estas

ferramentas serão necessárias para estimar e/ou calcular a distribuição de pesos dos códigos que serão estudados nesta tese.

No segundo capítulo, baseando-se nas referências [2, 13], iniciamos o estudo de códigos diedrais. Em seguida, conforme as referências [8, 3], apresentamos a decomposição de Wedderburn da álgebra de grupos diedral $\mathbb{F}_q D_{2n}$, onde $(q, 2n) = 1$, e por último, usando extensões de corpos, faremos uma construção de alguns códigos diedrais baseando-se na teoria de códigos cíclicos irredutíveis.

O Capítulo 3, seguindo as referências [1, 5, 6], será apresentada uma construção de códigos cíclicos irredutíveis, usando a função traço da extensão. Em seguida aproveitamos essa ideia para o cálculo do peso de algumas palavras de um código diedral. Nessa construção temos dois tipos de código diedrais. Os códigos diedrais não autorrecíprocos, podem ser vistos visto como o produto cartesiano de dois códigos cíclicos. Desta forma os resultados para os códigos diedrais não autorrecíprocos seguem naturalmente da teoria de códigos cíclicos. Por outra lado, os códigos diedrais autorrecíprocos possuem uma forma mais particular, que é uma concatenação de códigos cíclicos com propriedade adicional entre eles.

Neste sentido, os códigos autorrecíprocos são mais interessantes, pois não podem ser obtidos a partir do produto direto de códigos cíclicos, por isso possui suas particularidades.

Dando continuidade a teoria de códigos diedrais autorrecíprocos, no Teorema 3.2.3, apresentamos uma fórmula geral para o peso de cada palavra. Essa fórmula depende de somas de Gauss de carateres adequados, mas como tais somas são difíceis de ser calculada em geral, e quando é fácil não tem muito interesse, então desenvolvemos alguns outros teoremas, nos quais conseguimos calcular de maneira plausível, para alguns casos particulares.

Inicialmente, no Corolário 3.2.4, apresentamos uma cota inferior para a distância mínima destes códigos. Com base em novos lemas e condições especiais, obtivemos o Teorema 3.2.9, que fornece o peso de cada palavra do código, com o calculo exato destas somas de Gauss.

Um outro resultado apresentado nesta tese, é o Teorema 3.2.13, que se aplica a uma subclasse de códigos não abrangida pelo resultado anterior e nos fornece uma fórmula mais simples de calcular para esta subclasse. O Corolário associado a esse teorema assegura que, para uma família de códigos específica sobre um corpo $\mathbb{F}_q$ de dimensão $2q$ e q um quadrado, toda palavra não nula do código terá peso $\frac{2(q^2-1)}{s}$ ou $\frac{2(q-1)^2}{s}$, em que s é um valor previamente determinado. Ao longo dessa teoria desenvolvemos também alguns resultados que nos fornece a distribuição de peso em alguns códigos.

1 Preliminares algébricas

1.1 Corpos finitos

Iniciamos este capítulo introduzindo algumas propriedades de corpos finitos, que serão de suma importância nos próximos capítulos. Ao longo deste texto, $\mathbb{F}_q$ denotará um corpo finito com q elementos.

Definição 1.1.1. *Dado corpo finito $\mathbb{K}$, definimos a caraterística de $\mathbb{K}$ como o menor inteiro positivo c tal que $c \cdot 1 = 0$. Denotamos a característica por $\mathbb{C}har(\mathbb{K})$.*

É fácil verificar que a caraterística de qualquer corpo finito sempre é um número primo. Em geral temos o seguinte resultado.

Proposição 1.1.2 (Theorem 2.2 [11])**.** *Para todo corpo finito $\mathbb{F}_q$ com q elementos, se cumprem as seguintes propriedades:*

1. *$\mathbb{Z}_p \subseteq \mathbb{F}_q$, onde p é a caraterística de $\mathbb{F}_q$.*
2. *Existe $r \geqslant 1$, tal que $q = p^r$.*

Observemos que os elementos não nulos de qualquer corpo sempre forma um grupo com o produto. No caso em que é considerado um corpo finito, se tem um resultado mais específico, como mostrado no seguinte resultado.

Teorema 1.1.3 (Theorem 2.8 [11])**.** *$\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ é um grupo cíclico.*

Definição 1.1.4. *Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de elemento primitivo de $\mathbb{F}_q$.*

Em geral para todo grupo cíclico com n elementos, se γ é um gerador, então γ^i também será um gerador se, e somente se, $(i, n) = 1$. Pelo comentário anterior, como $\mathbb{F}_q^*$ possui $q-1$ elementos, o número de elementos primitivos do corpo $\mathbb{F}_q$ é $\varphi(q-1)$, onde φ é a função de Euler. Além disso, $a^{q-1} = 1$ para todo $a \in \mathbb{F}_q^*$ e desta forma temos o seguinte resultado.

Proposição 1.1.5 (Lemma 2.3. [11])**.** *Seja $\mathbb{F}$ um corpo finito com q elementos e $\overline{\mathbb{F}}$ se fecho algébrico. Um elemento de α de $\overline{\mathbb{F}}$ pertence a $\mathbb{F}$ se, e somente se, $\alpha^q = \alpha$.*

Lema 1.1.6 (Lemma 2.4. [11])**.** *O polinômio $x^q - x \in \mathbb{F}_p[x]$ se decompõe em $\mathbb{F}_q[x]$ como*

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$$

desta forma $\mathbb{F}_q$ é o corpo de decomposição de $x^q - x$.

A partir do lema anterior, segue-se que existe um único corpo com q elementos.

Teorema 1.1.7 (Teorema 4 [10]). *Dois corpos finitos com o mesmo número de elementos são isomorfos.*

Sempre que utilizamos $\mathbb{F}_q$ fica subentendido que representa o único corpo com $q = p^r$ elementos e caraterística p.

Proposição 1.1.8 (Proposição 4 [10]). *Seja $\mathbb{F}_q$ um corpo finito de característica p. Se $a, b \in \mathbb{F}_q$, então*

$$(a \pm b)^p = a^p \pm b^p.$$

Até o momento, fica subtendido que corpos com q elementos podem funcionar como corpos de decomposição para polinômios específicos. Uma pergunta natural é como construir de forma explícita tais corpos. Para isso consideremos um polinômio $f(x) \in \mathbb{F}_q[x]$ de grau m, que seja irredutível nesse domínio. Desta forma $\langle f(x) \rangle$ é um ideal maximal neste domínio e portanto o anel quociente $\dfrac{\mathbb{F}_q[x]}{\langle f(x) \rangle}$ é de fato um corpo. Como cada classe de equivalência possui um único representante que tem grau menor que m, temos que o número de representantes é q^m, e, assim, este corpo possui q^m elementos. Reciprocamente temos.

Teorema 1.1.9 (Teorema 2 [10]). *Para cada número natural m, existe pelo menos um polinômio irredutível de grau m em $\mathbb{F}_q[x]$.*

Corolário 1.1.10. *Existe $f(x) \in \mathbb{F}_q[x]$ irredutível tal que*

$$\mathbb{F}_{q^m} \simeq \frac{\mathbb{F}_q[x]}{\langle f(x) \rangle}$$

em que

$$\frac{\mathbb{F}_p[x]}{\langle f(x) \rangle} = \{a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \mid a_i \in \mathbb{F}_q\}.$$

Em particular como toda raiz de $f(x)$ está em $\mathbb{F}_{q^m}$, temos que $f(x)$ divide $x^{q^m} - x$. Em geral, se tem os seguintes resultados.

Lema 1.1.11 (Lemma 2.13. [11]). *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau m, então*

$$f(x) \mid (x^{q^s} - x) \text{ se, e somente se, } m \mid s.$$

1.1.1 Anéis de polinômios

Nesta seção apresentaremos alguns resultados da teoria de anéis de polinômios que serão utilizados nos próximos capítulos.

Proposição 1.1.12 (Proposição 1 [10]). *Todo ideal de $\mathbb{F}_q[x]$ é principal, isto é, para todo ideal I de $\mathbb{F}_q[x]$, existe um único polinômio f em I, de grau mínimo, tal que $I = \langle f \rangle$.*

De fato, para qualquer corpo $\mathbb{K}$, o anel de polinômios $\mathbb{K}[x]$ é um domínio euclidiano, com a divisão de polinômios e portanto também é um domínio de ideais principais. Desta forma, para todo ideal $I \subset \mathbb{K}[x]$ se define o anel quociente $\dfrac{\mathbb{K}[x]}{I}$, que, dependendo da escolha de I, é possível encontrar algumas estruturas que serão importantes nesse trabalho. Especificamente, apresentamos a seguinte definição.

Definição 1.1.13. *Definimos R_n como sendo o anel das classes residuais em $\mathbb{F}_q[x]$ módulo $x^n - 1$, ou seja,*

$$R_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}.$$

Assim se $f(x) \in \mathbb{F}_q[x]$, denotaremos sua classe por $\overline{f(x)}$, onde

$$\overline{f(x)} = \{f(x) + g(x)(x^n - 1) \mid g(x) \in \mathbb{F}_q[x]\}.$$

Observemos que R_n é um espaço vetorial de dimensão n sobre $\mathbb{F}_q$ com base $\overline{1}, \overline{x}, \overline{x^2}, ..., \overline{x^{n-1}}$.

Como veremos em uma próxima seção, uma forma natural de representar códigos cíclicos de comprimento n, é ver eles como ideais do anel R_n. Estes ideais são caraterizados na seguinte proposição.

Proposição 1.1.14 (Proposição 2 [10]). *Todo ideal de R_n é da forma $\langle \overline{g} \rangle$, onde g é um divisor de $x^n - 1$.*

1.1.2 Fatoração e polinômios ciclotômicos

Esta seção tem como propósito estudar os corpos de decomposição do polinômio $x^n - 1 \in \mathbb{F}_q[x]$ e obter informações sobre a estrutura do conjunto das raízes da unidade. O objetivo é apresentar resultados sobre corpos finitos que é um dos principais instrumentos desse trabalho. Ao longo dessa seção $\mathbb{K}$ e $\mathbb{F}$ serão corpos finitos. Para todo polínomio não nulo $f(x) \in \mathbb{F}[x]$, definimos o corpo de decomposição de f como o mínimo corpo que contém $\mathbb{F}$ e as raizes de $f(x)$.

Definição 1.1.15. *Seja n um inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre o corpo $\mathbb{K}$ é chamado o n-ésimo corpo ciclotômico sobre $\mathbb{K}$ e denotamos por $\mathbb{K}^{(n)}$. Uma raiz de $x^n - 1$ em $\mathbb{K}^{(n)}$ é chamada de n-ésima raiz da unidade sobre $\mathbb{K}$ e o conjunto de todas as raízes é denotado por $\mathbb{E}^{(n)}$.*

Observemos que se tomássemos o corpo $\mathbb{Q}$, o número de raízes n-ésimas da unidade que estão no fecho de $\mathbb{Q}$ é n e logo $\#\mathbb{E}^{(n)} = n$, mas isso não necessariamente é verdade para um corpo finito. Por exemplo, se

$$\mathbb{K} = \mathbb{F}_p, \text{ então } \#\mathbb{E}^{(p^j)} = 1 \quad \text{para todo } j \in \mathbb{N}.$$

Teorema 1.1.16 (Theorem 2.42 [11])**.** *Sejam n um inteiro positivo e $\mathbb{K}$ um corpo de característica p. Então:*

1. *Se p não divide n, então $\mathbb{E}^{(n)}$ é um grupo cíclico de ordem n com respeito a multiplicação em $\mathbb{K}^{(n)}$.*
2. *Se p divide n, i.e., $n = mp^l$ com m e l inteiros positivos e $p \nmid m$. Então $\mathbb{K}^{(n)} = \mathbb{K}^{(m)}$, $\mathbb{E}^{(n)} = \mathbb{E}^{(m)}$, e as raízes de $x^n - 1$ em $\mathbb{K}^{(n)}$ são os m elementos de $\mathbb{E}^{(m)}$.*

Definição 1.1.17. *Sejam $\mathbb{K}$ um corpo de característica p e n um inteiro positivo não divisível por p. Então um gerador do grupo cíclico $\mathbb{E}^{(n)}$ é chamado de raiz n-ésima primitiva da unidade.*

Definição 1.1.18. *Sejam $\mathbb{K}$ um corpo de característica p, n um inteiro positivo não divisível por p e ξ uma raiz n-ésima da unidade sobre $\mathbb{K}$. Então o polinômio*

$$Q_n(x) = \prod_{\substack{s=1 \\ mdc(s,n)=1}}^{n} (x - \xi^s)$$

é chamado de n-ésimo polinômio ciclotômico sobre $\mathbb{K}$.

Teorema 1.1.19 (Theorem 2.45 [11])**.** *Sejam $\mathbb{K}$ um corpo de característica p e n um inteiro não divisível por p. Então*

1. $x^n - 1 = \prod_{d|n} Q_d(x)$;
2. $Q_n(x) \in \mathbb{F}_p[x]$.

É conhecido que os polinômios ciclotômicos são irredutíveis quando consideramos eles no anel $\mathbb{Q}[x]$. Já quando eles são considerados sobre corpos finitos, eles em geral são redutíveis. Para verificar qual é a relação entre as raízes de um polinômio irredutível sobre $\mathbb{F}_q$, precisamos da seguinte definição.

Definição 1.1.20. *Sejam $\mathbb{F}_{q^m}$ uma extensão do corpo $\mathbb{F}_q$ e $\alpha \in \mathbb{F}_{q^m}$. Os elementos $\alpha, \alpha^q, ..., \alpha^{q^{m-1}}$ são chamados conjugados de α com respeito a $\mathbb{F}_q$.*

Desta forma, o seguinte teorema caracteriza a estrutura das raízes de um polinômio irredutível.

Teorema 1.1.21 (Theorem 2.14 e Corollary 2.15 [11]). *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio mônico irredutível com $\deg(f) = m$. Se α é uma raiz de $f(x)$, então $\alpha \in \mathbb{F}_{q^m}$ e todas as raízes de $f(x)$ são $\alpha, \alpha^q, ..., \alpha^{q^{m-1}}$. Além disso estas raízes são distintas. Em particular $\mathbb{F}_{q^m}$ é o corpo de decomposição de $f(x)$.*

Usando o resultado anterior, podemos determinar o número de fatores e o grau de cada um dos divisores irredutíveis do polinômio ciclotômico $Q_n(x)$.

Teorema 1.1.22 (Theorem 2.47 [11]). *Sejam $n \geqslant 1$ e $\mathrm{mdc}(n, q) = 1$, então $Q_n(x)$ se fatora em $\dfrac{\varphi(n)}{d}$ fatores irredutíveis de grau d sobre $\mathbb{F}_q[x]$, onde φ é a função de Euler e d é a ordem de q em $\mathbb{Z}_n^*$, ou seja, d é o menor inteiro positivo tal que $q^d \equiv 1 \ (mod\ n)$.*

1.1.3 Traço de uma extensão de corpos

Uma ferramenta que será amplamente utilizada ao longo deste trabalho é a função traço, que possui a seguinte definição.

Definição 1.1.23. *A função traço $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ é definida como*

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}$$

para todo $\alpha \in \mathbb{F}_{q^m}$. Se $\mathbb{F}_q$ é o subcorpo primo de $\mathbb{F}_{q^m}$, então o $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ é chamada função traço absoluto. No que segue deste texto, por simplicidade, usaremos a notação $Tr_{m,1}$ para representar o traço $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}$.

Observemos que o traço de α é a soma de α com seus conjugados na extensão $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$. O teorema a seguir revela algumas propriedades da função traço, em especial, demonstra que esta função é $\mathbb{F}_q$-linear.

Teorema 1.1.24 (Theorem 2.23 [11]). *A função traço $Tr_{m,1}$ satisfaz as seguintes propriedades*

1. *$Tr_{m,1}(\alpha + \beta) = Tr_{m,1}(\alpha) + Tr_{m,1}(\beta)$ para todo $\alpha, \beta \in \mathbb{F}_{q^m}$.*
2. *$Tr_{m,1}(c\alpha) = cTr_{m,1}(\alpha)$ para todo $c \in \mathbb{F}_q$ e $\alpha \in \mathbb{F}_{q^m}$.*
3. *$Tr_{m,1}$ é um transformação linear de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, onde $\mathbb{F}_{q^m}$ e $\mathbb{F}_q$ são vistos como espaços vetoriais sobre $\mathbb{F}_q$.*
4. *$Tr_{m,1}(a) = ma$ para todo $a \in \mathbb{F}_q$.*
5. *$Tr_{m,1}(\alpha^q) = Tr_{m,1}(\alpha)$ para todo $\alpha \in \mathbb{F}_{q^m}$.*

Como foi dito anteriormente $Tr_{m,1}$ é uma função $\mathbb{F}_q$-linear, mas o interessante é que toda função $\mathbb{F}_{q^m} \to \mathbb{F}_q$ que seja $\mathbb{F}_q$-linear está relacionada com a função traço, como mostra o seguinte teorema.

Teorema 1.1.25 (Theorem 2.24 [11]). *Seja $\mathbb{F}_{q^m}$ uma extensão finita de $\mathbb{F}_q$. Considerando $\mathbb{F}_{q^m}$ como $\mathbb{F}_q$-espaço vetorial, então para todo $\beta \in \mathbb{F}_{q^m}$ a transformação $L_\beta : \mathbb{F}_{q^m} \to \mathbb{F}_q$ definida por $L_\beta(\alpha) = Tr_{m,1}(\beta\alpha)$ para todo $\alpha \in \mathbb{F}_{q^m}$ é uma transformação linear de $\mathbb{F}_{q^m} \to \mathbb{F}_q$. Reciprocamente se $L : \mathbb{F}_{q^m} \to \mathbb{F}_q$ é uma transformação $\mathbb{F}_q$-linear, então existe um único $\beta \in \mathbb{F}_{q^m}$ tal que $L = L_\beta$.*

Finalmente é natural perguntar como determinar o núcleo da função traço. Este é um resultado muito importante e que se aplica a outro tipo de extensões, conhecido como Teorema 90 de Hilbert.

Teorema 1.1.26 (Theorem 2.25 [11]). *Seja $\mathbb{F}_{q^m}$ uma extensão finita de $\mathbb{F}_q$. Então para $\alpha \in \mathbb{F}_{q^m}$ temos $Tr_{m,1}(\alpha) = 0$, se, e somente se, $\alpha = \beta^q - \beta$ para algum $\beta \in \mathbb{F}_{q^m}$.*

Teorema 1.1.27 (Theorem 2.26 [11]). *Seja $\mathbb{F}_{q^n}$ uma extensão finita de $\mathbb{F}_q$ e $\mathbb{F}_{q^{mn}}$ uma extensão finita de $\mathbb{F}_{q^n}$. Então*

$$Tr_{\mathbb{F}_{q^{mn}}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^{mn}}/\mathbb{F}_{q^n}}(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)) \text{ para todo } \alpha \in \mathbb{F}_{q^{mn}}.$$

1.2 Caracteres e Soma de Gauss

Nesta seção vamos enunciar e demonstrar alguns resultados importantes sobre caracteres e soma de Gauss, que serão de grande importância para o desenvolvimento do nosso trabalho. Para uma leitura mais aprofundada desse assunto ver sugerimos a referência [1].

1.2.1 Caracteres

Seja G um grupo abeliano finito de ordem $|G|$ com elemento neutro denotado por 1(ou 1_G).

