BERTHA GISELLE LEON BENITEZ

Códigos cíclicos lineares com dual complementar sobre anéis finitos de característica ímpar

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2023

BERTHA GISELLE LEON BENITEZ

Códigos cíclicos lineares com dual complementar sobre anéis finitos de característica ímpar

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Teoria de códigos e corpos finitos.

Orientador: Prof.Dr.Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG 2023

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

B467
2023

Benitez, Bertha Giselle Leon, 1995-
Códigos cíclicos lineares com dual complementar sobre anéis finitos de característica ímpar [recurso eletrônico] / Bertha Giselle Leon Benitez. - 2023.

Orientador: Victor Gonzalo Lopez Neumann.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2023.408
Inclui bibliografia.

1. Matemática. I. Neumann, Victor Gonzalo Lopez,1974-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 160 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.posgrad.famat.ufu.br - pgmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 111, PPGMAT				
Data:	31 de julho de 2023	Hora de início:	10:00	Hora de encerramento:	11:30
Matrícula do Discente:	12122MAT001				
Nome do Discente:	Bertha Giselle Leon Benitez				
Título do Trabalho:	Códigos cíclicos lineares com dual complementar sobre anéis finitos de características ímpar				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Estudo de elementos primitivos e normais em corpos finitos				

Reuniu-se na Sala Multiuso da Biblioteca (Campus Santa Mônica) da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Abílio Lemos Cardoso Júnior - UFV; Guilherme Chaud Tizziotti - FAMAT/UFU e Victor Gonzalo Lopez Neumann - FAMAT/UFU, orientador da candidata.

Iniciando os trabalhos o presidente da mesa, Dr. Victor Gonzalo Lopez Neumann, apresentou a Comissão Examinadora e a candidata, agradeceu a presença do público, e concedeu a Discente a palavra para a exposição do seu trabalho. A duração da apresentação da Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir a candidata. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando a candidata:

Aprovada.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Guilherme Chaud Tizziotti**, **Professor(a) do Magistério Superior**, em 31/07/2023, às 11:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 31/07/2023, às 11:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Abílio Lemos Cardoso Júnior**, **Usuário Externo**, em 31/07/2023, às 17:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4680988** e o código CRC **21EC980B**.

Referência: Processo nº 23117.053201/2023-01 SEI nº 4680988

Dedicatória

À memória da minha querida avó e a minha amada mãe

Agradecimentos

Agradeço, primeiramente à Deus por me dar força, ser meu apoio, minha luz e meu caminho. Agradeço por colocar pessoas maravilhosas em meu caminho, que me acolheram neste país e me ofereceram sua amizade, apoio moral e estímulos com infinito amor e confiança.

Agradeço à minha incondicional e amada mãe, Yolanda Benitez, que mesmo à distância esteve presente a cada dia, celebrando minhas alegrias e me apoiando para superar os obstáculos e momentos difíceis.

Agradeço à minha família por me inspirar nos estudos, que iniciei com toda a responsabilidade que representa chegar ao fim desta etapa. Tenho admiração e respeito por cada um dos membros da família, que confiaram em mim e me ofereceram seu apoio incondicional. Em especial, agradeço à minha tia Bertha Helena Benitez, minha irmã Viviana León e meus adoráveis sobrinhos Tatiana e Kevin. Eles são o motor que me impulsiona a seguir todos os dias.

Agradeço à Universidade Federal de Uberlândia (UFU) por permitir que eu alcance esta meta, tornando-me uma profissional no campo que tanto me apaixona. A UFU possibilitou o conhecimento, as técnicas e a experiência adquirida por meio dos estudos e pesquisas.

Agradeço ao meu orientador, Victor G Lopez Neumann, que dedicou incondicionalmente seu tempo e conhecimento na orientação da minha tese de graduação. Sem ele, não teria sido possível concluí-la. Agradeço por seu infinito compromisso, disposição e, acima de tudo na sua humanidade, sempre disponível para ajudar as pessoas.

Agradeço aos docentes por sua meritória dedicação, experiência e compromisso. Suas lições e orientações fizeram parte da minha formação integral.

A Daniela Bermudez, agradeço infinitamente por tornarem minha estadia aqui no Brasil muito mais agradável e amena, por estarem ao meu lado todas as vezes em que eu me sentia desfalecer e por me ajudarem a me reerguer. A Josimar Joao Ramirez, Giovanny Barrera, Julian Carillo e Alejandra Herrera por deixarem marcas indeléveis em minha vida. Agradeço por sua paciência, compreensão e apoio incondicional. Agradeço por compartilharem meus triunfos.

Agradeço à CAPES pelo auxílio financeiro durante todo o período do mestrado.

Agradeço finalmente aos professores Guilherme Chaud Tizziotti e Abílio Lemos Cardoso Júnior por aceitarem o convite de fazerem parte da minha banca.

LEÓN BENITEZ, B. G. *Códigos cíclicos lineares com dual complementar sobre anéis finitos de característica ímpar.* 2023. x+38 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho, investigamos os códigos cíclicos em um anel finito não encadeado $R = \mathbb{F}_q[x]/(x^2-1)$. Denotando por v a classe de x nesse quociente, temos $R = \mathbb{F}_q + v\mathbb{F}_q$, em que $v^2 = 1$. Estabelecemos condições suficientes e necessárias para um código sobre R ser considerado um código linear com dual complementar (LCD). Além disso, exploramos as propriedades do código dual e seu relacionamento com os códigos LCD. Demonstramos que a função de Gray de um código LCD de comprimento n em $\mathbb{F}_q + v\mathbb{F}_q$ resulta em um código LCD de comprimento $2n$ em $\mathbb{F}_q^{2n}$, e outras propriedades deles.

Palavras-chave: Anel não encadeado, Código cíclico, Código dual, Código LCD, Código reversível e Função de Gray.

LEÓN BENITEZ, B. G. *Linear cyclic codes with dual complement over finite rings of odd characteristic.* 2023. x+38 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we investigate cyclic codes in a finite non-chain ring $R = \mathbb{F}_q[x]/(x^2 - 1)$. Denoting by v the class of x in this quotient, we have $R = \mathbb{F}_q + v\mathbb{F}_q$, where $v^2 = 1$. We establish sufficient and necessary conditions for a code over R to be considered a linear code with dual complement (LCD). Furthermore, we explore the properties of the dual code and its relationship with LCD codes. We demonstrate that the Gray map of an LCD code of length n in $\mathbb{F}_q + v\mathbb{F}_q$ results in an LCD code of length $2n$ in $\mathbb{F}_q^{2n}$, and other properties of them

Keywords: Non-chain ring, Cyclic code, LCD code, Dual code, Reversible code, Gray map.

Conteúdo

Introdução

A teoria de códigos desempenhou um papel crucial na melhoria da confiabilidade e eficiência de sistemas de comunicação e armazenamento de dados. Em particular, os códigos corretores de erros têm sido fundamentais para superar os desafios da transmissão de informações em ambientes ruidosos. Neste trabalho, focamos nos códigos lineares com dual complementar (LCD), a função de Gray e os códigos duais no contexto dos anéis finitos, explorando sua importância para o desenvolvimento de sistemas de codificação robustos.

Ao longo da história, pesquisadores reconheceram a importância dos anéis finitos na teoria da codificação. Esses anéis, como o anel finito $\mathbb{F}_q + v\mathbb{F}_q$ com $v^2 = 1$, têm se mostrado ambientes matemáticos poderosos para a construção de códigos corretores de erros eficientes. Sua estrutura algébrica única permite projetar e analisar códigos capazes de lidar com interferências e erros típicos de sistemas de comunicação e armazenamento.

Os códigos LCD, em particular, despertaram grande interesse devido à sua capacidade de corrigir e detectar eficientemente erros múltiplos. Esses códigos possuem uma estrutura especial que aproveita as propriedades dos anéis finitos, tornando-os altamente eficazes na recuperação de dados danificados ou distorcidos. À medida que avançamos na evolução dos códigos corretores de erros, compreender e aproveitar as vantagens dos códigos LCD no contexto dos anéis finitos tornou-se cada vez mais importante.

A função de Gray, por outro lado, tem sido uma ferramenta inestimável no design e otimização de códigos corretores de erros. Sua origem remonta à década de 1940, quando Frank Gray desenvolveu um método inovador para representar números binários de forma sequencial, minimizando as transições entre bits adjacentes. Desde então, a função de Gray tem encontrado aplicações em diversos campos, incluindo a teoria de códigos.

Os códigos duais têm sido um componente fundamental na teoria de códigos; aqui especificamente sobre anéis finitos. Esses códigos, que estão intimamente relacionados aos códigos LCD, têm sido estudados e aplicados há décadas. Sua estrutura dual e suas propriedades matemáticas especiais permitiram o desenvolvimento de técnicas mais sofisticadas corretoras de erros e abriram novas possibilidades na transmissão e armazenamento de dados.

No primeiro capítulo, apresentaremos as principais estruturas algébricas, como anéis comutativos com unidade e álgebra linear sobre corpos finitos. Abordaremos conceitos como espaço vetorial e módulo, fornecendo as bases teóricas para o estudo dos códigos lineares. Essa introdução será fundamental para os capítulos subsequentes, onde exploraremos os códigos lineares em detalhes. No segundo capítulo, abordaremos os conceitos de códigos lineares, cíclicos, reversíveis e duais. Exploraremos suas propriedades que possuem estruturas especiais.

No terceiro capítulo, abordaremos o anel $R = \mathbb{F}_{p^m} \oplus v\mathbb{F}_{p^m}$ e suas propriedades relevantes para o trabalho. Faremos referência ao artigo [1] para fornecer informações detalhadas sobre o

assunto. Além disso, introduziremos a função de Gray e discutiremos sua definição e utilidade. Também exploraremos a matriz geradora do código linear C sobre R, apresentando suas características e resultados importantes. Ao longo deste capítulo, forneceremos os fundamentos teóricos necessários para entender as próximas seções do trabalho

No último capítulo, abordaremos a caracterização dos códigos cíclicos LCD em relação aos polinômios geradores. Revisaremos a estrutura dos códigos LCD sobre um corpo finito e exploraremos os polinômios geradores dos códigos cíclicos. Apresentaremos resultados teóricos, incluindo teoremas e provas, que estabelecem condições necessárias e suficientes para a existência de códigos cíclicos que contenham seu código dual. Essa caracterização é essencial para a construção de códigos quânticos eficientes e robustos. Ao explorar esses resultados, baseados em referências confiáveis, aprofundaremos nosso conhecimento sobre os códigos cíclicos LCD e sua relação com os polinômios geradores, contribuindo para a área da teoria da informação quântica.

Bertha Giselle Leon Benitez
Uberlândia-MG, 31 de Julho de 2023.

Capítulo 1

Estruturas Algébricas

Neste capítulo forneceremos algumas definições das estruturas algébricas, que serão de muita utilidade e que com certeza o leitor já está familiarizado com elas, esses conceitos serão encontrados em [3] e [9].

1.1 Anéis

Ao longo deste trabalho, **anel** significa anel comutativo com elemento unidade, isto é, um anel comutativo R tal que existe $1 \in R$ que satisfaz $x1 = 1x = x$.

Se $f_1, f_2, \ldots, f_n \in R$, denotaremos por $(f_1, f_2, \ldots, f_n)$ o ideal de R gerado por $f_1, f_2, \ldots, f_n$. Em particular, se $n = 1$, o ideal gerado por f_1 em R é denotado por (f_1).

Observação 1.1. *Não excluímos a possibilidade na qual* 1 *seja igual a* 0*. Se sim, então para qualquer* $x \in R$*, temos*

$$x = x1 = x0 = 0$$

e assim R *tem apenas um elemento, que é* 0 *. Neste caso* R *é o anel zero, denotado por* $\{0\}$*.*

Definição 1.2. *Seja* R *um anel com unidade* $1 \neq 0$*. Um elemento* $u \in R$ *é um elemento* ***invertível*** *de* R *se tiver um inverso multiplicativo em* R*. Se cada elemento diferente de zero de* R *for invertível, então* R *é um* ***corpo****.*

Definição 1.3. *Um subconjunto* S *de um anel* R *é um* ***subanel*** *de* R *se* S *é um anel com as operações de* R *e contém o elemento identidade de* R*; um* ***subcorpo*** *é definido de forma semelhante para um subconjunto de um corpo.*

Definição 1.4. *Um anel* R *é chamado* ***anel semilocal*** *se possui apenas um número finito de ideais maximais.*

Definição 1.5. *Um anel* R *é chamado de* ***anel em cadeia*** *se todos os seus ideais formam uma cadeia sob a inclusão. Isso significa que, para qualquer par de ideais* I *e* J *desse anel, ou* $I \subseteq J$ *ou* $J \subseteq I$*.*

Exemplo 1.6. *Se* n *é um inteiro positivo e* q *a potência de um primo, então o anel* $\mathbb{F}_q[x]/(x^n)$ *é um anel em cadeia. Denotando por* u *a classe de* x *módulo* (x^n)*, os ideias de* $\mathbb{F}_q[x]/(x^n)$ *são*

$$0 \subset (u^{n-1}) \subset (u^{n-2}) \subset \cdots \subset (u^2) \subset (u) \subset \mathbb{F}_q[x]/(x^n).$$

Por exemplo, em [11], Qian estuda códigos sobre o anel em cadeia $\mathbb{F}_2[x]/(x^2)$*.*

Definição 1.7. *Um anel* R *que não é um anel em cadeia, será chamado* ***anel não encadeado****.*

Exemplo 1.8. *O anel* $R = \mathbb{F}_q[x]/(x^2 - 1)$*, com* q *a potência de um primo ímpar, que iremos estudar nesse trabalho, é um anel semilocal não encadeado (como veremos no Capítulo 3).*

1.2 Ideais

A seguir vamos apresentar o Primeiro Teorema do Isomorfismo para Anéis. Uma prova desse resultado pode ser encontrada em [3, página 307]

Teorema 1.9 (Primeiro Teorema do Isomorfismo para Anéis)**.** *Seja $\phi : R \to R'$ um homomorfismo de anéis. Se I é o núcleo de ϕ, então o anel quociente R/I também é um anel e existe um único isomorfismo $\mu : R/I \to \phi(R)$ tal que $\phi(x) = \mu(\gamma_I(x))$ para cada $x \in R$, onde $\gamma_I : R \to R/I$ é o homomorfismo canônico*

Vamos apresentar um resultado muito importante ao longo deste trabalho. O leitor pode encontrar uma prova dele em [8, página 117].

Teorema 1.10 (Correspondência de Ideais)**.** *Sejam R e R' anéis e ψ um homomorfismo sobrejetor de R em R' com núcleo I. Então, R' é isomorfo a R/I. Além do mais, existe uma correspondência bijetora, entre o conjunto dos ideais de R' e o conjunto dos ideais de R que contêm I. Esta correspondência pode ser conseguida associando a um ideal J' de R' o ideal $J = \psi^{-1}(J') = \{x \in R \mid \psi(x) \in J'\}$. Com J assim definido, R/J é isomorfo a R'/J'.*

Definição 1.11. *Dois ideais I, J, de um anel R, são ditos **coprimos** se $I + J = (1) = R$. Para ideais coprimos temos $I \cap J = IJ$.*

Exemplo 1.12. *No anel $\mathbb{F}[x]$, defina $I = (x)$ e $J = (x^2 - 1)$. Veja que $x^2 \in I$ e $1 - x^2 \in J$. Como $x^2 + (1 - x^2) = 1$, então todo elemento de $\mathbb{F}[x]$ pode ser escrito como soma de elementos de I e J. Em outras palavras, $I + J = \mathbb{F}[x]$, ou seja, I e J são coprimos. Em particular, isso implica $I \cap J = IJ = (x^3 - x)$.*

A seguir apresentaremos o Teorema Chinês dos Restos, uma prova desse resultado está em [9, Proposição 1.10]

Teorema 1.13 (Teorema Chinês dos Restos)**.** *Seja R um anel e $I_1, I_2, \ldots, I_n$ ideais de R, defina o homomorfismo*

$$\begin{aligned} f : \ R &\longrightarrow \ R/I_1 \times R/I_2 \times \cdots \times R/I_n \\ x &\longmapsto \ (x + I_1, x + I_2, \ldots, x + I_n). \end{aligned}$$

Então,

(a) Se I_i e I_j são coprimos com $i \neq j$, então $\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$;

(b) f é sobrejetora se, e somente, se I_i e I_j são coprimos com $i \neq j$;

(c) f é injetora se, e somente, se $\bigcap_{i=1}^{n} I_i = (0)$.

1.3 Espaços Vetoriais

Esta seção é um pequeno resumo das propriedades da álgebra linear, que são necessárias neste estudo, já que grande parte da teoria de códigos baseia-se na álgebra linear sobre corpos finitos, que o leitor pode aprofundar em [8].

Definição 1.14. *Um conjunto não vazio V é dito um **espaço vetorial** sobre um corpo F (ou F-espaço vetorial) se V é um grupo abeliano com relação a uma operação que indicamos com $+$, e se para todos $\lambda \in F$, $v \in V$ está definido um elemento indicado por $\lambda \cdot v \in V$ tal que*

- $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$,
- $(\lambda + \gamma) \cdot v = \lambda \cdot v + \gamma \cdot v$,
- $\lambda \cdot (\gamma \cdot v) = (\lambda \cdot \gamma) \cdot v$,
- $1 \cdot v = v$,

para todos $\lambda, \gamma \in F$, $v, w \in V$ *(onde* 1 *representa o elemento unidade de* F *com relação à multiplicação).*

Os elementos da forma $\lambda \cdot v$ serão também denotados λv. A seguir, lembremos mais alguns conceitos da álgebra linear.

Definição 1.15. *Um* ***subespaço vetorial*** *de um* F*-espaço vetorial é um subconjunto não vazio* W *de* V*, que com as operações acima definidas de* V*, também é um* F*-espaço vetorial. Equivalentemente,* W *é um subespaço vetorial de* V*, sempre que* $w_1, w_2 \in W$*,* $\lambda, \gamma \in F$ *implica que* $\lambda w_1 + \gamma w_2 \in W$

Observação 1.16. *Sejam* F *um corpo e* x *uma indeterminada. O anel* $F[x]$ *é um* F*-espaço vetorial. Seja* $n \in \mathbb{N}$*, defina*

$$F[x]_{n-1} = \{P(x) \in F[x] \mid \operatorname{grau} P(x) \leq n - 1\} \cup \{0\}.$$

O conjunto $F[x]_{n-1}$ *é um* F*-subespaço vetorial de* $F[x]$ *de dimensão* n*, com a seguinte base* $\{1, x, x^2, \ldots, x^{n-1}\}$.

