UNIVERSIDADE ESTADUAL DE MARINGÁ - UEM
CENTRO DE CIÊNCIAS EXATAS - CCE
DEPARTAMENTO DE MATEMÁTICA - DMA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA - PMA

FREDERICO VENTURA BATISTA

Códigos Binários Quase-Cíclicos e Códigos Estabilizadores obtidos via Plano Euclidiano Finito PEF $\mathbb{F}_{2^r}^2$

Tese apresentada ao Programa de Pós Graduação em Matemática do Departamento de Matemática do Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte das exigências para a obtenção do título de Doutor em Matemática. Área: Matemática Aplicada.

Maringá - PR
2023

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

FREDERICO VENTURA BATISTA

Códigos Binários Quase-Cíclicos e Códigos Estabilizadores obtidos via Plano Euclidiano Finito PEF $\mathbb{F}_{2^r}^2$

Tese apresentada ao Programa de Pós Graduação em Matemática do Departamento de Matemática do Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte das exigências para a obtenção do título de Doutor em Matemática.

Área de Concentração:
Matemática Aplicada.

Orientador:
Eduardo Brandani da Silva.

Versão original
Disponível na biblioteca da UEM

Maringá - PR
2023

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Setorial BSE-DMA-UEM, Maringá, PR, Brasil)

Batista, Frederico Ventura
B333c Códigos binários quase-cíclicos e códigos estabilizadores obtidos via Plano Euclidiano Finito PEF / Frederico Ventura Batista. -- Maringá, 2023.
92 f. : il.

Orientador: Profº. Drº. Eduardo Brandani da Silva.
Tese (doutorado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática - Área de Concentração: Matemática Aplicada, 2023.

1. Plano Euclidiano Finito. 2. Códigos quase-cíclicos. 3. Códigos estabilizadores. 4. Finite Euclidean Plan. 5. Quasi-cyclic codes. 6. Stabilizer codes. I. Silva, Eduardo Brandani da, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemática - Área de Concentração: Matemática Aplicada. III. Título.

CDD 22.ed. 003.54
Edilson Damasio CRB9-1.123

FREDERICO VENTURA BATISTA

CÓDIGOS BINÁRIOS QUASE-CÍCLICOS E CÓDIGOS ESTABILIZADORES OBTIDOS VIA PLANO EUCLIDIANO FINITO PEF F^2_2^R

Tese apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Doutor em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Prof. Dr. Eduardo Brandani da Silva - UEM (Presidente)
Prof. Dr. Giuliano Gadioli La Guardia - UEPG
Prof. Dr. Edson Donizete de Carvalho - UNESP/Ilha Solteira
Prof. Dr. Marcelo Escudeiro Hernandes - UEM
Prof. Dr. Francisco Nogueira Calmon Sobral - UEM

Aprovado em: 07 de julho de 2023.
Local de defesa: Videoconferência – Google Meet (https://meet.google.com/sty-owsd-xxj)

À Imaculada, minha mãe;
À Gláucia, minha esposa;
E aos meus filhos Lívia e Felipe,
sem os quais eu nada sou.

AGRADECIMENTOS

Agradeço primeiramente a Deus, em todas as suas formas, por guiar meus passos nesta jornada acadêmica e pessoal.

À minha mãe, Maria Imaculada Ventura, por ser a melhor mãe que um filho pode ter. Seu amor incondicional e apoio constante foram meu alicerce.

À minha esposa, Gláucia, por estar sempre ao meu lado, sendo a melhor companheira que um marido pode ter. Sua paciência, carinho e apoio foram essenciais para superar os desafios.

Aos meus filhos, Lívia e Felipe, este trabalho é dedicado a vocês. Cada esforço foi pensado para construir um futuro melhor para vocês.

Agradeço imensamente ao meu orientador, Prof. Dr. Eduardo Brandani da Silva, por acreditar em mim desde o início, pelo seu apoio intelectual e orientação valiosa ao longo deste percurso. Tal agradecimento se estende à todo o Programa de Pós-Graduação em Matemática da UEM.

Também sou grato aos meus amigos que estiveram presentes, seja de perto ou de longe: Robledo, Lindemberg, Vinícius e Marcos. Os amigos de toda uma vida: "Terceirão". Aos amigos da "Fubazada", por compartilharmos momentos inesquecíveis.

Um agradecimento especial vai para minha cadelinha Pitanga, que com sua alegria contagiante trouxe luz aos meus dias de estudo e concentração.

À instituição que represento, Instituto Federal Norte de Minas Gerais (IFNMG), pelo Programa de Bolsas para Qualificação de Servidores do IFNMG (PBQS), fornecendo o apoio financeiro e institucional que possibilitou essa jornada de aprimoramento."

“A paciência é uma virtude na ciência e na vida”
(Autor desconhecido).

RESUMO

BATISTA, F. V. **Códigos Binários Quase-Cíclicos e Códigos Estabilizadores obtidos via Plano Euclidiano Finito PEF** $\mathbb{F}_{2^r}^2$. 2023. 106 f. Tese (Doutorado - Programa de Programa de Pós Graduação em Matemática em Matemática Aplicada) - Centro de Ciências Exatas, Universidade Estadual de Maringá, Maringá - PR, 2023.

Neste trabalho foi desenvolvido o conceito de Plano Euclidiano Finito (PEF). As propriedades relacionadas ao PEF foram aplicadas à teoria de códigos lineares permitindo a obtenção de uma família de códigos quase-cíclicos binários auto-ortogonais em relação ao produto interno Euclidiano e ao produto interno simplético. Foi mostrado que com essa família de códigos é possível obter códigos estabilizadores por meio da determinação de seu grupo estabilizador.

Palavras-chave: 1. Plano Euclidiano Finito. 2. Códigos Quase-Cíclicos. 3. Códigos Estabilizadores.

ABSTRACT

BATISTA, F. V. **Binary Quasi-Cyclic Codes and Stabilizer Codes Obtained via Finite Euclidean Plane PEF** $\mathbb{F}_{2^r}^2$. 2023. 106 f. Thesis (Ph.D. - Postgraduate program in Applied mathematics) - Exact Sciences Center, State University of Maringá, Maringá - PR, 2023.

In this work, the concept of Finite Euclidean Plane (PEF) was developed. Properties related to PEF were applied to the theory of linear codes, allowing the derivation of a family of almost-cyclic binary self-orthogonal codes with respect to both Euclidean inner product and symplectic inner product. It was shown that with this family of codes, it is possible to obtain stabilizer codes by determining their stabilizer group.

Key-words: 1. Finite Euclidean Plan. 2. Quasi-Cyclic Codes . 3. Stabilizer Codes.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\mathbb{F}_q$: corpo finito contendo $q = p^m$ elementos em que p é um número primo e $m \in \mathbb{N}^*$

$\prec$: relação de ordem definida em $\mathbb{F}_{2^r}$

$\alpha^{-\infty}$: notação utilizada para representar o elemento neutro do corpo $\mathbb{F}_{2^r}$, em que os elementos não nulos são descritos por meio da potência de α

$\mathcal{I}_r$: conjunto de símbolos dado por $\{*, 0, 1, \ldots, 2^r - 1\}$, sendo r inteiro e positivo

z_{ij}: representa o par ordenado $(\alpha^i, \alpha^j) \in \mathbb{F}_{2^r}^2$, com $i, j \in \mathcal{I}_r$

$d_{\mathbb{F}_{2^r}^2}$: relação definida em $\mathbb{F}_{2^r}^2$ por $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}) = \left(\alpha^i + \alpha^j + \alpha^s + \alpha^t\right)^2$, em que $z_{ij} = (\alpha^i, \alpha^j)$ e $z_{st} = (\alpha^s, \alpha^t)$

PEF$\mathbb{F}_{2^r}^2$: espaço vetorial $\mathbb{F}_{2^r}^2$ munido com a relação $d_{\mathbb{F}_{2^r}^2}$

$||\cdot||_{\mathbb{F}_{2^r}}$: relação definida em PEF$\mathbb{F}_{2^r}^2$ dada por $||z_{ij}||_{\mathbb{F}_{2^r}} = d_{\mathbb{F}_{2^r}^2}(z_{ij}, 0)$

$\mathcal{Z}_i$: lista de elementos de $\mathbb{F}_{2^r}^2$ dada por $(z_{i*}, z_{i0}, z_{i1}, \ldots z_{i(2^r-2)})$, sendo $i \in \mathcal{I}_r$

Υ_r: matriz dada por $\Upsilon_r = \begin{bmatrix} \mathcal{Z}_* & \mathcal{Z}_0 & \mathcal{Z}_1 & \mathcal{Z}_2 & \cdots & \mathcal{Z}_{2^r-2} \\ \mathcal{Z}_{2^r-2} & \mathcal{Z}_* & \mathcal{Z}_0 & \mathcal{Z}_1 & \cdots & \mathcal{Z}_{2^r-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathcal{Z}_0 & \mathcal{Z}_1 & \mathcal{Z}_2 & \mathcal{Z}_3 & \cdots & \mathcal{Z}_* \end{bmatrix}$

$N(uv)$: matriz binária definida a partir de Υ_r atribuindo 1 nas posições correspondentes ao elemento z_{ij}, quando $||z_{ij}||_{\mathbb{F}_{2^r}} = \alpha^u$ ou quando $||z_{ij}||_{\mathbb{F}_{2^r}} = \alpha^v$ e 0 caso contrário, sendo $u, v \in \mathcal{I}_r$

$\mathcal{C}(uv)$: código linear gerado pela matriz $N(uv)$

$\mathcal{P}_n$: grupo de Pauli que age sobre n qubits

$N(uv : \zeta\eta)$: matriz binária de ordem $2^{r+1} \times 2^{2r}$ cujas primeiras 2^r linhas são dadas pelas linhas de $N(uv)$ e as demais linhas são referentes a matriz $N(\zeta\eta)$

$\mathcal{C}_{\mathcal{S}}(uv)$: código estabilizador associado ao grupo estabilizador $\mathcal{S}$ gerado pela matriz norma $N(uv)$

$\mathcal{C}_{\mathcal{S}(uv:\zeta\eta)}$: código estabilizador associado ao grupo estabilizador $\mathcal{S}(uv : \zeta\eta)$

SUMÁRIO

CAPÍTULO 1

INTRODUÇÃO

Neste texto será apresentado um estudo que teve como objetivo desenvolver um conceito algébrico e analisar suas implicações no âmbito da teoria dos códigos corretores de erros clássicos e quânticos.

A teoria dos códigos corretores de erros é um ramo interdisciplinar que combina matemática e engenharia, com aplicações nas mais variadas formas modernas relacionadas à teoria da informação e comunicação. Tal teoria tem sido amplamente estudada desde a publicação do artigo *"A mathematical theory of communication"*, por Claude Shannon em 1948 [60], que pode ser considerado como a primeira apresentação formal dos conceitos da mesma.

O principal aspecto da teoria dos códigos corretores de erros é lidar com a transmissão e armazenamento confiáveis de dados. Com a crescente quantidade de informações transmitidas e armazenadas diariamente, garantir a confiabilidade dos dados é uma preocupação cada vez maior. Nesse contexto, os códigos corretores de erros surgem como uma ferramenta para assegurar que os dados de informação possam ser transmitidos com uma excelente margem de segurança [42].

Um código corretor de erros tem por finalidade detetar e corrigir os erros que ocorrem durante a transmissão de dados. Esses erros podem ser causados por várias razões, como interferência na linha de transmissão, interferência eletromagnética, problemas de hardware ou software, entre outros. Com o auxílio dos códigos corretores de erros, é possível que os dados sejam recuperados mesmo quando houver erros na transmissão.

Sendo assim, a aplicação dos códigos corretores de erros é ampla, abrangendo áreas como a comunicação de dados, processamento digital de sinais e armazenamento de dados em dispositivos de memória [18]. Essa teoria é fundamental para garantir a segurança e integridade dos dados em sistemas críticos, como em sistemas médicos e de aviação, em que erros podem ter consequências graves.

A teoria dos Códigos Corretores de Erros também teve grandes avanços na área quântica. O surgimento dos códigos quânticos se deu na década de 90, quando a criptografia quântica foi estabelecida como um campo de pesquisa [24]. Nessa época, foi descoberto que a informação quântica é muito sensível às perturbações do meio ambiente, tornando a transmissão e o armazenamento de informação quântica uma tarefa

extremamente delicada [57]. Para corrigir os erros que afetam a informação quântica, foram desenvolvidos os Códigos Quânticos Corretores de Erros (CQCE), que utilizam conceitos da mecânica quântica para detectar e corrigir erros [51].

Os CQCE são fundamentais para o desenvolvimento de tecnologias quânticas, como a computação quântica e a criptografia quântica [25]. Eles são usados para proteger a informação quântica durante sua transmissão e armazenamento, garantindo a segurança e integridade dos dados [51]. Existem vários tipos de CQCE, como os códigos de Shor [62] e os códigos de Steane [66]. Todos eles utilizam a mecânica quântica para detectar e corrigir erros, tornando a informação quântica muito mais robusta e confiável.

Atualmente, os CQCE são uma área de pesquisa muito ativa, com muitos avanços recentes, como a descoberta dos códigos auto-corrigíveis [68] e o desenvolvimento de novas técnicas para detectar e corrigir erros quânticos de forma eficiente [19]. Além disso, os CQCE estão sendo aplicados em vários campos, como na comunicação quântica, na computação quântica e na simulação de sistemas quânticos [15]. A pesquisa nessa área é fundamental para o desenvolvimento de tecnologias quânticas cada vez mais avançadas e seguras.

Baseando-se nos fatos mencionados como motivação, o presente trabalho propõe-se a desenvolver uma nova abordagem na construção de códigos corretores de erros. Tal abordagem ocorre por meio da pesquisa relacionada às propriedades algébricas presentes em um conceito denominado como *Plano Euclidiano Finito* (PEF). A inspiração para utilizar o PEF como base para a realização deste estudo surgiu mediante pesquisas realizadas por Audrey Terras e Archie Medrano. Tais autores em trabalhos como [52] e [69] utilizam uma ideia recorrente na área da computação que consiste em modelar uma situação de caráter contínuo substituindo o corpo $\mathbb{R}$ por uma aproximação finita utilizando algum corpo finito $\mathbb{F}_q$, em que q é uma potência de um primo. Por meio de tal prática os autores mencionados obtiveram um objeto matemático similar ao espaço Euclidiano n-dimensional $\mathbb{R}^n$. Tal objeto foi nominado como *espaço Euclidiano finito n-dimensional*, definido sobre o corpo $\mathbb{F}_q$, denotado por $\mathbb{F}_q^n$. Nesse contexto, o PEF é visto como um espaço Euclidiano finito bidimensional, e que, para o presente trabalho, o corpo finito sobre o qual o PEF será definido possui característica 2.

Neste sentido, o conceito de PEF se mostra como um dos aspectos chave do presente trabalho. Tal afirmação será justificada ao longo do texto por meio da obtenção de uma família de códigos lineares que apresentam propriedades algébricas interessantes na teoria de Códigos Corretores de Erros, que foram determinadas através das propriedades relacionadas ao PEF. E são exatamente tais propriedades apresentadas pelos códigos pertencentes a tal família que permitem estabelecer a relação com os CQCE.

Assim, para a compreensão do trabalho realizado, o presente texto foi organizado da seguinte forma:

O Capitulo 2 apresenta conceitos da teoria de corpos finitos que são apresentados com o objetivo de dar o embasamento teórico para o desenvolvimento do conceito de PEF.

O Capítulo 3 também possui um caráter preliminar, no sentido de apresentar os conceitos básicos relacionados à teoria dos Códigos Corretores de Erros, em especial os códigos lineares.

No Capítulo 4 é introduzido o conceito de PEF, utilizando a notação PEF $\mathbb{F}_{2^r}^2$. São

demonstradas algumas propriedades relacionados ao PEF $\mathbb{F}_{2^r}^2$ e, em seguida, é introduzida a primeira contribuição da presente pesquisa ao se mostrar como tais propriedades são utilizadas para obter uma classe de QC-códigos binários com índice 2^r, em que $r \in \mathbb{N}^*$. O método empregado na construção de tais códigos tem como base o trabalho desenvolvido por Da Silva, Carneiro e Castelani apresentado em [12].

O Capítulo 5 apresenta os conteúdos referentes à teoria da Informação e Computação Quântica que foram utilizados para o desenvolvimento do trabalho que foi dedicado à elaboração de QECC.

O Capítulo 6 apresenta a segunda contribuição da pesquisa ao se mostrar como a teoria desenvolvida no Capítulo 4 pode ser usada na obtenção de QECC, em especial os QECC que pertencem à classe dos *códigos estabilizadores*.

Por fim, o Capítulo 7 apresenta um sumário dos resultados obtidos e previsões de trabalhos futuros.

CAPÍTULO 2

CORPOS FINITOS

Neste capítulo serão tratados alguns conceitos e resultados referentes à teoria de corpos finitos. Ao fazer isto, pretende-se verificar como é possível obter uma representação de um corpo finito de forma que seus elementos não nulos sejam obtidos como potências de um único elemento, pertencente ao corpo em questão, que possua determinadas propriedades, ou seja, serão utilizados os elementos primitivos para realizar tal representação. Nesse sentido, nesta parte do texto, a prioridade será explorar aspectos associados à extensão de corpos. Ressalta-se que não há a pretensão de realizar uma discussão detalhada acerca da teoria que envolve os corpos finitos, de modo que este capítulo tem um caráter de fornecer ao leitor parte dos pré-requisitos necessários para o bom entendimento das ferramentas algébricas necessárias para o desenvolvimento do trabalho. Neste sentido, para este capítulo, assim como para todo texto, é necessário que o leitor tenha um conhecimento prévio de alguns tópicos de Álgebra, como Teoria de Grupos por exemplo. Sendo assim, para maiores detalhes sobre os assuntos elencados previamente, indicamos as referências [22, 34, 44].

2.1 Conceitos Básicos

Esta seção começa com as definições de anel, corpo e alguns resultados cujas demonstrações podem ser verificadas, por exemplo, em [22].

Definição 2.1. *Um **anel** $(R, +, \cdot)$ é um conjunto não vazio R munido com duas operações denominadas soma e multiplicação denotadas, respectivamente, por $+$ e $\cdot$, de forma que :*

1. *$(R, +)$ é um grupo abeliano;*
2. *A operação de multiplicação é associativa;*
3. *A distributividade da multiplicação em relação a soma à esquerda e à direita são válidas. Isto é, para quaisquer $x, y, z \in R$ tem-se:*

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad (y + z) \cdot x = y \cdot x + z \cdot x. \tag{2.1}$$

Pode-se referir a um anel $(R, +, \cdot)$ por meio de uma notação abreviada que omite as operações de soma e multiplicação. Tal notação é dada por R e, portanto, está notação será usada no caso em que as operações estão subentendidas. Também é comum usar a notação xy para indicar a multiplicação entre os elementos $x, y \in R$. Tais recursos serão utilizados ao longo do texto. Também é importante mencionar que para as próximas definições, a não ser que seja mencionado o contrário, as notações 0 (zero ou *elemento nulo*) e 1 (um ou *identidade multiplicativa*) serão utilizadas como as notações dos elementos neutros das operações de soma e multiplicação, respectivamente.

Definição 2.2. *Seja R um anel. Com isso, considere as seguintes classificações:*

1. *R é um **anel com identidade**, se o anel possui identidade multiplicativa.*
2. *R é um **anel comutativo**, se a multiplicação for comutativa.*
3. *R é um **domínio de integridade**, se é comutativo, com unidade e se a identidade $x \cdot y = 0$ implica $x = 0$ ou $y = 0$, para quaisquer $x, y, z \in R$;*
4. *R é um **anel de divisão** se os elementos não nulos de R formam um grupo em relação a operação " $\cdot$ ";*
5. *R é um **corpo** se é um anel de divisão comutativo;*
6. *Dizemos que R é um **corpo finito**, quando R possui apenas uma quantidade finita de elementos.*

Pode-se verificar que todo corpo R é um domínio de integridade e também que os elementos 0 e 1 são únicos. A partir de agora, será adotada a notação no estilo "F" para representar um corpo qualquer. A notação no estilo "$\mathbb{F}_q$", com q potencia de algum número primo, indicará um corpo finito com q elementos. Além disso, a notação $\mathbb{N}^\star$ representará o conjunto dos números naturais não nulos, ou seja, $\mathbb{N}^\star = \mathbb{N} \setminus \{0\}$.

Definição 2.3. *A **ordem de um corpo** $\mathbb{F}_q$, denotada por $|\mathbb{F}_q|$, é igual ao número de elementos de $\mathbb{F}_q$. E a **ordem de um elemento** $\alpha \in \mathbb{F}_q^*$, denotada por $ord(\alpha)$, é igual ao número dado por:*

$$ord(\alpha) = \min\{n \in \mathbb{N}^* : \alpha^n = 1\}. \tag{2.2}$$

Definição 2.4. *A **característica** de um corpo F, denotada por $char\,(\mathrm{F})$, é dada pelo menor número $m \in \mathbb{N}$, para o qual temos :*

$$m \cdot x = \underbrace{x + x + \cdots + x}_{m \text{ vezes}} = 0. \tag{2.3}$$

para qualquer $x \in \mathrm{F}$. E, caso não exista tal número natural diremos que F é um corpo de característica zero, ou seja, $char\,(\mathrm{F}) = 0$.

Exemplo 2.5. *Como exemplos básicos de corpos tem-se os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ dos números racionais, reais e complexos, respectivamente, com as operações de soma e produto usuais. Taís corpos possuem infinitos elementos e têm característica 0.*

Algumas definições e resultados que serão apresentados adiante também se verificam na teoria de anéis. No entanto, no presente texto, tais conceitos serão considerados apenas relacionados à corpos finitos, uma vez que esse é o foco do capítulo. A seguir tem-se um teorema que relaciona a característica com a ordem de um corpo finito.

Teorema 2.6. *Dado um corpo $\mathbb{F}_q$, tem-se que $|\mathbb{F}_q| = p^n$ (ou seja, $q = p^n$) e $char(\mathbb{F}_q) = p$, em que, p é um número primo e $n \in \mathbb{N}$.*

O próximo resultado mostra que existem relações entre as operações envolvendo os elementos de um corpo finito e a característica do mesmo.

Teorema 2.7. *Seja $q = p^n$, p primo e considere o corpo $\mathbb{F}_q$. Então tem-se que:*

1. $(x \pm y)^{p^k} = x^{p^k} \pm y^{p^k}$, *para quaisquer* $x, y \in \mathbb{F}_q$ *e* $k \in \mathbb{N}^\star$;
2. *A equação* $x^{p^k} + y^{p^k} = 1$ *possui exatamente* p^n *soluções de pares ordenados* (x, y) *com* $x, y \in \mathbb{F}_{p^n}$ *para qualquer inteiro* $k \in \mathbb{N}^\star$.

A demonstração do item 2 do teorema 2.7 pode encontrada em [1]. Outra noção importante relacionada ao conceito de anéis é a definição de ideal.

Definição 2.8. *Seja R um anel comutativo com unidade. Um subconjunto não vazio $I \subset R$ é denominado um **ideal** de R quando é fechado para a soma e para o produto por qualquer elemento de R, mais especificamente, se $\alpha + \beta \in I$ e $\alpha \cdot r \in I$ para todos $\alpha, \beta \in I$ e $r \in R$.*

Exemplo 2.9. *Dado $\alpha \in R$, o conjunto dos múltiplos de α, isto é, $\{\alpha \cdot r : r \in R\}$ é um ideal, denominado de **ideal gerado por** α e denotado por $\langle\alpha\rangle$. Esse gerador α pode não ser o único gerador para $\langle\alpha\rangle$.*

Definição 2.10. *Um ideal $I \in R$ diz-se um **ideal principal** se $I = \langle\alpha\rangle$ para algum $\alpha \in R$. Se todos os ideais são principais, diz-se que R é um **anel de ideais principais**.*

2.1.1 Relação de Congruência e Anéis $\mathbb{Z}_n$

Uma das conexões importantes entre a teoria de anéis e a dos corpos finitos é feita por meio dos anéis $\mathbb{Z}_n$. Os conceitos básicos sobre tais tipos de anéis serão introduzidos nesta seção.

Definição 2.11. *Fixe $n \in \mathbb{N}^\star$. Dados $a, b \in \mathbb{Z}$, diz-se que a é **congruente a** b **módulo** n, e usa-se a notação $a \equiv b \mod n$, quando a diferença $a - b$ é divisível por n. Isto é*

$$a \equiv b \mod n \Leftrightarrow n|(a - b). \tag{2.4}$$

Na Definição 2.11, a relação definida em (2.4) é de equivalência em $\mathbb{Z}$, de modo que as classes de equivalência segundo tal relação são denominadas *classes de congruência*. Os inteiros a e b pertencem à mesma classe de equivalência se, e somente

se, possuem o mesmo resto na divisão por n. Sendo assim, se $\overline{a}$ denota a classe de equivalência de $a \in \mathbb{Z}$ em relação a congruência módulo n, o número de classes de equivalência distintas dessa relação é igual a n. E se $\mathbb{Z}_n$ é a notação usada para representar o conjunto dessas classes, tem-se:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}. \tag{2.5}$$

Sabemos que $\mathbb{Z}_n$ é um anel comutativo em relação às operações de soma e multiplicação dadas, respectivamente, por $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, para quaisquer $a, b \in \mathbb{Z}$. Associado à relação de congruência módulo n, segue o conceito de *ordem módulo* n.

Definição 2.12. *Fixado $n \in \mathbb{N}^\star$ define-se a **ordem de um inteiro** m **módulo** n, denotada por $ord_n(m)$, como a menor potência $r \in \mathbb{N}^\star$ tal que $m^r \equiv 1 \mod n$.*

Ainda em relação aos anéis $\mathbb{Z}_n$ tem-se o próximo resultado que possui grande relevância dentro da teoria de corpos finitos.

Teorema 2.13. *Para qualquer número primo p, o anel $\mathbb{Z}_p$ é um corpo. Além disso, a menos de isomorfismo existe apenas um corpo finito com p elementos que é dado por $\mathbb{Z}_p (\approx \mathbb{F}_p)$.*

Ou seja, de acordo com o Teorema 2.13 um corpo cuja ordem é dada por um número primo p é identificado com o corpo $\mathbb{Z}_p$. Nesse sentido, a não ser que seja mencionado o contrário, será acordado que ao longo do texto a notação dada por:

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}, \tag{2.6}$$

será utilizada para representar um corpo finito com p elementos, desde que p seja um número primo. Perceba que o Teorema 2.13 não abrange corpos finitos de qualquer ordem, uma vez que o Teorema 2.6 indica a existência de corpos cuja ordem seja dada por meio de alguma potência de número primo. Sobre isso, é natural questionar se para qualquer número primo p e qualquer natural n existe um corpo cuja ordem seja igual a p^n. A resposta para essa pergunta é sim, e tal fato será discutido nas próximas seções.

2.2 Anel de Polinômios

Nesta seção será introduzido o conceito de *polinômio* definido sobre um corpo. Os polinômios são fundamentais para mostrar que dado qualquer número primo p e qualquer $n \in \mathbb{N}^\star$ existe um corpo $\mathbb{F}_{p^n}$. Além disso, por meio dos polinômios pode-se obter uma forma de representar um corpo finito que é conveniente para o nosso trabalho.

Definição 2.14. *Um **polinômio** $f(x)$ **de grau** n definido sobre o corpo F é uma expressão da forma:*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n, \tag{2.7}$$

em que $n \in \mathbb{N}$, e para cada $i = 0, \ldots, n$ os ***coeficientes*** *$a_i \in \mathrm{F}$, com $a_n \neq 0$. O* ***grau do polinômio*** *$f(x)$ é denotado por $\partial(f)$ e corresponde ao expoente de a_n. Um polinômio de grau n é* ***mônico*** *se $a_n = 1$. O conjunto de todos os polinômios definidos sobre F é denotado por $\mathrm{F}[x]$.*

Um fato importante é que, por convenção, omite-se na expressão do polinômio o termo $a_i x^i$, toda vez que $a_i = 0$. Dois polinômios $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{m} b_i x^i$ de $\mathrm{F}[x]$ são iguais quando $a_i = b_i$ para qualquer $i \in \mathbb{N}$. Evidentemente, tal fato implica $\partial(f) = \partial(g)$. Pode-se definir operações de soma e multiplicação em $\mathrm{F}[x]$. Além disso, caso não seja feita alguma ressalva, todas as vezes que for utilizada a notação $\mathrm{F}[x]$ deve-se entender que F é um corpo.

Definição 2.15. *Sejam $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{m} b_i x^i$ polinômios de $\mathrm{F}[x]$. Sendo assim a* ***soma dos polinômios*** *$f(x)$ e $g(x)$ é o polinômio denotado por $(f+g)(x)$ definido da seguinte forma:*

$$(f+g)(x) = f(x) + g(x) = \sum_{i=0}^{k} c_i x^k, \tag{2.8}$$

de modo que $c_i = a_i + b_i$ para todo $i \in \mathbb{N}$. E a ***multiplicação entre os polinômios*** *é o polinômio denotado por $(f \cdot g)(x)$ e definido da seguinte forma:*

$$(f \cdot g)(x) = f(x) \cdot g(x) = \sum_{i=0}^{k} c_i x^k, \tag{2.9}$$

de modo que $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ para todo $i \in \mathbb{N}$.

Considere $f(x), g(x) \in \mathrm{F}[x]$. Pela da Definição 2.15 observa-se que segue das operações de soma e multiplicação as seguintes relações envolvendo o grau dos polinômios:

$$\partial(f+g) \leq \max\{\partial(f), \partial(g)\}; \tag{2.10}$$

$$\partial(f \cdot g) = \partial(f) + \partial(g). \tag{2.11}$$

Assim, considerando as operações que foram definidas no conjunto $\mathrm{F}[x]$, segue o próximo teorema.

Teorema 2.16. *O conjunto dos polinômios $\mathrm{F}[x]$ munido com as operações de soma e multiplicação dadas na Definição 2.15 possui uma estrutura de anel. Este anel é denominado* ***anel de polinômios*** *sobre F.*

O próximo resultado caracteriza todos os ideais do anel $\mathrm{F}[x]$.

Teorema 2.17. *Todo ideal em* $\mathrm{F}[x]$ *é da forma* $\langle p(x)\rangle$*, com* $p(x) \in \mathrm{F}[x]$.

Sendo assim, pela Definição 2.10, segue-se $\mathrm{F}[x]$ é um anel de ideias principais. Neste ponto do texto será introduzida a definição de polinômio irredutível.

Definição 2.18. *Seja* $f(x) \in \mathrm{F}[x]$ *tal que* $\partial(f) \geq 1$*. Diz-se que* $f(x)$ *é* ***irredutível*** *sobre* F *se todas as vezes a equação* $f(x) = g(x) \cdot h(x)$*, com* $g(x), h(x) \in \mathrm{F}[x]$*, implicar que* $g(x)$ *ou* $h(x)$ *são polinômios constantes, ou seja* $g(x) = a$ *ou* $h(x) = b$ *sendo* $a, b \in \mathrm{F}$*. Quando* $f(x)$ *não é irredutível sobre* F *diz-se que* $f(x)$ *é* ***redutível*** *sobre* F*.*

Exemplo 2.19. *Considere em* $\mathbb{F}_2[x]$ *os polinômios* $f(x) = x^2+x+1$ *e* $g(x) = x^4+x^2+1$*. O polinômio* $f(x)$ *é irredutível. De fato, suponha que existam polinômios* $h_1(x) = ax+b$ *e* $h_2(x) = cx + d$ *em* $\mathbb{F}_2[x]$*, de modo que que* $f(x) = h_1(x) \cdot h_2(x)$*. Dessa forma, em função dos conceitos de igualdade e de multiplicação entre polinômios temos que* $x^2 + x + 1 = acx^2 + (ad + bc)x + bd$ *implicaria em* $ac = 1, ad + bc = 1$ *e* $bd = 1$*. Porém, como* $\mathbb{F}_2 = \{0, 1\}$ *segue que* $ac = 1, bd = 1$ *implica* $a = b = c = d = 1$*. Isso contradiz o fato de se ter* $ad + bc = 1$ *uma vez que a* $char(\mathbb{F}_2) = 2$*. Já o polinômio* $g(x)$ *é redutível pois* $g(x) = f(x) \cdot f(x) = f^2(x)$*.*

Definição 2.20. *Se* $f(x) = \sum_{i=0}^{n} a_i x^i$ *é um polinômio não nulo de* $\mathrm{F}[x]$ *e* $\alpha \in \mathrm{F}$ *é tal que*

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0 \in \mathrm{F},$$

diz-se que α *é uma* ***raiz*** *de* $f(x)$ *em* F*.*

Outro fato relevante diz respeito a divisão polinomial. O objetivo aqui não é o de detalhar toda teoria relacionada a tal assunto. No entanto, em termos de contextualização, será enunciado o *Algoritmo da Divisão* através do teorema que segue, e posteriormente será feita uma discussão sobre as *classes residuais* de polinômios.

Teorema 2.21. *Sejam* $f(x), g(x) \in \mathrm{F}[x]$ *sendo* $g(x)$ *não nulo. Desta forma, existem* $q(x)$ *e* $r(x) \in \mathrm{F}[x]$ *tais que:*

$$f(x) = q(x) \cdot g(x) + r(x), \tag{2.12}$$

de forma que $r(x) = 0$ *ou* $\partial(r) < \partial(g)$*.*

A Eq. (2.12) representa a *divisão do polinômio* $f(x)$ por $g(x)$. A notação $\dfrac{f(x)}{g(x)}$, indica que está sendo considerada a divisão de $f(x)$ por $g(x)$. Ainda em relação à Eq. (2.12), o polinômio $g(x)$ é denominado *divisor* de $f(x)$. Já os polinômios $q(x)$ e $r(x)$ da Eq. (2.12) são denominados *quociente* e *resto*, respectivamente, da divisão de $f(x)$ por $g(x)$. Retomando o Teorema 2.12, considere os próximos conceitos.

Definição 2.22. *Sejam $f(x), g(x) \in \mathrm{F}[x]$. Diz-se que $f(x)$ é **divisível por** $g(x)$ (ou que $g(x)$ divide $f(x)$) quando o resto da divisão $\dfrac{f(x)}{g(x)}$ é igual a zero (polinômio nulo). Nesse caso usa-se a notação $g(x)|f(x)$.*

Por meio da Definição 2.22 introduz-se um conceito congruência similar ao que foi feito na Seção 2.1.1.