Definição 1.2.1. *Um caracter χ de G é um homomorfismo de G sobre o grupo multiplicativo dos números complexos com módulo 1, ou seja, $\chi : G \to S^1$, onde $S^1 = \{z \in \mathbb{C}; |z| = 1\}$.*

Dado que χ é um homomorfismo, então $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ para todo $g_1, g_2 \in G$. Observemos que $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$, então $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$ para cada $g \in G$, em que a barra denota a conjugação complexa. Cada caracter χ de G está associado ao caracter conjugado $\overline{\chi}$ definido por $\overline{\chi}(g) = \overline{\chi(g)}$ para todo $g \in G$. Como $\chi(1_G) = \chi(1_G \cdot 1_G) = \chi(1_G)\chi(1_G)$, então $\chi(1_G) = 1$. O produto de dois caracteres $\chi_1\chi_2$ é

definido por $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$ para todo $g \in G$. Com esse produto, o conjunto dos caracteres de G forma um grupo abeliano multiplicativo. Esse grupo é chamado de dual de G e será denotado por $\hat{G}$, ou seja,

$$\hat{G} = \{\chi : G \to S^1 \mid \chi \text{ é um homomorfismo}\}$$

com o elemento neutro sendo o caracter trivial χ_0, i. e., $\chi_0(g) = 1$ para todo $g \in G$.

Lema 1.2.2. *Seja G um grupo cíclico de ordem n, então $\hat{G}$ é também um grupo cíclico de ordem n.*

Demonstração. Seja g um gerador de G e portanto a ordem de g é n. Para um inteiro fixado j, $0 \leqslant j \leqslant n-1$, a função

$$\chi_j(g^k) = e^{\frac{2\pi ijk}{n}}, k = 0, 1, ..., n-1$$

define um caracter de G e além disso os elementos do conjunto $\mathcal{C} = \{\chi_j \mid j \in \{0, \dots n-1\}\}$ formam um subgrupo de $\hat{G}$ de ordem n.

Desta forma precisamos mostrar que todo elemento de $\hat{G}$ está em $\mathcal{C}$. Para isso observemos que se $\chi \in \hat{G}$, então

$$1 = \chi(g^n) = \chi(g)^n,$$

portanto $\chi(g)$ é uma raiz n-ésima da unidade e desta forma $\chi(g) = e^{\frac{2\pi ij}{n}}$ para algum j. Segue de forma direta que $\chi = \chi_j$, como queríamos demonstrar. □

Teorema 1.2.3 (Theorem 5.2 [11])**.** *Sejam H um subgrupo do grupo abeliano finito G e ψ um caracter de H. Então ψ pode ser estendido para um caracter de G; isto é, existe um caracter χ de G com $\chi(h) = \psi(h)$ para todo $h \in H$.*

Demonstração. Suponhamos que H seja um subgrupo próprio de G. Escolhemos $a \in G$ com $a \notin H$ e seja H_1 um subgrupo de G gerado por H e a. Seja m o menor inteiro positivo para o qual $a^m \in H$. Então cada elemento $g \in H_1$ pode ser escrito unicamente na forma $g = a^j h$ com $0 \leqslant j < m$ e $h \in H$. Definimos a função ψ_1 em H_1 por $\psi_1(g) = \omega^j \psi(h)$, onde ω é um número complexo fixo satisfazendo $\omega^m = \psi(a^m)$. Para verificar que ψ_1 é na verdade um caracter de H_1, seja $g_1 = a^k h_1$, $0 \leqslant k < m$, $h_1 \in H$ é outro elemento de H_1. Se $j + k < m$, então $\psi_1(gg_1) = \omega^{j+k}\psi(hh_1) = \psi_1(g)\psi_1(g_1)$. Se $j + k \geqslant m$, então $gg_1 = a^{j+k-m}(a^m hh_1)$, e também

$$\psi_1(gg_1) = \omega^{j+k-m}\psi(a^m hh_1) = \omega^{j+k-m}\psi(a^m)\psi(hh_1) = \omega^{j+k}\psi(hh_1) = \psi_1(g)\psi_1(g_1)$$

e $\psi_1(h) = \psi(h)$ para $h \in H$. Se $H_1 = G$, então segue o resultado. Caso contrário, podemos continuar o processo acima um número finito de vezes, obtendo uma extensão de ψ para G.

□

Corolário 1.2.4 (Corollary 5.3 [11]). *Para quaisquer dois elementos distintos $g_1, g_2 \in G$ existe um caracter $\chi \in G$ tal que $\chi(g_1) \neq \chi(g_2)$.*

Demonstração. Tomando $h = g_1 g_2^{-1}$, é suficiente mostrar que existe um caracter χ de G, com $\chi(h) \neq 1$, pois se $\chi(g_1) \neq \chi(g_2)$, então $\chi(g_1)\chi(g_2^{-1}) \neq \chi(g_2)\chi(g_2^{-1}) = 1$. Consideremos o grupo cíclico $H = \langle h \rangle$, sendo n_1 a ordem de H, definindo o caracter χ em H da seguinte forma $\chi(h^k) = e^{\frac{2\pi i k}{n_1}}$ para todo $k \in \mathbb{N}$, com $\chi(h) = e^{\frac{2\pi i}{n_1}} \neq 1$ e pelo Teorema 1.2.3 podemos estender χ para G, como queríamos demonstrar. □

As seguintes relações são conhecidas como relações de ortogonalidade.

Teorema 1.2.5 (Theorem 5.4 [11]). *Se χ é um caracter não trivial do grupo abeliano finito G, então*

$$\sum_{g \in G} \chi(g) = 0. \tag{1.1}$$

Se $g \in G$ com $g \neq 1_G$, então

$$\sum_{\chi \in \hat{G}} \chi(g) = 0. \tag{1.2}$$

Demonstração. Seja χ um caracter não trivial, então existe $h \in G$ com $\chi(h) \neq 1$. Assim

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg),$$

como g percorre todo grupo G, então gh também percorrerá todo o grupo G, desta forma temos que

$$\sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g).$$

Logo,

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0.$$

Já que $\chi(h) \neq 1$, isso implica que $\sum_{g \in G} \chi(g) = 0$, como queríamos mostrar. Agora, seja $g \in G$ com $g \neq 1_G$ e considere a função $\hat{g} : \hat{G} \to \mathbb{C}$ com $\hat{g}(\chi) = \chi(g)$. Então $\hat{g}$ é um caracter não trivial de $\hat{G}$. Mas pelo Corolário 1.2.4, existe $\chi \in \hat{G}$ com $\chi(g) \neq \chi(1_G) = 1$. Assim segue de (1.1) que

$$\sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} \hat{g}(\chi) = 0.$$

□

O seguinte resultado é conhecido como o Teorema Fundamental dos Grupos Abelianos Finitos.

Teorema 1.2.6 (Teorema V.8.1 [9]). *Todo grupo abeliano finito é isomorfo ao produto direto de grupos cíclicos.*

O resultado anterior será útil na prova do seguinte resultado que carateriza o dual de todo grupo abeliano finito.

Teorema 1.2.7. *Seja G um grupo abeliano finito, então $\hat{G} \simeq G$.*

Demonstração. Pelo Teorema 1.2.6, existem $G_1, \ldots, G_r$ grupos cíclicos tais que $G \simeq G_1 \times \cdots \times G_r$. Seja $e_j = (0, \ldots, 0, \hat{e}_j, 0, \ldots, 0)$, onde $G_j = \langle \hat{e}_j \rangle$ para $1 \leqslant j \leqslant r$. Definimos

$$\chi_j(e_j) = \begin{cases} 1, \text{ se } i \neq j; \\ \xi_{n_j}, \text{ se } i = j, \end{cases}$$

com $n_j = |G_j|$, assim χ_j é um caracter bem definido em $\hat{G}$. Todo elemento $\chi \in \langle \chi_1, \ldots, \chi_r \rangle$ pode ser escrito como $\chi = \chi_1^{\varepsilon_1} \cdot \chi_2^{\varepsilon_2} \cdot \ldots \cdot \chi_r^{\varepsilon_r}$, com os expoentes ϵ_j adequados e além disso, calculando χ nos geradores do e_j obtemos que $\chi(e_j) = \chi_j(e_j)^{\varepsilon_j} = \xi_{n_j}^{\varepsilon_j}$. Desta forma se $\xi_{n_j}^{\varepsilon_j} = 1$ isso implica que $n_j | \varepsilon_j$, segue que a ordem de χ_j é n_j. Portanto $| \langle \chi_1, \ldots, \chi_r \rangle | = n_1 \cdot \ldots \cdot n_r = | G |$.

Agora precisamos mostrar que $\hat{G} \subseteq \langle \chi_1 \cdot \ldots \cdot \chi_r \rangle$. Seja $\chi \in \hat{G}$ e $g \in G$, então $g = \hat{e}_1^{u_1}, \ldots, \hat{e}_r^{u_r}$ com $0 \leqslant u_j \leqslant n_j$ e

$$\begin{aligned} \chi(g) &= \chi(\hat{e}_1^{u_1}) \cdot \ldots \cdot \chi(\hat{e}_r^{u_r}) \\ &= \chi(\hat{e}_1)^{u_1} \cdot \ldots \cdot \chi(\hat{e}_r)^{u_r} \\ &= \chi_1(\hat{e}_1)^{u_1 \varepsilon_1} \cdot \ldots \cdot \chi_r(\hat{e}_r)^{u_r \varepsilon_r} \\ &= \chi_1^{\varepsilon_1}(\hat{e}_1)^{u_1} \cdot \ldots \cdot \chi_r^{\varepsilon_r}(\hat{e}_r)^{u_r} \end{aligned}$$

assim temos que $\chi = \chi_1^{\varepsilon_1} \cdot \ldots \cdot \chi_r^{\varepsilon_r}$, daí segue que $\chi \in \langle \chi_1, \ldots, \chi_r \rangle$. Portanto, $| G | = | \hat{G} |$, o que implica $G \simeq \hat{G}$.

□

Observemos que o isomorfismo de G a $\hat{G}$ não é natural, ele depende da representação de G como produto direto de grupos cíclicos, e está representação não é única.

Corolário 1.2.8. *Seja G um grupo abeliano que é o produto direto de grupos cíclicos de ordens $n_1, \ldots, n_r$. Então $\hat{G}$ também é o produto direto de grupos cíclicos de ordem $n_1, \ldots, n_r$.*

No que segue vamos considerar as duas estruturas (aditiva e multiplicativa) do corpo $\mathbb{F}_q$. Desta forma, podemos associar a $\mathbb{F}_q$ dois grupos naturais, dados pelas duas operações do corpo. O grupo aditivo formado pelos elementos de $\mathbb{F}_q$ e o grupo multiplicativo formado por $\mathbb{F}_q^*$. Cada um desses grupos geram um grupo de caracteres com diferentes estruturas. Em ambos os casos, os caracteres podem ser apresentados de forma explícita.

Consideremos primeiro o grupo aditivo de $\mathbb{F}_q$. Se p é a característica de $\mathbb{F}_q$, então pela Proposição 1.1.2 sabemos que $\mathbb{F}_q$ contém o subcorpo primo $\mathbb{Z}_p$. Seja $Tr : \mathbb{F}_q \to \mathbb{F}_p$ o traço absoluto de $\mathbb{F}_q$ para $\mathbb{F}_p$, então para cada $b \in \mathbb{F}_q$, a função $\psi_b : \mathbb{F}_q \to \mathbb{C}$, definida por

$$\psi_b(c) = e^{\frac{2\pi i Tr(bc)}{p}} \text{ para todo } c \in \mathbb{F}_q$$

é um caracter do grupo aditivo de $\mathbb{F}_q$, pois dado $c_1, c_2 \in \mathbb{F}_q$ temos que

$$\psi_b(c_1 + c_2) = e^{\frac{2\pi i Tr(b(c_1+c_2))}{p}} = e^{\frac{2\pi i (Tr(bc_1)+Tr(bc_2))}{p}} = e^{\frac{2\pi i Tr(bc_1)}{p}} e^{\frac{2\pi i Tr(bc_2)}{p}} = \psi_b(c_1)\psi_b(c_2).$$

O caracter ψ_1 é chamado de caracter canônico. O próximo teorema nos garante que todos os caracteres aditivos de $\mathbb{F}_q$ podem ser expressos em função de ψ_1.

Teorema 1.2.9 (Theorem 5.7 [11]). *Para todo $b \in \mathbb{F}_q$, a função definida por $\psi_b(c) = \psi_1(bc)$ para todo $c \in \mathbb{F}_q$ é um caracter de $(\mathbb{F}_q, +)$, e cada caracter aditivo de $\mathbb{F}_q$ é obtido dessa forma.*

Demonstração. Para $c_1, c_2 \in \mathbb{F}_q$, temos

$$\psi_b(c_1 + c_2) = \psi_1(bc_1 + bc_2) = \psi(bc_1)\psi(bc_2) = \psi_b(c_1)\psi_b(c_2),$$

provando a primeira parte. Sendo Tr o traço de $\mathbb{F}_q$ para $\mathbb{F}_p$, o caracter ψ_1 é não trivial. Portanto se $a, b \in \mathbb{F}_q$ com $a \neq b$, então

$$\frac{\psi_a(c)}{\psi_b(c)} = \frac{\psi_1(ac)}{\psi_1(bc)} = \psi_1((a-b)c) \neq 1$$

para um $c \in \mathbb{F}_q$ adequado, então ψ_a e ψ_b são caracteres distintos. Assim se b percorre $\mathbb{F}_q$, obtemos q caracteres aditivos distintos ψ_b. Por outro lado, pelo Teorema 1.2.7, $\mathbb{F}_q$ possui exatamente q caracteres aditivos, assim segue o resultado. □

Chamamos o caracter do grupo multiplicativo $\mathbb{F}_q^*$ de $\mathbb{F}_q$ de caracter multiplicativo de $\mathbb{F}_q$.

Teorema 1.2.10 (Theorem 5.8 [11]). *Se g é um elemento primitivo de $\mathbb{F}_q$. Para cada $j = 0, ..., q-2$, a função χ_j definida por $\chi_j(g^k) = e^{\frac{2\pi i j k}{q-1}}$ para $k = 0, ..., q-2$ determina um caracter multiplicativo de $\mathbb{F}_q$ com ordem $\dfrac{q-1}{mdc(q-1, j)}$, e cada caracter multiplicativo de $\mathbb{F}_q$ é obtido dessa forma.*

Demonstração. Segue do Teorema 1.2.7 e da demonstração do Lema 1.2.2. □

Corolário 1.2.11 (Corollary 5.9 [11]). *O grupo de caracteres multiplicativo de $\mathbb{F}_q$ é cíclico de ordem $q-1$. O elemento identidade do grupo de caracteres multiplicativo é chamado de caracter multiplicativo trivial e será denotado por χ_0.*

Demonstração. Pelo Teorema 1.2.10, quando $j = 1$, teremos um caracter de ordem $q - 1$, isso implica que o grupo de caracteres multiplicativo é cíclico. □

É conveniente estender o domínio da definição do caracter χ de $\mathbb{F}_q^*$ para $\mathbb{F}_q$. Para isso consideraremos $\chi_0(0) = 1$ e $\chi(0) = 0$, se χ é um caracter não trivial. Com essa definição temos que:

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = \begin{cases} q, & \text{se } \chi \text{ é trivial;} \\ 0, & \text{se } \chi \text{ não é trivial.} \end{cases} \tag{1.3}$$

1.2.2 Soma de Gauss

Nesta seção introduziremos uma função que relaciona os caracteres aditivo e multiplicativo de um corpo finito, chamada soma de Gauss. Também mostraremos algumas propriedade da soma de Gauss que serão empregadas nas seções subsequentes e que podem ser encontrados em [1]. Em particular, tais resultados estabelecerão um alicerce sólido para o posterior cálculo dos pesos de determinadas palavras-código nas próximas seções. Ao longo dessa seção denotaremos por χ como um caracter multiplicativo e ψ_b como um caracter aditivo.

Definição 1.2.12. *Dado $q = p^r$ e $b \in \mathbb{F}_q$, definimos a soma de Gauss dos caracteres χ e ψ_b, que denotaremos por $G(b, \chi)$, da seguinte forma*

$$G(b, \chi) = \sum_{c \in \mathbb{F}_q} \chi(c)\psi_b(c).$$

Como $G(b, \chi)$ é soma de no máximo q números de módulo 1, então o valor absoluto de $G(b, \chi)$ é no máximo q. Se $b = 1$, denotaremos $G(1, \chi)$ simplesmente como $G(\chi)$. Se χ é o caracter trivial, então

$$G(b, \chi) = \sum_{c \in \mathbb{F}_q} \chi(c)\psi_b(c) = \begin{cases} q, & \text{se } b = 0; \\ 0, & \text{se } b \neq 0. \end{cases}$$

Teorema 1.2.13. *Seja χ um caracter não trivial em $\mathbb{F}_q$ e $b \in \mathbb{F}_q^*$. Então,*

$$G(b, \chi) = \chi(b^{-1})G(\chi),$$

onde b^{-1} denota o inverso de b em $\mathbb{F}_q^*$.

Demonstração.

$$\begin{aligned} G(b,\chi) &= \sum_{\alpha\in\mathbb{F}_q} \chi(\alpha)\psi_b(\alpha) \\ &= \sum_{\alpha\in\mathbb{F}_q} \chi(\alpha)\chi(b)\chi^{-1}(b)\psi_1(\alpha b) \\ &= \chi^{-1}(b)\sum_{\alpha\in\mathbb{F}_q} \chi(\alpha b)\psi_1(\alpha b) \\ &= \chi(b^{-1})\sum_{\gamma\in\mathbb{F}_q} \chi(\gamma)\psi_1(\gamma) \\ &= \chi(b^{-1})G(\chi). \end{aligned}$$

□

O próximo teorema será útil para calcular em alguns casos e estimar em outros, a soma de Gauss.

Teorema 1.2.14. *Seja $b \in \mathbb{F}_q^*$ e χ um caracter não trivial em $\mathbb{F}_q$, então*

1. $G(b,\chi)G(b,\overline{\chi}) = \chi(-1)p^r = \chi(-1)q$,
2. $\overline{G(b,\chi)} = \chi(-1)G(b,\overline{\chi})$,
3. $\mid G(b,\chi) \mid = p^{r/2} = q^{1/2}$,
4. $G(b,\chi^p) = G(b^p,\chi)$.