1.4 Módulos

Motivados pela definição de **espaço vetorial**, a noção de **módulo** será uma generalização da mesma: ao invés de restringir os escalares a estarem num corpo, permitiremos que sejam elementos de um anel qualquer.

Definição 1.17. *Seja* R *um anel qualquer, um conjunto não vazio* M *é dito um* R***-módulo*** *(ou módulo sobre* R*) se* M *é um grupo abeliano com relação a uma operação* $+$ *tal que para todo* $r \in R$ *e todo* $m \in M$ *existe um elemento* $rm \in M$ *satisfazendo*

(a) $r(a + b) = ra + rb$,

(b) $(r + s)a = ra + sa$,

(c) $r(sa) = (rs)a$,

(d) $1a = a$,

para todos $a, b \in M$ *e* $r, s \in R$.

Definição 1.18. *Um subgrupo aditivo* N *do* R*-módulo* M *é denominado um* ***submódulo*** *de* M *se para todo* $r \in R$ *e* $n \in N$*, temos* $rn \in N$.

1.5 A Característica de um Corpo

Nesta seção estudaremos algumas propriedades dos corpos finitos fundamentadas em [7].

Se um corpo K é finito, então o número de elementos q, desse corpo, é a potência de um número primo. Como todos os corpos finitos com q elementos são isomorfos, denotaremos, de agora em diante, um corpo finito com q elementos por $\mathbb{F}_q$.

Seja K um corpo finito com elemento unidade 1. Considere o conjunto

$$\Lambda_K = \{n \in \mathbb{N} : n1 = \underbrace{1 + \cdots + 1}_{n\text{-vezes}} = 0\} \subset \mathbb{N},$$

em que $\mathbb{N}$ denota o conjunto dos inteiros positivos.

Pelo fato de K ser finito, existe um inteiro positivo n tal que $n1 = 0$. Logo, $\Lambda_K \neq \emptyset$. Assim, Λ_K é um conjunto não-vazio de $\mathbb{N}$, e pelo princípio da boa ordem, existe um elemento mínimo. A seguinte definição é motivada por esta propriedade.

Definição 1.19. *A **característica de um corpo finito** K é o inteiro positivo* $\mathrm{car}(K)$*, definido por*

$$\mathrm{car}(K) = \min \Lambda_K = \min\{n \in \mathbb{N} \mid n1 = 0\}.$$

Se um corpo F é um subcorpo de um corpo K, então $\mathrm{car}(K) = \mathrm{car}(F)$*, pois $\Lambda_F = \Lambda_K$.*

Note que K é um espaço vetorial sobre F.

Proposição 1.20. *Seja K um corpo finito, então* $\mathrm{car}(K)$ *é um número primo.*

Demonstração. Seja $m = \mathrm{car}(K)$ e suponhamos que m não seja primo. Logo, $m = m_1 \cdot m_2$, onde m_1 e m_2 são inteiros maiores do que 1 e menores do que m. Logo

$$0 = m1 = (m_1 \cdot m_2)\, 1 = m_1\, (m_2 1) = (m_1 1) \cdot (m_2 1)$$

Como K é um domínio, temos $m_1 1 = 0$ ou $m_2 1 = 0$, o que contradiz a minimalidade de m. □

Proposição 1.21. *Seja K um corpo finito com* $\mathrm{car}(K) = p$*. Se para $m \in \mathbb{Z}$ e $a \in K$ temos $ma = 0$, então m é um múltiplo de p ou $a = 0$.*

Demonstração. Suponhamos que $ma = 0$, logo, $(m1)a = 0$. E como K é um corpo, temos $m1 = 0$ ou $a = 0$. Basta agora mostrar que, se $m1 = 0$, então m é um múltiplo de p. De fato, suponhamos que $m1 = 0$. Pelo algoritmo da divisão, temos $m = \lambda p + r$, onde $0 \leq r < p$. Logo,

$$0 = m1 = (\lambda p + r)1 = \lambda(p1) + r1 = \lambda 0 + r1 = r1$$

e como p é o menor inteiro positivo tal que $p1 = 0$, segue que $r = 0$. Portanto, m é múltiplo de p. □

Teorema 1.22. *Seja K um corpo finito com* $\mathrm{car}(K) = p$*, onde p é um número primo. Então, K contém um subcorpo isomorfo a $\mathbb{Z}_p$. Em particular, K possui p^n elementos para algum inteiro positivo n.*

Demonstração. Considere a aplicação:

$$\begin{aligned} \psi : \mathbb{Z}_p &\longrightarrow K \\ \bar{n} &\longmapsto n1. \end{aligned}$$

Primeiramente, notemos que esta aplicação está bem definida, de fato, considere $\bar{n} = \bar{m}$, então existe um inteiro λ, tal que, $n = \lambda p + m$. Logo,

$$n1 = (\lambda p + m)1 = (\lambda p)1 + m1 = \lambda(p1) + m1 = 0 + m1 = m1.$$

Vamos verificar que está aplicação é um homomorfismo. De fato,

(i) $\psi(\bar{m}+\bar{n}) = \psi(\overline{m+n}) = (m+n)1 = m1 + n1 = \psi(\bar{m}) + \psi(\bar{n})$.

(ii) $\psi(\bar{m}\cdot\bar{n}) = \psi(\overline{mn}) = (mn)1 = (m1)(n1) = \psi(\bar{m})\psi(\bar{n})$.

(iii) $\psi(\overline{1}) = 1$.

Agora como K e $\mathbb{Z}_p$ são corpos e ψ é um homomorfismo, temos que $\psi(\mathbb{Z}_p)$ é um subcorpo de K, isomorfo a $\mathbb{Z}_p$. Portanto, K é um espaço vetorial sobre $\mathbb{Z}_p$ e como K é finito, segue que, tem dimensão finita sobre $\mathbb{Z}_p$. Seja $\{a_1, \ldots, a_n\}$ uma base de K sobre $\mathbb{Z}_p$, então, todo elemento de K se escreve de modo único na forma

$$\lambda_1 a_1 + \cdots + \lambda_n a_n,$$

onde os $\lambda_i \in \mathbb{Z}_p$, com $1 \leq i \leq n$. Portanto, segue que $|K| = p^n$. □

1.6 Potência de Característica

As potências da característica de um corpo finito possuem propriedades fundamentais que serão abordadas nesta seção. Essas propriedades têm implicações significativas nas operações e estrutura do corpo, e serão exploradas. Para os leitores interessados em aprofundar-se no assunto, é recomendado consultar [7].

Proposição 1.23. *Seja K um corpo finito de característica p e seja $q = p^r$, para algum inteiro positivo r. Se $a, b \in K$, então*

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

Demonstração. Provemos este resultado por indução sobre r. Pelo binômino de Newton, temos

$$(a \pm b)^p = a^p \pm \cdots + (\pm 1)^i \binom{p}{i} a^{p-i} b^i + \cdots \pm b^p.$$

Mas como $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, temos que $p \mid \binom{p}{i}$, para todo $i = 1, \ldots, p-1$. Ainda, notemos que $(-b)^p = -b$. De fato, se p é impar o resultado é óbvio. Por outro lado, se p é par então $p = 2$ e $-1 = 1$. Daí segue que

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

ou seja, o resultado vale para $r = 1$. Agora, suponha que o resultado seja válido para, $r - 1$.

$$(a \pm b)^{p^r} = \left((a \pm b)^{p^{r-1}}\right)^p = \left(a^{p^{r-1}} \pm b^{p^{r-1}}\right)^p = a^{p^r} \pm b^{p^r}.$$

Portanto $(a \pm b)^q = a^q \pm b^q$. □

Segue, por indução, que, se $a_1, \ldots, a_n$ são elementos de um corpo finito K, de característica p e se q é uma potência de p, então:

$$(a_1 + \cdots + a_n)^q = a_1^q + \cdots + a_n^q.$$

Temos também que, se $P(x) = a_0 + \cdots + a_{n-1}x^{n-1} + a_n x^n \in \mathrm{K}[x]$, então

$$P(x)^q = a_0^q + \cdots + a_{n-1}^q x^{(n-1)q} + a_n^q x^{nq}.$$

Corolário 1.24. *Seja K um corpo finito de característica p. Se $q = p^r$ para algum inteiro positivo r, então a aplicação f_q é um isomorfismo de corpos, onde*

$$\begin{aligned} f_q : K &\longrightarrow K \\ x &\longmapsto x^q. \end{aligned}$$

Demonstração. Temos claramente

$$f_q(ab) = (ab)^q = a^q b^q = f_q(a) f_q(b)$$

e pela proposição acima,

$$f_q(a+b) = (a+b)^q = a^q + b^q = f_q(a) + f_q(b)$$

Como $f_q(1) = 1$, segue que f_q é um homomorfismo, pois veja que,

(i) $f_q(a+b) = (a+b)^q = a^q + b^q = f_q(a) + f_q(b)$.

(ii) $f_q(ab) = (ab)^q = a^q b^q = f_q(a) f_q(b)$.

(iii) $f_q(1) = 1^q = 1$.

Além disso como f_q é um homomorfismo entre corpos, segue que f_q é injetora e, como K é finito, segue que f_q é bijetora; logo, é um isomorfismo. □

Capítulo 2

Teoria de Códigos

Neste capítulo, exploraremos a teoria dos códigos, abordando a definição de alguns conceitos fundamentais nessa área. Inicialmente, discutiremos os códigos sobre corpos finitos, apresentando definições e alguns teoremas importantes que o leitor pode ver com mais detalhe no livro [7]. Em seguida, iremos analisar como esses códigos se comportam quando são considerados sobre anéis finitos, que são de grande importância ao longo deste trabalho. Esses aspectos podem ser encontrados em [1] e [12].

2.1 Códigos Lineares

Uma classe muito importante de códigos utilizada na prática é a classe dos códigos lineares. Esses códigos são construídos a partir de espaços vetoriais sobre o corpo finito $\mathbb{F}_q$, que serve como o alfabeto dos símbolos. Para cada inteiro positivo n, podemos considerar um espaço vetorial $\mathbb{F}_q^n$ de dimensão n, onde cada elemento é um vetor de n símbolos pertencentes ao corpo $\mathbb{F}_q$. Os códigos lineares são subespaços desse espaço vetorial $\mathbb{F}_q^n$, que podem ser gerados por um conjunto de vetores chamados vetores geradores. Essa estrutura dos códigos lineares permite a utilização de técnicas eficientes de codificação e decodificação, tornando-os muito úteis em aplicações práticas de comunicação e armazenamento de dados.

A construção de um código corretor de erros começa com a definição de um conjunto finito chamado alfabeto, representado por A. O tamanho desse **alfabeto**, indicado por $|A|$, é denotado por q.

Definição 2.1. *Um **código** é um subconjunto adequado de A^n, onde n é um inteiro positivo.*

Para quantificar a proximidade entre palavras, é necessário introduzir uma métrica de distância entre elas no espaço A^n. A métrica de Hamming é uma medida comum usada para medir a distância entre palavras nesse contexto.

Definição 2.2. *Dados dois elementos $u, v \in A^n$, a **distância de Hamming** entre u e v é definida como*

$$d_H(u, v) = |\{i \mid u_i \neq v_i, 1 \leq i \leq n\}|$$

Definição 2.3. *Seja C um código. A **distância mínima** de C é o número*

$$d_H = \min\{d_H(u, v) \mid u, v \in C \text{ e } u \neq v\}.$$

Definição 2.4. *Um código $C \subset \mathbb{F}_q^n$ será chamado de **código linear** se for um subespaço vetorial de $\mathbb{F}_q^n$. Todo código linear é por definição um espaço vetorial de dimensão finita. Seja k a dimensão do código C e seja $\{v_1, v_2, \ldots, v_k\}$ uma de suas bases, portanto, todo elemento de C se escreve de modo único na forma*

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

onde os $\lambda_i, i = 1, \ldots, k$, *são elementos de* $\mathbb{F}_q$. *Segue daí que*

$$M = |C| = q^k$$

e, consequentemente,

$$\dim_K C = k = \log_q q^k = \log_q M.$$

Exemplo 2.5. *Seja* $C \subset \mathbb{F}_5^{15}$ *e suponha que a dimensão* $\dim(C) = 3$, *então exitem* $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_5^{15}$ *tais que*

$$C = \{a\alpha_1 + b\alpha_2 + c\alpha_3 \mid a, b, c \in \mathbb{F}_5\} \text{ e } |C| = 5^3$$

De maneira mais geral se C é um código linear sobre $\mathbb{F}_q$ de comprimento n, ou seja, $C \subset \mathbb{F}_q^n$, de $\dim(C) = k$, então $|C| = q^k$.

Definição 2.6. *Dado* $x \in \mathbb{F}_q^n$, *definimos* ***o peso de x*** *como sendo o número inteiro*

$$\omega_H(x) := |\{i \mid x_i \neq 0\}|.$$

Em outras palavras, temos

$$\omega_H(x) = d_H(x, 0).$$

Definição 2.7. *O* ***peso de um código linear*** C *é o inteiro*

$$\omega_H(C) := \min\{\omega_H(x) \mid 0 \neq x \in C\}.$$

Proposição 2.8. *Seja* $C \subset \mathbb{F}_q^n$ *um código linear com distância mínima* d_H. *Temos,*

i) para todos $u, v \in \mathbb{F}_q^n$ *temos* $d_H(u, v) = \omega_H(u - v)$;

ii) $d_H = \omega_H(C)$.

Demonstração. i) Temos

$$\begin{aligned} \omega_H(u - v) &= d_H(u - v, 0) \\ &= |\{i \mid u_i - v_i \neq 0, 1 \leq i \leq n\}| \\ &= |\{i \mid u_i \neq v_i, 1 \leq i \leq n\}| \\ &= d_H(u, v). \end{aligned}$$

ii) Para todo para de elementos $u, v \in C$ com $u \neq v$, temos $w = u - v \in C - \{0\}$ e $d_H(u, v) = \omega_H(w)$. □

2.2 Matriz Geradora de um Código

Considere um código linear $C \subset \mathbb{F}_q^n$. Os parâmetros do código linear C são representados por uma tripla de números inteiros (n, k, d), onde k é a dimensão de C sobre $\mathbb{F}_q$ e d representa a distância mínima de C, que é equivalente ao peso $\omega(C)$ do código C. O número de elementos em C, denotado por M, é igual a q^k.

Seja $\mathcal{B} = \{v_1, \ldots, v_k\}$ uma base ordenada de C. Podemos construir uma matriz G, cujas linhas são os vetores $v_i = (v_{i1}, \ldots, v_{in})$, ou seja,

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

A matriz G acima é chamada **matriz geradora** de C associada à base $\mathcal{B}$. Podemos definir uma transformação linear $T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$ através da multiplicação de um vetor $x = (x_1, \ldots, x_k) \in \mathbb{F}_q^k$ pela matriz G, ou seja,

$$T(x) = xG = x_1 v_1 + \cdots + x_k v_k.$$

Logo, $T\left(\mathbb{F}_q^k\right) = C$. Note que, a matriz geradora G não é única para o código C, pois ela depende da escolha da base $\mathcal{B}$. Além disso, uma base de um espaço vetorial pode ser obtida a partir de outra através de operações como permutação de elementos, multiplicação de um elemento por um escalar não nulo ou substituição de um vetor por ele mesmo somado a um múltiplo escalar de outro vetor da base.

Dessa forma, é possível obter diferentes matrizes geradoras para o mesmo código C através de uma sequência de operações, como permutação de linhas, multiplicação de uma linha por um escalar não nulo e adição de um múltiplo escalar de uma linha a outra. Por outro lado, é possível construir códigos a partir de matrizes geradoras G, tomando uma matriz cujas linhas sejam linearmente independentes e definindo o código como a imagem da transformação linear $T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$, onde $x \longmapsto xG$.

2.3 Códigos Duais

Nesta seção, vamos explorar o conceito de códigos duais na teoria de códigos lineares sobre o corpo finito $\mathbb{F}_q$. O código dual de um código linear C é definido como o conjunto de vetores que são ortogonais a todos os vetores em C. Utilizando a operação de produto interno, podemos caracterizar o código dual de forma mais precisa.

Sejam $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ elementos de $\mathbb{F}_q^n$. Definimos o **produto interno** de u e v como

$$\langle u, v \rangle = u_1 v_1 + \cdots + u_n v_n.$$

Essa operação possui as propriedades usuais de um produto interno, ou seja, é simétrica

$$\langle u, v \rangle = \langle v, u \rangle$$

e bilinear

$$\langle u + \lambda w, v \rangle = \langle u, v \rangle + \lambda \langle w, v \rangle$$

para todo $\lambda \in \mathbb{F}_q$.

Definição 2.9. *Para um código linear $C \subset \mathbb{F}_q^n$, definimos o seu **código dual** $C^\perp$ como o subconjunto de $\mathbb{F}_q^n$ ortogonal a C, isto é,*

$$C^\perp = \left\{ v \in \mathbb{F}_q^n \mid \langle v, u \rangle = 0, \, \forall u \in C \right\}.$$

Proposição 2.10. *Se $C \subset \mathbb{F}_q^n$ é um código linear, então $C^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$, ou seja, $C^\perp$ é linear.*

Demonstração. Claramente $C^\perp \neq \emptyset$, pois 0 pertence ao dual. Sejam $u, v \in C^\perp$ e $\lambda \in \mathbb{F}_q$. Temos, para todo $x \in C$, que

$$\langle u + \lambda v, x \rangle = \langle u, x \rangle + \lambda \langle v, x \rangle = 0$$

e, portanto, $u + \lambda v \in C^\perp$, provando que $C^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$. □

2.4 Códigos Cíclicos

A partir de agora, representaremos as coordenadas de $\mathbb{F}_q^n$ como $(x_0, \ldots, x_{n-1})$.

