Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação

Giuliano Gadioli La Guardia

Métodos de Construção de Códigos Quânticos *CSS* e Conexões entre Códigos Quânticos e Matróides

Campinas
2008

Giuliano Gadioli La Guardia

Métodos de Construção de Códigos Quânticos *CSS* e Conexões entre Códigos Quânticos e Matróides

Tese de doutorado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos exigidos para a obtenção do título de Doutor em Engenharia Elétrica.
Área de concentração: Telecomunicações e Telemática.

Orientador: Prof. Dr. Reginaldo Palazzo Jr.

Co-orientador: Prof. Dr. Carlile Lavor

Campinas
2008

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

La Guardia, Giuliano Gadioli
L138m Métodos de construção de códigos quânticos CSS e conexões entre códigos quânticos e matróides / Giuliano Gadioli La Guardia. --Campinas, SP: [s.n.], 2008.

Orientadores: Reginaldo Palazzo Junior, Carlile Campos Lavor.
Tese de Doutorado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Computadores quânticos. 2. Matróides. 3. Códigos de controle de erros (Teoria da informação). I. Palazzo Junior, Reginaldo. II. Lavor, Carlile Campos. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Titulo em Inglês: Construction methods of CSS quantum codes and relationships between quantum codes and matroids
Palavras-chave em Inglês: Quantum computers, Matroids, Error control codes (Information theory)
Área de concentração: Telecomunicações e Telemática
Titulação: Doutor em Engenharia Elétrica
Banca examinadora: Reginaldo Palazzo Junior, Antonio Aparecido de Andrade, Marcelo Muniz Silva Alves, Walter da Cunha Borelli, Jaime Portugheis
Data da defesa: 12/07/2008
Programa de Pós Graduação: Engenharia Eletrica

Giuliano Gadioli La Guardia
Bacharel em Matemática Pura – UNICAMP
Mestre em Matemática Pura – UNICAMP

Métodos de Construção de Códigos Quânticos *CSS* e Conexões entre Códigos Quânticos e Matróides

Tese de doutorado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos exigidos para a obtenção do título de Doutor em Engenharia Elétrica. Área de concentração: Telecomunicações e Telemática. Aprovada pela banca examinadora no dia 12 de Setembro de 2008.

Banca Examinadora:

Prof. Dr. Reginaldo Palazzo Jr. - Presidente
FEEC/UNICAMP
Prof. Dr. Antonio Aparecido de Andrade
IBILCE/UNESP
Prof. Dr. Marcelo Muniz Silva Alves
MAT/UFPR
Prof. Dr. Walter da Cunha Borelli
FEEC/UNICAMP
Prof. Dr. Jaime Portugheis
FEEC/UNICAMP
Prof. Dr. Carlos Eduardo Câmara - suplente
FCC/USF
Prof. Dr. Renato Baldini Filho - suplente
FEEC/Unicamp
Prof. Dr. Celso de Almeida - suplente
FEEC/Unicamp

Campinas
2008

COMISSÃO JULGADORA - TESE DE DOUTORADO

Candidato: Giuliano Gadioli La Guardia

Data da Defesa: 12 de setembro de 2008

Título da Tese: "Métodos de Construção de Códigos Quânticos CSS e Conexões entre Códigos Quânticos e Matróides"

Prof. Dr. Reginaldo Palazzo Júnior (Presidente): Reginaldo Palazzo Júnior

Prof. Dr. Antonio Aparecido de Andrade: Antonio Aparecido de Andrade

Prof. Dr. Marcelo Muniz Silva Alves:

Prof. Dr. Walter da Cunha Borelli: Borelli

Prof. Dr. Jaime Portugheis: Jaime Portugheis

Dedicada, com eternas alegrias, felicidades, paz, no céu eternamente, e eterno amor, ao meu filho, que ascendeu à Deus no dia 22 de setembro de 2008.

Agradecimentos

Agradeço,

- à Deus em primeiro lugar, por ser o responsável maior por tal conquista;
- ao meu orientador Prof. Dr. Reginaldo Palazzo Jr., por valorosa orientação e por ser um exemplo a ser seguido, tanto na área pessoal quanto na área profissional;
- ao meu co-orientador Prof. Dr. Carlile Campos Lavor, pelo apoio emocional e profissional;
- à banca examinadora: Prof. Dr. Reginaldo Palazzo Jr., Prof. Dr. Antonio Aparecido de Andrade, Prof. Dr. Marcelo Muniz Silva Alves, Prof. Dr. Walter da Cunha Borelli, Prof. Dr. Jaime Portugheis, Prof. Dr. Carlos Eduardo Câmara (suplente), Prof. Dr. Renato Baldini Filho (suplente) e Prof. Dr. Celso de Almeida (suplente), pelas excelentes correções e sugestões;
- à minha família, que esteve sempre presente, pelo constante apoio afetivo e pessoal;
- à minha namorada Gilcélia, pelo constante apoio afetivo, pessoal, e por ter me presenteado com a alegria de ter um filho;
- ao amigo Edson Donizete de Carvalho, por me apresentar e me indicar ao meu orientador, Prof. Dr. Reginaldo Palazzo Jr;
- às Prof[a]s Dras. Claudina Izepe Rodrigues, Eliane Quelho Frota Rezende, Maria Lúcia Bontorin de Queiroz e Vera Lucia Xavier Figueiredo, pelo carinho, dedicação e apoio profissional;
- aos amigos: João Henrique (Gauchão da Fronteira), João Coelho (Qualirão), Julio (Valderrama), Góis (Til), Ricardo Coração de Leão (Pancades), Renato (Renatiiiiiiiiiinho), Walter Furloni (Vavá), Vagner (Qualirinha), Vandenberg (Mundiça), Andréa e Luzinete (As Meninas), Clarice, Leandro, Wanessa, Talía (Secretália), Taís, Eduardo, Hugo, Hugo (P), Daniel (Mineiro), Polyane (Poly), Claudião, Fábio Hernandes (Prefeito), Sandro, Airton, Denise, Tiago (três segundos), André du Pin Calmon, Raquel Machado, André Pasqual, Rodrigo, Natália, Ricardo Coelho (Ceará), Fábio Benjovengo, Tatiana Pazeto (Tati), Alessandro, Rúbia, Vinícius e Giórgio, pelo apoio pessoal e científico;
- aos demais colegas do DT e do LTIA, pela ótima convivência;

- aos funcionários do DT, pelo carinho e competência profissional;
- aos amigos Gustavo e Éverton, pelo apoio computacional;
- aos amigos Valquíria e Nilton, pelo apoio pessoal;
- à amiga Quitéria, pelo apoio pessoal;
- aos Prof´s. Drs. Arnaldo Mandel e Cláudio Leonardo Lucchesi, pelo apoio profissional;
- aos professores do DEMAT, pela liberação para o doutorado;
- à UEPG, pelo apoio financeiro;
- à UNICAMP, pela ótima estrutura que oferece aos estudantes e pesquisadores;
- aos órgãos de fomento CAPES e FAPESP, pelo apoio financeiro;
- a todos que, de alguma forma, contribuíram para o meu crescimento pessoal ou profissional.

"A ciência humana de maneira nenhuma nega a existência de Deus. Quando considero quantas e quão maravilhosas coisas o homem compreende, pesquisa e consegue realizar, então reconheço claramente que o espírito humano é obra de Deus, e a mais notável"

Galileu Galilei

Resumo

Como principais contribuições desta tese, apresentamos novos métodos de construção que geram novas famílias de códigos quânticos *CSS*. As construções são baseadas em códigos cíclicos (clássicos) *BCH*, *Reed-Solomon*, *Reed-Muller*, *Resíduos quadráticos* e também nos códigos derivados do produto tensorial de dois códigos *Reed-Solomon*. Os principais códigos quânticos construídos neste trabalho, em termos de parâmetros, são os derivados dos códigos *BCH* clássicos. Além disso, estudamos as condições necessárias para analisar as situações nas quais os códigos cíclicos quânticos (clássicos) são códigos MDS (do inglês, Maximum-Distance-Separable codes). Apresentamos, também, novas conexões entre a teoria de matróides e a teoria dos códigos quânticos *CSS*, que acreditamos serem as primeiras conexões entre tais teorias. Mais especificamente, demonstramos que a função enumeradora de pesos de um código quântico *CSS* é uma avaliação do polinômio de Tutte da soma direta dos matróides originados a partir dos códigos clássicos utilizados na construção *CSS*.

Palavras-chave: Códigos Quânticos Calderbank-Shor-Steane *CSS*.
Códigos Cíclicos: *BCH*, *Reed-Solomon*, *Reed-Muller*, *Resíduos quadráticos*. Teoria de Matróides.

Abstract

This thesis proposes, as the main contributions, constructions method of new families of quantum *CSS* codes. These constructions are based on classical cyclic codes of the types *BCH*, *Reed-Solomon*, *Reed-Muller*, *Quadratic Residue* and also are based on product codes of classical *Reed-Solomon* codes. The main family of quantum codes constructed in this work, i. e., quantum codes having better parameters, are the ones derived from classical *BCH* codes. Moreover, we present some new conditions in which quantum *CSS* cyclic codes are quantum MDS codes. In addition, we provide the elements to connect matroid theory and quantum coding theory. More specifically, we show that the weight enumerator of a *CSS* quantum code is equivalent to evaluating the Tutte polynomial of the direct sum of the matroid associated to the classical codes used in the *CSS* construction.

Key-words: Quantum Calderbank-Shor-Steane (*CSS*) Codes. Cyclic Codes: *BCH*, *Reed-Solomon*, *Reed-Muller*, *Quadratic Residue*. Matroid Theory.

Lista de Tabelas

Lista de Acrônimos e Notações

CSS	código quântico Calderbank-Shor-Steane
BCH	código Bose-Chaudhuri-Hocquenghem
RS	código Reed-Solomon
RM	código Reed-Muller
RS	código Resíduos-Quadráticos
MDS	código com máxima distância de separação
$\mathcal{R}(r, m)$	código Reed-Muller de ordem r e comprimento $n = 2^m$
$CSS(C_1, C_2)$	código CSS derivado de C_1 e C_2
$\mathbb{Z}^+$	conjunto dos inteiros positivos
2^E	conjunto das partes de E
$\mid . \mid$	função módulo
$\mid v\rangle$	vetor (ket)
$\langle v \mid$	vetor dual a v (bra)
$(\cdot, \cdot)$ e $\langle . \rangle$	produto interno
$Tr(A)$	traço da matriz A
Tr_B	traço parcial sobre o sistema B
$\otimes$	produto tensorial
$*$	conjugado complexo
A^T	transposta da matriz A
$A^\dagger$	conjugado hermitiano da matriz A
∂	grau do polinômio
$\lceil x \rceil$	menor inteiro maior ou igual a x
$\lfloor x \rfloor$	maior inteiro menor ou igual a x
U	operador unitário
M_m	operador hermitiano
$\mid x_1 x_2 \cdots x_n\rangle$	estado geral de n qubits
$\|a_1\rangle\langle a_2\|$	operador linear
$\{p_i, \|\psi_i\rangle\}$	ensemble de estados puros
ρ	operador densidade

ρ^A	operador densidade reduzido de A
ε	operação quântica
$\mathcal{R}$	operação de correção de erro
$\mathcal{E}$	processo de ruído
ρ_{amb}	operador densidade do ambiente
I_r	matriz identidade de ordem r
I	matriz identidade de dimensão apropriada
$CNOT$	operador quântico Não-Controlado
H	matriz de Hadamard
$:=$	definição
$\equiv \ mod\ m$	congruência módulo m
$F[x]$	anel de polinômios na variável x
R_n	anel quociente
α	elemento primitivo de um corpo
$M^{(i)}$	polinômio minimal do elemento α^i
F_q	corpo contendo $q = p^m$ elementos, p primo
$C = C(n,k)$	código de bloco linear
$[n,k]$	parâmetros de um código clássico
$C^{\perp}$	dual do código de bloco linear C
δ	distância de projeto
d_{min}	distância mínima do código
β	base de F_{q^m} sobre F_q
$\beta^{\perp}$	base dual de β
$\mathbb{C}_s$	classe lateral ciclotômica contendo s
$[[n,k,d]]_q$	parâmetros de um código quântico q-ário
$\mathcal{I}$	conjunto dos conjuntos independentes de um matróide
$\mathcal{B}$	conjunto das bases de um matróide
$\mathcal{C}$	conjunto dos circuitos de um matróide
$M\|X$	matróide restrição
$M[A]$	matróide vetorial da matriz A
r	função posto de um matróide
cl	operador fecho de um matróide
$M_1 \oplus M_2$	matróide soma direta
M^*	matróide dual de M
$\mathcal{B}^*$	conjunto das bases do matróide dual de M
$V(m,F)$	espaço vetorial de dimensão m sobre o corpo F
M_C	matróide derivado do código $C(n,k)$
C_M	código derivado do matróide M
$T_M(x,y)$	polinômio de Tutte de M
$A_C(z)$	função enumeradora de pesos de $C(n,k)$

Sumário

Introdução Geral

A teoria dos códigos quânticos corretores de erros [1–3] tem recebido muita atenção na última década, devido à sua importância na transmissão e armazenamento de informação quântica. Com o provável advento do computador quântico, pesquisas em relação a tais assuntos têm avançado rapidamente. De fato, esta teoria se infiltra em muitas áreas de pesquisa. Os exemplos mais conhecidos de códigos quânticos corretores de erros são os códigos de Shor [1] e a classe de códigos denominados *CSS* (Calderbank-Shor-Steane) [1]. O código de Shor foi o primeiro código quântico construído. Este codifica 1 qubit em 9 qubits e é capaz de corrigir 1 erro quântico arbitrário em qualquer um dos qubits. É um código quântico de repetição.

Os códigos *CSS* formam uma subclasse contida na classe de códigos estabilizadores [1], e tal subclasse é a principal ferramenta utilizada para a construção de bons códigos quânticos, [2, 4–20]. Poucos trabalhos existentes na literatura não utilizam a construção *CSS* para a geração de códigos quânticos, como, por exemplo, [21–24].

Em relação à criação de novos códigos quânticos, a maioria dos trabalhos apresentados na literatura são baseados em construções de códigos *CSS* derivados de um único código clássico auto-ortogonal C [2, 5–15, 17–20]. Em [11] são apresentados códigos *CSS* derivados de um único código convolucional clássico, auto-ortogonal.

Existem poucos trabalhos disponíveis na literatura com respeito à construção de códigos *CSS* derivados de dois códigos clássicos lineares distintos, não necessariamente auto-ortogonais, como, por exemplo, [4, 16, 25], onde os códigos clássicos lineares envolvidos na construção *CSS* são códigos de bloco. Motivados por este fato, estabelecemos o objetivo principal deste trabalho.

O objetivo principal deste trabalho é propor novos métodos de construção que possibilitem a geração de novas famílias de bons códigos quânticos *CSS*, ou seja, códigos *CSS* comparáveis ou melhores que os códigos disponíveis na literatura. Para estabelecer tais métodos de construção, serão utilizados dois códigos clássicos distintos, não necessariamente auto-ortogonais. Uma das vantagens oferecidas por estes métodos de construção é que é possível

gerar códigos quânticos que agem nos qudits de forma a proteger os mesmos de forma desigual, ou seja, o código fornece proteções desiguais para os qudits. Desta forma, considerando construções de códigos *CSS* a partir de dois códigos clássicos distintos, não necessariamente auto-ortogonais, geramos novas famílias de códigos *CSS*, derivados de códigos clássicos cíclicos, *BCH*, *Reed-Solomon*, *Reed-Muller* e *Resíduos Quadráticos*. Além disso, baseado em idéias contidas em [14], construímos novas famílias de códigos quânticos *CSS* derivados de códigos gerados pelo produto tensorial de códigos clássicos *Reed-Solomon*.

Enfatizamos que em todos os novos métodos de construção que estão sendo propostos neste trabalho, são utilizados códigos clássicos lineares de bloco. As famílias de códigos quânticos gerados neste trabalho são compostas por bons códigos e, com exceção da família de códigos *CSS* derivados de códigos *Reed-Muller*, as demais são novas e não disponíveis na literatura. Pretendemos, futuramente, apresentar trabalhos onde são utilizados dois códigos convolucionais (não necessariamente auto-ortogonais) para a obtenção de novas famílias de códigos *CSS*.

Uma segunda etapa do desenvolvimento deste trabalho foi estabelecer condições para garantir que um código cíclico clássico (quântico) seja um código MDS (do inglês, maximum distance separable codes).

A terceira etapa deste trabalho consiste de conexões estabelecidas entre a teoria de códigos quânticos *CSS* e a teoria de matróides. Apesar deste não ser o objetivo principal, conseguimos resultados relevantes neste sentido, como, por exemplo, demonstrar que a função enumeradora de pesos de um códigos quântico *CSS* é uma avaliação do polinômio de Tutte do matróide soma direta derivado dos códigos clássicos utilizados na construção *CSS*. A tese está organizada como segue.

O Capítulo 1 apresenta uma revisão da Teoria de Codificação Quântica, contendo, como elemento principal a definição dos códigos quânticos de Calderbank-Shor-Steane, *CSS*.

No Capítulo 2, estabelecemos as primeiras contribuições desta tese. Apresentamos um método de construção que gera novas famílias de bons códigos quânticos *CSS* q-ários, derivados de dois códigos *Reed-Solomon* clássicos distintos, não necessariamente auto-ortogonais.

No Capítulo 3, que é o principal e mais importante capítulo deste trabalho, apresentamos seis novos métodos de construção, onde tais métodos produzem inúmeras novas famílias de bons códigos quânticos *CSS*, derivados de dois códigos clássicos cíclicos distintos q-ários, não necessariamente auto-ortogonais. Os principais métodos de construção apresentados no Capítulo 3 são os Métodos de Construção II, III e VI. Entretanto, o Método de Construção IV também gera novas famílias de bons códigos quânticos ternários. Tal método de construção tem como base algumas propriedades convenientes que as classes laterais ciclotômicas para $p = 3$ e $n = 3^m - 1$ possuem.

O Capítulo 4 estabelece um método de construção de códigos *CSS* derivados de códigos *Reed-Muller* e um método de construção de códigos *CSS* derivados de dois códigos do tipo *Resíduos quadráticos*.

O Capítulo 5 apresenta um novo método de construção de códigos *CSS* a partir de códigos-produto. Tal método de construção é baseado em propriedades de códigos produto clássicos.

No Capítulo 6, estabelecemos novas conexões entre a teoria dos códigos quânticos (clássicos) cíclicos e códigos quânticos (clássicos) MDS. Mais precisamente, estabelecemos condições para que um código quântico (clássico) cíclico seja um código MDS.

No Capítulo 7, que é um dos principais capítulos deste trabalho, estabelecemos as primeiras conexões entre a teoria de matróides e a teoria dos códigos quânticos *CSS*.

Finalmente, no Capítulo 8, relatamos as considerações finais deste trabalho.

As principais contribuições deste trabalho estão presentes nos Capítulos 3, 6 e 7.

Capítulo 1

Revisão de Codificação Quântica

Este capítulo apresenta uma revisão da teoria de codificação quântica. São definidos alguns conceitos e resultados necessários ao devenvolvimento desta tese, tais como, os Axiomas da Mecânica Quântica [1], os tipos mais comuns de erros quânticos [1], o Teorema da Discretização de Erros [1] e o principal elemento desta tese, ou seja, a classe dos códigos estabilizadores Calderbank-Shor-Steane (*CSS*) [1]. Enfatizamos que todos os resultados pertencentes a este capítulo podem ser encontrados em [1]. Algumas demonstrações de resultados em [1] não são encontradas na literatura, assim as apresentaremos no decorrer deste capítulo.

Ressaltamos que todos os métodos de construção de códigos quânticos propostos neste trabalho são métodos que utilizam a construção *CSS*, onde os códigos clássicos necessários para tais construções sempre serão dois códigos cíclicos clássicos distintos, não necessariamente auto-ortogonais.

O capítulo está organizado como segue. Na Seção 1.1, apresentamos os conceitos preliminares. Na Seção 1.2, descrevemos alguns tipos de ruídos quânticos e de operações quânticas e na Seção 1.3, introduzimos a teoria da correção quântica de erros.

1.1 Conceitos Preliminares

Enfatizamos, mais uma vez, que todos os resultados pertencentes a este capítulo podem ser encontrados em [1]. Começaremos esta seção definindo bit quântico, ou qubit, e depois enunciaremos os quatro postulados da mecânica quântica.

Definição 1.1.1 *Um qubit é um vetor unitário em um espaço vetorial complexo de duas dimensões. Podemos representar o estado geral de um qubit por*

$$| \psi\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle,$$

onde α e β são números complexos e os vetores $|\ 0\rangle$ e $|\ 1\rangle$ são vetores dados por $|\ 0\rangle = [1\ 0]^T$ e $|\ 1\rangle = [0\ 1]^T$, onde $[\quad]^T$ indica a operação de transposição de matrizes e $|\ .\ |$ denota o módulo de um número complexo. Além disso, $|\ \alpha\ |^2 + |\ \beta\ |^2 = 1$.

A notação $|\ .\rangle$ é chamada de notação de Dirac.

Os vetores $|\ 0\rangle$ e $|\ 1\rangle$ são denominados estados da base computacional e formam uma base ortonormal no espaço vetorial complexo de duas dimensões. Quando medimos um qubit, encontramos o estado $|\ 0\rangle$ com probabilidade $|\ \alpha\ |^2$ e o estado $|\ 1\rangle$ com probabilidade $|\ \beta\ |^2$.

Antes de prosseguir, enunciaremos as definições de *espaço de Hilbert*, *operador adjunto*, *operador hermitiano* e *operador unitário*.

Definição 1.1.2 *Dizemos que V é um espaço de Hilbert se V é um espaço vetorial com produto interno, completo em relação a este produto interno. Em outras palavras, toda seqüência de Cauchy converge para um elemento do conjunto, onde a convergência é em relação a este produto interno de V.*

Definição 1.1.3 *Seja T um operador linear em um espaço de Hilbert V. Então, existe um único operador linear $T^\dagger$ em V, tal que, para todos vetores $|\ v\rangle$, $|\ w\rangle$ em V,*

$$(|\ v\rangle, A\ |\ w\rangle) = (A^\dagger\ |\ v\rangle, |\ w\rangle),$$

onde $(\cdot,\cdot)$ denota o produto interno de V. Tal operador é denominado operador adjunto ou conjugado hermitiano de T.

Definição 1.1.4 *O operador linear $|w\rangle\langle v|$ de V para W (V e W são espaços vetoriais) é um operador cuja ação é dada por $(|w\rangle\langle v|)(|\ v'\rangle) = \langle v\ |\ v'\rangle\ |\ w\rangle$, onde $|\ v\rangle$ e $|\ v'\rangle$ são vetores de V e $|\ w\rangle$ é um vetor de W.*

Definição 1.1.5 *Seja T um operador linear em um espaço vetorial V. Se o operador adjunto de T, denotado $T^\dagger$, é o próprio operador T, ou seja $T^\dagger = T$, dizemos que T é operador auto-adjunto ou hermitiano.*

Definição 1.1.6 *Seja U um operador linear em um espaço vetorial V. Suponha que a matriz T_U seja a matriz que representa o operador U. Então, dizemos que U é um operador unitário se ${T_U}^\dagger T_U = I$, onde I é a matriz identidade e $\dagger$ é o conjugado (complexo) tranposto da respectiva matriz.*

Enunciaremos, a seguir, os quatro postulados que regem a mecânica quântica. O Postulado 1.1.1 estabelece o local no qual a mecânica quântica se desenrola, ou seja, o espaço de Hilbert.

Postulado 1.1.1 *A qualquer sistema físico isolado, existe associado um espaço vetorial complexo com produto interno (ou seja, um espaço de Hilbert), conhecido como espaço de estados do sistema. O sistema é completamente descrito pelo seu vetor de estado, um vetor unitário no espaço de estados.*

Já sabemos qual é o local que se desenrola a mecânica quântica. O Postulado 1.1.2, descreve como o sistema quântico evolui com o tempo.

Postulado 1.1.2 *A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Em outras palavras, o estado* $\mid \psi\rangle$ *de um sistema em um tempo* t_1 *está relacionado ao estado* $\mid \psi^{'}\rangle$ *do sistema em* t_2 *por um operador unitário* U *que depende somente de* t_1 *e* t_2*:*

$$\mid \psi^{'}\rangle = U \mid \psi\rangle.$$

Conforme o postulado anterior, a evolução de um sistema quântico fechado é descrita por um operador unitário. Mas o que acontece se quisermos inferir a respeito desse sistema? O que ocorre é que, para sabermos o que está acontecendo em um sistema quântico, precisaremos realizar uma medida sobre este. Para explicar o que acontece nessas situações, introduzimos o Postulado 1.1.3, que fornece o modo como as medidas sobre sistemas quânticos devem ser descritas.