Demonstração. 1. Pelo Teorema 1.2.13 e a identidade $\chi^{-1}(b) = \chi(b^{-1}) = \overline{\chi}(b)$, temos que

$$\begin{aligned} \sum_{b\in\mathbb{F}_q} G(b,\chi)G(b,\overline{\chi}) &= \sum_{b\in\mathbb{F}_q} \chi(b^{-1})G(\chi)\overline{\chi}(b^{-1})G(\overline{\chi}) \\ &= \sum_{b\in\mathbb{F}_q} \overline{\chi}(b)G(\chi)\chi(b)G(\overline{\chi}) \\ &= G(\chi)G(\overline{\chi})\sum_{b\in\mathbb{F}_q} \overline{\chi}(b)\chi(b) \\ &= G(\chi)G(\overline{\chi})\sum_{b\in\mathbb{F}_q^*} 1, \end{aligned}$$

logo

$$\sum_{b\in\mathbb{F}_q} G(b,\chi)G(b,\overline{\chi}) = (p^r-1)G(\chi)G(\overline{\chi}). \tag{1.4}$$

Por outro lado

$$G(b,\chi)G(b,\overline{\chi}) = \sum_{\gamma\in\mathbb{F}_q} \chi(\gamma)\psi_\gamma(b)\sum_{\delta\in\mathbb{F}_q} \overline{\chi}(\delta)\psi_\delta(b) = \sum_{\gamma,\delta\in\mathbb{F}_q} \chi(\gamma)\overline{\chi}(\delta)\psi_{\gamma+\delta}(b).$$

Somando sobre $b \in \mathbb{F}_q$, e usando as relações em (1.3), temos que

$$\begin{aligned}\sum_{b\in\mathbb{F}_q} G(b,\chi)G(b,\overline{\chi}) &= \sum_{\gamma,\delta\in\mathbb{F}_q} \chi(\gamma)\overline{\chi}(\delta)\sum_{b\in\mathbb{F}_q}\psi_{\gamma+\delta}(b)\\ &= p^r\sum_{\gamma\in\mathbb{F}_q}\chi(\gamma)\overline{\chi}(-\gamma)\\ &= p^r\sum_{\gamma\in\mathbb{F}_q}\chi(\gamma)\overline{\chi}(\gamma)\overline{\chi}(-1)\\ &= p^r\chi(-1)\sum_{\gamma\in\mathbb{F}_q^*}1\\ &= p^r(p^r-1)\chi(-1).\end{aligned}$$

Portanto

$$\sum_{b\in\mathbb{F}_q} G(b,\chi)G(b,\overline{\chi}) = p^r(p^r-1)\chi(-1). \tag{1.5}$$

Comparando (1.4) e (1.5) temos que

$$G(\chi)G(\overline{\chi}) = \chi(-1)p^r.$$

Aplicando o Teorema 1.2.13, obtemos

$$G(b,\chi)G(b,\overline{\chi}) = \chi(b^{-1})\overline{\chi}(b^{-1})G(\chi)G(\overline{\chi}) = \chi(-1)p^r,$$

como queríamos.

2. Observemos que

$$\begin{aligned}\overline{G(b,\chi)} &= \sum_{\alpha\in\mathbb{F}_q}\overline{\chi(\alpha)\psi_b(\alpha)}\\ &= \sum_{\alpha\in\mathbb{F}_q}\overline{\chi}(\alpha)\psi_{-b}(\alpha)\\ &= \sum_{\alpha\in\mathbb{F}_q}\overline{\chi}(\alpha)\psi_b(-\alpha),\ \text{fazendo } c=-\alpha,\ \text{temos}\\ &= \sum_{c\in\mathbb{F}_q}\overline{\chi}(-c)\psi_b(c)\\ &= \overline{\chi}(-1)\sum_{c\in\mathbb{F}_q}\overline{\chi}(c)\psi_b(c)\\ &= \overline{\chi}(-1)G(b,\overline{\chi})\\ &= \chi(-1)G(b,\overline{\chi})\end{aligned}$$

3. Este item segue de (1) e (2), pois

$$|\ G(b,\chi)\ |^2 = G(b,\chi)\overline{G(b,\chi)} = G(b,\chi)\chi(-1)G(b,\overline{\chi}) = \chi^2(-1)p^r = p^r$$

assim

$$|\ G(b,\chi)\ | = p^{r/2}.$$

4. Para provar este item, usaremos que $Tr(\alpha) = Tr(\alpha^p)$ para todo $\alpha \in \mathbb{F}_q$. De fato

$$\begin{aligned} G(b, \chi^p) &= \sum_{\alpha \in \mathbb{F}_q} \chi^p(\alpha)\psi_b(\alpha) \\ &= \sum_{\alpha \in \mathbb{F}_q} \chi^p(\alpha)\psi_1(b\alpha) \\ &= \sum_{\alpha \in \mathbb{F}_q} \chi^p(\alpha)\psi_1(b^p\alpha^p) \\ &= \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha^p)\psi_{b^p}(\alpha^p) \\ &= G(b^p, \chi), \end{aligned}$$

onde na última igualdade é usado o fato que α^p também percorre todo $\mathbb{F}_q$.

□

Calcular o valor da soma de Gauss é uma tarefa difícil na maioria dos casos, porém em alguns casos pode ser calculada. Os teoremas seguintes determinam de forma explícita o valor da soma de Gauss, quando a ordem do caracter multiplicativo e p satisfazem uma relação especial.

Teorema 1.2.15 (Theorem 11.6.1 [1])**.** *Seja χ um caracter multiplicativo em $\mathbb{F}_{p^{2t}}$ de ordem d. Suponhamos que $p^t \equiv -1 \pmod{d}$ para algum inteiro t. Então*

$$p^{-t}G(\chi) = \begin{cases} 1, & \text{se } p = 2 \\ (-1)^{(p^t+1)/d}, & \text{se } p > 2. \end{cases}$$

Demonstração. Seja γ um gerador do grupo cíclico $\mathbb{F}_{q^2}^*$, onde $q = p^t$. Desta forma $c = \gamma^{q+1}$ é um gerador de $\mathbb{F}_q^*$. Cada $\alpha \in \mathbb{F}_{q^2}^*$ pode ser escrito de forma única na forma

$$\alpha = \gamma^{(q+1)u+v} = c^u\gamma^v, \text{ com } 0 \leqslant u < q-1, 0 \leqslant v < q+1.$$

Notemos que $\chi(c) = \chi(\gamma^{q+1}) = 1$, pois, por hipótese, a ordem de χ divide $q+1$. Desta forma

$$\chi(\alpha) = \chi(\gamma^{(q+1)u+v}) = \chi(\gamma^v) = \chi^v(\gamma)$$

e

$$G(\chi) = \sum_{\alpha \in \mathbb{F}_{q^2}^*} \chi(\alpha)\psi_1(\alpha) = \sum_{u=0}^{q-2}\sum_{v=0}^{q} \chi^v(\gamma)\psi_1(c^u\gamma^v) = \sum_{v=0}^{q} \chi^v(\gamma) \sum_{h \in \mathbb{F}_q^*} \psi_1(h\gamma^v).$$

Para todo $h \in \mathbb{F}_q^*$ temos que

$$Tr_{(2t,1)}(h\gamma^v) = Tr_{(t,1)}(Tr_{(2t,t)}(h\gamma^v)) = Tr_{(t,1)}(hw) \quad \text{onde} \quad w = Tr_{(2t,t)}(\gamma^v) \in \mathbb{F}_q.$$

Assim

$$\sum_{h\gamma^v} \psi_1(h\gamma^v) = \sum_{h \in \mathbb{F}_q^*} e^{2\pi i Tr(hw)/p} = \begin{cases} -1, & \text{se } w \neq 0 \\ q-1, & \text{se } w = 0. \end{cases}$$

Como $w = \gamma^v + \gamma^{vq}$, segue que $w = 0$ se, e somente se, $\gamma^{v(q-1)} = -1$.

No caso em que a caraterística é 2, esta equação é equivalente a $\gamma^{v(q-1)} = 1$, e desta forma $v(q-1)$ é um múltiplo da ordem de γ que é $q^2 - 1$. Assim v é um múltiplo de $q+1$, mas como $v < q+1$, concluímos que $v = 0$.

No caso que $p \neq 2$, temos que $\gamma^{2v(q-1)} = 1$, e portanto $2v(q-1)$ é múltiplo de $q^2 - 1$, o que implica que $(q+1)/2$ divide v. Como $v < q+1$ temos que $v = 0$ ou $(q+1)/2$, mas $v = 0$ é impossível pois $\gamma^{v(q-1)} = -1$.

Para calcular a soma de Gauss, suponhamos primeiro $p = 2$ e desta forma

$$G(\chi) = -\sum_{v=1}^{q} \chi^v(\gamma) + (q-1)\chi^0(\gamma) = q - \sum_{v=0}^{q} \chi^v(\gamma) = q$$

como queríamos. Agora suponhamos que $p > 2$. Então de forma similar

$$G(\chi) = -\sum_{\substack{v=0 \\ v \neq (q+1)/2}}^{q} \chi^v(\gamma) + (q-1)\chi^{(q+1)/2}(\gamma) = q\chi^{(q+1)/2}(\gamma).$$

Já que $\chi(\gamma) = e^{2\pi ij/d}$ para algum j relativamente primo com d, segue que

$$p^{-t}G(\chi) = \chi^{(q+1)/2}(\gamma) = e^{\pi ij(q+1)/d} = (-1)^{j(q+1)/d} = (-1)^{(q+1)/d}$$

onde a última igualdade vem do fato de que quando j é par, devemos ter d ímpar e $(q+1)/d$ par.

□

O próximo teorema determina a ordem de $p \pmod d$ quando -1 é uma potência de $p \pmod d$ e que será util para calcular a soma de Gauss para carateres definidos em algumas extensões de corpos.

Lema 1.2.16 (Theorem 11.6.2 [1])**.** *Seja $d > 2$ um inteiro. Suponha que existe um inteiro positivo t tal que $p^t \equiv -1 \pmod d$, e assumamos que t é mínimo com esta propriedade. Então $2t$ é a ordem de $p \pmod d$.*

Demonstração. Seja N a ordem de $p \pmod d$. Já que $p^{2t} \equiv 1 \pmod d$, então $N|2t$. Assumamos que $N \neq 2t$, desse modo $N \leqslant t$. Assim $-1 \equiv p^{t-N} \pmod d$, mas $t - N > 0$, contradizendo o fato da minimalidade de t. □

Definição 1.2.17. *Se χ é um caracter em $\mathbb{F}_q$. O levantamento canônico χ' do caracter χ de $\mathbb{F}_q$ para a extensão de corpo $\mathbb{F}_{q^v}$ é definido por*

$$\chi'(\alpha) = \chi(\mathbb{N}_{\mathbb{F}_{q^v}/\mathbb{F}_q}(\alpha)),$$

onde $\mathbb{N}_{\mathbb{F}_{q^v}/\mathbb{F}_q}(\alpha)) = \prod_{j=0}^{v-1} \alpha^{q^j}$ é a norma do elemento α com respeito à extensão $\mathbb{F}_{q^v}/\mathbb{F}_q$.

Teorema 1.2.18 (Theorem 11.6.3 [1]). *Seja $d > 2$ e suponhamos que existe um inteiro positivo t tal que $p^t \equiv -1 \pmod{d}$. Se t é o menor inteiro com esta propriedade e χ é um caracter multiplicativo de ordem d em $\mathbb{F}_{p^r}$, então existe um inteiro s tal que $r = 2ts$ e*

$$G(\chi) = \begin{cases} (-1)^{s-1}\sqrt{p^r}, & \text{se } p=2 \\ (-1)^{s-1+\frac{s(p^t+1)}{d}}\sqrt{p^r}, & \text{se } p \geqslant 3 \end{cases}$$

Além disso, para $1 \leqslant j \leqslant d-1$, a soma de Gauss $G_r(\chi^j)$ é dada por

$$G(\chi^j) = \begin{cases} (-1)^j\sqrt{p^r}, & \text{se } d \text{ é par, } p, \ s \ \text{e} \ \dfrac{p^t+1}{d} \ \text{são ímpares;} \\ (-1)^{s-1}\sqrt{p^r}, & \text{caso contrário.} \end{cases}$$

Demonstração. Como d divide a ordem de $\mathbb{F}_{p^r}^*$, segue que $p^r \equiv 1 \pmod{d}$. Além disso, pelo Lema 1.2.16, $2t$ é a ordem de $p \pmod{d}$, e assim $2t$ divide r, desta forma existe um inteiro s tal que $r = 2ts$. Como $d|(p^r - 1)$, então pelo Teorema 11.4.4$(c)(e)$ de [1], χ é o levantamento de algum caracter λ de ordem d em $\mathbb{F}_{p^{2t}}$. Pelo Teorema 11.5.2 de [1], temos que

$$G(\chi) = G(\chi) = (-1)^{s-1}G^s(\lambda).$$

Pelo Teorema 1.2.15, temos que

$$G(\chi) = (-1)^{s-1}G^s(\lambda) = \begin{cases} (-1)^{s-1}\sqrt{p^r}, & \text{se } p = 2 \\ (-1)^{s-1+\frac{s(p^t+1)}{d}}\sqrt{p^r}, & \text{se } p \geqslant 3. \end{cases}$$

Agora para calcular $G(\chi^j)$, observemos que a ordem de χ^j é igual a $\dfrac{d}{mdc(j,d)}$, assim

$$G(\chi^j) = \begin{cases} (-1)^{s-1}\sqrt{p^r}, & \text{se } p = 2 \\ (-1)^{s-1+\frac{s(p^t+1)}{\frac{d}{mdc(j,d)}}}\sqrt{p^r}, & \text{se } p \geqslant 3 \end{cases}$$

e se p, s e $\dfrac{p^t+1}{d}$ forem ímpares, teremos

$$G(\chi^j) = (-1)^{mdc(j,d)}\sqrt{p^r}$$

além disso, se d for par, o $mdc(j,d)$ depende apenas de j, como queríamos. □

1.3 Códigos Lineares sobre corpos finitos

Nesta seção será introduzido algumas noções básicas da teoria de códigos. Nas seguintes seções, $\mathbb{F}_q^n$ denotará um espaço vetorial sobre $\mathbb{F}_q$ de dimensão n, cujos elementos são n-uplas $a = (a_1, ..., a_n)$ com $a_i \in \mathbb{F}_q$.

1.3.1 Códigos lineares

Definição 1.3.1. *Dados $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n) \in \mathbb{F}_q^n$ definimos a distância entre a e b como*

$$d(a, b) := |\{i; a_i \neq b_i\}|.$$

Essa função d é uma métrica em $\mathbb{F}_q^n$ chamada distância de Hamming. Em particular, vale a desigualdade triangular $d(a, c) \leqslant d(a, b) + d(b, c)$ para todo $a, b, c \in \mathbb{F}_q^n$. O peso de um elemento $a \in \mathbb{F}_q^n$ é definido como

$$wt(a) := d(a, 0) =| \{i; a_i \neq 0\} | .$$

Definição 1.3.2. *Um código linear C de comprimento n sobre $\mathbb{F}_q$ é um subespaço linear de $\mathbb{F}_q^n$; os elementos de C são chamados palavras códigos. A dimensão de C como $\mathbb{F}_q$-espaço vetorial é chamada de dimensão do código. Um $[n, k]$-código é um código de comprimento n e dimensão k.*
A distancia mínima $d(C)$ de um código $C \neq 0$ é definido como

$$d(C) := min\{d(a, b) \mid a, b \in C \text{ e } a \neq b\} = min\{w(c) \mid 0 \neq c \in C\}.$$

Um $[n, k]$-código com distancia mínima d será denotado por $[n, k, d]$-código.

Uma maneira para descrever um código específico C explicitamente é escrever sua base como um espaço vetorial sobre $\mathbb{F}_q$.

Definição 1.3.3. *Seja C é um $[n, k]$-código sobre $\mathbb{F}_q$. Uma matriz geradora de C é uma matriz $k \times n$ cujas linhas forma uma base de C.*

Definição 1.3.4. *O produto interno formal em $\mathbb{F}_q^n$ é definido por*

$$\langle a, b\rangle := \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n) \in \mathbb{F}_q^n$.

Definição 1.3.5. *Se $C \subset \mathbb{F}_q^n$ é um código linear, então*

$$C^{\perp} := \{u \in \mathbb{F}_q^n \mid \langle u, c\rangle = 0 \text{ para todo } c \in C\}$$

é chamado o dual de C. O código C é chamado auto-dual (resp. auto-ortogonal) se $C = C^{\perp}$ (resp. $C \subseteq C^{\perp}$).

Lema 1.3.6. *O dual de um $[n, k]$-código é um $[n, n-k]$-código e $C = (C^{\perp})^{\perp}$. Em particular, a dimensão de um código auto-dual de comprimento n é $\dfrac{n}{2}$.*

Definição 1.3.7. *Uma matriz geradora H de $C^{\perp}$ é chamada de matriz de teste de paridade de C.*

A matriz de teste de paridade H de um $[n,k]$ código C é uma $(n-k)\times n$ matriz de posto $n-k$ e

$$C = \{u \in \mathbb{F}_q^n \mid Hu^T = 0\}.$$

1.3.2 Códigos cíclicos

Uma classe de códigos lineares de grande relevância neste trabalho são os códigos cíclicos, definidos da seguinte forma.

Definição 1.3.8. *Um $[n,k]$-código linear $C \subset \mathbb{F}_q^n$ sobre o corpo finito $\mathbb{F}_q$ é chamado cíclico se $(c_0, c_1, ..., c_{n-1}) \in C$ implica que $(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$.*

Uma representação útil de códigos cíclicos pode ser obtida a partir da relação que existe entre $\mathbb{F}_q^n$ e R_n.

De fato definindo a transformação linear

$$\begin{array}{rccc} \nu: & \mathbb{F}_q^n & \longrightarrow & R_n \\ & (a_0, ..., a_{n-1}) & \longmapsto & a_0 + a_1x + \cdots + a_{n-1}x^{n-1}, \end{array} \tag{1.6}$$

de forma direta pode ser mostrado que ν é um $\mathbb{F}_q$-transformação linear bijetiva. A partir disso identificamos cada vetor $(c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_q^n$ com

$$c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in R_n,$$

assim qualquer código de comprimento n sobre $\mathbb{F}_q$ corresponde a um subconjunto de R_n.

Lema 1.3.9. *Um código linear é cíclico se, e somente se, o subconjunto correspondente em R_n via isomorfismo ν é um ideal no anel R_n.*

A partir do Lema 1.3.9 e da Proposição 1.1.14, podemos afirmar que todo código cíclico possui um gerador que é um polinômio que divide o polinômio $x^n - 1$.

Seja $x^n - 1 = \prod_{i=1}^{\ell} f_i(x)$ a fatoração de $x^n - 1$ em fatores mônicos irredutíveis sobre $\mathbb{F}_q[x]$. Se C é um código cíclico, teremos que $C = \langle f(x) \rangle$, onde $f(x) \mid (x^n - 1)$. Seja $h(x) = \dfrac{x^n - 1}{f(x)}$ o polinômio de teste de paridade de C, então $h(x) = h_1(x) \cdots h_t(x)$, onde $h_j(x)$ $(1 \leqslant j \leqslant t)$ são polinômios irredutíveis sobre $\mathbb{F}_q[x]$ com grau m_j. No caso que n é primo relativo com a caraterística do corpo, os fatores de $x^n - 1$ são simples e portanto os fatores de $f(x)$ e $h(x)$ também serão. Se g_j é uma raiz de $h_j(x)$, então as raízes de $h_j(x)$ são $g_j, g_j^q, \ldots, g_j^{q^{m_j-1}} \in \mathbb{F}_{q^{m_j}}$. No que segue, vamos assumir que n é primo relativo com a caraterística.

Definição 1.3.10. *A raiz g_i de $h_i(x)$ é chamada de um zero do código C. Dizemos que o número de zeros de $C = \langle f(x) \rangle$ é o número de fatores irredutíveis de $h(x) = \dfrac{x^n - 1}{f(x)}$ sobre $\mathbb{F}_q[x]$.*

Da definição anterior temos que um código com um zero é um código que cujo polinômio teste de paridade é um divisor irredutível de $x^n - 1$.