Definição 2.11. *Um código linear $C \subset \mathbb{F}_q^n$ será chamado de* ***código cíclico*** *se, para todo $c = (c_0, \ldots, c_{n-1}) \in C$, o vetor $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.*

Equivalentemente, o código linear C será um código cíclico se, dada a permutação π de $\{0, \ldots, n-1\}$ definida por

$$\pi(i) = \begin{cases} i-1 & \text{se } i \geq 1, \\ n-1 & \text{se } i = 0 \end{cases}$$

e, sendo

$$T_\pi\left(c_0, c_1, \ldots, c_{n-1}\right) = \left(c_{n-1}, c_0, \ldots, c_{n-2}\right),$$

tivermos $T_\pi(\mathrm{c}) \in C$ para todo $c \in C$; ou seja, $T_\pi(C) \subset C$.

Definição 2.12. *Um código C, é chamado* ***reversível*** *se para todo $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, temos $(c_{n-1}, c_{n-2}, \ldots, c_0) \in C$.*

Capítulo 3

Anel não Encadeado e Semilocal

Neste capítulo vamos apresentar algumas propriedades do anel $R = \mathbb{F}_{p^m} \oplus v\mathbb{F}_{p^m}$. Características e resultados importantes de R serão destacados, os quais o leitor pode encontrar em [1].

Seja $\mathbb{F}_{p^m}$ um corpo finito de característica p, com p um primo impar e m um inteiro positivo. Ao longo deste trabalho vamos usar $q = p^m$ e definimos o anel

$$R = \mathbb{F}_q \oplus v\mathbb{F}_q = \{a + vb \mid a, b \in \mathbb{F}_q\}, \quad \text{onde } v^2 = 1,$$

com operações de adição e multiplicação decorrentes dessa relação. Isto é, $(a+vb)+(c+vd) = (a+c)+v(b+d)$ e

$$(a + vb)(c + vd) = (ac + bd) + v(ad + bc).$$

Note que R é um anel de ideais principais. Para provar isso, mostremos que R é isomorfo a $\mathbb{F}_q[x]/(x^2 - 1)$. Considere a função ψ definida como segue:

$$\begin{array}{rccc} \psi: & \mathbb{F}_q[x] & \longrightarrow & R \\ & f(x) & \longmapsto & f(v). \end{array}$$

É claro que ψ é um homomorfismo de anéis, de fato, sejam $f(x), g(x) \in \mathbb{F}_q[x]$. Então,

$$\begin{aligned} \psi(f(x) + g(x)) &= \psi((f+g)(x)) = (f+g)(v) = f(v) + g(v), \\ \psi(f(x) \cdot g(x)) &= \psi((f \cdot g)(x)) = (f \cdot g)(v) = f(v) \cdot g(v). \end{aligned}$$

Assim, ψ é um homomorfismo. Além disso, ψ é sobrejetor pois se $a+vb \in R$, então $\psi(a+bx) = a + bv$, com $a + bx \in \mathbb{F}_q[x]$.

Vamos provar $\ker \psi = (x^2 - 1)$. Se $f(x) \in (x^2 - 1)$, então existe $g(x) \in \mathbb{F}_q[x]$ tal que $f(x) = (x^2 - 1) \cdot g(x)$. Assim,

$$\psi(f(x)) = \psi((x^2 - 1) \cdot g(x)) = \psi(x^2 - 1) \cdot \psi(g(x)) = (v^2 - 1) \cdot g(v) = 0.$$

Daí, $f(x) \in \ker \psi$. Isso prova $(x^2 - 1) \subseteq \ker \psi$.

Se $f(x) \in \ker \psi$, pelo algoritmo da divisão, existem $q(x), r(x) \in \mathbb{F}_q[x]$ tais que

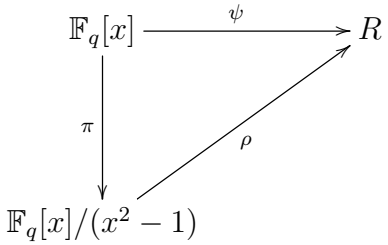
$$f(x) = (x^2 - 1) \cdot q(x) + r(x),$$

com $r(x) = 0$ ou $\operatorname{grau} r < 2$. Então, existem $a, b \in \mathbb{F}_q[x]$ tais que $r(x) = a + bx$, e note que

$$0 = \psi(f(x)) = \psi(x^2 - 1) \cdot \psi(q(x)) + \psi(a + bx) = a + bv \in R = \mathbb{F}_q \oplus v\mathbb{F}_q.$$

Daí $a = b = 0$, e, portanto, $f(x) \in (x^2 - 1)$. Ou seja, $\ker \psi = (x^2 - 1)$.

Denotemos $\pi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q[x]/(x^2-1)$ o homomorfismo canônico. Pelo primeiro teorema de isomorfismo, veja o Teorema 1.9, existe um único isomorfismo ρ que faz o seguinte diagrama comutar

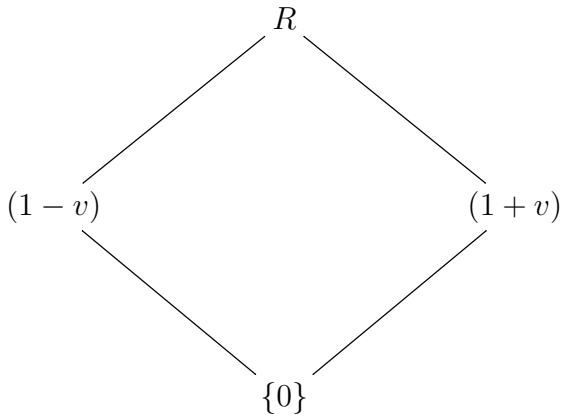


e, ρ está definido por $\rho(\overline{a+bx}) = a + bv$.

Do Teorema 1.10, sabemos que existe uma correspondência biunívoca entre os ideais I de R e os ideais J de $\mathbb{F}_q[x]$ que contêm (x^2-1). Essa correspondência é dada por $\rho(\pi(J)) = I$ e $\pi^{-1}(\rho^{-1}(I)) = J$. Como $\mathbb{F}_q$ é corpo, então $\mathbb{F}_q[x]$ é domínio principal. Dessa forma, se J é um ideal de $\mathbb{F}_q[x]$, então existe $f(x) \in \mathbb{F}_q[x]$ tal que $J = (f(x))$. Daí, $I = \rho(\pi(J)) = (f(v))$, em outras palavras, R é um anel de ideais principais.

Se $J = (f(x))$ é um ideal de $\mathbb{F}_q[x]$ que contêm (x^2-1), então $x^2-1 \in (f(x))$, ou seja, $f(x) \mid x^2-1$. Como os divisores mônicos de x^2-1 são 1, $x-1$, $x+1$ e x^2-1, então os únicos ideais de R são $(1) = R$, $(1-v)$, $(1+v)$ e $(1-v^2) = \{0\}$.

A seguir temos o seguinte diagrama dos ideais de R:



Em outras palavras, acabamos de provar o seguinte resultado.

Proposição 3.1. *R é um anel semilocal com dois ideais maximais, a saber $(1-v)$ e $(1+v)$. Em particular, R não é um anel em cadeia.*

Além do isomorfismo $R \cong \mathbb{F}_q[x]/(x^2-1)$, também temos outro isomorfismo dado pelo teorema chinês dos restos. Observe que para os ideais $I = (x-1)$ e $J = (x+1)$ de $\mathbb{F}_q[x]$, temos $IJ = (x^2-1)$ e em característica ímpar, $I + J = \mathbb{F}_q[x]$, pois $\frac{1}{2}(x+1) - \frac{1}{2}(x-1) = 1$. Como I e J são coprimos, pelo teorema chinês dos restos, temos também o seguinte isomorfismo $\mathbb{F}_q[x]/(x+1)(x-1) \cong \mathbb{F}_q[x]/(x-1) \times \mathbb{F}_q[x]/(x+1)$ dado por

$$f(x) + (x^2-1) \longmapsto (f(x) + (x-1), f(x) + (x+1)).$$

Por outro lado, $\mathbb{F}_q[x]/(x-1)$ e $\mathbb{F}_q[x]/(x+1)$ são isomorfos a $\mathbb{F}_q$. Esses isomorfismos são dados pelo homomorfismo avaliação. Isto é

$$\begin{array}{rccc} \mathrm{av}_1 : & \mathbb{F}_q[x]/(x-1) & \longrightarrow & \mathbb{F}_q \\ & f(x) + (x-1) & \longmapsto & f(1) \end{array} \quad \text{e} \quad \begin{array}{rccc} \mathrm{av}_{-1} : & \mathbb{F}_q[x]/(x+1) & \longrightarrow & \mathbb{F}_q \\ & f(x) + (x+1) & \longmapsto & f(-1). \end{array}$$

A composta desses isomorfismos, juntamente com o isomorfismo

$$\mathbb{F}_q[x]/(x+1)(x-1) \cong \mathbb{F}_q[x]/(x-1) \times \mathbb{F}_q[x]/(x+1),$$

é o isomorfismo

$$\begin{array}{rccc} F: & \mathbb{F}_q[x]/(x^2-1) & \longrightarrow & \mathbb{F}_q^2 \\ & f(x)+(x^2-1) & \longmapsto & (f(1), f(-1)). \end{array}$$

Isso implica que $\tilde{\rho} = F \circ \rho^{-1} : R \longrightarrow \mathbb{F}_q^2$ é um isomorfismo que é dado por

$$\tilde{\rho}(a+bv) = (a+b, a-b)\,.$$

Lembre que esse é um isomorfismo caso $\mathbb{F}_q$ seja de característica ímpar.

3.1 Códigos Lineares sobre Anéis

A teoria de códigos lineares sobre anéis é uma área de estudo fundamental na teoria aqui trabalhada. Ela envolve a construção de códigos que operam não apenas em corpos finitos, mas também em anéis, que são estruturas algébricas mais gerais.

Definição 3.2. *Um código linear C de comprimento n sobre um anel R é um R-submódulo de R^n e os elementos de C são chamados palavras do código.*

Definição 3.3. *O código dual $C^\perp$ de um código linear $C \subset R^n$ é definido por*

$$C^\perp = \{a \in R^n \mid \langle a, b\rangle = 0,\ \forall b \in C\}\,,$$

onde o produto interno euclidiano de dois elementos de R^n, $c = (c_1, \ldots, c_n)$ e $d = (d_1, \ldots, d_n)$, é definido por

$$\langle c, d\rangle = \sum_{i=1}^{n} c_i d_i.$$

Vejamos então que $C^\perp$ é um código linear, de fato, $C^\perp \neq \emptyset$ e para quaisquer $c, d \in C^\perp$ e $\lambda \in R$, temos, para todo $x \in C$, que

$$\langle c + \lambda d, x\rangle = \langle c, x\rangle + \lambda\langle d, x\rangle = 0.$$

Portanto, $c + \lambda d \in C^\perp$. Isso prova que $C^\perp$ é um R-submódulo de R^n.

Definição 3.4. *Um código C, é chamado* ***auto-ortogonal*** *se $C \subseteq C^\perp$, e* ***auto-dual*** *se $C = C^\perp$.*

Vamos estudar agora a estrutura do anel R. Para tal, vamos provar que

$$R = (1-v) \oplus (1+v) = (1-v)\mathbb{F}_q \oplus (1+v)\mathbb{F}_q.$$

Veja que $(1-v)$ e $(1+v)$ são ideais de R. Quando escrevemos soma direta, estamos dizendo que todo elemento de R se escreve de forma única como uma soma de elementos de $(1-v)$ e $(1+v)$. Em outras palavras, iremos provar que $R = (1-v) + (1+v)$ e $(1-v) \cap (1+v) = \{0\}$. Para provar a segunda igualdade, provaremos $(1-v) = (1-v)\mathbb{F}_q$ e $(1+v) = (1+v)\mathbb{F}_q$. Provemos esses resultados por etapas.

Lema 3.5. *Sejam $(1-v)\mathbb{F}_q$ e $(1+v)\mathbb{F}_q$ definidos por*

$$(1-v)\mathbb{F}_q = \{a(1-v) \mid a \in \mathbb{F}_q\} \quad e \quad (1+v)\mathbb{F}_q = \{b(1+v) \mid b \in \mathbb{F}_q\}.$$

Temos $(1-v) = (1-v)\mathbb{F}_q$ e $(1+v) = (1+v)\mathbb{F}_q$.

Demonstração. Seja $(1-v)(a+bv)$ um elemento do ideal $(1-v)$. Temos

$$\begin{aligned}(1-v)(a+bv) &= a-av+bv-bv^2\\ &= a-av+bv-b\\ &= (a-b)-(a-b)v\\ &= (a-b)(1-v),\end{aligned}$$

com $a-b\in\mathbb{F}_q$, portanto $(1-v)\subseteq(1-v)\mathbb{F}_q$. Por outro lado, como $\mathbb{F}_q\subseteq R$ então $(1-v)\mathbb{F}_q\subseteq(1-v)$, daí $(1-v)\mathbb{F}_q=(1-v)$. De forma similar $(1+v)\mathbb{F}_q=(1+v)$, pois

$$(1+v)(a+bv)=(a+b)(1+v).$$

□

Proposição 3.6. $R=(1-v)\oplus(1+v)=(1-v)\mathbb{F}_q\oplus(1+v)\mathbb{F}_q$.

Demonstração. Vamos provar que $R=(1-v)\mathbb{F}_q\oplus(1+v)\mathbb{F}_q$. De fato, veja que $2\in\mathbb{F}_q$ e $2\neq 0$, pois trabalhamos em característica ímpar. Assim, $2^{-1}=\frac{1}{2}\in\mathbb{F}_q$. Dado $a+bv\in R$, temos

$$\frac{1}{2}(a-b)(1-v)+\frac{1}{2}(a+b)(1+v)=\frac{1}{2}(a-b-av+bv+a+b+av+bv)=a+bv.$$

Logo, $a+bv\in(1-v)\mathbb{F}_q+(1+v)\mathbb{F}_q$, pois $\frac{1}{2}(a-b),\frac{1}{2}(a+b)\in\mathbb{F}_q$. Como $(1-v)\mathbb{F}_q\subseteq R$ e $(1+v)\mathbb{F}_q\subseteq R$, então $R=(1-v)\mathbb{F}_q+(1+v)\mathbb{F}_q$. Pelo Lema 3.5, temos $(1-v)=(1-v)\mathbb{F}_q$ e $(1+v)=(1+v)\mathbb{F}_q$. Assim, os ideiais $I=(1-v)$ e $J=(1+v)$ são coprimos, pois $R=I+J$. Pelo Teorema 1.13, temos $I\cap J=IJ$. Como $IJ=(1-v)(1+v)=(0)$, então a soma é direta, isto é, $R=I\oplus J$. □

Veja que a proposição anterior indica que todo elemento $\alpha\in R$ se escreve de forma única como $\alpha=(1-v)a+(1+v)b$, com $a,b\in\mathbb{F}_q$.

3.2 Função de Gray

Motivados pelas construções acima, nesta seção vamos definir a função de Gray. Pela Proposição 3.6, a função

$$\begin{array}{rccc}\psi: & R & \longrightarrow & \mathbb{F}_q^2\\ & (1-v)a+(1+v)b & \longmapsto & (a,b)\end{array}$$

é uma bijeção. Essa bijeção pode ser estendida a uma função $\psi_0:R^n\longrightarrow\mathbb{F}_q^{2n}$ definindo, para todo $(\alpha_1,\alpha_2,\ldots,\alpha_n)\in R^n$,

$$\psi_0((\alpha_1,\alpha_2,\ldots,\alpha_n))=(\psi(\alpha_1),\psi(\alpha_2),\ldots,\psi(\alpha_n)).$$

É claro que ψ é uma aplicação linear sobre $\mathbb{F}_q$, de fato, se $\alpha=(1-v)a_1+(1+v)b_1\in R$, $\beta=(1-v)a_2+(1+v)b_2\in R$ e $c\in\mathbb{F}_q$, então

$$\begin{aligned}\psi(\alpha+c\beta) &= \psi((1-v)a_1+(1+v)b_1+c((1-v)a_2+(1+v)b_2))\\ &= \psi((1-v)(a_1+ca_2)+(1+v)(b_1+cb_2))\\ &= (a_1+ca_2,b_1+cb_2)\\ &= (a_1,b_1)+c(a_2,b_2)\\ &= \psi(\alpha)+c\psi(\beta).\end{aligned}$$

Veja que ψ não é um homomorfismo de anéis pois, para $c \in \mathbb{F}_q \subseteq R$, temos $c = \frac{c}{2}(1-v)+\frac{c}{2}(1+v)$, isto é, $\psi(c) = \left(\frac{c}{2}, \frac{c}{2}\right)$. Dessa forma, para $\alpha = (1-v)a + (1+v)b \in R$, temos

$$\psi(c\alpha) = (ca, cb) \neq \left(\frac{ca}{2}, \frac{cb}{2}\right) = \psi(c)\psi(\alpha).$$

Alguns autores, como em [6], definem a função de Gray como ψ. No entanto, em [1] a função de Gray é definida da seguinte forma:

Definição 3.7. *Seja $M \in GL_2(\mathbb{F}_q)$, onde $GL_2(\mathbb{F}_q)$ é o conjunto de todas as matrizes invertíveis 2×2 sobre $\mathbb{F}_q$. Como M é invertível, a aplicação linear*

$$\begin{array}{rccc} \mu: & \mathbb{F}_q^2 & \longrightarrow & \mathbb{F}_q^2 \\ & (a,b) & \longmapsto & (a,b)M \end{array}$$

é bijetora. Definimos a ***função de Gray*** *como*

$$\begin{array}{rccc} \phi = \mu \circ \psi: & R & \longrightarrow & \mathbb{F}_q^2 \\ & (1-v)a + (1+v)b & \longmapsto & (a,b)M. \end{array}$$

Observação 3.8. *É claro que a função ϕ é bijetora e pode ser estendida a uma função $\phi_0 : R^n \longrightarrow \mathbb{F}_q^{2n}$, da mesma maneira que estendemos ψ_0, isto é, para todo $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in R^n$, define-se*

$$\phi_0((\alpha_1, \alpha_2, \ldots, \alpha_n)) = (\phi(\alpha_1), \phi(\alpha_2), \ldots, \phi(\alpha_n)).$$

Como ψ e μ são aplicações lineares bijetoras sobre $\mathbb{F}_q$, as funções ϕ e ϕ_0 também são aplicações lineares bijetoras.