Postulado 1.1.3 *As medidas quânticas são descritas por operadores de medida* $\{M_m\}$*. Esses operadores atuam sobre o espaço de estados do sistema. O índice* m *se refere aos possíveis resultados da medida. Se o estado de um sistema quântico for* $\mid \psi\rangle$*, imediatamente antes da medida, a probabilidade de um estado* m *ocorrer é dada por:*

$$p(m) = \langle \psi \mid M_m^{\dagger} M_m \mid \psi \rangle = (M_m \mid \psi\rangle, M_m \mid \psi\rangle),$$

e o estado do sistema após a medida será:

$$\frac{M_m \mid \psi\rangle}{\sqrt{\langle \psi \mid M_m^{\dagger} M_m \mid \psi \rangle}},$$

onde $\langle . \rangle$ *denota o produto interno.*

Os operadores de medida satisfazem a relação de completitude:

$$\sum_m M_m^{\dagger} M_m = I,$$

onde I *é o operador identidade.*

O Postulado 1.1.4, dado a seguir, descreve estados de um sistema composto, ou seja, descreve como o espaço de estados de um sistema composto deve ser construído a partir dos espaços de estados dos sistemas individuais.

Postulado 1.1.4 *O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas físicos individuais. Se os sistemas forem numerados de* 1 *até* n *e o sistema* i *for preparado no estado* $|\psi_i\rangle$*, decorre que o estado do sistema composto será dado por*

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle.$$

Tendo como base o Postulado 1.1.4, segue a definição de estados com n qubits.

Definição 1.1.7 *O estado geral de* n *qubits é uma combinação linear de estados da base computacional, onde os estados da base são dados por produtos tensoriais da forma*

$$|x_1 x_2 \cdots x_n\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle,$$

onde $x_i = |0\rangle$ *ou* $x_i = |1\rangle$*, para todo* $i = 1, 2, \cdots, n$*.*

Na seqüência, apresentamos conceitos tais como ruído quântico e operações quânticas. Antes disso, alguns conceitos preliminares serão estabelecidos.

Definição 1.1.8 *Seja* A *uma matriz. Definimos traço de* A*, denotado* $Tr(A)$*, como sendo a soma dos elementos de sua diagonal principal, ou seja,*

$$Tr(A) \equiv \sum_i A_{ii}.$$

O traço possui duas propriedades:

1) $Tr(A + B) = Tr(A) + Tr(B)$ (linearidade),

2) $Tr(AB) = Tr(BA)$ (propriedade cíclica),

onde A e B são duas matrizes quaisquer.

Definição 1.1.9 *Seja* T *um operador linear sobre um espaço vetorial* V*,* $|\psi\rangle \in V$ *e* $\langle . \rangle$ *um produto interno em* V*. Dizemos que* T *é um operador positivo se* $\langle \psi | A | \psi \rangle \geq 0$*, para todo* $|\psi\rangle \in V$*.*

Definição 1.1.10 *Considere um sistema quântico em um dentre muitos estados $|\psi_i\rangle$, com probabilidade p_i, sendo i um índice. Chamaremos o conjunto $\{p_i, |\psi_i\rangle\}$ um ensemble de estados puros. O operador densidade do sistema é definido por*

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

O operador densidade é também denominado *matriz densidade*.

Teorema 1.1.1 *Um operador ρ é operador densidade de um ensemble $\{p_i, |\psi_i\rangle\}$ se, e somente se, satisfizer as seguintes condições:*
1. *O traço de ρ deve ser igual a 1.*
2. *ρ deve ser positivo.*

Definição 1.1.11 *Suponha que se tenha dois sistemas A e B, cujo estado seja descrito por um operador densidade ρ^{AB}. O operador reduzido para o sistema A é definido por*

$$\rho^A \equiv Tr_B(\rho^{AB}),$$

onde Tr_B é uma operação conhecida como traço parcial sobre B. O traço parcial é definido por

$$Tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2| Tr_B(|b_1\rangle\langle b_2|),$$

onde $|a_1\rangle$ e $|a_2\rangle$ são quaisquer dois vetores do espaço de A e $|b_1\rangle$ e $|b_2\rangle$ são quaisquer dois vetores do espaço de B. Além disso, o traço parcial é uma operação linear.

O operador densidade reduzido de um sistema A é, de fato, uma descrição para o estado desse sistema (vide [1], página 136).

Definição 1.1.12 *Dizemos que um sistema quântico cujo vetor de estado $|\psi\rangle$ é conhecido exatamente está em um estado puro. Nesse caso, o operador densidade é simplesmente $\rho = |\psi\rangle\langle\psi|$. Quando isso não ocorre, dizemos que ρ é uma mistura de estados; em outras palavras dizemos que há uma mistura de diferentes estados puros no ensemble que define ρ.*

Teorema 1.1.2 *(Decomposição de Schmidt) Seja $|\psi\rangle$ um estado puro de um sistema AB. Então, existem estados ortonormais $|i_A\rangle$ de A e $|i_B\rangle$ de B tais que*

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle,$$

onde λ_i são números reais não negativos satisfazendo a condição $\Sigma_i {\lambda_i}^2 = 1$. Esses números são denominados coeficientes de Schmidt.

O Teorema da Decomposição de Schmidt é uma ferramenta importante e será utilizado na demonstração do Teorema 1.1.3. Como não encontramos a demonstração de tal resultado em nenhuma referência utilizada para a confecção desta tese, o faremos aqui.

Teorema 1.1.3 *Operadores densidade reduzidos são operadores densidade.*

Demonstração: Caso 1: Sejam A e B dois sistemas. Provaremos, sem perda de generalidade, que ρ^A é, de fato, um operador densidade para o sistema A.

Como ρ^{AB} é operador densidade para o sistema composto AB, então

$$\rho^{AB} = \sum_{i,j} p_{ij} |a_i b_j\rangle\langle a_i b_j|,$$

onde $|a_i\rangle$ são estados de A e $|b_j\rangle$ são estados de B; aqui, consideramos que nenhum estado é emaranhado, onde estado emaranhado significa um estado quântico que não pode ser decomposto em produto tensorial de estados de um qubit.

Então, temos que

$$\rho^A \equiv Tr_B(\rho^{AB}) = Tr_B(\sum_{i,j} p_{ij} |a_i b_j\rangle\langle a_i b_j|). \tag{1.1}$$

Agora, demonstraremos que a equação

$$|x_1 x_2\rangle\langle y_1 y_2| = |x_1\rangle\langle y_1| \otimes |x_2\rangle\langle y_2| \tag{1.2}$$

é verdadeira, para quaisquer estados $|\psi\rangle$ do sistema composto AB.

Seja $|\psi\rangle$ um estado qualquer do sistema composto AB. Conseqüentemente,

$$\begin{aligned} |x_1 x_2\rangle\langle y_1 y_2|(|\psi\rangle) = & \\ & \stackrel{dec.Schmidt}{=} |x_1 x_2\rangle\langle y_1 y_2|(\sum_i \lambda_i |i_A\rangle|i_B\rangle) \\ & = \left(\sum_i \lambda_i \langle y_1 y_2 | i_A i_B\rangle\right) |x_1 x_2\rangle, \end{aligned}$$

ou ainda

$$\begin{aligned} [|x_1\rangle\langle y_1| \otimes |x_2\rangle\langle y_2|](|\psi\rangle) = & \\ & \stackrel{dec.Schmidt}{=} [|x_1\rangle\langle y_1| \otimes |x_2\rangle\langle y_2|](\sum_i \lambda_i |i_A\rangle|i_B\rangle) \\ & = \sum_i \lambda_i [\langle y_1|i_A\rangle|x_1\rangle] \otimes [\langle y_2|i_B\rangle|x_2\rangle] \\ & = \sum_i \lambda_i [\langle y_1|i_A\rangle\langle y_2|i_B\rangle] |x_1 x_2\rangle \\ & \stackrel{def}{=} \left(\sum_i \lambda_i \langle y_1 y_2 | i_A i_B\rangle\right) |x_1 x_2\rangle. \end{aligned}$$

Como para quaisquer estados do sistema composto as imagens das aplicações são iguais, podemos concluir que

$$|x_1x_2\rangle\langle y_1y_2| = |x_1\rangle\langle y_1| \otimes |x_2\rangle\langle y_2|,$$

donde a equação (1.1) é igual a:

$$= Tr_B(\sum_{i,j} p_{ij}|a_i\rangle\langle a_i| \otimes |b_j\rangle\langle b_j|) \stackrel{def}{=} \sum_{i,j} p_{ij}|a_i\rangle\langle a_i|Tr_B(|b_j\rangle\langle b_j|) = \sum_i p_i|a_i\rangle\langle a_i|.$$

Logo,

$$\rho^A = \sum_i p_i|a_i\rangle\langle a_i| \ ,$$

e assim, concluímos que ρ^A é um operador densidade para o sistema A.

Caso 2: No caso de existir estados emaranhados, utilizaremos a Decomposição de Schmidt. A demonstração que apresentaremos agora abrange todos os casos possíveis. O Caso 1 é um caso particular desta.

Sabemos que

$$\rho^{AB} = \sum_i p_i|\psi_i\rangle\langle\psi_i|.$$

Utilizando a Decomposição de Schmidt, segue que

$$\begin{aligned}
\rho^A \equiv Tr_B(\rho^{AB}) &= Tr_B(\sum_i p_i \sum_{j_i} \lambda_{j_i}(\lambda_{j_i})^*|j_{iA}j_{iB}\rangle\langle j_{iA}j_{iB}|) \\
&= \sum_i p_i \sum_{j_i} {\lambda_{j_i}}^2|j_{iA}\rangle\langle j_{iA}|Tr_B|j_{iB}\rangle\langle j_{iB}| \\
&= \sum_i p_i \sum_{j_i} {\lambda_{j_i}}^2|j_{iA}\rangle\langle j_{iA}| \\
&= p_1 \sum_{j_1} {\lambda_{j_1}}^2|j_{1A}\rangle\langle j_{1A}| + \cdots + p_n \sum_{j_n} {\lambda_{j_n}}^2|j_{nA}\rangle\langle j_{nA}| \\
&= \sum_{i,j_i} p_i{\lambda_{j_i}}^2|j_{iA}\rangle\langle j_{iA}| \\
&= \sum_{j_i} \zeta_{j_i}|j_{iA}\rangle\langle j_{iA}|,
\end{aligned}$$

onde

$$\zeta_{j_i} = p_i \sum_{j_i} {\lambda_{j_i}}^2, \ \sum_{j_i} \zeta_{j_i} = 1,$$

e os ζ_{j_i} são números reais não negativos.

Assim, ρ^A é um operador densidade para o sistema A. □

1.2 Ruído Quântico e Operações Quânticas

O formalismo das operações quânticas é uma ferramenta genérica para a descrição da evolução de sistemas quânticos em diversas situações, incluindo mudanças de estados quânticos, assim como processos Markovianos descrevem mudanças aleatórias em estados clássicos. Da mesma forma que um estado clássico é descrito por um vetor de probabilidades, os estados quânticos serão descritos por um operador densidade (matriz densidade) ρ, cujas propriedades já foram listadas. De forma análoga ao caso clássico, estados quânticos se transformam como

$$\rho' = \varepsilon(\rho), \tag{1.3}$$

onde ε é uma operação quântica. Dois exemplos de operações quânticas são as transformações unitárias e as medidas, para as quais, $\varepsilon(\rho) = U\rho U^\dagger$ e $\varepsilon(\rho) = M_m \rho {M_m}^\dagger$, respectivamente.

As operações quânticas refletem as mudanças dinâmicas de um estado quântico que resulta de algum processo físico; ρ é o estado antes de o processo ocorrer e $\varepsilon(\rho)$ é o estado final após o processo ter ocorrido, possivelmente, a menos de um fator de normalização.

Apresentaremos três definições equivalentes para as operações quânticas, que oferecem diferentes vantagens, dependendo das aplicações desejadas.

A primeira definição é baseada na idéia do estudo da dinâmica como resultado da interação de um sistema e sua vizinhança. Essa definição é concreta e fácil de ser relacionada ao mundo real, mas não é matematicamente adequada.

A segunda é conhecida como representação de operador soma e a terceira definição é feita através dos axiomas fisicamente motivados.

1.2.1 O Ambiente e as operações quânticas

A dinâmica de um sistema quântico fechado é descrita por transformações unitárias. Uma forma geral de se descrever a dinâmica de um sistema quântico aberto é vê-la como surgindo de uma interação entre o sistema de interesse, que chamamos de sistema principal, e um ambiente. Juntos, o sistema e o ambiente formam um sistema quântico fechado. Em outras palavras, suponha que se tenha um sistema em um estado ρ e que seja mandado através de uma caixa (transformação unitária) acoplada ao ambiente. Em geral, o estado final do sistema, $\varepsilon(\rho)$, pode não estar relacionado a ρ por uma transformação unitária. Suporemos que o estado de entrada do sistema seja o produto $\rho \otimes \rho_{amb}$. Após a transformação U da caixa, o sistema não interage mais com o ambiente, e podemos fazer o traço parcial sobre o ambiente para obtermos o estado reduzido do sistema em separado:

$$\varepsilon(\rho) = Tr_{amb}[U(\rho \otimes \rho_{amb})U^\dagger]. \tag{1.4}$$

Essa é a primeira das três definições equivalentes. Em geral, não é necessário que o sistema e o ambiente iniciem em um estado produto. Contudo, em muitos casos de interesse prático, essa suposição é razoável e, na maior parte de nossas discussões, as operações quânticas serão sobre um mesmo espaço A. Mesmo assim, o formalismo das operações quânticas permite que se descreva a dinâmica quântica quando o sistema e a vizinhança não partem de um estado produto.

Convém notar que estamos descrevendo operações quânticas como surgindo da interação de um *sistema principal* e do *ambiente*. Porém, é conveniente generalizar a definição de modo a permitir espaços de entrada e saída diferentes.

1.2.2 Representação de operador-soma

Podemos reformular a equação (1.4) de forma que esta se apresente somente em termos de operadores do espaço de Hilbert do sistema principal. Este fato produz uma melhoria para a manipulação de operações quânticas. Explicitaremos agora, tal reformulação.

Seja $|e_k\rangle$ uma base ortonormal do espaço de estados (que possui dimensão finita) do ambiente, e $\rho_{amb} = |e_0\rangle\langle e_0|$ seu estado inicial, que é o operador densidade associado ao estado puro inicial $|e_0\rangle$ do ambiente. A suposição de que o ambiente parte de um estado puro pode ser feita sem perda de generalidade, pois se o estado fosse um estado misto, poderíamos introduzir um sistema extra para "purificar" o ambiente (vide [1], Seção 2.5).

Embora o sistema extra seja "fictício", não faz diferença para a dinâmica do sistema principal, e portanto, pode ser usado em passos intermediários do cálculo. Logo, a equação (1.4) pode ser escrita como

$$\varepsilon(\rho) \overset{\mathbf{a})}{=} \sum_k \langle e_k|U[\rho \otimes |e_0\rangle\langle e_0|]U^\dagger|e_k\rangle \overset{\mathbf{b})}{=} \sum_k E_k \rho {E_k}^\dagger, \tag{1.5}$$

onde $E_k \equiv \langle e_k|U|e_0\rangle$ é um operador (*) sobre o espaço de estados do sistema principal. A equação acima é conhecida como a representação de operador-soma de ε.

A passagem *a)* se explica pelos fatos considerados a seguir.

Um operador linear pode ser representado de maneira única por uma matriz, uma vez fixada a base. Calculando, então, o produto interno do estado resultante da aplicação da matriz correspondente ao operador linear, a cada estado da base, pelo mesmo estado, teremos os elementos da diagonal principal da matriz, pois quando fazemos esses produtos internos, estamos calculando os coeficientes de $U|e_i\rangle$, em relação ao estado $|e_i\rangle$. Somando-se esses produtos internos, que são números complexos, resultará na operação de traço. Podemos proceder desta forma, pois sabemos que o ambiente não afeta o sistema principal.

A passagem *b)* se deve essencialmente ao fato de que portas de 1 qubit e a porta $CNOT$

são portas universais, ou seja, qualquer operador unitário arbitrário pode ser expresso como produto de operadores unitários com o operador $CNOT$.

(*) Para melhor entendimento, segue um exemplo. Em termos de matrizes a porta $CNOT$ pode ser representada por

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

De outro modo, pode ser escrita em termos de operadores lineares como sendo

$$CNOT = |0_P 0_A\rangle\langle 0_P 0_A| + |0_P 1_A\rangle\langle 0_P 1_A| + |1_P 1_A\rangle\langle 1_P 1_A| + |1_P 1_A\rangle\langle 1_P 1_A|.$$

Logo,

$$E_0 = \langle 0_A|U|0_A\rangle = |0_P\rangle\langle 0_P|$$

e

$$E_1 = \langle 1_A|U|0_A\rangle = |1_P\rangle\langle 1_P|,$$

e assim,

$$\varepsilon(\rho) = E_0\rho E_0 + E_1\rho E_1.$$

Na verdade, (*) é um exemplo que mostra que $E_k \equiv \langle e_k|U|e_0\rangle$ é um operador sobre o espaço de estados do sistema principal, e não um escalar. Qualquer transformação unitária pode agir em qubits separadamente, deixando invariante os demais qubits. Isso porque, além dos projetores constituintes da porta $CNOT$ possuírem essa característica, claramente todas as portas de 1 qubit também agem em cada qubit separadamente.

Os elementos E_k são chamados de *elementos de operação* da operação quântica ε. Como no caso clássico, temos uma distribuição de probabilidade descrevendo a relação sistema-ruído. Analogamente para o caso quântico, requeremos que o traço de $\varepsilon(\rho)$ seja igual a 1:

$$1 = Tr(\varepsilon(\rho)) = Tr(\sum_k E_k\rho {E_k}^\dagger) \overset{def1_{1)}}{=} \sum_k Tr(E_k\rho {E_k}^\dagger) \tag{1.6}$$

$$\overset{def1_{2)}}{=} \sum_k Tr({E_k}^\dagger E_k\rho) = Tr(\sum_k {E_k}^\dagger E_k\rho). \tag{1.7}$$

Como essa relação deve valer para todo ρ, devemos ter

$$\sum_k E_k {E_k}^\dagger = I. \tag{1.8}$$

Em seguida, demonstraremos essa última afirmação para o espaço de um qubit.

Suponha que T seja um operador no espaço de estados de um qubit. Suponha também que, para todo operador densidade ρ, $Tr(T\rho) = 1$. Assim, segue que $E = I$, onde I é a matriz identidade.

Demonstração: Seja T um operador linear no espaço de estados de um qubit, representado pela matriz

$$T = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

onde a, b, c, d são números complexos. Seja $\rho = |0\rangle\langle 0|$. Escrevendo em forma matricial, sabemos que

$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad e \quad T\rho = \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix}.$$

Como $Tr(T\rho) = 1$, temos $a = 1$.

Analogamente, considerando $\rho = |1\rangle\langle 1|$, temos que

$$\rho = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad e \quad T\rho = \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix},$$

donde $d = 1$. Conseqüentemente, a matriz de T é dada por

$$T = \begin{bmatrix} 1 & b \\ c & 1 \end{bmatrix}.$$

Fazendo $\rho = 1/2(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)$, concluímos que

$$T\rho = \begin{bmatrix} 1 & b \\ c & 1 \end{bmatrix} \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = \begin{bmatrix} 1/2 + b/2 & 1/2 + b/2 \\ 1/2 + c/2 & 1/2 + c/2 \end{bmatrix}.$$

Como $Tr(T\rho) = 1$, são válidas as equações

$$\frac{b+c}{2} + 1 = 1, \quad donde \quad \frac{b+c}{2} = 0 \quad e \quad b = -c.$$

Logo, concluímos que

$$T = \begin{bmatrix} 1 & b \\ -b & 1 \end{bmatrix}.$$

□

A equação (1.11) é conhecida como *relação de completitude*. Essa relação é satisfeita para operações que preservam o traço. Existem também operações que não preservam o traço, para as quais

$$\sum_k E_k {E_k}^\dagger \leq I. \tag{1.9}$$

A notação $A \leq B$ denota $A(x) \leq B(x)$, para todo x pertencente ao domínio de A, que é igual ao domínio de B.

Aplicações ε como a equação (1.3), para os quais $\sum_k E_k {E_k}^\dagger \leq I$, fornecem a segunda definição de operação quântica. A representação de operador soma é importante porque fornece uma forma *intrínseca* de caracterização da dinâmica do sistema principal, pois os elementos de operação atuam somente neste.

1.2.3 Interpretação física do operador-soma

Consideremos o princípio da medida implícita: sem perda de generalidade, qualquer "condutor quântico aberto" (qubits não sofrem medições), ao final de um circuito, pode ser considerado medido. Em outras palavras, se o sistema possui 2 qubits, a matriz densidade reduzida do primeiro qubit não é afetada por medidas sobre o segundo qubit.

Suponha que seja feita uma medida na base $|e_k\rangle$ do ambiente, após a transformação U ter atuado. Aplicando o princípio da medida implícita, decorre que tal operação afeta somente o estado do ambiente e não muda o estado do sistema principal.

Se ρ_k é o estado do sistema principal e k é o resultado da medida, segue que

$$\begin{aligned}\rho_k &\propto Tr_E(|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|) \\ &= \langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle = E_k \rho {E_k}^\dagger.\end{aligned}$$

Normalizando ρ_k,

$$\rho_k = \frac{E_k \rho {E_k}^\dagger}{Tr(E_k \rho {E_k}^\dagger)},$$

encontramos a probabilidade de que o resultado seja k:

$$Tr(|e_k\rangle\langle e_k|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_k\rangle\langle e_k|) = Tr(E_k \rho {E_k}^\dagger),$$

donde

$$\varepsilon(\rho) = \sum_k p(k)\rho_k = \sum_k E_k \rho {E_k}^\dagger.$$

Isso fornece uma interpretação física do que acontece com os elementos de operação $\{E_k\}$, em uma operação quântica. A ação da operação quântica é equivalente a tomar o estado ρ e substituí-lo aleatoriamente por

$$\rho_k = E_k \rho {E_k}^\dagger / Tr(E_k \rho {E_k}^\dagger),$$

com probabilidade $Tr(E_k \rho {E_k}^\dagger)$. Nesse sentido, a situação é muito semelhante ao que ocorre com o conceito de canais de comunicação ruidosos.

1.2.4 Medidas e representação do operador-soma

Estenderemos o resultado anterior, realizando uma medida sobre o sistema combinado. Essa possibilidade física está naturalmente conectada às operações quânticas que não preservam o traço.

Suponha que o sistema principal se encontre inicialmente em um estado ρ. Denotaremos o sistema principal pela letra Q e o ambiente pela letra E, onde Q e E são independentes. O estado inicial do sistema composto será, então,

$$\rho^{QE} = \rho \otimes \sigma.$$

Seja U uma transformação unitária entre os sistemas. Após essa interação, uma medida projetiva é realizada no sistema conjunto, descrita pelos projetores P_m. O estado final de QE é dado por

$$\frac{P_m U(\rho \otimes \sigma) U^\dagger P_m}{Tr(P_m U(\rho \otimes \sigma) U^\dagger)},$$

para o resultado m da medida. Aplicando o traço sobre os estados de E, obtemos o estado final somente de Q,

$$\frac{Tr_A(P_m U(\rho \otimes \sigma) U^\dagger P_m)}{Tr(P_m U(\rho \otimes \sigma) U^\dagger)},$$

para o resultado m da medida. Essa representação do estado final envolve o estado inicial σ do ambiente, a interação U e os operadores de medida P_m.

Definamos uma aplicação

$$\varepsilon_m(\rho) \equiv Tr_A(P_m U(\rho \otimes \sigma) U^\dagger P_m),$$

de forma que o estado final de Q se torne o estado $\varepsilon_m(\rho)/Tr(\varepsilon_m(\rho))$. Seja $\sigma = \Sigma_j q_j |j\rangle\langle j|$ uma decomposição de ensemble para σ. Introduzindo uma base ortonormal $|e_k\rangle$ para o ambiente E, concluímos que

$$\varepsilon_m(\rho) = \sum_{jk} q_j Tr_A(|e_k\rangle\langle e_k| P_m U(\rho \otimes |j\rangle\langle j|) U^\dagger P_m |e_k\rangle\langle e_k|) =$$

$$\sum_{jk} E_{jk} \rho {E_{jk}}^\dagger,$$

onde $E_{jk} \equiv \sqrt{q_j}\langle e_k| P_m U |j\rangle$.

Essa equação é uma generalização da equação (1.3) e fornece uma maneira explícita para o cálculo dos operadores que aparecem na representação de operador-soma.