Definição 2.23. *Fixe $f(x) \in \mathrm{F}[x]$. Dados $g(x), h(x) \in \mathrm{F}[x]$, diz-se que $g(x)$ e $h(x)$ são **congruentes módulo** $f(x)$ se $f(x)|(g-h)(x)$. Nesse caso, utiliza-se a notação $g(x) \equiv h(x) \mod f(x)$.*

É possível mostrar que a relação de congruência dada na Definição 2.23 é de equivalência sobre $\mathrm{F}[x]$, de modo que, fixado o polinômio $f(x) \in \mathrm{F}[x]$, a classe de equivalência para um polinômio $g(x) \in \mathrm{F}[x]$ de acordo com a congruência mencionada, denotada por $[g(x)]_f$, é dada pelo conjunto:

$$[g(x)]_f = \{g(x) + q(x) \cdot f(x) : q(x) \in \mathrm{F}[x]\}. \tag{2.13}$$

Dessa forma, $[g(x)]_f$ é denominado como *classe residual* do polinômio $g(x)$ módulo $f(x)$ em $\mathrm{F}[x]$ e o conjunto de todas essa classes é denotada por:

$$\frac{\mathrm{F}[x]}{\langle f(x)\rangle}, \tag{2.14}$$

e denominado de *anel quociente de polinômios*. A denominação de anel dada para o conjunto $\dfrac{\mathrm{F}[x]}{\langle f(x)\rangle}$ se deve ao próximo resultado e pode ser verificado, por exemplo, em [30].

Teorema 2.24. *O conjunto $\dfrac{\mathrm{F}[x]}{\langle f(x)\rangle}$ munido com as operações de soma e multiplicação dadas, respectivamente, por:*

$$[g(x)]_f + [h(x)]_f = [(g+h)(x)]_f \tag{2.15}$$

$$[g(x)]_f \cdot [h(x)]_f = [(g \cdot h)(x)]_f \tag{2.16}$$

possui a estrutura de um anel. Além disso, se $f(x)$ é irredutível então $\dfrac{\mathrm{F}[x]}{\langle f(x)\rangle}$ é um corpo.

Agora, será feita uma discussão relacionada a questão de fatorar polinômios. Quando um polinômio $f(x) \in \mathrm{F}[x]$ pode ser representado em termos de um produto cujos fatores são outros polinômios de $\mathrm{F}[x]$, ou seja,

$$f(x) = \prod_{i=1}^{m} g_i(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_m(x), \tag{2.17}$$

com $g_1(x), g_2(x), \ldots, g_m(x) \in \mathrm{F}[x]$, com $m \in \mathbb{N}^\star$, diz-se que $\prod_{i=1}^{m} g_i(x)$ é uma *forma fatorada* de $f(x)$. Sobre tal fato, apresenta-se o seguinte resultado.

Teorema 2.25. *Os polinômios de $\mathrm{F}[x]$ podem ser fatorados de forma única, a menos da ordem dos fatores, por meio de polinômios irredutíveis.*

Diante de tais fatos, dá-se seguimento com o resultado.

Proposição 2.26. *Sejam $f(x) \in \mathrm{F}[x]$ e $\alpha \in \mathrm{F}$. Então α é uma raiz de $f(x)$ se, e somente se, o polinômio mônico $x - \alpha$ divide $f(x)$.*

Finalizando esta seção apresenta-se agora um resultado que garante que para qualquer corpo $\mathbb{F}_q$ existem polinômios mônicos irredutíveis de grau m em $\mathbb{F}_q[x]$, para qualquer $m \in \mathbb{N}^\star$. E para tal resultado é necessário apresentar a definição de *função de Möbius*.

Definição 2.27. *A **Função de Möbius**, denotada por μ, é a função com domínio $\mathbb{N}$ dada por*

$$\mu(n) = \begin{cases} 1, & \textit{se n = 1}, \\ (-1)^k, & \textit{se n é o produto de k primos distintos}, \\ 0, & \textit{se n é divisível por um quadrado de um número primo qualquer}. \end{cases} \tag{2.18}$$

Considerando a definição 2.27, segue o teorema.

Teorema 2.28. *Denote por $I_q(n)$ o número de polinômios mônicos e irredutíveis de grau n em $\mathbb{F}_q[x]$. Dessa forma:*

$$I_q(n) = \frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{\frac{n}{d}}. \tag{2.19}$$

Note que o Teorema 2.28 mostra que para quaisquer $n, q \in \mathbb{N}^\star$ existe um polinômio $f(x) \in \mathbb{F}_q[x]$ com $\partial(f) = n$ que é mônico e irredutível, uma vez que $I_q(n) > 0$. Para comprovar que $I_q(n) > 0$ para quaisquer $q, n \in \mathbb{N}^\star$ observe que, de acordo com a Definição 2.27, tem-se $\mu(1) = 1$ e se $n > 1$ então $\mu(n) \geq -1$. Desse modo, fixe n inteiro positivo e considere $d_1, d_2, \ldots, d_k$ os divisores positivos de n dados em ordem crescente, ou seja, $d_m < d_{m+1}$. Perceba que $d_m \geq m$ para cada $m = 1, \ldots, k$. Com isso:

$$\frac{n}{d_m} \leq n - m, \tag{2.20}$$

para cada $m = 2, \ldots, k$. Dessa forma, dado $q \in \mathbb{N}^\star$ segue que:

$$
\begin{aligned}
I_q(n) = \frac{1}{n}\sum_{d \mid n} \mu(d)\, q^{\frac{n}{d}} &\geq \frac{1}{n}\left(q^n - \sum_{m=1}^{n-1} q^m\right) \\
&\geq \frac{1}{n}\left(q^n - q\left(\frac{q^{n-1}-1}{q-1}\right)\right) \\
&\geq \frac{q}{n}\left(q^{n-1} - (q^{n-1}-1)\right) \\
&= \frac{q}{n} \\
&> 0.
\end{aligned}
$$

Exemplo 2.29. *Considerando $\mathbb{F}_2[x]$, tem-se que o número de polinômios mônicos irredutíveis de grau 2 nesse anel é $I_2(2) = 1$. Tal polinômio é dado por $f(x) = x^2+x+1$. Agora, para $\mathbb{F}_3[x]$ o número de polinômios mônicos e irredutíveis de grau 2 é dado por $I_3(2) = 3$, e em $\mathbb{F}_5[x]$ temos $I_5(2) = 10$.*

Existem várias pesquisas relacionadas a determinação de polinômios irredutíveis definidos sobre um corpo finito. Não se pretende realizar uma discussão aprofundada em tal assunto, mas deixa-se como sugestão de leitura sobre tal tema, por exemplo, as seguintes referências: [11, 38, 39, 63].

2.3 Extensões de Corpos

Este trabalho tem como base corpos finitos da forma $\mathbb{F}_{2^n}$, com $n \in \mathbb{N}^\star$. Isto é, o presente estudo irá utilizar como uma de suas ferramentas básicas corpos de ordem 2^n que possuem característica igual a 2. Mas, como foi mencionado na seção anterior é preciso garantir a existência de corpos de tal natureza. Nesse sentido, nessa seção será abordado o tema *extensão de corpos*. Uma das utilidades de tal ferramenta é garantir que para qualquer número primo p, e qualquer $n \in \mathbb{N}^\star$, exista um corpo finito da forma $\mathbb{F}_{p^n}$.

2.3.1 Existência e Unicidade de Corpos da forma $\mathbb{F}_{p^n}$

Definição 2.30. *Seja F um corpo. Um **subcorpo** de F é um subconjunto $\mathrm{E} \subseteq \mathrm{F}$ que também é um corpo em relação às operações de F. Nesse caso, diz-se que F é uma **extensão** de E. Se $\mathrm{E} \subsetneq \mathrm{F}$, então E é denominado como um **subcorpo próprio** de F. Um corpo que não possui subcorpos próprios é chamado de **corpo primo**.*

Em relação a Definição 2.30, é feita a seguinte observação. Se F é um corpo e $\mathrm{F}_1, \mathrm{F}_2$ são subcorpos de F, então $\mathrm{F}_1 \cap \mathrm{F}_2$ também é um subcorpo de F. Verifica-se, sem muitas dificuldades, que tal fato é válido para uma interseção arbitrária de subcorpos. Desse modo, segue o seguinte resultado.

Proposição 2.31. *Seja F um corpo. Então F possui um menor subcorpo. Em outras palavras, todo corpo F possui um subcorpo primo.*

Por intermédio da Proposição 2.31 tem-se o próximo teorema.

Teorema 2.32. *Suponha que para o corpo $\mathbb{F}_q$, se tenha $char\,(\mathbb{F}_q) = p$. Então o subcorpo primo de $\mathbb{F}_q$ é isomorfo ao corpo $\mathbb{F}_p$.*

Seguem agora os fatos que permitem garantir a existência e unicidade de corpos $\mathbb{F}_{p^n}$, para qualquer p primo e qualquer $n \in \mathbb{N}^\star$. De início apresenta-se a definição de *corpo de decomposição* de um polinômio.

Definição 2.33. *Considere o polinômio $f(x) \in \mathrm{F}[x]$. O **corpo de decomposição de** $f(x)$ é a menor extensão K de F na qual $f(x)$ se decompõe em fatores lineares de $\mathrm{K}[x]$.*

Teorema 2.34. *Seja $f(x) \in \mathrm{F}[x]$. Então o corpo de decomposição de $f(x)$ existe e é único a menos de isomorfismo.*

Proposição 2.35. *Considere p primo e tome em $\mathbb{F}_p[x]$ o polinômio $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$, em que $n \in \mathbb{N}^*$. Então o corpo de decomposição de $f(x)$ é um corpo finito F tal que $|\mathrm{F}| = p^n$ e $f(x)$ pode ser decomposto da seguinte forma:*

$$x^{p^n} - x = \prod_{a \in \mathrm{F}} (x - a). \tag{2.21}$$

Teorema 2.36. *Para qualquer primo p e qualquer $n \in \mathbb{N}^\star$, existe um corpo finito com p^n elementos. Além disso, todo corpo finito com p^n é isomorfo ao corpo de decomposição de $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.*

Sendo assim, segue imediatamente do Teorema 2.36 o fato de que se dois corpos finitos possuem a mesma ordem então eles são "iguais". Ou seja:

Corolário 2.37. *Todos os corpos finitos de ordem p^n, com p primo e $n \in \mathbb{N}^\star$, são isomorfos entre si.*

2.3.2 Representação dos Corpos $\mathbb{F}_{p^n}$

Serão vistas agora formas e métodos para se representar um corpo finito. No caso, representar um corpo finito significa obter uma forma de descrever todos os elementos desse corpo, bem como as operações de soma e de multiplicação associadas ao mesmo. A primeira forma de se representar um corpo finito é estender a notação apresentada pela Eq. (2.6) de modo que, dado p primo e $n \in \mathbb{N}^*$, temos:

$$\mathbb{F}_{p^n} = \{0, 1, 2, \ldots, p^n - 1\}. \tag{2.22}$$

Nesta situação, as operações de soma e multiplicação são feitas levando-se em consideração a congruência módulo p^n. Repare que a Eq. (2.22) faz uso de p^n símbolos. Tal fato pode ser um problema quando se pensa em termos computacionais e na questão de armazenamento de informações.

O próximo método que permite representar um corpo finito é retratado por meio do teorema que se segue. Tal resultado envolve os conceitos de polinômio irredutível e de classes residuais.

Teorema 2.38. *Considere p um número primo qualquer e suponha que $f(x) \in \mathbb{F}_p[x]$ seja um polinômio irredutível sobre $\mathbb{F}_p$ tal que $\partial(f) = n$, $n \in \mathbb{N}^*$. Assim, o conjunto formado por todos os polinômios de $\mathbb{F}_p[x]$ que possuem grau menor ou igual a $n-1$ e operações realizadas módulo $f(x)$, formam um corpo de ordem p^n.*

Exemplo 2.39. *Considere em $\mathbb{F}_2$ o polinômio irredutível dado por $f(x) = x^4 + x + 1$. Sendo assim, de acordo com o Teorema 2.38, o conjunto dado por $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, x^3+x^2, x^3+x+1, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1\}$, munido com as operações de soma e produto módulo $f(x)$, possui uma estrutura de corpo que, de acordo com o Corolário 2.37, pode ser identificado como $\mathbb{F}_{2^4} = \mathbb{F}_{16}$.*

Agora será vista a segunda forma de representar corpos finitos. Para isso considere o que segue.

Teorema 2.40. *Seja $\mathbb{F}_q$ um corpo. Então, o conjunto $\mathbb{F}_q \setminus \{0\}$ é um grupo multiplicativo cíclico de ordem $q-1$. Dessa forma, tem-se que $a^q = a$ para todo $a \in \mathbb{F}_q$.*

Desse modo, o Teorema 2.40 diz que, todo corpo $\mathbb{F}_q$ possui um elemento α de forma que $\langle\alpha\rangle = \mathbb{F}_q \setminus \{0\}$. Ou seja, usando os termos da teoria de grupos, pode-se dizer que α é um *gerador* do grupo cíclico $\mathbb{F}_q \setminus \{0\}$. Esse fato motiva a próxima definição.

Definição 2.41. *Um gerador do grupo multiplicativo cíclico $\mathbb{F}_q \setminus \{0\}$ é chamado de* ***elemento primitivo*** *de $\mathbb{F}_q$.*

Observe que, pelos resultados vistos até o momento, se $\alpha \in \mathbb{F}_{p^n}$ é um elemento primitivo, então :

$$\mathbb{F}_{p^n} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}. \tag{2.23}$$

A representação para um corpo $\mathbb{F}_{p^n}$ na Eq. (2.23) é muito útil quando se trabalha com a operação de multiplicação. De fato, de acordo com o Teorema 2.40, se $\alpha \in \mathbb{F}_{p^n}$ é um elemento primitivo todos os elementos não nulos de $\mathbb{F}_{p^n}$ são dados como potências de α e $\alpha^{p^n-1} = 1$. Com isso, dados $i, j \in \mathbb{Z}$, tem-se que α^i e α^j representam dois elementos quaisquer de $\mathbb{F}_{p^n}$, e a multiplicação desses elementos é efetuada de modo que

$$\alpha^i \cdot \alpha^j = \alpha^{[i+j]_{p^n-1}}, \tag{2.24}$$

sendo que $[i+j]_{p^n-1}$ representa o resto da divisão de $i+j$ por p^n-1.

Por outro lado, para efetuar a soma entre elementos de $\mathbb{F}_q$ é preciso recorrer a tabelas conhecidas como *Tabelas Logarítmicas de Zech (TLZ)* [30]. A seguir, um estudo de como tal procedimento funciona. Deste modo, considerando que $i < j$ segue que

$$\alpha^i + \alpha^j = \alpha^i(1 + \alpha^{j-i}). \tag{2.25}$$

Nesse caso, sabendo para cada inteiro m qual é o inteiro denotado por $\mathfrak{z}(m)$, de modo que:

$$\alpha^{\mathfrak{z}(m)} = 1 + \alpha^m, \tag{2.26}$$

então a soma indicada na Eq. (2.25) seria dada por uma multiplicação. Isto é:

$$\alpha^i + \alpha^j = \alpha^i \cdot \alpha^{\mathfrak{z}(j-i)}. \tag{2.27}$$

Sendo assim, a TLZ irá fornecer os valores de $\mathfrak{z}(m)$, sendo $1 \leq m \leq p^n - 2$, de modo que a Eq. (2.26) seja satisfeita.

Exemplo 2.42. *Considere o corpo $\mathbb{F}_8 = \mathbb{F}_{2^3}$ obtido utilizando-se o Teorema 2.38 por meio do polinômio irredutível $f(x) = x^3 + x + 1$. Dessa forma tem-se $\mathbb{F}_8 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$. Levando-se em conta as operações de $\mathbb{F}_8$ sendo realizadas em módulo $f(x)$, segue que $\alpha = x$ é um elemento primitivo de $\mathbb{F}_8$. Pelo teorema 2.40 chega-se em $\alpha^8 = \alpha$, logo $\alpha^7 = x^7 = 1$. Além disso, $\alpha^2 = x^2, \alpha^3 = x+1, \alpha^4 = x^2 + x, \alpha^5 = x^2 + x + 1, \alpha^6 = x^2 + 1$. Usando esta representação do corpo $\mathbb{F}_8$, para efetuar a soma entre os elementos de $\mathbb{F}_8$ dados como potências do elemento primitivo $\alpha = x$ de uma forma mais eficiente, pode-se utilizar a TLZ, que nesta situação, é dada pela tabela 2.1. Por exemplo, para realizar a soma entre α^4 e α^6 deve-se proceder da seguinte maneira: $\alpha^4 + \alpha^6 = \alpha^4(1 + \alpha^2)$. Como $\mathfrak{z}(2) = 6$, segue que $\alpha^4 + \alpha^6 = \alpha^4 \cdot \alpha^6 = \alpha^{\{10\}_7} = \alpha^3$.*

Tabela 2.1: *TLZ para o Exemplo 2.42.*

m	1	2	3	4	5	6
$\mathfrak{z}(m)$	3	6	1	5	4	2

Evidentemente as formas de representação de corpos finitos que foram apresentadas aqui são equivalentes, tendo em vista o fato de que corpos finitos de mesma ordem são isomorfos. O Exemplo 2.42 mostra como os métodos discutidos até aqui são de fato eficientes a partir do momento em que imaginamos o emprego destas técnicas em situações em que são considerados corpos com uma grande quantidade de elementos. Será visto na próxima seção como obter uma representação do corpo $\mathbb{F}_{p^n}$ conforme a Eq. (2.23) de uma forma mais assertiva.

2.4 Polinômios Ciclotômicos: Uma forma de Representar os Corpos $\mathbb{F}_{p^n}$

Esta é a seção final deste Capítulo. Determinaremos agora qual será o procedimento adotado neste trabalho em relação a representação dos corpos finitos. Como já foi mencionado na seção anterior, o interesse é obter uma representação dos elementos do corpo $\mathbb{F}_{p^n}$ como potências de elementos primitivos. Nesta seção será utilizado o conceito de *polinômios ciclotômicos*. Tais polinômios permitem encontrar, de uma forma eficiente, elementos primitivos de um corpo finito. De início, considere a definição a seguir.

Definição 2.43. *Seja $n \in \mathbb{N}^*$. O corpo de decomposição de $x^n - 1$ sobre o corpo F é chamado de n-**ésimo corpo ciclotômico** sobre F e é denotado por $\mathrm{F}^{(n)}$. As raízes de $x^n - 1$ em $\mathrm{F}^{(n)}$ são chamadas de n-**ésimas raízes da unidade** sobre F e o conjunto de todas essas raízes é denotado por $\mathrm{F}^{(n)}_{roots}$.*

A seguir é apresentado o primeiro resultado relacionado corpos ciclotômicos e raízes n-ésimas.

Proposição 2.44. *Considere o corpo F tal que $char(\mathrm{F}) = p$, p primo, e seja $n \in \mathbb{N}^*$. Se p não divide n então $\mathrm{F}^{(n)}_{roots}$ é um grupo cíclico de ordem n com respeito à multiplicação de $\mathrm{F}^{(n)}$.*

Definição 2.45. *Seja F um corpo com $char(\mathrm{F}) = p$ e $n \in \mathbb{N}^*$ não divisível por p. Então o gerador do grupo cíclico $\mathrm{F}^{(n)}_{roots}$ é chamado de n-**ésima raiz primitiva da unidade** sobre F.*

Definição 2.46. *Seja F um corpo com $char(\mathrm{F}) = p$, sendo p um número primo. Dado $n \in \mathbb{N}^\star$ não divisível por p, e α uma n-ésima raiz primitiva da unidade sobre F. Então o polinômio*

$$Q_n(x) = \prod_{\substack{r=1 \\ mdc(r,n)=1}}^{n} (x - \alpha^r), \tag{2.28}$$

*é chamado de n-**ésimo polinômio ciclotômico sobre** F.*

Considerando a definição 2.46, segue o próximo resultado.

Teorema 2.47. *Seja F um corpo tal que $char(\mathrm{F}) = p$ e $n \in \mathbb{N}^\star$ não divisível por p.*

1. $x^n - 1 = \prod_{d|n} Q_d(x)$.
2. *O n-ésimo polinômio ciclotômico $Q_n(x)$ sobre F satisfaz a seguinte equação*

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}. \tag{2.29}$$

Exemplo 2.48. *Considere o corpo $\mathbb{F}_4$ e $n = 15$. Desse modo segue:*

- $Q_1 = (x - 1)$.
- $Q_3(x) = \prod_{d|3} (x^d - 1)^{\mu(3/d)} = (x - 1)^{\mu(3)}(x^3 - 1)^{\mu(1)} = x^2 + x + 1$.
- $Q_5(x) = \prod_{d|5} (x^d - 1)^{\mu(5/d)} = (x - 1)^{\mu(5)}(x^5 - 1)^{\mu(1)} = x^4 + x^3 + x^2 + x + 1$.

- $Q_{15}(x) = \prod_{d|15}(x^d - 1)^{\mu(15/d)} = (x-1)^{\mu(15)}(x^3-1)^{\mu(5)}(x^5-1)^{\mu(3)}(x^{15}-1)^{\mu(1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$

Sendo assim, segue que:

$$(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^8-x^7+x^5-x^4+x^3-x+1) = x^{15}-1.$$

A seguir serão apresentados mais resultados que auxiliarão a determinar qual polinômio irredutível escolher de forma a obter um elemento primitivo.

Definição 2.49. *Seja m um número inteiro positivo e considere a fatoração de m em potência de primos dada por $m = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. Então, a **função de Euler** do número m, denotada por φ, é definida da seguinte forma*

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right). \tag{2.30}$$

Teorema 2.50. *Considerando a função de Euler φ, segue que o corpo finito $\mathbb{F}_q$ possui $\varphi(q-1)$ elementos primitivos, em que $q = p^n$ com p primo e $n \in \mathbb{N}$.*

Exemplo 2.51. *Tome o corpo $\mathbb{F}_4$ como exemplo. Considerando a função de Euler, tem-se que $\mathbb{F}_4$ possui $\varphi(4-1) = \varphi(3) = 3\left(1-\frac{1}{3}\right) = 2$ elementos primitivos. Assim, sabendo que o corpo $\mathbb{F}_4$ possui 4 elementos dentre os quais estão o 0 e o 1, pode-se concluir que os demais elementos serão primitivos. Isso significa que qualquer polinômio irredutível de grau 2 sobre $\mathbb{F}_2$ que for escolhido fornecerá uma raiz como elemento primitivo. Em contrapartida, se for utilizado o raciocínio anterior veremos que o corpo $\mathbb{F}_7$ possui um total de $\varphi(6) = 3$ elementos primitivos. Como, obviamente, a ordem de $\mathbb{F}_7$ é 7, não se pode escolher qualquer polinômio irredutível para encontrarmos uma raiz que seja um elemento primitivo neste corpo.*

Como considerações finais são apresentados os seguintes teoremas.

Teorema 2.52. *Sejam $q, n \in \mathbb{N}$ tais que $mdc(q,n) = 1$. Então o polinômio $Q_n(x)$ possui uma forma fatorada sobre $\mathbb{F}_q[x]$ composta por $\frac{\varphi(n)}{d}$ fatores mônicos irredutíveis distintos de mesmo grau d, sendo $d = ord_n(q)$. Além disso, $\mathbb{F}_{q^d}$ é o corpo de decomposição de qualquer um desses fatores*

Teorema 2.53. *O corpo $\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre qualquer um de seus subcorpos.*

Dessa forma, considere o seguinte resumo que segue para estabelecer um método de representar os corpos $\mathbb{F}_{p^n}$. De acordo com o Teorema 2.53, o corpo $\mathbb{F}_{p^n}$ é o (p^n-1)-ésimo corpo ciclotômico sobre $\mathbb{F}_p$. Assim, como $mdc(p, p^n-1) = 1$, considere o polinômio ciclotômico $Q_{p^n-1}(x)$. Pelo Teorema 2.52, $Q_{p^n-1}(x)$ possui uma fatoração

sobre $\mathbb{F}_p$ composta por $\dfrac{\varphi(p^n-1)}{d}$ polinômios mônicos e irredutíveis de mesmo grau $d = ord_{p^n-1}(p)$. Assim, pelo item 1 do Teorema 2.47 , uma raiz de qualquer um desses polinômios será uma (p^n-1)-ésima raiz primitiva da unidade sobre $\mathbb{F}_p$. Isto é, fixada uma dessas raízes, segue que $(\mathbb{F}_{p^n})_{root}$ é um grupo cíclico, em relação à multiplicação de $\mathbb{F}_{p^n}$, que possui exatamente p^n-1 elementos, de acordo com a Proposição 2.44. Logo, considerando $0 \in \mathbb{F}_{p^n}$, tem-se que $(\mathbb{F}_{p^n})_{root} \cup \{0\}$ é um corpo em relação às operações de $\mathbb{F}_{p^n}$, que possui p^n elementos, sendo que os elementos não nulos são dados por meio de potências.

Por meio de alguns exemplos será mostrado como tal rotina funciona na prática.

Exemplo 2.54. *Agora será mostrado como obter uma representação do corpo $\mathbb{F}_{16}$. Como $16 = 2^4$, segue que $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ é igual ao décimo quinto corpo ciclotômico sobre $\mathbb{F}_2$. Do Exemplo 2.48, obtém-se $Q_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$. Note que $\varphi(15) = 8$ e $ord_{15}(2) = 4$. Sendo assim, pelo Teorema 2.52, $Q_{15}(x)$ admite uma fatoração sobre $\mathbb{F}_2$ composta por 2 polinômios mônicos irredutíveis de grau 4. Tal fatoração é dada por $Q_{15}(x) = (x^4+x+1)(x^4+x^3+1)$. Desse modo pode-se escolher uma raiz de qualquer um dos polinômios presentes na decomposição de $Q_{15}(x)$ para obter uma representação de $\mathbb{F}_{16}$ da forma $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$. A seguir, seguem duas TLZ (2.2 e 2.3) para a situação ilustrada. A primeira foi construída considerando que o elemento primitivo usado na representação de $\mathbb{F}_{16}$ é uma raiz de $p_1(x) = x^4 + x + 1$, e a outra foi obtida tomando-se como elemento primitivo uma raiz de $p_2(x) = x^4 + x^3 + 1$.*

Tabela 2.2: *TLZ de $\mathbb{F}_{16}$ considerando $p_1(x)$.*

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mathfrak{z}(m)$	4	8	14	1	10	13	9	2	7	5	12	11	6	3

Tabela 2.3: *TLZ de $\mathbb{F}_{16}$ considerando $p_2(x)$.*

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mathfrak{z}(m)$	12	9	4	3	10	8	13	6	2	5	14	1	7	11

Exemplo 2.55. *Seguindo os mesmos passos do Exemplo 2.54 pode-se obter uma representação em termos de potências de um elemento primitivo, por exemplo, para $\mathbb{F}_{27} = \mathbb{F}_{3^3}$. Nesse caso, seguem as seguintes informações:*

- $\mathbb{F}_{27} = \mathbb{F}_3^{(26)}$. *Ou seja, $\mathbb{F}_{27}$ é o vigésimo sexto corpo ciclotômico sobre $\mathbb{F}_3$.*
- *Os polinômios $f_1(x) = x^3+2x+1$, $f_2(x) = x^3+2x^2+1$, $f_3(x) = x^3+x^2+2x+1$ e $f_4(x) = x^3+2x^2+x+1$, são irredutíveis sobre $\mathbb{F}_3$ e $Q_3(x) = f_1(x)f_2(x)f_3(x)f_4(x)$.*

Por fim, apresentam-se TLZ em 2.4, 2.5, 2.6 e 2.7 de acordo com cada um dos fatores mônicos irredutíveis de $Q_{26}(x)$.

Desse modo observa-se, com os Exemplos 2.54 e 2.55, que o método escolhido para representar um corpo finito $\mathbb{F}_{p^n}$ é interessante do ponto de vista de se obter todos os elementos não nulos representados por meio de uma potência, uma vez que isso significa que o corpo $\mathbb{F}_{p^n}$ fica caracterizado por meio de um único elemento. No entanto, tal elemento está associado a um determinado polinômio presente na fatoração do (p^n-1)-polinômio ciclotômico relacionado e, por consequência, a operação de adição deste corpo é obtida por meio da TLZ associada ao polinômio. Sendo assim, pode-se dizer que encontrar a forma fatorada do (p^n-1)-polinômio ciclotômico é um ponto central do presente trabalho. Sobre tal questão, é possível citar diversos trabalhos como [7, 8, 17, 31, 53] que são dedicados a determinar métodos para obter a fatoração de polinômios, ou critérios para descobrir quando um polinômio é irredutível sobre $\mathbb{F}_p$ e possui uma raiz que é um elemento primitivo de $\mathbb{F}_p^{(n)}$. No entanto, no Capítulo 4, será visto que tal questão não interfere na parte teórica do presente trabalho.

Tabela 2.4: *TLZ construída considerando* $f_1(x)$.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$\mathfrak{z}(m)$	9	21	1	18	17	11	4	15	3	6	10	2	$\nexists$	16	25	22	20	7	23	5	12	14	24	19	8

Tabela 2.5: *TLZ construída considerando* $f_2(x)$.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$\mathfrak{z}(m)$	18	7	2	12	14	21	3	19	6	4	1	2	$\nexists$	24	16	20	23	11	22	15	9	8	25	5	17

Tabela 2.6: *TLZ construída considerando* $f_3(x)$.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$\mathfrak{z}(m)$	8	6	24	3	19	18	22	10	20	1	16	9	$\nexists$	23	5	17	11	2	15	12	14	25	21	4	7

Tabela 2.7: *TLZ construída considerando* $f_4(x)$.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$\mathfrak{z}(m)$	19	22	5	1	12	14	11	24	15	9	21	3	$\nexists$	17	10	25	6	16	4	8	7	23	2	20	18

CAPÍTULO 3

CÓDIGOS CORRETORES DE ERROS

Pode-se considerar que a Teoria dos Códigos Corretores de Erros foi apresentada pela primeira vez, de formalmente, por Claude Shannon em 1948, por meio da publicação do artigo *"A mathematical theory of communication"* [60]. Desde então, essa teoria tem se desenvolvido como uma disciplina interdisciplinar que combina matemática e engenharia, com aplicações em diversas formas modernas relacionadas à Teoria da Informação e Comunicação. Essa teoria lida principalmente com a transmissão e o armazenamento confiáveis de dados. Uma vez que os meios de informação nem sempre são totalmente confiáveis na prática, os códigos corretores de erros surgem como uma ferramenta para garantir a transmissão de dados de informação com uma excelente margem de segurança.

3.1 Códigos: Conceitos Básicos

Esta seção apresenta as definições básicas relacionadas à Teoria de Códigos. Para esta parte do texto, as principais referências são [30, 33, 47, 55, 58, 70].

Definição 3.1. *Um conjunto finito $\mathcal{A}$ será chamado de **alfabeto**, e a notação $|\mathcal{A}|$ representará o número de elementos de $\mathcal{A}$. As **palavras** de $\mathcal{A}$ são as sequências finitas formadas por símbolos pertencentes a $\mathcal{A}$. O **comprimento** de uma palavra é igual ao número de símbolos presentes em sua composição.*

Exemplo 3.2. *Uma forma interessante de se exemplificar o conceito de código pode ser retratada por uma das formas de comunicação mais utilizada pela humanidade: o idioma. Por exemplo, na língua portuguesa é utilizado um alfabeto composto por 26 letras e as palavras desse idioma são as sequências dessas letras. Note, no entanto, que a língua portuguesa não é formada por todas as sequências possíveis obtidas a partir das letras do alfabeto, como é o caso da sequencia de letras dada por "leeeespa" não representa uma palavra do idioma português.*

Definição 3.3. *Seja $\mathcal{A}$ um alfabeto. Um **código corretor de erros** de comprimento n é um subconjunto próprio qualquer de $\mathcal{A}^n$. Isto é, um código $\mathcal{C}$ é um subconjunto tal que:*

$$\mathcal{C} \subset \mathcal{A}^n = \underbrace{\mathcal{A} \times \mathcal{A} \times \cdots \times \mathcal{A}}_{n \text{ vezes}}.$$

Além disso, se $|\mathcal{A}| = q$, diz-se que $\mathcal{C}$ é um ***código*** q***-ário***.

Vale ressaltar que na literatura também são considerados códigos que possuem palavras com comprimentos distintos [58]. No entanto, de acordo com a Definição 3.3, neste trabalho serão considerados apenas códigos cujas palavras possuem o mesmo comprimento. Nesse caso, diz que esses códigos são *códigos de bloco*.