Seja C um código sobre R de comprimento n, isto é, $C \subseteq R^n$ é um R-submódulo de R^n. Para $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in C$, existem únicos $a_i, b_i \in \mathbb{F}_q$ tais que $\alpha_i = (1-v)a_i + (1+v)b_i$, para todo $1 \leq i \leq n$. Portanto,

$$\begin{array}{rcl} \alpha & = & ((1-v)a_1 + (1+v)b_1, (1-v)a_2 + (1+v)b_2, \ldots, (1-v)a_n + (1+v)b_n) \\ & = & (1-v)(a_1, a_2, \ldots, a_n) + (1+v)(b_1, b_2, \ldots, b_n). \end{array}$$

Definimos então

$$\begin{array}{rcl} C_1 & = & \{a \in \mathbb{F}_q^n \mid \exists b \in \mathbb{F}_q^n \text{ tal que } (1-v)a + (1+v)b \in C\} \text{ e} \\ C_2 & = & \{b \in \mathbb{F}_q^n \mid \exists a \in \mathbb{F}_q^n \text{ tal que } (1-v)a + (1+v)b \in C\}. \end{array}$$

Veja que C_1 e C_2 são códigos lineares de comprimento n sobre $\mathbb{F}_q$. Além disso, temos o seguinte resultado.

Lema 3.9. $C = (1-v)C_1 \oplus (1+v)C_2$.

Demonstração. Seja $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in C$. Como vimos acima, existem únicos $a_i, b_i \in \mathbb{F}_q$ tais que

$$\alpha_i = (1-v)a_i + (1+v)b_i$$

e, portanto,

$$\alpha = (1-v)a + (1+v)b,$$

onde $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ e $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$. Por definição de C_1 e C_2, temos $a \in C_1$ e $b \in C_2$. Assim

$$C \subseteq (1-v)C_1 + (1+v)C_2.$$

Por outro lado, seja $a \in C_1$, então existe $b \in C_2$ tal que

$$\alpha = (1-v)a + (1+v)b \in C.$$

Como C é um R-módulo, então $2^{-1}(1-v)\alpha \in C$. Assim,

$$\begin{aligned} 2^{-1}(1-v)\alpha &= 2^{-1}(1-v)(1-v)a + 2^{-1}(1-v)(1+v)b \\ &= 2^{-1}(1-v-v+v^2)a + 2^{-1}(1+v-v-v^2)b \\ &= 2^{-1}2(1-v)a + 2^{-1}(0)b \\ &= (1-v)a. \end{aligned}$$

Isso implica $(1-v)a \in C$. De forma similar, prova-se que se $b \in C_2$, então $(1+v)b \in C$. Em outras palavras

$$(1-v)C_1 + (1+v)C_2 \subseteq C.$$

Provemos que a soma é direta, ou seja

$$(1-v)C_1 \cap (1+v)C_2 = \{0\}.$$

Seja $\alpha \in (1-v)C_1 \cap (1+v)C_2$. Isso quer dizer que existem $a \in C_1$ e $b \in C_2$ tais que

$$\alpha = (1-v)a = (1+v)b.$$

Multiplicando a segunda igualdade por $1-v$ e como

$$(1-v)^2 = 2(1-v) \quad \text{e} \quad (1-v)(1+v) = 0,$$

temos $2(1-v)a = 0$. Escrevendo $a = (a_1, \ldots, a_n)$, vemos que

$$(2(1-v)a_1, \ldots, 2(1-v)a_n) = (0, \ldots, 0).$$

Ou seja, para todo $1 \leq i \leq n$,

$$2a_i - 2a_i v = 0 = 0 + 0v.$$

Logo, $a_i = 0$, ou ainda, $a = 0$. Assim, $\alpha = 0$ e, portanto,

$$(1-v)C_1 \cap (1+v)C_2 = \{0\}.$$

Conclui-se que

$$C = (1-v)C_1 \oplus (1+v)C_2.$$

□

Observe que como $C \subseteq R^n$, então $C^\perp \subseteq R^n$. Da mesma forma, como $C_1, C_2 \subseteq \mathbb{F}_q^n$, então $C_1^\perp, C_2^\perp \subseteq \mathbb{F}_q^n$. Com isso em mente, provamos o seguinte resultado.

Lema 3.10. $C^\perp = (1-v)C_1^\perp \oplus (1+v)C_2^\perp$.

Demonstração. Primeiro vamos definir:

$$C^\perp = \{\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{F}_q^n \mid \langle \beta, \alpha \rangle = 0, \, \forall \alpha \in C\}.$$

Seja $\beta \in C^\perp$, então β se escreve de maneira única como $\beta = (1-v)x + (1+v)y$, com $x, y \in \mathbb{F}_q^n$ e sejam:

$$C_1^\perp = \{a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n \mid \langle a, a' \rangle = 0, \, \forall a' = (a'_1, a'_2, \ldots, a'_n) \in C_1\}$$

e

$$C_2^{\perp} = \{b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n \mid \langle b, b' \rangle = 0, \, \forall b' = (b'_1, b'_2, \ldots, b'_n) \in C_1\}$$

Dado $\alpha \in C$, nos sabemos que $\alpha \in C$ se escreve de maneira única como $\alpha = (1-v)a + (1+v)b$ com $a \in C_1$ e $b \in C_2$, consideremos agora

$$\begin{aligned} \langle \beta, \alpha \rangle &= \langle (1-v)x + (1+v)y, (1-v)a + (1+v)b \rangle \\ &= \langle (1-v)x, (1-v)a \rangle + \langle (1+v)y, (1+v)b \rangle, \end{aligned}$$

pois

$$\begin{aligned} \langle (1-v)x, (1+v)b \rangle &= (1-v)(1+v)\langle x, b \rangle = 0 \\ \langle (1-v)y, (1+v)a \rangle &= (1-v)(1+v)\langle y, a \rangle = 0. \end{aligned}$$

Como $v^2 = 1$, temos

$$\begin{aligned} (1-v)(1-v) &= 2(1-v) \quad \text{e} \\ (1+v)(1+v) &= 2(1+v). \end{aligned}$$

Então,

$$\langle \beta, \alpha \rangle = 2(1-v)\langle x, a \rangle + 2(1+v)\langle y, b \rangle = 0.$$

Assim, $\langle \beta, \alpha \rangle = 0$. Isto ocorre se, e somente se, $\langle x, a \rangle = 0$ e $\langle y, b \rangle = 0$. Então, $\beta \in C^{\perp}$ se, e somente se, para todos $a \in C_1$ e $b \in C_2$ tais que

$$\langle x, a \rangle = 0 \quad \text{e} \quad \langle y, b \rangle = 0.$$

O qual ocorre se, e somente se, $x \in C_1^{\perp}$ e $y \in C_2^{\perp}$. Em outras palavras,

$$C^{\perp} = (1-v)C_1^{\perp} \oplus (1+v)C_2^{\perp}.$$

□

Observação 3.11. *A notação $C = (1-v)C_1 \oplus (1+v)C_2$ usada acima, será utilizada ao longo deste trabalho.*

3.3 Matriz Geradora

A matriz geradora do código linear C sobre R é dada por:

$$G = \begin{bmatrix} (1-v)G_1 \\ (1+v)G_2 \end{bmatrix}$$

onde G_1, G_2 são matrizes geradoras de C_1 e C_2 respectivamente e $|C| = |C_1||C_2|$. De fato suponha que $\{v_1, v_2, \ldots, v_{k_1}\}$ é base de C_1 e $\{w_1, w_2, \ldots, w_{k_2}\}$ é base de C_2. Para $\alpha \in C$ existem únicos $x \in C_1$ e $y \in C_2$ tais que

$$\alpha = (1-v)x + (1+v)y,$$

de modo que existem únicos $a_1, a_2, \ldots, a_{k_1} \in \mathbb{F}_q^n$ e $b_1, b_2, \ldots, b_{k_2} \in \mathbb{F}_q^n$ tais que

$$\begin{aligned} x &= a_1 v_1 + a_2 v_2 + \cdots + a_{k_1} v_{k_1} \\ y &= b_1 w_1 + b_2 w_2 + \cdots + b_{k_2} w_{k_2}. \end{aligned}$$

Então,

$$\alpha = (1-v)a_1v_1 + (1-v)a_2v_2 + \cdots + (1-v)a_{k_1}v_{k_1} + (1+v)b_1w_1 + (1+v)b_2w_2 + \cdots + (1+v)b_{k_2}w_{k_2}$$

de modo que, $\{(1-v)v_1, (1-v)v_2, \ldots, (1-v)v_{k_1}, (1+v)w_1, (1+v)w_2, \ldots, (1+v)w_{k_2}\}$ é uma base de C. Assim, a matriz geradora de C é

$$\begin{bmatrix} (1-v)v_1 \\ (1-v)v_2 \\ \vdots \\ (1-v)v_{k_1} \\ (1+v)w_1 \\ (1+v)w_2 \\ \vdots \\ (1+v)w_{k_1} \end{bmatrix} = \begin{bmatrix} (1-v)G_1 \\ (1+v)G_2 \end{bmatrix}.$$

Definição 3.12. *Como no caso de códigos sobre corpos finitos, definimos a* ***distância de Hamming*** *entre dois elementos $\alpha, \beta \in R^n$, denotado por $d_H(\alpha, \beta)$, como sendo o número de coordenadas nas quais α e β são diferentes. Define-se também o* ***peso de Hamming*** *de $\alpha \in R^n$, denotado por $w_H(\alpha)$, como sendo o número de componentes diferentes de zero em α. Dessa forma, para $\alpha, \beta \in R^n$, tem-se $d_H(\alpha, \beta) = w_H(\alpha - \beta)$. A* ***distância de Hamming*** *de um código linear C sobre R é definida por*

$$d_H = \min\{d_H(\alpha, \beta) \mid \alpha, \beta \in C \text{ e } \alpha \neq \beta\} = \min\{w_H(\alpha) \mid 0 \neq \alpha \in C\}.$$

Motivados pela função de Gray vamos apresentar as seguintes definições.

Definição 3.13. *Definimos o* ***peso de Gray*** *para $c \in C$ por*

$$w_G(c) = \omega_H(\phi_0(c)).$$

Então, o peso de Gray para a palavra $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in C$ é

$$w_G(\alpha) = \sum_{i=1}^{n} w_G(\alpha_i),$$

onde o peso de Gray de $\alpha_i \in R$ é definido por $w_G(\alpha_i) = \omega_H(\phi(\alpha_i))$, para todo $i = 1, \ldots, n$. A ***distância de Gray*** *entre duas palavras α,$\beta \in C$ como*

$$d_G(\alpha - \beta) = w_G(\alpha - \beta).$$

Além disso, a distância de Gray do código linear C é

$$d_G(C) = \min\{w_G(\alpha) \mid 0 \neq \alpha \in C\}.$$

A discussão acima conclui que o mapa de Gray $\phi_0 : R^n \longrightarrow \mathbb{F}_q^{2n}$ é uma função linear que preserva a distância entre os espaços (R^n, d_G) e $(\mathbb{F}_q^{2n}, d_H)$, e preserva o peso entre os espaços (R^n, w_G) e $(\mathbb{F}_q^{2n}, w_H)$. Consequentemente, para um código linear $[n, k, d_G]$, sua imagem de Gray $\phi_0(C)$ é um código linear $[2n, k, d_G]$ sobre $\mathbb{F}_q$, onde $d_G = d_H$.

Teorema 3.14. *Seja C um código linear auto-ortogonal de comprimento n sobre R e M uma matriz invertível 2×2 sobre $\mathbb{F}_q$ tal que $MM^{\perp} = \lambda I_2$, onde $M^{\perp}$ é a transposta de M, I_2 é a matriz identidade e $0 \neq \lambda \in \mathbb{F}_q$. Então, a imagem de Gray $\phi_0(C)$ é um código linear auto-ortogonal de comprimento $2n$ sobre $\mathbb{F}_q$.*

Demonstração. Seja C um código linear auto-ortogonal de comprimento n, ou seja, $C \subseteq C^{\perp}$, e sejam $c, d \in \phi_0(C)$. Então, existem $\alpha, \beta \in C$ tais que $c = \phi_0(\alpha)$ e $d = \phi_0(\beta)$, onde

$$\alpha = ((1-v)a_1 + (1+v)b_1, (1-v)a_2 + (1+v)b_2, \ldots, (1-v)a_n + (1+v)b_n) = (1-v)a + (1+v)b$$

e

$$\beta = ((1-v)\tilde{a}_1 + (1+v)\tilde{b}_1, (1-v)\tilde{a}_2 + (1+v)\tilde{b}_2, \ldots, (1-v)\tilde{a}_n + (1+v)\tilde{b}_n) = (1-v)\tilde{a} + (1+v)\tilde{b},$$

com $a_i, b_i, \tilde{a}_i, \tilde{b}_i \in \mathbb{F}_q^n$, para todo $i = 1, 2, \ldots, n$. Para provar que $\phi_0(C)$ é auto-ortogonal, precisamos mostrar que $\langle c, d\rangle = 0$. Como C é auto-ortogonal, temos que

$$\begin{aligned} 0 &= \langle \alpha, \beta\rangle = \sum_{i=1}^{n}((1-v)a_i + (1+v)b_i)((1-v)\tilde{a}_i + (1+v)\tilde{b}_i) \\ &= \sum_{i=1}^{n} 2(1-v)a_i\tilde{a}_i + 2(1+v)b_i\tilde{b}_i \\ &= 2(1-v)\sum_{i=1}^{n} a_i\tilde{a}_i + 2(1+v)\sum_{i=1}^{n} b_i\tilde{b}_i \\ &= 2(1-v)\langle a, \tilde{a}\rangle + 2(1+v)\langle b, \tilde{b}\rangle. \end{aligned}$$

Como $R = (1-v)\mathbb{F}_q \oplus (1+v)\mathbb{F}_q$, temos $\langle a, \tilde{a}\rangle = 0$ e $\langle b, \tilde{b}\rangle = 0$.

Além disso, note que $\phi_0(\alpha) = ((a_i, b_i)M)_{1\leq i\leq n}$ e $\phi_0(\beta) = \left((\tilde{a}_i, \tilde{b}_i)M\right)_{1\leq i\leq n}$. Então,

$$\begin{aligned} \langle c, d\rangle &= \langle \phi_0(\alpha), (\phi_0(\beta))\rangle = \sum_{i=1}^{n}\langle (a_i, b_i)M, (\tilde{a}_i, \tilde{b}_i)M\rangle \\ &= \sum_{i=1}^{n}(a_i, b_i)M \cdot ((\tilde{a}_i, \tilde{b}_i)M)^{\perp} = \sum_{i=1}^{n}(a_i, b_i)MM^{\perp}(\tilde{a}_i, \tilde{b}_i)^{\perp} \\ &= \lambda\sum_{i=1}^{n}(a_i, b_i)(\tilde{a}_i, \tilde{b}_i)^{\perp} = \lambda\sum_{i=1}^{n}(a_i\tilde{a}_i + b_i\tilde{b}_i) \\ &= \lambda\left(\sum_{i=1}^{n} a_i\tilde{a}_i + \sum_{i=1}^{n} b_i\tilde{b}_i\right) = \lambda(\langle a, \tilde{a}\rangle + \langle b, \tilde{b}\rangle) = 0. \end{aligned}$$

Como supomos que $c, d \in \phi_0(C)$, temos $\phi_0(C) \subseteq \phi_0(C)^{\perp}$. Assim, $\phi_0(C)$ é um código linear auto-ortogonal de comprimento $2n$ sobre $\mathbb{F}_q$. □

Corolário 3.15. *Sejam $\alpha = (1-v)a + (1+v)b \in R^n$ e $\beta = (1-v)\tilde{a} + (1+v)\tilde{b} \in R^n$, onde $a, b, \tilde{a}, \tilde{b} \in \mathbb{F}_q^n$ são como no teorema anterior. Então,*

$$\langle \alpha, \beta\rangle = 2(1-v)\langle a, \tilde{a}\rangle + 2(1+v)\langle b, \tilde{b}\rangle$$

e

$$\langle \phi_0(\alpha), \phi_0(\beta)\rangle = \lambda\left(\langle a, \tilde{a}\rangle + \langle b, \tilde{b}\rangle\right).$$

Demonstração. Segue diretamente da prova do teorema anterior. □

Capítulo 4

Códigos LCD

O objetivo deste capitulo é caracterizar de forma abrangente o código cíclico LCD de comprimento n, em relação aos polinômios geradores. Para alcançar esse objetivo, vamos primeiro relembrar a estrutura dos códigos LCD sobre $\mathbb{F}_q$, conforme estabelecido no Lema 4.20 e no Lema 4.23. Portanto, estaremos fornecendo uma compreensão completa e aprofundada dos códigos cíclicos LCD em relação aos polinômios geradores.

4.1 Polinômios Geradores de um Código Cíclico

A teoria que vamos abordar nesta seção é de suma importância para as seções seguintes sobre os códigos LCD.

Definição 4.1. *Definimos o seguinte isomorfismo linear:*

$$t : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/(x^n - 1),$$

dada por $t(c_0, \ldots, c_{n-1}) = \overline{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}}$.

Vamos provar que t é uma transformação linear de $\mathbb{F}_q$-espaços vetoriais. De fato, se $(a_0, \ldots, a_{n-1}), (b_0, \ldots, b_{n-1}) \in \mathbb{F}_q^n$ e $\lambda \in \mathbb{F}_q$, temos

$$\begin{aligned} t((a_0, \ldots, a_{n-1}) + \lambda(b_0, \ldots, b_{n-1})) &= t(a_0 + \lambda b_0, \ldots, a_{n-1} + \lambda b_{n-1}) \\ &= \overline{a_0 + \lambda b_0 + (a_1 + \lambda b_1)x + \cdots + (a_{n-1} + \lambda b_{n-1})x^{n-1}} \\ &= \overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}} + \lambda\overline{b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}} \\ &= t(a_0, \ldots, a_{n-1}) + \lambda t(b_0, \ldots, b_{n-1}). \end{aligned}$$

Assim, t é uma transformação linear. Vejamos que t é injetora.

$$\begin{aligned} (c_0, \ldots, c_{n-1}) \in \ker(t) &\iff t(c_0, \ldots, c_{n-1}) = \overline{0} \\ &\iff c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1}x^{n-1} \in (x^n - 1) \\ &\iff c_0 = c_1 = c_2 = \cdots = c_{n-1} = 0. \end{aligned}$$

Logo, t é injetora, pois $\ker(t) = \{0\}$. Como ambos espaços têm q^n elementos, t é sobrejetora. Assim temos que t é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais. Note que $\dim(\mathbb{F}_q^n) = n$ e $\dim(\mathbb{F}_q[x]/(x^n - 1)) = n$. Denotemos por $\{e_1, \ldots, e_n\}$ a base canônica de $\mathbb{F}_q^n$. Observe que $\{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$ é uma base de $\mathbb{F}_q[x]/(x^n - 1)$.