1.2.5 Modelos de sistema-ambiente para operador-soma

Foi demonstrado que sistemas quânticos que interagem dão origem de forma natural a uma representação de operador-soma para operações quânticas. E o problema recíproco? Dado um conjunto de operadores E_k, existe algum modelo razoável para o ambiente, para o sistema e para a dinâmica, que dê origem a operações quânticas com aqueles elementos de operação? Em particular, mostraremos que, para qualquer operação quântica ε que preserve ou não o traço, com elementos de operação E_k, existe um modelo de ambiente E, partindo de um estado puro $|e_0\rangle$, uma dinâmica especificada pelo operador unitário U e um projetor P_m sobre E, tais que

$$\varepsilon(\rho) = Tr_A(PU(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger P).$$

Primeiramente, suponha que ε seja uma operação quântica que preserva o traço. Suponha também que ε possua representação de operador-soma gerada pelos elementos de operação E_k, que satisfazem a relação de completitude. Assim, precisamos encontrar um operador unitário apropriado, U, que modele a dinâmica.

Seja $|e_k\rangle$ uma base ortonormal de E em correspondência 1-1 com o índice k dos operadores E_k. Note que, por definição, E possui tal base; o que se deseja é encontrar um modelo para o ambiente que dê origem à dinâmica descrita pelos elementos de operação E_k. Defina um operador U do seguinte modo,

$$U|\psi\rangle|e_0\rangle \equiv \sum_k E_k|\psi\rangle|e_k\rangle,$$

onde $|e_0\rangle$ é um estado-padrão do ambiente modelo. Ainda, observe que, para estados arbitrários $|\psi\rangle|\varphi\rangle$ do sistema principal, são válidas as seguintes equações

$$\langle\psi|\langle e_0|U^\dagger U|\varphi\rangle|e_0\rangle = \sum_k \langle\psi|{E_k}^\dagger E_k|\varphi\rangle = \langle\psi|\varphi\rangle,$$

onde foi utilizada a relação de completitude.

Assim, o operador U pode ser visto como um operador unitário que atua sobre todo o espaço de estados do sistema conjunto, devido ao teorema dado a seguir.

Teorema 1.2.1 *Seja V um espaço de Hilbert com subespaço W e $U : W \longrightarrow V$ um operador unitário que preserva o produto interno, ou seja, para quaisquer $|w_1\rangle, |w_2\rangle$ em W,*

$$\langle w_1|U^\dagger U|w_2\rangle = \langle w_1|w_2\rangle.$$

Então, existe um operador unitário $U' : V \longrightarrow V$ que estende U.

Demonstração: Suponha que $U(W)$ tenha dimensão d e que V tenha dimensão n. Suponha ainda que $\beta = \{|e_1\rangle, \cdots, |e_d\rangle\}$ seja uma base ortonormal de $U(W)$. Completamos essa base para formar uma base ortonormal de V, utilizando o processo de Gram-Schmidt.

Sejam $|e_{d+1}\rangle, \cdots, |e_n\rangle$ os vetores ortonormais que completam β para formar uma base de V. Definimos, agora, o operador $U^{'}$, que será o operador que estende U:

$$\begin{aligned} U^{'}|w\rangle = U|w\rangle, \quad |w\rangle \ \epsilon \ W, \\ U^{'}|e_{d+1}\rangle = |e_{d+1}\rangle \\ U^{'}|e_{d+2}\rangle = |e_{d+2}\rangle \\ \cdots \\ U^{'}|e_n\rangle = |e_n\rangle. \end{aligned}$$

Decorrente dessa definição, a matriz do operador $U^{'}$ é composta somente por vetores ortonormais, donde o operador $U^{'}$ é unitário e ainda estende U, o que conclui a demonstração. □

Falta demonstrar que a seguinte equação é válida:

$$Tr_A(U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger) = \sum_k E_k \rho {E_k}^\dagger.$$

Demonstração: De fato,

$$Tr_A(U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger) = \sum_k \langle e_k|U[\rho \otimes |e_0\rangle\langle e_0|]U^\dagger|e_k\rangle = \sum_k F_k \rho {F_k}^\dagger,$$

onde $F_k \equiv \langle e_k|U|e_0\rangle$. Mas, $U|\psi\rangle|e_0\rangle \equiv \sum_k E_k|\psi\rangle|e_k\rangle$. Assim, pela ortonormalidade dos estados $|e_k\rangle$, vale a seguinte equação

$$F_k \equiv \langle e_k|U|e_0\rangle = \langle e_k| \sum_{k'} E_{k'}|\psi\rangle|e_{k'}\rangle = E_k.$$

Logo,

$$Tr_A(U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger) = \sum_k E_k \rho {E_k}^\dagger,$$

e portanto, o modelo fornece operações quânticas ε com elementos de operação $\{E_k\}$. □

1.2.6 Abordagem axiomática para as operações quânticas

Definiremos uma operação quântica ε como sendo uma aplicação de um conjunto de operadores densidade de um espaço de entrada Q_1 para um conjunto de operadores densidade de um espaço Q_2, com as seguintes propriedades axiomáticas (no nosso caso $Q_1 = Q_2 = Q$):

A1) $\mathrm{Tr}[\varepsilon(\rho)]$ é a probabilidade de que o processo representado por ε ocorra, quando ρ for o estado inicial. Logo, $0 \leq Tr[\varepsilon(\rho)] \leq 1$.

A2) ε é uma aplicação *linear convexa* sobre o primeiro conjunto de matrizes densidade, ou seja, para probabilidades $\{p_i\}$, é válida a equação

$$\varepsilon\left(\sum_i p_i\rho_i\right) = \sum_i p_i\varepsilon(\rho_i). \tag{1.10}$$

A3) ε é uma aplicação *positiva completa*, isto é, se ε mapeia operadores densidade de um sistema Q_1 para operadores densidade de um sistema Q_2, $\varepsilon(A)$ deve ser positivo para qualquer operador positivo A. Além disso, se introduzirmos um sistema extra R com dimensão arbitrária, deve valer que $(I\otimes\varepsilon)(A)$ é positivo para qualquer operador positivo A sobre o sistema combinado RQ_1, onde I é a aplicação identidade sobre R.

Esses três axiomas, que formam a abordagem axiomática para operações quânticas, são equivalentes à representação de operador-soma, como veremos no Teorema 1.2.2, dado a seguir. Essa abordagem axiomática para operações quânticas é um outro modo de se interpretar o que ocorre em um sistema quântico aberto, quando um ruído age sobre este.

Teorema 1.2.2 *A aplicação ε satisfaz os axiomas* **A1, A2 e A3** *se, e somente se,*

$$\varepsilon(\rho) = \sum_i E_i\rho{E_i}^\dagger,$$

para algum conjunto de operadores $\{E_i\}$ que mapeiam o espaço de Hilbert de entrada para o espaço de Hilbert de saída, onde $\sum_k E_k{E_k}^\dagger \leq I$.

A notação $A \leq B$ denota $A(x) \leq B(x)$, para todo x pertencente ao domínio de A, que é igual ao domínio de B.

Uma pergunta surge naturalmente. Será que o conjunto de operadores $\{E_i\}$ que mapeia o espaço de Hilbert de entrada para o espaço de Hilbert de saída é único? A resposta para essa pergunta é dada pelo Teorema 1.2.3.

Teorema 1.2.3 *(Liberdade Unitária na representação de operador-soma) Sejam $\{E_1, ..., E_m\}$ e $\{F_1, ..., F_n\}$ elementos de operação que originam as operações quânticas ε e F, respectivamente. Adicionando operadores nulos na lista menor, podemos assegurar que $m = n$. Logo, $\varepsilon = F$ se, e somente se, existirem números complexos u_{ij} tais que $E_i = \Sigma_j u_{ij}F_j$ e u_{ij} sejam os elementos de uma matriz unitária m por m.*

A positividade completa é uma propriedade muito importante das operações quânticas, pois permite que operadores densidade sejam "levados" em operadores densidade, além de transformar operadores densidade do sistema conjunto em operadores densidade.

Exemplo 1.2.1 *(Exemplo de um operador que é positivo mas não é positivo completo) Considere a transposição de um único qubit, que transpõe o operador densidade na base computacional:*

$$\left[\begin{array}{cc} a & b \\ c & d \end{array}\right] \xrightarrow{T} \left[\begin{array}{cc} a & c \\ b & d \end{array}\right].$$

Essa aplicação preserva a positividade de um único qubit.

De fato, a operação de transposição leva operadores densidade em operadores densidade, pois

$$\rho^T = (\sum_i p_i|\psi_i\rangle\langle\psi_i|)^T = \sum_i p_i(|\psi_i\rangle\langle\psi_i|)^T = \sum_i p_i|\psi_i{}^*\rangle\langle\psi_i{}^*|.$$

Além disso, se A é um operador positivo, onde

$$A = \left[\begin{array}{cc} a & b \\ c & d \end{array}\right],$$

temos que

$$(c(\lambda))_A = det(A - \lambda I) = (a-\lambda)(d-\lambda) - cb.$$

Como

$$A^T = \left[\begin{array}{cc} a & c \\ b & d \end{array}\right],$$

concluímos que

$$(c(\lambda))_{A^T} = det(A^T - \lambda I) = (a-\lambda)(d-\lambda) - bc,$$

donde $(c(\lambda))_A = (c(\lambda))_{A^T}$.
Como o operador A é positivo, seu transposto possui os mesmos autovalores. Assim, a transposição também é um operador positivo.

Suponha agora que o qubit seja parte de um sistema de dois qubits, inicialmente no estado emaranhado $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Suponha também que a operação de transposição seja aplicada ao primeiro dos dois qubits, enquanto o segundo qubit evolui com a dinâmica usual. Calculando o operador densidade após as operações, deduzimos que

$$\begin{aligned} & T \otimes \mathcal{I}(|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|) \\ & \overset{(3)}{=} T \otimes \mathcal{I}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|) \\ & = 1/2(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|) \end{aligned}$$

$$= 1/2 \left(\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right] + \left[\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right] + \left[\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right] + \left[\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \right)$$

$$= 1/2 \left(\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \right).$$

Esse operador tem autovalores $1/2$*,* $1/2$*,* $1/2$ *e* $-1/2$*, donde não é um operador positivo. Portanto, tal operador não pode ser um operador densidade.*

1.2.7 Exemplos de operações e ruídos quânticos

Traço

A operação mais simples relacionada à medida é a aplicação traço: $\rho \longrightarrow Tr(\rho)$, que é, de fato, uma operação quântica.

Para verificar este fato, seja H_Q um espaço de Hilbert gerado por uma base ortonormal $|1\rangle, ..., |d\rangle$, e seja $H_Q{}'$ um espaço de saída unidimensional, gerado pelo estado $|0\rangle$.

Definamos

$$\varepsilon(\rho) \equiv \sum_{i=1}^{d} |0\rangle\langle i|\rho|i\rangle\langle 0|.$$

Pelo Teorema 1.2.2, $\varepsilon(\rho)$ é uma operação quântica.

Agora, demonstraremos que é válida a equação

$$\varepsilon(\rho) = Tr(\rho)|0\rangle\langle 0|.$$

Demonstração: Sabemos que

$$\langle i|\rho|i\rangle = Tr(\rho|i\rangle\langle i|)$$

(vide [1], equações (2.60) e (2.61)).

Além disso, vale que

$$\varepsilon(\rho) \quad = \quad \sum_{i=1}^{d} |0\rangle\langle i|\rho|i\rangle\langle 0| = \sum_{i=1}^{d} |0\rangle Tr(\rho|i\rangle\langle i|)\langle 0|. \tag{1.11}$$

Utilizaremos e demonstraremos a equação a seguir:

$$\sum_i |w\rangle\langle v_i| = |w\rangle(\sum_i \langle v_i|). \tag{1.12}$$

Considere $|v\rangle$ sendo um vetor qualquer do sistema. Então,

$$\sum_i |w\rangle\langle v_i|(|v\rangle) = \sum_i |w\rangle\langle v_i|v\rangle \overset{def}{=} \sum_i (\langle v_i|v\rangle)|w\rangle. \tag{1.13}$$

Ainda, são válidas as equações

$$\left[|w\rangle(\sum_i \langle v_i|)\right](|v\rangle) = |w\rangle\left[(\sum_i \langle v_i|)(|v\rangle)\right] \overset{def}{=} |w\rangle\left[\sum_i (\langle v_i|v\rangle)\right] = \sum_i (\langle v_i|v\rangle)|w\rangle,$$

donde concluímos a equação (1.12).

A equação (1.11) é igual a

$$= \quad |0\rangle Tr(\rho \sum_i |i\rangle\langle i|)\langle 0| = |0\rangle tr(\rho I)\langle 0| = Tr(\rho)|0\rangle\langle 0|,$$

e assim,

$$\varepsilon(\rho) = Tr(\rho)|0\rangle\langle 0|.$$

Portanto, a menos do fator multiplicativo $|0\rangle\langle 0|$, essa operação quântica é idêntica à operação traço. □

Traço parcial

Suponha que se tenha um sistema conjunto QR e que se queira realizar o traço sobre o subsistema R. Seja $|j\rangle$ uma base para o sistema R e defina um operador linear

$$E_i : H_{QR} \longrightarrow H_Q,$$

$$E_i\left(\sum_j \lambda_j |q_j\rangle|j\rangle\right) \equiv \lambda_i |q_i\rangle,$$

onde λ_j são números complexos e $|q_i\rangle$ são estados arbitrários do sistema Q. Defina uma operação quântica ε com elementos de operação $\{E_i\}$ dada por

$$\varepsilon(\rho) \equiv \sum_i E_i \rho {E_i}^\dagger.$$

Pelo Teorema 1.2.2, essa é uma operação quântica do sistema QR para o sistema Q. Note que

$$\varepsilon(\rho \otimes |j\rangle\langle j^{'}|) = \rho\delta_{j,j'} = Tr_R(\rho \otimes |j\rangle\langle j^{'}|),$$

onde ρ é um operador hermitiano no espaço de estados de Q e $|j\rangle$ e $|j^{'}\rangle$ são elementos de uma base ortonormal de R. Pela linearidade de ε e pelas propriedades da operação Tr_R, segue que $\varepsilon = Tr_R$.

Canal de inversão de bit e inversão de fase

O canal de *inversão de bit* inverte o estado de um qubit de $|0\rangle$ para $|1\rangle$ (e vice-versa) com probabilidade de *1-p*. Seus elementos de operação são dados por

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad e \quad E_1 = \sqrt{1-p}X = \sqrt{1-p}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

O canal de *inversão de fase* tem os seguintes elementos de operação:

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad e \quad E_1 = \sqrt{1-p}Z = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Canal de despolarização

O canal de despolarização é um importante tipo de ruído quântico. Suponha que se tenha um qubit com probabilidade p de ser despolarizado, ou seja, de ser substituído pelo estado completamente misturado $I/2$. A probabilidade de que ele permaneça polarizado é $1-p$. O estado do sistema após esse processo de ruído é:

$$\varepsilon(\rho) = \frac{pI}{2} + (1-p)\rho.$$

Essa equação pode ser colocada na forma de operação quântica:

$$\varepsilon(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z).$$

Atenuação de amplitude

Uma importante aplicação das operações quânticas é a dissipação de energia de sistemas quânticos. Qual a dinâmica de um átomo que espontaneamente emite um fóton? Como um sistema de spins a altas temperaturas se aproxima do equilíbrio com o ambiente? Cada um desses processos têm características particulares, mas o comportamento geral de todos eles é

bem caracterizado por uma operação quântica conhecida como *atenuação de amplitude*. Os elementos de operação são dados por:

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \qquad E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}.$$

1.2.8 Limitações do formalismo de operações quânticas

Suponha que um único qubit seja preparado em algum estado desconhecido ρ. Imagine que dentre os graus de liberdade esteja um qubit que, como conseqüência secundária da preparação, será posto no estado $|0\rangle$, caso ρ pertença à metade inferior da esfera de Bloch, ou no estado $|1\rangle$, caso ρ pertença à metade superior da esfera de Bloch. Então, o estado do sistema após a preparação será igual a

$$\rho \otimes |0\rangle\langle 0| \otimes \ \textit{outros graus de liberdade},$$

se ρ estiver na parte inferior da esfera, ou

$$\rho \otimes |1\rangle\langle 1| \otimes \ \textit{outros graus de liberdade},$$

se ρ estiver na parte superior da esfera.

Suponha que a interação seja tal que uma operação $CNOT$ seja implementada entre o sistema principal e o qubit extra no sistema de laboratório. Dessa forma, se o vetor inicial estiver na metade inferior da esfera de Bloch, o estado permanecerá invariante no processo, mas se estiver na metade superior, ele será rodado para a metade inferior, donde não se tem, obviamente, uma aplicação afim atuando na esfera de Bloch. Pelo Teorema 1.2.2, essa operação não pode ser uma operação quântica. Logo, não podemos esquecer que, existem circunstâncias fisicamente razoáveis sob as quais o formalismo de operações quânticas pode não descrever adequadamente o que ocorre com o sistema.

1.3 Teoria da Correção Quântica de Erro

Para desenvolver uma teoria geral de correção quântica de erro, devemos fazer o menor número possível de suposições acerca da natureza do ruído e do procedimento utilizado para a correção de erro. Serão feitas duas suposições gerais: a de que o ruído é descrito por uma operação quântica $\mathcal{E}$ e a de que o procedimento completo para a correção de erro é efetuado por uma operação quântica $\mathcal{R}$ que preserva o traço, a qual é denominada de *correção de erro*. Essa operação de correção unifica, em uma única etapa, os dois passos da detecção-recuperação.

Para que a correção seja considerada bem sucedida, requeremos que, para qualquer estado ρ cujo suporte pertença ao subespaço do código C, seja válida a expressão

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho.$$

As *condições* para a *correção quântica de erro* são um conjunto simples de equações que podem ser verificadas para determinar se um dado código de correção de fato protege o estado contra um tipo particular de ruído $\mathcal{E}$. Todas essas considerações são retratadas no Teorema 1.3.1:

Teorema 1.3.1 *(**Condições para correção quântica de erro**) Seja C um código quântico e P um projetor sobre C. Seja $\mathcal{E}$ uma operação quântica com elementos de operação $\{E_i\}$. Uma condição necessária e suficiente para a existência de uma operação de correção de erro $\mathcal{R}$ corrigindo $\mathcal{E}$ sobre C é que*

$$PE_i^\dagger E_j P = \alpha_{ij} P,$$

para alguma matriz hermitiana α de números complexos. Os elementos de operação $\{E_i\}$ do ruído $\mathcal{E}$ são denominados erros, e, se existir tal operação $\mathcal{R}$, dizemos que $\{E_i\}$ constitui um conjunto de erros corrigíveis.

1.3.1 Discretização dos erros

Nesta subseção, enunciaremos o Teorema 1.3.2, conhecido como teorema da Discretização dos Erros, que é de fundamental importância na teoria da codificação quântica. O teorema afirma que, se um código quântico corrige erros quânticos num determinado conjunto finito de elementos de operação, então o código também corrige qualquer erro que é dado por qualquer combinação linear destes elementos de operação.

Teorema 1.3.2 *Seja C um código quântico e $\mathcal{R}$ a operação de correção de erro, construída na demonstração do Teorema 1.3.1, para a recuperação de um processo de ruído $\mathcal{E}$ com elementos de operação $\{E_i\}$. Seja $\mathcal{F}$ uma operação quântica com elementos de operação $\{F_j\}$, que são combinações lineares dos elementos $\{E_i\}$, isto é, $F_j = \sum_i m_{ji} E_i$, para alguma matriz de números complexos m_{ji}. Então, a operação de correção de erro $\mathcal{R}$ também corrige os efeitos do processo de ruído $\mathcal{F}$ sobre o código C.*

1.3.2 Códigos degenerados

Existe uma classe interessante de códigos quânticos, conhecida como códigos *degenerados*, que apresentam uma propriedade notável que não existe nos códigos clássicos.

Definição 1.3.1 *Um código é denominado degenerado se o efeito de dois tipos diferentes de erros a uma palavra-código dá origem a uma mesma palavra corrompida.*

Esse efeito não ocorre nos códigos clássicos, pois erros em bits diferentes necessariamente levam a diferentes palavras corrompidas.

A vantagem de se ter um código degenerado é que, de algum modo, estes são capazes de "empacotar" mais informação do que os códigos clássicos, pois erros distintos não necessariamente levam o espaço do código para espaços ortogonais, e é possível (embora ainda não demonstrado) que esta capacidade extra possa levar a códigos degenerados capazes de armazenar informação quântica mais eficientemente do que os códigos não-degenerados.

A desvantagem é que algumas das técnicas de demonstração utilizadas classicamente para provar certos limites para correção de erros ficam invalidadas, pois não podem ser aplicadas aos códigos degenerados.

1.3.3 O limitante quântico de Hamming

O *limitante quântico de Hamming* é aplicável somente aos códigos não-degenerados.

Suponha que um código não-degenerado seja usado para codificar k qubits em n qubits, de forma que este possa corrigir erros em qualquer subconjunto com t ou menos qubits. Suponha que ocorram j erros, nos quais $j \leq t$. Então, existem

$$\left(\begin{array}{c} n \\ j \end{array} \right)$$

conjuntos de posições possíveis para o erro ocorrer. Para cada um destes conjuntos, existem três tipos de erros possíveis, as três *matrizes de Pauli* X, Y, Z, que podem ocorrer em cada qubit, resultando num total de 3^j erros possíveis, pois as combinações lineares de X, Y e Z também são erros possíveis. As matrizes X, Y, Z, são dadas, respectivamente, por

$$X = \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right], \quad Y = \left[\begin{array}{cc} 0 & -i \\ i & 0 \end{array} \right], \quad Z = \left[\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right].$$

O número total de erros que podem ocorrer em t ou menos qubits é, portanto:

$$\sum_{j=0}^{t} \left(\begin{array}{c} n \\ j \end{array} \right) 3^j.$$

Para codificar k qubits de forma não-degenerada, cada um destes erros deve corresponder a um subespaço ortogonal com 2^k dimensões. Todos esses subespaços devem estar contidos

em um espaço total com 2^n dimensões dos n qubits, o que implica na inequação

$$\sum_{j=0}^{t} \left(\begin{array}{c} n \\ j \end{array} \right) 3^j 2^k \leq 2^n,$$

denominada limite quântico de Hamming.

Introduziremos, agora, um limitante que é utilizado para todo tipo de código quântico, denominado *limitante quântico de Singleton*:

Teorema 1.3.3 *[1] Suponha que um código quântico C codifique k qubits em n qubits e é capaz de corrigir erros em quaisquer t qubits. Então o código deve satisfazer à relação $n \geq 2d - 2 + k$.*

1.3.4 Códigos Calderbank-Shor-Steane, *CSS*

Os códigos de Calderbank-Shor-Steane, ou mais resumidamente códigos CSS, formam uma importante subclasse de uma classe mais geral de códigos estabilizadores.

Sejam C_1 e C_2 códigos clássicos lineares com parâmetros $[n,\ k_1]$ e $[n,\ k_2]$, respectivamente, tais que $C_2 \subset C_1$ e tanto C_1 quanto ${C_2}^{\perp}$ corrigem t erros. Então, existe um código quântico $CSS(C_1,\ C_2)$, com parâmetros $[n,\ k_1 - k_2]$, capaz de corrigir erros arbitrários em t qubits, denominado código *CSS* de C_1 sobre C_2. Tal código $CSS(C_1,\ C_2)$ é gerado pela seguinte construção.

Seja $x \in C_1$ uma codificação no código C_1. O estado quântico $\mid x + C_2\rangle$ por:

$$\mid x + C_2\rangle \equiv \frac{1}{\sqrt{\mid C_2 \mid}} \sum_{y \in C_2} \mid x + y\rangle,$$

onde "+" indica a adição binária módulo 2.

Seja $x^{'}$ um elemento de C_1 tal que $x - x^{'} \in C_2$. Então, concluímos que

$$\mid x + C_2\rangle = \mid x^{'} + C_2\rangle,$$

e, portanto, o estado $\mid x + C_2\rangle$ depende somente do espaço quociente de C_1/C_2 no qual se encontra x, o que explica o notação de espaços quociente utilizada para $\mid x + C_2\rangle$. Além disso, se x e $x^{'}$ pertencem a diferentes classes laterais de C_2, resulta que, para nenhum $y, y^{'} \in C_2$ ocorre $x + y = x^{'} + y^{'}$, e, conseqüentemente, $\mid x + C_2\rangle$ e $\mid x^{'} + C_2\rangle$ são estados ortogonais. O código quântico $CSS(C_1,\ C_2)$ é definido como sendo o espaço vetorial gerado pelos estados $\mid x + C_2\rangle$, para todo $x \in C_1$. O número de espaços quociente de C_2 em C_1 é igual a $\mid C_1 \mid / \mid C_2 \mid$, e portanto, a dimensão do código $CSS(C_1,\ C_2)$ é igual a $\mid C_1 \mid / \mid C_2 \mid = 2^{k_1 - k_2}$, donde CSS$(C_1,\ C_2)$ é um código quântico com parâmetros $[n,\ k_1 - k_2]$.