Uma forma alternativa de definir um código cíclico a partir de extensões do corpo $\mathbb{F}_q$ é a seguinte: para m inteiro positivo, denotamos por θ o gerador de $\mathbb{F}_{q^m}^*$. Dados t inteiros $z_1, \ldots, z_t$, onde $0 \leqslant z_i \leqslant q^m - 2$, tais que não estão na mesma classe de q equivalência módulo $q^m - 1$, isto é, a congruência $z_i q^l \not\equiv z_j \pmod{q^m - 1}$ não tem solução em l para todo $i \neq j$, denotamos por $\alpha_j = \theta^{-z_j}$, $h_j(x) \in \mathbb{F}_q[x]$ o polinômio minimal de α_j, m_j o grau de h_j, $\delta = \text{mdc}(q^m - 1, z_1, ..., z_t)$ e $n = \dfrac{q^m - 1}{\delta}$. Consideremos a transformação linear $c : \mathbb{F}_{q^{m_1}} \times \cdots \times \mathbb{F}_{q^{m_t}} \to \mathbb{F}_q^n$ definida por

$$c(a_1, ..., a_t) = \left(\sum_{j=1}^{t} Tr_{m_j,1}(a_j \alpha_j^0), \sum_{j=1}^{t} Tr_{m_j,1}(a_j \alpha_j^1), ..., \sum_{j=1}^{t} Tr_{m_j,1}(a_j \alpha_j^{(n-1)}) \right) \tag{1.7}$$

onde $Tr_{m_j,1}$ denota o traço da função de $\mathbb{F}_{q^{m_j}}$ para $\mathbb{F}_q$. A imagem da transformação c

$$C = \{c(a_1, ..., a_t) \mid a_j \in \mathbb{F}_{q^{m_j}}\}$$

é um subespaço vetorial de $\mathbb{F}_q^n$, isto é, um código linear de comprimento n sobre $\mathbb{F}_q$. Facilmente se verifica que $c(a_1\alpha_1, \ldots, a_t\alpha_t)$ gera uma palavra do código que é um shift as coordenadas da palavra $c(a_1, ..., a_t)$. Portanto C é um código cíclico. Vejamos que todo código cíclico C pode ser obtido como imagem de uma transformação linear da forma mostrada em (1.7).

Teorema 1.3.11. *Seja C um $[n, k]$-código cíclico gerado por $f(x)$ divisor de $x^n - 1$. Então C pode ser escrito como imagem de uma transformação linear da forma mostrada em (1.7).*

Demonstração. Consideremos $h(x) = \dfrac{x^n - 1}{f(x)}$, onde $h(x) = h_1(x) \cdots h_t(x)$ é a fatoração de $h(x)$ em fatores irredutíveis. Denotamos por m_j o grau de $h_j(x)$ e por α_j é uma raiz de $h_j(x)$, e portanto $\mathbb{F}_q[\alpha_j] = \mathbb{F}_{q^{m_j}}$. Seja $c : \mathbb{F}_q^{m_1} \times \cdots \times \mathbb{F}_q^{m_t} \to \mathbb{F}_q^n$ a transformação linear definida em (1.7). Afirmamos que a imagem de c é isomorfa ao código gerado por $f(x)$ em R_n.

Sabemos que $dim_{\mathbb{F}_q}(\mathbb{F}_q^{m_1} \times \cdots \times \mathbb{F}_q^{m_t}) = m_1 + m_2 + \cdots + m_t = deg(h(x))$. Suponhamos que existe $(\beta_1, \cdots, \beta_t) \in Ker(c)$, assim $\sum_{j=1}^{t} Tr_{m_j,1}(\beta_j \alpha_j^{-l}) = 0$ para todo $l = 0, 1, \cdots, n-1$, desta forma se $Q(x) \in \mathbb{F}_q[x]$ com $Q(x) = \sum_{l=0}^{n-1} a_l x^l$ então

$$\sum_{j=1}^{t} Tr_{m_j,1}(\beta_j Q(\alpha_j^{-1})) = \sum_{j=1}^{t} Tr_{m_j,1}(\beta_j \sum_{l=0}^{n-1} a_l \alpha_j^{-l}) = \sum_{l=0}^{n-1} a_l \sum_{j=1}^{t} Tr_{m_j,1}(\beta_j \alpha_j^{-l}) = 0.$$

Para cada $Q(x) \in \mathbb{F}_q[x]$ e cada $i = 1, ..., t$, pelo Teorema chinês do resto (Ver [3]), existe um polinômio

$$P_{Q,i}(x) \in \mathbb{F}_q[x]$$

com as seguintes propriedades

$$\begin{cases} P_{Q,i}(x) \equiv 0 \mod \dfrac{h^*(x)}{h_i^*(x)} \\ P_{Q,i}(x) \equiv Q(x) \mod h_i^*(x), \end{cases}$$

onde $h^*(x) = x^{\deg(h)} h(1/x)$ é o polinômio reciproco de $h(x)$. Já que $(\beta_1, ..., \beta_n) \in Ker(c)$, segue que

$$0 = \sum_{j=1}^{t} Tr_{m_j,1}(\beta_j P_{Q,i}(\alpha_j^{-1})).$$

Como $P_{Q,i}(\alpha_j^{-1}) = 0$ para $i \neq j$, então teremos que

$$\sum_{j=1}^{t} Tr_{m_j,1}(\beta_j P_{Q,i}(\alpha_j^{-1})) = Tr_{m_i,1}(\beta_i Q(\alpha_i^{-1})).$$

Observe que $Q(\alpha_i^{-1})$ percorre todos os elementos de $\mathbb{F}_{q^{m_i}} = \mathbb{F}_q[\alpha_i]$ quando variamos $Q(x)$, isto é, $Tr_{m_i,1}(\beta_i \theta) = 0$ para todo $\theta \in \mathbb{F}_{q^{m_i}}$, isso implica que $\beta_i = 0$, logo c é injetiva. Portanto a imagem é um $[n, k]$-código cíclico, onde $k = m_1 + \cdots + m_t = deg(h(x))$.

Agora vamos mostrar que $h(x)$ é o polinômio de teste de paridade de $Im(c)$. No que segue, por abuso de notação, usando o isomorfismo definido em (1.6), vamos denotar cada elemento de $Im(c)$, segundo a conveniência, ou bem como a n-tupla $(c_0, ..., c_{n-1})$ ou como o polinômio $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in R_n$. Desta forma $h(x) = \sum_{i=0}^{k} h_i x^i$ é polinômio teste de paridade de $Im(c)$ se

$$\left(\sum_{l=0}^{n-1} c_l x^l \right) \left(\sum_{i=0}^{k} h_i x^i \right) \equiv 0 \mod (x^n - 1).$$

Como $(c_0, ..., c_{n-1}) \in Im(c)$, então $c_l = \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{-l})$, assim

$$\begin{aligned} \left(\sum_{l=0}^{n-1} c_l x^l \right) \left(\sum_{i=0}^{k} h_i x^i \right) =& h_0 \left(\sum_{j=0}^{t} Tr(\beta_j), \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{-1}), ..., \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{-(n-1)}) \right) + \\ & h_1 \left(\sum_{j=0}^{t} Tr(\beta_j \alpha_j), \sum_{j=0}^{t} Tr(\beta_j), ..., \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{-(n-2)}) \right) + \cdots \\ & h_k \left(\sum_{j=0}^{t} Tr(\beta_j \alpha_j^{n-1}), \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{n-2}), ..., \sum_{j=0}^{t} Tr(\beta_j) \right). \end{aligned}$$

Observemos que se somarmos os termos da coordenada $l+1$-ésima para algum $l \in \{0, ..., k\}$ teremos

$$h_0 \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{-l}) + h_1 \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{-l+1}) + \cdots + h_k \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{-l+(k)}) =$$
$$\sum_{i=0}^{k} h_i \sum_{j=0}^{t} Tr(\beta_j \alpha_j^{-l+i}) = \sum_{j=0}^{t} Tr\left(\beta_j \alpha_j^{-l} \sum_{i=0}^{k} h_i \alpha_j^i\right) =$$
$$\sum_{j=0}^{t} Tr\left(\beta_j \alpha_j^{-l} h(\alpha_j)\right) = 0.$$

Daí como C tem dimensão k e polinômio teste de paridade h segue que é isomorfo ao código gerado por $f(x)$. □

Usando a caraterização obtida a partir do teorema anterior, temos que o peso de Hamming de uma palavra código $c(a_1, ..., a_t) \in C$, pode ser calculada a partir da fórmula

$$w(c(a_1, ..., a_t)) = n - Z(c(a_1, \ldots, a_t)),$$

onde $Z(c(a_1, \cdots, a_t))$ é a quantidade de coordenadas nulas da palavra $c(a_1, ..., a_t)$, ou seja,

$$Z(c(a_1, \cdots, a_t)) = \mid \{0 \leqslant i \leqslant n-1; \sum_{j=1}^{t} Tr_{(m_j,1)}(a_j \alpha_j^{-i}) = 0\} \mid \tag{1.8}$$

Sendo ψ_1 o caracter aditivo canônico, segue de (1.1) que

$$\frac{1}{q} \sum_{y \in \mathbb{F}_q} \psi_1(ay) = \begin{cases} 1, & \text{se } a = 0 \\ 0, & \text{se } a \neq 0, \end{cases} \tag{1.9}$$

substituindo a por $\sum_{j=1}^{t} Tr_{(m_j,1)}(a_j \alpha_j^{-i})$ em (1.9), teremos que

$$\frac{1}{q} \sum_{y \in \mathbb{F}_q} \psi_1\left(y \sum_{j=1}^{t} Tr_{(m_j,1)}(a_j \alpha_j^{-i})\right) = \begin{cases} 1, & \text{se } \sum_{j=1}^{t} Tr_{(m_j,1)}(a_j \alpha_j^{-i}) = 0 \\ 0, & \text{se } \sum_{j=1}^{t} Tr_{(m_j,1)}(a_j \alpha_j^{-i}) \neq 0. \end{cases} \tag{1.10}$$

Usando (1.10), podemos reescrever $Z(c(a_1, \cdots, a_t))$ da seguinte forma:

$$\begin{aligned} Z(c(a_1, \cdots, a_t))) &= \sum_{i=0}^{n-1} \frac{1}{q} \sum_{y \in \mathbb{F}_q} \psi_1\left(y \sum_{j=1}^{t} Tr_{(m_j,1)}(a_j \alpha_j^{-i})\right) \\ &= \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q} \psi_1\left(y \sum_{j=1}^{t} Tr_{(m_j,1)}(a_j \alpha_j^{-i})\right) \\ &= \frac{n}{q} + \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q^*} \psi_1\left(\sum_{j=1}^{t} Tr_{(m_j,1)}(y a_j \alpha_j^{-i})\right) \end{aligned}$$

Já que ψ_1 é o caracter aditivo canônico de $\mathbb{F}_q$. Então $\Psi_j = \psi_1 \circ Tr_{(m_j,1)}$ é o caracter aditivo canônico de $\mathbb{F}_{q^{m_j}}$. Pela ortogonalidade do caracter aditivo temos que

$$Z(c(a_1, \ldots, a_t)) = \frac{n}{q} + \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q^*} \prod_{j=1}^{k} \Psi_j(y a_j \alpha_j^{-i})). \tag{1.11}$$

Dessa forma

$$w(c(a_1, \ldots, a_t)) = n - \frac{n}{q} - \frac{1}{q} \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_q^*} \prod_{j=1}^{k} \Psi_j(y a_j \alpha_j^{-i})).$$

Em geral, calcular o valor da função Z para um conjunto específico de $(a_1, \ldots, a_t)$ não é trivial. No entanto, esta fórmula será útil para determinar a distribuição de pesos em alguns códigos.

2 Códigos diedrais e suas propriedades

Nesse capítulo, apresentamos os objetos principais desse trabalho: os códigos diedrais, que são ideais à esquerda da álgebra de grupo $\mathbb{F}_q D_{2n}$, onde D_{2n} é o grupo diedral de ordem $2n$. Para chegar a essa definição, começamos o capítulo apresentando os objetos envolvidos nela. Em seguida, estudamos a decomposição de Wedderburn da álgebra $\mathbb{F}_q D_{2n}$ seguindo a referência [3] e também elementos idempotentes. Por fim, apresentamos a construção de códigos diedrais e suas propriedades principais.

2.1 Definições iniciais

A fim de definir a classe de códigos diedrais, começamos apresentando a noção geral de álgebra de grupo.

Definição 2.1.1. *Dado $\mathbb{K}$ um corpo e G um grupo finito, a álgebra de grupo de $\mathbb{K}G$ é o conjunto*

$$\mathbb{K}G := \left\{ \sum_{\gamma \in G} a_\gamma \gamma \mid a_\gamma \in \mathbb{K} \right\},$$

dotado de três operações: soma, produto e multiplicação por escalares definidas de forma natural: para quaisquer $a_\gamma, b_\gamma \in \mathbb{K}$ e $c \in \mathbb{K}$

$$\sum_{\gamma \in G} a_\gamma \gamma + \sum_{\gamma \in G} b_\gamma \gamma = \sum_{\gamma \in G} (a_\gamma + b_\gamma)\gamma$$

$$c \left(\sum_{\gamma \in G} a_\gamma \gamma \right) = \sum_{\gamma \in G} c a_\gamma \gamma$$

$$\left(\sum_{\gamma \in G} a_\gamma \gamma \right) \cdot \left(\sum_{\gamma \in G} b_\gamma \gamma \right) = \sum_{\gamma \in G} \left(\sum_{\mu\nu = \gamma} a_\mu b_\nu \right) \gamma.$$

Com estas operações $\mathbb{K}G$ é um álgebra sobre $\mathbb{K}$, chamada de álgebra de grupo. Em particular $\mathbb{K}G$ é um espaço vetorial sobre $\mathbb{K}$ com a base canônica $\{\gamma\}_{\gamma \in G}$.

Aqui, estamos interessados na álgebra de grupo formada pelo corpo finito $\mathbb{F}_q$ e pelo grupo diedral de ordem $2n$, cuja definição relembramos a seguir.

Definição 2.1.2. *Para todo inteiro $n \geqslant 3$ definimos o grupo diedral de ordem $2n$ como o grupo que tem uma apresentação da seguinte forma*

$$D_{2n} = \langle \alpha, \beta ; \alpha^n = 1, \beta^2 = 1, \beta\alpha = \alpha^{-1}\beta \rangle.$$

Outras noções importantes são a de $G-$código à esquerda e de código de grupo à esquerda, que apresentamos a seguir.

Definição 2.1.3. *Se G é um grupo de ordem n e $C \subset \mathbb{F}_q^n$ é um código linear, então dizemos que C é um G-código à esquerda se existe uma bijeção $\tau : E \longrightarrow G$, onde E é uma base de $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$ tal que a extensão linear de τ é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais $\mathbb{F}_q^n$ para $\mathbb{F}_qG$, de tal forma que a imagem C via o isomorfismo é um ideal à esquerda de $\mathbb{F}_qG$.*

Definição 2.1.4. *Um código de grupo à esquerda é um $\mathbb{F}_q$- código linear o qual é um G-código à esquerda para algum grupo G.*

É fácil verificar que um código cíclico de comprimento n é um código linear que é um C_n-código, onde C_n é um grupo cíclico com n elementos.

Estamos prontos para, enfim, definir os objetos principais dessa pesquisa.

Definição 2.1.5. *Um código diedral sobre $\mathbb{F}_q$ de comprimento $2n$, ou D_{2n}-código à esquerda sobre $\mathbb{F}_q$, é um ideal à esquerda de $\mathbb{F}_qD_{2n}$.*

Para a construção de exemplo não triviais de códigos diedrais, precisamos de uma apresentação do anel de grupo $\mathbb{F}_qD_{2n}$ em componentes simples. Para isso, na seguinte seção estudaremos a estrutura dos códigos diedrais, isso é, a estrutura dos ideais à esquerda da álgebra de grupos $\mathbb{F}_qD_{2n}$.

2.2 Decomposição de Wedderburn

Dizemos que uma álgebra é *simples* se não tem ideais bilaterais não triviais. De igual forma dizemos que uma álgebra é *semissimples* se é soma direta de álgebras *simples*. O Teorema de Wedderburn(Theorem 2.6.18 [12]) nos garante que toda álgebra *semissimples* é soma direta de álgebras de matrizes sobre uma álgebra de divisão F. Além disso, pelo pequeno Teorema de Wedderburn sabemos que toda álgebra de divisão finita é um corpo finito.

A partir desse ponto, consideraremos $\mathbb{F}_q$ um corpo com q elementos, com q sendo uma potência de algum primo diferente de 2, e $n \geqslant 3$ um inteiro primo relativo com q. Com esta hipótese, pelo Teorema de Maschke(Theorem 3.4.7 [12]) a álgebra de Grupos $\mathbb{F}_qD_{2n}$ é *semissimples*. No que segue mostraremos explicitamente a decomposição desta álgebra em componentes *simples*. Esta decomposição será útil para determinar de forma explicita os ideais de $\mathbb{F}_qD_{2n}$.

Definição 2.2.1. *Dado um polinômio $g(x)$ com $g(0) \neq 0$, denotamos por $g^*(x)$ o polinômio recíproco de $g(x)$, isto é, $g^*(x) = x^{deg(g)}g\left(\frac{1}{x}\right)$.*

Definição 2.2.2. *Um polinômio é chamado autorrecíproco se $g(x)$ e $g^*(x)$ possuem as mesmas raízes, com a mesma multiplicidade, no corpo de decomposição.*

Lema 2.2.3 (Remark 3.2 [3]). *Se β é uma raiz do polinômio $g(x) \in \mathbb{F}_q[x]$, então β^{-1} é uma raiz do polinômio $g^*(x)$. Além disso, quando $g(x)$ é autorrecíproco e ± 1 não são raízes de $g(x)$, então existe um polinômio $h(x) \in \mathbb{F}_q[x]$ de grau $\dfrac{deg(g(x))}{2}$, tal que β é uma raiz de $g(x)$ se, e somente se, $\beta + \beta^{-1}$ é uma raiz de $h(x)$.*

Observemos que se $g(x)$ é um polinômio autorrecíproco que não tem ± 1 como raízes, então as raízes de $g(x)$ podem ser agrupadas em pares $\alpha \neq \alpha^{-1}$, logo o grau de $g(x)$ é par.

Consideremos a decomposição do polinômio $x^n - 1 \in \mathbb{F}_q[x]$ em fatores mônicos irredutíveis, da seguinte forma:

$$x^n - 1 = f_1 f_2 \cdots f_r f_{r+1} f_{r+1}^* f_{r+2} f_{r+2}^* \cdots f_{r+s} f_{r+s}^*$$

onde $f_1 = x - 1$, $f_2 = x + 1$ se n é par e $f_j^* = f_j$ para $2 \leqslant j \leqslant r$, onde r é o número de fatores autorrecíprocos na fatoração e $2s$ é o número de fatores não autorrecíprocos.

Teorema 2.2.4 (Theorem 3.1 [3]). *A álgebra de grupo $\mathbb{F}_q D_{2n}$ tem decomposição de Wedderburn da forma*

$$\mathbb{F}_q D_{2n} \cong \bigoplus_{j=1}^{r+s} A_j \tag{2.1}$$

onde

$$A_j = \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q \text{ se } j \leqslant \delta \\ M_2(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]) \text{ se } \delta + 1 \leqslant j \leqslant r + s \end{cases} \quad \text{com } \delta = \begin{cases} 1 & \text{se } n \text{ é ímpar} \\ 2 & \text{se } n \text{ é par} \end{cases}$$

com α_j raiz do polinômio $f_j(x)$. Além disso, se $r + 1 \leqslant j \leqslant r + s$, então $f_j \neq f_j^*$ e $M_2(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]) = M_2(\mathbb{F}_q[\alpha_j])$.