Lembremos que, se C é um código linear em $\mathbb{F}_q^n$, então C é subespaço vetorial de $\mathbb{F}_q^n$ e, portanto, $t(C)$ é subespaço vetorial de $\mathbb{F}_q[x]/(x^n - 1)$.

Proposição 4.2. *Seja C um subconjunto de $\mathbb{F}_q^n$. Temos que C é um código linear cíclico se, e somente se, $t(C)$ é um ideal de $\mathbb{F}_q[x]/(x^n-1)$.*

Demonstração. Suponha que C é um código linear cíclico. Já sabemos que $t(C)$ é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[x]/(x^n-1)$, ou seja, para $\overline{a(x)}, \overline{b(x)} \in t(C)$ e $\lambda \in \mathbb{F}_q$, temos

$$\overline{a(x)+b(x)} \in t(C) \quad \text{e} \quad \lambda\overline{a(x)} \in t(C).$$

Para provar que $t(C)$ é ideal de $\mathbb{F}_q[x]/(x^n-1)$, resta provar que se $\overline{a(x)} \in \mathbb{F}_q[x]/(x^n-1)$ e $\overline{b(x)} \in t(C)$, então $\overline{a(x)b(x)} \in t(C)$.

Seja $b(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in \mathbb{F}[x]$ tal que $\overline{b(x)} \in t(C)$, ou seja, $(b_0, \ldots, b_{n-1}) \in C$. Então

$$\begin{aligned} \overline{x} \cdot \overline{b(x)} &= \overline{b_0x + b_1x^2 + \cdots + b_{n-1}x^n} \\ &= \overline{b_{n-1} + b_0x + b_1x^2 + \cdots + b_{n-2}x^{n-2}} \\ &= t(b_{n-1}, b_0, b_1, \ldots, b_{n-2}) \end{aligned}$$

Como C é cíclico, $(b_{n-1}, b_0, b_1, \ldots, b_{n-2}) \in C$, logo $\overline{x} \cdot \overline{b(x)} \in t(C)$. Se escrevemos

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1},$$

então $\overline{a(x)b(x)} \in t(C)$, já que por indução temos que, para todo $j \geq 0$, $\overline{a_jx^j} \cdot \overline{b(x)} \in t(C)$. Assim, $t(C)$ é um ideal de $\mathbb{F}_q[x]/(x^n-1)$.

Suponha agora que $t(C)$ é um ideal de $\mathbb{F}_q[x]/(x^n-1)$. Já sabemos que C é um código linear. Provemos que C é cíclico. Considere $(a_0, ..., a_{n-1}) \in C$. Como $\overline{x} \cdot t(a_0, \ldots, a_{n-1}) \in t(C)$, temos

$$\begin{aligned} \overline{x} \cdot t(a_0, \ldots, a_{n-1}) &= \overline{x} \cdot \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} = \overline{a_0x + a_1x^2 + \cdots + a_{n-1}x^n} \\ &= \overline{a_{n-1} + a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1}} = t(a_{n-1}, a_0, \ldots, a_{n-2}) \in t(C). \end{aligned}$$

Logo, $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C$, ou seja, C é cíclico. □

Estamos agora interessados em ver como são os ideais de $\mathbb{F}_q[x]/(x^n-1)$. Para isto definamos

$$\pi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q[x]/(x^n-1),$$

o homomorfismo quociente.

Os ideais de $\mathbb{F}_q[x]/(x^n-1)$ são da forma $\pi(I)$, onde I é um ideal de $\mathbb{F}_q[x]$ que contem (x^n-1), ou seja, $(x^n-1) \subseteq I$. Como $\mathbb{F}_q[x]$ é um domínio euclidiano, com a função grau, então $\mathbb{F}_q[x]$ é um domínio principal. Isso implica para todo ideal I existe um único $g(x) \in \mathbb{F}_q[x]$ mônico tal que $I = (g(x))$.

Se $(x^n-1) \subseteq I = (g(x))$ então $x^n - 1 \in (g(x))$, ou seja, existe $h(x) \in \mathbb{F}_q[x]$ tal que $x^n - 1 = g(x)h(x)$. Em particular, todo ideal de $\mathbb{F}_q[x]/(x^n-1)$ é da forma $(\overline{g(x)})$, onde $g(x) \in \mathbb{F}_q[x]$ é mônico e $g(x) \mid x^n - 1$.

Definição 4.3. *Se C é um código cíclico, o polinômio mônico $g(x) \in \mathbb{F}_q[x]$ tal que $g(x) \mid x^n-1$ e $t(C) = (\overline{g(x)})$, é chamado de* ***polinômio gerador do código*** *C.*

Observe que se C é um código linear cíclico e $g(x)$ é o polinômio gerador de C, então $C = t^{-1}((\overline{g(x)}))$.

Proposição 4.4. *Seja C um código cíclico. C é de dimensão k se, e somente se, o polinômio gerador de C é de* grau $n-k$.

Demonstração. Da hipótese temos que $t(C) = (\overline{g(x)})$, onde $g(x) \in \mathbb{F}_q[x]$ é mônico e divisor de $x^n - 1$. Se grau $g(x) = n - k$, devemos provar que $\dim(\overline{g(x)}) = k$. Considere o seguinte conjunto

$$V = \{\overline{g(x)a(x)} \mid a(x) = 0 \text{ ou grau } a(x) < k\}.$$

Provemos que uma base de V é $\{\overline{g(x)}, \overline{xg(x)}, \ldots, \overline{x^{k-1}g(x)}\}$, isto é, $\dim V = k$. Seja $\overline{a(x)g(x)} \in V$, com $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} \in \mathbb{F}_q[x]$. Então,

$$\overline{a(x)g(x)} = a_0\overline{g(x)} + a_1\overline{xg(x)} + \cdots + a_{k-1}\overline{x^{k-1}g(x)},$$

ou seja, $\{\overline{g(x)}, \overline{xg(x)}, \ldots, \overline{x^{k-1}g(x)}\}$ gera V.

Suponha que

$$\alpha_0\overline{g(x)} + \alpha_1\overline{xg(x)} + \cdots + \alpha_{k-1}\overline{x^{k-1}g(x)} = 0,$$

para $\alpha_0, \alpha_1, \ldots, \alpha_{k-1} \in \mathbb{F}_q$. Escrevendo

$$\alpha(x) = \alpha_0 + \alpha_1x + \cdots + \alpha_{k-1}x^{k-1},$$

temos $\overline{\alpha(x)g(x)} = \overline{0}$, ou seja, $\alpha(x)g(x) \in (x^n - 1)$. Mas se $\alpha(x) \neq 0$, então

$$\text{grau } \alpha(x)g(x) = \text{grau } \alpha(x) + \text{grau } g(x) \leq k - 1 + n - k = n - 1.$$

Como todo múltiplo não nulo de $x^n - 1$ é de grau maior igual a n, isto é um contradição. Logo, $\alpha(x) = 0$, ou seja, $\alpha_0 = \alpha_1 = \cdots = \alpha_{k-1} = 0$. Assim,

$$\{\overline{g(x)}, \overline{xg(x)}, \ldots, \overline{x^{k-1}g(x)}\}$$

é base de V, ou seja, $\dim V = k$.

Por definição $V \subseteq (\overline{g(x)})$. Seja $\overline{f(x)} \in (\overline{g(x)})$, então

$$\overline{f(x)} = \overline{g(x)\tilde{f}(x)},$$

para algum $\tilde{f}(x) \in \mathbb{F}_q[x]$. Lembremos que se $\overline{f(x)} = \overline{g(x)\tilde{f}(x)}$, então

$$f(x) = g(x)\tilde{f}(x) + (x^n - 1)\tilde{\tilde{f}}(x),$$

para algum $\tilde{\tilde{f}}(x) \in \mathbb{F}_q[x]$.

Além disso, como $g(x) \mid x^n - 1$, definindo $h(x) = (x^n - 1)/g(x)$, temos

$$f(x) = g(x)(\tilde{f}(x) + h(x)\tilde{\tilde{f}}(x)).$$

Pelo algoritmo da divisão, existem $q(x), r(x) \in \mathbb{F}_q[x]$, com $r(x) = 0$ ou grau $r(x) <$ grau $h(x) = k$, tais que

$$\tilde{f}(x) + h(x)\tilde{\tilde{f}}(x) = h(x)q(x) + r(x).$$

Dessa forma, $f(x) = g(x)(h(x)q(x) + r(x)) = (x^n - 1)q(x) + g(x)r(x)$, ou seja,

$$\overline{f(x)} = \overline{r(x)g(x)}.$$

Como $r(x) = 0$ ou grau $r(x) < k$, temos $\overline{f(x)} \in V$. Concluímos que

$$V = (\overline{g(x)}) \quad \text{e} \quad \dim(\overline{g(x)}) = k.$$

Em particular, $\dim C = k$ se, e somente se, grau $g(x) = n - k$. □

Corolário 4.5. *Se* $g(x) = a_0 + a_1x + \cdots + a_{n-k-1}x^{n-k-1} + x^{n-k} \in \mathbb{F}_q[x]$ *é o polinômio gerador de* C*, então*

$$\{(a_0, a_1, \ldots, a_{n-k-1}, 1, 0, \ldots, 0), (0, a_0, a_1, \ldots, a_{n-k-1}, 1, 0, \ldots, 0), (\underbrace{0, \ldots, 0}_{k-1}, a_0, a_1, \ldots, a_{n-k-1}, 1)\}$$

é base de C

Demonstração. Na prova da proposição anterior vimos que uma base de $(\overline{g(x)})$ como $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q[x]/(x^n - 1)$ é

$$\{\overline{g(x)}, \overline{xg(x)}, \ldots, \overline{x^{k-1}g(x)}\}.$$

Como $C = t^{-1}(\overline{g(x)})$, então

$$\{t^{-1}(\overline{g(x)}), t^{-1}(\overline{xg(x)}), t^{-1}(\overline{x^2g(x)}), \cdots, t^{-1}(\overline{x^{k-1}g(x)})\}$$

é base de C. Note que

$$\begin{aligned} t^{-1}(\overline{g(x)}) &= (a_0, a_1, \ldots, a_{n-k-1}, 1, 0, \ldots, 0). \\ t^{-1}(\overline{xg(x)}) &= (0, a_0, a_1, \ldots, a_{n-k-1}, 1, 0, \ldots, 0). \\ &\vdots \\ t^{-1}(\overline{x^{k-1}g(x)}) &= (\underbrace{0, \ldots, 0}_{k-1}, a_0, a_1, \ldots, a_{n-k-1}, 1). \end{aligned}$$

□

Definição 4.6. *Seja* $h(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_0 \in \mathbb{F}_q[x]$*. O* ***polinômio recíproco*** *de* $h(x)$ *é* $h^*(x) = a_0x^k + a_1x^{k-1} + \cdots + a_k$*. Se* $h(x)$ *for mônico e* $h(0) \neq 0$*, ou seja, se* $a_k = 1$ *e* $a_0 \neq 0$*, definimos o* ***polinômio reciproco mônico*** *de* $h(x)$*, como sendo o polinômio mônico associado ao reciproco de* $h(x)$ *(denotado por* $\tilde{h}(x)$*), ou seja,* $\tilde{h}(x) = h(0)^{-1}h^*(x)$*.*

Observe que se h é de grau k, então $h^*(x) = x^kh(1/x)$ e se h for mônico e $h(0) \neq 0$, então $\tilde{h}(x) = x^kh(0)^{-1}h(1/x)$.

Definição 4.7. *Diremos que o polinômio mônico* $h(x)$*, com* $h(0) \neq 0$*, é* ***auto-recíproco*** *se* $\tilde{h}(x) = h(x)$*.*

Antes de enunciar o próximo lema, gostaríamos de lembrar que T_π foi definido na Definição 2.11 e o isomorfismo t foi definido no início do capítulo.

Lema 4.8. *Para todo* $c \in \mathbb{F}_q^n$*, temos* $t(T_\pi(c)) = \overline{xt(c)}$*.*

Demonstração. Seja $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$, veja que

$$\begin{aligned} t(T_\pi(c)) &= t(c_{n-1}, c_0, \ldots, c_{n-2}) \\ &= \overline{c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-2}} \\ &= \overline{c_{n-1}x^n + c_0x + \cdots + c_{n-2}x^{n-2}} \\ &= \overline{x}(\overline{c_0 + c_1x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}}) \\ &= \overline{xt(c)}. \end{aligned}$$

□

Lema 4.9. *Sejam $g(x) \in \mathbb{F}_q[x]$ de grau $n-k$ e $f(x) \in \mathbb{F}_q[x]$ um polinômio de grau menor que n. Sejam ainda $a = t^{-1}(\overline{g(x)})$ e $b = t^{-1}(\overline{f(x)})$. Então,*

$$\begin{aligned}\overline{f(x)g^*(x)} &= \overline{\langle T_\pi^{-(n-k)}(a), b\rangle + \langle T_\pi^{-(n-k)+1}(a), b\rangle x + \cdots + \\ &\quad + \langle a, b\rangle x^{n-k} + \langle T_\pi(a), b\rangle x^{n-k+1} + \cdots + \langle T_\pi^{k-1}(a), b\rangle x^{n-1}} \\ &= \sum_{d=0}^{n-1} \langle T_\pi^{-(n-k)+d}(a), b\rangle \overline{x^d}.\end{aligned}$$

Demonstração. Denotemos $a = (a_0, a_1, \ldots, a_{n-k}, 0, \ldots, 0)$ e $b = (b_0, \ldots, b_{n-1})$. Dessa forma $g(x) = a_0 + a_1 x + \cdots + a_{n-k}x^{n-k}$ e $f(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ e, desse modo, $g^*(x) = a_{n-k} + a_{n-k-1}x + \cdots + a_1 x^{n-k-1} + a_0 x^{n-k}$.

Calculemos primeiro o produto

$$\begin{aligned}f(x)g^*(x) &= \left(\sum_{i=0}^{n-1} b_i x^i\right)\left(\sum_{j=0}^{n-k} a_{n-k-j}x^j\right) \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-k}(b_i a_{n-k-j}x^{i+j}).\end{aligned}$$

Para $d = i + j$, temos $0 \leq d \leq n-1+n-k$. Dividimos os valores de d em três casos:

(1) $0 \leq d \leq n-k-1$

(2) $n-k \leq d \leq n-1$

(3) $n \leq d \leq n+n-k-1$

Caso (1): Quando $0 \leq d \leq n-k-1$, como $d = i+j$, os valores de i e j variam de acordo com a seguinte tabela:

i	0	1	$\cdots$	d
j	d	$d-1$	$\cdots$	0

Nesse caso, $0 \leq i \leq d$ e $j = d - i$, satisfaz $0 \leq j = d - i \leq d \leq n-k-1$. Logo, a soma parcial de $f(x)g^*(x)$, com $0 \leq d \leq n-k-1$ é

$$\sum_{d=0}^{n-k-1}\left(\sum_{i=0}^{d} b_i a_{n-k-d+i}\right)x^d.$$

Caso (2): Quando $n-k \leq d \leq n-1$, como $d = i+j$, os valores de i e j variam de acordo com a seguinte tabela:

i	$d-(n-k)$	$d-(n-k-1)$	$\cdots$	d
j	$n-k$	$n-k-1$	$\cdots$	0

Escrevendo $l = n-k-j$, temos $0 \leq l \leq n-k$ e $i = d-(n-k-l) = d-(n-k)+l$. Assim, Logo, a soma parcial de $f(x)g^*(x)$, correspondente a $n-k \leq d \leq n-1$ é

$$\sum_{d=n-k}^{n-1}\left(\sum_{l=0}^{n-k} b_{d-(n-k)+l}a_l\right)x^d.$$

Caso (3): Quando $n \leq d \leq n+n-k-1$, como $d = i+j$, os valores de i e j variam de acordo com a seguinte tabela:

i	$n-1$	$n-2$	$\cdots$	$d-(n-k)$
j	$d-(n-1)$	$d+1-(n-1)$	$\cdots$	$n-k$

Nesse caso, $d-(n-k) \leq i \leq n-1$ e, como $j = d-i$, temos $n-k-j = n-k-(d-i) = i-(d-n+k)$. Logo, a soma parcial de $f(x)g^*(x)$, correspondente a $n \leq d \leq n+n-k-1$ é

$$\sum_{d=n}^{n+n-k-1} \left(\sum_{i=d-n+k}^{n-1} b_i a_{i-(d-n+k)} \right) x^d.$$

Como no anel $\mathbb{F}_q[x]/(x^n-1)$, temos $\overline{x^n} = \overline{1}$, vamos realizar a substituição $d = n + \tilde{d}$. Já que $\overline{x^d} = \overline{x^{\tilde{d}}}$, temos

$$\sum_{d=n}^{n+n-k-1} \left(\sum_{i=d-n+k}^{n-1} b_i a_{i-(d-n+k)} \right) \overline{x^d} = \sum_{\tilde{d}=0}^{n-k-1} \left(\sum_{i=d+k}^{n-1} b_i a_{i-\tilde{d}-k} \right) \overline{x^{\tilde{d}}}.$$

Substituindo a nova variável $\tilde{d}$ por d, podemos escrever

$$\sum_{d=n}^{n+n-k-1} \left(\sum_{i=d-n+k}^{n-1} b_i a_{i-(d-n+k)} \right) \overline{x^d} = \sum_{d=0}^{n-k-1} \left(\sum_{i=d+k}^{n-1} b_i a_{i-d-k} \right) \overline{x^d}.$$

A partir dos três casos acima, deduzimos que $\overline{f(x)g^*(x)}$ é da forma

$$\begin{aligned} \overline{f(x)g^*(x)} &= \sum_{d=0}^{n-k-1} \left(\sum_{i=0}^{d} b_i a_{n-k-d+i} \right) \overline{x^d} + \sum_{d=n-k}^{n-1} \left(\sum_{l=0}^{n-k} b_{d-(n-k)+l} a_l \right) \overline{x^d} \\ &\quad + \sum_{d=0}^{n-k-1} \left(\sum_{i=d+k}^{n-1} b_i a_{i-d-k} \right) \overline{x^d}. \end{aligned}$$

Em outras palavras,

$$\overline{f(x)g^*(x)} = \sum_{d=0}^{n-k-1} \left(\sum_{i=0}^{d} b_i a_{n-k-d+i} + \sum_{i=d+k}^{n-1} b_i a_{i-d-k} \right) \overline{x^d} + \sum_{d=n-k}^{n-1} \left(\sum_{l=0}^{n-k} b_{d-(n-k)+l} a_l \right) \overline{x^d}.$$

Para $1 \leq j \leq n-k$, temos

$$T_\pi^{-j}(a) = (a_j, a_{j+1}, \ldots, a_{n-k}, 0, \ldots, 0, a_0, \ldots, a_{j-3}, a_{j-2}, a_{j-1}).$$

Assim,

$$\langle T_\pi^{-j}(a), b \rangle = a_j b_0 + \cdots + a_{n-k} b_{n-k-j} + a_0 b_{n-j} + \cdots + a_{j-1} b_{n-1}$$

Escrevendo $d = (n-k) - j$, vemos que se $1 \leq j \leq n-k$, então $0 \leq d \leq n-k-1$, e o produto interno pode ser escrito como

$$\begin{aligned} \langle T_\pi^{-(n-k)+d}(a), b \rangle &= a_{(n-k)-d} b_0 + \cdots + a_{n-k} b_d + a_0 b_{d+k} + \cdots + a_{(n-1)-d-k} b_{n-1} \\ &= \sum_{i=0}^{d} a_{n-k-d+i} b_i + \sum_{i=d+k}^{n-1} a_{i-d-k} b_i. \end{aligned}$$

Ou seja, $\langle T_\pi^{-(n-k)+d}(a), b \rangle$ é o coeficiente de $\overline{x^d}$ em $\overline{f(x)g^*(x)}$, para $0 \leq d \leq n-k-1$.