Explorando as propriedades básicas de correção de erros de C_1 e ${C_2}^{\perp}$ para detectar e corrigir erros quânticos, observamos que é possível corrigir erros em até t bits e erros de inversão de fase no código $CSS(C_1,\ C_2)$, utilizando as propriedades de correção de C_1 e ${C_2}^{\perp}$, respectivamente. Suponha que erros de inversão de bit sejam descritos por um vetor de n bits e_1 com componentes iguais a 1, onde ocorreram as inversões, e 0, onde elas não ocorreram, e que erros de inversão de fase sejam descritos por um vetor de n bits e_2 com componentes iguais a 1 onde ocorreram as inversões, e 0 onde elas não ocorreram. Se o estado original era $\mid x + C_2\rangle$, o estado corrompido será:

$$\frac{1}{\sqrt{\mid C_2 \mid}} \sum_{y \in C_2} (-1)^{(x+y).e_2} \mid x + y + e_1\rangle.$$

Para detectar onde ocorreu uma inversão de bit, é conveniente introduzir um sistema auxiliar contendo qubits suficientes para armazenar a síndrome para o código C_1 e que sejam todos inicializados no estado $\mid 0\rangle$. Utilizamos a computação reversível [1] para aplicar a matriz de paridade H_1 para o código C_1, levando o estado

$$\mid x + y + e_1\rangle \mid 0\rangle$$

para o estado

$$\mid x + y + e_1\rangle \mid 0\rangle \mid H_1(x + y + e_1)\rangle = \mid x + y + e_1\rangle \mid H_1 e_1\rangle,$$

já que $(x+y) \in C_1$ é aniquilado pela matriz verificadora de paridade. O efeito desta operação é produzir o estado

$$\frac{1}{\sqrt{\mid C_2 \mid}} \sum_{y \in C_2} (-1)^{(x+y).e_2} \mid x + y + e_1\rangle \mid H_1 e_1\rangle.$$

A detecção de erros de inversão de bit é completada medindo-se o sistema auxiliar para obter o resultado $H_1 e_1$. Após este procedimento, o sistema auxiliar é descartado, permanecendo o estado

$$\frac{1}{\sqrt{\mid C_2 \mid}} \sum_{y \in C_2} (-1)^{(x+y).e_2} \mid x + y + e_1\rangle.$$

Conhecendo a síndrome de erro $H_1 e_1$, podemos inferir sobre o erro e_1, pois C_1 corrige até t erros, o que completa a etapa da detecção. A recuperação é obtida simplesmente aplicando portas CNOT aos qubits cujas posições em e_1 acusaram uma inversão de bit. Dessa forma, todos os erros serão corrigidos, permanecendo o estado

$$\frac{1}{\sqrt{\mid C_2 \mid}} \sum_{y \in C_2} (-1)^{(x+y).e_2} \mid x+y \rangle.$$

Considere a porta lógica (ou matriz unitária) Hadamard H dada por

$$H = 1/\sqrt{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Para detectar erros de inversão de fase, aplicamos portas Hadamard a cada qubit, donde o estado passa a ser o estado

$$\frac{1}{\sqrt{\mid C_2 \mid 2^n}} \sum_{z} \sum_{y \in C_2} (-1)^{(x+y).(e_2+z)} \mid z \rangle,$$

onde a soma é realizada para todos os valores possíveis z de n bits. Definindo $z^{'} \equiv z + e_2$, esse estado pode ser reescrito como:

$$\frac{1}{\sqrt{\mid C_2 \mid 2^n}} \sum_{z^{'}} \sum_{y \in C_2} (-1)^{(x+y).(z^{'})} \mid z^{'} + e_2 \rangle.$$

Supondo que $z^{'} \in {C_2}^{\perp}$, decorre que $\sum_{y \in C_2} (-1)^{y.z^{'}} = \mid C_2 \mid$. Se $z^{'} \notin {C_2}^{\perp}$, teremos $\sum_{y \in C_2} (-1)^{y.z^{'}} = 0$, e então, podemos escrever o estado como sendo

$$\frac{1}{\sqrt{2^n / \mid C_2 \mid}} \sum_{z^{'} \in {C_2}^{\perp}} (-1)^{x.z^{'}} \mid z^{'} + e_2 \rangle,$$

que possui a mesma forma de um erro de inversão de bit descrito pelo vetor e_2. Como no caso da detecção de erros de inversão de bit, introduzimos um sistema auxiliar e aplicamos reversivelmente a matriz verificadora de paridade H_2 para o código ${C_2}^{\perp}$, para obter $H_2 e_2$, e implementamos a correção de "inversão de bit" para e_2, o que resulta no estado

$$\frac{1}{\sqrt{2^n / \mid C_2 \mid}} \sum_{z^{'} \in {C_2}^{\perp}} (-1)^{x.z^{'}} \mid z^{'} \rangle.$$

Aplicando portas de Hadamard a cada um dos qubits, como a porta Hadamard é auto-inversa, concluímos que a operação leva de volta ao estado codificado original

$$\mid x + C_2 \rangle \equiv \frac{1}{\sqrt{\mid C_2 \mid}} \sum_{y \in C_2} \mid x+y \rangle.$$

Resumindo o processo: Sejam C_1 e C_2 códigos clássicos lineares com parâmetros $[n, k_1]$ e $[n, k_2]$, respectivamente, tais que $C_2 \subset C_1$ e ambos, C_1 e ${C_2}^{\perp}$ corrigem erros em até t bits. Então, o código quântico $CSS(C_1,\ C_2)$ possui parâmetros $[n,\ k_1 - k_2]$ e é capaz de corrigir erros arbitrários em até t qubits. Além disso, as etapas de detecção e correção dos erros requerem somente a aplicação de portas Hadamard e $CNOT$, onde a porta lógica $CNOT$ é dada pela matriz unitária

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

Em cada caso, é necessário apenas um número linear de portas quânticas no tamanho do código. Além disso, a codificação e a decodificação também podem ser realizadas utilizando-se apenas um número linear de portas quânticas no tamanho do código.

Observação 1.3.1 *É conveniente enfatizar que todas as construções e conceitos relativos aos códigos quânticos* CSS *binários também são válidos quando considerados se o alfabeto é um alfabeto q-ário, onde q é potência de primo, [2,16]. Nestes casos, ao invés de escrevermos qubits, escreveremos qudits, conforme a notação adotada em [2, 16] e também empregada na maioria dos trabalhos disponíveis na literatura.*

Capítulo 2

Construções de Códigos *CSS* Derivados de Códigos Reed-Solomon

Uma classe bem conhecida de códigos quânticos é a classe dos códigos *CSS* (Calderbank-Shor-Steane), [1]. Em relação à construção de tais códigos, grande parte dos trabalhos disponíveis na literatura são baseados na construção do código *CSS* a partir de um único código clássico auto-ortogonal C, $[3, 5–11, 13–15, 17–20, 26–31]$. Recentemente, os autores em [32] unificaram a construção de códigos quânticos MDS, aplicando o método de construção hermitiano derivados de códigos *Reed-Solomon generalizados* clássicos, auto-ortogonais, onde o produto interno considerado é o produto interno hermitiano.

Por outro lado, poucos trabalhos disponíveis na literatura utilizam dois códigos clássicos (não necessariamente auto-ortogonais) para a obtenção de códigos *CSS*. Exemplos de trabalhos neste contexto são $[4, 16, 25]$.

Sabemos que ao se considerar métodos de construção de códigos quânticos *CSS* derivados de dois códigos clássicos distintos, não necessariamente auto-ortogonais, estes geram códigos quânticos com distâncias mínimas maiores e mais próximas entre si. Além disso, os códigos *CSS* resultantes podem agir nos qudits fornecendo proteções desiguais para os mesmos. Essas vantagens possibilitam a construção de códigos quânticos *CSS* com melhores parâmetros quando comparados aos códigos quânticos *CSS* gerados a partir de um único código clássico auto-ortogonal disponíveis na literatura. Baseados nestes fatos, definimos o objetivo principal do capítulo.

A principal contribuição deste capítulo é a proposta de um novo método de construção que produz famílias de bons códigos quânticos *CSS* q-ários, (q é uma potência de primo), utilizando para isso, dois códigos (clássicos) *Reed-Solomon* q^l-ários (l é um inteiro positivo) distintos, não necessariamente auto-ortogonais. Além disso, quando a construção *CSS* é realizada sobre o corpo F_{q^l} em si mesmo, os códigos quânticos resultantes são códigos MDS.

Para garantir que os códigos *CSS* q-ários possuam distância mínima maior ou igual a d, onde $d \geq 2$ é um número inteiro, devemos encontrar o valor mínimo de l tal que a desigualdade $q^l \geq 2(d-1)+1 = 2d-1$ seja satisfeita. Essa desigualdade fornece o corpo de menor cardinalidade no qual os códigos clássicos *RS* q-ários C_1 e $C_2^{\perp}$ deverão ser construídos para que possuam distância mínima maior ou igual a d, e ao mesmo tempo fornece a menor expansão q-ária dos códigos C_1 e C_2 com respeito à uma base β (fixa, porém qualquer) de F_{q^l} sobre F_q.

Depois da construção dos códigos C_1, C_2 e $C_2^{\perp}$ pelo método proposto, construiremos os códigos clássicos q-ários $\beta(C_1)$, $\beta(C_2)$ e $(\beta(C_2))^{\perp}$. Uma vantagem fornecida por esse método é a flexibilidade na escolha de cada código clássico para a geração do código *CSS*, resultando em códigos quânticos com distâncias mínimas tão grandes quanto desejado.

É bem conhecido o fato que, para $q = 2^m$, sempre existem bases auto-duais β, de F_{2^m} sobre F_2. Em outras palavras, a propriedade $\beta = \beta^{\perp}$ é utilizada para garantir que $[\beta(C)]^{\perp} = \beta(C^{\perp})$, implicando na auto-ortogonalidade do código binário $\beta(C)$, isto é, $\beta(C) \subset [\beta(C)]^{\perp}$. Em [3] esse fato foi empregado para a construção de códigos *CSS*, uma vez que a imagem de códigos auto-ortogonais resulta em códigos que também são auto-ortogonais. Para códigos q-ários, $(q = p^m,\ p \neq 2)$, nem sempre é possível garantir a existência de bases auto-duais, impossibilitando tais construções. Como para o método de construção utilizando-se dois códigos clássicos na geração do código *CSS* a condição de auto-ortogonalidade não é necessária, essa estratégia permite maior flexibilidade na escolha dos códigos clássicos apropriados, generalizando o método de construção proposto em [3] para códigos *CSS* q-ários. Uma desvantagem do método de construção *CSS* utilizando-se dois códigos clássicos para a geração do código *CSS* ao invés de se considerar um único código auto-ortogonal é que este apresenta um aumento de complexidade no processo de decodificação.

O capítulo está organizado como segue. Na Seção 2.1, descrevemos os conceitos preliminares necessários ao desenvolvimento do capítulo. Na Seção 2.2, propomos novos métodos de construção de códigos quânticos *CSS*. Mais especificamente, nas Subseções 2.2.1 e 2.2.2, apresentamos os métodos de construção p-ários e q-ários, respectivamente, onde p é um primo e q é potência de primo. Na Seção 2.3, calculamos a taxa dos novos códigos quânticos *Reed-Solomon* gerados pelos métodos de construção sendo propostos, e, na Seção 2.4, exibimos tabelas contendo alguns desses bons códigos quânticos. Finalmente, na Seção 2.5, estabelecemos os comentários finais do capítulo.

2.1 Revisão de códigos cíclicos

Nesta seção apresentamos uma revisão sobre códigos cíclicos, necessária ao desenvolvimento deste capítulo. Para todo o contexto deste trabalho, salvo menção em contrário,

consideramos o corpo de Galois $F_q = GF(q)$ e $q = p^m$, onde p é um número primo. Todos os resultados desta seção (Seção 2.1) são encontrados em [33].

Considere o anel quociente $R_n = F_q[x]/(x^n - 1)$, consistindo de classes de resíduos $F_q[x]$ *mod* $(x^n - 1)$.

Definição 2.1.1 *[33] Um ideal C de R_n é um subespaço linear de R_n tal que, se $c(x) \in C$, então $r(x)c(x) \in C$, onde $r(x) \in R_n$.*

Definição 2.1.2 *[33] Um código cíclico de comprimento n é um ideal de R_n.*

O próximo teorema infere à respeito ao código dual de um código cíclico.

Teorema 2.1.1 *[33] Seja $g(x)$ o polinômio gerador para o código cíclico C. Então, o código dual de C, denotado por $C^\perp$, é cíclico e tem polinômio gerador $g(x)^\perp = x^{\partial h(x)}h(x^{-1})$, onde $h(x) = (x^n - 1)/g(x)$ e ∂ denota o grau do polinômio.*

Observação 2.1.1 *É bem conhecido que o código que possui polinômio gerador $h(x)$ é equivalente ao código dual $C^\perp$. Baseado nesse fato e para simplificação da notação, identificamos o código dual $C^\perp$ com o código gerado pelo polinômio $h(x)$.*

O Teorema 2.1.2 fornece um limitante para a distância mínima de um código cíclico.

Teorema 2.1.2 *[33](Teorema do Limitante do BCH) Seja C um código cíclico com polinômio gerador $g(x)$ tal que, para algum inteiro $b \geq 0$, $\delta \geq 1$, $\alpha \in F_{q^m}$ e $g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0$, ou seja, o código tem uma seqüência de $\delta - 1$ potências consecutivas de α como zeros. Então, a distância mínima de C é, no mínimo, igual a δ.*

Definição 2.1.3 *[33] Seja $\alpha \in F_{q^m}$ e $M^{(a)}(x)$ o polinômio minimal de α^a sobre F_q. Um código cíclico de comprimento n sobre F_q é um código* BCH *com distância de projeto δ se, para algum inteiro $b \geq 0$, $g(x) = mmc\{M^{(b)}(x), M^{(b+1)}(x), \cdots, M^{(b+\delta-2)}(x)\}$, ou seja, $g(x)$ é o polinômio mônico de menor grau sobre F_q tendo $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$ como zeros.*

Assim, a distância mínima de um código *BCH* é maior ou igual à distância de projeto δ. Segue a definição do código clássico *Reed-Solomon* (RS).

Definição 2.1.4 *[33] Um código* Reed-Solomon *sobre o corpo F_q (q é potência de primo) é um código* BCH *de comprimento $n = q - 1$.*

A dimensão do código RS é dada por $k = n - \partial(g(x)) = n - \delta + 1$, e a distância mínima, d_{min}, coincide com a distância de projeto, isto é, $d_{min} = n - k + 1$.

2.2 Novos Métodos de Construção

A principal contribuição desta seção é o Teorema 2.2.2. Este afirma que existe um código quântico q-ário $CSS(\beta(C_1), \beta(C_2))$ com parâmetros

$$[[N = l(q^l - 1), K = lk, D \geq d]]_q,$$

$k = q^l - 2d + 1$ e $d \geq 2$ é um número inteiro.

A seguir, apresentamos o processo de construção *CSS* (veja, por exemplo, [16]).

Lema 2.2.1 *Sejam C_1 e C_2 dois códigos clássicos lineares com parâmetros $[n, k_1, d_1]_q$ e $[n, k_2, d_2]_q$, respectivamente, tal que $C_2 \subset C_1$. Então, existe um código quântico $[[n, K = k_1 - k_2, D]]_q$, onde $D = \min\{wt(c) \mid c \in (C_1 \backslash C_2) \cup ({C_2}^{\perp} \backslash {C_1}^{\perp})\}$. A codificação e a decodificação do código* CSS *é baseada na codificação e na decodificação dos códigos clássicos considerados no processo de construção.*

2.2.1 Método de construção p-ário

Nesta subseção é considerado o caso onde os códigos clássicos *RS* C_1, C_2 e ${C_2}^{\perp}$ serão construídos sobre F_{p^m}, onde p é um primo e $m \geq 1$ é um número inteiro. O caso cujos códigos clássicos *RS* C_1, C_2 e ${C_2}^{\perp}$ serão construídos sobre F_{q^l}, onde q é potência de primo e $l \geq 1$ é um inteiro, é análogo ao primeiro caso e será apresentado na Subseção 2.2.2.

Suponha que $d \geq 2$ seja um inteiro fixo. Iniciamos a construção dos códigos quânticos *CSS* p-ários (p primo) escolhendo o menor inteiro positivo $m \geq 1$ que satisfaz a desigualdade $p^m \geq 2d - 1$. Essa desigualdade fornece o corpo de menor cardinalidade no qual os códigos clássicos *RS* C_1, C_2 e ${C_2}^{\perp}$ serão construídos para que os códigos C_1 e ${C_2}^{\perp}$ possuam distância mínima maior ou igual a d, e ao mesmo tempo, produz a menor expansão q-ária de C_1 e C_2 com respeito a uma base (fixa, porém qualquer) β de F_{p^m} sobre F_p. Note que C_1, C_2 e ${C_2}^{\perp}$ possuem comprimento $n = q - 1$, onde $q = p^m$.

Seja C_1 um código *RS* sobre F_{p^m}, gerado pelo polinômio

$$g_1(x) = (x - 1)(x - \alpha^1)(x - \alpha^2) \cdots (x - \alpha^{d-2}),$$

onde α é um elemento primitivo do corpo F_{p^m} e $d \geq 2$ é um número natural. Sabemos que $\partial g_1(x) = d - 1$, onde ∂ denota o grau do polinômio $g_1(x)$. Pelo Teorema 2.1.2 (limitante do *BCH*) e usando o fato de C_1 ser um código *Reed-Solomon*, a distância mínima de C_1 é igual a d. A dimensão de C_1 é $k_1 = p^m - 1 - (d - 1) = p^m - d$.

Considere, agora, todas as potências de α ordenadas em ordem crescente de seus expoentes:

$$\alpha^0 = 1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{p^m - 2}.$$

Sabemos que o conjunto das "não raízes" de $g_1(x)$ é o conjunto

$$NRg_1 = \{\alpha^{(d-1)}, \alpha^d, \alpha^{(d+1)}, \cdots, \alpha^{(p^m-2)}\}.$$

Além disso, considere o conjunto das últimas $d-1$ "não raízes" de $g_1(x)$ ordenado em ordem crescente de seus expoentes, dado por

$$A = \{\alpha^{(p^m-d)}, \alpha^{[p^m-(d-1)]}, \alpha^{[p^m-(d-2)]}, \alpha^{[p^m-(d-3)]}, \cdots, \alpha^{(p^m-3)}, \alpha^{(p^m-2)}\}.$$

Seja C_2 o código RS gerado pelo polinômio

$$g_2(x) = \prod_{j=0}^{p^m-d-1} (x - \alpha^j).$$

Por construção, $C_2 \subset C_1$ e C_2 possui dimensão $k_2 = d-1$.

Sabemos que o dual do código C_2, denotado por ${C_2}^{\perp}$, é equivalente ao código C_3, gerado pelo polinômio $g_3(x) = (x^{(p^m-1)} - 1)/g_2(x)$, que é o produto de $(x - \alpha^j)$, para cada $\alpha^j \in A$, ou seja,

$$g_3(x) = \prod_{\alpha^j \in A} (x - \alpha^j) = (x - \alpha^{(p^m-d)})(x - \alpha^{[(p^m-(d-1)]}) \cdots (x - \alpha^{(p^m-2)}).$$

Assim, identificamos o código ${C_2}^{\perp}$ com o código C_3. Como $\partial(g_3(x)) = d-1$, o código $C_2^{\perp}$ possui distância mínima igual a d.

Antes de continuarmos, é apropriado revisar os conceitos de *aplicação traço* e *base dual*. Para maiores detalhes, indicamos [34].

Definição 2.2.1 *[34] Seja $q = p^m$ uma potência de primo. A* aplicação traço $Tr : F_q \longrightarrow F_p$ *é definida como sendo $Tr(a) := \sum_{i=0}^{m-1} a^{p^i}$, para todo $a \in F_q$.*

Definição 2.2.2 *[34] Dada uma base $\beta = \{b_1, b_2, \cdots, b_m\}$ de F_{p^m} sobre F_p, uma* base dual *à base β, denotada por $\beta^{\perp}$, é uma base $\beta^{\perp} = \{{b_1}^*, {b_2}^*, \cdots, {b_m}^*\}$ com $Tr(b_i {b_j}^*) = \delta_{ij}$, para todo $i, j \in \{1, \cdots, m\}$.*

Os próximos três resultados podem ser encontrados em [3]:

- (i) Toda base admite base dual;

- (ii) Seja $C = [N, K, D_1]$ um código linear de comprimento N, dimensão K, e distância mínima D_1 sobre F_{p^m}. Seja $\beta = \{b_1, b_2, \cdots, b_m\}$ uma base de F_{p^m} sobre F_p. Então, a expansão p-ária de C com respeito à β, denotada por $\beta(C)$, é o código linear p-ário $C_p = [mN, mK, D_2 \geq D_1]$ dado por $C_p = \beta(C) := \{(c_{ij})_{i,j} \in F_p^{mN} \mid \mathbf{c} = (\sum_j c_{ij} b_j)_i \in C\}$;

- (iii) Seja $C = [N, K, D]$ um código linear sobre F_{p^m}. Seja $C^\perp$ o código dual de C. Então, o código dual da expansão p-ária $\beta(C)$ do código C com respeito à base β é a expansão p-ária $\beta^\perp(C^\perp)$ do código dual $C^\perp$ com respeito à base $\beta^\perp$.

Aplicando esses três resultados aos códigos C_1, C_2 e ${C_2}^\perp$, previamente construídos, produz-se códigos $\beta(C_1)$, $\beta(C_2)$ e $[\beta(C_2)]^\perp$, respectivamente, satisfazendo o seguinte teorema:

Teorema 2.2.1 *Seja $q = p^m$ uma potência de primo. Então, existem códigos quânticos $CSS(\beta(C_1), \beta(C_2))$ p-ários com parâmetros $[[N = m(p^m - 1), K = mk, D \geq d]]_p$, onde $k = p^m - 2d + 1$.*

Demonstração: Considere β como sendo uma base qualquer de F_{p^m} sobre F_p e seja $\beta^\perp$ sua respectiva base dual. Inicialmente, demonstraremos que os códigos $\beta(C_1)$, $\beta(C_2)$ e $[\beta(C_2)]^\perp$ satisfazem às seguintes condições: $\beta(C_2) \subset \beta(C_1)$ e cada um dos códigos $\beta(C_1)$ e $[\beta(C_2)]^\perp$ possuem distância mínima maior ou igual a d.

Considere os códigos C_1, C_2 e ${C_2}^\perp$, previamente construídos. Como $C_2 \subset C_1$, é claro que $\beta(C_2) \subset \beta(C_1)$. Além disso, como C_1 possui distância mínima igual a d, por (ii), obtemos o código $\beta(C_1)$, que também possui distância mínima maior ou igual a d.

Sabemos que ${C_2}^\perp$ possui distância mínima igual a d. Aplicando (iii) ao código ${C_2}^\perp$, segue que $[\beta(C_2)]^\perp = \beta^\perp({C_2}^\perp)$. Como $\beta^\perp$ é uma base de F_{p^m} sobre F_p, aplicando (ii) ao código $\beta^\perp({C_2}^\perp)$ concluímos que tal código também possui distância mínima maior ou igual a d, donde $[\beta(C_2)]^\perp$ possui distância mínima maior ou igual a d.

Por (ii), os códigos $\beta(C_1)$, $\beta(C_2)$ e $[\beta(C_2)]^\perp$ são lineares.

Sabemos que os códigos C_1 e C_2 têm dimensões $k_1 = p^m - d$ e $k_2 = d - 1$, respectivamente. Novamente, por (ii), segue que a dimensão dos códigos $\beta(C_1)$ e $\beta(C_2)$ são $K_1 = mk_1 = m(p^m - d)$ e $K_2 = mk_2 = m(d - 1)$, respectivamente. Conseqüentemente, aplicando a construção *CSS* aos códigos $\beta(C_1)$ e $\beta(C_2)$, geramos um código quântico *CSS* com parâmetros $[[N = m(p^m - 1), K = mk, D \geq d]]_p$, onde $k = p^m - 2d + 1$. □

A construção proposta consiste dos seguintes passos:

- Construa códigos clássicos *RS* q-ários ($q = p^m$) C_1, C_2 e ${C_2}^{\perp}$ sobre F_{p^m}, onde m é o menor inteiro positivo satisfazendo $p^m \geq 2d-1$, com polinômios geradores $g_1(x)$, $g_2(x)$, e $g_3(x)$. Os códigos C_1 e ${C_2}^{\perp}$ possuem distância mínima maior ou igual a d;

- Escolha uma base β de F_{p^m} sobre F_p. Expanda os códigos C_1 e C_2 com respeito à base β. Os códigos resultantes $\beta(C_1)$ e $\beta(C_2)$ são p-ários e lineares. Além disso, é válida a inclusão $\beta(C_2) \subset \beta(C_1)$;

- Considere a base dual à β, denotada por $\beta^{\perp}$, e expanda o código ${C_2}^{\perp}$ com respeito à base $\beta^{\perp}$. Assim, geramos o código $\beta^{\perp}({C_2}^{\perp})$, que é p-ário e linear. Note que o Item (iii) garante que a igualdade $(\beta(C_2))^{\perp} = \beta^{\perp}({C_2}^{\perp})$ é verdadeira, e assim, por (ii), o código $[\beta(C_2)]^{\perp}$ possui distância mínima maior ou igual a d. Além disso, por (ii), o código $\beta(C_1)$ também possui distância mínima maior ou igual a d;

- Aplique o Teorema 2.2.1.