2.3 Idempotentes

Um elemento $e \neq 0$ em um anel A é dito idempotente se $e^2 = e$. Um idempotente é chamado primitivo se ele não pode ser escrito como $e = e' + e''$, onde e', e'' são elementos idempotentes não nulos de A tais que $e'e'' = 0$. Um família de idempotentes primitivos $e_1, \ldots, e_r$ satisfazendo as seguintes condições:

1. $e_i \neq 0$ para todo $1 \leqslant i \leqslant r$,
2. se $i \neq j$, então $e_i e_j = 0$,
3. $e_1 + \cdots + e_r = 1$

é chamada família completa de idempotentes ortogonais.

Observemos que se e é um idempotente de A, então Ae é um ideal à esquerda de A. Desta forma fica natural determinar ideais à esquerda a partir de idempotentes.

Lema 2.3.1. *Se e é um idempotente do anel A, então $1-e$ é um idempotente ortogonal a e.*

Demonstração.

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$$

e

$$e(1-e) = e - e^2 = e - e = 0.$$

□

Teorema 2.3.2 (Teorema 2 [7])**.** *O número de ideais à esquerda de posto k em $M_n(\mathbb{F}_q)$ é*

$$\frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)\cdots(q-1)}.$$

Corolário 2.3.3. *Todo ideal não trivial à esquerda de $M_2(\mathbb{F}_q)$, pode ser gerado por um idempotente da seguinte forma:*

$$\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} \text{ ou } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

para algum $x \in \mathbb{F}_q$.

Demonstração. Pelo Teorema 2.3.2, segue que $M_2(\mathbb{F}_q)$ possui $q+1$ ideais a esquerda de posto 1. Observemos que como $x \in \mathbb{F}_q$, então temos $q+1$ idempotentes da seguinte forma:

$$\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} \text{ ou } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Considere x e y pertencente a $\mathbb{F}_q$, se

$$\begin{pmatrix} 1 & y \\ 0 & 0 \end{pmatrix}$$

pertence ao ideal gerado por

$$\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}$$

então existem $a, b, c, d \in \mathbb{F}_q$ tais que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 0 \end{pmatrix}$$

isso implica que

$$\begin{pmatrix} a & ax \\ c & cx \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 0 \end{pmatrix}$$

daí temos que $x = y$, desta forma esses idempotentes geram ideais à esquerda distintos. Como esses idempotentes possui posto 1, podemos concluir o resultado. □

Partindo disso, se I_j é um ideal à esquerda não trivial de $A_j = M_{2\times 2}(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}])$, e do fato que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & ax \\ c & cx \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix},$$

segue que

$$I_j = \left\{ \begin{pmatrix} a & ax \\ c & cx \end{pmatrix} \mid a, c \in \mathbb{F}_q[\alpha_j + \alpha_j^{-1}] \right\} = \left\langle \begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & x \end{pmatrix} \right\rangle_{\mathbb{F}_q[\alpha_j+\alpha_j^{-1}]}$$

ou

$$I_j = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \mid b, d \in \mathbb{F}_q[\alpha_j + \alpha_j^{-1}] \right\} = \left\langle \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle_{\mathbb{F}_q[\alpha_j+\alpha_j^{-1}]}.$$

Em particular, a dimensão I_j como $\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]$-espaço vetorial é 2.

Proposição 2.3.4. *Seja I_j um ideal à esquerda não trivial de $M_{2\times 2}(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}])$, onde $j > \delta$, então*

$$dim_{\mathbb{F}_q} I_j = \begin{cases} 2deg(f_j) & se \quad f_j \neq f_j^* \\ deg(f_j) & se \quad f_j = f_j^* \end{cases}$$

Demonstração. A proposição segue do fato que $dim_{\mathbb{F}_q} M_{2\times 2}(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]) = 4 \times [\mathbb{F}_q[\alpha_j + \alpha_j^{-1}] : \mathbb{F}_q]$, e pelo Lema 2.2.3 temos que

$$[\mathbb{F}_q[\alpha_j + \alpha_j^{-1}] : \mathbb{F}_q] = \begin{cases} deg(f_j) & se \quad f_j \neq f_j \\ \frac{1}{2}deg(f_j) & se \quad f_j = f_j. \end{cases}$$

□

2.4 Construção de códigos diedrais

Os códigos diedrais são pouco estudados na literatura e o proposito desta seção é mostrar como podemos usar as técnicas conhecidas de códigos cíclicos neste tipo de códigos. Desta forma resultado presentes neste seção são originais. Iniciamos nossa construção dos códigos diedrais, que é o principal objeto de estudo deste trabalho. Usando a apresentação de D_{2n} da forma

$$D_{2n} = \langle \alpha, \beta | \alpha^n = 1, \beta^2 = 1, \beta\alpha = \alpha^{-1}\beta \rangle,$$

temos que $\mathbb{F}_q D_{2n} = \{P(\alpha) + Q(\alpha)\beta \mid P(x), Q(x) \in \mathbb{F}_q[x]\}$, com $deg(P(x)) \leqslant n-1$ e $deg(Q(x)) \leqslant n-1$, onde $P(x) = \sum_{j=0}^{n-1} a_j x^j$ e $Q(x) = \sum_{j=0}^{n-1} b_j x^j$. Considerando $(\mathbb{F}_q D_{2n}, +)$ como espaço vetorial sobre $\mathbb{F}_q$, se verifica de forma direta que a função

$$\begin{array}{rccc} \Phi: & \mathbb{F}_q D_{2n} & \longrightarrow & \mathbb{F}_q^{2n} \\ & P(\alpha)+Q(\alpha)\beta & \longmapsto & (a_0, ...a_{n-1}, b_0, ..., b_{n-1}) \end{array} \tag{2.2}$$

é um isomorfismo de $\mathbb{F}_q$ espaços vetoriais.

Tomemos $\alpha_1, \alpha_2 \in \mathbb{F}_{q^m}$ com $ord(\alpha_1) = ord(\alpha_2) = n$ e $f_{\alpha_1}(x)$, $f_{\alpha_2}(x) \in \mathbb{F}_q[x]$ polinômios mônicos mínimos de α_1 e α_2 respectivamente com $deg(f_{\alpha_1}) = deg(f_{\alpha_2}) = m = ord_n q < n$. Definimos a transformação $\mathbb{F}_q$-linear

$$\begin{array}{rccc} C: \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_q^{2n} \\ (\beta_1, \beta_2) & \longmapsto & (Tr(\beta_1\alpha_1^0), ..., Tr(\beta_1\alpha_1^{n-1}), Tr(\beta_2\alpha_2^0), ..., Tr(\beta_2\alpha_2^{n-1})) \end{array} \tag{2.3}$$

onde Tr denota a função traço de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. A imagem da transformação C é um $\mathbb{F}_q$ subespaço linear de $\mathbb{F}_q^{2n}$.

Lema 2.4.1. *O núcleo da aplicação C é trivial.*

Demonstração. Seja $(\beta_1, \beta_2) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ tal que $Tr(\beta_1\alpha_1^j) = 0 = Tr(\beta_2\alpha_2^j)$ para $j \in \{0, \ldots, n-1\}$. Já que $ord(\alpha_1) = n$, então α_1 é raiz de $x^n - 1$, assim $f_{\alpha_1} \mid (x^n - 1)$. Como o polinômio mínimo de α sobre $\mathbb{F}_q$ tem grau m, então $1, \alpha_1, \alpha_1^2, \ldots, \alpha_1^{m-1}$ são $L.I.$ sobre $\mathbb{F}_q$. Desta forma se $Tr(\beta_1\alpha_1^j) = 0$ para todo j, usando a linearidade do traço, segue que $Tr(\beta_1(\sum_{j=0}^{m-1} c_j\alpha_1^j)) = 0$, para toda escolha de $c_0, \ldots, c_{m-1} \in \mathbb{F}_q$, isso implica que $Tr(\beta_1\rho) = 0$ para todo $\rho \in \mathbb{F}_{q^m}$ e isso só acontece se $\beta_1 = 0$. De forma análoga mostramos que $\beta_2 = 0$. □

Agora que sabemos que C é linear e injetiva. Verificaremos que para escolhas adequadas de α_1 e α_2, a imagem de C é um código diedral. Para tal, precisamos de alguns lemas.

Lema 2.4.2. *Seja Φ o isomorfismo dado em (2.2) e C a transformação linear injetiva dada em (2.3). Se $P(\alpha) + Q(\alpha)\beta \in \mathbb{F}_q D_{2n}$ é tal que $\Phi(P(\alpha) + Q(\alpha)\beta) \in Im(C)$, então existe $(\gamma_1, \gamma_2) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ tal que $C(\gamma_1, \gamma_2) = \Phi(\alpha(P(\alpha) + Q(\alpha)\beta))$.*

Demonstração. Seja

$$\Phi(P(\alpha) + Q(\alpha)\beta) = (a_0, ..., a_{n-1}, b_0, ..., b_{n-1}) \in Im(C),$$

isto é, existe $(\beta_1, \beta_2) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$, tal que $C(\beta_1, \beta_2) = \Phi(P(\alpha) + Q(\alpha)\beta)$. Como

$$C(\beta_1, \beta_2) = (Tr(\beta_1), Tr(\beta_1\alpha_1^1), ..., Tr(\beta_1\alpha_1^{n-1}), Tr(\beta_2), Tr(\beta_2\alpha_2^1), ..., Tr(\beta_2\alpha_2^{n-1})),$$

e

$$\Phi(\alpha(P(\alpha)+Q(\alpha)\beta)) = (a_{n-1}, a_0, ..., a_{n-2}, b_{n-1}, b_0, ..., b_{n-2}),$$

devemos mostrar que existe (γ_1, γ_2) tal que

$$C(\gamma_1, \gamma_2) = (Tr(\beta_1\alpha_1^{n-1}), Tr(\beta_1), ..., Tr(\beta_1\alpha_1^{n-2}), Tr(\beta_2\alpha_2^{n-1}), Tr(\beta_2), ..., Tr(\beta_2\alpha_2^{n-2})).$$

Para isso, se verifica diretamente que basta tomarmos $(\gamma_1, \gamma_2) = (\beta_1\alpha_1^{n-1}, \beta_2\alpha_2^{n-1})$. □

Lema 2.4.3. *Sejam $\alpha_1 = \alpha_2^{-1}$ e $P(\alpha)+Q(\alpha)\beta \in \mathbb{F}_q D_{2n}$ tal que $\Phi(P(\alpha)+Q(\alpha)\beta) \in Im(C)$, então existem $(\omega_1, \omega_2) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ tal que $C(\omega_1, \omega_2) = \Phi(\beta(P(\alpha)+Q(\alpha)\beta))$.*

Demonstração. Seja $\Phi(P(\alpha)+Q(\alpha)\beta) = (a_0, ..., a_{n-1}, b_0, ..., b_{n-1})$, então

$$\Phi(\beta(P(\alpha)+Q(\alpha)\beta)) = (b_0, b_{n-1}, ..., b_1, a_0, a_{n-1}, ..., a_1),$$

precisamos encontrar (ω_1, ω_2) tal que

$$\Phi(\omega_1, \omega_2) = (Tr(\beta_2), Tr(\beta_2\alpha_2^{n-1}), ..., Tr(\beta_2\alpha_2^1), Tr(\beta_1), Tr(\beta_1\alpha_1^{n-1}), ..., Tr(\beta_1\alpha_1)),$$

para que isso aconteça é suficiente tomarmos $(\omega_1, \omega_2) = (\beta_2, \beta_1)$, pois

$$\Phi(\beta_2, \beta_1) = (Tr(\beta_2), Tr(\beta_2\alpha_1), ..., Tr(\beta_2\alpha_1^{n-1}), Tr(\beta_1), Tr(\beta_1\alpha_2), ..., Tr(\beta_1\alpha_2^{n-1})$$

e como $\alpha_1 = \alpha_2^{-1}$, segue que

$$\Phi(\beta_2, \beta_1) = (Tr(\beta_2), Tr(\beta_2\alpha_2^{n-1}), ..., Tr(\beta_2\alpha_2^1), Tr(\beta_1), Tr(\beta_1\alpha_1^{n-1}), ..., Tr(\beta_1\alpha_1^1))$$

□

Estamos agora prontos para provar que, com certa condição, a imagem da aplicação C é um código diedral com comprimento e dimensão conhecidos.

Proposição 2.4.4. *Se $\alpha_1 = \alpha_2^{-1}$, então a imagem de C é um código diedral de comprimento $2n$ e dimensão $2\,deg(f)$.*

Demonstração. Precisamos mostrar que $Im(C)$ é um D_{2n}-código à esquerda, para isso basta mostrarmos que $\Phi^{-1}(Im(C))$ é um ideal à esquerda de $\mathbb{F}_q D_{2n}$. Seja $P(\alpha)+Q(\alpha)\beta \in \mathbb{F}_q D_{2n}$ com $\Phi(P(\alpha)+Q(\alpha)\beta) \in Im(C)$, então deve existir (γ_1, γ_2) e (ω_1, ω_2) pertencentes a $\mathbb{F}_q^m \times \mathbb{F}_q^m$ de forma que $C(\gamma_1, \gamma_2) = \Phi(\alpha(P(\alpha)+Q(\alpha)\beta))$ e $C(\omega_1, \omega_2) = \Phi(\beta(P(\alpha)+Q(\alpha)\beta))$, os Lemas 2.4.2 e 2.4.3 garantem a existência. Portanto $\Phi^{-1}(Im(C))$ é um ideal à esquerda de $\mathbb{F}_q D_{2n}$. Assim concluímos que $Im(C)$ é um código diedral. Como C é injetiva, pela Proposição 2.3.4 a dimensão de $Im(C)$ é igual a $2deg(f)$ e por estar contido em $\mathbb{F}_q^{2n}$, segue que $Im(C)$ possui comprimento $2n$. □

Sabemos que $Im(C)$ é um código diedral, então existe um ideal à esquerda $J \subset \mathbb{F}_q D_{2n}$ tal que $\Phi(J) = Im(C)$. Se J for minimal, então pelo Teorema 2.2.4, existe $j \in \mathbb{N}$ tal que a projeção sobre a j-ésima componente na decomposição de Wedderburn, é o ideal à esquerda $I_j \subset A_j$ e $J \simeq (0, \cdots, 0, I_j, 0, \cdots 0)$, como $dim_{\mathbb{F}_q} J = 2m$ com $m = deg(f_j)$, onde f_j é o polinômio mínimo de α, então $dim_{\mathbb{F}_q} I_j = 2m$, o que implica que $f_j \neq f_j^*$. Agora se J não é minimal, então existe $I \subsetneq J$ minimal e analogamente existe $j \in \mathbb{N}$ de forma que $I \simeq (0, \cdots, 0, I_j, 0, \cdots, 0)$, como $dim_{\mathbb{F}_q} I_j < 2m$, onde I_j é minimal, pela Proposição 2.3.4 temos que $dim_{\mathbb{F}_q} I_j = m$, isso implica que $f_j = f_j^*$.

Já que $C(\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}) = J$, vamos supor que J não é minimal, então existe um $\mathbb{F}_q$-subespaço de $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ que é isomorfo ao ideal minimal $I \subsetneq J$, vamos procurar os subespaços de $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ que são isomorfos a I quando $f_j = f_j^*$. Para isso vamos considerar a transformação linear

$$\begin{array}{ccc} \rho : \mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}} & \longrightarrow & \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \\ (\beta_1, \beta_2) & \longmapsto & \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} \end{array}$$

onde u_{11}, u_{12}, u_{21} e u_{22} são elementos de $\mathbb{F}_{q^m}$ que serão determinados de forma apropriada para que a imagem da composição $C \circ \rho$ seja um código diedral. Para verificar que condições precisamos impor sobre estes elementos, precisaremos do seguinte teorema. Afim de facilitar a escrita utilizaremos a seguinte notação:

$$((a\alpha_1^j)_{j\in[0,n-1]}, (b\alpha_2^j)_{j\in[0,n-1]}) = (a\alpha_1^0, ..., a\alpha_1^{n-1}, b\alpha_2^0, ..., b\alpha_2^{n-1}).$$

Teorema 2.4.5. *Se $\alpha \in \overline{\mathbb{F}}_q$ um elemento de ordem n tal que $f_\alpha(x) = f_\alpha^*(x)$, considere $\alpha_1 = \alpha_2^{-1} = \alpha$ e*

$$A = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}^{-1} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$$

$$B = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}^{-1} \begin{pmatrix} u_{21} & u_{22} \\ u_{11} & u_{12} \end{pmatrix}$$

para que $C(\rho(\mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}))$ seja um subcódigo diedral de $\mathbb{F}_q D_{2n}$ é suficiente que A e B pertençam a $GL(\mathbb{F}_q(\alpha + \alpha^{-1}), 2)$.

Demonstração. Suponha que A e B pertença a $GL(\mathbb{F}_q(\alpha + \alpha^{-1}), 2)$. Como ρ é uma transformação linear, temos que $C(\rho(\mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}))$ é um subespaço de $\mathbb{F}_q^{2n}$, assim precisamos mostrar que se A e B cumprem as condições no enunciado, então o código gerado é um código diedral. Para isso, seja $(\beta_1, \beta_2) \in \mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}$, cuja imagem é

$$\begin{aligned} C(\rho(\beta_1, \beta_2)) &= (Tr((u_{11}\beta_1 + u_{12}\beta_2)\alpha_1^j)_{j\in[0,n-1]}, Tr((u_{21}\beta_1 + u_{22}\beta_2)\alpha_2^j)_{j\in[0,n-1]}) \\ &= (Tr((u_{11}\beta_1 + u_{12}\beta_2)\alpha^j)_{j\in[0,n-1]}, Tr((u_{21}\beta_1 + u_{22}\beta_2)\alpha^{-j})_{j\in[0,n-1]}), \end{aligned}$$

precisamos verificar que existem (γ_1, γ_2) e (ω_1, ω_2) em $\mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}$ de tal forma que se cumpram as relações

$$\begin{aligned} C(\rho(\gamma_1, \gamma_2)) &= (Tr((u_{11}\beta_1 + u_{12}\beta_2)\alpha_1^{j-1})_{j\in[0,n-1]}, Tr((u_{21}\beta_1 + u_{22}\beta_2)\alpha_2^{j-1})_{j\in[0,n-1]}) \quad (2.4) \\ &= (Tr((u_{11}\beta_1 + u_{12}\beta_2)\alpha^{j-1})_{j\in[0,n-1]}, Tr((u_{21}\beta_1 + u_{22}\beta_2)\alpha^{-j+1})_{j\in[0,n-1]}) \end{aligned}$$

$$\begin{aligned} C(\rho(\omega_1, \omega_2)) &= (Tr((u_{21}\beta_1 + u_{22}\beta_2)\alpha_2^{-j})_{j\in[0,n-1]}, Tr((u_{11}\beta_1 + u_{12}\beta_2)\alpha_1^{-j})_{j\in[0,n-1]}) \quad (2.5) \\ &= (Tr((u_{21}\beta_1 + u_{22}\beta_2)\alpha^{j})_{j\in[0,n-1]}, (Tr((u_{11}\beta_1 + u_{12}\beta_2)\alpha^{-j}))_{j\in[0,n-1]}) \end{aligned}$$

como

$$\begin{aligned} C(\rho(\gamma_1, \gamma_2)) &= ((Tr((u_{11}\gamma_1 + u_{12}\gamma_2)\alpha^{j})_{j\in[0,n-1]}, Tr((u_{21}\gamma_1 + u_{22}\gamma_2)\alpha^{-j}))_{j\in[0,n-1]}) \\ C(\rho(\omega_1, \omega_2)) &= ((Tr((u_{11}\omega_1 + u_{12}\omega_2)\alpha^{j})_{j\in[0,n-1]}, Tr((u_{21}\omega_1 + u_{22}\omega_2)\alpha^{-j}))_{j\in[0,n-1]}) \end{aligned}$$

é suficiente termos

$$\begin{aligned} u_{11}\gamma_1 + u_{12}\gamma_2 &= (u_{11}\beta_1 + u_{12}\beta_2)\alpha^{-1} \\ u_{21}\gamma_1 + u_{22}\gamma_2 &= (u_{21}\beta_1 + u_{22}\beta_2)\alpha^{1} \end{aligned}$$

daí

$$\begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} u_{11}\alpha^{-1} & u_{12}\alpha^{-1} \\ u_{21}\alpha & u_{22}\alpha \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix},$$

isso implica que

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}^{-1} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = A \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}.$$

Como a matriz $A \in GL(\mathbb{F}_q(\alpha + \alpha^{-1}), 2)$ e $(\beta_1, \beta_2) \in \mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}$, segue que (γ_1, γ_2) pertence a $\mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}$.