Agora, para $0 \leq j \leq k-1$, temos

$$T_\pi^j(a) = (\underbrace{0, 0, \ldots, 0}_{j}, a_0, \ldots, a_{n-k}, 0, \ldots, 0)$$

Assim,

$$\langle T_\pi^j(a), b\rangle = a_0 b_j + \cdots + a_{n-k} b_{n-k+j}.$$

Escrevendo $d = (n-k)+j$, vemos que se $0 \leq j \leq k-1$, então $n-k \leq d \leq n-1$, e o produto interno pode ser escrito como

$$\langle T_\pi^{d-(n-k)}(a), b\rangle = a_0 b_{d-(n-k)} + \cdots + a_{n-k} b_d = \sum_{l=0}^{n-k} a_l b_{d-(n-k)+l}.$$

Ou seja, $\langle T_\pi^{d-(n-k)}(a), b\rangle$ é o coeficiente de $\overline{x^d}$ em $\overline{f(x)g^*(x)}$, para $n-k \leq d \leq n-1$. Dessa forma obtemos o resultado desejado. □

Motivados pelo lema acima vamos provar o seguinte resultado:

Lema 4.10. *Seja C um código cíclico sobre $\mathbb{F}_q$ de polinômio gerador $g(x) \in \mathbb{F}_q[x]$ de grau $n-k$, e seja ainda $a = t^{-1}(g(x))$. Então, $b \in C^\perp$ se, e somente se, $\langle T_\pi^j(a), b\rangle = 0$, para todo $-(n-k) \leq j \leq k-1$.*

Demonstração. Pelo Corolário 4.5, $\{a, T_\pi(a), \ldots, T_\pi^{k-1}(a)\}$ é uma base de C. Observe que um elemento $b \in C^\perp$ se, e somente se, b é perpendicular aos elementos de uma base de C. Por outro lado, se b for perpendicular aos elementos de uma base de C, será perpendicular a todos os elementos de C e, em particular, também será perpendicular aos elementos $T_\pi^j(a)$ para $-(n-k) \leq j < 0$, pois também são elementos de C. □

Lema 4.11. *Sejam $g(x) \in \mathbb{F}_q[x]$ um divisor mônico de $x^n - 1$ e $h(x) = (x^n-1)/g(x)$. Para todo $f(x) \in \mathbb{F}_q[x]$ temos que $\overline{g(x)f(x)} = \overline{0}$ se, e somente se, $\overline{f(x)} \in (\overline{h(x)})$.*

Demonstração. Suponha $\overline{g(x)f(x)} = \overline{0}$. Então existe $s(x) \in \mathbb{F}_q[x]$ tal que

$$g(x)f(x) = (x^n - 1)s(x).$$

Já que $x^n - 1 = g(x)h(x)$, então $g(x)f(x) = g(x)h(x)s(x)$. Como $\mathbb{F}_q[x]$ é um domínio, então $f(x) = h(x)s(x)$, ou seja $\overline{f(x)} \in (\overline{h(x)})$.

Suponha agora que $\overline{f(x)} \in (\overline{h(x)})$. Isso implica que existe $s(x) \in \mathbb{F}_q[x]$ tal que

$$\overline{f(x)} = \overline{h(x)s(x)}.$$

Logo, existe $u(x) \in \mathbb{F}_q[x]$ tal que

$$f(x) = h(x)s(x) + (x^n - 1)u(x).$$

Dessa forma,

$$\begin{aligned} g(x)f(x) &= \underbrace{g(x)h(x)}_{(x^n-1)} s(x) + g(x)(x^n-1)u(x) \\ &= (x^n-1)(s(x) + g(x)u(x)), \end{aligned}$$

que implica $\overline{g(x)f(x)} = \overline{0}$. □

Observe que se $x^n - 1 = g(x)h(x)$, então $g(0)h(0) = -1$ e

$$\begin{aligned} \tilde{g}(x)\tilde{h}(x) &= g(0)^{-1}x^{n-k}g(1/x)h(0)^{-1}x^k h(1/x) \\ &= g(0)h(0)x^n g(1/x)h(1/x) \\ &= (-1)x^n((1/x)^n - 1) \\ &= x^n - 1. \end{aligned}$$

Logo, o lema anterior também pode ser aplicado aos polinômios $\tilde{g}(x)$ e $\tilde{h}(x)$ (de fato é isso que faremos).

Proposição 4.12. *Se $g(x)$ é o polinômio gerador do código cíclico C, então $C^{\perp}$ é cíclico e seu polinômio gerador é $\tilde{h}(x)$, onde $h(x) = (x^n - 1)/g(x)$.*

Demonstração. Pelo Lema 4.10, $b \in C^{\perp}$ se, e somente se, $\langle T_{\pi}^{j}(a), b\rangle = 0$, para todo $-(n-k) \leq j \leq k-1$. Denotando $\overline{f(x)} = t(b)$, pelo Lema 4.9, a última asserção equivale a dizer que $\overline{f(x)g^{*}(x)} = \overline{0}$. Como $g(x)$ e $\tilde{g}(x)$ são associados, então $b \in C^{\perp}$ exatamente quando $\overline{f(x)\tilde{g}(x)} = \overline{0}$. Agora, pelo Lema 4.11, temos $b = t^{-1}(\overline{f(x)}) \in C^{\perp}$ se, e somente se, $\overline{f(x)} \in (\tilde{h}(x))$. Em outras palavras, $t(C^{\perp}) = (\tilde{h}(x))$ e, pela Proposição 4.2, $C^{\perp}$ é cíclico. □

4.2 Códigos Cíclicos sobre o Anel Semilocal não Encadeado

Esta seção aborda o estudo de códigos cíclicos e sua relação com códigos duais, com o objetivo de obter códigos quânticos utilizando a construção CSS (Calderbank-Shor-Steane). Os códigos cíclicos são caracterizados como ideais em um anel comutativo finito. Nesta seção, apresentaremos resultados importantes, desde teoremas até provas, que fornecem condições necessárias e suficientes para a existência de códigos cíclicos que contenham seu código dual. Esses resultados são fundamentais para a construção de códigos quânticos eficientes e robustos.

Vamos explorar resultados e teoremas, que caracterizam os códigos cíclicos e seus códigos duais. Os principais resultados serão abordados com base em referências como [2], [11] e [13] onde são apresentadas provas e estudos relacionados. Essas referências são fundamentais para o desenvolvimento da teoria e para a compreensão dos conceitos envolvidos na construção de códigos quânticos utilizando a técnica CSS.

O definição de código cíclico sobre R é equivalente à definição de código cíclico sobre um corpo finito.

Definição 4.13. *Um código linear C de comprimento n sobre R será chamado de* ***código cíclico*** *se, para todo $c = (c_0, \ldots, c_{n-1}) \in C$, temos $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.*

Lema 4.14. *Seja $C = (1-v)C_1 \oplus (1+v)C_2$ um código linear sobre R. Então C é um código cíclico sobre R se, e somente se, C_1 e C_2 são códigos cíclicos.*

Demonstração. Seja T_{π} como na Definição 2.11. Estendemos a definição de T_{π} a R^n de forma natural. Ou seja, se $(\alpha_0, \ldots, \alpha_{n-1}) \in R^n$, então $T_{\pi}(\alpha_0, \ldots, \alpha_{n-1}) = (\alpha_{n-1}, \alpha_0, \ldots, \alpha_{n-2})$.

Sejam $c \in C_1$ e $d \in C_2$. Se C_1 e C_2 são códigos cíclicos, então $T_{\pi}(c) \in C_1$ e $T_{\pi}(d) \in C_2$. Para cada $\alpha \in C$, existem únicos $c \in C_1$ e $d \in C_2$ tais que $\alpha = (1-v)c + (1+v)d$. Veja que $T_{\pi}(\alpha) = (1-v)T_{\pi}(c) + (1+v)T_{\pi}(d)$, como $T_{\pi}(c) \in C_1$ e $T_{\pi}(d) \in C_2$ então $T_{\pi}(\alpha) \in C$, ou seja, C é cíclico.

Por outro lado, seja $c \in C_1$, então $\alpha = (1-v)c + (1+v)0 = (1-v)c \in C$. Logo, $T_{\pi}(\alpha) = (1-v)T_{\pi}(c) \in C$, ou seja, $T_{\pi}(c) \in C_1$. Da mesma forma, se $d \in C_2$, então $\alpha = (1-v)0 + (1+v)d = (1+v)d \in C$. Portanto, $T_{\pi}(\alpha) = (1+v)T_{\pi}(d) \in C$, daí que $T_{\pi}(d) \in C_2$. Em outras palavras, C_1 e C_2 são cíclicos. □

Da mesma forma que T_{π} foi estendido para uma transformação de R^n em R^n, podemos fazer a mesma coisa para a transformação t (ver Definição 4.1) e estender da seguinte forma:

Definição 4.15. *Definimos o seguinte isomorfismo linear:*

$$t : R^n \longrightarrow R[x]/(x^n - 1),$$

dada por $t(c_0, \ldots, c_{n-1}) = \overline{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}}$.

Como o polinômio $x^n - 1$ é mônico, o algoritmo da divisão em $R[x]$, com o divisor sendo $x^n - 1$, funciona. Ou seja, dado $f(x) \in R[x]$, existem únicos $q(x), r(x) \in R[x]$, tais que

$$f(x) = q(x)(x^n - 1) + r(x),$$

onde $r(x) = 0$ ou $\text{grau}(r(x)) \leq n - 1$. Em outras palavras, para todo $f(x) \in R[x]$, existe um polinômio $r(x)$ de grau menor ou igual a $n - 1$ tal que $\overline{f(x)} = \overline{r(x)}$ em $R[x]/(x^n - 1)$.

Como $R = (1 - v)\mathbb{F}_q + (1 + v)\mathbb{F}_q$, para todos $f(x), r(x) \in R[x]$, existem únicos

$$f_1(x), f_2(x), r_1(x), r_2(x) \in \mathbb{F}_q[x]$$

tais que $f(x) = (1 - v)f_1(x) + (1 + v)f_2(x)$ e $r(x) = (1 - v)r_1(x) + (1 + v)r_2(x)$. Além disso, $\overline{f(x)} = \overline{r(x)}$ em $R[x]/(x^n - 1)$ se, e somente se, $\overline{f_1(x)} = \overline{r_1(x)}$ e $\overline{f_2(x)} = \overline{r_2(x)}$ em $\mathbb{F}_q[x]/(x^n - 1)$.

Lema 4.16. *Seja $C = (1 - v)C_1 \oplus (1 + v)C_2$ um código cíclico de comprimento n sobre R. Então, $t(C) = (\overline{(1 - v)g_1(x)}, \overline{(1 + v)g_2(x)})$ e $|t(C)| = q^{2n - (\text{grau}(g_1(x)) + \text{grau}(g_2(x)))}$, onde $g_1(x)$ e $g_2(x)$ são os polinômios geradores de C_1 e C_2, respectivamente.*

Demonstração. Como $C_1 = (g_1(x))$, $C_2 = (g_2(x))$ e $C = (1 - v)C_1 \oplus (1 + v)C_2$, então $t(C) = \{\overline{(1 - v)g_1(x)r_1(x)} + \overline{(1 + v)g_2(x)r_2(x)} \mid r_1(x), r_2(x) \in \mathbb{F}_q[x]\}$. Portanto,

$$t(C) \subseteq (\overline{(1 - v)g_1(x)}, \overline{(1 + v)g_2(x)}) \subseteq R[x]/(x^n - 1).$$

Seja $\overline{(1 - v)g_1(x)t_1(x) + (1 + v)g_2(x)t_2(x)} \in (\overline{(1 - v)g_1(x)}, \overline{(1 - v)g_2(x)})$, onde $\overline{t_1(x)}, \overline{t_2(x)} \in R[x]/(x^n - 1)$. Como $\overline{g_1(x)t_1(x)} \in t(C_1)$ e $\overline{g_2(x)t_2(x)} \in t(C_2)$, então

$$\overline{(1 - v)g_1(x)t_1(x) + (1 + v)g_2(x)t_2(x)} \in (1 - v)t(C_1) + (1 + v)t(C_2) = t(C).$$

Isso implica a igualdade. Além disso, como $|t(C)| = |t(C_1)||t(C_2)|$, temos

$$|t(C)| = q^{2n - (\text{grau}(g_1(x)) + \text{grau}(g_2(x)))}.$$

□

Teorema 4.17. *Seja $C = (1 - v)C_1 \oplus (1 + v)C_2$ um código cíclico de comprimento n sobre R. Então, $t(C) = (\overline{g(x)})$, onde $g(x) = (1 - v)g_1(x) + (1 + v)g_2(x)$ e $g_i(x)$ é o polinômio gerador de C_i, para $i = 1, 2$.*

Demonstração. Pelo Lema 4.16, só precisamos provar que

$$(\overline{g(x)}) = (\overline{(1 - v)g_1(x)}, \overline{(1 + v)g_2(x)}).$$

Como $g(x) = (1 - v)g_1(x) + (1 + v)g_2(x)$, então $(\overline{g(x)}) \subseteq (\overline{(1 - v)g_1(x)}, \overline{(1 + v)g_2(x)})$.

Por outro lado, veja que

$$\begin{aligned} g(x) &= (1 - v)g_1(x) + (1 + v)g_2(x) \\ (1 - v)g(x) &= (1 - v)^2 g_1(x) + 0 \\ &= 2(1 - v)g_1(x). \end{aligned}$$

De forma similar, $(1 + v)g(x) = 2(1 + v)g_2(x)$. Como a característica é ímpar, temos

$$\begin{aligned} \overline{(1 - v)g_1(x)} &= \overline{2^{-1}(1 - v)g(x)} \in (\overline{g(x)}) \quad \text{e} \\ \overline{(1 + v)g_2(x)} &= \overline{2^{-1}(1 + v)g(x)} \in (\overline{g(x)}). \end{aligned}$$

Isto implica

$$(\overline{(1 - v)g_1(x)}, \overline{(1 + v)g_2(x)}) \subseteq (\overline{g(x)}).$$

Portanto, $t(C) = (\overline{g(x)})$. □

Teorema 4.18. *Seja $C = (1-v)C_1 \oplus (1+v)C_2$ um código cíclico de comprimento n sobre R e $t(C) = \overline{((1-v)g_1 + (1+v)g_2)}$, onde $g_i(x)$ é o polinômio gerador de C_i, para $i = 1, 2$. Então, $C^\perp \subseteq C$ se, e somente se, $x^n - 1 \equiv 0 \pmod{(g_i(x)\tilde{g}_i(x))}$.*

Demonstração. Para $i = 1, 2$, pela Proposição 4.12, o polinômio gerador de $C_i^\perp$ é $\tilde{h}_i(x)$.

Como $C^\perp \subseteq C$ é equivalente a $C_1^\perp \subseteq C_1$ e $C_2^\perp \subseteq C_2$. Provemos $C_1^\perp \subseteq C_1$ se, e somente se, $x^n - 1 \equiv 0 \pmod{(g_1(x)\tilde{g}_1(x))}$, pois o mesmo resultado valerá para $i = 2$.

Se $C_1^\perp \subseteq C_1$, então $t(C_1^\perp) \subseteq t(C_1)$, ou seja $\overline{\tilde{h}_1(x)} \in (\overline{g_1(x)})$. Assim, existe $k(x) \in \mathbb{F}_q[x]$ tal que $\tilde{h}_1(x) = g_1(x)k(x)$, ou seja, $g_1(x)k(x) = (x^n - 1)q(x) + \tilde{h}_1(x)$, para algum $q(x) \in \mathbb{F}_q[x]$. Como $g_1(x) \mid (x^n - 1)$, então $g_1(x) \mid \tilde{h}_1(x) = (x^n - 1)/\tilde{g}_1(x)$. Daí, $g_1(x)\tilde{g}_1(x) \mid (x^n - 1)$, ou seja, $x^n - 1 \equiv 0 \pmod{(g_1(x)\tilde{g}_1(x))}$.