2.2.2 Método de construção q-ário

Nesta subseção, estendemos o método de construção p-ário, demonstrado na Subseção 2.2.1, ao método de construção q-ário, onde q é potência de primo. O Lema 2.2.2, dado na seqüência, é uma generalização de (iii), encontrado em [3].

Lema 2.2.2 *[3] Seja $C = [N, K, D]$ um código linear sobre F_{q^l}. Seja $C^{\perp}$ o código dual de C. Então, o código dual da expansão q-ária $\beta(C)$ do código C com respeito à base β é a expansão q-ária $\beta^{\perp}(C^{\perp})$ do código dual $C^{\perp}$ com respeito à base $\beta^{\perp}$.*

Demonstração: Considere $c \in C$ e $d \in C^{\perp}$ como sendo elementos arbitrários do código e de seu respectivo dual. Então,

$$0 = \sum_{i=1}^{N} c_i d_i = \sum_{i=1}^{N} \left(\sum_{j=1}^{l} c_{ij} b_j \right) \left(\sum_{r=1}^{l} d_{ir} b_r' \right), \tag{2.1}$$

onde $\beta = \{b_1, \cdots, b_l\}$ é uma base de F_{q^l} sobre F_q e $\beta^{\perp} = \{b_1', \cdots, b_l'\}$ é a base dual correspondente. Aplicando o traço na equação (2.1) e reescrevendo os somatórios, resulta em

$$0 = \sum_{i=1}^{N} \sum_{j=1}^{l} \sum_{r=1}^{l} c_{ij} d_{ir} Tr(b_j b_r') = \sum_{i=1}^{N} \sum_{j=1}^{k} c_{ij} d_{ij},$$

e assim, $\beta^{\perp}(C^{\perp}) \subset [\beta(C)]^{\perp}$. Como cada um dos conjuntos possuem $q^{l(N-K)}$ elementos, fica demonstrado que $\beta^{\perp}(C^{\perp}) = [\beta(C)]^{\perp}$, como desejado. □

Observação 2.2.1 *Note que a demonstração do Lema 2.2.2 é somente a demonstração de (ii) (dada em [3]) trocando p por q.*

Tendo como base tais resultados, demonstraremos o principal teorema desta subseção:

Teorema 2.2.2 *Seja q uma potência de primo. Então, existem códigos quânticos q-ários* $CSS(\beta(C_1), \beta(C_2))$ *com parâmetros* $[[N = l(q^l - 1), K = lk, D \geq d]]_q$*, onde* $k = q^l - 2d + 1$ *e* $d \geq 2$*,* $l \geq 1$ *são números inteiros.*

Demonstração: É bem conhecido que (i)([3]) também é válido se considerarmos o corpo F_{q^l} como sendo um espaço vetorial sobre F_q. Além disso, (ii)([3]) pode ser generalizado de forma direta quando consideramos F_{q^l} ao invés de F_{p^m}, onde q é potência de primo e l é um inteiro positivo. Em outras palavras, para generalizar (ii)([3]), é suficiente considerar (ii)([3]) (dado em [3]) trocando p por q. Além disso, o Lema 2.2.2 é uma generalização de (iii)([3]) e já foi demonstrado. Então, [(i), (ii) e (iii)]([3]) também são válidos quando aplicados ao espaço vetorial (de dimensão l) F_{q^l} sobre F_q.

Aplicando o mesmo método de construção realizado na Subseção 3.1, geramos códigos clássicos *RS* C_1, C_2 e ${C_2}^{\perp}$ sobre F_{q^l}. Além disso, como [(i), (ii) e (iii)]([3]) são válidos, procedendo como na demonstração do Teorema 2.2.1, podemos construir códigos clássicos $\beta(C_1)$, $\beta(C_2)$ e $[\beta(C_2)]^{\perp}$, sobre F_q, satisfazendo às seguintes condições: $\beta(C_2) \subset \beta(C_1)$ e cada um dos códigos $\beta(C_1)$ e $[\beta(C_2)]^{\perp}$ possui distância mínima maior ou igual a d. Assim, aplicando a construção *CSS* a cada um dos códigos $\beta(C_1)$, $\beta(C_2)$ e $[\beta(C_2)]^{\perp}$, obtemos códigos quânticos q-ários $CSS(\beta(C_1), \beta(C_2))$ com parâmetros $[[N = l(q^l - 1), K = lk, D \geq d]]_q$, onde $k = q^l - 2d + 1$. □

Observação 2.2.2 *Se no método de construção proposto não considerarmos nenhuma expansão, ou seja, se o método de construção for aplicado ao espaço vetorial* $F(q^l)$ *sobre si mesmo, então o espaço vetorial possuirá dimensão* 1*, e assim, aplicando o Teorema 2.2.2, os códigos* CSS *resultantes são MDS e reproduzem algumas famílias de códigos quânticos MDS construídos em [27].*

Em seguida, mostraremos como o método proposto funciona.

Exemplo 2.2.1 *Considere a construção de um código* CSS 3*-ário que corrige erros arbitrários em* 4 *qudits. Calculando m segue que* $2d - 1 = 2.9 - 1 = 17 \leq 3^3$*. Assim, os códigos* C_1*,* C_2 *e* ${C_2}^{\perp}$ *são construídos sobre* F_{3^3} *e possuem comprimento* 26*.*

Seja α *um elemento primitivo do corpo* F_{27} *e considere os códigos cíclicos dados por*

$$C_1 = \langle g_1(x) \rangle = \langle (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^7) \rangle,$$

$$C_2 = \langle g_2(x) \rangle = \langle (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{17}) \rangle$$

e

$$C_2{}^{\perp} = \langle g^{\perp}{}_2(x) \rangle = \langle (x-\alpha^{18})(x-\alpha^{19})\cdots(x-\alpha^{25}) \rangle.$$

Calculando os parâmetros dos códigos C_1 e C_2 segue que $n = 26$, $k_1 = 26-8 = 18$, $k_2 = 8$ e $k = 18-8 = 10$. Pelo Teorema 2.2.2, o código quântico $CSS(\beta(C_1), \beta(C_2))$ possui parâmetros $[[78, 30, D \geq 9]]$ e corrige erros arbitrários em 4 qudits.

Exemplo 2.2.2 *Considere a construção de um código* CSS *3-ário que corrige erros em 5 qudits. Os códigos C_1, C_2 e $C_2{}^{\perp}$ possuem comprimento 26 pois $2d+1 = 2.11-1 = 21 \leq 3^3$. Seja α um elemento primitivo de F_{3^3} e considere*

$$C_1 = \langle g_1(x) \rangle = \langle (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^9) \rangle,$$

$$C_2 = \langle g_2(x) \rangle = \langle (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{15}) \rangle$$

e

$$C_2{}^{\perp} = \langle g^{\perp}{}_2(x) \rangle = \langle (x-\alpha^{16})\cdots(x-\alpha^{25}) \rangle.$$

Sabemos que C_1 e C_2 possuem parâmetros $n = 26$, $k_1 = 26-10 = 16$, $k_2 = 10$ e $k = 16-10 = 6$. Pelo Teorema 2.2.2, o código $CSS(\beta(C_1), \beta(C_2))$ possui parâmetros $[[78, 18, D \geq 11]]_3$.

Exemplo 2.2.3 *Considere a construção de um código* CSS *sobre o corpo F_{5^m} corrigindo erros arbitrários em 22 qudits.*

Os códigos C_1, C_2 e $C_2{}^{\perp}$ possuem comprimento 5^3, pois $2d-1 = 89 \leq 5^3$. Considere α um elemento primitivo do corpo F_{5^3}. Sejam

$$C_1 = \langle g_1(x) \rangle = \langle (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{43}) \rangle,$$

$$C_2 = \langle g_2(x) \rangle = \langle (x-1)(x-\alpha)\cdots(x-\alpha^{79}) \rangle$$

e

$$C_2{}^{\perp} = \langle g^{\perp}{}_2(x) \rangle = \langle (x-\alpha^{80})(x-\alpha^{81})\cdots(x-\alpha^{123}) \rangle.$$

Os códigos C_1 e C_2 possuem parâmetros, respectivamente, dados por $k_1 = 124-44 = 80$, $k_2 = 44$, $k = 80-44 = 36$, e assim, $K = 108$ e $N = 372$. Pela aplicação do Teorema 2.2.2, o código $CSS(\beta(C_1), \beta(C_2))$ possui parâmetros $[[372, 108, D \geq 45]]_5$.

Exemplo 2.2.4 *Considere a construção de um código* CSS 7*-ário com distância mínima maior ou igual a* 10. C_1, C_2 *e* ${C_2}^{\perp}$ *possuem comprimento* $7^2 - 1 = 48$, *pois* $2d - 1 = 2.10 - 1 = 19 \leq 7^2$. *Seja* α *um elemento primitivo de* F_{7^2}.

Seja

$$C_1 = \langle g_1(x) \rangle = \langle (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^8) \rangle,$$

$$C_2 = \langle g_2(x) \rangle = \langle (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{16}) \rangle$$

e

$${C_2}^{\perp} = \langle {g^{\perp}}_2(x) \rangle = \langle (x-\alpha^{17})\cdots(x-\alpha^{25}) \rangle.$$

Os códigos C_1 *e* C_2 *possuem parâmetros, respectivamente, dados por* $k_1 = 49 - 10 = 39$, $k_2 = 10 - 1 = 9$, $k = 30$, *e assim,* $K = 60$ *e* $N = 96$. *Pelo Teorema 2.2.2, o código* $CSS(\beta(C_1), \beta(C_2))$ *tem parâmetros* $[[96, 60, D \geq 10]]_7$.

2.3 Taxas dos Novos Códigos *CSS*

Nesta seção, calcularemos a taxa das novas famílias de códigos *CSS* gerados pelos métodos propostos deste capítulo.

Sabemos que os códigos quânticos *CSS* propostos possuem parâmetros $[[N = l(q^l - 1), K = lk, D \geq d]]_q$, onde $k = q^l - 2d + 1$. A taxa do código é uma função de l e d, a qual é dada por

$$r(l, d) = \frac{l(q^l - 2d + 1)}{l(q^l - 1)}. \tag{2.2}$$

Fixando d e fazendo l tender ao infinito, temos que

$$\lim_{l \to \infty} r(l, d) = \lim_{l \to \infty} \frac{l(q^l - 2d + 1)}{l(q^l - 1)} = 1. \tag{2.3}$$

Assim, concluímos que, quando o valor de l tende ao infinito, a taxa entre a dimensão e o comprimento da palavra-código dos códigos quânticos propostos tende ao valor 1, o que é um bom resultado. Em outras palavras, fixando o número de erros que se quer corrigir, é possível obter códigos quânticos com taxas tão altas quanto desejado.

2.4 Tabelas de Novos Códigos *CSS*

Nas Tabelas 2.1 e 2.2, N é o comprimento da palavra-código, K é a dimensão, e D é a distância mínima do código.

Tabela 2.1: Parâmetros de alguns Novos Códigos *CSS* para $p = 3, 5, 7, 11, 13$

$[[N = m(p^m - 1), K = m(p^m - 2d + 1), D \geq d]]_p$
$[[16, 8, D \geq 3]]_3$
$[[16, 4, D \geq 4]]_3$
$[[48, 32, D \geq 5]]_5$
$[[48, 28, D \geq 6]]_5$
$[[48, 24, D \geq 7]]_5$
$[[48, 20, D \geq 8]]_5$
$[[48, 16, D \geq 9]]_5$
$[[48, 12, D \geq 10]]_5$
$[[48, 8, D \geq 11]]_5$
$[[48, 4, D \geq 12]]_5$
$[[96, 80, D \geq 5]]_7$
$[[96, 72, D \geq 7]]_7$
$[[96, 60, D \geq 10]]_7$
$[[96, 40, D \geq 15]]_7$
$[[96, 32, D \geq 17]]_7$
$[[96, 24, D \geq 19]]_7$
$[[96, 16, D \geq 21]]_7$
$[[96, 8, D \geq 23]]_7$
$[[240, 200, D \geq 11]]_{11}$
$[[240, 156, D \geq 22]]_{11}$
$[[240, 120, D \geq 31]]_{11}$
$[[240, 80, D \geq 41]]_{11}$
$[[240, 36, D \geq 52]]_{11}$
$[[336, 256, D \geq 21]]_{13}$
$[[336, 216, D \geq 31]]_{13}$
$[[336, 132, D \geq 52]]_{13}$
$[[336, 4, D \geq 84]]_{13}$

Observação 2.4.1 *Ressaltamos um fato interessante: Na Tabela 2.2, exibimos alguns novos códigos quânticos construídos pelo métodos propostos neste capítulo, que estendem uma família de códigos apresentados em [19]. Em outras palavras, os autores de [19] apresentam códigos quânticos com parâmetros* $[[189, 183, 2]]_{64}$ *até* $[[189, 69, 21]]_{64}$*, com distâncias mínimas até* 21*. Utilizando o método de construção proposto neste capítulo, reproduzimos todos esses códigos e, além disso, também estendemos tal família, ou seja, também construímos códigos com parâmetros* $[[189, 66, \geq 22]]_{64}$ *até* $[[189, 6, \geq 32]]_{64}$*, com distâncias mínimas até* 32*. Este fato decorre da restrição que o processo de construção* CSS *derivado de um único código clássico auto-ortogonal apresenta quando comparado ao processo de construção* CSS *derivado de dois códigos clássicos distintos, não necessariamente auto-ortogonais.*

Tabela 2.2: Parâmetros de alguns Novos Códigos *CSS* para $q = 64$

$[[N = l(q^l - 1), K = l(q^l - 2d + 1), D \geq d]]_q$
$[[189, 69, D \geq 21]]_{64}$
$[[189, 63, D \geq 22]]_{64}$
$[[189, 57, D \geq 23]]_{64}$
$[[189, 51, D \geq 24]]_{64}$
$[[189, 45, D \geq 25]]_{64}$
$[[189, 39, D \geq 26]]_{64}$
$[[189, 33, D \geq 27]]_{64}$
$[[189, 27, D \geq 28]]_{64}$
$[[189, 21, D \geq 29]]_{64}$
$[[189, 15, D \geq 30]]_{64}$
$[[189, 9, D \geq 31]]_{64}$
$[[189, 3, D \geq 32]]_{64}$

2.5 Considerações Finais

Foram construídas novas famílias de códigos *CSS* q-ários, onde q é uma potência de primo. Essas famílias generalizam as construções de códigos *CSS* binários apresentadas em [3] e possuem taxa de codificação tendendo ao valor 1. Além disso, na Tabela 2.2, exibimos alguns novos códigos quânticos construídos pelo métodos propostos neste capítulo, que estendem uma família de códigos apresentados em [19].

Capítulo 3

Construções de Códigos *CSS* Derivados de Códigos Cíclicos

Em relação à construção de códigos quânticos, grande parte dos trabalhos disponíveis na literatura são baseados na construção do código *CSS* a partir de um único código clássico auto-ortogonal C, [3, 5–11, 13–15, 17–20, 26–31].

Por outro lado, poucos trabalhos disponíveis na literatura utilizam dois códigos clássicos (não necessariamente auto-ortogonais) para a obtenção de códigos *CSS*. Exemplos de trabalhos neste contexto são [4, 16, 25].

Em [25] foram construídos códigos *CSS* a partir de dois códigos clássicos *LDPC* e em [4,16] foram estabelecidas as condições de existência para códigos quânticos *BCH*.

O objetivo principal do capítulo é propor seis novos métodos de construção de famílias de bons códigos *CSS* q-ários (q é potência de primo), onde cada código *CSS* é derivado de dois códigos clássicos cíclicos distintos, não necessariamente auto-ortogonais. Para explicarmos um pouco mais detalhadamente tais construções faremos um breve resumo.

O primeiro método de construção sendo proposto é baseado na construção de códigos cíclicos (clássicos) binários com comprimento $n = 2^{t+3} - 1$, para garantir que o código quântico *CSS* resultante seja capaz de corrigir erros quânticos arbitrários em t qubits. Mais especificamente, utilizaremos essencialmente o Teorema 3.1.10 encontrado em [33]: para $q = 2$ e $n = 2^m - 1$, as classes laterais $\mathbb{C}_1, \mathbb{C}_3, \mathbb{C}_5, \cdots, \mathbb{C}_i$ são todas distintas e cada uma contém exatamente m elementos, desde que $i < 2^{\lceil m/2 \rceil} + 1$, onde $\lceil x \rceil$ denota o menor inteiro maior ou igual a x, para garantir a existência de um número suficientemente grande de classes laterais distintas, cada uma possuindo cardinalidade igual a $t + 3$, permitindo a geração de códigos cíclicos (clássicos) C_1, C_2 e ${C_2}^{\perp}$ de tal modo que C_1 e ${C_2}^{\perp}$ corrijam t erros e que também seja verdadeira a inclusão $C_2 \subsetneqq C_1$. Depois destes procedimentos, aplicaremos a construção *CSS*. Além disso, demonstramos que as taxas de codificação destas novas famílias de códigos

CSS tendem para o valor 1.

O segundo método de construção é baseado na construção de códigos cíclicos (clássicos) q-ários com comprimentos $n = q^{t+1} - 1$, para garantir que o código quântico *CSS* seja capaz de corrigir erros quânticos arbitrários em t qudits. Utilizaremos dois lemas contidos em [16] para garantir a existência de um número suficientemente grande de classes laterais ciclotômicas distintas, todas estas com cardinalidade $t + 1$, para que seja possível a construção de códigos cíclicos (clássicos) C_1, C_2 e ${C_2}^{\perp}$ de tal forma que C_1 e ${C_2}^{\perp}$ corrijam t erros e que também seja verdadeira a inclusão $C_2 \subsetneqq C_1$. Depois disso, aplicaremos a construção *CSS*. Analogamente ao primeiro método de construção sendo proposto, as taxas das novas famílias de códigos *CSS* derivadas do segundo método de construção proposto também tendem ao valor 1.

O terceiro método de construção é baseado na construção de códigos cíclicos q-ários com comprimentos q^2-1, onde q é uma potência de primo maior ou igual a 5. A principal diferença entre esse método e os anteriores é que são demonstradas condições especiais, para este caso, que produzem um aumento do número de classes laterais distintas, aprimorando-se, então, os parâmetros das famílias de códigos quânticos *CSS* geradas por tal método. Em outras palavras, os resultados demonstrados em [16] restringem a quantidade de classes laterais ciclotômicas distintas. Tendo com base tais considerações, é claro que tais códigos também possuem taxa de codificação tendendo ao valor 1.

No quarto método de construção, são geradas novas famílias de códigos quânticos com parâmetros $[[3^m - 1, k \geq 3^m - 8m - 3, \geq 8]]_3$, $[[n, k \geq n - 2m - 2, d \geq 3]]_3$, $[[n, k \geq n - 4m, \geq 4]]_3$, $[[n, k \geq n - 4m - 2, \geq 5]]_3$ e $[[n, k \geq n - 6m - 2, d \geq 6]]_3$, respectivamente. Este método de construção é um tipo especial de construção que também gera bons códigos quânticos, devido à propriedades convenientes que algumas classes laterais possuem. Tais famílias de códigos 3-ários também possuem taxa de codificação tendendo ao valor 1.

O quinto método de construção gera novas famílias de bons códigos quânticos p-ários (p primo) com parâmetros $[[p^3 - 1, p^3 - 21, \geq 5]]_p$.

Finalmente, o sexto método de construção consiste na construção de códigos *CSS* a partir de códigos cíclicos (clássicos) não primitivos. Tal método de construção também gera códigos quânticos q-ários cujos comprimentos das palavras-código também são próximos ao limitante de Singleton.

O capítulo está organizado como segue. Na Seção 3.1, apresentamos os conceitos preliminares sobre corpos, classes ciclotômicas e códigos cíclicos. Na Seção 3.2, apresentamos nossas contribuições: estabelecemos novos métodos de construção de códigos *CSS* derivados de códigos cíclicos clássicos, ou seja, os seis métodos de construção aqui citados. Na Seção 3.3, exibimos tabelas contendo parâmetros de alguns bons códigos *CSS* gerados pelos métodos propostos. Na Seção 3.4 comparamos esses parâmetros com parâmetros dos códigos disponíveis na literatura e, na Seção 3.5, relatamos as considerações finais do capítulo.

3.1 Conceitos Preliminares

Esta seção tem por objetivo apresentar uma revisão dos conceitos sobre códigos cíclicos, necessários para o desenvolvimento deste trabalho. Para maiores detalhes sobre esses conceitos, sugerimos as referências [33, 35, 36]. Todos os resultados apresentados nesta seção são encontrados em [33].

Seja $F_q[x]$ o anel de polinômios com coeficientes num corpo F_q. Considere o anel quociente $R_n = F_q[x]/(x^n - 1)$, consistindo das classes de resíduos do anel $F_q[x]$ *módulo* $(x^n - 1)$. Cada polinômio de grau menor ou igual a $(n-1)$ pertence a classes residuais diferentes, donde são considerados representantes das mesmas.

Considere $\beta \in F_q$. Pelo Teorema de Fermat, podemos afirmar que cada $\beta \in F_q$ satisfaz a equação

$$x^q - x = 0.$$

Esse polinômio é mônico, ou seja, possui coeficiente líder igual a 1, e possui coeficientes no corpo F_p. Mas β pode ser raiz de uma equação polinomial de menor grau. Isso origina a seguinte definição:

Definição 3.1.1 *[33] Seja $q = p^m$, onde p é um número primo. O polinômio minimal sobre F_p de β é o polinômio mônico de menor grau, $M(x)$, com coeficientes em F_p tal que $M(\beta) = 0$.*

Evidentemente, o polinômio minimal é sempre irredutível. Podemos calcular polinômios irredutíveis utilizando o Teorema 3.1.1, dado a seguir:

Teorema 3.1.1 *[33] $x^{p^m} - x$ = produto de todos polinômios mônicos e irredutíveis sobre F_p, cujo grau divide m.*

Segue a definição de *classes laterais ciclotômicas*:

Definição 3.1.2 *[33] A operação de multiplicação por p divide os inteiros módulo $(p^m - 1)$ em conjuntos denominados classes laterais ciclotômicas mod $(p^m - 1)$. As classes laterais ciclotômicas contendo um elemento s são definidas por*

$$\{s, ps, p^2 s, p^3 s, \cdots, p^{m_s - 1} s\},$$

onde m_s é o menor inteiro positivo tal que

$$p^{m_s} s \equiv s \ mod \ (p^m - 1).$$

Se s é o menor número na classe lateral, a classe lateral é denotada por $\mathbb{C}_s$.

Podemos pensar também que um código C é cíclico se é um código linear e se qualquer deslocamento cíclico de uma palavra-código é também uma palavra código, isto é, se $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ então $(c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$. Geralmente identifica-se cada palavra-código $(c_0, c_1, \cdots, c_{n-1}) \in F_q^n$, com o polinômio de coeficientes $c_i \in F_q$, a saber, $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$.

O Teorema 3.1.2 enumera algumas propriedades dos códigos cíclicos:

Teorema 3.1.2 *[33] Seja C um ideal não nulo em R_n, ou seja, um código cíclico de comprimento n. Então*
(a) Existe um único polinômio mônico $g(x)$ com grau minimal em C.
(b) $C = \langle g(x) \rangle$, isto é, $g(x)$ é um polinômio gerador de C.
(c) $g(x)$ é um fator de $x^n - 1$.
(d) Qualquer $c(x) \in C$ pode ser escrito unicamente como $c(x) = f(x)g(x)$ em $F[x]$, onde $f(x) \in F[x]$ tem grau menor que $n - r$, $r = \partial g(x)$. A dimensão do código C é igual a $n - r$. Assim, a mensagem $f(x)$ se torna a palavra-código $f(x)g(x)$.
(e) Se $g(x) = g_0 + g_1 x + \cdots + g_r x^r$, então C é gerado como subespaço de F^n, pelas linhas da matriz geradora

$$T = \begin{bmatrix} g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_r & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_r & 0 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_r & 0 & \cdot & \cdot & 0 \\ \cdot & & & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & & & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_r \end{bmatrix}.$$

Pelo Teorema 2.1.3, sabemos que o código que possui polinômio gerador $h(x)$ é equivalente ao código dual $C^{\perp}$. Esse fato será utilizado exaustivamente neste capítulo, onde consideraremos o código cíclico ${C_2}^{\perp}$ como sendo o código gerado pelo polinômio $h(x) = (x^n - 1)/g(x)$.