Para mostrar a existência de ω_1 e ω_2, precisamos que

$$\begin{aligned} &Tr((u_{11}\omega_1 + u_{12}\omega_2)\alpha^{j}) = Tr((u_{21}\beta_1 + u_{22}\beta_2)\alpha^{j}) \text{ para todo } j \in \{0, \ldots, n-1\} \\ &Tr((u_{21}\omega_1 + u_{22}\omega_2)\alpha^{-j}) = Tr((u_{11}\beta_1 + u_{12}\beta_2)\alpha^{-j}) \text{ para todo } j \in \{0, \ldots, n-1\} \end{aligned}$$

desta forma, para que as igualdades anteriores sejam verdadeira, é suficiente que se cumpram as seguintes relações

$$(u_{11}\omega_1 + u_{12}\omega_2)\alpha^{j} = (u_{21}\beta_1 + u_{22}\beta_2)\alpha^{j}, \text{ para todo } j \in \{0, \ldots, n-1\}$$

$$(u_{21}\omega_1 + u_{22}\omega_2)\alpha^{-j} = (u_{11}\beta_1 + u_{12}\beta_2)\alpha^{-j}, \text{ para todo } j \in \{0, \ldots, n-1\}$$

o que é equivalente ao sistema de equações

$$\begin{aligned} u_{11}\omega_1 + u_{12}\omega_2 &= u_{21}\beta_1 + u_{22}\beta_2 \\ u_{21}\omega_1 + u_{22}\omega_2 &= u_{11}\beta_1 + u_{12}\beta_2. \end{aligned}$$

Reescrevendo o sistema como produto de matrizes obtemos que

$$\begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} u_{21} & u_{22} \\ u_{11} & u_{12} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_1 \end{pmatrix}$$

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}^{-1} \begin{pmatrix} u_{21} & u_{22} \\ u_{11} & u_{12} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_1 \end{pmatrix} = B \begin{pmatrix} \beta_1 \\ \beta_1 \end{pmatrix}$$

Como a matriz B pertence a $\mathbb{F}_q(\alpha+\alpha^{-1})$ segue que (ω_1, ω_2) pertence a $\mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}$. Então A e B pertencem a $GL(\mathbb{F}_q(\alpha+\alpha^{-1}), 2)$ e assim temos que $C(\rho(\mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}))$ é um código diedral de $\mathbb{F}_q^{2n}$. □

Desta forma, basta encontrar uma matriz apropriada

$$\begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$$

que satisfaça as condições do Teorema 2.4.5 para que $C(\rho(\mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}))$ seja um código diedral.

Corolário 2.4.6. *A matriz*

$$\begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} = \begin{pmatrix} 1 & -\alpha \\ 1 & -\alpha^{-1} \end{pmatrix}$$

satisfaz as condições do Teorema 2.4.5.

Demonstração. Seja

$$\begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} = \begin{pmatrix} 1 & -\alpha \\ 1 & -\alpha^{-1} \end{pmatrix},$$

então

$$A = \begin{pmatrix} \frac{-\alpha^{-1}}{\alpha-\alpha^{-1}} & \frac{\alpha}{\alpha-\alpha^{-1}} \\ \frac{-1}{\alpha-\alpha^{-1}} & \frac{1}{\alpha-\alpha^{-1}} \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 1 & -\alpha \\ 0 & -\alpha^{-1} \end{pmatrix} = \begin{pmatrix} \alpha+\alpha^{-1} & -1 \\ 1 & 0 \end{pmatrix}$$

e

$$B = \begin{pmatrix} \frac{-\alpha^{-1}}{\alpha-\alpha^{-1}} & \frac{\alpha}{\alpha-\alpha^{-1}} \\ \frac{-1}{\alpha-\alpha^{-1}} & \frac{1}{\alpha-\alpha^{-1}} \end{pmatrix} \begin{pmatrix} 1 & -\alpha \\ 1 & -\alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

pertencem a $GL(\mathbb{F}_q(\alpha+\alpha^{-1}), 2)$. □

3 Códigos e seus pesos

Um dos problemas mais relevantes da teoria de códigos lineares é determinar a distribuição de pesos de um código C de comprimento n, isto é, encontrar o polinômio enumerador de peso de C, $W_C(x) = A_0 + A_1x + A_2x^2 + \cdots + A_nx^n$, onde A_i é o número de palavras código de peso i em C. Além de ser um problema complexo, a determinação da distribuição de pesos em códigos lineares é também um problema NP-difícil. Isso significa que não existe um algoritmo eficiente conhecido que possa resolver esse problema em tempo polinomial para todos os casos. Mesmo para códigos de comprimento relativamente curto, o número de possíveis palavras-código e suas respectivas distribuições de pesos pode crescer exponencialmente, tornando a sua análise uma tarefa computacionalmente intensiva. Uma ferramenta importante para abordar esse problema é a identidade de MacWilliams, que estabelece uma relação entre os polinômios enumeradores de peso de um código e seu dual. Esta identidade fornece uma maneira eficiente de calcular a distribuição de pesos de um código a partir do seu dual e vice-versa, simplificando bastante a análise em certos casos.

Nesse capítulo, estamos interessados em estudar a distribuição de pesos de códigos cíclicos irredutíveis utilizando a referência [1] e, em seguida, expandir os resultados para códigos diedrais nos casos em que o polinômio teste de paridade $h(x)$ é ou não autorrecíproco. Vemos que o caso não autorrecíproco segue diretamente do cálculo de peso do caso cíclico, desta forma concluímos que tais códigos diedrais são basicamente a concatenação de dois códigos cíclicos. Assim, o caso mais interessante é quando temos um código diedral autorrecíproco, como veremos na subseção 3.2.2.

3.1 Códigos cíclicos irredutíveis

Nesta seção estudaremos os códigos cíclicos com um zero (ver Definição 1.3.10) e Seja $f(x) \in \mathbb{F}_q[x]$ um divisor de $x^n - 1$ e $h(x) = \dfrac{x^n - 1}{f(x)}$ irredutível em $\mathbb{F}_q[x]$ com $deg(h(x)) = m$, onde m é a ordem de $q \mod n$. Esta última condição é técnica e implica que $h(x)$ é um fator irredutível do polinômio ciclotômico $Q_n(x)$, desta forma o código de comprimento n gerado não é redundante. Neste caso $q^m = 1 + ns$ para algum $s \in \mathbb{N}$ e existe θ um gerador adequado de $\mathbb{F}_{q^m}^*$ de tal forma que $\alpha = \theta^s$ é uma raiz de $h(x)$. Como $h(x)$ é irredutível, temos que

$$h(x) = \prod_{i=0}^{m-1} (x - \alpha^{q^i}).$$

Seja $C = \langle f(x) \rangle$ um ideal de $\mathbb{F}_q[x]/(x^n - 1)$ que representa um $[n, m]$-código linear sobre $\mathbb{F}_q$ e $h(x) \in \mathbb{F}_q[x]$ o polinômio teste de paridade do código C. Conforme o Teorema 1.3.11,

podemos expressar o código C da seguinte forma

$$C = \{c(\beta) \mid \beta \in \mathbb{F}_{q^m}\},$$

com

$$c(\beta) = \left(Tr_{m,1}(\beta\alpha^0), Tr_{m,1}(\beta\alpha^1), ..., Tr_{m,1}(\beta\alpha^{(n-1)})\right) \tag{3.1}$$

Por (1.11) o número de coordenadas nulas de $c(\beta)$ é dada por

$$Z(c(\beta)) = \frac{n}{q} + \frac{1}{q}\sum_{j=0}^{n-1}\sum_{a\in\mathbb{F}_q^*}\Psi(a\beta\alpha^{-j}) \tag{3.2}$$

onde $\Psi : \mathbb{F}_{q^m} \to \mathbb{C}$ é o caracter aditivo canônico.

O teorema abaixo nos mostra como calcular o peso de uma palavra do código utilizando a soma de Gauss.

Teorema 3.1.1 (Theorem 11.7.2 [1]). *Para $\beta \in \mathbb{F}_{q^m}^*$, o peso $w(c(\beta))$ da palavra código em (3.1) é*

$$w(c(\beta)) = \frac{q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{i=1}^{d-1}\overline{\chi}_d^i(\beta)G(\chi_d^i)$$

onde χ_d é um caracter multiplicativo de ordem d com $d = mdc\left(\frac{q^m-1}{q-1}, s\right)$ e G é a soma de Gauss.

Demonstração.

$$\begin{aligned} w(c(\beta)) = n - Z(c(\beta)) &= n - \frac{n}{q} - \frac{1}{q}\sum_{a\in\mathbb{F}_q^*}\sum_{j=0}^{n-1}\Psi(a\beta\alpha^{-j}), \text{ usando que } \mathbb{F}_q^* = \langle\theta^{\frac{q^m-1}{q-1}}\rangle \\ &= n - \frac{n}{q} - \frac{1}{q}\sum_{l=0}^{q-2}\sum_{j=0}^{n-1}\Psi(\theta^{\frac{(q^m-1)l}{q-1}}\beta\theta^{-js}). \end{aligned}$$

Como $d = mdc\left(\frac{q^m-1}{q-1}, s\right)$, teremos que $d \left| \left(\frac{q^m-1}{q-1}l - sj\right)\right.$. Assim

$$\frac{(q^m-1)l}{q-1} - sj = d\left(\frac{(q^m-1)l}{d(q-1)} - \frac{sj}{d}\right).$$

Já que o $mdc\left(\frac{(q^m-1)}{d(q-1)}, \frac{s}{d}\right) = 1$, então a combinação linear de $\frac{q^m-1}{q-1}$ e s percorre todas as d-ésimas potências, desta forma temos $\frac{q^m-1}{d}$ d-ésimas potências em $\mathbb{F}_{q^m}^*$. Como $0 \leqslant l \leqslant q-2$ e $0 \leqslant j \leqslant n-1$, teremos $(q-1)n$ d-ésimas potências nesta soma, assim cada d-ésima potência se repete

$$\frac{(q-1)n}{\frac{q^m-1}{d}} = \frac{(q-1)nd}{q^m-1} = \frac{(q-1)d}{s}.$$

As d-ésimas potências em $\mathbb{F}_{q^m}^*$ formam um grupo multiplicativo que denotaremos por C_d e de isso resulta que

$$\sum_{l=0}^{q-2}\sum_{j=0}^{n-1}\Psi(\theta^{\frac{(q^m-1)l}{q-1}}\beta\theta^{-js}) = \frac{(q-1)d}{s}\sum_{x\in C_d}\Psi(\beta x).$$

Tomando $x = y^d$ com $x \in C_d$, a equação $y^d - x = 0$ possui d soluções para y em $\mathbb{F}_{q^m}^*$, então

$$\sum_{x\in C_d}\Psi(\beta x) = \frac{1}{d}\sum_{y\in\mathbb{F}_{q^m}^*}\Psi(\beta y^d). \tag{3.3}$$

Se $\chi_d : \mathbb{F}_{q^m}^* \to \mathbb{C}$ é um caracter multiplicativo de ordem d, então

$$\frac{1}{d}\sum_{i=0}^{d-1}\chi_d^i(z) = \begin{cases} 1, \text{ se } z \text{ é uma } d\text{-ésima potência} \\ 0, \text{ se } z \text{ não é uma } d\text{-ésima potência} \end{cases}$$

Assim podemos reescrever (3.3) da seguinte forma:

$$\begin{aligned}
\sum_{y\in\mathbb{F}_{q^m}^*}\Psi(\beta y^d) &= \sum_{z\in\mathbb{F}_{q^m}^*}\Psi(\beta z)(1+\chi_d(z)+...+\chi_d^{d-1}(z)) \\
&= \sum_{z\in\mathbb{F}_{q^m}^*}\Psi(\beta z) + \sum_{z\in\mathbb{F}_{q^m}^*}\sum_{i=1}^{d-1}\Psi(\beta z)\chi_d^i(z) \\
&= -1 + \sum_{i=1}^{d-1}\sum_{z\in\mathbb{F}_{q^m}^*}\Psi(\beta z)\chi_d^i(\beta z)\overline{\chi}_d^i(\beta) \\
&= -1 + \sum_{i=1}^{d-1}G(\chi_d^i)\overline{\chi}_d^i(\beta),
\end{aligned}$$

portanto temos que

$$\begin{aligned}
w(c(\beta)) = n - Z(c(\beta)) &= n - \frac{n}{q} - \frac{1}{q}\sum_{l=0}^{q-2}\sum_{i=0}^{n-1}\Psi(\theta^{\frac{(q^m-1)l}{q-1}}\beta\theta^{-js}) \\
&= n - \frac{n}{q} - \frac{(q-1)d}{qs}\frac{1}{d}\left(-1 + \sum_{i=1}^{d-1}G(\chi_d^i)\overline{\chi}_d^i(\beta)\right) \\
&= n - \frac{n}{q} + \frac{(q-1)}{qs} - \frac{(q-1)}{qs}\left(\sum_{i=1}^{d-1}G(\chi_d^i)\overline{\chi}_d^i(\beta)\right) \\
&= \frac{q^m-1}{s} - \frac{q^m-1}{qs} + \frac{q-1}{qs} - \frac{(q-1)}{qs}\left(\sum_{i=1}^{d-1}G(\chi_d^i)\overline{\chi}_d^i(\beta)\right) \\
&= \frac{q^m(q-1)}{qs} - \frac{q-1}{qs}\left(\sum_{i=1}^{d-1}G(\chi_d^i)\overline{\chi}_d^i(\beta)\right).
\end{aligned}$$

□

A partir do Teorema 3.1.1 podemos mostrar que existe uma cota inferior para a distância mínima.

Corolário 3.1.2 (Corollary 11.7.3 [1]). *O código cíclico irredutível gerado por $f(x)$ possui distância mínima maior ou igual a*

$$\frac{(q-1)}{qs}(q^m-(d-1)q^{m/2})$$

Demonstração. Segue dos Teoremas 3.1.1 e 1.2.14

$$\begin{aligned} w(c(\beta)) &= \frac{q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{i=1}^{d-1}\overline{\chi}_d^i(\beta)G(\chi_d^i) \\ &\geqslant \frac{q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{i=1}^{d-1}|\overline{\chi}_d^i(\beta)||G(\chi_d^i)| \\ &= \frac{q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{i=1}^{d-1}q^{m/2} \\ &= \frac{q^m(q-1)}{qs} - \frac{(q-1)}{qs}q^{m/2}(d-1)) \\ &= \frac{(q-1)}{qs}(q^m-(d-1)q^{m/2}) \end{aligned}$$

□

Esta cota é atingível quando $G(\chi_d^i) = \chi_d^i(\beta)q^{m/2}$ para todo i, que é conhecido na literatura como soma de Gauss pura, ver [1].

3.2 Códigos diedrais

Sejam $f(x)$ e $h(x)$ polinômios em $\mathbb{F}_q[x]$, de tal forma que $h(x) = \dfrac{x^n-1}{f(x)}$ seja um fator irredutível de $Q_n(x)$ em $\mathbb{F}_q[x]$. Em particular $\deg(h(x)) = m$, onde m é a ordem de $q \mod n$, e daqui temos que $q^m = 1 + ns$ para algum $s \in \mathbb{N}$ e

$$h(x) = \prod_{i=0}^{m-1}(x-\alpha_1^{q^i}).$$

Observação 3.2.1. *Dado que $h(x)$ é um polinômio irredutível em $\mathbb{F}_q[x]$, então $h^*(x)$ é irredutível com* $\deg(h(x)) = \deg(h^*(x)) = m$.

Vamos aproveitar a ideia do cálculo de peso no Teorema 3.1.1 para códigos cíclicos e aplicar este processo para códigos diedrais. Seja α_1 raiz de $h(x)$ e α_2 raiz de $h^*(x)$, com $\alpha_1 = \alpha_2^{-1}$ e $ord(\alpha_1) = ord(\alpha_2) = n$. Seja C a função definida em (2.3), isto é,

$$\begin{array}{rcl} C : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_q^{2n} \\ (\beta_1, \beta_2) & \longmapsto & (Tr(\beta_1\alpha_1^0), ..., Tr(\beta_1\alpha_1^{n-1}), Tr(\beta_2\alpha_2^0), ..., Tr(\beta_2\alpha_2^{n-1})) \end{array} \tag{3.4}$$

com $(\beta_1, \beta_2) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ e $\alpha_1 = \alpha_2^{-1}$.