Exemplo 3.4. *Considerando o conjunto $\{0, 1\}$ como alfabeto, os códigos obtidos são chamados de códigos binários. Neste contexto, os conjuntos $\mathcal{C}_1 = \{(010), (000), (101), (110)\}$ e $\mathcal{C}_2 = \{(1001), (1110), (0101)\}$ são exemplos de códigos binários de comprimento 3 e 4, respectivamente.*

Segundo [70], a teoria dos códigos de correção de erros trata da transmissão e armazenamento confiáveis de dados. Um dos grandes problemas em relação à teoria da informação é que os meios de transmissão não são totalmente confiáveis na prática, no sentido de que o *ruído* (qualquer forma de interferência) frequentemente causa a distorção dos dados. Para lidar com esta situação inevitável alguma forma de *redundância* é incorporada aos dados originais. Com esta redundância, mesmo que sejam introduzidos *erros* (até algum nível de tolerância), a informação original pode ser recuperada, ou pelo menos a presença de erros pode ser detectada. Com o objetivo de ilustrar a questão de *interferência*, *redundância* e *erro* considere o próximo exemplo

Exemplo 3.5. *Suponha que um robô se mova sobre um tabuleiro quadriculado de forma que siga apenas um dos comandos por vez: Leste, Oeste, Norte ou Sul. Assim, o robô se desloca do centro de uma casa para o centro da casa adjacente que é indicada pelo comando recebido. Os comandos recebidos pelo robô são codificados como elementos do conjunto $\{0, 1\} \times \{0, 1\}$ da seguinte forma: A informação correspondente ao lado direito*

Tabela 3.1: *Codificação das direções recebidas pelo robô.*

Direção	coordenadas
Leste	00
Oeste	01
Norte	10
Sul	11

da Tabela 3.1 é chamada de código da fonte. *Agora, suponha que esses pares ordenados que constituem o código fonte devam ser transmitidos via rádio e que o sinal no caminho sofra algum tipo de interferência de tal modo que a mensagem 00 seja recebida pelo robô como 01. Desta forma, o robô passaria a ir para Oeste ao invés de ir para Leste. Sendo assim, para se evitar tal fato, as palavras são recodificadas para que sejam introduzidas redundâncias que permitam detectar e corrigir erros. O código pode ser modificado como é mostrado na tabela 3.2. Observe que nessa recodificação as duas primeiras posições*

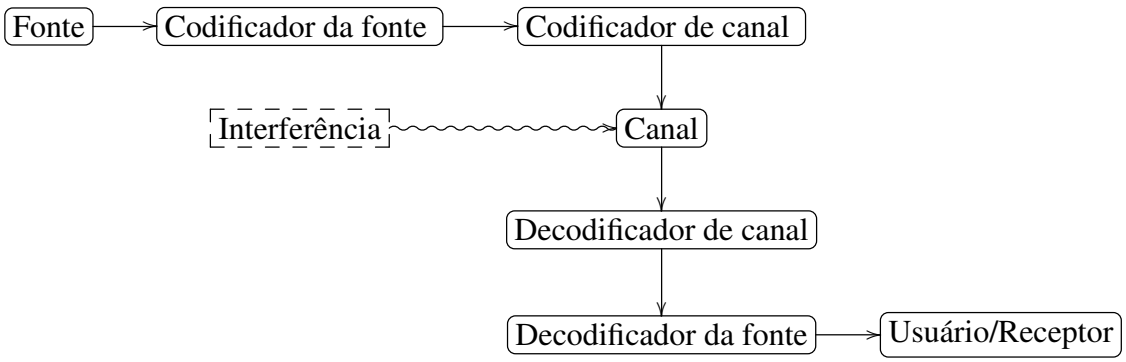
Tabela 3.2: *Recodificação das direções recebidas pelo robô.*

Direção	Coordenadas	Pós codificação
Leste	00	00000
Oeste	01	01011
Norte	10	10110
Sul	11	11101

reproduzem o código da fonte, enquanto que as três posições restantes são redundâncias introduzidas. O novo código introduzido, e exemplificado pela Tabela 3.2, é denominado código do canal. *Desta vez suponha que a direção para a qual o robô deve se deslocar seja o Oeste, ou seja, a informação enviada é 01011, porém, devida a interferências no canal, a mensagem recebida é 01111. Assim é possível detectar o erro se a mensagem recebida for comparada com todas as possíveis mensagens do código de modo a notar que esta não pertence ao código. Além disso, a mensagem do código que tem menor número de componentes diferentes da mensagem recebida é 01011, que é precisamente a mensagem enviada. Logo, é possível corrigir o erro.*

O processo de codificação e decodificação dado pelo Exemplo 3.5 pode ser, de modo geral, simplificado e esquematizado como mostra a Figura 3.1.

Figura 3.1: *Esquema simples de um sistema de comunicação.*



3.1.1 Métrica de Hamming

É possível introduzir uma noção de proximidade entre palavras de um mesmo código de bloco de comprimento n. Tal noção é dada por meio do conceito de *distância de Hamming*.

Definição 3.6. *Dados dois elementos $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$ de um espaço $\mathcal{A}^n$, chama-se **distância de Hamming** de x a y, e denota-se por $d_H(x, y)$, ao número de coordenadas em que estes elementos diferem entre si, isto é:*

$$d_H(x, y) = |\{i \ : \ x_i \neq y_i, \ 1 \leq i \leq n\}|. \tag{3.1}$$

*Dado um código $\mathcal{C} \subset \mathcal{A}^n$, chama-se **distância mínima de Hamming** de $\mathcal{C}$ ao número denotado por $d_H(\mathcal{C})$ e definido da seguinte forma:*

$$d_H(\mathcal{C}) = \min\{d_H(x, y) \ : \ x, y \in \mathcal{C}, \ x \neq y\}. \tag{3.2}$$

Assim segue o seguinte resultado.

Proposição 3.7. *A distância de Hamming d_H é, de fato, uma métrica. Ou seja, dados $u, v, w \in \mathcal{A}^n$, têm-se:*

i) $d_H(u, v) \geq 0$*, valendo a igualdade se, e só se,* $u = v$*;*

ii) $d_H(u, v) = d_H(v, u)$*;*

iii) $d_H(u, v) \leq d_H(u, w) + d_H(w, v)$.

Portanto, a Proposição 3.7 mostra que a distância de Hamming é uma métrica que é chamada de *métrica de Hamming*. Desse modo, vê-se que o espaço $\mathcal{A}^n$ possui uma estrutura de espaço métrico.

Note que um código $\mathcal{C} \subset \mathcal{A}^n$ pode ser caracterizado em função de três parâmetros: o comprimento, o número de palavras e a distância mínima. A princípio, se for considerado que m representa o número de elementos de $\mathcal{C}$, para se calcular a distância mínima $d_H(\mathcal{C})$ seria necessário calcular $\dfrac{m!}{2!(m-2)!}$ distâncias, fato que exige um esforço computacional elevado. No entanto, serão apresentados alguns conceitos e resultados que possibilitam estabelecer estratégias para se calcular $d_H(\mathcal{C})$ de uma forma mais viável. Maiores detalhes sobre tal fato podem ser verificados em [30].

Primeiramente, dado um código $\mathcal{C}$ com distância $d_H(\mathcal{C})$, define-se:

$$\kappa = \left\lfloor \frac{d_H(\mathcal{C}) - 1}{2} \right\rfloor, \tag{3.3}$$

em qee $\lfloor t \rfloor$ representa a parte inteira de um número real t.

Teorema 3.8. *Seja $\mathcal{C}$ um código com distância mínima $d_H(\mathcal{C})$. Então $\mathcal{C}$ pode corrigir até κ erros e detectar até $d_H(\mathcal{C}) - 1$ erros.*

Observe que, de acordo com o Teorema 3.8, quanto maior for a distância mínima de um código, maior será a sua capacidade de correção de erros. Nesse sentido, para a teoria de códigos, é de suma importância poder determinar o valor de $d_H(\mathcal{C})$, ou ao menos poder definir uma cota inferior para a distância mínima.

3.1.2 Códigos Equivalentes

Aqui será apresentada a definição de *códigos equivalentes*. Para explorar tal conceito é necessário que se defina o que é uma *isometria.*

Definição 3.9. *Seja $\mathcal{A}$ um alfabeto e $n \in \mathbb{N}^*$. Uma função $F : \mathcal{A}^n \longrightarrow \mathcal{A}^n$ é uma* ***isometria*** *de $\mathcal{A}^n$ se preserva distâncias de Hamming. Isto é:*

$$d_H(F(x), F(y)) = d_H(x, y); \quad \forall\, x, y, \in \mathcal{A}^n. \tag{3.4}$$

As características apresentadas por uma isometria são dadas na forma do próximo resultado.

Proposição 3.10. *Em relação às isometrias seguem as seguintes propriedades.*

i) Toda isometria de $\mathcal{A}^n$ é uma bijeção de $\mathcal{A}^n$.

ii) A função identidade de $\mathcal{A}^n$ é uma isometria.

iii) Se F é uma isometria de $\mathcal{A}^n$, então F^{-1} é uma isometria de $\mathcal{A}^n$.

iv) Se F e G são isometrias de $\mathcal{A}^n$, então a composição $F \circ G$ também é uma isometria de $\mathcal{A}^n$.

Com isso tem-se a próxima definição.

Definição 3.11. *Dados dois códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ em $\mathcal{A}^n$, diz-se que $\mathcal{C}_2$ é um* ***código equivalente*** *a $\mathcal{C}_1$ se existir uma isometria F de $\mathcal{A}^n$ tal que $F(\mathcal{C}_1) = \mathcal{C}_2$.*

É possível verificar que a Definição 3.11 de fato determina uma relação de equivalência sobre o conjunto de todos os códigos de $\mathcal{A}^n$. Nesse caso, os códigos que pertencem a mesma classe de equivalência possuem os mesmos parâmetros, ou seja, se os códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ de $\mathcal{A}^n$ são equivalentes, então o comprimento, a dimensão e a distância mínima de $\mathcal{C}_1$ e $\mathcal{C}_2$ são iguais. Mais detalhes sobre códigos podem ser verificados nas referências [30, 33, 47].

3.2 Códigos Lineares

A princípio existem dois tipos de classes de códigos corretores de erros: o lineares e os não lineares. Os códigos que serão apresentados neste trabalho pertencem à primeira destas classes e possuem como alfabeto um corpo $\mathbb{F}_q$.

Definição 3.12. *Um código $\mathcal{C} \subset \mathbb{F}_q^n$ será chamado de* ***código linear q-ário*** *se for um subespaço vetorial de $\mathbb{F}_q^n$.*

Observe que, de acordo com a Definição 3.12, todo código linear é um espaço vetorial de dimensão finita. Dado um código linear $\mathcal{C}$, seja k sua dimensão e tome $\{u_1, u_2, \ldots, u_k\}$ como sendo uma de suas bases. Desse modo, qualquer elemento $u \in \mathcal{C}$ se escreve de forma única como:

$$u = \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_k u_k \tag{3.5}$$

onde $\lambda_i \in \mathbb{F}_q,\ i = 1, \ldots, k$. Sendo assim, utilizando o fato de que temos q escolhas para cada $\lambda_i \in \mathbb{F}_q$, segue que o número de palavras m do código $\mathcal{C}$ é dado por:

$$m = |\mathcal{C}| = q^k, \tag{3.6}$$

e, como consequência,

$$\dim_{\mathbb{F}_q} \mathcal{C} = k = \log_q q^k = \log_q m. \tag{3.7}$$

Assim, verifica-se que o número de palavras de um código linear q-ário $\mathcal{C}$ depende de sua dimensão. Desde modo, ao longo do texto, a terna $[n, k, d_H(\mathcal{C})]_q$, em que n é o comprimento, k é a dimensão e $d_H(\mathcal{C})$ é a distância mínima, será utilizada para se referir aos *parâmetros de um código linear q-ário.*

Definição 3.13. *Dado $u \in \mathbb{F}_q^n$, definimos o* ***peso de Hamming de*** *u, denotado por $wt_H(u)$ como sendo o número inteiro dado por*

$$wt_H(u) := |\{i \ :\ u_i \neq 0\}|, \tag{3.8}$$

isto é,

$$wt_H(u) = d_H(u, 0). \tag{3.9}$$

Definição 3.14. ***O peso de Hamming um código linear*** *$\mathcal{C}$, denotado por $wt_H(\mathcal{C})$, é o número inteiro dado por:*

$$wt_H(\mathcal{C}) := \min\{wt_H(u) \ :\ u \in \mathcal{C} \setminus \{0\}\}. \tag{3.10}$$

O próximo resultado estabelece a relação entre a distância mínima e o peso de um código.

Proposição 3.15. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear com distância mínima $d_H(\mathcal{C})$. Desse modo:*

i) $\forall\, u, v, \in \mathbb{F}_q^n,\quad d_H(u, v) = wt_H(u - v)$*;*

ii) $d_H(\mathcal{C}) = wt_H(\mathcal{C})$.

Como último resultado dessa seção, segue um lema relacionado à códigos binários.

Lema 3.16. *Sejam $x, y \in \mathbb{F}_2^n$. Sendo assim, temos que:*

$$wt_H(x + y) = wt_H(x) + wt_H(y) - 2|x \cap y|, \tag{3.11}$$

em que $|x \cap y|$ representa o número de coordenadas não nulas que x e y possuem em comum.

Demonstração: Primeiramente, observe que para vetores binários tem-se a seguinte igualdade:

$$wt_H(x+y) = d_H(x-y, 0).$$

Agora, sem perda de generalidade, suponha que x e y possuam apenas uma coordenada em comum. Sendo assim, $wt_H(x+y) = d_H(x-y,0) = (wt_H(x)-1) + (wt_H(y)-1)$. Procedendo com esse raciocínio $|x \cap y|$ vezes, segue o resultado. □

3.2.1 Matriz Geradora

Levando-se em consideração a teoria de álgebra linear, os subespaços vetoriais $\mathcal{C}$ de um espaço vetorial $\mathbb{F}_q^n$ podem ser descritos por meio de matrizes. No caso, considerando o corpo finito $\mathbb{F}_q$, seja $\mathcal{B} = \{\mathrm{v}_1, \mathrm{v}_2, \ldots, \mathrm{v}_k\}$, uma base para o código linear $\mathcal{C} \subset \mathbb{F}_q^n$, e seja G a matriz cujas linhas são os vetores $\mathrm{v}_i = (v_{i1}, v_{i2}, \ldots, v_{in}) \in \mathcal{B}$, com $i = 1, \ldots, k$. Isto é:

$$G = \begin{bmatrix} \mathrm{v}_1 \\ \mathrm{v}_2 \\ \vdots \\ \mathrm{v}_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{bmatrix}. \tag{3.12}$$

Desta forma segue a próxima definição.

Definição 3.17. *Uma **matriz geradora** G **de um** código linear $\mathcal{C} \subset \mathbb{F}_q^n$ de dimensão k é uma matriz de ordem $k \times n$ cujas linhas formam uma base para $\mathcal{C}$.*

Desse modo, pela Definição 3.17, as palavras de um código linear $\mathcal{C}$ pertencem ao espaço gerado pelas linhas de G. Neste caso, diz-se que $\mathcal{C}$ é um *código gerado pela matriz* G. Note que, é possível associar uma determinada matriz $\tilde{G}$ de ordem $k_1 \times n$ a um código $\mathcal{C} \subset \mathbb{F}_q^n$, de dimensão k_2 cujas palavras estejam no espaço gerado pelas linhas de $\tilde{G}$. No entanto, neste caso, a dimensão de $\mathcal{C}$ será menor ou igual ao número de linhas de $\tilde{G}$, ou seja, $k_2 \leq k_1$. Para isso supõe-se que algumas linhas de $\tilde{G}$ são linearmente dependentes. No entanto, uma matriz geradora conforme a Definição 3.17 pode ser obtida pela remoção das linhas de $\tilde{G}$ que causam a dependência linear. Dessa forma, ocasionalmente pode-se dizer que a matriz $\tilde{G}$ é uma matriz geradora de $\mathcal{C}$, embora isso não seja tecnicamente correto quando $k_2 < k_1$, entretanto, o significado deve ser claro. Em qualquer caso, a dimensão k_1 do código associado a $\tilde{G}$ é o número de linhas linearmente independentes, ou seja, o posto de $\tilde{G}$.

Ainda em relação à matriz G da Eq. (3.12), considere a transformação linear dada por:

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & x & \mapsto & x \cdot G \end{array}. \tag{3.13}$$

Com isso, se considerarmos $x = (x_1, x_2, \ldots, x_k)$, temos $T(x) = x_1 \mathrm{v}_1 + x_2 \mathrm{v}_2 + \cdots + x_k \mathrm{v}_k$, ou seja, temos que T é uma transformação linear injetora. Logo, do teorema do núcleo e da imagem segue que para se obter um código linear $\mathcal{C} \subset \mathbb{F}_q^n$ de dimensão k basta definir uma transformação linear injetora $T : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$ e considerar que $Im(T) = \mathcal{C}$. Observe que a matriz G depende da escolha da base $\mathcal{B}$.

Exemplo 3.18. *Considere a matriz G definida sobre o corpo $\mathbb{F}_2$:*

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Definindo a transformação linear:

$$\begin{array}{rccc} T: & \mathbb{F}_2^3 & \longrightarrow & \mathbb{F}_2^6 \\ & x & \mapsto & x \cdot G \end{array},$$

obtém-se o código linear: $\mathcal{C} \subset \mathbb{F}_2^6$ de parâmetros $[6, 3, 1]$, dado por $\mathcal{C} = \{(0,0,0,0,0,0), (1,0,1,1,1,0), (1,0,1,1,0,0), (1,0,1,0,0,1), (0,0,0,0,1,0), (0,0,0,1,1,1), (0,0,0,1,0,1), (1,0,1,0,1,1)\}$. Nesse caso, por exemplo, as palavras (110) e (011) do código fonte são codificadas, respectivamente, como $(0,1,0,0,1,0)$ e $(0,1,0,1,0,1)$.

Percebe-se que como a base para um código linear $\mathcal{C} \subset \mathbb{F}_q^n$ não é única, então a matriz geradora G para $\mathcal{C}$ também não o será. Operações elementares sobre as linhas (multiplicar uma linha por um escalar, adicionar um múltiplo escalar de uma linha a outra e trocar duas linhas) realizadas em G fornecem matrizes que também geram $\mathcal{C}$. Em algumas ocasiões, uma matriz geradora pode ser mais útil do que outra. Por exemplo, se pudermos encontrar uma matriz geradora com a forma:

$$\Big[I_k \,\vdots\, A \Big], \tag{3.14}$$

em que I_k é a matriz identidade de ordem k e A é uma matriz de ordem $k \times (n-k)$ e pensarmos em termos de resolução de sistemas lineares, as soluções do sistema associado a G aparecerão nas primeiras k posições da palavra código. Sendo assim, tem-se a definição que segue.

Definição 3.19. *Uma matriz geradora G de um código $\mathcal{C} \subset \mathbb{F}_q^n$ está na **matriz na forma padrão** quando:*

$$G = \Big[I_k \,\vdots\, A \Big], \tag{3.15}$$

em que A é uma matriz de ordem $k \times (n-k)$.

Note que, nem sempre é possível achar uma matriz geradora de um código $\mathcal{C}$ na forma padrão utilizando apenas as operações elementares sobre as linhas. Tal

fato pode ser exemplificado através da matriz G que aparece no Exemplo 3.18. No entanto, acrescentando às operações elementares sobre as linhas de uma matriz geradora a operação do tipo: *permutação entre as colunas*, pode-se demonstrar o próximo resultado que pode ser verificado em [30].

Teorema 3.20. *Dado um código linear $\mathcal{C} \subset \mathbb{F}_q^n$, existe um código equivalente $\mathcal{C}'$ que possui matriz geradora na forma padrão.*

Exemplo 3.21. *Dessa forma, combinando as operações elementares sobre linhas com a operação de permutação de colunas é possível obter a partir da matriz G dada no Exemplo 3.18, uma matriz na forma G' padrão dada por:*

$$G' = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

E de acordo com o Teorema 3.20, o código gerado por G' é equivalente ao código gerado por G.

3.2.2 Matriz Teste de Paridade

Para iniciar esta Seção, considere a Definição que segue:

Definição 3.22. *Dada uma matriz M definimos o **posto** de M, denotado por $rank(M)$ como a dimensão do espaço gerado pelas colunas de M.*

Relacionado ao conceito de matriz geradora está o conceito de matriz teste de paridade.

Definição 3.23. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear de dimensão k. Uma matriz H de ordem $(n-k) \times n$ é chamada **matriz teste de paridade** de $\mathcal{C}$, quando $rank(H) = n - k$ e se $u \in \mathcal{C}$ se, e só se, $H \cdot u^T = 0$.*

Perceba que, de acordo com a Definição 3.23, um elemento de $\mathbb{F}_q^n$ é visto como uma matriz linha.

A seguir, tem-se uma proposição relacionada à matriz teste de paridade.

Proposição 3.24. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear de dimensão k e suponha que $G = \left[I_k \,\vdots\, A \right]$, seja uma matriz geradora de $\mathcal{C}$ na forma padrão. Sendo assim:*

i) $H = \left[-A^T \,\vdots\, I_{n-k} \right]$ é uma matriz teste de paridade de $\mathcal{C}$;

ii) se H é uma matriz teste de paridade de $\mathcal{C}$, então $G \cdot H^T = 0$;

O próximo resultado fornece uma alternativa para se calcular a distância mínima de um código linear por intermédio da matriz teste de paridade.

Teorema 3.25. *Seja H a matriz teste de paridade de um código $\mathcal{C}$. A distância mínima de C é igual a d se, e só se, quaisquer $d-1$ colunas de H são linearmente independentes e existem d colunas de H linearmente dependentes.*

Exemplo 3.26. *Retomando o Exemplo 3.21, segue que a matriz teste de paridade que é obtida por meio de G', é dada por:*

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A 3ª coluna de H é nula. Sendo assim, de acordo com o Teorema 3.25, segue que a distância mínima do código gerado por G, que é equivalente ao código gerado por G', é igual a 1. Perceba que o exemplo 3.18, mostra que a palavra $(0,0,0,0,1,0)$ faz parte do código gerado por G.

3.2.3 Códigos Quase-Cíclicos

Nesta seção será apresentado o conceito de códigos *quase-cíclicos (ou QC-códigos)*. Tal classe de códigos lineares surge como uma generalização dos *códigos cíclicos* que, por sua vez, são interessantes do ponto de vista computacional pois possuem bons algoritmos de codificação e de decodificação [33, 45, 47, 55]. Além disso, os QC-códigos são parte fundamental do presente trabalho, uma vez que uma das contribuições do presente texto é justamente a determinação de uma família de QC-códigos binários com determinado tipo de propriedades.

Definição 3.27. *A aplicação:*

$$\begin{array}{rccc} \psi: & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (c_0,\ldots,c_{n-1}) & \mapsto & (c_{n-1},c_0,\ldots,c_{n-2}), \end{array} \tag{3.16}$$

*é denominada **desvio cíclico**.*

Tendo em vista o conceito apresentado na Definição 3.27, segue a definição de código quase-cíclico.

Definição 3.28. *Dado o corpo $\mathbb{F}_q$, seja $n = lm$ de modo que $l, m \in \mathbb{N}^*$. Um código linear $\mathcal{C} \subset \mathbb{F}_q^n$ é chamado de **código quase-cíclico de índice l** ou **l-QC-código** se $\mathcal{C}$ é invariante em relação à aplicação ψ^l, isto é, $\mathcal{C} = \psi^l(\mathcal{C})$. Quando $l = 1$, diz-se que $\mathcal{C}$ é um **código cíclico***

Seguindo na direção de obter informações sobre a matriz geradora de uma classe de QC-códigos, seja B a matriz quadrada, com entradas em $\mathbb{F}_q$, da forma:

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \dots & b_{m-2} & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \dots & b_{m-3} & b_{m-2} \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ b_1 & b_2 & b_3 & \dots & b_{m-1} & b_0 \end{bmatrix}. \tag{3.17}$$

Uma matriz da forma B na Eq. (3.17) é denominada *matriz circulante*. Uma classe de QC-códigos pode ser construída (levando-se em conta operações elementares sobre as linhas e permutação de colunas) por meio de matrizes circulantes. Neste caso, a matriz geradora G de um l-QC-código $\mathcal{C} \in \mathbb{F}_q^{lm}$ pode ser representada da seguinte forma:

$$G = \Big[B_0 \,\vdots\, B_1 \,\vdots\, \dots \,\vdots\, B_{l-1} \Big], \tag{3.18}$$

de maneira que cada B_i é uma matriz circulante de ordem m. Pode-se verificar, por exemplo, em [10, 13, 47] que a álgebra das matrizes circulantes de ordem m sobre um corpo $\mathbb{F}_q$ é isomorfa à álgebra dos polinômios no anel $R_m = \dfrac{\mathbb{F}_q[x]}{\langle x^m - 1 \rangle}$ se for considerado que uma matriz na forma apresentada na Eq. (3.17) está associada ao polinômio $\widehat{b}(x) = \displaystyle\sum_{i=0}^{m-1} b_i x^i$, em que os coeficientes de $\widehat{b}(x)$ são as entradas da primeira linha da matriz apresentada na Eq. (3.17). Nesse sentido, levando-se em conta a matriz 3.18, para cada $i \in \{0, \dots, l-1\}$ seja $\widehat{b}_i(x) \in R_m$ o polinômio associado à matriz B_i. Tais polinômios são chamados de *polinômios geradores do QC-código* $\mathcal{C} \in \mathbb{F}_q^{lm}$ e, nesta situação, usa-se a notação:

$$\mathfrak{b}(x) = (\widehat{b}_0(x), \widehat{b}_1(x), \dots, \widehat{b}_{l-1}(x)), \tag{3.19}$$

que é denominada de *gerador do QC-código* $\mathcal{C} \in \mathbb{F}_q^{lm}$. Um fato conhecido, e que pode ser verificado em [73], é que sendo $g(x)$ o polinômio dado por:

$$g(x) = mdc\left(\mathfrak{b}(x), x^m - 1\right) = mdc\left(\widehat{b}_0(x), \widehat{b}_1(x), \dots, \widehat{b}_{l-1}(x), x^m - 1\right), \tag{3.20}$$

tem-se que a dimensão k do QC-código $\mathcal{C}$ gerado por $\mathfrak{b}(x)$ (conforme 3.19) é igual ao grau do polinômio $h(x)$ dado por:

$$h(x) = \frac{x^m - 1}{g(x)}. \tag{3.21}$$

Exemplo 3.29. *Considere o código binário* $\mathcal{C} \subset \mathbb{F}_2^6$ *cuja matriz geradora* G *é dada por:*

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Assim $\mathcal{C}$ é um 2-QC-código. Para ficar mais fácil de visualizar que $\mathcal{C}$ possui índice 2, pode-se escrever G da seguinte forma:

$$G = \begin{bmatrix} 11 & 01 & 00 \\ 00 & 11 & 01 \\ 01 & 00 & 11 \end{bmatrix}.$$

Considerando que o comprimento do código $\mathcal{C}$ é $n = 6$ e sabendo que $l = 2$, pode-se obter um código equivalente a $\mathcal{C}$ cuja matriz geradora é uma formada por dois blocos de matrizes circulantes de ordem 3. Assim, através de uma permutação de colunas que resulte na coluna 2 ocupando o lugar da coluna 4, a coluna 3 ocupando o lugar da coluna 2, a coluna 4 no lugar da coluna 5, e a coluna 5 no lugar da coluna 3, segue que:

$$G' = \begin{bmatrix} 100 & 110 \\ 010 & 011 \\ 001 & 101 \end{bmatrix},$$

de modo que as matrizes circulantes são:

$$B_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ e } B_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Com isso, o gerador do 2-QC-código gerado por G' é dado por $\mathfrak{b}(x) = (1, 1 + x)$ o que resulta em:

$$h(x) = \frac{x^3 - 1}{mdc(x^3 - 1, \mathfrak{b}(x))} = x^3 - 1.$$

Portanto, a dimensão de $\mathcal{C}$ é $k = 3$.

CAPÍTULO 4

CÓDIGOS 2^r-QC BINÁRIOS VIA PEF $\mathbb{F}_{2^r}^2$

Este capítulo apresenta parte das contribuições originais deste trabalho e será divido em duas partes. Na primeira parte será desenvolvido o conceito de *plano Euclidiano finito* (PEF). A outra parte do capítulo tem como objetivo apresentar uma família de códigos binários, desenvolvidos a partir da noção de PEF, que possuem interessantes propriedades algébricas. A saber, o conceito de PEF foi inspirado nos trabalhos dados pelas referências [52, 69]. Nessas referências os autores trabalham com o conceito de *espaço Euclidiano finito n-dimensional* que surge na tentativa de simular as propriedades do espaço Euclidiano com o diferencial de que o corpo base para este espaço é um corpo finito. Nesse sentido, o PEF se apresenta como um tipo de espaço Euclidiano finito de dimensão 2.

4.1 O Plano Euclidiano Finito $\mathbb{F}_{2^r}^2$ (PEF $\mathbb{F}_{2^r}^2$)

Considere o corpo $\mathbb{F}_{2^r}$, representado da forma:

$$\mathbb{F}_{2^r} = \{0, 1, \alpha, \alpha^2, \cdots \alpha^{2^r-2}\}, \tag{4.1}$$

de modo que r seja um inteiro positivo e α seja um elemento primitivo de $\mathbb{F}_{2^r}$. Note que, a princípio, não é especificado qual é o polinômio irredutível $f(x) \in \mathbb{F}_2[x]$ está sendo considerado de forma que $f(\alpha) = 0$. Mas, todas as discussões feitas no capítulo 2 garantem que tal tipo de corpo existe e que $char(\mathbb{F}_{2^r}) = 2$.

4.1.1 Relação $\preceq$ em $\mathbb{F}_{2^r}$

Nesse momento, é introduzido um artifício que nos permite representar todos os elementos do corpo $\mathbb{F}_{2^r}$ como potências do elemento primitivo α. Isso será feito por intermédio da seguinte notação:

$$\alpha^* := 0. \tag{4.2}$$

Assim, a representação em (4.1) dá lugar a seguinte forma de apresentação dos elementos de $\mathbb{F}_{2^r}$:

$$\mathbb{F}_{2^r} = \{\alpha^* = 0, \alpha^0 = 1, \alpha^1, \alpha^2, \ldots, \alpha^{2^r-2}\}. \tag{4.3}$$

Então, ao se considerar a Eq. (4.3), percebe-se que existe uma bijeção entre os elementos de $\mathbb{F}_{2^r}$ e os elementos do conjunto que será denotado por $\mathcal{I}_r$ e que é dado por:

$$\mathcal{I}_r = \{*, 0, 1, 2, \ldots, 2^r - 2\}. \tag{4.4}$$

Além disso, a notação introduzida na Eq. (4.2), permite estabelecer em $\mathbb{F}_{2^r}$ uma relação conforme a definição a seguir.

Definição 4.1. *Dado $r \in \mathbb{N}^*$ considere o corpo finito $\mathbb{F}_{2^r}$ representado conforme a Eq. (4.3). Assim, define-se em $\mathbb{F}_{2^r}$ a **relação precede**, denotada por $\preceq$, de modo que para qualquer $i, j \in \mathcal{I}_r$, tem-se:*

$$\alpha^i \preceq \alpha^j \Leftrightarrow \begin{cases} i = * \ \textit{e} \ \ j \in \mathcal{I}_r; \\ \qquad \textit{ou} \\ i \leq j \ \ \textit{com} \ \ i, j \neq *. \end{cases} \tag{4.5}$$

Observe que a relação $\preceq$ dada na Definição 4.1 determina uma relação de ordem total em $\mathbb{F}_{2^r}$, conforme é mostrado no próximo lema.

Lema 4.2. *A relação $\preceq$ definida conforme a expressão (4.1) é uma relação de ordem total sobre $\mathbb{F}_{2^r}$.*

Demonstração: Para mostrar que $\preceq$ é reflexiva, considere $i \in \mathcal{I}_r$. Se $i = *$ então $\alpha^i \preceq \alpha^i$ é garantido por meio da primeira condição dada na expressão (4.5), e se $i \neq *$ então a reflexividade é garantida pela segunda condição. Agora, suponha que se tenha $\alpha^i \preceq \alpha^j$ e $\alpha^j \preceq \alpha^i$ para determinados $i, j \in \mathcal{I}_r$. Dessa forma, se $i = *$ então, pela primeira condição de 4.5, deve-se ter também $j = *$ e, com isso, $\alpha^i = \alpha^j$. Caso se tenha $i \neq *$ então, como estamos supondo que $\alpha^j \preceq \alpha^i$, segue que $j \neq *$. Assim, novamente pela segunda condição de 4.5, conclui-se que $i \leq j$ e $j \leq i$. Ou seja, $\alpha^i = \alpha^j$. Por fim, para mostrar a transitividade, basta observar que seguindo o que foi estabelecido na Definição 4.1 tem-se:

$$\alpha^* = 0 \preceq \alpha^0 = 1 \preceq \alpha^1 \preceq \alpha^2 \preceq \cdots \preceq \alpha^{2^r-2}.$$

□

Diante do que foi visto, o produto cartesiano $\mathbb{F}_{2^r}^2$ passa a ter a seguinte representação:

$$\mathbb{F}_{2^r}^2 = \{(\alpha^i, \alpha^j) \mid i, j \in \mathcal{I}_r\}. \tag{4.6}$$

Note que, uma vez determinado qual o elemento primitivo da representação (4.3), os pares ordenados de $\mathbb{F}_{2^r}^2$ ficam dependendo unicamente da escolha dos índices em $\mathcal{I}_r$. Por essa razão será adotada a seguinte notação em para os elementos de $\mathbb{F}_{2^r}^2$:

$$z_{ij} := (\alpha^i, \alpha^j), \text{ com } i, j \in \mathcal{I}_r. \tag{4.7}$$

Com isso, de agora em diante, fica estabelecido que, a menos de menções contrárias, todas as vezes que as notações $\mathbb{F}_{2^r}^2$ e z_{ij} forem usadas deve-se levar em conta todas os fatos vistos até este ponto do texto.

Assim, retomando as operações do corpo $\mathbb{F}_{2^r}$, induz-se uma adição e uma multiplicação por escalar em $\mathbb{F}_{2^r}^2$ conforme a definição que segue.

Definição 4.3. *Sejam $z_{ij} = (\alpha^i, \alpha^j)$ e $z_{st} = (\alpha^s, \alpha^t)$ pertencentes a $\mathbb{F}_{2^r}^2$ e $\alpha^m \in \mathbb{F}_{2^r}$. Dessa forma são definidas operações de **adição e de multiplicação por escalar em** $\mathbb{F}_{2^r}^r$ denotadas, respectivamente, por $\dot{+}$ e $\bullet$, de modo que:*

$$z_{ij} \dot{+} z_{st} := (\alpha^i + \alpha^s, \alpha^j + \alpha^t); \tag{4.8}$$

$$\alpha^m \bullet z_{ij} := (\alpha^m \alpha^i, \alpha^m \alpha^j). \tag{4.9}$$

Sendo assim, por meio da Definição 4.3, percebe-se que $\mathbb{F}_{2^r}^2$ tem uma estrutura de espaço vetorial de dimensão 2 sobre $\mathbb{F}_2$.

4.1.2 Distância e Norma em $\mathbb{F}_{2^r}^2$

A próxima definição introduzirá um conceito que foi utilizada em [52] e [69], e que constitui um objeto matemático similar à distância Euclidiana.

Definição 4.4. *A **distância de** $\mathbb{F}_{2^r}^2$, denotada por $d_{\mathbb{F}_{2^r}^2}$, é definida de modo que dados $z_{ij} = (\alpha^i, \alpha^j), z_{st} = (\alpha^s, \alpha^t) \in \mathbb{F}_{2^r}^2$, tem-se:*

$$d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}) = \left(\alpha^i + \alpha^j + \alpha^s + \alpha^t\right)^2. \tag{4.10}$$

Ao analisar a Definição 4.4, percebe-se que a distância $d_{\mathbb{F}_{2^r}^2}$ não é de fato uma métrica, basta observar por exemplo que $d_{\mathbb{F}_{2^r}^2}$ assume valores em $\mathbb{F}_{2^r}$. No entanto, tendo em vista as propriedades de uma métrica, constata-se que $d_{\mathbb{F}_{2^r}^2}$ possui algumas características interessantes. Tal fato se apresenta por meio da próxima proposição.