Suponha agora que $g_1(x)\tilde{g}_1(x) \mid x^n - 1$. Nesse caso, $g_1(x) \mid (x^n - 1)/\tilde{g}_1(x) = \tilde{h}_1(x)$. Ou seja, $\overline{\tilde{h}_1(x)} \in (\overline{g_1(x)})$. Em outras palavras, $t(C_1^\perp) \subseteq t(C_1)$. □

4.3 Códigos LCD sobre o Anel Semilocal não Encadeado

É importante ressaltar que os resultados e análises apresentados nesta seção são baseados em três artigos importantes: [1], [10] e [12]. Tais artigos fornecem uma base sólida para nossas investigações e contribuem significativamente para o conhecimento existente nessa área.

Antes de tratar códigos cíclicos LCD sobre o anel R, relembraremos alguns resultados sobre códigos cíclicos LCD sobre um corpo finito.

Definição 4.19. *Um código linear C de comprimento n sobre $\mathbb{F}_q$, é dito* ***dual complementar linear*** *ou LCD, se $C \cap C^\perp = \{0\}$.*

Lema 4.20. *Seja C um código cíclico de comprimento n sobre $\mathbb{F}_q$ de polinômio gerador $g(x)$. Então, C é um código cíclico LCD se, e somente se, $g(x)$ é auto-recíproco e todos os fatores irredutíveis mônicos de $g(x)$ têm a mesma multiplicidade em $g(x)$ e em $x^n - 1$.*

Demonstração. Suponha que C é LCD. Pela Proposição 4.12, o polinômio gerador de $C^\perp$ é $\tilde{h}(x)$, sendo $h(x) = (x^n - 1)/g(x)$. Assim,

$$\{\overline{0}\} = t(C \cap C^\perp) = (\overline{g(x)}) \cap (\overline{\tilde{h}(x)}) = (\overline{\operatorname{mmc}(g(x), \tilde{h}(x))}).$$

Isso quer dizer que $\operatorname{mmc}(g(x), \tilde{h}(x))$ é múltiplo de $x^n - 1$. Por outro lado, $\operatorname{mmc}(g(x), \tilde{h}(x))$ é um divisor de $g(x)\tilde{h}(x)$, ou seja, $(x^n - 1) \mid g(x)\tilde{h}(x)$. Mas,

$$n \leq \operatorname{grau}(g(x)\tilde{h}(x)) = \operatorname{grau}(g(x)) + \operatorname{grau}(\tilde{h}(x)) = \operatorname{grau}(g(x)) + \operatorname{grau}(h(x)) = n.$$

Como, além disso, $g(x)$ e $\tilde{h}(x)$ são mônicos, então $g(x)\tilde{h}(x) = x^n - 1$. Daí $\tilde{g}(x) = g(x)$ e $\tilde{h}(x) = h(x)$. Para provar que todos os fatores irredutíveis mônicos de $g(x)$ têm a mesma multiplicidade em $g(x)$ e em $x^n - 1$, basta observar que $\operatorname{mmc}(g(x), h(x))$ é múltiplo de $x^n - 1$ e $\operatorname{mmc}(g(x), h(x))$ é um divisor de $g(x)h(x)$. Ou seja, $\operatorname{mmc}(g(x), h(x)) = g(x)h(x)$. Em outras palavras, $\operatorname{mdc}(g(x), h(x)) = 1$. Isso equivale a dizer que todos os fatores irredutíveis mônicos de $g(x)$ têm a mesma multiplicidade em $g(x)$ e em $x^n - 1$.

Suponha agora que $g(x)$ é auto-recíproco e que todo fator mônico irredutível de $g(x)$ tem mesma multiplicidade em $g(x)$ e em $x^n - 1$. Isso significa que $\operatorname{mdc}\left(g(x), \frac{x^n-1}{g(x)}\right) = 1$ e $\tilde{g}(x) = g(x)$. Dessa forma se $h(x) = (x^n - 1)/g(x)$, então $\tilde{h}(x) = h(x)$ é o polinômio gerador de $C^\perp$.

Como $\operatorname{mdc}(g(x), h(x)) = 1$, então

$$t(C \cap C^\perp) = (\overline{g(x)}) \cap (\overline{h(x)}) = (\operatorname{mmc}(\overline{g(x)}, \overline{h(x)})) = (\overline{g(x)h(x)}) = (\overline{x^n - 1}) = \{\overline{0}\}.$$

Portanto, C é um código LCD. □

Observação 4.21. *Assim como para $a, b \in \mathbb{F}_q$ temos $(a+b)^p = a^p + b^p$, também temos o mesmo resultado em $\mathbb{F}_q[x]$. Isto é, se $f(x), g(x) \in \mathbb{F}_q[x]$, então*

$$(f(x) + g(x))^p = f(x)^p + g(x)^p.$$

Dessa forma, no contexto do Lema 4.20, se $n = n_0 \cdot p^e$, tal que n_0 é primo com p, na prática podemos escolher $g(x)$ e $h(x)$ da seguinte forma:

$$\begin{aligned} x^n - 1 &= (x^{n_0} - 1)^{p^e} \\ &= (f_1 f_2 \cdots f_r f_{r+1} \cdots f_s)^{p^e} \\ &= \underbrace{(f_1 f_2 \cdots f_r)^{p^e}}_{g(x)} \underbrace{(f_{r+1} \cdots f_s)^{p^e}}_{h(x)}, \end{aligned}$$

onde $f_1, \ldots f_s$ são todos os fatores mônicos irredutíveis de $x^n - 1$.

Observação 4.22. *Observe também que se $\mathrm{mdc}(n, p) = 1$, então todo fator irredutível de $x^n - 1$ tem multiplicidade 1. Logo, todo fator mônico irredutível de $g(x)$ tem a mesma multiplicidade em $g(x)$ e em $x^n - 1$. Em particular, C é um código cíclico LCD, se e somente se, $g(x)$ é auto-reciproco.*

Lema 4.23. *Seja C um código cíclico de comprimento n sobre $\mathbb{F}_q$ de polinômio gerador $g(x)$, onde $\mathrm{mdc}(n, p) = 1$. Então, C é um código cíclico LCD se, e somente se, C é um código cíclico reversível.*

Demonstração. Suponha que C é LCD. Nesse caso, pela Observação 4.22, $g(x) = \tilde{g}(x)$. Seja $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, então $g(x) \mid f(x)$, onde $f(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$. Isso implica que $g^*(x) \mid f^*(x)$. Como $g(x) = \tilde{g}(x)$ e $g^*(x)$ são associados, então $g(x) \mid f^*(x)$. Em outras palavras, $(c_{n-1}, \ldots, c_0) = t^{-1}(f^*(x)) \in C$. Ou seja, C é reversível.

Agora suponha que C é reversível. Seja $t^{-1}(g(x)) = (a_0, \ldots, a_{n-k}, 0, \ldots, 0) \in C$. Como C é reversível, temos $(0, \ldots, 0, a_{n-k}, \ldots, a_0) \in C$. Em outras palavras, $t(0, \ldots, 0, a_{n-k}, \ldots, a_0) = x^{k-1} g^*(x) \in t(C)$ e, como C é cíclico, $g^*(x) \in t(C)$. Daí $g(x) \mid g^*(x)$, ou ainda, $g(x) \mid \tilde{g}(x)$. Como $g(x)$ e $\tilde{g}(x)$ são mônicos de mesmo grau, então $g(x) = \tilde{g}(x)$, em outras palavras C é LCD. □

Definição 4.24 (LCD)**.** *Como na Definição 4.19, um código linear C de comprimento n sobre R, é dito* ***dual complementar linear*** *ou LCD, se $C \cap C^\perp = \{0\}$.*

Teorema 4.25. *Seja $C = (1-v)C_1 \oplus (1+v)C_2$ um código de comprimento n sobre R. Então, C é um código LCD se, e somente se, C_1 e C_2 são códigos LCD sobre $\mathbb{F}_q$.*

Demonstração. Lembremos que $C = (1-v)C_1 \oplus (1+v)C_2$ e $C^\perp = (1-v)C_1^\perp \oplus (1+v)C_2^\perp$. Então suponha que C é um código LCD, ou seja,

$$C \cap C^\perp = (1-v)C_1 \cap C_1^\perp \oplus (1+v)C_2 \cap C_2^\perp = \{0\},$$

isto ocorre se, e somente se,

$$C_1 \cap C_1^\perp = \{0\} \quad \text{e} \quad C_2 \cap C_2^\perp = \{0\},$$

ou seja, C_1 e C_2 são códigos LCD. □

Teorema 4.26. *Sejam $C = (1-v)C_1 \oplus (1+v)C_2$ um código cíclico de comprimento n sobre R e $g_i(x)$ o polinômio gerador de C_i, para $i = 1, 2$. Então, C é um código cíclico LCD se, e somente se, $g_i(x)$ é auto-recíproco e todos os fatores irredutíveis mônicos de $g_i(x)$ têm a mesma multiplicidade em $g_i(x)$ e em $x^n - 1$ para $i = 1, 2$.*

Demonstração. Pelo Lema 4.14 e pelo Teorema 4.25, temos que C é um código cíclico LCD sobre R se, e somente se, C_1 e C_2 são códigos cíclicos LCD sobre $\mathbb{F}_q$. Por outro lado, pelo Lema 4.20, para $i = 1, 2$, dizer que C_i é um código cíclico LCD sobre $\mathbb{F}_q$ é equivalente a dizer que $g_i(x)$ é auto-recíproco e todos os fatores irredutíveis mônicos de $g_i(x)$ têm a mesma multiplicidade em $g_i(x)$ e em $x^n - 1$. □

Teorema 4.27. *Seja $C = (1-v)C_1 \oplus (1+v)C_2$ um código cíclico de comprimento n sobre R, com $\mathrm{mdc}(n, p) = 1$. Então, C é um código cíclico LCD se, e somente se, C_1 e C_2 são códigos cíclicos reversíveis de comprimento n.*

Demonstração. Como no teorema anterior, pelo Lema 4.14 e pelo Teorema 4.25, temos que C é um código cíclico LCD sobre R se, e somente se, C_1 e C_2 são códigos cíclicos LCD sobre $\mathbb{F}_q$. Como $\mathrm{mdc}(n, p) = 1$, aplicamos o Lema 4.23 que diz que C_1 e C_2 são códigos cíclicos LCD se, e somente se, C_1 e C_2 são códigos cíclicos reversíveis. □

Teorema 4.28. *Sejam $C = (1-v)C_1 \oplus (1+v)C_2$ um código cíclico de comprimento n sobre R e $g_i(x)$ o polinômio gerador de C_i, para $i = 1, 2$, com $\mathrm{mdc}(n, p) = 1$. Então, C é um código LCD se, e somente se, $g_i(x)$ for auto-recíproco para $i = 1, 2$.*

Demonstração. Pelo Teorema 4.26, temos que C é um código LCD de comprimento n sobre R se, e somente se, $g_i(x)$ é auto-recíproco e todos os fatores irredutíveis mônicos de $g_i(x)$ têm a mesma multiplicidade em $g_i(x)$ e em $x^n - 1$ para $i = 1, 2$. Como $\mathrm{mdc}(n, p) = 1$, então $g_i(x)$ e $\dfrac{x^n - 1}{g_i(x)}$ são primos entre si. Isso significa que, de qualquer forma, todos os fatores irredutíveis mônicos de $g_i(x)$ têm a mesma multiplicidade em $g_i(x)$ e em $x^n - 1$. □

Para os resultados a seguir vamos considerar ϕ_0 a função de Gray definida como na Observação 3.8. Além disso, vamos considerar a matriz M, que define ϕ_0, satisfazendo $MM^{\perp} = \lambda I_2$, onde $\lambda \in \mathbb{F}_q^*$ e I_2 é a matriz identidade 2×2.

Lema 4.29. *Seja C um código linear de comprimento n sobre R. Então, $\phi_0(C^{\perp}) = \phi_0(C)^{\perp}$.*

Demonstração. Se $w \in \phi_0(C)^{\perp}$, como ϕ_0 é um isomorfismo, existe $d \in R^n$ tal que $\phi_0(d) = w$. Como $R^n = (1-v)\mathbb{F}_q^n \oplus (1+v)\mathbb{F}_q^n$, existem únicos $d^{(1)}, d^{(2)} \in \mathbb{F}_q^n$ tais que $d = (1-v)d^{(1)} + (1+v)d^{(2)}$. Por definição, para todo $v \in \phi_0(C)$, temos $\langle v, w\rangle = 0$, e como ϕ_0 é um isomorfismo, então para todo $c \in C$, temos $\langle \phi_0(c), \phi_0(d)\rangle = 0$.

Provemos que $d \in C^{\perp}$. Em outras palavras, devemos provar que para todo $c \in C$, temos $\langle c, d\rangle = 0$. Seja então $c \in C$. Como $C = (1-v)C_1 \oplus (1+v)C_2$, existem $c^{(1)} \in C_1$ e $c^{(2)} \in C_2$, tais que $c = (1-v)c^{(1)} + (1+v)c^{(2)}$. Assim, $(1-v)c^{(1)} + (1+v)0 = (1-v)c^{(1)} \in C$ e $(1-v)0 + (1+v)c^{(2)} = (1+v)c^{(2)} \in C$. Como $\phi_0(d) \in \phi_0(C)^{\perp}$, então $\langle \phi_0((1-v)c^{(1)}), \phi_0(d)\rangle = 0$ e $\langle \phi_0((1+v)c^{(2)}), \phi_0(d)\rangle = 0$. Pelo Corolário 3.15, temos

$$\langle \phi_0((1-v)c^{(1)}, \phi_0(d)\rangle = \lambda(\langle c^{(1)}, d^{(1)}\rangle + \langle 0, d^{(2)}\rangle) = \lambda\langle c^{(1)}, d^{(1)}\rangle.$$

Ou seja, $\langle c^{(1)}, d^{(1)}\rangle = 0$. Da mesma forma $\langle \phi_0((1+v)c^{(2)} \cdot \phi_0(d)\rangle = \lambda\langle c^{(2)}, d^{(2)}\rangle$, o que implica $\langle c^{(2)}, d^{(2)}\rangle = 0$. Portanto,

$$\langle c, d\rangle = 2(1-v)\langle c^{(1)}, d^{(1)}\rangle + 2(1+v)\langle c^{(2)}, d^{(2)}\rangle = 0.$$

Em outras palavras, $d \in C^{\perp}$. Concluímos que $\phi_0(C)^{\perp} \subseteq \phi_0(C^{\perp})$.

Reciprocamente, seja $w \in \phi_0(C^{\perp})$, então existe $d \in C^{\perp}$ tal que $\phi_0(d) = w$. Para todo $c \in C$ temos $\langle c, d\rangle = 0$. Denotando $c^{(1)}, c^{(2)}, d^{(1)}, d^{(2)}$, como no caso anterior, temos

$$\langle c, d\rangle = 2(1-v)\langle c^{(1)}, d^{(1)}\rangle + 2(1+v)\langle c^{(2)}, d^{(2)}\rangle = 0.$$

Como $R = (1-v)\mathbb{F}_q \oplus (1+v)\mathbb{F}_q$, temos $\langle c^{(1)}, d^{(1)}\rangle = 0$ e $\langle c^{(2)}, d^{(2)}\rangle = 0$. Pelo Corolário 3.15, isso implica $\langle \phi_0(c), \phi_0(d)\rangle = 0$ e, portanto, $\phi_0(d) \in \phi_0(C)^{\perp}$. Em outras palavras, $\phi_0(C^{\perp}) \subseteq \phi_0(C)^{\perp}$. Isso prova o lema. □

Lema 4.30. *Seja C um código linear de comprimento n sobre R. Então,*

$$\phi_0(C \cap C^\perp) = \phi_0(C) \cap \phi_0(C)^\perp.$$

Demonstração. Como ϕ_0 é uma função, para quaisquer conjuntos A e B, temos $\phi_0(A \cap B) = \phi_0(A) \cap \phi_0(B)$. Daí, segue que $\phi_0(C \cap C^\perp) = \phi_0(C) \cap \phi_0(C^\perp)$. Conclui-se pelo Lema 4.29. □

Teorema 4.31. *Seja C um código linear de comprimento n sobre R. Então C é um código LCD se, e somente se $\phi_0(C)$, a imagem de Gray de C, é um código LCD de comprimento $2n$ sobre $\mathbb{F}_q$.*

Demonstração. Suponha que C seja um código LCD de comprimento n sobre R. Isso significa que $C \cap C^\perp = 0$. Pelo Lema 4.30, temos

$$\phi_0(C) \cap \phi_0(C)^\perp = \phi_0(C \cap C^\perp) = 0$$

Em outras palavras, $\phi_0(C)$ é um código LCD de comprimento $2n$ sobre $\mathbb{F}_q$.

Reciprocamente, suponha que $\phi_0(C)$ seja um código LCD de comprimento $2n$ sobre $\mathbb{F}_q$. Pelo Lema 4.30, temos

$$\phi_0(C \cap C^\perp) = \phi_0(C) \cap \phi_0(C)^\perp = 0.$$

Como ϕ_0 é um isomorfismo sobre $\mathbb{F}_q$, podemos concluir que $C \cap C^\perp = 0$. Portanto, C é um código LCD de comprimento n sobre R. □

4.4 Códigos Quânticos

Como nosso tema principal são os códigos LCD e suas propriedades, não faremos uma exploração profunda dos códigos quânticos. No entanto, a seguir compartilharemos dois resultados interessantes sobre a existência desse tipo de códigos. A definição de código quântico se encontra em [1, Definition 3.2], e se o leitor desejar ver as demonstrações e aprofundar-se no assunto, pode consultar [1] e [5].