Suponha agora que C seja um código *BCH*, sobre o corpo F_q, de comprimento $n = q^m - 1$ e *distância de projeto* δ. Com essa notação, temos:

Teorema 3.1.3 *[33] Para $q = 2$ e $n = 2^m - 1$, as classes laterais $\mathbb{C}_1, \mathbb{C}_3, \mathbb{C}_5, \cdots, \mathbb{C}_i$ são todas distintas e cada uma contém exatamente m elementos, desde que*

$$i < 2^{\lceil m/2 \rceil} + 1,$$

onde $\lceil x \rceil$ denota o menor inteiro maior ou igual a x.

O Teorema 3.1.3 será uma ferramenta fundamental para a realização do primeiro método de construção proposto neste capítulo.

3.2 Construções de Códigos *CSS* Binários e q-ários

Esta seção tem como objetivos principais, a elaboração dos seis métodos de construção de códigos quânticos *CSS*, anteriormente mencionados.

O primeiro método de construção, descrito na Subseção 3.2.1, é baseado em códigos (clássicos) cíclicos binários, e os demais métodos são derivados de códigos cíclicos p-ários (p primo) ou q-ários, onde q é potência de primo. Enfatizamos, novamente, que todos esses seis novos métodos de construção propostos neste capítulo, que geram novas famílias de códigos *CSS*, utilizam dois códigos cíclicos (clássicos) distintos.

Os cinco primeiros métodos de construção são derivados de códigos cíclicos (clássicos) primitivos e o sexto método é derivado de códigos cíclicos (clássicos) não primitivos.

3.2.1 Método de construção I - *CSS* binários

Nesta subseção, apresentaremos um novo método de construção de códigos quânticos *CSS* binários. Tal método é fundamentalmente descrito no Teorema 3.2.1. Este teorema garante a construção de três códigos cíclicos binários C_1, C_2 e ${C_2}^{\perp}$, com parâmetros $[n, k_1]$, $[n, k_2]$, e $[n, n-k_2]$, respectivamente, tal que $C_2 \subset C_1$ e tanto C_1 quanto ${C_2}^{\perp}$ corrigem t erros, para todo $t \geq 2$.

Com este propósito, construiremos tais códigos sobre o corpo $F_{2^{t+3}}$, para assegurar que o código quântico *CSS* corrija erros quânticos arbitrários em t qubits. Este é o argumento principal de tal construção.

O primeiro método de construção que apresentaremos pode ser resumido como segue.

Para que o código quântico $CSS(C_1, C_2)$ corrija erros quânticos arbitrários em t qubits, construiremos códigos cíclicos C_1 e C_2 (e assim, ${C_2}^{\perp}$) sobre o corpo $F_{2^{t+3}}$.

Entretanto, para fornecer um aumento da taxa, construiremos também códigos cíclicos sobre o corpo F_{2^l}, onde $l < t+3$. Este procedimento é possível quando utilizadas as idéias contidas no Teorema 3.1.3. Devido à sua importância, enfatizaremos esta afirmação na Observação 3.2.2, dada em seguida. De fato, este processo de construção será exaustivamente utilizado na construção dos códigos quânticos *CSS* desta tese.

Iniciaremos o método de construção demonstrando o Lema 3.2.1.

Lema 3.2.1 *Para $t \geq 4$, vale a desigualdade $2^{t+3} \geq (4t+1)(t+3) = 4t^2 + 13t + 3$.*

Demonstração: Considere a função $h(t) = 2^{t+3} - 4t^2 - 13t - 3$. Então $h'(t) = (\ln 2)2^{t+3} - 8t - 13$ e $h''(t) = (\ln 2)^2 2^{t+3} - 8$. Como $h''(t) > 0$, para todo $t \geq 4$, $h'(t)$ é uma função estritamente crescente. Além disso, como $h'(4) > 0$ temos que $h'(t) > 0$, para todo $t \geq 4$.

Assim, $h(t)$ é estritamente crescente. Como $h(4) > 0$, $h(t) > 0$, para todo $t \geq 4$ donde $2^{t+3} \geq 4t^2 + 13t + 3$, para todo $t \geq 4$, concluindo a demonstração. □

Enfatizamos a expressão do Lema 3.2.1 para esclarecer as idéias utilizadas aqui. De fato, suponha que $\mathbb{C}_s$ seja uma classe lateral ciclotômica contendo o elemento s. Suponha também que $M^{(i)}(x)$ seja o polinômio minimal do elemento $\alpha^i \in F_{p^m}$, onde α é um elemento primitivo do corpo F_{p^m}. Então, se $i \in \mathbb{C}_s$, temos que

$$M^{(i)}(x) = \prod_{j \in C_s} (x - \alpha^j). \tag{3.1}$$

O número de elementos de C_s (nesse caso, $n = 2^{t+3} - 1$) é igual a $m = t + 3$ ou um divisor de $t + 3$; como o grau de $M^{(i)}(x)$ é a cardinalidade de C_s, o Lema 3.2.1 garanete a existência de, "pelo menos", $4t + 1$ polinômios mônicos, irredutíveis sobre o corpo F_2, cujo grau divide $m = t + 3$. Conseqüentemente, pelo Lema 3.2.1 e pela equação (3.1), existem, sobre o corpo $F_{2^{t+3}}$, no mínimo $4t+1$ classes ciclotômicas distintas, permitindo a escolha dos códigos C_1, C_2 e ${C_2}^{\perp}$ satisfazendo as hipóteses da construção do código quântico *CSS*. Mais especificamente, o Lemma 3.2.1 mostra que o corpo $F_{2^{t+3}}$ é um candidato eficaz para tal construção, pois nesse corpo existem muitas classes laterais ciclotômicas distintas. Explicaremos estes fatos detalhadamente na seqüência.

Como a idéia é a construção de códigos *BCH* C_1 contendo t classes laterais ciclotômicas distintas (donde o código C_1 conterá uma seqüência de, no mínimo, $2t$ números consecutivos, e assim, C_1 corrigirá t ou mais erros), e códigos cíclicos ${C_2}^{\perp}$ contendo $2t$ classes laterais ciclotômicas distintas de tal modo que essas classes laterais contenham uma seqüência de, no mínimo, $2t$ números consecutivos, e assim, o código ${C_2}^{\perp}$ corrigirá t ou mais erros, temos que garantir que o corpo utilizado em tal construção contenha mais que $3t$ classes laterais ciclotômicas distintas.

Provaremos agora o Lema 3.2.2, que relata uma propriedade importante da distância de projeto do código C_1.

Lema 3.2.2 *Seja $p = 2$ e $n = 2^{t+3} - 1$. Suponha que $\mathbb{C}_1, \mathbb{C}_3, \mathbb{C}_5, \cdots, \mathbb{C}_{2t-1}$ sejam classes laterais distintas. Então, o conjunto $A = \mathbb{C}_1 \cup \cdots \cup \mathbb{C}_{2t-1}$ contém todos os números $1 \leq j \leq 2t$.*

Demonstração: Por hipótese, as classes laterais ciclotômicas $\mathbb{C}_1, \mathbb{C}_3, \cdots, \mathbb{C}_{2t-1}$ são distintas. Seja $\mathbb{C}_s = \{s, 2s, 2^2s, 2^3s, \cdots, 2^{m_s-1}s\}$, onde m_s é o menor inteiro positivo tal que $2^{m_s}s \equiv s \bmod (2^m - 1)$, onde $m = t + 3$. Pela definição de classes laterais ciclotômicas, o conjunto A contém todos os números ímpares menores do que $2t - 1$. Falta demonstrar que A contém todos os números pares.

Para tal, suponha que $r = 2k_1, r < 2t-1$. Se k_1 é ímpar, então $k_1 \in \mathbb{C}_{k_1} \subset A$, e assim $r \in A$. Se k_1 é par, então ou $r = 2^l, 1 \leq l \leq m-1$ ou $r = 2^s k_2$, onde k_2 é impar.

Caso 1: Se $r = 2^l$, onde $1 \leq l \leq m-1$, então $r \in \mathbb{C}_1 \subset A$.

Caso 2: Se $r = 2^s k_2$, onde k_2 é ímpar, $r \in \mathbb{C}_{k_2} \subset A$, e assim, $r \in A$.

Seja $r = 2t$. Se t é par e $r = 2^l,\ 1 \leq l \leq m-1$, então $r \in \mathbb{C}_1 \subset A$. De outro modo, se $r = 2^s k_3$, onde k_3 é ímpar, $r \in \mathbb{C}_{k_3} \subset A$, donde $r \in A$. Note que, como $k_3 < 2t-1$, temos que $\mathbb{C}_{k_3} \subset A$.

Uma demonstração alternativa para este lema é apresentada a seguir.

Por hipótese, as classes laterais ciclotômicas $\mathbb{C}_1, \cdots, \mathbb{C}_{2t-1}$ são distintas. Se s é o menor elemento da classe lateral, então sua respectiva classe lateral é denotada por $\mathbb{C}_s$. Assim, todos os números j, onde $1 \leq j \leq 2t$, pertencem ao conjunto $A = \mathbb{C}_1 \cup \cdots \cup \mathbb{C}_{2t-1}$. Provaremos esta afirmação por absurdo.

Suponha que exista um número $j_1, 1 \leq j_1 \leq 2t$, tal que $j_1 \notin A$. Então, existe uma classe lateral $\mathbb{C}_k$ tal que $j_1 \in \mathbb{C}_k$, onde $\mathbb{C}_k \nsubseteq A$, caso contrário, $j_1 \in A$. Como as classes laterais ciclotômicas são todas disjuntas, segue que $k \geq 2t+1$, pois k é o menor elemento contido na classe lateral $\mathbb{C}_k$. Conseqüentemente, como $j_1 \in \mathbb{C}_k$, temos que $j_1 \geq k \geq 2t+1$, o que é um absurdo. □

Lema 3.2.3 *Seja $p = 2$ e $n = 2^{t+3} - 1$. Então, as classes laterais ciclotômicas $\mathbb{C}_1, \mathbb{C}_3, \mathbb{C}_5, \cdots, \mathbb{C}_{2t+1}$ são distintas, para todo $t \geq 4$. Além disso, cada classe lateral contém $t+3$ elementos.*

Demonstração: Para demonstrar este lema, utilizaremos o Teorema 3.1.3, com $i = 2t+1$. É suficiente provar que $2^{\lceil (t+3)/2 \rceil} + 1 > 2t+1$.

Considere a função $g(t) = 2^{(t+3)/2} - 2t$, $t \geq 4$. Calculando sua derivada temos que: $g'(t) = 1/2(\ln 2)2^{(t+3)/2} - 2$. Como $g'(t) > 0$, para todo $t \geq 4$, segue que $g(t)$ é uma função estritamente crescente, para todo $t \geq 4$. Além disso, $g(4) = 8\sqrt{2} - 8 > 0$. Assim, concluímos que $g(t) > 0$, para todo $t \geq 4$. Portanto, $2^{(t+3)/2} + 1 > 2t+1$ e assim, $2^{\lceil (t+3)/2 \rceil} + 1 > 2t+1$. □

O Lema 3.2.3 assegura que os códigos C_2 e C_1 são diferentes, ou seja, $C_2 \subsetneq C_1$. Esboçaremos a seguir, a construção dos códigos quânticos *CSS*.

Considere o corpo $F_{2^{t+3}}$ e seja C_1 o código *BCH* binário de comprimento $n = 2^{t+3} - 1$, gerado pelo produto dos polinômios minimais

$$g_1(x) = \langle M^{(1)} M^{(3)} M^{(5)} \cdots M^{(2t-1)} \rangle.$$

Seja ${C_2}^{\perp}$ o código cíclico gerado pelo polinômio ${g_2}^{\perp}(x)$, que é o produto dos $2t$ polinômios minimais

$$\langle M^{(2t+3)}M^{(2t+5)}M^{(2t+7)}\cdots M^{(2t+4t+1)}\rangle = \langle M^{(2t+3)}M^{(2t+5)}M^{(2t+7)}\cdots M^{(6t+1)}\rangle,$$

e seja C_2 o código cíclico de comprimento $n = 2^{t+3}-1$, gerado pelo polinômio $g_2(x)$, que é o produto dos polinômios minimais dados por

$$g_2(x) = \langle M^{(0)}M^{(1)}M^{(3)}M^{(5)}\cdots M^{(2t-1)}M^{(2t+1)}\cdot\prod_i M^{(i)}\rangle,$$

onde $M^{(i)}$ são os polinômios minimais tais que

$$i \notin \{2t+3, 2t+5, 2t+7, \cdots, 6t+1\},$$

e i percorre os representantes das classes laterais ciclotômicas mod $2^{t+3}-1$.

Então, $C_2 \subset C_1$ e ambos os códigos C_1 e ${C_2}^{\perp}$ corrigem erros em t bits.

Pelo Lema 3.2.2, o código C_1 possui uma seqüência de pelo menos $2t$ potências consecutivas de α como raízes, a saber, α^1, α^2, α^3, α^4, $\cdots$, α^{2t}, onde α é um elemento primitivo do corpo $F_{2^{t+3}}$. Isso ocorre porque todos elementos contidos nas classes laterais $\mathbb{C}_i$ são tais que, se $j \in \mathbb{C}_i$, então α^j é uma raiz do polinômio minimal $M^{(i)}$. Devido a este fato e pela aplicação do Lema 3.2.2, o polinômio gerador do código C_1, $g_1(x)$, possui, no mínimo, α^1, α^2, α^3, α^4, $\cdots$, α^{2t} como respectivas raízes, porque são zeros dos polinômios minimais $M^{(1)}, M^{(3)}, M^{(5)}, \cdots, M^{(2t-1)}$. Assim, pelo Teorema 2.1.5, a distância mínima do código C_1 é, no mínimo, igual a $2t+1$. Portanto, o código C_1 corrige, no mínimo, t erros.

Provaremos, agora, que a distância de projeto do código ${C_2}^{\perp}$ é, de fato, maior que $2t+1$, e assim, o código ${C_2}^{\perp}$ corrige t ou mais erros.

O Lema 3.2.4 mostra dois resultados diferentes. O primeiro resultado afirma que no conjunto

$$B = \{\mathbb{C}_{2t+3}, \mathbb{C}_{2t+5}, \mathbb{C}_{2t+7}, \cdots, \mathbb{C}_{2^{\lceil (t+3)/2\rceil}+1}\},$$

existem $2t$ ou mais classes laterais ciclotômicas distintas, todas elas contendo $t+3$ elementos. O segundo resultado assegura que essas classes laterais distintas são distintas das classes laterais $\{\mathbb{C}_1, \mathbb{C}_3, \cdots, \mathbb{C}_{2t+1}\}$.

Para situar o leitor, o Lema 3.2.4 é essencial para a construção porque garante que as classes laterais ciclotômicas dos códigos C_1 e ${C_2}^{\perp}$ são todas distintas. Pelo Teorema 2.1.5, concluímos que o código C_3 tendo polinômio gerador $h(x)$, onde $h(x) = (x^{2^{t+3}}-1)/g_2(x)$, é equivalente ao código dual ${C_2}^{\perp}$. Assim, sem perda de generalidade, identificamos os códigos ${C_2}^{\perp}$ e C_3, ou seja,

$${C_2}^{\perp} := C_3.$$

Este fato será utilizado exaustivamente neste trabalho. Então, podemos considerar que o conjunto de definição do código ${C_2}^{\perp}$, contenha $2t$ classes laterais ciclotômicas do conjunto $B = \{\mathbb{C}_{2t+3}, \mathbb{C}_{2t+5}, \mathbb{C}_{2t+7}, \cdots, \mathbb{C}_{2^{\lceil (t+3)/2 \rceil}+1}\}$. Como, pelo Lema 3.2.5, os últimos elementos de tais classes laterais formam uma seqüência de, no mínimo, $2t$ números naturais consecutivos, então o polinômio gerador do código ${C_2}^{\perp}$ possui, no mínimo, uma seqüência de $2t$ ou mais potências consecutivas de α como raízes. Pelo Teorema 2.1.5, a distância mínima do código ${C_2}^{\perp}$ é, pelo menos, igual a $2t+1$. Assim, o código ${C_2}^{\perp}$ corrige t ou mais erros.

Ilustraremos a idéia acima mencionada, ou seja, o novo método de construção, através de um esquema gráfico:

$$\underbrace{\mathbb{C}_0 \overbrace{\mathbb{C}_1\ \mathbb{C}_3\ \mathbb{C}_5\ \cdots\ \mathbb{C}_{2t-1}}^{C_1}\ \mathbb{C}_{2t+1}}_{C_2}\ \overbrace{\mathbb{C}_{2t+3}\ \cdots\ \mathbb{C}_{6t+1}}^{{C_2}^{\perp}}\ \underbrace{\mathbb{C}_{s_1}\ \cdots\ \mathbb{C}_{s_n}}_{C_2}.$$

Os conjuntos $\mathbb{C}_0,\ \mathbb{C}_1,\ \cdots, \mathbb{C}_{s_n}$ são todas as classes laterais ciclotômicas para $p = 2$ e $n = 2^{t+3} - 1$.

Lema 3.2.4 *Seja $p = 2$ e $n = 2^{t+3} - 1$. O número de classes laterais ciclotômicas distintas, consecutivas, todas com cardinalidade $t+3$, contidas no conjunto*

$$B = \{\mathbb{C}_{2t+3}, \mathbb{C}_{2t+5}, \mathbb{C}_{2t+7}, \cdots, \mathbb{C}_{2^{\lceil (t+3)/2 \rceil}+1}\},$$

(que contém o conjunto de definição de ${C_2}^{\perp}$, como será explicitado no Teorema 3.2.1) é maior ou igual a $2t$. Além disso, essas classes laterais são distintas das classes laterais $\mathbb{C}_1, \mathbb{C}_3, \mathbb{C}_5, \cdots, \mathbb{C}_{2t+1}$. Em outras palavras, é válida a seguinte desigualdade: $2^{\lceil (t+3)/2 \rceil} + 1 > 2(2t+1) + 2t + 3$, para todo $t \geq 9$.

Demonstração: Primeiramente, observe no Lema 3.2.4, que a expressão "classes laterais ciclotômicas consecutivas" significa classes laterais da forma $\mathbb{C}_i$ e $\mathbb{C}_{i+2}$, onde i é um número natural satisfazendo $1 \leq i \leq 2^{t+3} - 1$.

Agora, devemos mostrar que $2^{\lceil (t+3)/2 \rceil} - 6t - 4 > 0$. Se isso ocorre, pelo Teorema 3.1.3 (no Teorema 3.1.3, substituímos o valor de i por $i = 2(2t+1) + (2t+3)$), segue que, no conjunto B, existem pelo menos $2t+1$ classes laterais ciclotômicas distintas, consecutivas, sendo que todas estas possuem cardinalidade $t+3$.

É claro que, se provarmos a desigualdade $2^{(t+3)/2} - 6t - 4 > 0$, o lema estará provado. Para provar esta desigualdade, considere a função $f(t) = 2^{(t+3)/2} - 6t - 4$. Calculando sua derivada, temos que $f'(t) = \frac{(\ln 2)}{2} 2^{(t+3)/2} - 6$. Calculando a segunda derivada de $f(t)$, resulta que $f''(t) = \frac{(\ln 2)^2}{4} 2^{(t+3)/2}$. Evidentemente, $f''(t) > 0$, e assim, a função $f'(t)$ é uma função estritamente crescente, para todo $t \geq 9$. Como $f'(9) > 0$, implica que $f'(t) > 0$, para todo

$t \geq 9$. Assim, $f(t)$ é uma função estritamente crescente, para todo $t \geq 9$. Mas $f(9) = 6 > 0$, e então $f(t) > 0$, para todo $t \geq 9$. Portanto, existem pelo menos $2t + 1$ classes laterais ciclotômicas distintas consecutivas (cada uma delas contendo $t + 3$ elementos), do código ${C_2}^{\perp}$, e essas classes laterais são distintas das classes laterais $\mathbb{C}_1, \mathbb{C}_3, \cdots, \mathbb{C}_{2t+1}$. Assim, segue a demonstração deste resultado. □

Lema 3.2.5 *Seja $p = 2$ e $n = 2^{t+3} - 1$. Então, os últimos elementos nas $2t$ ou mais classes laterais ciclotômicas, distintas e consecutivas, cada uma destas com $t + 3$ elementos, dadas por*

$$\{\mathbb{C}_{2t+3}, \mathbb{C}_{2t+5}, \mathbb{C}_{2t+7}, \cdots, \mathbb{C}_{2(2t-1)+(2t+3)}, \cdots\},$$

(que contém o conjunto de definição do código ${C_2}^{\perp}$, dadas no Lema 3.2.4), formam uma seqüência de, no mínimo, $2t$ números naturais consecutivos.

Demonstração: Pelo Lema 3.2.4, existem $2t$ ou mais classes laterais ciclotômicas distintas consecutivas, todas contendo $t + 3$ elementos. Sejam

$$\{\mathbb{C}_{2t+3}, \mathbb{C}_{2t+5}, \mathbb{C}_{2t+7}, \cdots, \mathbb{C}_{2(2t-1)+(2t+3)}, \cdots\}$$

tais classes laterais.

Considere $\mathbb{C}_s$ e $\mathbb{C}_{s+2}$ sendo duas dessas classes. Sejam u e v os últimos elementos de $\mathbb{C}_s$ e $\mathbb{C}_{s+2}$, respectivamente, sem levar em conta a operação mod. Portanto, segue que

$$u = s.2^{m-1} = s.2^{t+2} \qquad e \qquad v = (s+2).2^{m-1} = (s+2).2^{t+2}.$$

Assim, temos que $v = s.2^{t+2} + 2^{t+3}$, ou seja,

$$v \equiv s.2^{t+2} + 1 \ \ mod\ (2^{t+3} - 1).$$

Então,

$$v \equiv u + 1 \ \ mod\ (2^{t+3} - 1).$$

Seja $q = 2^{t+3} - 1$ e expanda v e $u+1$ em termos do algoritmo de Euclides sobre q. Então, existem números inteiros a, b, r_1 e r_2, onde $0 \leq r_1 < q$ e $0 \leq r_2 < q$, tais que

$$v = aq + r_1 \qquad e \qquad u + 1 = bq + r_2.$$

Como $v \equiv u + 1 \ \ mod\ (2^{t+3} - 1)$, segue que $r_1 = r_2$. Denotaremos este número comum por v^*. Assim, temos que

$$v = aq + v^* \qquad e \qquad u + 1 = bq + v^*,$$

onde $0 \leq v^* < q$. Portanto,

$$u = bq + v^* - 1.$$

Considere $u^* = v^* - 1$; é claro que $1 \leq u^* < q$. Além disso, pela unicidade do resto no algoritmo da divisão de Euclides, concluímos que u^* é o resto da divisão do número u pelo número $q = 2^{t+3} - 1$.

Então, os representantes v^* e u^* dos números v e u respectivamente, são números consecutivos, ou seja, $v^* = u^* + 1$, concluindo a demonstração. □

Observe que o Lema 3.2.5 continua válido mesmo sem considerar a hipótese que cada uma destas classes laterais contenha $t + 3$ elementos: Suponha que $q = 2$ e $n = 2^m - 1$. Se $\mathbb{C}_s \neq \mathbb{C}_{s+2}$ e $s + 2 \neq 0$ então os termos $u = s2^{m-1} \in \mathbb{C}_s$ e $v = (s + 2)2^{m-1} \in \mathbb{C}_{s+2}$ são consecutivos mod n. Entretanto, preferimos manter tal hipótese para que o leitor saiba que cada classe lateral contida no conjunto de definição do código ${C_2}^{\perp}$, que será construído no Teorema 3.2.1, possui $t + 3$ elementos, e isso possibilita explicitar a dimensão do código *CSS* resultante do método de construção proposto.

Enunciamos então, a contribuição principal desta subseção:

Teorema 3.2.1 *Seja $F_{2^{t+3}}$ o corpo de Galois e seja C_1 o código* BCH *binário, primitivo e senso estrito de comprimento $n = 2^{t+3} - 1$, gerado pelo polinômio $g_1(x)$, que é o produto dos polinômios minimais*

$$g_1(x) = \langle M^{(1)} M^{(3)} M^{(5)} \cdots M^{(2t-1)} \rangle.$$

Escolha as primeiras $2t$ classes laterais ciclotômicas distintas, consecutivas, contidas no conjunto $B = \{\mathbb{C}_{2t+3}, \mathbb{C}_{2t+5}, \mathbb{C}_{2t+7}, \cdots, \mathbb{C}_{2^{\lceil (t+3)/2 \rceil} - 1}\}$.