Proposição 4.5. *Para a distância $d_{\mathbb{F}_{2^r}^2}$ são válidas as seguintes propriedades:*

i) $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}) \succeq 0, \ \forall \ z_{ij}, z_{st} \in \mathbb{F}_{2^r}^2$.

ii) $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{ij}) = 0, \ \forall \ z_{ij} \in \mathbb{F}_{2^r}^2$.

iii) $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}) = d_{\mathbb{F}_{2^r}^2}(z_{st}, z_{ij}), \ \forall \ z_{ij}, z_{st} \in \mathbb{F}_{2^r}^2$.

iv) $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}) = d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{uv}) + d_{\mathbb{F}_{2^r}^2}(z_{uv}, z_{st}), \ \forall \ z_{ij}, z_{st}, z_{uv} \in \mathbb{F}_{2^r}^2$.

v) $d_{\mathbb{F}_{2^r}^2}(z_{ij} \dot{+} z_{uv}, z_{st} \dot{+} z_{uv}) = d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}),\ \forall\ z_{ij}, z_{st}, z_{uv} \in \mathbb{F}_{2^r}^2$.

Demonstração: Sejam $z_{ij}, z_{st}, z_{uv} \in \mathbb{F}_{2^r}^2$. i) Basta observar que $d_{\mathbb{F}_{2^r}^2}$ assume valores em $\mathbb{F}_{2^r}$ e considerar a ordem $\preceq$ estabelecida em $\mathbb{F}_{2^r}$. ii) De fato, pela Definição 4.4, tem-se $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{ij}) = (\alpha^i + \alpha^j + \alpha^i + \alpha^j)^2$. Como $char(\mathbb{F}_{2^r}) = 2$, segue que $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{ij}) = 0$. iii) Segue diretamente da comutatividade da operação $\dot{+}$ em $\mathbb{F}_{2^r}^2$. iv) Mais uma vez considere, a expressão (4.10) e tome um elemento $z_{uv} \in \mathbb{F}_{2^r}^2$. Dessa forma, do fato de que $char(\mathbb{F}_{2^r}) = 2$, tem-se $(\alpha^i + \alpha^j + \alpha^s + \alpha^t)^2 = (\alpha^i + \alpha^u + \alpha^u + \alpha^j + \alpha^s + \alpha^v + \alpha^v + \alpha^t)^2$. Isso mostra que $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}) = d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{uv}) + d_{\mathbb{F}_{2^r}^2}(z_{uv}, z_{st})$. v) Esta propriedade também segue diretamente iv). □

Observe que, em geral, não se pode dizer que $d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}) = 0$ implica em $z_{ij} = z_{st}$. Por exemplo, perceba que $d_{\mathbb{F}_{2^r}^2}(z_{i*}, z_{*i}) = 0$, para qualquer $i \in \mathcal{I}_r$. Outro ponto interessante é dado na propriedade iv), que tem como inspiração a desigualdade triangular de uma métrica.

Deste modo, tendo em vista as discussões feitas até então no presente capítulo, define-se o *plano Euclidiano Finito sobre* $\mathbb{F}_{2^r}$.

Definição 4.6. ***O plano Euclidiano Finito sobre*** $\mathbb{F}_{2^r}$*, denotado por* $\mathrm{PEF}\ \mathbb{F}_{2^r}^2$*, é definido como o produto cartesiano* $\mathbb{F}_{2^r}^2$ *munido com a distância* $d_{\mathbb{F}_{2^r}^2}$.

O conceito de distância em $\mathbb{F}_{2^r}^2$ é utilizado para definir um análogo à norma Euclidiana.

Definição 4.7. *A* ***norma*** *do* $\mathrm{PEF}\ \mathbb{F}_{2^r}^2$*, denotada por* $||\cdot||_{\mathbb{F}_{2^r}}$*, é definida para cada elemento de* $\mathbb{F}_{2^r}^2$ *de tal forma que:*

$$||z_{ij}||_{\mathbb{F}_{2^r}} = d_{\mathbb{F}_{2^r}^2}(z_{ij}, 0) = (\alpha^i + \alpha^j)^2. \tag{4.11}$$

Note que, pela Definição 4.7, $||z_{ij}||_{\mathbb{F}_{2^r}} \in \mathbb{F}_{2^r}$ para todo $z_{ij} \in \mathbb{F}_{2^r}^2$ O próximo resultado destaca duas propriedades que a norma do $\mathrm{PEF}\ \mathbb{F}_{2^r}$ possui.

Proposição 4.8. *Para a norma* $||\cdot||_{\mathbb{F}_{2^r}}$*, são válidas as seguintes propriedades:*

i) $||z_{ij}||_{\mathbb{F}_{2^r}} = 0 \Leftrightarrow i = j,\ \forall\ i, j \in \mathcal{I}_r$;

ii) $||z_{ij} \dot{+} z_{st}||_{\mathbb{F}_{2^r}} = ||z_{ij}||_{\mathbb{F}_{2^r}} + ||z_{st}||_{\mathbb{F}_{2^r}},\ \forall\ i, j, s, t \in \mathcal{I}_r$;

iii) $||z_{ij}||_{\mathbb{F}_{2^r}} = ||z_{in}||_{\mathbb{F}_{2^r}} + ||z_{nj}||_{\mathbb{F}_{2^r}},\ \forall\ i, j, n \in \mathcal{I}_r$.

Demonstração: $i)$ Suponha que $||z_{ij}||_{\mathbb{F}_{2^r}} = 0$ para determinado $z_{ij} \in \mathbb{F}_{2^r}^2$. Assim, de acordo com (4.11), segue que $d_{\mathbb{F}_{2^r}^2}(z_{ij}, 0) = 0 \Leftrightarrow (\alpha^i + \alpha^j)^2 = 0$. Como $\mathbb{F}_{2^r}^2$ é um corpo com $char(\mathbb{F}_{2^r}) = 2$, segue que $\alpha^i + \alpha^j = 0$ implicando em $\alpha^i = \alpha^j$. Nessa situação, como os elementos de $\mathbb{F}_{2^r}$ estão em bijeção com o conjunto de índices $\mathcal{I}_r$, segue o resultado. $ii)$ Pela definição tem-se que $||z_{ij} \dot{+} z_{st}||_{\mathbb{F}_{2^r}} = d_{\mathbb{F}_{2^r}^2}(z_{ij} \dot{+} z_{st}, 0) = 0$. Através das propriedades $iii), iv)$ e $v)$ da proposição 4.5, chega-se em $d_{\mathbb{F}_{2^r}^2}(z_{ij} \dot{+} z_{st}, z_{st} \dot{+} z_{st}) = d_{\mathbb{F}_{2^r}^2}(z_{ij}, z_{st}) = d_{\mathbb{F}_{2^r}^2}(z_{ij}, 0) + d_{\mathbb{F}_{2^r}^2}(z_{st}, 0)$, que por definição prova a igualdade. $iii)$

Pela definição, segue que $||z_{ij}||_{\mathbb{F}_{2^r}} = d_{\mathbb{F}_{2^r}^2}(z_{ij}, 0) = (\alpha^i + \alpha^j)^2$. Dessa forma, como $char(\mathbb{F}_{2^r}^2) = 2$, segue que $(\alpha^i + \alpha^j)^2 = (\alpha^i + \alpha^n + \alpha^n + \alpha^j)^2 = (\alpha^i + \alpha^n)^2 + (\alpha^n + \alpha^j)^2$, para qualquer $n \in \mathcal{I}_r$. □

Em relação ao Item $i)$ da Proposição 4.8, evidentemente se for considerado que $i, j \in \mathbb{N}$ então a igualdade $||z_{ij}||_{\mathbb{F}_{2^r}} = 0$ irá acontecer se, e somente se, $i \equiv j \mod 2^r - 1$. No entanto, sempre será considerado que os expoentes dos elementos de $\mathbb{F}_{2^r}$ pertencem a $\mathcal{I}_r$.

Com isso, se encerra a primeira parte deste capítulo onde foram introduzidas as ferramentas básicas em relação ao PEF $\mathbb{F}_{2^r}$. E as aplicações dos conceitos vistos aqui serão exploradas na próxima seção.

4.2 Códigos 2^r-QC Binários via PEF $\mathbb{F}_{2^r}^2$

Nesta seção será mostrado como aplicar os conceitos relacionados ao PEF $\mathbb{F}_{2^r}^2$ para obtenção de uma família de códigos binários quase-cíclicos com propriedades algébricas interessantes do ponto de vista da teoria da informação quântica.

4.2.1 Matriz Norma

Levando-se em conta todas as questões referentes ao conceito de PEF $\mathbb{F}_{2^r}^2$ que foram feitas até o momento, dado um índice $i \in \mathcal{I}_r$ defina as listas $\mathcal{Z}_i$ da seguinte forma:

$$\mathcal{Z}_i = (z_{i*}, z_{i0}, z_{i1}, \ldots, z_{i(2^r-2)}). \tag{4.12}$$

Com estas listas constrói-se uma matriz, denotada por Υ_r, conforme as instruções que seguem. A primeira linha de Υ_r, denotada por L_0, é obtida considerando as listas $\mathcal{Z}_i$ ordenadas da seguinte forma:

$$L_0 = \Big(\mathcal{Z}_* \,\vdots\, \mathcal{Z}_0 \,\vdots\, \mathcal{Z}_1 \,\vdots\, \ldots \,\vdots\, \mathcal{Z}_{2^r-2}\Big). \tag{4.13}$$

As próximas $2^r - 1$ linhas são obtidas por meio de um deslocamento para à direita das listas $\mathcal{Z}_i$ da linha anterior. Assim, a partir de (4.13), temos:

$$L_1 = \Big(\mathcal{Z}_{2^r-2} \,\vdots\, \mathcal{Z}_* \,\vdots\, \mathcal{Z}_0 \,\vdots\, \ldots \,\vdots\, \mathcal{Z}_{2^r-3}\Big)$$

$$L_2 = \Big(\mathcal{Z}_{2^r-3} \,\vdots\, \mathcal{Z}_{2^r-2} \,\vdots\, \mathcal{Z}_* \,\vdots\, \ldots \,\vdots\, \mathcal{Z}_{2^r-4}\Big)$$

$$\vdots$$

$$L_{2^r-1} = \Big(\mathcal{Z}_0 \,\vdots\, \mathcal{Z}_1 \,\vdots\, \mathcal{Z}_2 \,\vdots\, \ldots \,\vdots\, \mathcal{Z}_*\Big)$$

Portanto, a matriz Υ_r é dada por:

$$\Upsilon_r = \left[\begin{array}{c|c|c|c|c|c} \mathcal{Z}_* & \mathcal{Z}_0 & \mathcal{Z}_1 & \mathcal{Z}_2 & \cdots & \mathcal{Z}_{2^r-2} \\ \hline \mathcal{Z}_{2^r-2} & \mathcal{Z}_* & \mathcal{Z}_0 & \mathcal{Z}_1 & \cdots & \mathcal{Z}_{2^r-3} \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline \mathcal{Z}_0 & \mathcal{Z}_1 & \mathcal{Z}_2 & \mathcal{Z}_3 & \cdots & \mathcal{Z}_* \end{array}\right] \tag{4.14}$$

Com isso nota-se que a matriz Υ_r possui como entradas elementos do PEF $\mathbf{F}_{2^r}^2$. Antes de prosseguir, defina sobre o conjunto $\mathcal{I}_r$ um operador de desvio cíclico similar ao que foi feito na Definição 3.27, denotado por $\tilde{\psi}$, da seguinte forma:

$$\begin{aligned} &\tilde{\psi} : \mathcal{I}_r \longrightarrow \mathcal{I}_r \\ &\qquad x \longrightarrow \begin{cases} 0, & \text{se } x = *, \\ x+1, & \text{se } 0 \leq x \leq 2^r - 3, \\ *, & \text{se } x = 2^r - 2. \end{cases} \end{aligned} \tag{4.15}$$

Ainda em relação ao operador $\tilde{\psi}$, assume-se que $\tilde{\psi}^0$ representa aplicação identidade definida sobre $\mathcal{I}_r$. Com isso, tem-se que Υ_r é uma matriz $2^r \times 2^{2r}$, e tal fato permite dividir Υ_r em 2^r blocos de submatrizes quadradas de ordem 2^r cada, denotadas por $(\Upsilon_r)_i$, com $1 \leq i \leq 2^r$. Para cada $1 \leq i \leq 2^r$, a matriz $(\Upsilon_r)_i$ tem a seguinte forma:

$$(\Upsilon_r)_i = \begin{bmatrix} \mathcal{Z}_{\tilde{\psi}^{i-1}(*)} \\ \mathcal{Z}_{\tilde{\psi}^{i-1}(2^r-2)} \\ \vdots \\ \mathcal{Z}_{\tilde{\psi}^{i-1}(1)} \\ \mathcal{Z}_{\tilde{\psi}^{i-1}(0)} \end{bmatrix}. \tag{4.16}$$

Com isso a matriz Υ_r pode ser representada da seguinte forma:

$$\Upsilon_r = \left[(\Upsilon_r)_1 \,\middle|\, (\Upsilon_r)_2 \,\middle|\, \cdots \,\middle|\, (\Upsilon_r)_{2^r}\right] \tag{4.17}$$

A seguir, segue um teorema que relaciona a Υ_r com as matrizes circulantes.

Teorema 4.9. *Dada a matriz Υ_r definida em (4.14), para cada $k \in \mathbb{Z}$ com $1 \leq k \leq 2^r$, seja $\mathcal{Y}_k$ a matriz quadrada de ordem 2^r obtida tomando-se em Υ_r a k-ésima coluna seguida, respectivamente, das colunas $k + 2^r m$ de Υ_r, com $m \in \mathbb{Z}$ e $1 \leq m \leq 2^r - 1$. Dessa forma, tem-se que $\mathcal{Y}_k$ é uma matriz circulante.*

Demonstração: Primeiramente, considere a reindexação dada por $\phi : \mathcal{I}_r \to \{1, 2, 3, \ldots, 2^r\}$, em que:

$$\phi(x) = \begin{cases} 1, & \text{se } x = *, \\ x+2, & \text{se } 0 \leq x \leq 2^r - 2. \end{cases}$$

Assim, ϕ determina uma bijeção entre $\mathcal{I}_r$ e $\{1, 2, 3, \cdots, 2^r\}$. Com essa reindexação a lista $\mathcal{Z}_i$ definida em (4.12), fica associada à lista $\hat{\mathcal{Z}}_i$ de modo que $\hat{\mathcal{Z}}_i = (\hat{z}_{i\phi(*)}, \hat{z}_{i\phi(0)}, \hat{z}_{i\phi(1)}, \ldots \hat{z}_{i\phi(2^r-2)}) = (\hat{z}_{i1}, \hat{z}_{i2}, \hat{z}_{i3}, \ldots \hat{z}_{i(2^r)})$. Desta forma, a matriz Υ_r pode ser vista como uma matriz $\hat{\Upsilon}_r$ dada por:

$$\hat{\Upsilon}_r = \begin{bmatrix} \hat{\mathcal{Z}}_* & \hat{\mathcal{Z}}_0 & \hat{\mathcal{Z}}_1 & \hat{\mathcal{Z}}_2 & \cdots & \hat{\mathcal{Z}}_{2^r-2} \\ \hat{\mathcal{Z}}_{2^r-2} & \hat{\mathcal{Z}}_* & \hat{\mathcal{Z}}_0 & \hat{\mathcal{Z}}_1 & \cdots & \hat{\mathcal{Z}}_{2^r-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hat{\mathcal{Z}}_0 & \hat{\mathcal{Z}}_1 & \hat{\mathcal{Z}}_2 & \hat{\mathcal{Z}}_3 & \cdots & \hat{\mathcal{Z}}_* \end{bmatrix}.$$

Note que a distinção entre $\hat{\Upsilon}_r$ e Υ_r é feita apenas na reindexação dada por ϕ. Dessa forma, considere uma representação de $\hat{\Upsilon}_r$ semelhante à representação de Υ_r dada em (4.17). Com isso, para cada $k \in \mathbb{Z}$ com $1 \leq k \leq 2^r$, obtém-se uma matriz $\hat{\mathcal{Y}}_k$ conforme as instruções que seguem. Fixe a $k-$ésima coluna do bloco $\left(\hat{\Upsilon}_r\right)_1$ que será a primeira coluna de $\hat{\mathcal{Y}}_k$. A segunda coluna de $\hat{\mathcal{Y}}_k$ será dada pela coluna que ocupa a $k-$ésima posição no segundo bloco $\left(\hat{\Upsilon}_r\right)_2$ que, no caso, é a $k + 2^r$-ésima coluna da matriz $\hat{\Upsilon}_r$. Prosseguindo dessa maneira, a matriz $\hat{\mathcal{Y}}_k$ será uma matriz quadrada de ordem 2^r, cuja primeira coluna é a $k-$ésima coluna de $\hat{\Upsilon}_r$ e as demais $2^r - 1$ colunas correspondem às colunas que ocupam, em suas respectivas ordens, as posições $k + 2^r m$, onde $1 \leq m \leq 2^r - 1$, em relação à matriz $\hat{\Upsilon}_r$. Note que a matriz $\hat{\mathcal{Y}}_k$ é circulante, pois, de acordo com o processo de construção descrito, sua forma é dada por:

$$\hat{\mathcal{Y}}_k = \begin{bmatrix} \hat{z}_{*k} & \hat{z}_{0k} & \hat{z}_{1k} & \hat{z}_{2k} & \cdots & \hat{z}_{(2^r-2)k} \\ \hat{z}_{(2^r-2)k} & \hat{z}_{*k} & \hat{z}_{0k} & \hat{z}_{1k} & \cdots & \hat{z}_{(2^r-3)k} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hat{z}_{0k} & \hat{z}_{1k} & \hat{z}_{2k} & \hat{z}_{3k} & \cdots & \hat{z}_{*k} \end{bmatrix}.$$

Com isso a matriz $\hat{\mathcal{Y}}_k$ possui o mesmo formato da matriz dada em (3.17). Por fim, basta reverter a reindexação ϕ para se obter uma matriz $\mathcal{Y}_k$ que satisfaz as condições dadas pelo enunciado. □

A próxima definição mostra como utilizar Υ_r e a norma $||\cdot||_{\mathbb{F}_{2^r}}$ para obter matrizes binárias.

Definição 4.10. *Fixe dois parâmetros $u, v \in \mathcal{I}_r$. A* ***matriz norma-***(uv) ***de*** Υ_r*, denotada*

por $N(uv)$, é a matriz obtida através de Υ_r por meio da seguinte regra:

$$z_{ij} \xrightarrow{\textit{substituído em}\,\Upsilon_r} \begin{cases} 1, & \textit{se } ||z_{ij}||_{\mathbb{F}_{2^r}} = \alpha^u \textit{ ou } ||z_{ij}||_{\mathbb{F}_{2^r}} = \alpha^v; \\ 0, & \textit{caso contrário } . \end{cases} \tag{4.18}$$

Exemplo 4.11. *Para $r = 2$ tem-se o corpo $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ de modo que α seja a raiz do polinômio $f(x) = x^2 + x + 1$. Isto é, $\alpha^2 = \alpha + 1$. Assim, a matriz Υ_2, é dada por:*

$$\Upsilon_2 = \begin{bmatrix} z_{**} & z_{*0} & z_{*1} & z_{*2} & z_{0*} & z_{00} & z_{01} & z_{02} & z_{1*} & z_{10} & z_{11} & z_{12} & z_{2*} & z_{20} & z_{21} & z_{22} \\ z_{2*} & z_{20} & z_{21} & z_{22} & z_{**} & z_{*0} & z_{*1} & z_{*2} & z_{0*} & z_{00} & z_{01} & z_{02} & z_{1*} & z_{10} & z_{11} & z_{12} \\ z_{1*} & z_{10} & z_{11} & z_{12} & z_{2*} & z_{20} & z_{21} & z_{22} & z_{**} & z_{*0} & z_{*1} & z_{*2} & z_{0*} & z_{00} & z_{01} & z_{02} \\ z_{0*} & z_{00} & z_{01} & z_{02} & z_{1*} & z_{10} & z_{11} & z_{12} & z_{2*} & z_{20} & z_{21} & z_{22} & z_{**} & z_{*0} & z_{*1} & z_{*2} \end{bmatrix} \tag{4.19}$$

Agora, considere a Tabela 4.1, na qual foram calculadas a norma de todos os elementos de PEF $\mathbb{F}_4^2$.

Tabela 4.1: *Normas dos elementos do PEF $\mathbb{F}_4^2$.*

$\|\|z_{**}\|\|_{\mathbb{F}_4} = 0$	$\|\|z_{*0}\|\|_{\mathbb{F}_4} = 1$	$\|\|z_{*1}\|\|_{\mathbb{F}_4} = \alpha^2$	$\|\|z_{*2}\|\|_{\mathbb{F}_4} = \alpha$
$\|\|z_{0*}\|\|_{\mathbb{F}_4} = 1$	$\|\|z_{00}\|\|_{\mathbb{F}_4} = 0$	$\|\|z_{01}\|\|_{\mathbb{F}_4} = \alpha$	$\|\|z_{02}\|\|_{\mathbb{F}_4} = \alpha^2$
$\|\|z_{1*}\|\|_{\mathbb{F}_4} = \alpha^2$	$\|\|z_{10}\|\|_{\mathbb{F}_4} = \alpha$	$\|\|z_{11}\|\|_{\mathbb{F}_4} = 0$	$\|\|z_{12}\|\|_{\mathbb{F}_4} = 1$
$\|\|z_{2*}\|\|_{\mathbb{F}_4} = \alpha$	$\|\|z_{20}\|\|_{\mathbb{F}_4} = \alpha^2$	$\|\|z_{21}\|\|_{\mathbb{F}_4} = 1$	$\|\|z_{22}\|\|_{\mathbb{F}_4} = 0$

Assim, de acordo com a Tabela 4.1 e a Definição 4.10 tem-se, por exemplo as matrizes $N(**), N(12)$ e $N(01)$, conforme (4.20), (4.21) e (4.22), respectivamente.

$$N(**) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \tag{4.20}$$

$$N(12) = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \tag{4.21}$$

$$N(01) = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{4.22}$$

Observe que, de acordo com a Definição 4.10, tem-se de imediato o próximo corolário.

Corolário 4.12. *Dados os parâmetros $u, v \in \mathcal{I}_r$, tem-se que $N(uv) = N(vu)$.*

Tendo em vista o resultado 4.12, e levando-se em conta que o total de combinações que podem ser feitas tomando dois parâmetros em $\mathcal{I}_r$, segue que o número de matrizes distintas do tipo $N(uv)$ é dado por $2^{r-1}(2^r + 1)$. Utilizando o Item 2 do Teorema 2.7 e o Lema 3.16, é possível verificar o próximo resultado que mostra que matrizes $N(uv)$ não possuem linhas e nem colunas nulas. É crucial destacar que o teorema em questão foi concebido de maneira inteiramente original pelo autor, representando, assim, uma contribuição inédita deste trabalho.

Teorema 4.13. *Dados $u, v \in \mathcal{I}_r$ considere a matriz norma $N(uv)$. Com isso, segue que:*

i) Se $u = v$, então o peso de cada linha de $N(uv)$ é igual a 2^r. Caso contrário, o peso de Hamming de cada linha é 2^{r+1}.

ii) Se $u = v$, então o peso de Hamming de cada coluna de $N(uv)$ é igual a 1. Caso contrário, o peso de cada coluna é 2.

Demonstração: $i)$ Dados $u, v \in \mathcal{I}_r$, de acordo com a Definição 4.10, deve-se verificar o número de soluções das equações dadas por:

$$||z_{ij}||_{\mathbb{F}_{2^r}} = \alpha^u \text{ e } ||z_{ij}||_{\mathbb{F}_{2^r}} = \alpha^v. \tag{4.23}$$

Considerando que $x = \alpha^i$ e $y = \alpha^j$, as equações em (4.23) recaem em uma equação da forma:

$$x^2 + y^2 = c, \tag{4.24}$$

em que $c \in \mathbb{F}_{2^r}$. Se $c = 0$, segue que a Eq. (4.24) terá como solução 2^r elementos da forma (α^l, α^l). Caso contrário, $c \neq 0$, a Eq. (4.24) é equivalente a

$$\hat{x}^2 + \hat{y}^2 = 1. \tag{4.25}$$

Neste caso, para obter a Eq. (4.25) basta dividir ambos os lados da Eq. (4.24) por c e considerar o fato de que todos os elementos de $\mathbb{F}_{2^r}$ podem ser representados como quadrados de elementos de $\mathbb{F}_{2^r}$. Neste caso, de acordo com o Lema 2.7, a Eq. (4.25) também possui 2^r soluções. Logo, quando $u = v$ as Equações (4.23) são iguais e segue que o peso de cada linha, nesse caso será 2^r. Quando $u \neq v$, os conjuntos de soluções das Equações (4.23) são disjuntos. Portanto, o peso de cada linha para o caso $u \neq v$ é $2^r + 2^r = 2^{r+1}$. $ii)$ O raciocínio é análogo ao que foi feito para demonstrar $i)$. Considere z_{il} um elemento de uma coluna qualquer de Υ_r. Segue que $z_{il} = (\alpha^i, \alpha^l)$. Dessa forma, considerando por exemplo o parâmetro u, tem-se que $||z_{il}||_{\mathbb{F}_{2^r}} = \alpha^u$, é equivalente a:

$$(\alpha^i)^2 = c. \tag{4.26}$$

Observe que na Eq. (4.26) está sendo considerado que $\alpha^u + (\alpha^l)^2 = c \in \mathbb{F}_{2^r}$. Assim, levando-se em conta que apenas $x = \alpha^i$ está variando, obtém-se de (4.26) uma equação de grau 2 equivalente à expressão dada por:

$$x^2 = c. \tag{4.27}$$

Para resolver a Eq. (4.27), note que a aplicação quadrática $t \mapsto t^2$ é um $\mathbb{F}_{2^r}$-monomorfismo de $\mathbb{F}_{2^r}$ e, portanto, um automorfismo, pois $\mathbb{F}_{2^r}$ é finito. Assim, segue que $x^2 = c$ tem uma única raiz em $\mathbb{F}_{2^r}$. Isso prova o resultado. □

A princípio as matrizes norma $N(uv)$ não podem ser consideradas como matrizes geradoras de códigos, uma vez que nem sempre suas linhas formam um conjunto linearmente independente. Como exemplo de tal fato, considere a matriz $N(01)$ apresentada no Exemplo 4.11. Entretanto, conforme o comentário que segue logo após a Definição 3.17, será feito um abuso de notação para convencionar que a notação

$$\mathcal{C}(uv) \tag{4.28}$$

representa um código que é gerado por uma matriz obtida a partir de $N(uv)$ ao retirarmos as linhas que causam a dependência linear. Nesse sentido, será feito também um abuso de linguagem para dizer que os códigos $\mathcal{C}(uv)$ são códigos *gerados* pelas matrizes $N(uv)$. Com tal fato em mente, apresenta-se o próximo resultado que diz respeito a distância mínima de tais códigos, e que também é mais uma contribuição original do autor.

Teorema 4.14. *Considerando o código $\mathcal{C}(uv)$ gerado pela matriz norma $N(uv)$, segue que:*

$$d_H\left(\mathcal{C}(uv)\right) = \begin{cases} 2^r, & \textit{se } u = v \\ 2^{r+1}, & \textit{se } u \neq v \end{cases}. \tag{4.29}$$

Demonstração: Suponha que $u = v$. Nesse caso o peso de cada linha de $N(uu)$ é igual a 2^r. Com isso, segue que $d_H\left(\mathcal{C}(uu)\right) \leq 2^r$. De (4.17) tem-se:

$$N(uu) = \Big[N(uu)_1 \,\vdots\, N(uu)_2 \,\vdots\, \cdots \,\vdots\, N(uu)_{2^r}\Big], \tag{4.30}$$

em que cada $N(uu)_i$ é uma matriz quadrada de ordem 2^r cujo peso de cada linha e cada coluna é igual a 1. Assim, considerando que para cada $i \in \{1, \ldots, 2^r\}$ a notação $d_H\left(N(uu)_i\right)$ representa a distância mínima do espaço gerado pelas linhas de $N(uu)_i$, segue que:

$$d_H\left(\mathcal{C}(uu)\right) \geq \sum_{i=1}^{2^r} d_H\left(N(uu)_i\right) \geq \sum_{i=1}^{2^r} 1 = 2^r. \tag{4.31}$$

O caso em que $u \neq v$ segue de forma análoga com a ressalva que o peso de cada linha e cada coluna de $N(uv)_i$ é igual a 2 e que, pelo lema 3.16, os elementos do espaço gerado pelas linhas de $N(uv)_i$ tem peso par. □

O Teorema 4.13, mostra que as matrizes $N(uv)$ possuem característica distintas a depender da forma como os parâmetros $u, v \in \mathcal{I}_r$ são tomados. Nesse sentido, será realizado um estudo que busca relacionar os parâmetros com tais características.

4.2.2 Códigos $\mathcal{C}(uv)$ para $u = v$

Nessa seção serão consideradas às matrizes norma da forma $N(uu)$, com $u \in \mathcal{I}_r$. Assim, para tais matrizes, apresentam-se mais contribuições originais do presente trabalho na forma dos seguintes resultados.

Teorema 4.15. *As linhas de $N(uu)$ são linearmente independentes.*

Demonstração: Como $N(uu)$ possui 2^r linhas segue que $rank\,(N(uu)) \leq 2^r$. Agora, suponha que $rank\,(N(uu)) = \delta$ seja estritamente menor que 2^r. Assim, para cada $1 \leq i \leq 2^r$, considere as linhas de $N(uu)$ como vetores da forma $L_i = (a_{i1}, a_{i2}, \ldots, a_{i2^{2r}})$. Conforme a hipótese feita em relação a $rank\,(N(uu))$, seja $\mathcal{L} = \{L_1, L_2, \ldots, L_\delta\}$ o conjunto formado por δ linhas linearmente independentes de $N(uu)$. Então, existe uma linha L_s em $N(uu)$ tal que:

$$L_s = \lambda_1 L_1 + \lambda_2 L_2 + \cdots + \lambda_\delta L_\delta, \tag{4.32}$$

em que $\lambda_i \in \mathbb{F}_{2^r}$ e $1 \leq i \leq \delta$. Por outro lado, o Teorema 4.13 mostra que o peso de cada linha é igual a 2^r. Então, seja a_{st}, com $1 \leq t \leq 2^{2r}$, uma das entradas não nulas de L_s. Levando em conta a combinação linear dada pela Eq. (4.32), segue que:

$$a_{st} = \lambda_1 a_{1t} + \lambda_2 a_{2t} + \cdots + \lambda_\delta a_{\delta t}. \tag{4.33}$$

Observe que as entradas $a_{st}, a_{1t}, a_{2t}, \ldots, a_{\delta t}$ fazem parte de uma das colunas de $N(uu)$. No entanto, o Teorema 4.13 garante que cada coluna de $N(uu)$ tem um peso igual a 1. Então, como é assumido que a_{st} é um elemento não nulo, segue que $a_{1t} = a_{2t} = \cdots = a_{\delta t} = 0$. Ou seja, a Eq. (4.33) leva a $1 = 0$, o que é um absurdo. Portanto, $rank\,(N(uu)) = 2^r$. □

Sendo assim, as constatações dos Teoremas 4.15 e 4.14 justificam o próximo resultado que caracterizam os códigos $\mathcal{C}(uu)$ por meio dos parâmetros.

Corolário 4.16. *As matrizes norma da forma $N(uu)$ geram 2^r-QC-códigos cujos parâmetros são $[2^{2r}, 2^r, 2^r]_2$.*

4.2.3 Códigos $\mathcal{C}(uv)$ para $u \neq v$

Agora considere as matrizes norma da forna $N(uv)$, com a condição $u \neq v$ sendo $u, v \in \mathcal{I}_r$. Note que o Teorema 4.14 determina qual é a distância mínima para os códigos $\mathcal{C}(uv)$. Sendo assim, resta realizar um estudo relacionado à dimensão dos códigos $\mathcal{C}(uv)$, com $u \neq v$ para que todos os parâmetros fiquem determinados. Primeiramente, considere o seguinte resultado que pode ser verificado em [61].

Proposição 4.17. *Seja G uma matriz circulante de ordem n definida sobre $\mathbb{F}_2$ cujo peso é par, isto é o peso de Hamming de cada linha é um número par. Dessa forma, a soma das i-ésimas linhas para $i = 1, \ldots, n-1$ é equivalente a n-ésima linha.*

Assim, considerando a Proposição 4.17 combinado com os Teoremas 4.9 e 4.13, chega-se ao próximo resultado.

Corolário 4.18. *Dados $u, v \in \mathcal{I}_r$ com $u \neq v$ têm-se que $rank(N(uv)) \leq 2^r - 1$. E tal fato equivale a $\dim(\mathcal{C}(uv)) \leq 2^r - 1$.*

A título de informação as Tabelas 4.2 e 4.3 mostram a dimensão do código $\mathcal{C}(uv)$ para $r = 2$ e $r = 3$, respectivamente.

Tabela 4.2: *Dimensão dos códigos $\mathcal{C}(uv)$, para $u \neq v$ e $r = 2$.*

$\dim(N(uv))$	$*$	0	1	2
$*$	4	3	3	2
0	3	4	2	3
1	3	2	4	3
2	2	3	3	4

Tabela 4.3: *Dimensão dos códigos $\mathcal{C}(uv)$, para $u \neq v$ e $r = 3$.*

$\dim(N(uv))$	$*$	0	1	2	3	4	5	6
$*$	8	7	7	7	7	7	7	7
0	7	8	7	7	7	7	7	7
1	7	7	8	7	7	7	7	7
2	7	7	7	8	7	7	7	7
3	7	7	7	7	8	7	7	7
4	7	7	7	7	7	8	7	7
5	7	7	7	7	7	7	8	7
6	7	7	7	7	7	7	7	8

4.2.4 Ortogonalidade dos códigos $\mathcal{C}(uv)$

Nesta seção será dado prosseguimento ao estudo relacionado às características envolvendo os parâmetros $u, v \in \mathcal{I}_r$ dos códigos $\mathcal{C}(uv)$, dando ênfase à um dos tópicos da teoria de códigos corretores de erros que trada de *códigos duais*. Perceba que os códigos $\mathcal{C}(uv)$ são subespaços vetoriais de $\mathbb{F}_2^{2^{2r}}$. Sendo assim, além do produto *interno Euclidiano*, pode-se definir em $\mathbb{F}_2^{2^{2r}}$ o produto *interno simplético*. As definições de tais conceitos são apresentadas a seguir.