3.2.1 Código não autorrecíproco

Seja $h(x)$ um polinômio não autorrecíproco, ou seja, $h(x) \neq h^*(x)$, em particular se α_1 é raiz de $h(x)$, então $\alpha_2 = \alpha_1^{-1}$ não é raiz de $h(x)$. Pela Proposição 2.4.4, α_1 e α_2 determinam o código diedral $Im(C)$. Este, por sua vez, será denominado como código diedral não autorrecíproco. A condição de $h(x)$ ser um fator irredutível de $Q_n(x)$ nos garante que o código gerado não é formado por várias cópias de códigos de comprimento menor concatenadas. Podemos escrever as palavras do código $D = Im(C)$ da seguinte forma:

$$C(\beta_1, \beta_2) = (Tr(\beta_1\alpha_1^0), ..., Tr(\beta_1\alpha_1^{n-1}), Tr(\beta_2\alpha_2^0), ..., Tr(\beta_2\alpha_2^{n-1})) \tag{3.5}$$

$$= (Tr(\beta_1\alpha^0), ..., Tr(\beta_1\alpha^{n-1}), Tr(\beta_2\alpha^0), ..., Tr(\beta_2\alpha^{-(n-1)})) \tag{3.6}$$

com $\alpha = \alpha_1 = \alpha_2^{-1}$. Denotando por $Z(C(\beta_1, \beta_2))$ a quantidade de coordenadas nulas da palavra $C(\beta_1, \beta_2)$, sabemos que

$$\begin{aligned} Z(C(\beta_1, \beta_2)) &= |\{0 \leqslant i \leqslant n-1; Tr(\beta_1\alpha_1^i) = 0\}| + |\{0 \leqslant j \leqslant n-1; Tr(\beta_2\alpha_2^j) = 0\}| \\ &= Z(c(\beta_1)) + Z(c(\beta_2)) \\ &= \frac{n}{q} + \frac{1}{q}\sum_{i=0}^{n-1}\sum_{a\in\mathbb{F}_q^*}\Psi(a\beta_1\alpha^i) + \frac{n}{q} + \frac{1}{q}\sum_{j=0}^{n-1}\sum_{a\in\mathbb{F}_q^*}\Psi(a\beta_2\alpha^{-j}) \\ &= \frac{2n}{q} + \frac{1}{q}\left(\sum_{i=0}^{n-1}\sum_{a\in\mathbb{F}_q^*}\Psi(a\beta_1\alpha^i) + \sum_{j=0}^{n-1}\sum_{a\in\mathbb{F}_q^*}\Psi(a\beta_2\alpha^{-j})\right) \end{aligned} \tag{3.7}$$

onde $Z(c(\beta_1))$ e $Z(c(\beta_2))$ denota os zeros da palavra de um código cíclico conforme (3.2). Então a partir da teoria de códigos cíclicos podemos calcular o peso das palavras desses códigos diedrais. Isto é, para fatores não autorrecíprocos de $x^n - 1$ os códigos diedrais são essencialmente concatenação de dois códigos cíclicos de comprimento n. No que segue, estudaremos o caso mais interessante em que o fator de $x^n - 1$ é autorrecíproco, e neste caso o ideal que gera o código no anel de grupos $\mathbb{F}_qD_{2n}$ não é central e não pode ser visto como concatenação de códigos cíclicos.

3.2.2 Código autorrecíproco

Agora vamos fazer o cálculo de peso no caso em que o polinômio $h(x)$ é um polinômio autorrecíproco, ou seja, $h(x) = h^*(x)$. Utilizando a matriz do Corolário 2.4.6,

temos que o número de zeros da palavra $C(\rho(\beta_1,\beta_2))$ com $(\beta_1,\beta_2)\in \mathbb{F}_{q^{\frac{m}{2}}}\times\mathbb{F}_{q^{\frac{m}{2}}}$ é dado por

$$\begin{aligned} Z(C(\rho(\beta_1,\beta_2))) &= Z(C(\beta_1-\alpha\beta_2,\beta_1-\alpha^{-1}\beta_2)) \\ &= \frac{1}{q}\sum_{i=0}^{n-1}\sum_{a\in\mathbb{F}_q}\Psi(a(\beta_1-\alpha\beta_2)\alpha^i)+\frac{1}{q}\sum_{i=0}^{n-1}\sum_{a\in\mathbb{F}_q}\Psi(a(\beta_1-\alpha^{-1}\beta_2)\alpha^{-i}) \\ &= \frac{2n}{q}+\frac{1}{q}\left(\sum_{i=0}^{n-1}\sum_{a\in\mathbb{F}_q^*}\Psi(a(\beta_1-\alpha\beta_2)\alpha^i)+\sum_{j=0}^{n-1}\sum_{a\in\mathbb{F}_q^*}\Psi(a(\beta_1-\alpha^{-1}\beta_2)\alpha^{-j})\right) \end{aligned}$$

Com o objetivo de calcular o peso das palavras, encontramos uma relação entre $\beta_1-\alpha\beta_2$ e $\beta_1-\alpha^{-1}\beta_2$, dada pelo lema abaixo:

Lema 3.2.2. *Dados $(\beta_1,\beta_2)\in\mathbb{F}_{q^{\frac{m}{2}}}\times\mathbb{F}_{q^{\frac{m}{2}}}$, existe $\vartheta\in\mathbb{N}$, com $1\leqslant\vartheta\leqslant q^{\frac{m}{2}}+1$ tal que*

$$\beta_1-\alpha\beta_2=\theta^{(q^{\frac{m}{2}}-1)\vartheta}(\beta_1-\alpha^{-1}\beta_2).$$

Demonstração. Observemos que

$$\left(\frac{\beta_1-\alpha\beta_2}{\beta_1-\alpha^{-1}\beta_2}\right)^{q^{\frac{m}{2}}}=\left(\frac{\beta_1-\alpha^{q^{\frac{m}{2}}}\beta_2}{\beta_1-\alpha^{-q^{\frac{m}{2}}}\beta_2}\right)=\left(\frac{\beta_1-\alpha^{-1}\beta_2}{\beta_1-\alpha\beta_2}\right)$$

isso implica que

$$\left(\frac{\beta_1-\alpha\beta_2}{\beta_1-\alpha^{-1}\beta_2}\right)^{q^{\frac{m}{2}}+1}=1$$

então

$$ord\left(\frac{\beta_1-\alpha\beta_2}{\beta_1-\alpha^{-1}\beta_2}\right)\Big|\left(q^{\frac{m}{2}}+1\right).$$

Seja $\vartheta_0\in\mathbb{N}$ tal que

$$\frac{\beta_1-\alpha\beta_2}{\beta_1-\alpha^{-1}\beta_2}=\theta^{\vartheta_0} \tag{3.8}$$

desta forma temos que

$$ord\left(\frac{\beta_1-\alpha\beta_2}{\beta_1-\alpha^{-1}\beta_2}\right)=\frac{q^m-1}{mdc(q^m-1,\vartheta_0)}$$

logo

$$\frac{q^m-1}{mdc(q^m-1,\vartheta_0)}\Big|(q^{\frac{m}{2}}+1),$$

daí

$$\frac{q^m-1}{q^{\frac{m}{2}}+1}\Big|mdc(q^m-1,\vartheta_0),$$

portanto

$$(q^{\frac{m}{2}}-1)|mdc(q^m-1,\vartheta_0)$$

e temos

$$(q^{\frac{m}{2}}-1)|\vartheta_0.$$

Desta forma

$$\vartheta_0 = (q^{\frac{m}{2}} - 1)\vartheta, \text{ com } 1 \leqslant \vartheta \leqslant q^{\frac{m}{2}} + 1$$

e de (3.8) concluímos que

$$\beta_1 - \alpha\beta_2 = \theta^{(q^{\frac{m}{2}}-1)\vartheta}(\beta_1 - \alpha^{-1}\beta_2).$$

□

O próximo resultado nos apresenta uma forma de calcular o peso das palavras do código diedral.

Teorema 3.2.3. *Seja C um código diedral gerado pelo polinômio autorrecíproco $f(x)$ e suponhamos que $h(x) = \dfrac{x^n - 1}{f(x)}$ seja um fator irredutível de $Q_n(x)|(x^n - 1)$. Então C tem comprimento $2n$, dimensão m e para $(\beta_1, \beta_2) \in \mathbb{F}_{q^{\frac{m}{2}}} \times \mathbb{F}_{q^{\frac{m}{2}}}$, o peso de $C(\rho(\beta_1, \beta_2))$ é dado por*

$$w(C(\rho(\beta_1, \beta_2))) = \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{i=1}^{d-1} G(\chi_d^i)[\overline{\chi}_d^i(\beta_1 - \alpha\beta_2) + \overline{\chi}_d^i(\beta_1 - \alpha^{-1}\beta_2)],$$

onde $s = \dfrac{q^m - 1}{n}$, $d = mdc\left(\dfrac{q^m - 1}{q-1}, s\right) = \dfrac{q^m - 1}{n(q-1)} mdc(n, q-1)$.

Demonstração. Pelo Teorema 3.1.1 temos que

$$\begin{aligned} w(C(\rho(\beta_1, \beta_2))) =& \frac{q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{i=1}^{d-1} \overline{\chi}_d^i(\beta_1 - \alpha\beta_2)G(\chi_d^i) \\ &+ \frac{q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{i=1}^{d-1} \overline{\chi}_d^i(\beta_1 - \alpha^{-1}\beta_2)G(\chi_d^i) \\ =& \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{i=1}^{d-1} G(\chi_d^i)[\overline{\chi}_d^i(\beta_1 - \alpha\beta_2) + \overline{\chi}_d^i(\beta_1 - \alpha^{-1}\beta_2)]. \end{aligned}$$

de onde concluímos o resultado. □

Corolário 3.2.4. *Para $(\beta_1, \beta_2) \in \mathbb{F}_{q^{\frac{m}{2}}} \times \mathbb{F}_{q^{\frac{m}{2}}}$, o código C possui cota inferior para a distância mínima, dada por*

$$w(C(\rho(\beta_1, \beta_2))) \geqslant \frac{(q-1)}{qs}(2q^m - q^{\frac{m}{2}}2(d-1))$$

Demonstração. Segue dos Teoremas 3.2.3 e 1.2.14, e do Lema 3.2.2 que

$$\begin{aligned}
w(C(\rho(\beta_1,\beta_2))) &= \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{j=1}^{d-1} G(\chi_d^j)[\overline{\chi}_d^i(\beta_1-\alpha\beta_2)+\overline{\chi}_d^i(\beta_1-\alpha^{-1}\beta_2)] \\
&= \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{j=1}^{d-1} G(\chi_d^j)[\overline{\chi}_d^j(\beta_1-\alpha^{-1}\beta_2)(\overline{\chi}_d^j(\theta^{(q^{\frac{m}{2}}-1)\vartheta})+1)] \\
&\geqslant \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{j=1}^{d-1} q^{\frac{m}{2}}|\overline{\chi}_d^j(\beta_1-\alpha^{-1}\beta_2)(\overline{\chi}_d^j(\theta^{(q^{\frac{m}{2}}-1)\vartheta})+1)| \\
&= \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}q^{\frac{m}{2}}\sum_{j=1}^{d-1}|\overline{\chi}_d^j(\theta^{(q^{\frac{m}{2}}-1)\vartheta})+1| \\
&\geqslant \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}q^{\frac{m}{2}}2(d-1) \\
&= \frac{(q-1)}{qs}(2q^m - q^{\frac{m}{2}}2(d-1)).
\end{aligned}$$

□

O resultado abaixo nos mostra que o número de pares (β_1,β_2) que satisfazem a relação do Lema 3.2.2 quando fixamos ϑ é uniforme, o que nos permitira calcular a distribuição de pesos do código.

Lema 3.2.5. *Dado $\vartheta \in \mathbb{N}$, com $1 \leqslant \vartheta \leqslant q^{\frac{m}{2}}+1$, existem exatamente $q^{\frac{m}{2}}-1$ pares $(\beta_1,\beta_2) \in \mathbb{F}_{q^{\frac{m}{2}}}^2$, de forma que*

$$\beta_1 - \alpha\beta_2 = \theta^{(q^{\frac{m}{2}}-1)\vartheta}(\beta_1-\alpha^{-1}\beta_2). \tag{3.9}$$

Demonstração. Fixando $\vartheta \in \mathbb{N}$, com $1 \leqslant \vartheta \leqslant q^{\frac{m}{2}}+1$, suponhamos que existe $(\beta_1,\beta_2) \in \mathbb{F}_q^{\frac{m}{2}} \times \mathbb{F}_q^{\frac{m}{2}}$ tal que

$$\beta_1-\alpha\beta_2 = \theta^{(q^{\frac{m}{2}}-1)\vartheta}(\beta_1-\alpha^{-1}\beta_2) \Rightarrow \beta_1(1-\theta^{(q^{\frac{m}{2}}-1)\vartheta}) = \beta_2(\alpha-\alpha^{-1}\theta^{(q^{\frac{m}{2}}-1)\vartheta})$$

então

$$\frac{\beta_1}{\beta_2} = \frac{(\alpha-\alpha^{-1}\theta^{(q^{\frac{m}{2}}-1)\vartheta})}{(1-\theta^{(q^{\frac{m}{2}}-1)\vartheta})}$$

Observemos que a segunda parte da igualdade é constante, pois ϑ é fixo, então se tivermos outra solução β_1',β_2', teremos a seguinte relação:

$$\frac{\beta_1}{\beta_2} = \frac{\beta_1'}{\beta_2'}$$

mas isso acontece se, e somente se,

$$\beta_1' = \beta_1\lambda \text{ e } \beta_2' = \beta_2\lambda \text{ com } \lambda \in \mathbb{F}_{q^{\frac{m}{2}}}^*. \tag{3.10}$$

Isto é, no caso que (3.9) tiver uma solução, então esta equação possui exatamente $q^{\frac{m}{2}}-1$ soluções, pois λ pode variar por $\mathbb{F}^*_{q^{\frac{m}{2}}}$. Desta forma sabemos que a equação (3.9) possui ou 0 ou $q^{\frac{m}{2}}-1$ soluções. Observemos que o número total de pares (β_1,β_2) não nulos possíveis é $q^{\frac{m}{2}}.q^{\frac{m}{2}}-1=q^m-1$, e podemos organizar os pares (β_1,β_2) em conjuntos com $q^{\frac{m}{2}}-1$ elementos de forma que, cada conjunto se associe por (3.9) a um único ϑ, então a quantidade de ϑ associados esses conjuntos é igual a $\dfrac{q^m-1}{q^{\frac{m}{2}}-1}=q^{\frac{m}{2}}+1$. Assim concluímos que para todo ϑ, existem $q^{\frac{m}{2}}-1$ pares (β_1,β_2) que satisfazem (3.9), como queríamos. □

Lema 3.2.6. *Sejam $\beta_1,\beta_2\in\mathbb{F}_{q^{\frac{m}{2}}}$, α, θ e ϑ definidos como no lema anterior, i.e, $\beta_1-\alpha\beta_2=\theta^{(q^{m/2}-1)\vartheta}(\beta_1-\alpha^{-1}\beta_2)$. Se l é um inteiro com $1\leqslant l\leqslant q^m-1$ de forma que $\beta_1-\alpha^{-1}\beta_2=\theta^l$, então*

$$l\equiv\vartheta \pmod{q^{\frac{m}{2}}+1}.$$

Demonstração. Seja $\beta_1-\alpha^{-1}\beta_2=\theta^l$, com $1\leqslant l\leqslant q^m-1$ então

$$\beta_1^{q^{\frac{m}{2}}}-\alpha^{-q^{\frac{m}{2}}}\beta_2^{q^{\frac{m}{2}}}=\theta^{lq^{\frac{m}{2}}}$$

$$\beta_1-\alpha^{-q^{\frac{m}{2}}}\beta_2=\theta^{lq^{\frac{m}{2}}}$$

como α é conjugado de α^{-1}, então $\alpha^{-1}=\alpha^{q^{\frac{m}{2}}}$ e com isso

$$\beta_1-\alpha\beta_2=\theta^{lq^{\frac{m}{2}}}$$

e

$$\frac{\beta_1-\alpha\beta_2}{\beta_1-\alpha^{-1}\beta_2}=\theta^{l(q^{\frac{m}{2}}-1)}$$

por (3.9), temos que

$$\theta^{l(q^{\frac{m}{2}}-1)}=\theta^{\vartheta(q^{\frac{m}{2}}-1)}.$$

Como a ordem de θ é q^m-1 segue que

$$l(q^{m/2}-1)\equiv\vartheta(q^{m/2}-1) \pmod{q^m-1}.$$

Simplificando nesta igualdade o fator $(q^{m/2}-1)$ segue que

$$l\equiv\vartheta \pmod{q^{\frac{m}{2}}+1} \text{ com } 1\leqslant l\leqslant q^m-1. \tag{3.11}$$

□

Observação 3.2.7. *É importante observar que, com base nos lemas anteriores, depois de determinar os pesos possíveis que aparecem, a distribuição de pesos do código pode ser obtida de forma direta a partir de uma função que depende unicamente de ϑ, i.e., a frequência de cada peso depende unicamente de ϑ.*

Lema 3.2.8. *O código diedral autorrecíproco possui no máximo $d+1$ valores para o peso de suas palavras.*

Demonstração. O peso de um palavra varia conforme a escolha do β_1, β_2, e cada um destes pares está dentro do conjunto $\mathbb{F}_{q^{\frac{m}{2}}} \times \mathbb{F}_{q^{\frac{m}{2}}}$. Pelo Teorema 3.2.3, observamos que no cálculo do peso, a parte que depende desta escolha de par é

$$\overline{\chi}_d^j(\beta_1 - \alpha^{-1}\beta_2)((\overline{\chi}_d^j(\theta^{(q^{\frac{m}{2}}-1)\vartheta}) + 1).$$

Sendo $\beta_1 - \alpha^{-1}\beta_2 = \theta^l$, segue que

$$\overline{\chi}_d^j(\beta_1 - \alpha^{-1}\beta_2)(\overline{\chi}_d^j(\theta^{(q^{\frac{m}{2}}-1)\vartheta}) + 1) = e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1).$$

Suponhamos $0 < l_1 < d$, se $l \equiv l_1 \pmod{d}$, consideremos $l = l_1 + dn_1$ para algum $n_1 \in \mathbb{Z}$, então

$$e^{-\frac{2\pi ij}{d}l_1}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1) = e^{-\frac{2\pi ij}{d}(l_1+dn_1)}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1) = e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1)$$

como

$$l \equiv \vartheta \pmod{q^{\frac{m}{2}} + 1} \text{ e } 1 \leqslant l \leqslant q^m - 1$$

existe $l_0 \in \mathbb{Z}$ com

$$l = \vartheta + l_0(q^{\frac{m}{2}} + 1)$$

com isso

$$\begin{aligned} e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1) &= e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)(l-l_0(q^{\frac{m}{2}}+1))} + 1) \\ &= e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)l} + 1) \\ &= e^{-\frac{2\pi ij}{d}q^{\frac{m}{2}}l} + e^{-\frac{2\pi ij}{d}l} \end{aligned}$$

então a partir da seguinte igualdade

$$e^{-\frac{2\pi ij}{d}l_1}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1) = e^{-\frac{2\pi ij}{d}q^{\frac{m}{2}}l} + e^{-\frac{2\pi ij}{d}l}$$

podemos concluir que há no máximo $d+1$ valores possíveis para o peso de uma palavra. □

Devido a dificuldade de calcular a soma de Gauss, procuramos alguns casos particulares de códigos diedrais, que possibilite calcular o peso com maior facilidade.