Seja ${C_2}^{\perp}$ o código cíclico de comprimento $n = 2^{t+3} - 1$, gerado pelo polinômio ${g_2}^{\perp}(x)$, que é o produto dos $2t$ polinômios minimais

$$\langle M^{(2t+3)} M^{(2t+5)} M^{(2t+7)} \cdots M^{(2t+4t+1)} \rangle = \langle M^{(2t+3)} M^{(2t+5)} M^{(2t+7)} \cdots M^{(6t+1)} \rangle.$$

Considere ainda, o código cíclico C_2 de comprimento $n = 2^{t+3} - 1$, gerado pelo polinômio $g_2(x)$, que é o produto dos polinômios minimais

$$g_2(x) = M^{(0)} M^{(1)} M^{(3)} M^{(5)} \cdots M^{(2t-1)} M^{(2t+1)} \cdot \prod_i M^{(i)},$$

onde $M^{(i)}$ são os polinômios minimais tais que

$$i \notin \{2t + 3, 2t + 5, 2t + 7, \cdots, 6t + 1\},$$

onde i percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod $2^{t+3}-1$. Então, $C_2 \subset C_1$ e tanto C_1 quanto ${C_2}^{\perp}$ corrigem erros em t bits. Conseqüentemente, o código $CSS(C_1, C_2)$ possui os seguintes parâmetros

1. *Dimensão (k): $k = n - 3t^2 - 9t$;*
2. *Comprimento da Palavra-código (n): $n = 2^{t+3} - 1$;*
3. *Distância Mínima (d): $d \geq 2t + 1$.*

Equivalentemente, o código possui parâmetros

$$[[2^{t+3} - 1, 2^{t+3} - 1 - 3t^2 - 9t, d \geq 2t + 1]],$$

sendo capaz de corrigir erros quânticos arbitrários em t qubits, para todo $t \geq 9$.

Demonstração:

Pelas aplicações sucessivas dos Lemas 3.2.1 ao Lema 3.2.5, concluímos que é válida a inclusão $C_2 \subset C_1$ e que o código quântico $CSS(C_1, C_2)$ corrige t ou mais erros. Calculemos, agora, a dimensão dos códigos *CSS*.

Relembremos a equação (3.1): se $i \in \mathbb{C}_s$ então $M^{(i)}(x) = \prod_{j \in C_s} (x - \alpha^j)$.

A equação (3.1) significa que o grau do polinômio minimal $M^{(i)}(x)$ é igual à cardinalidade da respectiva classe lateral C_s, e assim, o grau do polinômio gerador de um código cíclico é igual à cardinalidade de seu conjunto de definição.

Como C_1 é um código cíclico sua dimensão, k_1, é dada por $k_1 = n - \partial(g_1(x))$, onde $n = 2^{t+3} - 1$ é o comprimento da palavra-código. Ainda, pela equação (3.1), $\partial(g_1(x))$ é igual à cardinalidade do conjunto de definição do código C_1. Além disso, pelo Lema 3.2.3 o conjunto de definição do código C_1 tem $t(t + 3)$ elementos, e assim

$$k_1 = 2^{t+3} - 1 - t(t + 3).$$

Similarmente, a dimensão do código cíclico C_2, a saber k_2, é igual a

$$k_2 = p^{t+1} - 1 - {k_2}^{\perp} = 2^{t+3} - 1 - [2^{t+3} - 1 - (t + 3)(2t)] = (2t)(t + 3),$$

onde ${k_2}^{\perp}$ é a dimensão do código ${C_2}^{\perp}$.

Então,

$$k_1 - k_2 = 2^{t+3} - 1 - (t + 3)t - (2t)(t + 3) = 2^{t+3} - 3t^2 - 9t - 1,$$

e assim, a dimensão do código quântico $CSS(C_1, C_2)$ é igual a $2^{t+3} - 1 - 3t^2 - 9t - 1$, completando a demonstração. □

Calcularemos, em seguida, a taxa desses códigos quânticos. Para isso, suponha que

$$f(t) = \frac{2^{t+3} - 1 - 3t^2 - 9t}{2^{t+3} - 1}.$$

Então, segue que

$$\lim_{t \longrightarrow \infty} f(t) = 1.$$

Conseqüentemente, a taxa assintótica dos códigos *CSS* tendem para um.

Listamos abaixo, os pontos principais do método de construção.

1. Os códigos quânticos *CSS* que corrigem erros quânticos arbitrários em t qubits são construídos sobre o corpo $F_{2^{t+3}}$.

2. O Lema 3.2.1 possibilita a escolha dos polinômios $g_1(x)$ e $g_2(x)$, geradores dos códigos C_1 e C_2, respectivamente, dados por

   $$g_1(x) = \langle M^{(1)} M^{(3)} M^{(5)} \cdots M^{(2t-1)} \rangle$$

   e

   $$g_2(x) = \langle M^{(0)} M^{(1)} M^{(3)} M^{(5)} \cdots M^{(2t-1)} M^{(2t+1)} \cdot \prod_i M^{(i)} \rangle,$$

   onde $M^{(i)}$ são os polinômios minimais tais que

   $$i \notin \{2t+3, 2t+5, 2t+7, \cdots, 6t+1\},$$

   onde i percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod $2^{t+3} - 1$.

3. Pelo Teorema 2.1.5 e pelos Lemas 3.2.2 e 3.2.3, concluímos que a distância mínima do código C_1 é maior ou igual a $2t + 1$, para todo $t \geq 9$.

4. Pelos Lemas 3.2.4 e 3.2.5, concluímos que a distância mínima do código dual ${C_2}^{\perp}$ é maior ou igual a $2t + 1$. Assim, o código quântico *CSS* corrige erros quânticos arbitrários em t qubits, para todo $t \geq 9$.

Embora o Teorema 3.2.1 garanta a construção de códigos quânticos *CSS* para todo $t \geq 9$, apresentaremos exemplos de construções, que são similares ao método de construção utilizado

no Teorema 3.2.1, que originam códigos quânticos *CSS* que corrigem erros quânticos arbitrários para $t = 2, 3, 4, 5, 6, 7, 8$ qubits. Esse fato ocorre pois, no Teorema 3.1.3, o limitante superior $2^{\lceil m/2 \rceil} + 1$ é relativamente baixo, e isso induz que o Teorema 3.2.1 seja verdadeiro para todo $t \geq 9$.

Entretanto, por verificação direta, notamos que, para os casos $t = 2, 3, 4, 5, 6, 7, 8$ também é possível realizar uma construção similar àquela utilizada no Teorema 3.2.1. De fato, o limitante superior $2^{\lceil m/2 \rceil} + 1$, dado no Teorema 3.1.3, pode ser melhorado. Além disso, pela aplicação do método de construção descrito na Observação 3.2.2, garantimos a aplicação do mesmo método de construção descrito no Teorema 3.2.1, para gerar códigos quânticos *CSS*, para os casos onde $t = 2, 3, 4, 5, 6, 7, 8$. Conseqüentemente, podemos supor, sem perda de generalidade, que o Teorema 3.2.1 é verdadeiro para todo $t \geq 2$.

Novamente, ressaltamos que, como o código ${C_2}^{\perp}$ é equivalente ao código gerado pelo polinômio $h(x)$, podemos considerar, sem perda de generalidade, que o código ${C_2}^{\perp}$ é gerado pelo polinômio $h(x)$. Note que todas as construções, para $t = 2, 3, 4, 5, 7$, são similares às desenvolvidas no Teorema 3.2.1.

Observação 3.2.2 *É possível construir códigos cíclicos binários C_1, C_2 e ${C_2}^{\perp}$, de comprimento $n = 2^l - 1$, onde $l < t+3$ que também corrigem t erros. Para isso, é suficiente verificar que as classes ciclotômicas relacionadas aos códigos C_1 e ${C_2}^{\perp}$, são todas distintas e que cada uma destas contém l elementos. Descrevemos o método de construção em seguida.*

Seja C_1 o código BCH *de comprimento $n = 2^l - 1$, gerado pelo polinômio $g_1(x)$, que é o produto dos polinômios minimais*

$$g_1(x) = \langle M^{(1)} M^{(3)} M^{(5)} \cdots M^{(2t-1)} \rangle.$$

Seja ${C_2}^{\perp}$ o código cíclico de comprimento $n = 2^l - 1$, gerado pelo polinômio ${g_2}^{\perp}(x)$, que é o produto dos $2t$ polinômios minimais

$$\langle M^{(2t+3)} M^{(2t+5)} M^{(2t+7)} \cdots M^{(2t+4t+1)} \rangle = \langle M^{(2t+3)} M^{(2t+5)} M^{(2t+7)} \cdots M^{(6t+1)} \rangle,$$

e seja C_2 o código cíclico de comprimento $n = 2^l - 1$, gerado pelo polinômio $g_2(x)$, que é o produto dos polinômios minimais

$$g_2(x) = \langle M^{(0)} M^{(1)} M^{(3)} M^{(5)} \cdots M^{(2t-1)} M^{(2t+1)} \cdot \prod_i M^{(i)} \rangle,$$

onde $M^{(i)}$ são todos os polinômios minimais tais que

$$i \notin \{2t + 3, 2t + 5, 2t + 7, \cdots, 6t + 1\}$$

e i percorre os representantes das classes laterais ciclotômicas mod $2^l - 1$.

Então, $C_2 \subset C_1$ e tanto C_1 quanto ${C_2}^{\perp}$ corrigem erros em t bits. Estes fatos possibilitam as construções dos códigos quânticos CSS.

Exemplo 3.2.1 *Considere os códigos cíclicos C_1 e C_2 com comprimento $2^6 - 1 = 63$, cujos polinômios geradores são dados por*

$$C_1 = \langle g_1(x) \rangle = \langle M^{(1)} M^{(3)} \rangle,$$

$$C_2{}^{\perp} = \langle g_2{}^{\perp}(x) \rangle = \langle M^{(15)} M^{(31)} \rangle,$$

e

$$C_2 = \langle g_2(x) \rangle = \langle M^{(0)} M^{(1)} M^{(3)} M^{(5)} M^{(7)} M^{(9)} M^{(11)} M^{(13)} M^{(21)} M^{(23)} M^{(27)} \rangle.$$

Por construção, o código C_1 corrige 2 erros e ainda vale a inclusão $C_2 \subset C_1$. Além disso, existe uma seqüência de números naturais consecutivos, $59, 60, 61, 62$, relacionada ao código $C_2{}^{\perp}$. Disso decorre que o código $C_2{}^{\perp}$ também corrige 2 erros. A dimensão do código CSS *é $63 - 24 = 39$.*

Pelo mesmo método utilizado no Teorema 3.2.1 e pela Observação 3.2.2, geramos o código $CSS(C_1, C_2)$, com parâmetros $[[63, 39, 5]]$ que corrige erros quânticos arbitrários em 2 qubits.

Exemplo 3.2.2 *Neste exemplo, reproduzimos, por inspeção direta, todos os códigos quânticos* BCH*, exceto três, construídos em [13]. Além disso, geramos um novo código $[[63, 10, 8]]$. Exibiremos alguns destes códigos apresentando os respectivos polinômios geradores:*

1) $[[7, 1, 3]]$*;*
$C_1 = \langle M^{(1)} \rangle$; $C_1[7, 4, 3]$ *e* $C_2{}^{\perp} = \langle M^{(3)} \rangle$; $C_2{}^{\perp}[7, 4, 3]$*;*

2) $[[31, 1, 7]]$*;*
$C_1 = \langle M^{(1)} M^{(3)} M^{(5)} \rangle$; $C_1[31, 16, 7]$ *e* $C_2{}^{\perp} = \langle M^{(7)} M^{(11)} M^{(15)} \rangle$; $C_2{}^{\perp}[31, 16, 7]$.

3) $[[63, 10, 8]]$*;*
$C_1 = \langle M^{(1)} M^{(3)} M^{(5)} M^{(7)} \rangle$; $C_1[63, 39, 9]$ *e*
$C_2{}^{\perp} = \langle M^{(11)} M^{(13)} M^{(21)} M^{(23)} M^{(27)} M^{(31)} \rangle$; $C_2{}^{\perp}[63, 34, 7]$.

4) $[[127, 29, 15]]$*;*
$C_1 = \langle M^{(1)} M^{(3)} M^{(5)} M^{(7)} M^{(9)} M^{(11)} M^{(13)} \rangle$; $C_1[127, 78, 15]$ *e*
$C_2{}^{\perp} = \langle M^{(15)} M^{(23)} M^{(29)} M^{(31)} M^{(47)} M^{(55)} M^{(63)} \rangle$; $C_2{}^{\perp}[127, 78, 15]$.

Exemplo 3.2.3 *Pelo mesmo método utilizado no Teorema 3.2.1 e pela Observação 3.2.2, construímos o novo código quântico*

$CSS(C_1, C_2) = [[255, 143, 15]]$*;*
$C_1 = \langle M^{(1)} M^{(3)} M^{(5)} M^{(7)} M^{(9)} M^{(11)} M^{(13)} \rangle$; $C_1[255, 199, 15]$ *e*
$C_2{}^{\perp} = \langle M^{(31)} M^{(47)} M^{(61)} M^{(63)} M^{(111)} M^{(125)} M^{(127)} \rangle$; $C_2{}^{\perp}[255, 199, 15]$.

Exemplo 3.2.4 *Neste exemplo, construímos três novos códigos* CSS*:*
1) $CSS(C_1, C_2) = [[511, 241, \geq 31]]$*, onde*
$C_1 = \langle M^{(1)}M^{(3)}M^{(5)}M^{(7)} \cdots M^{(27)}M^{(29)} \rangle$; $C_1[512, 376, 31]$ *e*
${C_2}^{\perp} = \langle M^{(127)}M^{(255)}M^{(191)}M^{(63)}M^{(223)}M^{(125)}M^{(95)}M^{(31)}M^{(239)}M^{(123)} \cdots$
$\cdots M^{(175)}M^{(61)}M^{(111)}M^{(79)}M^{(47)} \rangle$; ${C_2}^{\perp}[512, 376, 31]$.

2) $CSS(C_1, C_2) = [[1023, 743, \geq 29]]$*, onde*
$C_1 = \langle M^{(1)}M^{(3)}M^{(5)}M^{(7)} \cdots M^{(25)}M^{(27)} \rangle$; $C_1[1023, 883, 29]$ *e*
${C_2}^{\perp} = \langle M^{(511)}M^{(255)}M^{(383)}M^{(127)}M^{(447)}M^{(253)}M^{(191)}M^{(63)}M^{(251)}M^{(479)} \cdots$
$\cdots M^{(351)}M^{(125)}M^{(223)}M^{(159)} \rangle$; ${C_2}^{\perp}[1023, 883, 29]$.

3) $[[1023, 723, \geq 31]]$*, onde*
$C_1 = \langle M^{(1)}M^{(3)}M^{(5)}M^{(7)}M^{(9)}M^{(11)}M^{(13)}M^{(15)}M^{(17)}$
$M^{(19)}M^{(21)}M^{(23)}M^{(25)}M^{(27)}M^{(29)} \rangle$; $C_1[1023, 873, 31]$ *e*
${C_2}^{\perp} = \langle M^{(511)}M^{(255)}M^{(383)}M^{(127)}M^{(447)}M^{(253)}M^{(191)}M^{(63)}M^{(251)}M^{(479)}M^{(351)}$
$M^{(125)}M^{(223)}M^{(159)}M^{(95)} \rangle$; ${C_2}^{\perp}[1023, 873, 31]$.

3.2.2 Método de construção II - *CSS* q-ários

A principal contribuição desta subseção é o Teorema 3.2.6. Este teorema mostra que, para que os códigos quânticos *CSS* corrijam erros quânticos arbitrários em t qudits, devemos construir códigos cíclicos p-ários (p primo) C_1, C_2 e ${C_2}^{\perp}$ sobre o corpo $F_{p^{t+1}}$.

Uma importante diferença entre o caso binário e o caso p-ário é que os métodos de construção p-ários serão realizados sobre o corpo $F_{p^{t+1}}$, enquanto que no caso binário os códigos *CSS* são construídos sobre o corpo $F_{2^{t+3}}$.

O Teorema 3.2.6, fornece um método de construção de códigos quânticos *CSS*, baseado na construção de três códigos cíclicos p-ários. Tal teorema gera família de bons códigos $CSS(C_1, C_2)$ com parâmetros $[[n, k = k_1 - k_2, d \geq 2t + 1]]$, que corrigem erros quânticos arbitrários em t qubits, para todo $t \geq 2$. Enfatizamos, novamente, que os códigos cíclicos p-ários C_1, C_2 e ${C_2}^{\perp}$ serão construídos sobre o corpo $F_{p^{t+1}}$. Na seqüência, definimos os códigos quânticos *CSS* q-ários.

Definição 3.2.1 *[16] Sejam C_1 e C_2 dois códigos clássicos lineares com parâmetros $[n, k_1, d_1]_q$ e $[n, k_2, d_2]_q$, respectivamente, tal que $C_2 \subset C_1$. Então, existe um código quântico $[[n, K = k_1 - k_2, D]]_q$, onde $D = \min\{wt(c) \mid c \in (C_1 \backslash C_2) \cup ({C_2}^{\perp} \backslash {C_1}^{\perp})\}$. A codificação e a decodificação do código* CSS *é baseada na codificação e na decodificação dos códigos clássicos considerados no processo de construção.*

Os Lemas 3.2.6 e 3.2.7 também são encontrados em [16]. Denotaremos $m = ord_n(q)$ a

ordem multiplicativa de q módulo m, ou seja, m é o menor inteiro tal que $n \mid (q^m - 1)$. Assim, os zeros do polinômio $x^n - 1$ pertencem ao corpo F_{q^m} e não pertence a nenhum corpo de menor cardinalidade.

Lema 3.2.6 *[16] Seja n um inteiro positivo e considere q uma potência de primo tal que $mdc(n, q) = 1$ e $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$, onde $m = ord_n(q)$ e $\lfloor x \rfloor$ denota o maior inteiro menor ou igual a x. As classes laterais ciclotômicas $\mathbb{C}_x = \{xq^j \ mod\, n \mid 0 \leq j < m\}$ possuem cardinalidade m, para todo x tal que $1 \leq x \leq nq^{\lceil m/2 \rceil}/(q^m - 1)$.*

Lema 3.2.7 *[16] Seja $n \geq 1$ um inteiro e q uma potência de primo tal que $mdc(n, q) = 1$ e $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$, onde $m = ord_n(q)$. Se x e y são números distintos pertencentes ao intervalo $1 \leq x, y \leq min\ \{\lfloor nq^{\lceil m/2 \rceil}/(q^m - 1) - 1 \rfloor, n - 1\}$ tais que não vale a congruência $x, y \equiv 0\ mod\ q$, então as classes laterais ciclotômicas q-árias de x e y módulo n são distintas.*

Para todo o contexto desta subseção, utilizaremos a seguinte afirmação, que prova que a função $g(p) = p^{(t+1)/2} - 2pt - 2t - 4$ é uma função estritamente crescente e também prova que $g(p) > 0$, para todo $p \geq 3$ e para todo número inteiro fixo $t > 7$. Este resultado será utilizado nas demonstrações dos Lemas 3.2.8, 3.2.9, 3.2.10, 3.2.11 e 3.2.12, onde provaremos que tais lemas são válidos para todo primo p, $p \geq 3$. Mais especificamente, utilizaremos esta afirmação implicitamente na demonstração desses cinco lemas.

Afirmação 3.2.3 *Para todo número inteiro $t \geq 7$ fixo, e para todo inteiro $p \geq 3$, a função $g(p) = p^{(t+1)/2} - 2pt - 2t - 4$ é uma função estritamente crescente da variável p. Além disso, $g(p) > 0$.*

Demonstração: Calculando a derivada da função $g(p)$, temos que $g'(p) = \frac{t+1}{2} p^{\frac{t-1}{2}} - 2t$. Calculando a derivada da função $g'(p)$, segue que $g''(p) = \frac{t+1}{2}\frac{t-1}{2} p^{\frac{t-3}{2}}$.

Como $g''(p) > 0$, para todo $p > 0$ e para todo $t > 1$ fixo, deduzimos que $g'(p)$ é uma função estritamente crescente, para todo $p > 0$ e para todo $t > 1$ fixado. Como $g'(3) > 0$, para todo $p \geq 3$ e para todo $t \geq 4$, $g'(p) > 0$, para todo $p \geq 3$ e para todo $t \geq 4$. Então $g(p)$ é uma função estritamente crescente, onde $p \geq 3$ e $t \geq 4$ é um inteiro fixado. Como $g(3) = 3^{(t+1)/2} - 8t - 4 > 0$, para todo $t \geq 7$, concluímos que $g(p) > 0$, para todo $p \geq 3$ e para todo inteiro $t \geq 7$. □

Começaremos a construção dos códigos quânticos *CSS* p-ários considerando o Lema 3.2.8 que, como no caso binário, garante a escolha dos polinômios minimais que gerarão os códigos C_1, C_2 e ${C_2}^{\perp}$.

Lema 3.2.8 *Para $t \geq 3$ e para todo número primo fixado $p \geq 3$, é válida a desigualdade $p^{t+1} \geq (4t+1)(t+1)$.*

Demonstração: Considere a função $h(t) = p^{t+1} - 4t^2 - 5t - 1$. Podemos gerar uma função similar à função dada na Afirmação 3.2.3, e assim, é suficiente mostrar que $h(t) > 0$, para $p = 3$ e para todo $t \geq 3$.

Calculando as primeiras derivadas obtemos $h'(t) = (\ln p)p^{t+1} - 8t - 5$ e $h''(t) = (\ln p)^2 p^{t+1} - 8$. Como $h''(t) > 0$, para todo $t \geq 3$ e para $p = 3$, $h'(t)$ é uma função estritamente crescente. Além disso, como $h'(3) > 0$, segue que $h'(t) > 0$, para todo $t \geq 3$. Assim, $h(t)$ é estritamente crescente. Como $h(3) > 0$, temos que $h(t) > 0$, para todo $t \geq 3$. Logo, $p^{t+1} \geq (4t+1)(t+1),\ t \geq 3$, como requerido. □

Novamente, de acordo com o Teorema 3.1.1, o Lema 3.2.8 afirma sobre a existência de "pelo menos" $4t+1$ polinômios mônicos irredutíveis, sobre o corpo F_p, cujo grau divide $m = t+1$. Pela definição de classes laterais ciclotômicas, existe um conjunto com pelo menos $4t+1$ tais classes laterais distintas, permitindo a escolha para os códigos C_1, C_2 e ${C_2}^{\perp}$, onde estes satisfazem as hipóteses da construção do código *CSS*. Mais especificamente, o Lema 3.2.8 afirma que o corpo $F_{p^{t+1}}$ é um candidato eficaz para a construção dos códigos quânticos *CSS*, pois nesse corpo, existem muitas classes laterais ciclotômicas distintas. Adiante, explicaremos esse fato em detalhes.

Como no caso binário, a idéia é a construção de um código *BCH* C_1 contendo "no máximo" $2t$ classes laterais ciclotômicas distintas de tal modo que a união de tais classes contenha uma seqüência de, pelo menos, $2t$ números naturais consecutivos. Isso significa que o código C_1 corrigirá t erros. Além disso, também queremos construir um código cíclico ${C_2}^{\perp}$ contendo $2t$ classes laterais ciclotômicas distintas, de tal modo que tais classes laterais contenham uma seqüência de, no mínimo, $2t$ números naturais consecutivos, donde o código ${C_2}^{\perp}$ corrigirá t erros. Baseados nessas afirmações, precisamos garantir que o corpo utilizado para tais construções possua cardinalidade grande o suficiente para conter mais do que $4t$ classes laterais distintas, o que foi demonstrado no Lema 3.2.8.

Observação 3.2.4 *No caso binário sabemos que, se k for um número par, as classes laterais ciclotômicas $\mathbb{C}_k$ são iguais às classes laterais da forma $\mathbb{C}_j$, onde j é um número ímpar. Evidentemente, no caso p-ário, as únicas classes laterais consideradas são as classes da forma*

$$\{\mathbb{C}_1, \mathbb{C}_2, \cdots, \mathbb{C}_{p-1}, \mathbb{C}_{p+1}, \mathbb{C}_{p+2}, \mathbb{C}_{p+3}, \cdots, \mathbb{C}_{2p-1}, \cdots, \mathbb{C}_{2n+1}\},$$

onde n é um número natural. Assim, serão consideradas apenas as classes laterais da forma $\mathbb{C}_m$, onde $p \nmid m$, onde utilizamos a notação $\nmid$ significando que p não divide m. Suporemos que esta condição será satisfeita em todo contexto desta tese.

Na seqüência, demonstramos o Lema 3.2.9.

Lema 3.2.9 *Seja $p \geq 3$ um primo fixo e $n = p^{t+1} - 1$. Sejam*

$$\{\mathbb{C}_1, \mathbb{C}_2, \cdots, \mathbb{C}_{p-1}, \mathbb{C}_{p+1}, \mathbb{C}_{p+2}, \cdots, \mathbb{C}_{2p-1}, \mathbb{C}_{2p+1}, \mathbb{C}_{2p+2}, \cdots, \mathbb{C}_{2t}\},$$

classes laterais ciclotômicas distintas. Então, o conjunto $A = \mathbb{C}_1 \cup \cdots \cup \mathbb{C}_{2t}$ contém todos os números $1 \leq j \leq 2t$.