Definição 4.19. *Dados $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ o produto interno Euclidiano entre x e y é dado por*

$$\langle x, y \rangle_E = \sum_{i=1}^{n} x_i y_i. \tag{4.34}$$

Com isso, dado um código linear $\mathcal{C} \subset \mathbb{F}_q^n$, o conjunto dado por

$$\mathcal{C}^{\perp_E} = \{x \in \mathbb{F}_q^n \ : \ \langle x, y \rangle_E = 0, \ \forall \, y \in \mathcal{C}\}, \tag{4.35}$$

*é chamado de **código dual Euclidiano** de $\mathcal{C}$. Quando temos $\mathcal{C} \subseteq \mathcal{C}^{\perp_E}$, dizemos que o código $\mathcal{C}$ é **auto-ortogonal Euclidiano.***

O produto interno simplético será definido por meio do produto interno Euclidiano. Para isso, consideremos a notação notação $(x|y)$, que representará o vetor dado pela justaposição de vetores x e y. Dessa forma:

Definição 4.20. *Sejam $x = (x_1|x_2), y = (y_1|y_2) \in \mathbb{F}_q^{2n}$, em que x_1, x_2, y_1 e y_2 pertencem a $\mathbb{F}_q^n$, o **produto interno simplético** entre x e y é dado por:*

$$\langle x, y \rangle_s = x \Omega_n y^T = \langle x_1, y_2 \rangle_E - \langle x_2, y_1 \rangle_E, \tag{4.36}$$

de modo que :

$$\Omega_n = \left[\begin{array}{c:c} 0 & I_n \\ \hdashline -I_n & 0 \end{array}\right]. \tag{4.37}$$

*De maneira análoga ao caso Euclidiano, dado um código linear $\mathcal{C} \subset \mathbb{F}_q^{2n}$, define-se o **código dual simplético** de $\mathcal{C}$, denotado por $\mathcal{C}^{\perp_s}$, de forma que:*

$$\mathcal{C}^{\perp_s} = \{x \in \mathbb{F}_q^{2n} \ : \ \langle x, y \rangle_s = 0, \ \forall \, y \in \mathcal{C}\}. \tag{4.38}$$

*Assim, o código $\mathcal{C}$ é **auto-ortogonal simplético** quando $\mathcal{C} \subseteq \mathcal{C}^{\perp_s}$.*

Considere $\mathcal{C} \subset \mathbb{F}_2^{2n}$ um código de dimensão k. Seguindo uma linha de raciocínio daquela que foi utilizada na Definição 3.15, por meio do método de eliminação gaussiana, combinada com permutação de colunas, é possível representar a matriz geradora de $\mathcal{C}$ da seguinte forma:

$$G = \left[\begin{array}{c:c:c} I_k & A & B \end{array}\right], \tag{4.39}$$

sendo que A é uma matriz de ordem $k \times (n-k)$ e B é uma matriz de ordem $k \times n$. Quando uma matriz estiver na forma dada pela Eq. (4.39), diz-se que ela se encontra na *forma padrão simplética*. No que se diz respeito à ortogonalidade envolvendo os produtos internos no caso Euclidiano e no caso simplético para códigos binários será enunciado o próximo lema que é um compilado de resultados conhecidos que podem ser verificados nas referências [37, 46, 72].

Lema 4.21. *Sejam $\mathcal{C}_1 \subset \mathbb{F}_2^n$ e $\mathcal{C}_2 \subset \mathbb{F}_2^{2n}$ códigos lineares, ambos de dimensão k. Suponha ainda que G_1 e G_2 sejam as matrizes geradoras de $\mathcal{C}_1$ e $\mathcal{C}_2$, respectivamente. Sendo assim, segue que:*

i) $\mathcal{C}_1$ *é auto-ortogonal Euclidiano se, e somente, se* $G_1 \cdot G_1^T = 0$.

ii) $\mathcal{C}_2$ *é auto-ortogonal simplético se, e somente, se* $G_2 \cdot \Omega_n \cdot G_2^T = 0$.

iii) $\dim(\mathcal{C}_1^{\perp_E}) = n - k$ *e* $\dim(\mathcal{C}_2^{\perp_s}) = 2n - k$.

iv) Se $G_1 = \left[I_k \,\middle\vdots\, A_{k\times(n-k)} \right]$, *então a matriz* $H_E = \left[-A^T \,\middle\vdots\, I_{n-k} \right]$ *é a matriz geradora de* $\mathcal{C}_1^{\perp_E}$.

v) Se $G_2 = \left[I_k \,\middle\vdots\, B_{k\times(n-k)} \,\middle\vdots\, C_{k\times n} \right]$, *então a matriz* $H_s = \left[\begin{array}{c:c:c} 0 & B_{k\times(n-k)}^T & I_{n-k} \\ \hdashline I_n & C_{k\times n}^T & 0 \end{array}\right]$ *é a matriz geradora de* $\mathcal{C}_2^{\perp_s}$.

A próxima contribuição original deste trabalho se apresenta na forma de um resultado que permitirá estabelecer qual é a relação dos código $\mathcal{C}(uv)$ com a ortogonalidade no caso Euclidiano e no caso simplético. Para isso, fixados $u, v \in \mathcal{I}_r$ considere a matriz $N(uv)$. Retomando as listas $\mathcal{Z}_i$ definidas na Eq. (4.12), e levando em consideração a Definição 4.10, pode-se representar $N(uv)$ da seguinte forma:

$$N(uv) = \left[\begin{array}{c:c:c:c:c:c} N(\mathcal{Z}_*(uv)) & N(\mathcal{Z}_0(uv)) & N(\mathcal{Z}_1(uv)) & N(\mathcal{Z}_2(uv)) & \cdots & N(\mathcal{Z}_{2^r-2}(uv)) \\ \hdashline N(\mathcal{Z}_{2^r-2}(uv)) & N(\mathcal{Z}_*(uv)) & N(\mathcal{Z}_0(uv)) & N(\mathcal{Z}_1(uv)) & \cdots & N(\mathcal{Z}_{2^r-3}(uv)) \\ \hdashline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hdashline N(\mathcal{Z}_0(uv)) & N(\mathcal{Z}_1(uv)) & N(\mathcal{Z}_2(uv)) & N(\mathcal{Z}_3(uv)) & \cdots & N(\mathcal{Z}_*(uv)) \end{array}\right], \quad (4.40)$$

sendo que, para cada $i \in \mathcal{I}_r$, a notação:

$$N(\mathcal{Z}_i(uv)) \quad (4.41)$$

representa o resultado obtido ao se aplicar a regra (4.18) aos elementos da lista $\mathcal{Z}_i$ associados à matriz $N(uv)$. Ou seja, $N(\mathcal{Z}_i(uv))$ é um elemento de $\mathbb{F}_2^{2^r}$ que, de acordo com o Teorema 4.13, possui no máximo duas entradas não-nulas e tal situação depende se u é ou não igual a v. Considerando tais fatos, chega-se ao próximo resultado.

Proposição 4.22. *Considere a matriz norma $N(uv)$ e fixe um índice $i \in \mathcal{I}_r$. Se $u \neq v$, então existe um único índice $j \in \mathcal{I}_r$ diferente de i, tal que $N(\mathcal{Z}_i(uv)) = N(\mathcal{Z}_j(uv))$. Caso se tenha $u = v$, então $N(\mathcal{Z}_i(uv)) \neq N(\mathcal{Z}_j(uv))$ sempre que $i \neq j$.*

Demonstração: Suponha que $u \neq v$. Dessa forma, existem índices $m, n \in \mathcal{I}_r$ distintos tais que $||z_{in}||_{\mathbb{F}_{2^r}} = \alpha^u$ e $||z_{im}||_{\mathbb{F}_{2^r}} = \alpha^v$. Dessa maneira, pelo Item $iii)$ da Proposição 4.8, segue que $||z_{nm}||_{\mathbb{F}_{2^r}} = \alpha^u + \alpha^v$. Por outro lado, o Teorema 4.13 Item $ii)$ garante a existência de um único índice $j \in \mathcal{I}_r$ diferente de i, tal que $||z_{jn}||_{\mathbb{F}_{2^r}} = \alpha^v$. Considerando os índices j e m, tal fato implica em $||z_{jm}||_{\mathbb{F}_{2^r}} = \alpha^u$. Agora, se $u = v$, usando novamente o Item $ii)$ do Teorema 4.13, pode-se afirmar que tal índice j não existe. Com isso, conclui-se o resultado. □

Perceba que a Proposição 4.22 mostra que para qualquer matriz norma $N(uv)$ se $N(\mathcal{Z}_i(uv)) \neq N(\mathcal{Z}_j(uv))$, então as entradas não nulas de $N(\mathcal{Z}_i(uv))$ ocorrem obrigatoriamente em posições diferentes das entradas não nulas de $N(\mathcal{Z}_j(uv))$. Ou seja, tem-se imediatamente o seguinte resultado.

Corolário 4.23. *Dada a matriz norma $N(uv)$, consideremos a representação dada em (4.40). Sendo assim,*

1. *Se $u \neq v$, então $\langle N(\mathcal{Z}_i(uv)), N(\mathcal{Z}_j(uv)\rangle_E = 0, \ \forall \ i, j \in \mathcal{I}_r$;*

2. *Se $u = v$, então* $\langle N(\mathcal{Z}_i(uv)), N(\mathcal{Z}_j(uv)\rangle_E = \begin{cases} 0, \text{ se } \ i \neq j; \\ 1, \text{ se } \ i = j. \end{cases}$.

Com isso, segue o teorema que relaciona os códigos obtidos por meio das matrizes norma com os conceitos de ortogonalidade vistos nas Definições 4.34 e 4.19.

Teorema 4.24. *Dados $u, v \in \mathcal{I}_r$, temos que:*

i) $N(uv) \cdot N(uv)^T = 0$. *Ou seja, os códigos $\mathcal{C}(uv)$ são auto-ortogonais Euclidianos.*

ii) $N(uv) \cdot \Omega_{2^{2r-1}} \cdot N(uv)^T = 0$. *Ou seja, os códigos $\mathcal{C}(uv)$ são auto-ortogonais simpléticos.*

Demonstração: Note que, considerando as linhas da matriz Υ_r que são obtidas por meio da Eq. (4.13), a representação da matriz norma dada na Eq. (4.40) e a notação introduzida pela Eq. (4.41), tem-se que as 2^r linhas de $N(uv)$, denotadas por $N(L_i(uv))$, são dadas

da seguinte forma:

$$
\begin{aligned}
N(L_0(uv)) &= N(uv) = \left(\begin{array}{c|c|c|c|c} N(\mathcal{Z}_*(uv)) & N(\mathcal{Z}_0(uv)) & N(\mathcal{Z}_1(uv)) & \dots & N(\mathcal{Z}_{2^r-2}(uv)) \end{array}\right) \\
N(L_1(uv)) &= \left(\begin{array}{c|c|c|c|c} N(\mathcal{Z}_{2^r-2}(uv)) & N(\mathcal{Z}_*(uv)) & N(\mathcal{Z}_0(uv)) & \dots & N(\mathcal{Z}_{2^r-3}(uv)) \end{array}\right) \\
N(L_2(uv)) &= \left(\begin{array}{c|c|c|c|c} N(\mathcal{Z}_{2^r-3}(uv)) & N(\mathcal{Z}_{2^r-2}(uv)) & N(\mathcal{Z}_*(uv)) & \dots & N(\mathcal{Z}_{2^r-4}(uv)) \end{array}\right) \\
&\vdots \\
N(L_{2^r-1}(uv)) &= \left(\begin{array}{c|c|c|c|c} N(\mathcal{Z}_0(uv)) & N(\mathcal{Z}_1(uv)) & N(\mathcal{Z}_2(uv)) & \dots & N(\mathcal{Z}_*(uv)) \end{array}\right).
\end{aligned}
$$

Desse modo, o que determina a multiplicação entre uma linha e uma coluna da matriz $N(uv)$ são produtos dados por $N(\mathcal{Z}_i(uv)) \cdot (N(\mathcal{Z}_j(uv)))^T$. Considerando tal fato e o resultado 4.23, conclui-se que $N(L_i(uv)) \cdot (N(L_j(uv)))^T = 0$, para quaisquer $i, j \in \mathcal{I}_r$. Logo, $N(uv) \cdot N(uv)^T = 0$. O mesmo argumento mostra que $N(uv) \cdot \Omega_{2^{2r-1}} \cdot N(uv)^T = 0$, uma vez que, no caso binário, o produto $N(uv) \cdot \Omega_{2^{2r-1}}$ implica apenas uma permutação entre as de 2^{2r-1} primeiras colunas de $N(uv)$, com as suas 2^{2r-1} colunas restantes. □

CAPÍTULO 5

TÓPICOS DA TEORIA DA INFORMAÇÃO QUÂNTICA

O objetivo deste Capítulo é fornecer uma introdução rápida e relativamente técnica de alguns tópicos relacionados à teoria da Informação e Computação Quântica, dando ênfase ao tópico de *Códigos Corretores de Erros Quânticos (CCEQ)*. A grosso modo, pode-se dizer que os CCEQ são códigos corretores de erros que atendem aos princípios da Mecânica Quântica. O ferramental matemático que é utilizado para estudar a mecânica quântica é dado pela formulação de *Dirac*. Tal formulação tem como base noções relacionadas à Números Complexos, Álgebra Linear, Álgebra Tensorial, e será utilizada ao longo de todo Capítulo. Para não fugir do propósito do texto, que é a de estudar aspectos relacionados à Teoria de Códigos, recomenda-se as referências [14, 20, 36, 40, 43, 51, 54] para uma visão mais ampla sobre a relação entre a fundamentação de teoria da Física Quântica e a teoria da Informação.

5.1 Qubit e o Espaço de Estados

O conceito mais básico associado à teoria de Informação e Comunicações Digitais é o *bit* (abreviação do termo em inglês *binary unit*). Um bit pode assumir dois, e somente dois, possíveis valores: 0 ou 1. Considerando condições relacionadas à Física, uma situação que pode ser descrita por meio de um bit é a indicação de dois níveis de tensão distintos, por exemplo. Em relação à teoria da Informação Quântica a unidade fundamental de informação é conhecida por *bit quântico*, e recebe a designação de *qubit*. O interessante é que um qubit pode assumir dois possíveis valores e qualquer combinação linear intermediária entre eles em um espaço tridimensional. A título de informação, os experimentos envolvendo polarizações do fóton, ou os estados de excitação de um átomo, ou os estados de alinhamentos de um spin nuclear são citados como situações que podem ser modeladas por meio da ideia de qubit. A seguir introduz-se o primeiro Postulado da mecânica quântica que tem como propósito estabelecer o ambiente matemático no qual se desenvolve a teoria da Mecânica Quântica. É fundamental observar que, neste Capítulo, serão apresentados outros Postulados vinculados à Mecânica Quântica. No entanto,

essa exposição seguirá uma sequência diferente da ordem de apresentação tradicional encontrada em outras fontes, devido à adaptação à estrutura de escrita selecionada para este texto.

Postulado 1. ***(1º Postulado da Mecânica Quântica)*** *Todo sistema físico isolado está associado a um espaço de Hilbert, conhecido como* ***espaço de estados****. O* ***estado*** *do sistema é dado por um vetor unitário, chamado* ***vetor de estado****, que pertence a esse espaço de estados. Dessa forma, o estado do sistema é completamente descrito pelo seu vetor de estado, que é um elemento do espaço de Hilbert associado ao sistema.*

Em função da proposta do presente trabalho, serão considerados apenas espaços de Hilbert que sejam isomorfos a $\left(\mathbb{C}^2\right)^n$. Nesse sentido, de acordo com Postulado 1, um estado pode ser representado por um vetor coluna com n componentes complexas, denominado "*ket*". A notação de Dirac usada para representar um ket é dada por $|x\rangle$. A cada ket corresponde um vetor linha de mesma dimensão n, chamado "*bra*", e representado por $\langle x|$, cujas componentes são dadas pelo conjugado das componentes correspondentes do ket. Assim, um ket e um bra são representados, respectivamente, da seguinte forma:

$$|x\rangle = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad \text{e} \quad \langle x| = \begin{bmatrix} x_1^* & x_2^* & \cdots & x_n^* \end{bmatrix}, \tag{5.1}$$

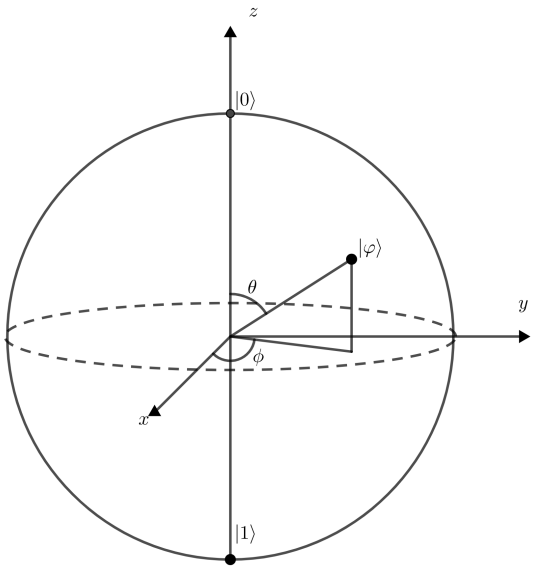
onde x_i^* indica o complexo conjugado de x_i. Observe que, $\langle x| = (|x\rangle^*)^T$, isto é, o bra é o conjugado transposto do ket. De acordo com [56], os termos bra e ket foram escolhidos pois originam-se da divisão do vocábulo inglês *braket*, que significa colchete. Como se o símbolo matemático representativo do colchete $\langle\ ,\ \rangle$ resultasse da junção de um bra e um ket. Como foi mencionado, a unidade básica da informação quântica é o qubit que, em relação à notação de Dirac, pode assumir dois estados: $|0\rangle$ e $|1\rangle$. Os estados $|0\rangle$ e $|1\rangle$ são representados, respectivamente, nas formas matriciais dadas por:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \text{e} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{5.2}$$

Na teoria da informação clássica os bits são representados como setas apontando para cima ($\uparrow$) no caso do estado 1, e uma seta para baixo ($\downarrow$) para indicar o estado 0. Na teoria da informação quântica, uma maneira de representar um qubit é por meio da *esfera de Bloch* que é representada conforme a Figura 5.1.

A esfera de Bloch é uma ferramenta importante na computação quântica e no estudo dos sistemas quânticos de dois níveis. Nela, o polo norte equivale ao estado $|0\rangle$ e o polo sul corresponde ao estado $|1\rangle$ e os outros locais na esfera são chamados de *superposições* dos estados $|0\rangle$ e $|1\rangle$. A superposição de estados as vezes é retratada como um Postulado adicional da mecânica. Aqui, este princípio será apresentado de modo formal através da próxima definição.

Figura 5.1: *Esfera de Bloch e representação de um estado $|\varphi\rangle$.*



Definição 5.1. *Um **estado de superposição** para um qubit é descrito pela forma:*

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{5.3}$$

em que $\alpha, \beta \in \mathbb{C}$ são as amplitudes dos estados $|0\rangle$ e $|1\rangle$, respectivamente, e satisfazem a seguinte condição

$$|\alpha|^2 + |\beta|^2 = 1, \tag{5.4}$$

sendo que $|x| = x \cdot x^*$, $\forall x \in \mathbb{C}$.

Na teoria da mecânica quântica, a condição sobre um estado de superposição, apresentada em 5.4, se justifica pelo fato de que $|\alpha|^2$ e $|\beta|^2$ representam as probabilidades de se encontrar os estados $|0\rangle$ e $|1\rangle$, respectivamente, após se medir o qubit $|\varphi\rangle$. E, como probabilidades, a soma deve ser sempre igual a 1. Neste sentido, o conceito de superposição de estados é interpretado como se o estado $|\varphi\rangle$ estivesse simultaneamente nos estados $|0\rangle$ e $|1\rangle$ e, após a medida o estado deve entrar em colapso tornando-se $|0\rangle$ ou $|1\rangle$, com suas respectivas probabilidades. De acordo com [14], a propriedade da superposição faz parecer que um qubit pode conter uma quantidade infinita de informações, devido às infinitas possibilidades de escolhas para α e β em $\mathbb{C}$. No entanto, essa conclusão não é verdadeira, pois não é possível extrair uma quantidade infinita de informações do qubit. Independentemente do tipo de medição, a medida de um qubit resultará sempre em um estado $|0\rangle$ ou $|1\rangle$. De toda forma, essa propriedade é muito importante para a computação quântica.

5.2 O Produto Tensorial

Na teoria clássica, ao considerar dois bits, obtêm-se quatro estados diferentes: $00, 01, 10, 11$, que correspondem respectivamente às representações binárias dos números $0, 1, 2$ e 3. Algo similar ocorre na teoria quântica, uma vez que pode ser necessário definir uma base que contenha múltiplos qubits para que se possa modelar um determinado sistema físico isolado. A operação usual para definir esta base é o produto tensorial entre qubits sobre o espaço vetorial complexo, em que as estruturas da mecânica quântica são descritas. Nesta seção serão apresentados, de modo breve, os conceitos básicos relacionados ao produto tensorial tomando como base a notação de Dirac para definir o produto interno $\langle\cdot|\cdot\rangle$ do espaço de Hilbert $(\mathbb{C}^2)^n$.

Definição 5.2. *Dados quaisquer $|x\rangle, |y\rangle$ e $|z\rangle \in \mathbb{C}^{2^n}$ e para quaisquer $\lambda_1, \lambda_2 \in \mathbb{C}$ o **produto interno** de $\mathbb{C}^{2^n}$, denotado por $\langle\cdot|\cdot\rangle$, é uma aplicação de $\mathbb{C}^{2^n} \times \mathbb{C}^{2^n}$ em $\mathbb{C}$, que satisfaz as seguintes condições:*

i) $\langle x|y\rangle = \langle y|x\rangle^*$;

ii) $\langle x|x\rangle \geq 0$ *com a igualdade ocorrendo se, e só se,* $|x\rangle = 0$;

iii) $\langle x|\lambda_1 y + \lambda_2 z\rangle = \lambda_1\langle x|y\rangle + \lambda_2\langle x|z\rangle$.

*Assim, os estados $|x\rangle$ e $|y\rangle$ em $\mathbb{C}^{2^n}$ são **ortogonais**, quando $\langle x|y\rangle = 0$.*

Definido o produto interno, define-se a *norma* de um vetor em $\mathbb{C}^{2^n}$.

Definição 5.3. *A **norma** de um estado $|x\rangle \in \mathbb{C}^{2^n}$, denotada por $||x||$, é dada por:*

$$||x|| = \sqrt{\langle x|x\rangle}. \tag{5.5}$$

*Quando $||x|| = 1$, diz-se que $|x\rangle$ é um **estado unitário**. Um conjunto de estado $\{|x_1\rangle, \ldots, |x_k\rangle\}$ é **ortonormal** quando todos os estados são unitários, e dois-a-dois ortogonais.*

Como a dimensão de $\mathbb{C}^{2^n}$ é igual a 2^n, é possível tomar um conjunto $\{|e_1\rangle, |e_2\rangle, \ldots, |e_{2^n}\rangle\}$ de estados ortonormais, isto é, $\langle e_i|e_j\rangle = \delta_{i,j}$, onde $\delta_{i,j}$ representa o *delta de Kronecker*. Com isso, para todo $|x\rangle \in \mathbb{C}^{2^n}$, segue que:

$$|x\rangle = x_1|e_1\rangle + x_2|e_2\rangle + \cdots + x_{2^n}|e_{2^n}\rangle. \tag{5.6}$$

Desta forma, o produto interno de dois vetores $\langle x|y\rangle$ pode ser escrito da seguinte maneira:

$$\langle x|y\rangle = \begin{bmatrix} x_1^* & x_2^* & \cdots & x_{2^n}^* \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{2^n} \end{bmatrix} = x_1^* y_1 + x_2^* y_2 + \cdots + x_{2^n}^* y_{2^n}. \tag{5.7}$$

Definição 5.4. *O **produto transposto** entre os estados $|x\rangle, |y\rangle \in \mathbb{C}^{2^n}$, denotado por $|x\rangle\langle y|$, é definido da seguinte forma:*

$$|x\rangle\langle y| = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2^n} \end{bmatrix} \cdot \begin{bmatrix} y_1^* & y_2^* & \cdots & y_{2^n}^* \end{bmatrix} = \begin{bmatrix} x_1y_1^* & x_1y_2^* & \cdots & x_1y_{2^n}^* \\ x_2y_1^* & x_2y_2^* & \cdots & x_2y_{2^n}^* \\ \vdots & \vdots & \cdots & \vdots \\ x_{2^n}y_1^* & x_{2^n}y_2^* & \cdots & x_{2^n}y_{2^n}^* \end{bmatrix}. \tag{5.8}$$

Os conceitos vistos até aqui fornecem a caracterização dos espaços vetoriais complexos. A seguir são dadas as propriedades do produto tensorial de acordo com a notação de Dirac.

Definição 5.5. *Suponha que $\mathcal{V}$ e $\mathcal{W}$ sejam espaços vetoriais de dimensões m e n, respectivamente. O **produto tensorial** $\mathcal{V} \otimes \mathcal{W}$ é um espaço vetorial $mn-$dimensional. Os elementos de $\mathcal{V} \otimes \mathcal{W}$ são combinações lineares dos produtos tensoriais $|v\rangle \otimes |w\rangle$, com $|v\rangle \in \mathcal{V}$ e $|w\rangle \in \mathcal{W}$, satisfazendo as seguintes propriedades: dados $z \in \mathbb{C}, |v\rangle, |v_1\rangle, |v_2\rangle \in \mathcal{V}$ e $|w\rangle, |w_1\rangle, |w_2\rangle \in \mathcal{W}$ tem-se:*

i) $z(|v\rangle \otimes |w\rangle) = z(|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$,

ii) $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = (|v_1\rangle \otimes |w\rangle) + (|v_2\rangle \otimes |w\rangle)$,

iii) $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = (|v\rangle \otimes |w_1\rangle) + (|v\rangle \otimes |w_2\rangle)$.

As notações $|v\rangle|w\rangle, |v, w\rangle$ e $|vw\rangle$ também são utilizadas para indicar o produto tensorial $|v\rangle \otimes |w\rangle$. Ainda em relação à notações, também é comum empregar as notações $|u\rangle^{\otimes^n}$ e $\mathcal{V}^{\otimes^n}$ para denotar, respectivamente o seguinte:

$$|u\rangle^{\otimes^n} = \underbrace{|u\rangle \otimes \cdots \otimes |u\rangle}_{\text{n estados}} \quad \text{e} \quad \mathcal{V}^{\otimes^n} = \underbrace{\mathcal{V} \otimes \cdots \otimes \mathcal{V}}_{\text{n espaços}}. \tag{5.9}$$

Tendo em mente a ideia de produto tensorial apresenta-se o Postulado 2.

Postulado 2. ***(4º Postulado da Mecânica Quântica)** O espaço de estados de um sistema composto é o produto tensorial dos espaços de estados dos componentes. Se $|\varphi_1\rangle, \ldots, |\varphi_n\rangle$ descrevem os estados de n sistemas quânticos isoladamente, o estado do sistema composto é dado por $|\varphi_1\rangle \otimes \cdots \otimes |\varphi_n\rangle$.*

Ao analisar o Postulado 2 poderia surgir o seguinte questionamento: por que usar o produto tensorial? De acordo com [51] o motivo do uso do produto tensorial neste Postulado está relacionado ao uso do princípio da superposição. Note que para sistemas compostos, parece natural que se $|v\rangle$ é um estado do sistema $\mathcal{V}$ e $|w\rangle$ é um estado do sistema $\mathcal{W}$, então deve haver algum estado correspondente, que podemos denotar por $|v\rangle|w\rangle$, do sistema de composto $\mathcal{V} \otimes \mathcal{W}$. Com isso o Postulado 2 é obtido ao se aplicar o princípio de superposição a estados de produto dessa forma.

O Postulado 2 está relacionado com a modelagem de sistemas cujos estados com mais de um qubit. De modo geral, o estado $|v\rangle$ com n qubits é uma superposição dos 2^n estados de $\mathbb{C}^{2^n}$ representados por:

$$|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle, \tag{5.10}$$

de modo que a sequência dentro de cada ket em (5.10) é a representação binária dos números $0, 1, \ldots, 2^n - 1$. Portanto, observa-se que:

$$\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\} \tag{5.11}$$

formam uma base ortonormal para o espaço de estados com n qubits. Os estados representados em (5.11) formam um conjunto que é chamado de *base computacional de estados com n qubits*. Assim, para cada estado de n qubits $|v\rangle \in \mathbb{C}^{2^n}$, têm-se:

$$|v\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle, \tag{5.12}$$

com a restrição:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1. \tag{5.13}$$

Para explicitar como, de fato, são feitos os cálculos envolvendo o produto tensorial, segue a próxima definição que é a representação do produto tensorial por meio de matrizes. Tal representação é conhecida como o *produto de Kronecker*.

Definição 5.6. *Sejam $A = (a_{ij})_{n\times m}$ e $B = (b_{ij})_{s\times t}$ matrizes cujas entradas pertençam ao corpo* F. *Sendo assim, a representação matricial do produto tensorial $A \otimes B$, conhecida como* ***produto de Kronecker****, é dada por:*

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{bmatrix}, \tag{5.14}$$

Note que a matriz $A \otimes B$ tem ordem $ns \times mt$. Observe também que, por meio da Definição 5.6 constata-se que o produto tensorial não é comutativo.

Exemplo 5.7. *Considere as matrizes $A = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & -i & -i \\ -1 & 0 & 0 \end{bmatrix}$, definidas sobre o corpo $\mathbb{C}$. Dessa forma, segue que:*

$$A \otimes B = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & -i & -i & 0 & -i & -i \\ -1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & i & i \\ 0 & 0 & 0 & -1 & 0 & 0 \end{bmatrix} \text{ e } B \otimes A = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & -i & -i & -i & -i \\ 0 & 0 & 0 & i & 0 & i \\ -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

A seguir, apresentam-se algumas propriedades relacionadas ao produto de Kronecker.

Proposição 5.8. *Sejam A, B, C e D matrizes cujas entradas pertençam ao corpo* F. *Dessa forma, supondo que em cada item as ordens das matrizes permitem realizar as operações indicadas, por meio da Definição 5.6 conclui-se que:*

i) $A \otimes (B + C) = A \otimes B + A \otimes C$;

ii) $(B + C) \otimes A \otimes (B + C) = B \otimes A + C \otimes A$;

iii) $(\lambda A) \otimes B = A \otimes (\lambda B) = \lambda(A \otimes B),\ \lambda \in \mathrm{F}$;

iv) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$;

v) $A \otimes 0 = 0 \otimes A = 0$, *em que* 0 *representa a matriz nula;*

vi) $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$.

5.2.1 Operadores lineares

Neste ponto do texto se faz necessário introduzir o conceito de *operador linear*. Operadores lineares estão relacionados com outros Postulados da mecânica quântica.

Definição 5.9. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais. Uma aplicação $A : \mathcal{V} \longrightarrow \mathcal{W}$ é chamada de* ***operador linear*** *se:*

$$A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i A|v_i\rangle. \tag{5.15}$$

Neste caso, a notação $A|v\rangle$ indica que o operador A está aplicado em $|v\rangle$, isto é, $A|v\rangle = A\left(|v\rangle\right)$. Quando $A : \mathcal{V} \longrightarrow \mathcal{V}$, diz-se que o operador A está definido no espaço vetorial $\mathcal{V}$. O ***operador identidade*** *de $\mathcal{V}$, denotador por $I_{\mathcal{V}}$ é definido de modo que $I_{\mathcal{V}}|v\rangle = |v\rangle,\ \forall\, |v\rangle \in \mathcal{V}$.*

É comum a representação dos operadores lineares por meio de matrizes. Considere que $\mathcal{V}$ e $\mathcal{W}$ são espaços vetoriais sobre o corpo dos complexos. Dado um operador $A : \mathcal{V} \longrightarrow \mathcal{W}$, suponha que $\mathcal{B}_{\mathcal{V}} = \{|v_1\rangle, \ldots, |v_n\rangle\}$ e $\mathcal{B}_{\mathcal{W}} = \{|w_1\rangle, \ldots, |w_m\rangle\}$

sejam bases , respectivamente, de $\mathcal{V}$ e $\mathcal{W}$. Dessa forma, para cada $j \in \{1, 2, \ldots, n\}$ existem números complexos $a_{1j}, a_{2j}, \ldots, a_{mj}$ tais que:

$$A|v_j\rangle = \sum_{i=1}^{m} A_{ij}|w_1\rangle. \tag{5.16}$$

Deste modo, a matriz $(a_{ij})_{n\times m}$ é denominada como a *matriz do operador* A com respeito às bases $\mathcal{B}_\mathcal{V}$ e $\mathcal{B}_\mathcal{W}$. Nesta situação é usada a notação:

$$A = (a_{ij})_{n\times m}\,. \tag{5.17}$$

Por meio da matriz do operador, pode-se caracterizar a composição de dois operadores $A : \mathcal{V} \longrightarrow \mathcal{W}$ e $B : \mathcal{W} \longrightarrow \mathcal{U}$ da seguinte forma:

$$(B \circ A)\,|v\rangle = (B \cdot A)\,|v\rangle = B\,(A|v\rangle) = B \cdot A|v\rangle, \;\; \forall \;\; |v\rangle \in \mathcal{V}. \tag{5.18}$$

Quando se trata de operadores definidos em espaços vetoriais complexos, é importante estabelecer o conceito de *operadores Hermitianos* e *operadores unitários*. Para isso, é necessário definir o que é uma *matriz adjunta.*

Definição 5.10. *Seja $A = (a_{ij})_{n\times m}$ uma matriz cujas entradas sejam números complexos. Sendo assim, a* ***matriz adjunta*** *de A, denotada por $A^\dagger$, é definida de modo que:*

$$A^\dagger = \left[(a^*_{ij})_{n\times m}\right]^T. \tag{5.19}$$

Isto é, $A^\dagger$ é uma matriz obtida ao se conjugar todos as entradas de A e depois considerar a sua transposta.

Definição 5.11. *Seja A um operador linear definido sobre um espaço complexo $\mathcal{V}$. Sendo assim:*

i) A é um ***operador Hermitiano****, se $A = A^\dagger$;*

ii) A é um ***operador unitário****, se $A \cdot A^\dagger = I_\mathcal{V}$.*

Por intermédio do produto tensorial é possível obter um operador linear através de outros dois operadores previamente escolhidos. Tal fato é retratado na próxima definição.