Teorema 3.2.9. *Seja $\beta_1 - \alpha^{-1}\beta_2 = \theta^l$ para algum $l \in \mathbb{N}$, $d > 2$, suponhamos que existe um inteiro positivo t tal que $p^t \equiv -1 \pmod{d}$, e tomemos t o menor inteiro possível. Então existem inteiros s_0 e ϑ com $m = 2ts_0$ e $l \equiv \vartheta \pmod{q^{\frac{m}{2}} + 1}$ conforme 3.11, de forma que*

$$w(C(\rho(\beta_1, \beta_2))) = \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sqrt{q^m}\sum_{j=1}^{d-1}(-1)^j[e^{-\frac{2\pi ij}{d}q^{\frac{m}{2}}l} + e^{-\frac{2\pi ij}{d}l}]$$

se d é par, e q, s_0 e $\dfrac{q^t+1}{d}$ são ímpares. Caso contrário teremos

$$w(C(\rho(\beta_1, \beta_2))) = \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sqrt{q^m}\sum_{j=1}^{d-1}(-1)^{s_0-1}[e^{-\frac{2\pi ij}{d}q^{\frac{m}{2}}l} + e^{-\frac{2\pi ij}{d}l}].$$

Demonstração. Se χ é um caracter de ordem d em $\mathbb{F}_{q^m}$ para algum inteiro positivo m. Sendo $\beta_1 - \alpha^{-1}\beta_2 = \theta^l$, então

$$\overline{\chi}_d^j(\beta_1 - \alpha^{-1}\beta_2)(\overline{\chi}_d^j(\theta^{(q^{\frac{m}{2}}-1)\vartheta}) + 1) = e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1)$$

substituindo no Teorema 3.2.3 e aplicando o Teorema 1.2.18, segue que

$$w(C(\rho(\beta_1,\beta_2))) = \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{j=1}^{d-1}(-1)^j\sqrt{q^m}[e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1)]$$

se d é par, e q, s_0 e $\dfrac{q^t+1}{d}$ são ímpares. Caso contrário teremos

$$w(C(\rho(\beta_1,\beta_2))) = \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{j=1}^{d-1}(-1)^{s_0-1}\sqrt{q^m}[e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1)]$$

como

$$\begin{aligned} e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)(l+(q^{\frac{m}{2}}+1))} + 1) &= e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)l}e^{-\frac{2\pi ij}{d}(q^m-1)} + 1) \\ &= e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)l} + 1) \\ &= e^{-\frac{2\pi ij}{d}q^{\frac{m}{2}}l} + e^{-\frac{2\pi ij}{d}l} \end{aligned}$$

segue o resultado. □

Exemplo 3.2.10. *Seja $q = 5$, $d = 3$, $s = 3$ $m = 2$, $s_0 = 1$, então $t = 1$, $n = 8$ e $(q,n) = 1$, segue do Teorema 3.2.9 que*

$$\begin{aligned} w(C(\rho(\beta_1,\beta_2))) &= \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sqrt{q^m}\sum_{j=1}^{d-1}(-1)^{s_0-1}[e^{-\frac{2\pi ij}{d}q^{\frac{m}{2}}l} + e^{-\frac{2\pi ij}{d}l}]. \\ &= \frac{2.5^2(5-1)}{5.3} - \frac{(5-1)}{5.3}\sum_{j=1}^{3-1}(-1)^{1-1}\sqrt{5^2}[e^{-\frac{10\pi ij}{3}l} + e^{-\frac{2\pi ij}{3}l}] \\ &= \frac{40}{3} - \frac{4}{15}\sum_{j=1}^{3-1}5[e^{-\frac{10\pi ij}{3}l} + e^{-\frac{2\pi ij}{3}l}] \\ &= \frac{40}{3} - \frac{4}{3}\sum_{j=1}^{2}[e^{-\frac{4\pi ij}{3}l} + e^{-\frac{2\pi ij}{3}l}] \end{aligned}$$

a antepenúltima igualdade vem do Lema 3.11, que nos dá $l = 6l_0 + \vartheta$ com $1 \leqslant l_0 \leqslant 4$ e $1 \leqslant \vartheta \leqslant 6$. Como

$$e^{-\frac{4\pi ij}{3}\vartheta} + e^{-\frac{2\pi ij}{3}\vartheta} = \begin{cases} 2 & \text{se } 3 \mid \vartheta \\ -1 & \text{se } 3 \nmid \vartheta \end{cases}$$

então para $\vartheta = 3$ ou 6 temos

$$\frac{40}{3} - \frac{4}{3}\sum_{j=1}^{2}[e^{-\frac{4\pi ij}{3}\vartheta} + e^{-\frac{2\pi ij}{3}\vartheta}] = \frac{40}{3} - \frac{4}{3}\sum_{j=1}^{2}2 = \frac{24}{3} = 8,$$

e para $\vartheta = 1, 2, 4$ *ou* 5 *temos*

$$\frac{40}{3} - \frac{4}{3}\sum_{j=1}^{2}[e^{-\frac{4\pi ij}{3}\vartheta} + e^{-\frac{2\pi ij}{3}\vartheta}] = \frac{40}{3} - \frac{4}{3}\sum_{j=1}^{2} -1 = \frac{48}{3} = 16,$$

isto é, para 4 *valores de* ϑ*, possuiremos palavras de peso* 16 *e para* 2 *valores de* ϑ *teremos palavras de peso* 8*. Pelo Lema 3.2.5, segue que*

$$4(q^{\frac{m}{2}} - 1) = 4 \times 4 = 16$$

é a quantidade de palavras de peso igual a 16 e

$$2(q^{\frac{m}{2}} - 1) = 2 \times 4 = 8$$

é a quantidade de palavras de peso igual a 8.

Corolário 3.2.11. *Nas mesma condições do Teorema 3.2.9, se* $\dfrac{\vartheta}{d}$ *for inteiro e* s_0 *for ímpar, teremos que*

$$w(C(\rho(\beta_1, \beta_2))) = \frac{2(q^m + \sqrt{q^m})(q-1)}{qs}$$

se d *é par, e* q *e* $\dfrac{q^t + 1}{d}$ *são ímpares. Caso contrário teremos*

$$w(C(\rho(\beta_1, \beta_2))) = \frac{2(q-1)(q^m - (d-1)(-1)^{s_0 - 1}\sqrt{q^m})}{qs}.$$

Demonstração. Observe que $q^{\frac{m}{2}} + 1 = q^{ts_0} + 1 = (-1)^{s_0} + dk + 1$, para algum $k \in \mathbb{N}$, então se s_0 for ímpar, $q^{\frac{m}{2}} + 1$ será divisível por d. Assim

$$[e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1)] = [e^{-\frac{2\pi ij}{d}(l_0(q^{\frac{m}{2}}+1)+\vartheta))}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1)]$$

$$= [e^{-\frac{2\pi ij}{d}\vartheta}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta} + 1)] = 1(1+1) = 2,$$

e no caso que d for par, a soma ser reduz a

$$\sum_{j=1}^{d-1}(-1)^j\sqrt{q^m} = -\sqrt{q^m}.$$

□

Exemplo 3.2.12. *Seja* $q = 7$*,* $d = 5$*,* $s = 15$*,* $m = 4$*,* $s_0 = 1$*, então* $t = 2$*,* $n = 160$*,* $(q, n) = 1$*, Observe que* $7^2 + 1$ *é divisível por* 5 *e* $1 \leqslant \vartheta \leqslant 50$*, então pelo Corolário 3.2.11, para*

$$\vartheta = 5, 10, 15, 20, 25, 30, 35, 40, 45 \text{ ou } 50$$

temos

$$w(C(\rho(\beta_1,\beta_2))) = \frac{2(q-1)(q^m-(d-1)(-1)^{s_0-1}\sqrt{q^m})}{qs}$$
$$= \frac{2(7-1)(7^4-4(-1)^{1-1}\sqrt{7^4})}{7\cdot 15} = 252$$

e pelo Lema 3.2.5, há

$$10(q^{\frac{m}{2}}-1) = 10(7^2-1) = 480$$

palavras com peso igual a 252 *e para os outros valores de* ϑ *temos*

$$w(C(\rho(\beta_1,\beta_2))) = \frac{2q^m(q-1)}{qs} - \frac{(q-1)}{qs}\sum_{j=1}^{d-1}(-1)^{s_0-1}\sqrt{q^m}[e^{-\frac{2\pi ij}{d}l}(e^{-\frac{2\pi ij}{d}(q^{\frac{m}{2}}-1)\vartheta}+1)].$$

$$= \frac{2\cdot 7^4(7-1)}{7\cdot 15} - \frac{(7-1)}{7\cdot 15}\sum_{j=1}^{5-1}(-1)^{1-1}\sqrt{7^4}[e^{-\frac{2\pi ij}{5}l}(e^{-\frac{2\pi ij}{5}(7^{\frac{4}{2}}-1)\vartheta}+1)]$$
$$= \frac{4116}{15} - \frac{6}{105}\sum_{j=1}^{4}49[e^{-\frac{2\pi ij}{5}l}(e^{-\frac{2\pi ij}{5}48\vartheta}+1)]$$
$$= \frac{4116}{15} - \frac{42}{15}\sum_{j=1}^{4}[e^{-\frac{2\pi ij}{5}l}(e^{-\frac{2\pi ij}{5}8\vartheta}+1)]$$
$$= \frac{4116}{15} - \frac{42}{15}(\sum_{j=1}^{4}e^{-\frac{2\pi ij}{5}(8\vartheta+l)} + \sum_{j=1}^{4}e^{-\frac{2\pi ij}{5}l})$$
$$= \frac{4116}{15} - \frac{42}{15}(\sum_{j=1}^{4}e^{-\frac{2\pi ij}{5}(8\vartheta+50l_0+\vartheta)} + \sum_{j=1}^{4}e^{-\frac{2\pi ij}{5}(50l_0+\vartheta))})$$
$$= \frac{4116}{15} - \frac{42}{15}(\sum_{j=1}^{4}e^{-\frac{2\pi ij}{5}9\vartheta} + \sum_{j=1}^{4}e^{-\frac{2\pi ij}{5}\vartheta})$$
$$= \frac{4116}{15} - \frac{42}{15}(\sum_{j=1}^{4}e^{-\frac{8\pi ij}{5}\vartheta} + \sum_{j=1}^{4}e^{-\frac{2\pi ij}{5}\vartheta})$$
$$= \frac{4116}{15} - \frac{42}{15}(-1-1) = 280$$ *e pelo Lema 3.2.5, há*

$$40(q^{\frac{m}{2}}-1) = 1920$$

palavras com peso igual a 280*. Assim, o polinômio enumerador de peso de* C *é dado por* $W_C(x) = 1 + 480x^{252} + 1920x^{280}$.

O próximo teorema nos dá o valor do peso de $w(C(\rho(\beta_1,\beta_2)))$ para as palavras do código C.

Teorema 3.2.13. *Suponhamos que* $q = p^r$ *ímpar, com* $r = 2s_0$ *para algum inteiro* s_0 *e que o valor de* d *no Teorema 3.2.3 é igual a 2. Então para* $(\beta_1,\beta_2) \in \mathbb{F}_{q^{m/2}} \times \mathbb{F}_{q^{m/2}}$*, temos que*

$$w(C(\rho(\beta_1,\beta_2))) = \frac{2q^m(q-1)}{qs} + 2\epsilon\frac{(q-1)}{qs}\left(\frac{-1}{p}\right)^{s_0 m}\sqrt{q^m},$$

em que

$$\epsilon = \begin{cases} 1 & \text{se } (\beta_1 - \alpha^{-1}\beta_2) \text{ é um quadrado em } \mathbb{F}_{q^m} \\ -1 & \text{caso contrário.} \end{cases}$$

Demonstração. Pelos Teoremas 11.5.2 e 11.5.4 de [1], segue que

$$G_m(\chi_2) = -\left(\frac{-1}{p}\right)^{s_0 m}\sqrt{q^m},$$

e pelo Lema 3.2.2, sabemos que

$$\beta_1 - \alpha\beta_2 = \theta^{(q^{\frac{m}{2}}-1)\vartheta}(\beta_1 - \alpha^{-1}\beta_2),$$

como q é ímpar, então $q^{s_0} - 1$ é par, assim $q^{s_0} - 1 = 2z$ para algum $z \in \mathbb{Z}$, ja que χ_2 é o caracter quadrático, segue que

$$\chi_2(\theta^{(q^{s_0}-1)\vartheta}) = \chi_2((\theta^{z\vartheta})^2) = 1.$$

Aplicando estes resultandos no Teorema 3.2.3 e substituindo $d = 2$, concluímos o resultado. □

Corolário 3.2.14. *Considere um código C para o qual $q = p^{2s_0}$, $m = 2$. Nas condições do Teorema 3.2.13, para todo par $(\beta_1, \beta_2) \in \mathbb{F}_q^2$ não nulo, garante que*

$$w(C(\rho(\beta_1, \beta_2))) = \begin{cases} \dfrac{2(q^2-1)}{s} & \text{se } (\beta_1 - \alpha^{-1}\beta_2) \text{ é um quadrado em } \mathbb{F}_{q^m} \\ \dfrac{2(q-1)^2}{s} & \text{caso contrário.} \end{cases}$$

Demonstração. Pelo Teorema 3.2.13 temos que o peso de cada palavra com peso diferente de zero é dado por $\dfrac{2q^2(q-1)}{qs} + 2\epsilon\dfrac{(q-1)}{qs}\left(\dfrac{-1}{p}\right)^{s_0 2} = \dfrac{2q(q-1)}{s} + 2\epsilon\dfrac{(q-1)}{qs}q = \dfrac{2q(q-1)}{s} + 2\epsilon\dfrac{(q-1)}{s} = \dfrac{2(q-1)(q+\epsilon)}{s}$. □

Observação 3.2.15. *Vejamos que as condições do corolário anterior, caso existam elementos da forma $\beta_1 - \alpha^1\beta_2$ que não sejam quadrados em $\mathbb{F}_{q^m}$, se tem que $\dfrac{2(q-1)^2}{s}$ é inteiro. De fato, observemos que*

$$s \mid q^m - 1 = \frac{q^m - 1}{q-1}(q-1),$$

e daqui segue que

$$\frac{s}{mdc\left(\frac{q^m-1}{q-1}, s\right)} \mid (q-1)$$

Como $mdc\left(\dfrac{q^m-1}{q-1}, s\right) = d = 2$, isso implica

$$\frac{s}{2} \mid (q-1)$$

assim concluímos que $\dfrac{2(q-1)^2}{s}$ é sempre inteiro.

Exemplo 3.2.16. *Considere um código C para o qual $q = 9$, $n = 5$, $m = 2$, $s = 16$, $d = 2$, e $s_0 = 1$. O Corolário 3.2.14, para todo par $(\beta_1, \beta_2) \in \mathbb{F}_9^2$ não nulo, garante que*

$$w(C(\rho(\beta_1, \beta_2))) = \begin{cases} 10, & \text{se } (\beta_1 - \alpha^{-1}\beta_2) \text{ é um quadrado} \\ 8, & \text{caso contrário.} \end{cases}$$

e $W_C(x) = 1 + 40x^8 + 40x^{10}$.

4 Considerações Finais

Neste trabalho construímos de forma explicita códigos diedrais de comprimento $|D_{2n}| = 2n$, que são ideais a esquerda da álgebra de grupos $\mathbb{F}_q D_{2n}$. Para esta construção, realizamos duas abordagens. A primeira é usando a construção explícita de um homomorfismo de $\mathbb{F}_q D_{2n}$ com sua decomposição de Wedderburn. A segunda é usando extensões algébricas adequadas de corpo $\mathbb{F}_q$ de grau $m = ord_n q$, e construindo uma transformação $\mathbb{F}_q$-linear de $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ para o $\mathbb{F}_q$-espaço $2n$ dimensional $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$ conforme demonstrado na Proposição 2.4.4. É mostrado que as duas abordagens são equivalentes, no seguindo que todo código diedral pode ser construído por estes dois métodos.

Ressaltamos que, o a segunda abordagem já tem sido usada de forma clássica para a construção de códigos cíclicos lineares. Apesar desta técnica precisar do uso da função traço da extensão, essa forma é útil para encontrar fórmulas fechadas (não necessariamente simples) para o peso de uma palavra. Na prática, calcular o peso de uma palavra particular por este método não é a melhor técnica que pode ser usada, mas ela serve para medir de alguma forma quantas palavras têm um peso dado, o que nos permite em alguns casos encontrar a distribuição de pesos do código.

Neste trabalho foi determinado a distribuição de pesos de alguns códigos diedrais determinados por ideais à esquerda não centrais, que são gerados por algum fator irredutível de $x^n - 1$ autorrecíproco. Observamos que o caso de fatores não autorrecíprocos, o código diedral gerado é de fato uma concatenação de dois códigos cíclicos de comprimento n.

Quando o código é gerado por um fator não irredutível, a distribuição de pesos, mesmo de códigos cíclicos é um problema aberto para o caso geral, somente feito para alguns códigos gerados por polinômios com dois ou três fatores que cumprem alguma condição especial. Já no caso de códigos diedrais com dois o mais zeros, o problema é totalmente aberto.

Uma das contribuições destacadas nesta pesquisa foi mostrar como calcular a distribuição de peso de determinados códigos diedrais gerados por um fator irredutível. Para dar continuidade a esta pesquisa, propomos iniciar o desenvolvimento de códigos diedrais cujo polinômio teste de paridade $h(x)$ possui dois ou mais fatores irredutíveis, com algumas condições especiais que nos permitam o cálculo das somas de Gauss que devem aparecer nas expresões do cálculo dos pesos. Além disso, temos a intenção de explorar a aplicabilidade dessa teoria para códigos quatérnios.

Outra linha de pesquisa é determinar a distribuição de pesos códigos de grupos que são ideais a esquerda da álgebra de grupos $\mathbb{F}_q G$ onde G é um grupo com alguma

estrutura adequada. Um desses caso é quanto o grupo é metacíclico, onde é conhecida explicitamente a decomposição de Wedderburn na álgebra.

Referências

[1] Berndt, B. C., Williams, K. S., and Evans, R. J. Gauss and jacobi sums. Citado 11 vezes nas páginas 9, 10, 16, 21, 24, 25, 26, 43, 44, 46 e 56.

[2] Borello, M., and Jamous, A. Dihedral codes with prescribed minimum distance. In *International Workshop on the Arithmetic of Finite Fields* (2020), Springer, pp. 147–159. Citado na página 10.

[3] Brochero Martínez, F. Structure of finite dihedral group algebra. *Finite Fields and Their Applications 35* (2015), 204–214. Citado 4 vezes nas páginas 10, 30, 33 e 35.

[4] Delsarte, P. On subfield subcodes of modified reed-solomon codes (corresp.). *IEEE Transactions on Information Theory 21*, 5 (1975), 575–576. Citado na página 9.

[5] Ding, C., and Yang, J. Hamming weights in irreducible cyclic codes. *Discrete Mathematics 313*, 4 (2013), 434–446. Citado na página 10.

[6] Dinh, H. Q., Li, C., and Yue, Q. Recent progress on weight distributions of cyclic codes over finite fields. *Journal of Algebra Combinatorics Discrete Structures and Applications 2*, 1 (2015), 39–63. Citado na página 10.

[7] Ferraz, R. A., Milies, C. P., and Taufer, E. Left ideals of matrix rings and error-correcting codes. *Applicable Algebra in Engineering, Communication and Computing 32*, 3 (2021), 311–320. Citado na página 36.

[8] Gao, Y., Yue, Q., and Wu, Y. Lcd codes and self-orthogonal codes in generalized dihedral group algebras. *Designs, Codes and Cryptography 88*, 11 (2020), 2275–2287. Citado na página 10.

[9] Garcia, A., and Lequain, Y. Elementos de algebra, 6a ediçao. *Editora SBM* (2015). Citado na página 18.

[10] Hefez, A., and Villela, M. L. T. *Códigos corretores de erros*. Instituto de Matematica Pura e Aplicada, 2008. Citado 3 vezes nas páginas 9, 12 e 13.

[11] Lidl, R., and Niederreiter, H. *Introduction to finite fields and their applications*. Cambridge university press, 1994. Citado 9 vezes nas páginas 9, 11, 12, 14, 15, 16, 17, 18 e 20.

[12] Milies, C. P., and Sehgal, S. K. *An introduction to group rings*, vol. 1. Springer Science & Business Media, 2002. Citado na página 34.

[13] Olteanu, G., and Van Gelder, I. Construction of minimal non-abelian left group codes. *Designs, Codes and Cryptography 75*, 3 (2015), 359–373. Citado na página 10.

[14] Stichtenoth, H. *Algebraic function fields and codes*, vol. 254. Springer Science & Business Media, 2009. Citado na página 9.