Lema 4.32 (Construção CSS)**.** *[5, Theorem 3] Se C é um código linear $[n, k, d]$ com $t(C^\perp) \subseteq t(C)$ sobre $\mathbb{F}_q$, então existe um código corretor de erros quântico $[[n, 2k - n, d]]$ sobre $\mathbb{F}_q$.*

Teorema 4.33. *[1, Theorem 3.5] Seja $C = (1 - v)C_1 \oplus (1 + v)C_2$ um código cíclico de comprimento n sobre R e $\phi_0(C)$ tem os parâmetros $[2n, k, d_H]$. Se $t(C^\perp) \subseteq t(C)$, então existe um código quântico corretor de erros $[[2n, 2k - 2n, d_H]]$.*

4.5 Exemplos

A seguir, apresentaremos uma seleção de exemplos que exemplificam e respaldam a teoria exposta tanto na referência [1] como na [4]. Esses exemplos serão utilizados com o propósito de enriquecer e aplicar os conceitos teóricos discutidos nessas referências, proporcionando uma compreensão mais prática e tangível dos mesmos.

Ao explorar esses exemplos, buscamos estabelecer uma conexão mais concreta entre a teoria apresentada nas referências e sua aplicação em situações reais. Através desses exemplos, procuramos ilustrar como a teoria pode ser implementada e como seus princípios subjacentes podem influenciar diferentes cenários.

Exemplo 4.34. *Seja* $R = \mathbb{F}_5 + v\mathbb{F}_5, v^2 = 1$ *um anel finito e* $n = 66$. *Então*

$$\begin{aligned} x^{66} - 1 =& (x+1)(x+4)\left(x^2+x+1\right)\left(x^2+4x+1\right)\left(x^5+x^4+4x^3+4x^2+3x+1\right) \\ & \left(x^5+2x^4+4x^3+x^2+x+4\right)\left(x^5+3x^4+4x^3+4x^2+x+1\right)\left(x^5+4x^4\right. \\ & \left.+4x^3+x^2+3x+4\right)\left(x^{10}+x^9+2x^8+x^7+4x^6+x^5+3x^4+4x^3+3x+1\right) \\ & \left(x^{10}+2x^9+x^7+3x^6+4x^5+4x^4+4x^3+2x^2+4x+1\right)\left(x^{10}+3x^9+4x^7\right. \\ & \left.+3x^6+x^5+4x^4+x^3+2x^2+x+1\right)\left(x^{10}+4x^9+2x^8+4x^7+4x^6+4x^5\right. \\ & \left.+3x^4+x^3+2x+1\right) \in \mathbb{F}_5[x]. \end{aligned}$$

Seja

$$\begin{aligned} g_1 =& \left(x^5+x^4+4x^3+4x^2+3x+1\right)\left(x^{10}+x^9+2x^8+x^7+4x^6+x^5\right. \\ & \left.+3x^4+4x^3+3x+1\right), \\ g_2 =& \left(x^5+3x^4+4x^3+4x^2+x+1\right)\left(x^{10}+3x^9+4x^7+3x^6+x^5+4x^4\right. \\ & \left.+x^3+2x^2+x+1\right) \end{aligned}$$

Como $M = \begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}$ *satisfaz* $MM^{\perp} = 3I_2$, *onde* $M \in GL(\mathbb{F}_5)$ *e* I_2 *é a matriz identidade* 2×2, *então* $C = t^{-1}((1-v)g_1 + (1+v)g_2)$ *é um código cíclico de comprimento* 66 *sobre* R. *Além disso,* $\phi_0(C)$ *tem os parâmetros* $[132, 102, 4]$.

Dado que $x^{66} - 1 \equiv 0 \pmod{g_i(x)\tilde{g}_i(x)}$, *para* $i = 1$, *2, pelo Teorema 4.18, temos* $t(C^{\perp}) \subseteq t(C)$. *Portanto, pelo Teorema 4.33, existe um código quântico* $[[132, 72, 4]]$. *Este código quântico é superior ao código quântico conhecido* $[[132, 72, 2]]$.

Exemplo 4.35. *Seja* $R = \mathbb{F}_7 + v\mathbb{F}_7, v^2 = 1$ *um anel finito e* $n = 42$. *Então*

$$x^{42} - 1 = (x+1)^7(x+2)^7(x+3)^7(x+4)^7(x+5)^7(x+6)^7 \in \mathbb{F}_7[x].$$

Sejam $g_1 = (x+2)(x+3)^2$, $g_2 = (x+4)(x+5)^2$ *e* $M = \begin{bmatrix} 3 & 3 \\ 3 & 4 \end{bmatrix}$, *satisfazendo* $MM^{\perp} = 4I_2$, *onde* $M \in GL(\mathbb{F}_7)$ *e* I_2 *é a matriz identidade* 2×2.

Assim, $t(C) = ((1-v)g_1 + (1+v)g_2)$ *é um código cíclico de comprimento* 42 *sobre* R *e* $\phi(C)$ *possui os parâmetros* $[84, 78, 3]$.

Dado que $x^{42} - 1 \equiv 0 \pmod{g_i(x)\tilde{g}_i(x)}$, *para* $i = 1, 2$, *pelo Teorema 4.18, temos* $t(C^{\perp}) \subseteq t(C)$. *Portanto, pelo Teorema 4.33, existe um código quântico* $[[84, 72, 3]]$, *que possui a mesma distância mínima, mas uma taxa de código maior do que o código existente* $[[84, 60, 3]]$.

Exemplo 4.36. *Seja* $R = \mathbb{F}_{3^2} + v\mathbb{F}_{3^2}, v^2 = 1$ *um anel finito e* $n = 41$. *Então,*

$$\begin{aligned} x^{41} - 1 =& (x+2)\left(x^4+wx^3+w^5x^2+wx+1\right)\left(x^4+w^2x^3+w^3x^2+w^2x+1\right)\left(x^4+w^2x^3\right. \\ & \left.+w^6x^2+w^2x+1\right)\left(x^4+w^3x^3+w^7x^2+w^3x+1\right)\left(x^4+2x^3+wx^2+2x+1\right) \\ & \left(x^4+2x^3+w^3x^2+2x+1\right)\left(x^4+w^5x^3+w^5x+1\right)\left(x^4+w^6x^3+wx^2+w^6x+1\right) \\ & \left(x^4+w^6x^3+w^2x^2+w^6x+1\right)\left(x^4+w^7x^3+w^7x+1\right) \in \mathbb{F}_{3^2}[x], \end{aligned}$$

onde $w^2 + 2w + 2 = 0$.

Sejam $g_1 = x^4 + wx^3 + w^5x^2 + wx + 1$, $g_2 = x^4 + 2x^3 + w^3x^2 + 2x + 1$, $M = \begin{bmatrix} 2w & 1 \\ 1 & w \end{bmatrix}$, *satisfazendo* $MM^{\top} = (w+2)I_2$, $M \in GL(\mathbb{F}_9)$ *e* I_2 *é a matriz identidade* 2×2.

Observe que os polinômios $g_1(x)$ *e* $g_2(x)$ *são auto-recíprocos. Consequentemente, de acordo com o Teorema 4.31, o código* $C = t^{-1}((1-v)g_1 + (1+v)g_2)$ *é um código LCD de comprimento* 41 *sobre* R. *Portanto, a imagem de Gray* $\phi_0(C)$ *é um código LCD com os parâmetros* $[82, 74, 4]$. *Esse código é considerado quase ótimo de acordo com o banco de dados [4].*

A Tabela 4.1, que se encontra em [1], apresenta códigos corretores de erros quânticos sobre o corpo $\mathbb{F}_q$. Na primeira coluna, são indicados os comprimentos dos códigos cíclicos sobre R, enquanto a segunda e terceira colunas mostram os polinômios geradores correspondentes $g_i(x)$ para os códigos cíclicos $C_i, i = 1, 2$. Os parâmetros das imagens de Gray dos códigos cíclicos são listados na quarta coluna. Os códigos quânticos corretores de erros obtidos são apresentados na quinta coluna e comparados com os códigos de trabalhos anteriores na sexta coluna. Vale ressaltar que alguns dos códigos quânticos na quinta coluna são novos e são marcados como $[[n, k, d]]^*$.

Tabela 4.1: Nesta tabela, apresentamos um novo código quântico com seus respectivos parâmetros e destacamos as melhorias em comparação com o antigo QECC sobre um corpo finito de característica ímpar.

n	$g_1(x)$	$g_2(x)$	$\phi_0(C)$	$[[n,k,d]]$	$[[n',k',d']]$
30	$x+2$	$x+4$	$[60,58,2]$	$[[60,56,2]]_5$	$[[60,54,2]]_5[6]$
62	$\left(x^3+3x^2+x+1\right)$ $\left(x^3+x^2+x+4\right)$	$\left(x^3+x^2+3x+1\right)$ $\left(x^3+4x^2+4x+4\right)$	$[124,112,4]$	$[[124,100,4]]_5$	$[[124,100,3]]_5[17]$
75	$x+4$	x^2+x+1	$[150,147,2]$	$[[150,144,2]]_5$	$[[150,138,2]]_5[4]$
90	$x+1$	$x+4$	$[180,178,2]$	$[[180,172,2]]_5$	$[[180,168,2]]_5[4]$
48	$(x+2)(x+3)$ $\left(x^3+x+3\right)$	$(x+4)(x+5)$ $\left(x^3+5x+5\right)$	$[96,88,3]$	$[[96,80,3]]_7$	$[[96,74,3]]_7[6]$
84	$(x+2)$	$(x+4)$	$[168,166,2]$	$[[168,164,2]]_7$	$[[168,162,2]]_7[11]$
96	$(x+5)\left(x^4+x^2+1\right)$	$(x+3)\left(x^4+6x^2+6\right)$	$[192,182,3]$	$[[192,172,3]]_7$	$[[192,168,3]]_7[17]$
98	$(x+1)^8(x+6)$	$(x+1)(x+6)^8$	$[196,178,3]$	$[[196,160,3]]_7$	$[[196,132,3]]_7[17]$
18	$(x+3)$	$(x+9)$	$[36,34,2]$	$[[36,32,2]]_{13}$	$[[36,30,2]]_{13}[11]$
24	$(x+3)(x+8)$ $\left(x^2+4x+16\right)$	$(x+9)(x+15)$ $\left(x^2+13x+16\right)$	$[48,40,4]$	$[[48,32,4]]_{17}$	$[[48,30,4]]_{17}[11]$
38	$(x+1)^{10}(x+18)^6$	$(x+1)^6(x+18)^{10}$	$[76,44,11]$	$[[76,22,11]]^*_{19}$	...
55	$(x+4)^2\left(x^5+2x^4\right.$ $\left.+4x^3+x^2+x+4\right)$	$(x+4)^2\left(x^5+4x^4+\right.$ $\left.4x^3+x^2+3x+4\right)$	$[110,96,3]$	$[[110,82,3]]^*_{25}$	...
56	$\left(x+w^3\right)\left(x^3+w^5x^2\right.$ $\left.+w^{17}x+4\right)\left(x^3+\right.$ $\left.w^{14}x^2+w^7x+w^{15}\right)\left(x^3\right.$ $\left.+w^7x^2+w^5x+2\right)$	$\left(x+w^{21}\right)\left(x^3+wx^2\right.$ $\left.+w^{17}x+4\right)\left(x^3+\right.$ $\left.w^{16}x^2+w^{23}x+w^9\right)\left(x^3\right.$ $\left.+w^{23}x^2+wx+3\right)$	$[112,92,5]$	$[[112,72,5]]^*_{25}$	...
60	$(x+1)\left(x+w^{22}\right)^5$ $(x+4)\left(x+w^{14}\right)^4$ $(x+3)^2\left(x+w^{16}\right)$ $\left(x+w^{20}\right)^4$	$(x+1)\left(x+w^2\right)^5$ $(x+4)\left(x+w^{10}\right)^4$ $(x+2)^2\left(x+w^8\right)$ $\left(x+w^4\right)^4$	$[120,84,8]$	$[[120,48,8]]^*_{25}$	...
62	$\left(x^3+4x^2+3x+4\right)$ $\left(x^3+4x^2+3x+1\right)$ $\left(x^3+2x+1\right)$ $\left(x^3+4x^2+4\right)$ $\left(x^3+3x^2+4\right)$ $\left(x^3+x^2+4x+1\right)$	$\left(x^3+2x^2+x+4\right)$ $\left(x^3+3x^2+4x+1\right)$ $\left(x^3+2x^2+1\right)$ $\left(x^3+x+4\right)$ $\left(x^3+2x^2+4\right)$ $\left(x^3+4x^2+x+1\right)$	$[124,88,8]$	$[[124,52,8]]^*_{25}$	...

Da mesma forma, a Tabela 4.2, que também se encontra em [1], traz o comprimento dos códigos LCD sobre R na primeira coluna. As segunda e terceira colunas mostram os polinômios geradores correspondentes g_i para os códigos cíclicos $C_i, i = 1, 2$. Os parâmetros das imagens de Gray $\phi_0(C)$ dos códigos LCD sobre R são listados na quarta coluna, enquanto a quinta coluna indica se um código é ótimo ou quase ótimo. Além disso, alguns dos códigos listados na quinta coluna são novos códigos LCD e são denotados como $[n, k, d]^{\#}$.

Observa-se que chamamos um código linear $[n, k, d]$ de quase ótimo (ou próximo do ótimo) quando existe um código com parâmetros $[n, k, d']$ (conforme [4]) e a diferença $d' - d \leq 2$.

Tabela 4.2: Códigos LCD ótimos e quase ótimos sobre um corpo finito de característica ímpar de acordo com o banco de dados [4].

n	$g_1(x)$	$g_2(x)$	$\phi_0(C)$	
48	$x+1$	x^2+1	$[96, 93, 2]_5$	Ótimo
44	$x+1$	x^2+1	$[88, 85, 2]_7$	Ótimo
65	$x^{12}+4x^{10}+3x^9+x^8+x^7+4x^6$ $+x^5+x^4+3x^3+4x^2+1$	$x^{12}+2x^{11}+x^8+2x^6+x^4$ $+2x+1$	$[130, 106, 5]_7^{\#}$	...
20	$x+1$	x^2+wx+1	$[40, 37, 2]_9$	Quase ótimo
41	$x^4+wx^3+w^5x^2+wx+1$	$x^4+w^2x^3+w^3x^2+w^2x+1$	$[82, 74, 4]_9$	Quase ótimo
20	$(x+1)\left(x^2+8x$ $+1\right)\left(x^2+5x+1\right)$	$(x+1)\left(x^2+13x$ $+1\right)\left(x^2+15x+1\right)$	$[40, 30, 6]_{19}^{\#}$	...
25	$\left(x^2+5x+1\right)$ $\left(x^{10}+5x^5+1\right)$	$\left(x^2+15x+1\right)$ $\left(x^{10}+15x^5+1\right)$	$[50, 26, 4]_{19}^{\#}$	...
28	$(x+1)\left(x^6+11x^5+3x^4\right.$ $\left.+11x^3+3x^2+11x+1\right)$	$(x+1)\left(x^6+8x^5+3x^4\right.$ $\left.+8x^3+3x^2+8x+1\right)$	$[56, 42, 4]_{19}^{\#}$	...
34	$(x+1)\left(x^8+7x^7\right.$ $+9x^6+10x^5+15x^4+10x^3$ $\left.+9x^2+7x+1\right)$	$(x+1)\left(x^8+13x^7\right.$ $+15x^6+16x^5+8x^4+16x^3$ $\left.+15x^2+13x+1\right)$	$[68, 50, 4]$	...
35	$\left(x^2+5x+1\right)\left(x^6\right.$ $\left.+8x^5+17x^3+8x+1\right)$	$\left(x^2+15x+1\right)\left(x^6+2x^5\right.$ $\left.+6x^4+12x^3+6x^2+2x+1\right)$	$[70, 56, 5]_{19}^{\#}$	...
26	$(x+1)\left(x^2+wx\right.$ $\left.+1\right)\left(x^2+w^{22}x+1\right)$	$(x+1)\left(x^2+w^{10}x\right.$ $\left.+1\right)\left(x^2+w^{11}x+1\right)$	$[52, 42, 6]_{25}^{\#}$	...

Referências Bibliográficas

[1] M. Ashraf, N. Khan, and G. Mohammad. New quantum and lcd codes over the finite field of odd characteristic. *International Journal of Theoretical Physics*, pages 2322–2332,, 2021. https://doi.org/10.1007/s10773-021-04849-2.

[2] Y. Cengellenmis. On the cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$. *International Journal of Algebra*, pages 253–259, 2010.

[3] J.B Fraleigh and V.J Katz. *A First Course in Abstract Algebra*. Addison - Wesley, University of Oxford, 2003.

[4] M. Grassl. Bounds on the parameters of various types of codes. Disponível http://www.codetables.de//, 07/04/2020.

[5] M. Grassl and T. Beth. On optimal quantum codes. *International Journal of Quantum Information*, pages 55–64, 2004. https://doi.org/10.1142/S0219749904000079.

[6] F. Gursoy, I. Siap, and B. Yildiz. Construction of skew cyclic codes over $\mathbb{F}_q+v\mathbb{F}_q$. *Advances in Mathematics of Communications*, pages 313–322, 2014. https://doi.org/10.3934/amc.2014.8.313.

[7] A Hefez and M.L T Villela. *Códigos Corretores de Erros*. IMPA, Rio de Janeiro, 2017.

[8] I.N Hernstein. *Tópicos de Álgebra*. Editora da Univ. e Polígono, Uniserdidade de São Paulo, 1970.

[9] I.G Macdonald and M.F Atiyah. *Introduction to Commutative Algebra*. Addison - Wesley Publishing Company, University of Oxford, 1994.

[10] J.L. Massey. Linear codes with complementary duals. *Discrete Mathematics 106/107*, pages 337–342, 1992. https://doi.org/10.1016/0012-365X(92)90563-U.

[11] J. Qian. Quantum codes from cyclic codes over $\mathbb{F}_2+v\mathbb{F}_2$. *Journal of Information and Computational Science*, pages 1715–1722, 2013. https://doi.org/10.12733/jics20101705.

[12] X. Yang and J.L. Massey. The condition for a cyclic code to have a complementary dual. *Discrete Mathematics*, pages 391–393, 1994. https://doi.org/10.1016/0012-365X(94)90283-6.

[13] S. Zhu, Y. Wang, and M. Shi. Some results on cyclic codes over$\mathbb{F}_2 + v\mathbb{F}_2$. *IEEE Trans. Inf. Theory*, pages 2120–2128, 2010. https://doi.org/10.1109/TIT.2010.2040896.