Definição 5.12. *Dados dois operadores lineares A e B definidos sobre os espaços vetoriais $\mathcal{V}$ e $\mathcal{W}$, respectivamente o operador linear $A \otimes B$ em $\mathcal{V} \otimes \mathcal{W}$ é descrito por:*

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle, \tag{5.20}$$

em que $|v\rangle \in \mathcal{V}$ e $|w\rangle \in \mathcal{W}$.

Com as noções de operador Hermitiano e operador unitário é possível apresentar o Postulado 3 da mecânica quântica.

Postulado 3. ***(2º Postulado da Mecânica Quântica)*** *A evolução temporal de um sistema quântico fechado é descrita por um operador unitário. Isto é, se o estado do sistema quântico no instante t_1 é descrito pelo vetor $|\varphi_1\rangle$, então no instante t_2 o estado do sistema será dado por $|\varphi_2\rangle$ de modo que $|\varphi_1\rangle$ e $|\varphi_2\rangle$ estão relacionados por um operador unitário U que depende apenas de t_1 e t_2. E tal relação se dá da seguinte forma:*

$$|\varphi_2\rangle = U|\varphi_1\rangle. \tag{5.21}$$

O Postulado 3 não prediz quais são os operadores unitários que descrevem a dinâmica quântica do mundo real. A mecânica quântica apenas garante que a evolução de qualquer sistema quântico fechado pode ser descrita dessa forma. Uma pergunta óbvia para fazer é: quais operadores unitários são naturais a serem considerados? No caso de qubits únicos, segundo [51], verifica-se que qualquer operador unitário pode ser realizado em sistemas realistas.

Ainda em relação ao Postulado 3, a ação de um operador unitário sobre um estado preserva sua norma. Portanto, se $|\varphi\rangle$ é um estado unitário o estado $U|\varphi\rangle$, em que U é um operador unitário, também o será. Um algoritmo quântico consiste em uma prescrição de uma sequência de operadores unitários aplicados a uma condição inicial da forma:

$$|\varphi_n\rangle = (U_n \cdot \ldots \cdot U_1)|\varphi_1\rangle. \tag{5.22}$$

O estado $|\varphi_n\rangle$ é medido retomando o resultado do algoritmo. O Postulado da evolução pode ser colocado sob a forma de uma equação diferencial, chamada *equação de Schrödinger*. Essa equação fornece um método para se obter o operador U quando se é dado o contexto físico em questão. O objetivo da Física é descrever a dinâmica de sistemas físicos, por isso, a equação de Schrödinger tem um papel fundamental. O objetivo da ciência da computação é analisar e implementar algoritmos, logo, o cientista da computação quer saber se é possível implementar de alguma forma um operador unitário previamente escolhido. A forma da equação (5.21) é conveniente para a área de algoritmos quânticos.

Nessa dinâmica, saber quando dois operadores lineares comutam entre si, como será visto mais adiante, é algo importante dentro da teoria de códigos quânticos. Para auxiliar a verificação de tal fato serão definidos os conceitos de *comutador* e *anticomutador*.

Definição 5.13. *Sejam A e B dois operadores lineares em um mesmo espaço vetorial. O* ***comutador*** *entre A e B, denotado por $[A, B]$, da seguinte forma:*

$$[A, B] = A \cdot B - B \cdot A. \tag{5.23}$$

Analogamente, o ***anticomutador*** *entre A e B, denotado por $\{A, B\}$, é definido da seguinte maneira:*

$$\{A, B\} = A \cdot B + B \cdot A. \tag{5.24}$$

Note que, de acordo com a definição 5.13, se $[A, B] = 0$ então $A \cdot B = B \cdot A$. Logo os operadores A e B comutam entre si. E se $A, B = 0$, então A e B anticomutam, isto é, $A \cdot B = -B \cdot A$.

E finalizando esta seção segue o Postulado 4, também conhecido como Postulado das medidas.

Postulado 4. ***(3º Postulado da Mecânica Quântica)*** *As medidas quânticas são obtidas através de uma coleção de operadores de medição M_n. Esses operadores atuam no espaço de estado do sistema que está sendo medido. O índice n representa os resultados possíveis que podem ocorrer durante a medição. Se o estado do sistema quântico é $|v\rangle$ logo antes da medição, então a probabilidade de que o resultado n aconteça é calculada por meio de $p(n) = \langle v|M_n^\dagger M_n|v\rangle$. Após a medição, o estado do sistema é alterado para $|\varphi_m\rangle = \dfrac{M_n|v\rangle}{\sqrt{p(n)}}$. Os operadores de medição são regidos pela equação de completude $M_n^\dagger M_n = I$, onde I é o operador de identidade.*

Em relação aos experimentos envolvendo sistemas modelados pela física quântica, deve haver momentos em que o experimentalista, com seu equipamento experimental, possa realizar uma observação para descobrir o que está acontecendo dentro do sistema. Tal interação torna o sistema não mais fechado e, portanto, não necessariamente sujeito à evolução unitária. Desta forma, a grosso modo, pode-se dizer que o Postulado 4 fornece um meio para descrever os efeitos de medições em sistemas quânticos.

Um tipo especial de operador de medição é chamado de *medição projetiva*. Uma medição projetiva é descrita por um observável, M, que é um operador Hermitiano no espaço de estados do sistema em observação. O observável possui uma decomposição espectral, $M = \sum_m mP_m$, onde P_m é o projetor sobre o espaço próprio de M com autovalor m. Os possíveis resultados da medição correspondem aos autovalores, m, do observável. Após a medição do qubit $|v\rangle$, a probabilidade de obter m é igual a $p(m) = \langle v|P_m|v\rangle$. Se m ocorreu, o estado do sistema quântico após a medição é $|\varphi_m\rangle = \dfrac{P_m|v\rangle}{\sqrt{p(m)}}$.

Exemplo 5.14. *Suponha que o estado $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ esteja associado a um sistema quântico de $\mathbb{C}^2$. Considerando os operadores $M_0 = |0\rangle\langle 0|$ e $M_1 = |1\rangle\langle 1|$, observa-se que $\{M_0, M_1\}$ é um conjunto de operadores de medição. Deste modo, após a medição por tais operadores, segue que $p(0) = |\alpha|^2$, $p(1) = |\beta|^2$, $|\varphi_0\rangle = \dfrac{\alpha}{|\alpha|}|0\rangle$ e $|\varphi_1\rangle = \dfrac{\beta}{|\beta|}|1\rangle$. De modo geral, tomando $\mathbb{C}^{2^n}$, e a base computacional dada 5.11, segue o conjunto formado pelos operadores $M_k = |k\rangle\langle k|$, com $0 \leq k \leq 2^n - 1$ é um conjunto de operadores de medição. Logo, dado um estado $|\psi\rangle \in \mathbb{C}^{2^n}$ da forma $|\psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k|k\rangle$, após a medição por pelos medidores M_k tem-se que $p(k) = |\alpha_k|^2$ e $|\varphi_k\rangle = \dfrac{\alpha_k}{|\alpha_k|}|k\rangle$, sendo $0 \leq k \leq 2^n - 1$.*

5.3 Códigos Quânticos Corretores de Erros

Formalmente, um Código Quântico Corretor de Erros (CQCE) é definido da seguinte maneira:

Definição 5.15. *Um **código quântico corretor de erros (CQCE)**, é um subespaço $\mathcal{C}$ de dimensão q^k (q é potência de um número primo) de um espaço de Hilbert $(\mathbb{C}^q)^{\otimes^n} \cong \mathbb{C}^{q^n}$. A distancia mínima d do CQCE $\mathcal{C}$ é a menor distância de Hamming entre duas palavras código distintas. Ao código quântico $\mathcal{C}$ com comprimento n, dimensão q^k, e distância mínima d pode ser representado por meio da seguinte notação $\mathcal{C} = [\![n, k, d]\!]_q$.*

Assim como nos códigos clássicos, o problema de proteger uma informação de uma interferência (ruído) também é um dilema evidenciado na teoria da informação e computação quântica. Diante disso, os códigos corretores de erros quânticos tem como objetivo justamente recuperar um estado quântico original quando o mesmo é acometido por interferências entre o percurso percorrido até chegar ao receptor. Com isso, muitos dos estudos referentes aos códigos quânticos gira em torno de entender como tais códigos agem para proteger a informação quando se insere no contexto um canal pelo qual a informação irá transitar. Sendo assim, para entender a ideia de CQCE (informações referentes aos parâmetros, características algébricas de tais códigos vistos como subespaços vetoriais, etc), serão mostrados alguns dos possíveis erros que podem afetar um único qubit em tipos específicos de canais e depois tal noção será ampliada para situações que envolvam n qubits.

5.3.1 Operadores de Pauli

Na computação clássica a manipulação nos bits ocorre por meio de operações conhecidas como *portas lógicas*. Tal manipulação é, na sua essência, a conversão de uma forma para outra. Por exemplo, para portas que agem em um único bit de informação, a única porta não trivial é a que converte o bit 0 no bit 1 e vice-versa. No caso da computação quântica, as manipulações ficam a cargo das *portas quânticas*, das quais as mais importantes, no caso da ação em um qubit, são os *operadores de Pauli*. Tais operadores são dados pelas seguintes matrizes:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{5.25}$$

É comum encontrar na literatura a utilização das notações:

$$\sigma_0,\ \sigma_X,\ \sigma_Y \text{ e } \sigma_Z, \tag{5.26}$$

para se referir aos operadores I, X, Y e Z, respectivamente. No presente texto tais notações também serão empregadas de modo a não gerar confusão. Os operadores de Pauli são Hermitianos e unitários. Com isso, pode-se mostrar que seus autovalores são iguais a 1 ou -1.

Considerando a notação de Dirac, os operadores de Pauli admitem as seguintes

representações:

$$\begin{aligned}\sigma_0 &= |0\rangle\langle 0| + |1\rangle\langle 1|,\\ \sigma_X &= |1\rangle\langle 0| + |0\rangle\langle 1|,\\ \sigma_Y &= i|1\rangle\langle 0| - i|0\rangle\langle 1|\\ \sigma_Z &= |0\rangle\langle 0| - |1\rangle\langle 1|.\end{aligned} \tag{5.27}$$

Assim, a ação de cada operador de Pauli diferente da identidade sobre um estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, é dada da seguinte forma:

$$\begin{aligned}\sigma_X|\psi\rangle &= \beta|0\rangle + \alpha|1\rangle;\\ \sigma_Y|\psi\rangle &= i\left(-\beta|0\rangle + \alpha|1\rangle\right);\\ \sigma_Z|\psi\rangle &= \alpha|0\rangle - \beta|1\rangle.\end{aligned} \tag{5.28}$$

Em virtude das equações dadas em (5.28), os operadores σ_X, σ_Y e σ_Z recebem do inglês, respectivamente, as denominações *bit flip* (inversora de bit), *phase flip* (inversora de fase) e *bit and phase flip* (inversora de bit e de fase). O conceito de fase possui uma relação com os coeficientes α e β do estado $|\psi\rangle$ e admite mais de uma interpretação do ponto de vista físico. Além disso, existem outros tipos de portas quânticas que agem sobre um qubit. A discussão de tais fatos não é objetivo do presente trabalho e para tais detalhes indica-se a referência [51]. Mais propriedades relacionadas serão vistas mais adiante.

5.3.2 Código Corretor de Erros Bit Flip para Três Qubits

Esta seção trata de apresentar um exemplo com o intuito de ilustrar como os códigos quânticos funcionam na questão de proteção da informação. Para dar início, suponha que por um canal sejam enviados qubits de forma que, este canal os inverte com a probabilidade p e os mantém inalterados com probabilidade de $1 - p$. Ou seja, tal situação trata do canal *bit flip* cuja ação é dada por meio matriz de Pauli X. Desde modo, com base em [40], tal canal pode ser definido da seguinte maneira:

Definição 5.16. *Dado o qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ o **canal de inversão de bits** age sobre $|\psi\rangle$ da seguinte forma:*

- $X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$ *com probabilidade p;*
- $|\psi\rangle$ *com probabilidade $1 - p$.*

Assim, para proteger a informação dada pelo qubit $|\psi\rangle$ decorrentes dos efeitos de ruído do canal bit flip, utiliza-se o *código bit flip*. Tal código utiliza três qubits e tal fato é feito da seguinte maneira. Considere um qubit da forma $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ e assuma que $|\psi\rangle$ seja codificado com três qubits da seguinte forma:

$$|\psi\rangle_{cod} = \alpha|000\rangle + \beta|111\rangle. \tag{5.29}$$

Neste caso, define-se $|000\rangle$ e $|111\rangle$ como os estados lógicos $|0\rangle_L$ e $|1\rangle_L$, respectivamente. Ou seja:

$$|0\rangle_L := |000\rangle \text{ e } |1\rangle_L := |111\rangle. \tag{5.30}$$

Na realidade, a expressão (5.30) estabelece a seguinte codificação:

$$|0\rangle \overset{\text{codificação}}{\longrightarrow} |000\rangle \text{ e } |1\rangle \overset{\text{codificação}}{\longrightarrow} |111\rangle. \tag{5.31}$$

O canal bit flip é considerado independente, isto é, cada qubit passa pelo canal por meio de uma cópia independente, significando portanto que a ação de erro ocorre de forma separada em cada qubit ([40, 51]). Agora será mostrado como realizar os procedimentos de medições neste canal para a identificação dos erros. Suponha que o estado inicial $|\psi\rangle$ tenha sido codificado para o estado $|\psi\rangle_{cod}$ conforme a Eq. (5.29). Sabe-se que cada um dos três qubits passa pelo canal bit flip através de uma cópia independente. Sendo assim, assuma que tenha acontecido um erro em no máximo um qubit e que, por esse motivo, se deseje corrigir tal erro sem que haja a perda da superposição $|\psi\rangle_{cod} = \alpha|000\rangle + \beta|111\rangle$. Para se corrigir o erro e recuperar o estado original é utilizado um procedimento que consiste de duas etapas. A princípio, deve-se realizar uma medida sobre o estado quântico que irá detectar o erro, caso haja algum. O resultado desse processo de medição é denominado *síndrome de erro*. Em relação ao canal bit flip existem quatro tipos de síndromes de erro que correspondem aos operadores de projeção dados por:

$$\begin{aligned} P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| \\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110| \end{aligned} \tag{5.32}$$

O operador P_0 está associado a não ocorrência de erros, o operador P_1 está associado a ocorrência de erros no primeiro qubit, e os operadores P_2 e P_3 estão associados a ocorrência de erros no segundo e no terceiro qubit, respectivamente. A seguir segue a descrição de como o processo de detecção de erros funciona de fato. Suponha, sem perda de generalidade, que um erro tenha ocorrido no terceiro qubit. Deste modo, o estado:

$$|\psi\rangle_{cod} = \alpha|000\rangle + \beta|111\rangle,$$

se torna:

$$|\tilde{\psi}\rangle = \alpha|001\rangle + \beta|110\rangle.$$

Sendo assim, de acordo com o Postulado 4, ao se aplicar o operador P_3, obtem-se a probabilidade p_3 de modo que:

$$\begin{aligned} p_3 &= \langle\tilde{\psi}|P_3|\tilde{\psi}\rangle \\ &= (\alpha^*\langle 001| + \beta^*\langle 110|)(|001\rangle\langle 001|)(\alpha|001\rangle + \beta|110\rangle) \\ &\quad +(\alpha^*\langle 001| + \beta^*\langle 110|)(|110\rangle\langle 110|)(\alpha|001\rangle + \beta|110\rangle) \end{aligned} \tag{5.33}$$

Usando o fato de que os estados $|001\rangle$ e $|110\rangle$ fazem parte da base ortonormal para o espaço de estados em $\mathbb{C}^8$, segue da equação (5.33) que:

$$p_3 = \langle\tilde{\psi}|P_3|\tilde{\psi}\rangle = |\alpha|^2 + |\beta|^2 = 1$$

Com esta síndrome se identifica o erro no terceiro qubit. Note que, se a medição for feita, nesse caso, com os outros projetores, os resultados que encontraríamos seriam iguais a zero. Observe também que, durante esse processo de detecção o estado afetado pelos erros não é afetado pela medição da síndrome. O que ocorre é que a síndrome contém apenas informações sobre o qubit corrompido, mas nenhuma informação sobre o estado que está sendo medido uma vez que α e β são desconhecidos. Para recuperar o estado original $|\psi\rangle_{cod}$, basta utilizar novamente o código bit flip em $|\tilde{\psi}\rangle$ para inverter o terceiro qubit novamente. O procedimento mencionado para recuperação do estado pode ser aplicado independente de em qual qubit tenha ocorrido o erro. Se nenhum erro ocorrer neste processo, aplicando o operador P_0 tem-se $p_0 = 1$, ou seja, nenhum erro ocorreu. Procedendo da mesma forma, recupera-se o estado codificado original em todos os casos ([40]).

Agora, será mostrada uma forma alternativa para proceder o processo de medida. Para esta parte será introduzida uma notação com o intuito de abreviar a representação de operadores que possuem vários fatores em relação à representação com o produto de Kronecker. Tal notação funcionará da seguinte forma: considere um operador que agem em um estado de 5 qubits, por exemplo $X \otimes I \otimes Z \otimes Y \otimes I$ e $X \otimes X \otimes I \otimes Z \otimes I \otimes I$. Nesta situação usa-se, respectivamente, as notação $X_1 Z_3 Y_4$ e $X_1 X_2 Z_3$. Ou seja, nesta notação o subíndice índica em qual qubit o operador está agindo e o operador I é sempre omitido.

Com isso, considere a substituição dos quatro operadores de medida P_0, P_1, P_2 e P_3, pelos seguintes operadores:

$$Z_1 Z_2 := Z \otimes Z \otimes I, \tag{5.34}$$

$$Z_2 Z_3 := I \otimes Z \otimes Z. \tag{5.35}$$

Ambos operadores possuem autovalores -1 e 1. Suponha, desta vez, que a transmissão do estado $|\psi\rangle_{cod} = \alpha|000\rangle + \beta|111\rangle$ tenha resultado em uma alteração no primeiro qubit, ou seja, $|\tilde{\psi}\rangle = \alpha|100\rangle + \beta|011\rangle$. O operador $Z_1 Z_2$ compara o primeiro e o segundo qubit da seguinte forma: se após a transmissão os qubits em questão forem iguais, o resultado da medida será igual a 1, caso contrário, a medida resultará em -1. De modo análogo, o operador $Z_2 Z_3$ faz o mesmo processo no segundo e no terceiro qubit. Desta maneira, existem quatro possíveis resultados de síndrome, seguindo a mesma linha do processo utilizando os projetores. As quatro possibilidades são dadas pelas combinações dos valores das possíveis medições de $Z_1 Z_2$ e $Z_2 Z_3$, conforme é mostrado na Tabela 5.1.

Assim, para recuperar o estado quântico, basta proceder como no primeiro caso em que os projetores foram usados. A vantagem de se utilizar o segundo processo de síndrome é que neste processo são usados apenas dois operadores para detectar o erro ao invés de quatro operadores para medição como foi feito no primeiro processo apresentado.

Tabela 5.1: *Tabela de síndromes para os observáveis Z_1Z_2 e Z_2Z_3.*

Resultado da medida de Z_1Z_2	Resultado da medida de Z_2Z_3	Conclusão
1	1	não houve erro
1	-1	o erro ocorreu no terceiro qubit
-1	1	o erro ocorreu no primeiro qubit
-1	-1	o erro ocorreu no segundo qubit

5.3.3 Código Fase Shift para Três Qubits

Outro tipo de código quântico é código *fase shift* que se dá ao considerar a ação do canal de mesmo nome. O canal *fase shift* é representado pela ação do operador de Pauli Z. Assim como foi feito para o canal bit flip, segue a definição formal do canal fase shift.

Definição 5.17. *Dado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, o **canal fase shift** age em $|\psi\rangle$ da seguinte forma:*

- $Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$ *com probabilidade p;*
- $|\psi\rangle$ *com probabilidade $1-p$.*

O código fase shift consiste em usar a dinâmica do código bit flip para recuperar o estado codificado. Para isso usa-se um procedimento que consiste em "transformar"o canal fase flip em um canal do tipo bit flip. Tal fato é feito por meio da base de qubits dada por:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ e } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{5.36}$$

Observe que $Z|+\rangle = |-\rangle$ e $Z|-\rangle = |+\rangle$, logo Z atua como um bit flip na base $\{|-\rangle, |+\rangle\}$. Assim como no código bit flip, também define-se o qubits lógicos para o canal fase flip da seguinte maneira:

$$\begin{aligned} |0\rangle &\overset{\text{codificação}}{\longrightarrow} |0\rangle_L = |++\rangle; \\ |1\rangle &\overset{\text{codificação}}{\longrightarrow} |1\rangle_L = |--\rangle. \end{aligned} \tag{5.37}$$

A mudança de base dada pelas expressões (5.37) é obtida através da aplicação da porta quântica denominada *porta de Hadamard*, denotada por H e dada por:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{5.38}$$

sobre a base $\{|0\rangle, |1\rangle\}$. Desta forma pode-se proteger ao menos um qubit contra erros de inversão de fase. Assim, o processo de codificação, detecção e recuperação é o mesmo que o canal bit flip, porém em relação à base $\{|+\rangle, |-\rangle\}$. Mais detalhes sobre o procedimento de codificação para este canal podem ser vistos em [21].

5.3.4 Código de Shor

O código de Shor é o primeiro código de correção de erros quânticos capaz de proteger um único qubit arbitrário contra qualquer erro quântico [16, 20, 40, 43, 51]. Ele é construído por meio da concatenação dos procedimentos de detecção e correção de erros já conhecidos, a saber: bit flip e fase flip. As etapas de construção do código de Shor são as seguintes:
Etapa 1: A primeira etapa utiliza a codificação dada pelo canal fase flip. Isto é:

$$\begin{aligned} |0\rangle &\overset{\text{codificação}}{\longrightarrow} |++\rangle, \\ |1\rangle &\overset{\text{codificação}}{\longrightarrow} |--\rangle. \end{aligned}$$

Etapa 2: Na segunda etapa os qubits $|-\rangle$ e $|+\rangle$ são codificados por meio da aplicação do código bit flip, ou seja:

$$\begin{aligned} |+\rangle &\overset{\text{codificação}}{\longrightarrow} \frac{|000\rangle + |111\rangle}{\sqrt{2}}; \\ |-\rangle &\overset{\text{codificação}}{\longrightarrow} \frac{|000\rangle - |111\rangle}{\sqrt{2}}. \end{aligned} \tag{5.39}$$

O resultado deste processo é o código de Shor cujos qubits lógicos são dadas por:

$$\begin{aligned} |0\rangle \equiv |0\rangle_L &= \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}; \\ |1\rangle \equiv |1\rangle_L &= \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \end{aligned} \tag{5.40}$$

.

Considerando as etapas 1 e 2, será mostrado a seguir como o código de Shor corrige os erros do tipo bit flip e fase flip.
Correção de erros do tipo bit flip: sem perda de generalidade, assuma a existência de um erro do tipo bit flip no primeiro bloco de três qubits. Assim, realizando as medidas de Z_1Z_2 e Z_2Z_3 é possível identificar em qual qubit ocorreu o erro e corrigi-lo. O mesmo procedimento se aplica aos outros blocos: para se identificar erros no segundo bloco realiza-se a medida de Z_4Z_5 e Z_5Z_6, e para identificar erros no terceiro bloco realiza-se a medida de Z_7Z_8 e Z_8Z_9.
Correção de erros do tipo fase shift: Seguindo um raciocínio similar à correção de erros do tipo bit flip, será determinado um modo para a correção de erros do tipo fase shift. Por

exemplo, se a medição do observável $X_1X_2X_3X_4X_5X_6$ for realizada, seguida da medida de $X_4X_5X_6X_7X_8X_9$, um erro fase flip em qualquer um dos blocos será identificado e com isso tal erro poderá ser revertido utilizado o processo pertinente.

Correção de fase shift e bit flip no mesmo qubit: Este caso é uma aplicação direta dos anteriores. Isto é, basta aplicar o procedimento de recuperação do qubit que foi afetado pelo ruído do canal bit flip e depois aplicar o segundo procedimento para corrigir o erro de fase shift. Isto pode ser feito uma vez que ambos os processos de correção de erros ocorrem de forma independentes. Deste modo, o estabilizadores para o código Shor de nove qubits são dados pela Tabela 5.2

Tabela 5.2: *Tabela com os geradores e operações lógicas do código de Shor.*

Geradores	Operações Lógicas
M_1	Z_1Z_2
M_2	Z_2Z_3
M_3	Z_4Z_5
M_4	Z_5Z_6
M_5	Z_7Z_8
M_6	Z_8Z_9
M_7	$X_1X_2X_3X_4X_5X_6$
M_8	$X_4X_5X_6X_7X_8X_9$

O código de Shor possui parâmetros $[\![9, 1, 3]\!]_2$, isto é, o código utiliza nove qubits para codificar um qubit. Um dos pontos principais em relação ao código de Shor é o fato deste código ser capaz de corrigir um erro quântico arbitrário. De fato, note que as matrizes de Pauli formam uma base para o espaço das matrizes quadradas de ordem 2 com entradas em $\mathbb{C}$, $M_2(\mathbb{C})$. Com isso, dada uma matriz $E \in M_2(\mathbb{C})$ que é considerada uma *matriz erro* com ação em um qubit, segue que:

$$E = \alpha_1 I + \alpha_2 X + \alpha_3 Z + \alpha_4 (X \cdot Z), \tag{5.41}$$

sendo $\alpha_i \in \mathbb{C}$. Note que $X \cdot Z = iY$. Dessa forma, se $|\psi\rangle$ é um qubit, da Eq. (5.41) obtém-se:

$$E|\psi\rangle = \alpha_1 I|\psi\rangle + \alpha_2 X|\psi\rangle + \alpha_3 Z|\psi\rangle + \alpha_4 (X \cdot Z)|\psi\rangle. \tag{5.42}$$

Pelos princípios da mecânica quântica, após uma medição o estado $E|\psi\rangle$ deve colapsar para $|\psi\rangle X|\psi\rangle, Z|\psi\rangle$ ou $(X \cdot Z)|\psi\rangle$. Assim, como as matrizes de Pauli são inversíveis, é possível aplicar uma operação inversa para recuperar o estado $|\psi\rangle$. Isso significa, que se o código é capaz de corrigir erros do tipo bit flip (X), fase shift (Z), e bit fase shift $(X \cdot Z)$, então este código pode corrigir qualquer tipo de erro que é dada como combinação dos erros mencionados. Tal fato é uma aplicação do seguinte teorema:

Teorema 5.18. *[24] Se um código quântico corrige erros do tipo A e do tipo B então ele corrige qualquer combinação de erros de A e B.*

5.3.5 Condição para Correção de Erros Quânticos

Por meio dos exemplos de códigos quânticos mencionados nesta seção, surge o vislumbre de se obter uma teoria geral para a correção de erros em códigos quânticos, que tenha como base uma estrutura matemática, que venham auxiliar aos projetistas na analise se um determinado código é capaz de detectar e corrigir erros quânticos. É importante mencionar que a existência de tal estrutura matemática baseada nesta teoria não é suficiente para se garantir a existência de bons códigos quânticos. No entanto, ao recapitular o processo que um estado quântico percorre ao passar por um canal é possível, de modo intuitivo, estabelecer os conceitos para a teoria de correção de erros quântica. Até o momento, foi visto que um estado quântico de informação é codificado por meio de portas quânticas, que por sua vez são operadores unitários. Além disso, sabe-se que os códigos estão ambientados em um espaço de Hilbert. Nesse processo de codificação o canal sofre interferências denominadas *ruídos* causadas por operadores erro, que fazem com que o estado necessite passar pelo processo de medição, chamado *síndrome*, para que os erros ocasionados pelo ruído sejam identificados, possibilitando a recuperação do estado enviado.

De acordo com [51], algumas considerações devem ser feitas na construção da teoria que visa fornecer o processo de identificação de erro. Por exemplo, ao identificar erros em códigos quânticos, é importante tomar cuidado para identificar corretamente o subespaço para onde o estado quântico foi transportado. Para isso, é necessário garantir que todos os espaços vetoriais de destino sejam ortogonais e não deformados em relação ao espaço vetorial original de codificação. Isso é importante para que seja possível aplicar processos corretivos por meio da síndrome. Outro ponto importante acerca da estruturação de tal teoria é a de fazer o mínimo de suposições de modo a torná-la o mais geral. Nesse ponto, a referência [51] sugere que uma abordagem geral ocorre ao descrever o processo de ação do ruído como uma operação quântica E e o processo de recuperação como outra operação quântica R, sem fazer suposições sobre as etapas necessárias para a recuperação. Essa abordagem geral pode ser aplicada a diferentes tipos de códigos quânticos e sistemas quânticos em geral, tornando a teoria de correção de erros mais abrangente.

Para que o processo de correção seja bem-sucedido, é importante que qualquer estado quântico descrito por $|\psi\rangle$, que pode ser, sem perda de generalidade, representado na forma $\rho = |\psi\rangle\langle\psi|$, satisfaça a seguinte equação:

$$(R \circ E)\rho \propto \rho, \tag{5.43}$$

em que o símbolo $\propto$ é utilizado pelo fato de que em algumas ocasiões pode ocorrer de E não preservar o traço. Assim, para que a correção R tenha sucesso com probabilidade 1, pede-se que R preserve o traço ([2]). Portanto, os fatos mencionados até aqui permitem estabelecer as condições necessárias para garantir se um determinado código é capaz de corrigir os efeitos causados por determinado tipo de erro sobre um estado quântico, por

meio do próximo teorema. Sendo assim, tais condições funcionam como uma ferramenta útil na tarefa de se construir bons CQCE.

Teorema 5.19. *Seja $\mathcal{C}$ um código quântico e P um projetor sobre $\mathcal{C}$. Seja E uma operação quântica com elementos de operação $\{E_i\}$. Uma condição necessária e suficiente para a existência de uma operação de correção de erro R, corrigindo E sobre $\mathcal{C}$, é que:*

$$P \cdot E_i^{\dagger} \cdot E_j \cdot P = a_{ij} P, \tag{5.44}$$

*para alguma matriz hermitiana $A = [a_{ij}]$ de números complexos. Neste caso, os elementos de operação $\{E_i\}$ do ruído E são chamados de **erros**, e se existir tal operação R, diz-se que $\{E_i\}$ constitui um **conjunto de erros corrigíveis**([51]).*

5.3.6 Limitadores Quânticos de Hamming

Além das condições que foram apresentadas na Seção 5.3.5, existem outros critérios que são utilizados durante a construção de CQCE, a saber: o *limitante quântico de Hamming* e o *limitante quântico de Singleton*. Tais critérios fornecem restrições para a quantidade de erros que um CQCE, que possui determinadas características, pode corrigir em função de seus parâmetros, ou seja, comprimento, dimensão e distância mínima. A começar pelo limitante quântico de Hammig, considere a seguinte definição:

Definição 5.20. *Se $\mathcal{C}$ é um CQCE que admite uma matriz Hermitiana A que satisfaz a Eq. (5.44) e que tenha posto máximo, então $\mathcal{C}$ é denominado **CQCE não-degenerado**, caso contrário $\mathcal{C}$ é chamado de **CQCE degenerado**.*

Segundo [23, 51], a característica fundamental dos CQCE degenerados é a impossibilidade de se distinguir em que qubit ocorreu determinado erro utilizando tais códigos. Isso se deve ao fato de que o efeito do erro, para esta classe de códigos, é igual para diferentes qubits.

A definição dos CQCE não-degenerados se justifica devido ao fato de que o limitante de quântico de Hamming, que será apresentado em seguida, só é válido quando se consideram estes tipos de códigos quânticos. No entanto, [21] chama atenção para o fato de que o limitante de Hamming se verifica para todos os CQCE degenerados que se conhece, porém não existe prova geral que garante a sua validade sobre todos os códigos degenerados.

Teorema 5.21. *O limitante quântico de Hamming para um CQCE não-degenerado de comprimento n, dimensão k, e com capacidade de correção de erros t é dado por:*

$$\sum_{j=0}^{n} \binom{n}{j} 3^j 2^k \leq 2^n. \tag{5.45}$$

Nesse sentido, o limitante quântico de Hamming se torna uma ferramenta mais eficiente para garantir a existência ou não de um determinado código não-degenerado.

O limitante quântico de Singleton determina qual é o número máximo de erros que podem ser corrigidos por um CQCE qualquer. Desse modo segue o seguinte resultado:

Teorema 5.22. *Seja $\mathcal{C}$ um CQCE com parâmetros $[\![n, k, d]\!]_q$. Sendo assim, os parâmetros de $\mathcal{C}$ devem satisfazer a seguinte desigualdade:*

$$n - k \geq 2(d - 1). \tag{5.46}$$

*A desigualdade (5.46) é denominada de **limitante quântico de Singleton**. Diz-se que um código é **maximum distance separable** (MDS) se seus parâmetros satisfazem a inequação (5.46) com igualdade.*

As duas últimas seções desse capítulo dizem respeito a duas classes de CQCE que são temas de várias pesquisas: *códigos* CSS e os *códigos estabilizadores*.

5.4 Códigos CSS

Os códigos CSS são CQCE cuja denominação ocorre em homenagem a seus co-descobridores Robert Calderbank, Peter Shor e Andrew Steane [5] e [67], respectivamente. Esses códigos são interessantes porque ilustram como classes de códigos clássicos podem ser transformadas em classes de códigos quânticos. A obtenção de CQCE do tipo CSS é estabelecida por meio do próximo teorema, conhecido como *construção CSS* [4, 6, 26, 41, 51, 65].

Teorema 5.23. *Suponha que $\mathcal{C}_1$ e $\mathcal{C}_2$ sejam códigos lineares de $\mathbb{F}_q^n$ com parâmetros $[n, k_1, d_1]_q$ e $[n, k_2, d_2]_q$, respectivamente, tais que $\mathcal{C}_2 \subseteq \mathcal{C}_1$. Sendo assim, existe um código quântico $\mathcal{C} = [\![n, k_1 - k_2, d]\!]_q$. Neste caso, a distância mínima d de $\mathcal{C}$ é dada por:*

$$d = \min\{wt_H(c) \ : \ c \in (\mathcal{C}_1 \setminus \mathcal{C}_2) \cup (\mathcal{C}_2^{\perp_E} \setminus \mathcal{C}_1^{\perp_E})\} \geq \min\{d_1, d_2\}. \tag{5.47}$$

*Os códigos obtidos conforme $\mathcal{C}$ são denominados **códigos CSS**.*

Dessa forma, ao se considerar códigos auto-ortogonais Euclidianos, por meio do Teorema 5.23 se estabelece o próximo resultado.

Corolário 5.24. *Seja $\mathcal{C} \subset \mathbb{F}_q^n$ um código linear, com parâmetros $[n, k, d]_q$, auto-ortogonal com respeito ao produto interno euclidiano. Sendo assim, existe um código CSS com parâmetros $[\![n, n - 2k, d']\!]_q$, de forma que:*

$$d' = \min\{wt_H(c) \ : \ c \in \mathcal{C}^{\perp_E} \setminus \mathcal{C}\}, \tag{5.48}$$

em que d' é maior ou igual a distância de $\mathcal{C}^{\perp_E}$.

Exemplo 5.25. *Um exemplo muito conhecido de código CSS é o código de Steane [66]. Para obter tal código, considere o código linear $\mathcal{C} \subset \mathbb{F}_2^7$ cuja matriz geradora G é dada por:*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Note que G está na forma padrão, e que tal fato permite concluir que $dim(\mathcal{C}) = 4$. Dessa forma, de acordo com a Proposição 3.24 , segue que o código $\mathcal{C}^{\perp_E}$ é gerado pela matriz H, dada por:

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Perceba que quaisquer duas colunas de H formam um conjunto linearmente independente e que a 1ª coluna é uma combinação linear da 6ª e 7ª coluna. Sendo assim, de acordo com o Teorema 3.25, $d_H(\mathcal{C}) = 3$. Agora, observe que $H\dot{H}^T = 0$. Tal fato, de acordo com a proposição 3.24, mostra que $\mathcal{C}^{\perp_E} \subset \mathcal{C}$. Perceba também que, por definição, a matriz teste de paridade de $\mathcal{C}^{\perp_E}$ é G. Isso mostra que $d_H(\mathcal{C}^{\perp_E}) = 4$. Assim, tomando $\mathcal{C}_1 = \mathcal{C}$ e $\mathcal{C}_2 = \mathcal{C}^{\perp_E}$, tem-se que $\mathcal{C}_1 = [7, 4, 3]_2, \mathcal{C}_2 = [7, 3, 3]_2$ e $\mathcal{C}_2 \subset \mathcal{C}_1$. Logo a construção CSS garante que existe um código quântico quântico obtido por meio de $\mathcal{C}_1$ e $\mathcal{C}_2$ com parâmetros $[\![7, 1, 3]\!]_2$.

5.5 Códigos Estabilizadores

A seção anterior apresentou uma classe de CQCE que é a classe dos códigos CSS. Como foi visto, tais códigos podem ser obtidos por meio de códigos clássicos que possuem determinadas características. Nesse sentido, a presente seção tem por finalidade introduzir uma nova classe de CQCE. A classe a ser apresentada aqui contém a classe dos códigos CSS. Os códigos que pertencem a tal classe de CQCE são denominados *códigos estabilizadores*.

Para iniciar a discussão sobre os códigos estabilizadores, será feita uma discussão sobre o formalismo dos estabilizadores.

5.5.1 Formalismo dos Estabilizadores

Esta seção tem como base as referências [49, 50] e [71]. Na Seção 5.3.1 foram introduzidas os operadores de Pauli. Estes operadores determinam um grupo multiplicativo, chamado de **Grupo de Pauli** e denotado por $\mathcal{P}_1$, de modo que:

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}. \tag{5.49}$$

Nesse caso, os elementos de $\mathcal{P}_1$ agem sobre um único qubit. Por meio do produto tensorial estende-se a noção de grupo de Pauli definindo-se o grupo multiplicativo $\mathcal{P}_n$, denominado **grupo de Pauli que age sobre n-qubits**. O grupo $\mathcal{P}_n$ é definido da seguinte forma:

$$\mathcal{P}_n = \{i^\lambda M_1 \otimes M_2 \otimes \cdots \otimes M_n \ : \ M_j \in \{I, X, Y, Z\}, \text{ e } \lambda \in \{0, 1, 2, 3\}\}. \tag{5.50}$$

Note que $X \cdot Z = iY$. Sendo assim, dado $M \in \mathcal{P}_n$ tem-se que:

$$M = i^\lambda \bigotimes_{j=1}^{n} \left(X^{a_j} \cdot Z^{b_j}\right), \tag{5.51}$$

em que $a_j, b_j \in \{0, 1\}$ [71].

Mediante a representação dada na Eq. 5.51, considere as seguintes aplicações:

$$\begin{aligned} \Psi_X : \mathcal{P}_n &\longrightarrow \mathbb{F}_2^n \\ M &\mapsto \Psi_X \left(i^\lambda \bigotimes_{j=1}^{n} \left(X^{a_j} \cdot Z^{b_j} \right) \right) = (a_1, \ldots, a_n). \end{aligned} \tag{5.52}$$

$$\begin{aligned} \Psi_Z : \mathcal{P}_n &\longrightarrow \mathbb{F}_2^n \\ M &\mapsto \Psi_Z \left(i^\lambda \bigotimes_{j=1}^{n} \left(X^{a_j} \cdot Z^{b_j} \right) \right) = (b_1, \ldots, b_n). \end{aligned} \tag{5.53}$$

Sendo assim, por meio das aplicações (5.52) e (5.53), define-se um homomorfismo $\Psi : \mathcal{P}_n \longrightarrow \mathbb{F}_2^{2n}$, de modo que:

$$\begin{aligned} \Psi : \mathcal{P}_n &\longrightarrow \mathbb{F}_2^{2n} \\ M &\mapsto (\Psi_X(M), \Psi_Z(M)) = (a_1, \ldots, a_n, b_1, \ldots, b_n). \end{aligned} \tag{5.54}$$

Para que se consiga um isomorfismo por meio de Ψ, considera-se o grupo quociente:

$$\tilde{\mathcal{P}_n} = \mathcal{P}_n / \{\pm 1, \pm i\}, \tag{5.55}$$

e define-se:

$$\begin{aligned} \tilde{\Psi} : \mathbb{F}_2^{2n} &\longrightarrow \tilde{\mathcal{P}_n} \\ (\alpha|\beta) &\mapsto \bigotimes_{j=1}^{n} \left(X^{a_j} \cdot Z^{b_j} \right), \end{aligned} \tag{5.56}$$

de modo que $\alpha = (a_1, \ldots, a_n)$ e $\beta = (b_1, \ldots, b_n)$. De acordo com a aplicação (5.56), segue a identificação dos operadores de Pauli:

$$I := \tilde{\Psi}(0|0),\ X := \tilde{\Psi}(1|0),\ Y := \tilde{\Psi}(1|1),\ Z := \tilde{\Psi}(0|1). \tag{5.57}$$

Observe que, da definição de comutador e anticomutador apresentadas na Defnição 5.13, segue que:

$$[X, Y] = 2iZ,\ \ [Y, Z] = 2iX,\ \ [Z, X] = 2iY. \tag{5.58}$$

No entanto, para $n > 1$ é possível mostrar que se M e N pertencem a $\mathcal{P}_n$, então:

$$[M, N] = 0 \text{ ou } \{M, N\} = 0. \tag{5.59}$$

Ou seja, os elementos de $\mathcal{P}_n$ comutam ou anticomutam quando $n > 1$. De fato, sejam $M, N \in \mathcal{P}_n$. Considerando-se a Eq. 5.51 segue que:

$$M = i^\lambda \bigotimes_{j=1}^{n} \left(X^{a_j} \cdot Z^{b_j} \right) \text{ e } N = i^{\lambda'} \bigotimes_{j=1}^{n} \left(X^{a'_j} \cdot Z^{b'_j} \right), \tag{5.60}$$

donde:

$$\begin{aligned}
M \cdot N &= \left(i^{\lambda} \bigotimes_{j=1}^{n} \left(X^{a_j} \cdot Z^{b_j} \right) \right) \cdot \left(i^{\lambda'} \bigotimes_{j=1}^{n} \left(X^{a'_j} \cdot Z^{b'_j} \right) \right) \\
&= i^{\lambda+\lambda'} \left(\bigotimes_{j=1}^{n} X^{a_j} \cdot \bigotimes_{j=1}^{n} Z^{b_j} \right) \cdot \left(\bigotimes_{j=1}^{n} X^{a'_j} \cdot \bigotimes_{j=1}^{n} Z^{b'_j} \right) \\
&= i^{\lambda+\lambda'} (-1)^{\sum a'_j b_j} \bigotimes_{j=1}^{n} X^{a_j} \cdot \left(\bigotimes_{j=1}^{n} X^{a'_j} \cdot \bigotimes_{j=1}^{n} Z^{b'_j} \right) \cdot \bigotimes_{j=1}^{n} Z^{b'_j} \\
&= i^{\lambda+\lambda'} (-1)^{\sum a'_j b_j} \left(\bigotimes_{j=1}^{n} X^{a'_j} \cdot \bigotimes_{j=1}^{n} X^{a_j} \right) \cdot \left(\bigotimes_{j=1}^{n} Z^{b_j} \cdot \bigotimes_{j=1}^{n} Z^{b'_j} \right) \\
&= i^{\lambda+\lambda'} (-1)^{\sum (a'_j b_j + a_j b'_j)} \left(\bigotimes_{j=1}^{n} X^{a'_j} \cdot \bigotimes_{j=1}^{n} Z^{b'_j} \right) \cdot \left(\bigotimes_{j=1}^{n} X^{a_j} \cdot \bigotimes_{j=1}^{n} Z^{b_j} \right) \\
&= (-1)^{\sum (a'_j b_j + a_j b'_j)} N \cdot M. \qquad (5.61)
\end{aligned}$$

Ou seja, considerando a identificação:

$$M \leftrightarrow (\Psi_X(M), \Psi_Z(M)) \text{ e } N \leftrightarrow (\Psi_X(N), \Psi_Z(N)), \qquad (5.62)$$

a Eq. (5.61) implica em:

$$M \cdot N = (-1)^{\langle \Psi_X(M), \Psi_Z(N) \rangle_E + \langle \Psi_X(N), \Psi_Z(M) \rangle_E} N \cdot M \qquad (5.63)$$

A identificação realizada em (5.57) estabelecerá a relação importante entre matrizes binárias e a próxima classe de CQCE que será apresentada a seguir.

Definição 5.26. *Considere um estado qualquer $|u\rangle \in \mathbb{C}^{2^n}$ e $M \in \mathcal{P}_n$ um operador qualquer agindo em $|u\rangle$. Assim, $|u\rangle$ é estabilizado pelo operador M se $M|u\rangle = |u\rangle$. Neste caso, M é denominado* ***operador estabilizador*** *em relação a $|u\rangle$.*

Exemplo 5.27. *Considere o operador $X_1 Z_2 Z_3 \in \mathcal{P}_3$. Note que $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$ e $Z|0\rangle = |0\rangle$. Dessa forma, tomando em $\mathbb{C}^{2^3}$, o estado $|u\rangle$, dado por:*

$$|u\rangle = \frac{|000\rangle + |100\rangle}{\sqrt{2}},$$

segue que:

$$\begin{aligned}
X_1 Z_2 Z_3 |u\rangle &= \frac{X|0\rangle \otimes Z|0\rangle \otimes Z|0\rangle + X|1\rangle \otimes Z|0\rangle \otimes Z|0\rangle}{\sqrt{2}} \qquad (5.64) \\
&= \frac{|1\rangle \otimes |0\rangle \otimes |0\rangle + |0\rangle \otimes |0\rangle \otimes |0\rangle}{\sqrt{2}} \qquad (5.65) \\
&= |u\rangle.
\end{aligned}$$

Isso significa que $|u\rangle$ é estabilizado pelo operador $X_1 Z_2 Z_3$.

Definição 5.28. *Considere o grupo de Pauli $\mathcal{P}_n$. Um **grupo estabilizador** $\mathcal{S}$ de $\mathcal{P}_n$ é um subgrupo multiplicativo abeliano de $\mathcal{P}_n$ que não contém $-I$. Neste caso, diz-se que um conjunto $\{M_1, \ldots, M_l\} \subset \mathcal{S}$ de elementos linearmente independentes é um **gerador** de $\mathcal{S}$, e utiliza-se a notação:*

$$\mathcal{S} = \langle M_1, \ldots, M_l \rangle, \tag{5.66}$$

se todo elemento de $\mathcal{S}$ pode ser escrito como um produto tensorial dos elementos de $\{M_1, \ldots, M_l\}$.

Tendo em vista a Definição 5.28, segue a definição de código estabilizador.

Definição 5.29. *Seja $\mathcal{S}$ um grupo estabilizador de $\mathcal{P}_n$. O **código estabilizador** $\mathcal{C}_\mathcal{S}$ associado ao grupo estabilizador $\mathcal{S}$ é o autoespaço simultâneo com autovalor 1 de todos os elementos de $\mathcal{S}$. Isto é:*

$$\mathcal{C}_\mathcal{S} = \{|u\rangle \in \mathbb{C}^{2^n} : M|u\rangle = |u\rangle, \ \forall\, M \in \mathcal{S}\}. \tag{5.67}$$

Para ilustrar as Definições 5.28 e 5.29, considere o seguinte exemplo.

Exemplo 5.30. *Considerando o grupo de Pauli para dois qubits $\mathcal{P}_2$, tome os operadores:*

$$X \otimes X = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad e \quad Z \otimes Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Observe que $[X \otimes X, Z \otimes Z] = 0$ e $(X \otimes X)^2 = (Z \otimes Z)^2 = I \otimes I = I^{\otimes^2}$. Além disso, segue que $\langle XX, ZZ \rangle = \{I^{\otimes^2}, X \otimes X, Z \otimes Z, X \otimes X \cdot ZZ\}$. Portanto, $\mathcal{S} = \langle X \otimes X, Z \otimes Z \rangle$ é um grupo estabilizador de $\mathcal{P}_2$. Perceba que o autoespaço associado a 1 para o operador XX é gerado pelos estados $|00\rangle + |11\rangle$ e $|01\rangle + |11\rangle$ e para o operador ZZ o autoespaço associado a 1 é gerado pelos estados $|00\rangle$ e $|11\rangle$. Dessa forma, temos que código estabilizador $\mathcal{C}_S$ é o espaço gerado por $|00\rangle + |11\rangle$.

Perceba que o conjunto definido em (5.67) sugere a motivação para a denominação estabilizador, uma vez que a Definição 5.29 mostra que tais códigos estão relacionados com estados que são fixados (permanecem estáveis) mediante a aplicação de determinado grupo de operadores. A função dos geradores para os códigos estabilizadores está no fato de que eles, muitas vezes, atuam como uma ferramenta que auxilia a verificar se um determinado estado pertence ou não ao código. Pois, se para um grupo estabilizador $\mathcal{S}$ tem-se $\mathcal{S} = \langle M_1, \ldots, M_l \rangle$, basta verificar se $|u\rangle$ é fixado por cada M_i com $i \in \{1, \ldots, l\}$ para concluir que $|u\rangle \in \mathcal{C}_\mathcal{S}$. Desse modo, percebe-se uma semelhança entre os códigos estabilizadores e os códigos lineares clássicos uma vez que o conjunto gerador tem a mesma utilidade da matriz de verificação. Em outras palavras, de acordo com tal fato, pode-se considerar que os códigos estabilizadores são caracterizados em função de seus geradores. Com o objetivo de explorar os parâmetros de um código estabilizador, segue o primeiro resultado.

Teorema 5.31. *Seja $\mathcal{C}_{\mathcal{S}}$ um código estabilizador de modo que $\mathcal{S}$ possua $n-k$ geradores. Dessa forma segue que a dimensão de $\mathcal{C}_{\mathcal{S}}$ é igual a 2^k.*

Para explorar o conceito de distância mínima associado aos códigos estabilizadores, é necessário definir o que se entende por *operador erro*.

Definição 5.32. *Um **operador erro** E é um operador de $\mathcal{P}_n$ que leva um estado $|u\rangle \in \mathbb{C}^{2^n}$ a um estado corrompido $E|u\rangle$, isto é, um estado que não é estabilizado por E.*

Assim, dado um código estabilizador $\mathcal{C}_{\mathcal{S}}$, de acordo com a definição de operador de Pauli, um operador erro E comuta ou anticomuta com cada um geradores pertencentes a $\mathcal{S}$. Dessa forma, tem-se que:

$$(M_i \cdot E)|u\rangle = \begin{cases} E|u\rangle, \Rightarrow \text{erro não detectável;} \\ -E|u\rangle, \Rightarrow \text{erro detectável.} \end{cases} . \tag{5.68}$$

Com isso, para que $\varepsilon = \{E_\lambda\} \subset \mathcal{P}_n$ seja um conjunto de operadores erros que podem ser corrigidos pelo código estabilizador, deve-se ter:

$$E_{\lambda_i}^{\dagger} \cdot E_{\lambda_j} \notin \mathcal{N}(\mathcal{S}) \setminus \mathcal{S}, \ \ \forall\, E_{\lambda_i}, E_{\lambda_j} \in \varepsilon, \tag{5.69}$$

em que $\mathcal{N}(\mathcal{S})$ é o *normalizador* de $\mathcal{S}$ em $\mathcal{P}_n$ de modo que:

$$\mathcal{N}(\mathcal{S}) = \{N \in \mathcal{P}_n : N^{\dagger} \cdot M \cdot N \in \mathcal{S}, \ \forall\, M \in \mathcal{S}\}. \tag{5.70}$$

Dessa forma, é possível observar que $N(\mathcal{S})$ é, na verdade, a coleção de todos os operadores de $\mathcal{P}_n$ que comutam com $\mathcal{S}$, ou seja, no caso binário o normalizador é igual ao centralizador de $\mathcal{S}$. De fato, se $N \in \mathcal{N}(\mathcal{S})$, então segue que, para qualquer $M \in \mathcal{S}$:

$$N^{\dagger} \cdot M \cdot N = \pm N^{\dagger} \cdot N \cdot M = \pm M \Rightarrow M \cdot N = \pm N \cdot M. \tag{5.71}$$

Sabendo que a última equação dada em (5.71) é verdadeira para qualquer $M \in \mathcal{S}$ e que $-I \notin \mathcal{S}$, segue que $N \in \mathcal{N}(\mathcal{S})$ se, e só se $[N, M] = 0$, para todo $M \in \mathcal{S}$.

A distância de um código estabilizador é definida por meio do peso de Hamming e do homomorfismo Ψ estabelecido em (5.54).

Definição 5.33. *Seja $M \in \mathcal{P}_n$, e considere o vetor binário associado a M dado por $\Psi(M) = (\Psi_X(M), \Psi_Z(M))$. Com isso, define-se o **peso quântico** de M, denotado por $W_Q(M)$, da seguinte forma:*

$$W_Q(M) = wt_H(\Psi_X(M)) + wt_H(\Psi_Z(M)) - \langle \Psi_X(M), \Psi_Z(M) \rangle_E. \tag{5.72}$$

Note que $W_Q(M)$ é igual ao número de fatores que são diferentes do operador de Pauli I quando consideramos a representação de M como produto tensorial de elementos de $\mathcal{P}_1$.

Exemplo 5.34. *Considere em $\mathcal{P}_6$ o operador $M = X_1Z_3Y_4X_5Z_5$. Note que o número de fatores diferentes da identidade na representação de M é igual a 5. Ao se representar M conforme (5.51), tem-se que:*

$$M = i(X^1 \cdot Z^0) \otimes (X^0 \cdot Z^0) \otimes (X^0 \cdot Z^1) \otimes (X^1 \cdot Z^1) \otimes (X^1 \cdot Z^0) \otimes (X^0 \cdot Z^1).$$

Assim, utilizando a definição 5.33, segue que:

$$W_Q(M) = wt_H(1,0,0,1,1,0) + wt_H(0,0,1,1,0,1) - \langle (1,0,0,1,1,0), (0,0,1,1,0,1) \rangle_E.$$
$$\Rightarrow W_Q(M) = 5.$$

Diante destes fatos, a distância mínima de um código estabilizador é dada por:

$$d = \min\{W_Q(E) : E \in \mathcal{N}(\mathcal{S}) \setminus \mathcal{S}\}, \tag{5.73}$$

A partir de agora, a notação $[\![n, k, d]\!]$ será usada para representar os parâmetros de um código estabilizador. Esta notação difere da apresentada em (5.23) no subíndice.

Exemplo 5.35. *No exemplo 5.30, observa-se que $\mathcal{C}_\mathcal{S} = [\![2, 0, 2]\!]$. Além disso, temos que esse código atinge a distância máxima de acordo com o limitante (5.46).*

Agora, suponha que $\mathcal{C}_\mathcal{S}$ seja um código estabilizador com grupo estabilizador dado por $\mathcal{S} = \langle M_1, \ldots, M_{n-k} \rangle \subset \mathcal{P}_n$. Ao considerar $\mathcal{S}$ e a identificação dada em (5.57), pode-se associar à $\mathcal{C}_\mathcal{S}$ uma matriz binária da forma:

$$H = \begin{bmatrix} \Psi(M_1) \\ \Psi(M_2) \\ \vdots \\ \Psi(M_{n-k}) \end{bmatrix} = \begin{bmatrix} (\Psi_X(M_1), \Psi_Z(M_1)) \\ (\Psi_X(M_2), \Psi_Z(M_2)) \\ \vdots \\ (\Psi_X(M_{n-k}), \Psi_Z(M_{n-k})) \end{bmatrix} = [H_X \,|\, H_Z], \tag{5.74}$$

onde as matrizes H_X, H_Z são matrizes de ordem $(n-k)\times n$ que cujas linhas correspondem aos vetores binários dados por $\Psi_X(M_i)$ e $\Psi_Z(M_i)$, respectivamente. Logo, se $\mathcal{S}$ é um grupo estabilizador para um código $\mathcal{C}_S$ e M, N são dois geradores de $\mathcal{S}$, como $\mathcal{S}$ é um subgrupo de $\mathcal{P}$, segue-se de (5.63) a seguinte igualdade:

$$\langle \Psi_X(M), \Psi_Z(N) \rangle_E + \langle \Psi_X(N), \Psi_Z(M) \rangle_E = 0 \mod 2 \tag{5.75}$$

Dessa forma, a matriz $[H_X \,|\, H_Z]$ dada em (5.74) deve atender a seguinte condição:

$$H_X \cdot H_Z^T + H_Z \cdot H_X^T = 0 \mod 2 \tag{5.76}$$

Sendo assim, segue a próxima definição.

Definição 5.36. *Dado um grupo estabilizador $\mathcal{S} = \langle M_1, \ldots, M_{n-k} \rangle \subset \mathcal{P}_n$, com $n > 1$, a matriz binária H, obtida por através dos geradores de $\mathcal{S}$ conforme o que foi estabelecido em 5.74, é denominada* ***matriz de paridade quântica*** *associada a $\mathcal{S}$. E a Eq. (5.76) é denominada como* ***condição SIP*** *.*

A denominação condição SIP se deve a abreviação do termo em inglês *Symplectic Inner Product*, uma vez que, para o caso binário, a Eq. (5.75) que justifica a Eq. (5.76) equivale ao produto interno simplético definido em (4.20).

Observe que a matriz de paridade quântica pode auxiliar na determinação da distância mínima de um código estabilizador. Suponha que $E \in \mathcal{N}(\mathcal{S}) \setminus \mathcal{S}$. Sendo assim, tem-se que E comuta com todos os elementos de $\mathcal{S}$ e não pertence a $\mathcal{S}$. Pelo fato de comutar com todos os elementos de $\mathcal{S}$, e considerando a matriz de paridade $[H_X \mid H_Z]$ deve-se ter:

$$H_X \cdot \Psi_Z(E)^T + H_Z \cdot \Psi_X(E)^T = 0 \mod 2 \tag{5.77}$$

Dessa forma, a distância mínima do código $\mathcal{C}_S$ pode ser interpretada como o mínimo dos pesos quânticos dos elementos $E \in \mathcal{P}_n$ que satisfazem (5.77) e que não podem ser escritos como uma combinação linear dos geradores de $\mathcal{S}$. Maiores detalhes relacionados com o tratamento de códigos estabilizadores por meio de matrizes binárias podem ser encontrados em [16, 35, 48, 59, 71].

No início desta seção foi mencionado que os códigos CSS são uma subclasse dos códigos estabilizadores. Tal fato permite mostrar que a matriz de paridade associada a um código CSS obtido por meio de códigos clássicos $\mathcal{C}_1$ e $\mathcal{C}_2$ que atendem a condição $\mathcal{C}_2 \subseteq \mathcal{C}_1$, é dada por:

$$\left[\begin{array}{c:c} G(\mathcal{C}_2) & 0 \\ \hdashline 0 & H(\mathcal{C}_1) \end{array}\right]_{(n-k_1+k_2)\times 2n}, \tag{5.78}$$

sendo $G(\mathcal{C}_2)$ a matriz geradora de $\mathcal{C}_2$ e $H(\mathcal{C}_1)$ representa a matriz de verificação de paridade de um código $\mathcal{C}_1$ ([48]). Nesta situação a condição SIP é dada por:

$$G(\mathcal{C}_2) \cdot H(\mathcal{C}_1)^T = 0. \tag{5.79}$$

Exemplo 5.37. *Assim sendo, retomando o Exemplo 5.25, temos que uma matriz de paridade quântica para o código de 7 qubits de Steane é dada por:*

$$\left[\begin{array}{ccccccc:ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right].$$

De tal forma que o grupo estabilizador $\mathcal{S} \subset \mathcal{P}_7$ para este código possui 6 geradores que são dados por $M_1 = X_4X_5X_6X_7,\ M_2 = X_2X_3X_6X_7,\ M_3 = X_1X_3X_5X_7,\ M_4 = Z_4Z_5Z_6Z_7,\ M_5 = Z_2Z_3Z_6Z_7$ e $M_6 = Z_1Z_3Z_5Z_7$.

CAPÍTULO 6

CÓDIGOS ESTABILIZADORES VIA PEF $\mathbb{F}_{2^r}^2$

Este Capitulo tem como objetivo mostrar como utilizar a teoria que foi desenvolvida no Capítulo 4 combinada com os conceitos de códigos quânticos apresentados no Capítulo 5 para apresentando algumas construção de códigos estabilizadores. Como o número de colunas das matrizes norma são dados como potência de 2, os exemplos que serão dados apresentam operadores que possuem, em sua representação, um produto de kronecker que possui muitos fatores.

6.1 Códigos CSS via PEF $\mathbb{F}_{2^r}^2$

A primeira forma de se construir códigos quânticos utilizando o PEF $\mathbb{F}_{2^r}^2$ será por meio da construção CSS introduzida pelo Teorema 5.23. Recorde-se que, pelo Teorema 4.24, os códigos $\mathcal{C}(uv)$ são auto-ortogonais Euclidianos, isto é $\mathcal{C}(uv) \subset (\mathcal{C}(uv))^{\perp_E}$. Desse modo utilizando o Corolário 5.24 é possível utilizar os códigos $\mathcal{C}(uv)$ para obter códigos quânticos utilizando a construção CSS.

Exemplo 6.1. *Considere a matriz $N(12)$ dada em (4.21) que aparece no Exemplo 4.11, e que foi obtida via* PEF $\mathbb{F}_4^2$.

$$N(12) = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Perceba que a 4ª linha de $N(12)$ é combinação linear das outras três primeiras linhas. Nesse sentido, ao se retirar a 4ª linha de $N(12)$, obtém-se uma matriz $G(12)$, que é dada por:

$$G(12) = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Note que as linhas de $G(12)$, formam um conjunto linearmente independente. Sendo assim, segue que a $G(12)$ gera um código linear $\mathcal{C}(12)$ que possui parâmetros $[16, 3, 8]_2$ e que está contido no seu dual Euclidiano $\mathcal{C}^{\perp_E}(12)$ que, por sua vez, possui parâmetros $[16, 13, 2]_2$. Logo, considerando o Corolário 5.24, conclui-se que por meio da matriz $N(12)$ é possível garantir a existência de um CQCE, denotado por $\mathcal{C}_2(12)$ em que o subíndice indica o parâmetro $r = 2$, tal que $\mathcal{C}_2(12) = [\![16, 10, 2]\!]$. A matriz de paridade quântica de $\mathcal{C}_2(12)$ é dada por (6.1). Ou seja, o grupo estabilizador de $\mathcal{C}_2(12)$ é gerado por 6 estabilizadores pertencentes a $\mathcal{P}_{16}$ que são apresentados na Tabela 6.1.

Tomando como base o Exemplo 6.1 segue a Tabela 6.2 que apresenta os parâmetros e os grupos estabilizadores dos códigos quânticos obtidos com o auxilio do PEF $\mathbb{F}_4^2$ por meio da construção CSS.

A Tabela 6.2 mostra que os códigos quânticos obtidos pela construção CSS através das matrizes norma $N(uv)$ que estão associadas ao PEF $\mathbb{F}_4^2$ possuem distância mínima igual a 2. Percebe-se também que, para tais códigos vistos como códigos estabilizadores são gerados por operadores que pertencem a $\mathcal{P}_{16}$, isto é, operadores que agem sobre 16 qubits.

Na sequência será introduzida uma definição que mostrará que as matrizes normas atendem a condição SIP e, portanto, por meio delas é possível obter códigos estabilizadores por meio de uma outra construção diferente da CSS.

Definição 6.2. *Dada a matriz norma $N(uv)$ denote por $N_X(uv)$ e $N_Z(uv)$ as matrizes de ordem $2^r \times 2^{2r-1}$ obtidas ao se considerar as primeiras 2^{2r-1} colunas e as 2^{2r-1} últimas colunas de $N(uv)$, respectivamente. Com isso, obtém-se mais uma representação matricial de $N(uv)$, de modo que:*

$$N(uv) = [N_X(uv) \mid N_Z(uv)]. \tag{6.2}$$

*As matrizes $N_X(uv)$ e $N_Z(uv)$ serão denominadas, respectivamente, **parte** X e **parte** Z da matriz norma $N(uv)$.*

Observe que no Capítulo 4 foi demonstrado no Teorema 4.24 que as matrizes $N(uv)$, satisfazem são auto ortogonais simpléticas. Sendo assim, considerando tal fato e a representação das matrizes norma conforme a Eq. (6.2), segue que:

$$\begin{aligned} N(uv) \cdot \Omega_{2^{2r-1}} \cdot N(uv)^T &= 0 \\ [N_X(uv) \mid N_Z(uv)] \cdot \Omega_{2^{2r-1}} \cdot [N_X(uv) \mid N_Z(uv)]^T &= 0 \\ [N_X(uv) \mid N_Z(uv)] \cdot \left[\begin{array}{c:c} 0 & I \\ \hdashline -I & 0 \end{array}\right] \cdot \left[\begin{array}{c} (N_X(uv))^T \\ \hdashline (N_Z(uv))^T \end{array}\right] &= 0. \end{aligned} \tag{6.3}$$

$$\left[\begin{array}{cccccccccccccccc|cccccccccccccccc}
0&0&1&1&0&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&1&1&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&1&0&0&0&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&1&1&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&1&0&0&1&1&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&1&1&0&0&1&1
\end{array}\right] \quad (6.1)$$

Tabela 6.1: *Geradores do grupo estabilizador do código CSS $\mathcal{C}_2(12)$.*

gerador	operador
M_1	$X_3X_4X_7X_8X_9X_{10}X_{13}X_{14}$
M_2	$X_1X_2X_7X_8X_{11}X_{12}X_{13}X_{14}$
M_3	$X_1X_2X_5X_6X_{11}X_{12}X_{15}X_{16}$
M_4	$Z_3Z_4Z_7Z_8Z_9Z_{10}Z_{13}Z_{14}$
M_5	$Z_1Z_2Z_7Z_8Z_{11}Z_{12}Z_{13}Z_{14}$
M_6	$Z_1Z_2Z_5Z_6Z_{11}Z_{12}Z_{15}Z_{16}$

Como as matrizes em questão estão definidas sobre $\mathbb{F}_2$, segue da Eq. (6.3) que:

$$\left[N_Z(uv) \,\vdots\, N_X(uv)\right] \cdot \begin{bmatrix} (N_X(uv))^T \\ \hdashline (N_Z(uv))^T \end{bmatrix} = 0.$$

$$N_Z(uv) \cdot N(uv)_X^T + N_X(uv) \cdot N_Z(uv)^T = 0. \tag{6.4}$$

Assim, considerando a Definição 6.2 e a Eq. (6.4) chega-se ao próximo resultado que representa mais uma das contribuições originais do presente trabalho.

Corolário 6.3. *Dada a matriz norma $N(uv)$ segue que a parte X e a parte Z de N(uv), satisfazem à condição SIP, isto é:*

$$N_X(uv) \cdot N_Z(uv)^T + N)_Z(uv \cdot N_X(uv)^T \cong 0 \mod 2. \tag{6.5}$$

Exemplo 6.4. *Considerando mais uma vez o PEF $\mathbb{F}_4^2$ obtido conforme o Exemplo 4.11, tome a matriz norma $N(02)$ dada por:*

$$N(02) = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Perceba que ao se retirar a última linha de $N(02)$ obtém-se a matriz $N'(02)$ cujas linhas formam um conjunto linearmente independente, de modo que:

$$N'(02) = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

O número de colunas de $N'(02)$ é igual a 16 e a parte X e a parte Z de $N'(02)$, segue que:

$$N'_X(02) = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \quad e \quad N'_Z(02) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Observe que $N'_X(02) \cdot N'_Z(02)^T + N'_Z(02) \cdot N'_X(02)^T \cong 0 \mod 2$. Isso mostra que a matriz $N'(02)$ pode ser vista como uma matriz de paridade quântica. Nesse caso, cada linha de $N'(02)$ será vista como um operador de $\mathcal{P}_8$, de modo que tais operadores são dados por: $M_1 = Z_1X_2X_3Z_4X_5Z_6Z_7X_8$, $M_2 = Z_1X_2X_3Z_4Z_5X_6X_7Z_8$ e $M_3 = X_1Z_2Z_3X_4Z_5X_6X_7Z_8$. Assim, o código estabilizador $\mathcal{C}_{\mathcal{S}}(02)$ associado ao grupo estabilizador $\mathcal{S} = \langle M_1, M_2, M_3 \rangle$ possui parâmetros $[\![8, 5, 2]\!]$.

Seguindo os passos do Exemplo 6.4 foi possível determinar todos os códigos estabilizadores construídos por meio das matrizes normas construídas via PEF $\mathbb{F}_4^2$, considerando o Corolário 6.3 e tais códigos são apresentados na Tabela 6.3.

Perceba que os códigos $C_{\mathcal{S}}(*2)$ e $C_{\mathcal{S}}(01)$ apresentados na tabela 6.3 apresentam a distância máxima permitida de acordo com o limitante quântico de Singleton. Tais tipos de códigos são classificados em [27] como *QMDS* abreviação em inglês de *Quantum Maximum Distance Separable*. Ou seja, a distância entre os elementos dos códigos $C_{\mathcal{S}}(*2)$ e $C_{\mathcal{S}}(01)$ atinge o maior valor possível. Mais detalhes sobre códigos QMDS podem ser encontrados em [27] e [32].

Seguindo a linha de raciocínio de se obter códigos estabilizadores por meio de matrizes que atendam a condição SIP que sejam obtidas através da teoria desenvolvida no Capítulo 4, é apresentada a próxima definição.

Definição 6.5. *Considerando as matrizes normas $N(uv)$ e $N(\zeta\eta)$, definimos a matriz $N(uv : \zeta\eta)$, denominada **matriz dupla norma** em relação aos pares (u, v) e (ζ, η), de modo que:*

$$N(uv : \zeta\eta) = \left[\begin{array}{c} N(uv) \\ \hdashline N(\zeta\eta) \end{array}\right] = \left[\begin{array}{c:c} N_X(uv) & N_Z(uv) \\ \hdashline N_X(\zeta\eta) & N_Z(\zeta\eta) \end{array}\right]. \tag{6.6}$$

O exemplo que se segue mostra que as matrizes dupla norma podem ser uteis para obter códigos quânticos com uma distância maior.

Exemplo 6.6. *Agora, considere $r = 3$ para tomar matrizes normas construídas com o auxilio do* PEF $\mathbb{F}_8^3$. *Nesse caso, o polinômio usado para se obter* PEF $\mathbb{F}_8^3$ *é o polinômio $f(x) = x^3 + x + 1$. Desse modo, o código estabilizador que é obtido tomando-se em* PEF $\mathbb{F}_8^3$ *a matriz norma $N(*0)$ é o código $\mathcal{C}_{\mathcal{S}(*0)}$ cujo grupo estabilizador $\mathcal{S}(*0)$ possui*

os seguintes geradores:

$$
\begin{aligned}
M_1 &= X_1X_2Z_3Z_5X_{10}Z_{14}Z_{15}X_{19}X_{21}Z_{22}Z_{23}Y_{28}Y_{32};\\
M_2 &= Y_4Y_8X_9X_{10}Z_{11}Z_{13}X_{17}Z_{18}Z_{22}Z_{23}X_{27}X_{29}Z_{30}Z_{31};\\
M_3 &= Z_3Z_5X_6X_7Y_{12}Y_{16}X_{18}Z_{19}Z_{21}X_{25}X_{26}Z_{30}Z_{31};\\
M_4 &= Z_1Z_2X_6X_7Z_{11}Z_{13}X_{14}X_{15}Y_{20}Y_{24}X_{25}X_{26}Y_{27}Z_{29};\\
M_5 &= Z_1Z_2X_3X_5Z_9Z_{10}X_{14}X_{15}Z_{19}Z_{21}Z_{22}Z_{23}Y_{28}Y_{32};\\
M_6 &= Y_4Y_8Z_9Z_{10}X_{11}X_{13}Z_{17}Z_{18}X_{22}X_{23}Z_{27}X_{29}X_{30}X_{31};\\
M_7 &= X_3X_5Z_6Z_7Y_{12}Y_{16}Z_{17}Z_{18}X_{19}X_{21}Z_{25}Z_{26}X_{30}X_{31}.
\end{aligned}
$$

Assim, segue que $\mathcal{C}_{\mathcal{S}(*0)} = [\![32, 25, 2]\!]$. E considerando a matriz $N(*1)$ gera um código estabilizador $\mathcal{C}_{\mathcal{S}(*1)}$, cujo grupo estabilizador $\mathcal{S}(*1)$ tem como geradores os seguintes operadores:

$$
\begin{aligned}
N_1 &= X_1Z_5X_6Z_8Z_9X_{10}Z_{14}X_{15}Z_{18}X_{19}X_{20}Z_{32}X_{27}X_{28}Z_{29}Z_{32};\\
N_2 &= Z_3Z_4X_5X_8X_9Z_{13}X_{14}Z_{16}Z_{17}X_{18}Z_{22}X_{23}Z_{26}X_{27}X_{28}Z_{31};\\
N_3 &= X_2Z_3Z_4X_7Z_{11}Z_{12}X_{13}X_{16}X_{17}Z_{21}X_{22}Z_{24}Z_{25}X_{26}Z_{30}X_{31};\\
N_4 &= X_1Z_2X_6Z_7X_{10}Z_{11}Z_{12}X_{15}Z_{19}Z_{20}X_{21}X_{24}X_{25}Z_{29}X_{30}X_{32};\\
N_5 &= Z_1X_5Z_6X_8X_9Z_{10}X_{14}Z_{15}X_{18}Z_{19}Z_{20}X_{23}Z_{27}Z_{28}X_{29}X_{32};\\
N_6 &= X_3X_4Z_5Z_8Z_9X_{13}Z_{14}X_{16}X_{17}Z_{18}X_{22}X_{23}X_{26}Z_{27}Z_{28}X_{31};\\
N_7 &= Z_2X_3X_4Z_7X_{11}X_{12}Z_{13}Z_{16}Z_{17}X_{21}X_{22}X_{24}X_{25}Z_{26}X_{30}Z_{31}.
\end{aligned}
$$

Com isso, tem-se que $\mathcal{C}_{\mathcal{S}(*1)} = [\![32, 25, 2]\!]$. Agora, levando-se em conta a Definição 6.5, tem-se que a matriz dupla norma $N(*0 : *1)$ atende a condição SIP quando vista sob a forma da expressão 6.6. Sendo assim, $N(*0 : *1)$ gera um código estabilizador $\mathcal{C}_{\mathcal{S}(*0:*1)}$ de modo que, para este caso, os geradores do grupo estabilizador $\mathcal{S}(*0 : *1)$ são dados pelo através do conjunto:

$$\{M_i : 1 \leq i \leq 7\} \cup \{N_i : 1 \leq i \leq 7\}.$$

Com isso, segue que $\mathcal{C}_{\mathcal{S}(*0:*1)} = [\![32, 18, 4]\!]$

No Exemplo 6.6 afirmou-se que a matriz $N(*0 : *1)$, satisfaz a condição SIP. De forma geral, dados $u, v, \zeta, \eta \in \mathcal{I}_r$, para que uma matriz dupla norma $N(uv : \zeta\eta)$ satisfaça a condição SIP, de acordo com a expressão (5.76) e com a matriz dada em (6.6), deve-se ter:

$$N_X(uv) \cdot (N_Z(\zeta\eta))^T = N_Z(uv) \cdot (N_X(\zeta\eta))^T. \tag{6.7}$$

Assim, tendo como motivação a Definição 6.5, o Exemplo 6.6 e a Eq. (6.7), tem-se o seguinte resultado.

Teorema 6.7. *Se a matriz norma $N(uv : \zeta\eta)$ satisfaz a Eq. (6.7), então a mesma é a matriz de paridade quântica para um código estabilizador $\mathcal{C}_{\mathcal{S}(uv:\zeta\eta)}$ de modo que:*

$$\mathcal{C}_{\mathcal{S}(uv:\zeta\eta)} = \left[\!\!\left[2^{2r}, 2^{2r} - \dim(N(uv : \zeta\eta)), d \leq \frac{\dim(N(uv : \zeta\eta))}{2} + 1\right]\!\!\right] \tag{6.8}$$

Demonstração: O fato de que $N(uv : \zeta\eta)$ gera um código estabilizador é consequência direta da hipótese de que ela satisfaz a condição SIP. E a determinação dos parâmetros associados ao CQCE gerado é consequência do Teorema 5.31 e do limitante quântico de Singleton. □

Para finalizar este capítulo é apresentada a Tabela 6.4 que presenta alguns parâmetros de códigos estabilizadores que foram construídos via $\mathrm{PEF}\ \mathbb{F}_8^2$ tomando como base a Definição 6.5, o Teorema 6.7. Como é possível observar, foram obtidos códigos estabilizadores com distância mínima 2, 3 e 4.

Tabela 6.2: *Códigos CSS via PEF*$\mathbb{F}_4^2$

Código	Geradores	Parâmetros
$\mathcal{C}_2(**)$	$M_1 = X_1X_6X_{11}X_{16}$, $M_2 = X_4X_5X_{10}X_{15}$, $M_3 = X_3X_8X_9X_{14}$, $M_4 = X_2X_7X_{12}X_{13}$, $M_5 = Z_1Z_6Z_{10}Z_{16}$, $M_6 = Z_4Z_5Z_{10}Z_{15}$, $M_7 = Z_3Z_8Z_9Z_{14}$, $M_8 = Z_2Z_7Z_{12}Z_{13}$	$[\![16, 8, 2]\!]$
$\mathcal{C}_2(*0)$	$M_1 = X_1X_2X_5X_6X_{11}X_{12}X_{15}X_{16}$, $M_2 = X_3X_4X_5X_6X_9X_{10}X_{15}X_{16}$, $M_3 = X_3X_4X_7X_8X_9X_{10}X_{13}X_{14}$, $M_4 = Z_1Z_2Z_5Z_6Z_{11}Z_{12}Z_{15}Z_{16}$, $M_5 = Z_3Z_4Z_5Z_6Z_9Z_{10}Z_{15}Z_{16}$, $M_6 = Z_3Z_4Z_7Z_8Z_9Z_{10}Z_{13}Z_{14}$	$[\![16, 10, 2]\!]$
$\mathcal{C}_2(*1)$	$M_1 = X_1X_4X_6X_7X_{10}X_{11}X_{13}X_{16}$, $M_2 = X_1X_4X_5X_8X_{10}X_{11}X_{14}X_{15}$, $M_3 = X_2X_3X_5X_8X_9X_{12}X_{14}X_{15}$, $M_4 = Z_1Z_4Z_6Z_7Z_{10}Z_{11}Z_{13}Z_{16}$, $M_5 = Z_1Z_4Z_5Z_8Z_{10}Z_{11}Z_{14}Z_{15}$, $M_6 = Z_2Z_3Z_5Z_8Z_9Z_{12}Z_{14}Z_{15}$	$[\![16, 10, 2]\!]$
$\mathcal{C}_2(*, 2)$	$M_1 = X_1X_3X_6X_8X_9X_{11}X_{14}X_{16}$, $M_2 = X_2X_4X_5X_7X_{10}X_{12}X_{13}X_{15}$, $M_3 = Z_1Z_3Z_6Z_8Z_9Z_{11}Z_{14}Z_{16}$, $M_4 = Z_2Z_4Z_5Z_7Z_{10}Z_{12}Z_{13}Z_{15}$	$[\![16, 12, 2]\!]$
$\mathcal{C}_2(00)$	$M_1 = X_2X_5X_{12}X_{15}$, $M_2 = X_3X_6X_9X_{16}$, $M_3 = X_4X_7X_{10}X_{13}$, $M_4 = X_1X_8X_{11}X_{14}$, $M_5 = Z_2Z_5Z_{12}Z_{15}$, $M_6 = Z_3Z_6Z_9Z_{16}$, $M_7 = Z_4Z_7Z_{10}Z_{13}$, $M_8 = Z_1Z_8Z_{11}Z_{14}$	$[\![16, 12, 2]\!]$
$\mathcal{C}_2(01)$	$M_1 = X_2X_4X_5X_7X_{10}X_{12}X_{13}X_{15}$, $M_2 = X_1X_3X_6X_8X_9X_{11}X_{14}X_{16}$, $M_3 = Z_2Z_4Z_5Z_7Z_{10}Z_{12}Z_{13}Z_{15}$, $M_4 = Z_1Z_3Z_6Z_8Z_9Z_{11}Z_{14}Z_{16}$	$[\![16, 12, 2]\!]$
$\mathcal{C}_2(02)$	$M_1 = X_2X_3X_5X_8X_9X_{12}X_{14}X_{15}$, $M_2 = X_2X_3X_6X_7X_9X_{12}X_{13}X_{16}$, $M_3 = X_1X_4X_6X_7X_{10}X_{11}X_{13}X_{16}$, $M_4 = Z_2Z_3Z_5Z_8Z_9Z_{12}Z_{14}Z_{15}$, $M_5 = Z_2Z_3Z_6Z_7Z_9Z_{12}Z_{13}Z_{16}$, $M_6 = Z_1Z_4Z_6Z_7Z_{10}Z_{11}Z_{13}Z_{16}$	$[\![16, 10, 2]\!]$
$\mathcal{C}_2(11)$	$M_1 = X_4X_7X_{10}X_{13}$, $M_2 = X_1X_8X_{11}X_{14}$, $M_3 = X_2X_5X_{12}X_{15}$, $M_4 = X_3X_6X_9X_{16}$, $M_5 = Z_4Z_7Z_{10}Z_{13}$, $M_6 = Z_1Z_8Z_{11}Z_{14}$, $M_7 = Z_2Z_5Z_{12}Z_{15}$, $M_8 = Z_3Z_6Z_9Z_{16}$	$[\![16, 8, 2]\!]$
$\mathcal{C}_2(12)$	$M_1 = X_3X_4X_7X_8X_9X_{10}X_{13}X_{14}$, $M_2 = X_1X_2X_7X_8X_{11}X_{12}X_{13}X_{14}$, $M_3 = X_1X_2X_5X_6X_{11}X_{12}X_{15}X_{16}$, $M_4 = Z_3Z_4Z_7Z_8Z_9Z_{10}Z_{13}Z_{14}$, $M_5 = Z_1Z_2Z_7Z_8Z_{11}Z_{12}Z_{13}Z_{14}$, $M_6 = Z_1Z_2Z_5Z_6Z_{11}Z_{12}Z_{15}Z_{16}$	$[\![16, 10, 2]\!]$
$\mathcal{C}_2(22)$	$M_1 = X_3X_8X_9X_{14}$, $M_2 = X_2X_7X_{12}X_{13}$, $M_3 = X_1X_6X_{11}X_{16}$, $M_4 = X_4X_5X_{10}X_{15}$, $M_5 = Z_3Z_8Z_9Z_{14}$, $M_6 = Z_2Z_7Z_{12}Z_{13}$, $M_7 = Z_1Z_6Z_{11}Z_{16}$, $M_8 = Z_4Z_5Z_{10}Z_{15}$	$[\![16, 8, 2]\!]$

Tabela 6.3: *Códigos estabilizadores via PEF$\mathbb{F}_4^2$ utilizando o corolário 6.3.*

Código	Geradores de $\mathcal{S}$	Parâmetros
$\mathcal{C}_{\mathcal{S}}(**)$	$M_1 = X_1Z_3X_6Z_8$, $M_2 = Z_2X_4X_5Z_7$, $M_3 = Z_1X_3Z_6X_8$, $M_4 = X_2Z_4Z_5X_7$	$[\![8,4,2]\!]$
$\mathcal{C}_{\mathcal{S}}(*0)$	$M_1 = X_1X_2Z_3Z_4X_5X_6Z_7Z_8$, $M_2 = Z_1Z_2X_3X_4X_5X_6Z_7Z_8$, $M_3 = Z_1Z_2X_3X_4Z_5Z_6X_7X_8$	$[\![8,5,2]\!]$
$\mathcal{C}_{\mathcal{S}}(*1)$	$M_1 = X_1Z_2Z_3X_4Z_5X_6X_7Z_8$, $M_2 = X_1Z_2Z_3X_4X_5Z_6Z_7X_8$ $M_3 = Z_1X_2X_3Z_4X_5Z_6Z_7X_8$	$[\![8,5,2]\!]$
$\mathcal{C}_{\mathcal{S}}(*2)$	$M_1 = Y_1Y_3Y_6Y_8$, $M_2 = Y_2Y_4Y_5Y_7$	$[\![8,6,2]\!]$
$\mathcal{C}_{\mathcal{S}}(00)$	$M_1 = X_2Z_4X_5Z_7$, $M_2 = Z_1X_3X_6Z_8$, $M_3 = Z_2X_4Z_5X_7$, $M_4 = X_1Z_3Z_6X_8$	$[\![8,4,2]\!]$
$\mathcal{C}_{\mathcal{S}}(01)$	$M_1 = Y_2Y_4Y_5Y_7$,$M_2 = Y_1Y_3Y_6Y_8$	$[\![8,6,2]\!]$
$\mathcal{C}_{\mathcal{S}}(02)$	$M_1 = Z_1X_2X_3Z_4X_5Z_6Z_7$, $M_2 = Z_1X_2X_3Z_4Z_5X_6X_7Z_8$, $M_3 = X_1Z_2Z_3X_4Z_5X_6X_7Z_8$	$[\![8,5,2]\!]$
$\mathcal{C}_{\mathcal{S}}(11)$	$M_1 = Z_2X_4Z_5X_7$, $M_2 = X_1Z_3Z_6X_8$, $M_3 = X_2Z_4X_5Z_7$, $M_4 = Z_1X_3X_6Z_8$	$[\![8,4,2]\!]$
$\mathcal{C}_{\mathcal{S}}(12)$	$M_1 = Z_1Z_2X_3X_4Z_5Z_6X_7X_8$, $M_2 = X_1X_2Z_3Z_4Z_5Z_6X_7X_8$, $M_3 = X_1X_2Z_3Z_4X_5X_6Z_7Z_8$	$[\![8,5,2]\!]$
$\mathcal{C}_{\mathcal{S}}(22)$	$M_1 = Z_1X_3Z_6X_8$, $M_2 = X_2Z_4Z_5X_7$, $M_3 = X_1Z_3X_6Z_8$, $M_4 = Z_2X_4X_5Z_7$	$[\![8,4,2]\!]$

Tabela 6.4: *Códigos estabilizadores via PEF$\mathbb{F}_4^2$ utilizando o corolário 6.3.*

Parâmetros	Códigos
$[\![32,18,4]\!]$	$\mathcal{C}_{\mathcal{S}(*0:*1)}, \mathcal{C}_{\mathcal{S}(*0:*2)}, \mathcal{C}_{\mathcal{S}(*2:*4)}, \mathcal{C}_{\mathcal{S}(01:*0)}, \mathcal{C}_{\mathcal{S}(01:*1)}, \mathcal{C}_{\mathcal{S}(01:*2)}, \mathcal{C}_{\mathcal{S}(01:03)}, \mathcal{C}_{\mathcal{S}(01:05)}, \mathcal{C}_{\mathcal{S}(12:*1)}$
$[\![32,18,3]\!]$	$\mathcal{C}_{\mathcal{S}(*2:*3)}, \mathcal{C}_{\mathcal{S}(*2:*5)}, \mathcal{C}_{\mathcal{S}(*2:*6)}, \mathcal{C}_{\mathcal{S}(01:*4)}, \mathcal{C}_{\mathcal{S}(01:02)}, \mathcal{C}_{\mathcal{S}(01:04)}, \mathcal{C}_{\mathcal{S}(01:06)}, \mathcal{C}_{\mathcal{S}(13:12)}$
$[\![32,18,2]\!]$	$\mathcal{C}_{\mathcal{S}(01:*3)}, \mathcal{C}_{\mathcal{S}(01:*5)}, \mathcal{C}_{\mathcal{S}(01:*6)}, \mathcal{C}_{\mathcal{S}(14:23)}, \mathcal{C}_{\mathcal{S}(16:36)}$
$[\![32,19,2]\!]$	$\mathcal{C}_{\mathcal{S}(01:*3)}$

CAPÍTULO 7

CONSIDERAÇÕES FINAIS

Este trabalho teve como proposta realizar um estudo de códigos corretores de erros por meio de uma ferramenta algébrica denominada como *Plano Euclidiano Finito* (PEF). Tal ferramenta tem origem nos trabalhos realizados por Celniker [9], Medrano [52] e Terras [69], nos quais os autores apresentam um conceito mais geral chamado *espaço Euclidiano finito n-dimensional* a fim de pesquisarem aspectos relacionados à Teoria de Grafos com uma atenção especial para grafos de Ramanujan e também com implicações na teoria de análise harmônica realizada em espaços simétricos. A inspiração para utilizar o PEF no estudo de códigos originou-se do trabalho de Da Silva, Carneiro e Castelani [12] em que foram apresentadas famílias de códigos clássicos lineares binários e códigos não lineares e não binários por meio da definição de outro conceito cuja origem também remete aos trabalhos de Celniker, Medrano, e Terras, a saber: o *Semi-Plano Superior Finito.*

Ao explorar o PEF, como mostrado no Capítulo 4, foi possível obter uma família de códigos lineares binários quase-cíclicos auto-ortogonais em relação ao produto interno Euclidiano e ao produto interno simplético. A caracterização desses códigos foi realizada por meio de suas matrizes geradoras, o que permitiu a determinação de suas propriedades, incluindo comprimentos, dimensões e distâncias mínimas. Essa família de códigos está relacionada a três novos parâmetros que possuem uma natureza diferente dos parâmetros já mencionados, e que estão intrinsecamente relacionados aos conceitos associados ao PEF.

As propriedades relacionadas à ortogonalidade dos códigos obtidos no Capítulo 4 possuem implicações na Teoria da Computação e da Informação Quântica. Sendo assim, tal fato motivou a desenvolver o estudo que foi apresentado nos Capítulo 6, onde foi mostrado que a família de códigos quase-cíclicos obtida por meio do PEF possuem as características que proporcionam a obtenção de códigos quânticos corretores de erros, em especial códigos estabilizadores.

Assim, para a família de códigos quase-cíclicos obtida no Capítulo 4, foi adaptada uma técnica de construção de códigos estabilizadores. E dentre os códigos estabilizadores obtidos por tal técnica, chegou-se a códigos quânticos que atingem o valor máximo permitido para a distância mínima de acordo com o limitante quântico de Singleton, conforme é mostrado no Exemplo 6.4, considerando $r = 2$. Além disso, para $r = 3$,

foram apresentados alguns exemplos de códigos estabilizadores com distâncias mínimas iguais a 2, 3 e 4.

Diante dos fatos apresentados, conclui-se que o uso do PEF se demonstrou uma ferramenta promissora para a obtenção de códigos lineares e códigos quânticos corretores de erros com características importantes do ponto de vista da teoria da computação e da informação. Portanto, o presente trabalho introduz uma abordagem original no que se refere à concepção de novos códigos corretores de erros clássicos e também quânticos.

REFERÊNCIAS

[1] AABRANDT, A.; HANSEN, V. L. **The circle equation over finite fields**. Quaestiones Mathematicae. Journal of the South African Mathematical Society, v. 41, n. 5, p. 665–674, 2018.

[2] ALBUQUERQUE, C. D.; **Analise e construção de códigos quânticos topológicos sobre variedades bidimensionais**. 2009. 139 p. Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, Campinas, SP. Disponível em: https://hdl.handle.net/20.500.12733/1609549. Acesso em: 12 abr. 2023.

[3] BALL, S. **A course in algebraic error-correcting codes**. 1. ed. Cham, Switzerland: Springer Nature, 2020.

[4] CALDERBANK, A. R. et al. **Quantum error correction via codes over GF(4)**. IEEE transactions on information theory, v. 44, n. 4, p. 1369–1387, 1998.

[5] CALDERBANK, A. R.; SHOR, P. W. **Good quantum error-correcting codes exist.** Physical review. A, v. 54, n. 2, p. 1098–1105, 1996.

[6] CALDERBANK, A. R. et al. **Quantum Error Correction and Orthogonal Geometry.** Physical review letters, v. 78, n. 3, p. 405–408, 1997.

[7] CARDELL, S. D.; CLIMENT, J.-J. **A construction of primitive polynomials over finite fields**. Linear and multilinear algebra, v. 65, n. 12, p. 2424–2431, 2017.

[8] CHANG, Y.; CHOU, W.-S.; SHIUE, P. J.-S. **On the number of primitive polynomials over finite fields**. Finite fields and their applications, v. 11, n. 1, p. 156–163, 2005.

[9] CELNIKER, N. et al. **Is there life on finite upper half planes?**. Contemporary Mathematics, v. 143, p. 65-88, 1993.

[10] CHIMAL-DZUL, H.; LIEB, J.; ROSENTHAL, J. **Generator matrices of quasi-cyclic codes over extension fields obtained from gröbner basis**. IFAC-PapersOnLine, v. 55, n. 30, p. 61–66, 2022.

[11] COUVEIGNES, J.-M.; LERCIER, R. **Fast construction of irreducible polynomials over finite fields**. Israel journal of mathematics, v. 194, n. 1, p. 77–105, 2013.

[12] DA SILVA, E. B.; CARNEIRO, M. G.; CASTELANI, E. V. **New quasi-cyclic codes from finite upper half-planes**. International Journal of Information and Coding Theory. IJICOT, v. 5, n. 3/4, p. 239, 2020.

[13] DASKALOV, R.; HRISTOV, P. **New One-Generator Quasi-cyclic Codes over** $GF(7)$,Problems of Information Transmission v. 38, n. 1, p. 50–54, 2002.

[14] DE ALBUQUERQUE, C. D. **Análise e Construção de Códigos Quânticos Topológicos sobre Variedades Bidimensionais**. Campinas : Universidade Estadual de Campinas, 2009.

[15] DEVITT, S. J. et al. **Quantum error correction for beginners.** Reports on Progress in Physics, v. 76, n. 7, p. 076001, 2013.

[16] DJORDJEVIC, I. **Quantum information processing, quantum computing, and quantum error correction: An engineering approach.** 2. ed. San Diego, CA, USA: Academic Press, 2021.

[17] FITZGERALD, R. W. **A characterization of primitive polynomials over finite fields**. Finite fields and their applications, v. 9, n. 1, p. 117–121, 2003.

[18] FORNEY Jr., G. David. **Concatenated codes**. IRE International Convention Record, vol. 13, 1965, pp. 5-12.

[19] FOWLER, A. G. et al. **Surface codes: Towards practical large-scale quantum computation.** Physical Review A, v. 86, n. 3, p. 032324, 2012.

[20] GAITAN, F. **Quantum error correction and fault tolerant quantum computing.** Boca Raton, FL, USA: CRC Press, 2018.

[21] GAZZONI, W. C. **Propriedades Algébricas e Geométricas dos Códigos de Bloco Quânticos**. Campinas : Universidade Estadual de Campinas, 2004.

[22] GONÇALVES, A. **Introdução à Álgebra**. 6a ed. Rio de Janeiro: IMPA, 2017.

[23] GOTTESMAN, D. **An Introduction to Quantum Error Correction**. 2000. Disponível em: <http://arxiv.org/abs/quant-ph/0004072>.

[24] GOTTESMAN, D. **Stabilizer Codes and Quantum Error Correction**. [s.l.] California Institute of Technology, 1997.

[25] GOTTESMAN, D.; CHUANG, I. L. **Quantum Teleportation is a Universal Computational Primitive**. 1999. Disponível em: <http://arxiv.org/abs/quant-ph/9908010>.

[26] GRASSL, M. **New quantum codes from CSS codes.** Quantum information processing, v. 22, n. 1, 2023.

[27] GRASSL, M.; ROTTELER, M. **Quantum MDS codes over small fields**. 2015 IEEE International Symposium on Information Theory (ISIT). Anais...IEEE, 2015.

[28] GULLIVER, T. A. **CONSTRUCTION OF QUASI-CYCLIC CODES.** [s.l.] University of New Brunswick, 1989.

[29] GÜNERI, C.; ÖZDEMIR, F.; SOLÉ, P. **On the additive cyclic structure of quasi-cyclic codes**. Discrete mathematics, v. 341, n. 10, p. 2735–2741, 2018.

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

[31] HUANG, M.-D. A. **Factorization of polynomials over finite fields and decomposition of primes in algebraic number fields**. Journal of algorithms, v. 12, n. 3, p. 482–489, 1991.

[32] HUBER, F.; GRASSL, M. **Quantum codes of maximal distance and highly entangled subspaces**. Quantum, v. 4, n. 284, p. 284, 2020.

[33] HUFFMAN, W. C.; PLESS, V. **Fundamentals of error-correcting codes**. Cambridge, England: Cambridge University Press, 2012.

[34] HUNGERFORD, T. W. **Algebra**. 1974. ed. Nova Iorque, NY, USA: Springer, 2012.

[35] HWANG, Y.; CHOI, B.-S.; JEON, M. **On the construction of stabilizer codes with an arbitrary binary matrix**. Quantum information processing, v. 12, n. 1, p. 467–479, 2013.

[36] ITSKOV, M. **Tensor algebra and tensor analysis for engineers: With applications to continuum mechanics.** 5. ed. Basileia, Switzerland: Springer International Publishing, 2018.

[37] KAI, C; et al. **Weight Calculation And Purity Identification Of Symplectic Self-orthogonal Codes.** 3rd InternationalConference on Computer Science and Service System. Atlantis Press, p. 558-561, 2014.

[38] KYUREGHYAN, G. M.; KYUREGHYAN, M. K. **A recurrent construction of irreducible polynomials of fixed degree over finite fields**. Applicable algebra in engineering, communication and computing, v. 33, n. 2, p. 163–171, 2022.

[39] KYUREGYAN, M. K. **Iterated constructions of irreducible polynomials over finite fields with linearly independent roots**. Finite fields and their applications, v. 10, n. 3, p. 323–341, 2004.

[40] LA GUARDIA, G. G. **Quantum error correction: Symmetric, asymmetric, synchronizable, and convolutional codes**. 1. ed. Cham, Switzerland: Springer Nature, 2021.

[41] LA GUARDIA, G. G.; PALAZZO, R., Jr. **Constructions of new families of nonbinary CSS codes**. Discrete mathematics, v. 310, n. 21, p. 2935–2945, 2010.

[42] LERNER, B. S. **Computational complexity and information asymmetry in financial products**. Journal of Corporation Law, v. 34, n. 4, p. 927-971, 2008.

[43] LIDAR, D. A.; BRUN, T. A. (EDS.). **Quantum Error Correction.** Cambridge, England: Cambridge University Press, 2013.

[44] LIDL, R.; NIEDERREITER, H. **Introduction to Finite Fields and their Applications**. 2. ed. Cambridge, England: Cambridge University Press, 2012.

[45] LING, S.; XING, C. **Coding theory: A first course**. Cambridge, England: Cambridge University Press, 2006.

[46] LV, J.; LI, R.; WANG, J. **New binary quantum codes derived from one-generator quasi-cyclic codes**. IEEE access: practical innovations, open solutions, v. 7, p. 85782–85785, 2019.

[47] MACWILLIAMS, F. J.; SLOANE, N. J. A. **The theory of error-correcting codes.** [s.l.] North-Holland, 1988.

[48] NGUYEN, D. M. **Study on Constructions of Quantum Error Correction Codes**. [s.l.] UNIVERSITY OF ULSAN, 2020.

[49] NGUYEN, D.; KIM, S. **New constructions of quantum stabilizer codes based on difference sets.** Symmetry, v. 10, n. 11, p. 655, 2018.

[50] NGUYEN, D. M.; KIM, S. **A novel construction for quantum stabilizer codes based on binary formalism.** International journal of modern physics b, v. 34, n. 08, p. 2050059, 2020.

[51] NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information: 10Th Anniversary Edition.** Cambridge, England: Cambridge University Press, 2012.

[52] MEDRANO, A. et al. **Finite analogues of Euclidean space**. Journal of computational and applied mathematics, v. 68, n. 1–2, p. 221–238, 1996.

[53] OZDEMIR, E. **Factoring polynomials over finite fields**. International journal of number theory, v. 17, n. 07, p. 1517–1536, 2021.

[54] PARTHASARATHY, K. R. **Quantum computation, quantum error correcting codes and information theory**. Nova Deli, India: Narosa Publishing House, 2005.

[55] PETERSON, W. W.; WELDON, E. J. **Error-Correcting Codes**. 2. ed. Londres, England: MIT Press, 1972.

[56] PIQUEIRA, J. R. C. **Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e teletransporte.** Revista Brasileira de Ensino de Física, v. 33, n. 4, 2011.

[57] PREKILL, J. **Fault-tolerant quantum computation**. Introduction to quantum computation and information. World Scientific, 1997. p. 213-269.

[58] PU, I. M. **Fundamental Data Compression**. Oxford, England: Butterworth-Heinemann, 2006.

[59] RAVEENDRAN, N.; VASIĆ, B. **Trapping sets of quantum LDPC codes**. Quantum, v. 5, n. 562, p. 562, 2021.

[60] SHANNON, C. E. **A mathematical theory of communication**. The Bell System technical journal, v. 27, n. 3, p. 379–423, 1948.

[61] SHIMA, K.; DOI, H. **New proof techniques using the properties of circulant matrices for XOR-based (k, n) threshold secret sharing schemes**. Journal of Information Processing, 2021, 29: 266-274.

[62] SHOR, P. W. **Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer**. 1995. Disponível em: <http://arxiv.org/abs/quant-ph/9508027>.

[63] SHOUP, V. **New algorithms for finding irreducible polynomials over finite fields**. Mathematics of computation, v. 54, n. 189, p. 435, 1990.

[64] SHOUP, V. **Fast construction of irreducible polynomials over finite fields**. Journal of symbolic computation, v. 17, n. 5, p. 371–391, 1994.

[65] STEANE, A.**Enlargement of Calderbank Shor Steane quantum codes.** 1998. Disponível em: <http://arxiv.org/abs/quant-ph/9802061>.

[66] STEANE, A. **Multiple-particle interference and quantum error correction**. Proceedings. Mathematical, physical, and engineering sciences, v. 452, n. 1954, p. 2551–2577, 1996b.

[67] STEANE, A. **Simple Quantum Error Correcting Codes.** 1996. Disponível em: <http://arxiv.org/abs/quant-ph/9605021>.

[68] TERHAL, B. M. **Quantum error correction for quantum memories**. Reviews of modern physics, v. 87, n. 2, p. 307–346, 2015.

[69] TERRAS, A. **Harmonic analysis on symmetric spaces—euclidean space, the sphere, and the Poincaré upper half-plane**. Nova Iorque, NY, USA: Springer, 2016.

[70] VANSTONE, S. A.; VAN OORSCHOT, P. C. (EDS.). **An introduction to error correcting codes with applications**. Nova Iorque, NY, USA: Springer, 2014.

[71] XIAO, F.; CHEN, H. **Is A quantum stabilizer code degenerate or nondegenerate for Pauli channel?** 2010. Disponível em: <http://arxiv.org/abs/1009.3539>.

[72] XU, H.; DU, W. **On some binary symplectic self-orthogonal codes**. Applicable algebra in engineering, communication and computing, v. 33, n. 3, p. 321–337, 2022.

[73] ZERAATPISHEH, M.; ESMAEILI, M.; GULLIVER, T. A. **Quasi-cyclic codes: algebraic properties and applications**. Computational & Applied Mathematics, v. 39, n. 2, 2020.