Demonstração: Demonstraremos este lema por absurdo. Por hipótese, as classes laterais $\{\mathbb{C}_1, \mathbb{C}_2, \cdots, \mathbb{C}_{2t}\}$ são distintas. Suponha que exista um número $j_1, 1 \leq j_1 \leq 2t$, tal que $j_1 \notin A$. Então, existe uma classe lateral $\mathbb{C}_k$ tal que $j_1 \in \mathbb{C}_k$, onde $\mathbb{C}_k \nsubseteq A$, caso contrário $j_1 \in A$. Como todas as classes laterais ciclotômicas são distintas, segue que $k > 2t$, onde k é o menor elemento da classe lateral $\mathbb{C}_k$. Assim, como $j_1 \in \mathbb{C}_k$, segue que $j_1 \geq k \geq 2t$, uma contradição. □

Lema 3.2.10 *Seja $p \geq 3$ um primo fixo e $n = p^{t+1} - 1$. Se $p \nmid 2t + 1$, então as classes laterais ciclotômicas*

$$\{\mathbb{C}_1, \mathbb{C}_2, \cdots, \mathbb{C}_{p-1}, \mathbb{C}_{p+1}, \mathbb{C}_{p+2}, \mathbb{C}_{p+3}, \cdots, \mathbb{C}_{2p-1}, \mathbb{C}_{2p+1}, \mathbb{C}_{2p+2}, \cdots, \mathbb{C}_{2t}, \mathbb{C}_{2t+1}\}$$

são distintas, para todo $t \geq 4$, e cada classe lateral contém $t + 1$ elementos.

Demonstração: Considere, no Lema 3.2.7, $p = q$ e $n = p^{t+1} - 1$. Seja $x = 1$ e $y = 2t + 1$. Como $m = t + 1 > 1$, temos que

$$x, y \leq \lfloor p^{\lceil (t+1)/2 \rceil} - 1 \rfloor < n - 1.$$

Ainda, sabemos que $\text{mdc}(n, q) = 1$. Pela Observação 3.2.4, a congruência $x, y \equiv 0 \ mod \ q$ não é válida. Então, é suficiente provar que $\lfloor p^{\lceil (t+1)/2 \rceil} - 1 \rfloor > 2t + 1$.

Considere a função $g(t) = p^{(t+1)/2} - 2t - 3$, $t \geq 4$. Calculando a derivada da função $g(t)$ resulta $g'(t) = (\ln p)/2p^{(t+1)/2} - 2$. Como $g'(t) > 0$, para todo $t \geq 4$ e para $p = 3$, isso implica que $g(t)$ é uma função estritamente crescente, para todo $t \geq 4$. Ainda, $g(4) = 4,58 > 0$, no caso $p = 3$. Analogamente ao que já foi utilizado na demonstração do Lema 3.2.8, podemos gerar uma função similar à função dada na Afirmação 3.2.3 de tal forma que, como para todo número primo $p \geq 3$, temos que $g(4) > 0$, então, $g(t) > 0$, para todo $t \geq 4$ e para todo primo $p \geq 3$. Conseqüentemente, vale a desigualdade $p^{(t+1)/2} - 2 > 2t$, e assim, $\lfloor p^{\lceil (t+1)/2 \rceil} - 1 \rfloor > 2t + 1$. Pelo Lema 3.2.6, como $n = p^m - 1$, obtemos que as classes laterais ciclotômicas distintas, consideradas na hipótese, possuem cardinalidade $t + 1$. □

O Lema 3.2.10 garante que os códigos C_2 e C_1 são diferentes, ou seja, $C_2 \subsetneqq C_1$.

Lema 3.2.11 *Seja $p \geq 3$ um primo fixo, $p \nmid 2t+2$, e $n = p^{t+1} - 1$. Então, as $2t$ (ou mais) classes laterais ciclotômicas dadas por*

$$\{\mathbb{C}_{2t+2}, \mathbb{C}_{2t+2+p}, \mathbb{C}_{2t+2+2p}, \mathbb{C}_{2t+2+3p}, \cdots, \mathbb{C}_{2t+2+(2t-1)p}, \cdots\},$$

(que contém o conjunto de definição do código $C_2{}^{\perp}$, como será explicitado no Teorema 3.2.6) são todas distintas e cada uma destas contém $t+1$ elementos, para todo $t \geq 7$. Além disso, essas classes laterais ciclotômicas distintas, também são distintas das classes laterais $\mathbb{C}_1, \mathbb{C}_2, \cdots, \mathbb{C}_{2t+1}$. Em outras palavras, vale a desigualdade $\lfloor p^{\lceil (t+1)/2 \rceil} - 1 \rfloor > p(2t-1) + 2t + 2$, para todo $t \geq 7$.

Demonstração: No Lema 3.2.7, considere $p = q$, $n = p^{t+1} - 1$, $x = 1$ e $y = p(2t-1)+2t+2$. Devemos mostrar que $p^{\lceil (t+1)/2 \rceil} - 2pt - 2t - p - 2 > 0$. Se tal desigualdade é verdadeira, pelos Lemas 3.2.7 e 3.2.6, concluímos o resultado.

Analogamente ao que foi utilizado na demonstração dos Lemas 3.2.8 e 3.2.10, podemos gerar uma função similar à função dada na Afirmação 3.2.3 de tal forma que é suficiente mostrar que a desigualdade $p^{(t+1)/2} - 2pt - 2t - p - 2 > 0$ é verdadeira para todo $t \geq 7$ e para $p = 3$, para que se prove esse lema.

Fixemos, então, p primo e considere a função $f(t) = p^{(t+1)/2} - 2pt - 2t - p - 2$. Calculando a derivada de $f(t)$, temos que $f'(t) = \frac{(\ln p)}{2} p^{(t+1)/2} - 2p - 2$. Calculando, agora, a derivada segunda de $f(t)$ temos que $f''(t) = \frac{(\ln p)^2}{4} p^{(t+1)/2}$. Claramente, $f''(t) > 0$, para todo primo $p \geq 3$ e assim, $f'(t)$ é uma função estritamente crescente, para todo $t \geq 7$. Como $f'(7) > 0$, implica que $f'(t) > 0$, para todo $t \geq 7$ e para todo primo p. Disso decorre que $f(t)$ é uma função estritamente crescente, para todo $t \geq 7$. Como $f(7) > 0$, para $p = 3$, $f(t) > 0$, para todo $t \geq 7$ e para todo $p \geq 3$, donde a prova está completa. □

Observação 3.2.5 *Note que se supuséssemos que $p \mid 2t+2$, seria suficiente mostrar que as $2t$ ou mais classes laterais ciclotômicas*

$$\{\mathbb{C}_{2t+3}, \mathbb{C}_{2t+3+p}, \mathbb{C}_{2t+3+2p}, \cdots, \mathbb{C}_{2t+3+(2t-1)p}, \cdots\},$$

satisfariam a equação $\lfloor p^{\lceil (t+1)/2 \rceil} - 1 \rfloor > p(2t-1)+2t+3$, para todo $t \geq 7$, a qual é verdadeira: seja $g(t) = p^{(t+1)/2} - 2pt - 2t - 5$. Similarmente à demonstração do Lema 3.2.11, concluímos que $g(t) > 0$, para todo $t \geq 7$ e para todo primo $p \geq 3$. Assim, o resultado segue diretamente.

O Lema 3.2.12 demonstra a existência de uma seqüência de, no mínimo, $2t$ números naturais consecutivos, pertencentes ao conjunto de definição do código $C_2{}^{\perp}$, como será exibido no Teorema 3.2.6. Conseqüentemente, o código $C_2{}^{\perp}$ possuirá distância mínima pelo menos $2t+1$, e assim, o código corrigirá t erros.

Lema 3.2.12 *Seja $p \geq 3$ um primo fixo e $n = p^{t+1} - 1$. Suponha que $p \nmid 2t+2$. Então, os últimos elementos das $2t$ (ou mais) classes laterais ciclotômicas distintas (que contém o conjunto de definição do do código $C_2{}^{\perp}$, como será explicitado no Teorema 3.2.6), cada uma destas contendo $t+1$ elementos, dadas por*

$$\{\mathbb{C}_{2t+2}, \mathbb{C}_{2t+2+p}, \mathbb{C}_{2t+2+2p}, \mathbb{C}_{2t+2+3p}, \cdots, \mathbb{C}_{2t+2+(2t-1)p}, \cdots\},$$

formam uma seqüência de, no mínimo, $2t$ números naturais consecutivos.

Demonstração: Pelo Lema 3.2.11, existem $2t$ ou mais classes laterais ciclotômicas distintas, cada uma contendo $t+1$ elementos, dadas por

$$\{\mathbb{C}_{2t+2}, \mathbb{C}_{2t+2+p}, \mathbb{C}_{2t+2+2p}, \mathbb{C}_{2t+2+3p}, \cdots, \mathbb{C}_{2t+2+(2t-1)p}, \cdots\}.$$

Demonstraremos que os últimos elementos destas classes laterais formam uma seqüência de, no mínimo, $2t$ números naturais consecutivos.

Sejam

$$\{\mathbb{C}_{2t+2}, \mathbb{C}_{2t+3}, \cdots, \mathbb{C}_{2t+2+(2t-1)p}, \cdots\}$$

classes laterais ciclotômicas distintas, todas contendo exatamente $t+1$ elementos.

Sejam $\mathbb{C}_s$ e $\mathbb{C}_{s+p}$ duas destas classes. Considere u e v os últimos elementos das classes laterais $\mathbb{C}_s$ e $\mathbb{C}_{s+p}$, respectivamente, sem considerar a operação mod. Então, segue que

$$u = s.p^{m-1} = s.p^t$$

e

$$v = (s+p).p^{m-1} = (s+p).p^t.$$

Assim, $v = s.p^t + p^{t+1}$, donde

$$v \equiv s.p^t + 1 \ \ mod\ (p^{t+1} - 1).$$

Em outras palavras,

$$v \equiv u + 1 \ \ mod\ (p^{t+1} - 1).$$

Considere $q = p^{t+1} - 1$ e expanda v e $u+1$ em termos do algoritmo de Euclides sobre q. Então, existem números inteiros a, b, r_1 e r_2, onde $0 \leq r_1 < q$ e $0 \leq r_2 < q$ tais que

$$v = aq + r_1 \qquad e \qquad u + 1 = bq + r_2.$$

Como $v \equiv u+1 \mod (2^{t+3}-1)$, deduzimos que $r_1 = r_2$. Denotaremos este número comum por v^*. Assim, temos que

$$v = aq + v^* \qquad e \qquad u+1 = bq + v^*,$$

onde $0 \leq v^* < q$. Assim,

$$u = bq + v^* - 1.$$

Se $u^* = v^* - 1$, então $1 \leq u^* < q$.

Além disso, pela unicidade do resto no algoritmo da divisão de Euclides, concluímos que u^* é o resto da divisão do número u pelo número $q = p^{t+1} - 1$. Isso significa que os representantes v^* e u^* dos números v e u, respectivamente, são números consecutivos, ou seja, $v^* = u^* + 1$, concluindo a demonstração. □

Observe que o Lema 3.2.12 continua válido mesmo sem considerar a hipótese que cada uma destas classes laterais contém $t+1$ elementos, ou seja: suponha que $q = p$ e $n = p^m - 1$. Se $\mathbb{C}_s \neq \mathbb{C}_{s+p}$ e $s + p \neq 0$ então os termos $u = sp^{m-1} \in \mathbb{C}_s$ e $v = (s+p)p^{m-1} \in \mathbb{C}_{s+p}$ são consecutivos mod n. Entretanto, preferimos manter tal hipótese para que o leitor saiba que cada classe lateral contida no conjunto de definição do código ${C_2}^{\perp}$, que será construído no Teorema 3.2.6, possui $t+1$ elementos, e isso possibilita explicitar a dimensão do código *CSS* resultante deste novo método de construção sendo proposto.

Como resultado de aplicações sucessivas dos cinco lemas demonstrados, enunciamos a contribuição principal desta subseção:

Teorema 3.2.6 *Sejam C_1, C_2 e ${C_2}^{\perp}$ códigos cíclicos p-ários de comprimento $n = p^{t+1} - 1$.*

Caso 1*: $p \nmid 2t$ e $p \nmid 2t+1$. Seja C_1 o código* BCH *gerado pelo produto dos polinômios minimais*

$$C_1 = \langle g_1(x) \rangle = \langle M^{(1)} M^{(2)} M^{(3)} \cdots M^{(2t)} \rangle.$$

Se $p \nmid 2t+2$, considere as primeiras $2t$ classes laterais ciclotômicas distintas, consecutivas, contidas no conjunto

$$B = \{\mathbb{C}_{2t+2}, \mathbb{C}_{2t+2+p}, \mathbb{C}_{2t+2+2p}, \cdots, \mathbb{C}_{2t+2+(2t-1)p}, \cdots\},$$

(senão seria suficiente trocar $\mathbb{C}_{2t+2+ip}$ por $\mathbb{C}_{2t+3+ip}$, onde i é um número natural tal que $0 \leq i \leq 2t$).

Seja ${C_2}^{\perp}$ o código cíclico gerado pelo produto dos $2t$ polinômios minimais

$$M^{(2t+2)} M^{(2t+2+p)} M^{(2t+2+2p)} \cdots M^{(2t+2+(2t-1)p)},$$

e C_2 *o código cíclico gerado pelo produto dos polinômios minimais*

$$\left\langle M^{(0)}M^{(1)}M^{(2)}M^{(3)}\cdots M^{(2t)}M^{(2t+1)}\cdot\prod_i M^{(i)}\right\rangle,$$

onde $M^{(i)}$ *são todos os polinômios minimais tais que*

$$i\notin\{1,2,3,\cdots,2t,2t+2,2t+2+p,2t+2+2p,\cdots,2t+2+(2t-1)p\},$$

e i *percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod* $p^{t+1}-1$.

Caso 2*:* $p\mid 2t$*. Seja* C_1 *o código* BCH *gerado pelo produto dos polinômios minimais*

$$C_1=\langle g_1(x)\rangle=\langle M^{(1)}M^{(2)}M^{(3)}\cdots M^{(2t-1)}\rangle,$$

${C_2}^{\perp}$ *o código cíclico gerado pelo produto dos* $2t$ *polinômios minimais*

$$\langle M^{(2t+2)}M^{(2t+2+p)}M^{(2t+2+2p)}\cdots M^{(2t+2+(2t-1)p)}\rangle,$$

e C_2 *o código cíclico gerado pelo polinômio*

$$C_2=\langle g_2(x)\rangle=\left\langle M^{(0)}M^{(1)}M^{(2)}M^{(3)}\cdots M^{(2t+1)}\cdot\prod_i M^{(i)}\right\rangle,$$

onde $M^{(i)}$ *são todos os polinômios minimais tais que*

$$i\notin\{1,2,3,\cdots,2t-1,2t+2,2t+2+p,2t+2+2p,\cdots,2t+2+(2t-1)p\},$$

e i *percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod* $p^{t+1}-1$.

Caso 3*:* $p\nmid 2t$ *e* $p\mid 2t+1$*. Seja* C_1 *o código* BCH *gerado pelo polinômio*

$$g_1(x)=M^{(1)}M^{(2)}M^{(3)}\cdots M^{(2t)},$$

${C_2}^{\perp}$ *o código cíclico gerado pelo produto dos* $2t$ *polinômios minimais*

$$\langle M^{(2t+3)}M^{(2t+3+p)}M^{(2t+3+2p)}\cdots M^{(2t+3+(2t-1)p)}\rangle$$

e C_2 *o código cíclico gerado pelo produto dos polinômios minimais*

$$C_2=\langle g_2(x)\rangle=\left\langle M^{(0)}M^{(1)}M^{(2)}M^{(3)}\cdots M^{(2t)}\cdot\prod_i M^{(i)}\right\rangle,$$

onde $M^{(i)}$ *são todos os polinômios minimais tais que*

$$i\notin\{1,2,3,\cdots,2t,2t+3,2t+3+p,2t+3+2p,\cdots,2t+3+(2t-1)p\}$$

e i percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod $p^{t+1}-1$.

Então, para todo os casos, vale a inclusão $C_2 \subset C_1$ e cada um dos códigos C_1 e ${C_2}^{\perp}$ corrigem erros em t dits. Além disso, $n = p^{t+1}-1$, o código quântico $CSS(C_1, C_2)$ possui dimensão

$$k = n - 2t(t+1) - (2t-j)(t+1) = p^{t+1} - 1 - (t+1)(4t-j),$$

onde j é o número de classes laterais ciclotômicas do código C_1, indexadas por múltiplos de p, $j \leq 2t+1$ e possui parâmetros

$$[[p^{t+1}-1, p^{t+1}-1-(t+1)(4t-j), d \geq 2t+1]]_p$$

e corrige erros quânticos arbitrários em t qudits, para todo $t \geq 7$.

Demonstração:

Pelas aplicações sucessivas dos Lemas 3.2.8, 3.2.9, 3.2.10, 3.2.11 e 3.2.12, concluímos que $C_2 \subset C_1$ e que o código quântico $CSS(C_1, C_2)$ corrige t ou mais erros. Calculemos a dimensão dos novos códigos *CSS*.

Sabemos que a equação (3.1): se $i \in \mathbb{C}_s$ então

$$M^{(i)}(x) = \prod_{j \in C_s} (x - \alpha^j),$$

significa que o grau do polinômio minimal $M^{(i)}(x)$ é igual à cardinalidade da respectiva classe lateral C_s, e assim, o grau do polinômio gerador de um código cíclico é igual à cardinalidade de seu conjunto de definição.

Como C_1 é um código cíclico sua dimensão, k_1, é dada por $k_1 = n - \partial(g_1(x))$, onde $n = p^{t+1}-1$ é o comprimento da palavra-código. Ainda, pela equação (3.1), $\partial(g_1(x))$ é igual à cardinalidade do conjunto de definição do código C_1. Além disso, pelo Lema 3.2.10 o conjunto de definição do código C_1 tem $(t+1)(2t-j)$ elementos, e assim

$$k_1 = p^{t+1} - 1 - (t+1)(2t-j).$$

Similarmente, a dimensão do código cíclico C_2, a saber k_2, é igual a

$$k_2 = p^{t+1} - 1 - {k_2}^{\perp} = p^{t+1} - 1 - [p^{t+1} - 1 - (t+1)(2t)] = (2t)(t+1),$$

onde ${k_2}^{\perp}$ é a dimensão do código ${C_2}^{\perp}$.

Então,

$$k_1 - k_2 = p^{t+1} - 1 - (t+1)(2t-j) - (2t)(t+1) = p^{t+1} - 1 - (t+1)(4t-j),$$

e assim, a dimensão do código quântico $CSS(C_1, C_2)$ é igual a $p^{t+1} - 1 - (t+1)(4t-j)$.

□

Ilustraremos o **Caso 1** do Teorema 3.2.6, através de um esquema gráfico:

$$\underbrace{\mathbb{C}_0 \overbrace{\mathbb{C}_1\ \mathbb{C}_3\ \cdots\ \mathbb{C}_{2t}}^{C_1}\ \mathbb{C}_{2t+1}}_{C_2}\ \overbrace{\mathbb{C}_{2t+2}\ \mathbb{C}_{2t+2+p}\ \mathbb{C}_{2t+2+2p}\ \cdots\ \mathbb{C}_{2t+2+(2t-1)p}}^{C_2{}^{\perp}}\ \underbrace{\mathbb{C}_{r_1}\ \cdots\ \mathbb{C}_{r_n}}_{C_2},$$

onde $\mathbb{C}_0,\ \mathbb{C}_1,\ \cdots, \mathbb{C}_{r_n}$ são todas as classes laterais ciclotômicas para $q = p$ e $n = p^{t+1} - 1$.

Assim como no caso binário, também é válido para o caso p-ário o resultado a seguir:

$$\lim_{t \longrightarrow \infty} f(t) = 1,$$

onde

$$f(t) = \frac{p^{t+1} - 1 - (t+1)(4t-j)}{p^{t+1} - 1}.$$

Então, assintoticamente, a taxa desses códigos quânticos *CSS* tende para o valor 1.

Observação 3.2.7 *Note que o método de construção adotado no Teorema 3.2.6 também é válido quando for considerado $q = p^n$ ao invés de p (p primo) e F_{q^l}, onde $l \geq 2$, ao invés de F_q, pois tanto as propriedades das classes laterais ciclotômicas quanto as propriedades dos polinômios minimais são as mesmas quando consideradas sobre F_q ou quando consideradas sobre F_p. Em outras palavras, sabemos que as propriedades, descritas a seguir, são válidas:*

1. *$x^{q^m} - x$ = produto de todos os polinômios mônicos, irredutíveis sobre F_q, cujo grau divide m, onde $q = p^n$, p primo;*
2. *$M^{(s)}(x) = \prod_{i \in C_s} (x - \alpha^i)$, onde $M^{(i)}$ são todos os polinômios minimais e i percorre os representantes das classes laterais módulo $n = q^m - 1$.*

Observação 3.2.8 *Assim como no caso binário, é possível construir códigos cíclicos de comprimento $n = p^l - 1$, onde $l < t + 1$, que também corrigem t erros:*

Seja C_1 o código (clássico) BCH *gerado pelo polinômio*

$$g_1(x) = M^{(1)} M^{(2)} M^{(3)} \cdots M^{(2t)},$$

$C_2{}^{\perp}$ o código (clássico) cíclico gerado pelo produto dos $2t$ polinômios minimais

$$\langle M^{(i_1)} M^{(i_2)} M^{(i_3)} \cdots M^{(i_{2t})} \rangle,$$

onde o conjunto de definição do código $C_2{}^{\perp}$ *possui uma seqüência de, pelo menos,* $2t$ *números naturais consecutivos e*

$$C_2 = \langle g_2(x) \rangle = \left\langle M^{(0)} M^{(1)} M^{(2)} M^{(3)} \cdots M^{(2t)} \cdot \prod_i M^{(i)} \right\rangle,$$

onde $M^{(i)}$ *são todos os polinômios minimais tais que*

$$i \notin \{i_1, i_2, i_3, \cdots, i_{2t-1}, i_{2t}\},$$

onde i *percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod* $p^{t+1} - 1$, *e*

Note que o Teorema 3.2.6 contém a restrição $t \geq 7$. Entretanto, assim como no caso binário, podemos mostrar, por verificação direta, que nos casos $t = 2, 3, 4, 5, 6$, o método de construção é similar ao método utilizado na construção generalizada. Para isso, utilizaremos a construção descrita na Observação 3.2.8.

Exemplo 3.2.5 *Considerando na Observação 3.2.7 o valor de* $q = 4$, *construímos um código quântico* CSS 4*-ário com parâmetros* $[[15, 9, 3]]_4$.

Para isso, considere C_1 *o código* BCH, *primitivo, sobre* F_4 *e* $C_2{}^{\perp}$ *o código cíclico sobre* F_4 *gerados, respectivamente, pelo produto dos polinômios minimais:*

$$C_1 = \langle g_1(x) \rangle = \langle M^{(0)} M^{(1)} \rangle$$

e

$$C_2{}^{\perp} = \langle M^{(5)} M^{(6)} \rangle.$$

O código quântico CSS *gerado por tal construção atinge a máxima distância mínima, como demonstrado em [26].*

Exemplo 3.2.6 *Considere ainda, na Observação 3.2.7,* $q = 4$. *Seja* C_1 *o código* BCH *sobre* F_4 *e* $C_2{}^{\perp}$ *o código cíclico sobre* F_4 *gerados, respectivamente, pelo produto dos polinômios minimais:*

$$C_1 = \langle g_1(x) \rangle = \langle M^{(0)} M^{(1)} M^{(2)} \rangle$$

e

$$C_2{}^{\perp} = \langle M^{(5)} M^{(6)} M^{(7)} \rangle.$$

Então, construímos um código CSS 4*-ário com parâmetros* $[[15, 5, 4]]_4$. *Este código quântico também atinge a máxima distância mínima, como demonstrado em [26].*

Exemplo 3.2.7 *Considere os códigos cíclicos C_1 e C_2, sobre o corpo F_7, com comprimento* 2400*, dados pelos produto de polinômios minimais:*

$$C_1 = \langle g_1(x) \rangle = \langle M^{(1)} M^{(2)} M^{(3)} M^{(4)} M^{(5)} \cdots M^{(46)} \rangle,$$

e seja C_2 gerado pelo produto de polinômios minimais

$$C_2 = \langle g_2(x) \rangle = \langle M^{(0)} M^{(1)} M^{(2)} M^{(3)} M^{(4)} M^{(5)} M^{(6)} M^{(8)} \cdots M^{(46)} M^{(47)} \cdots M^{(2057)} \rangle,$$

exceto pelos polinômios $\prod_i M^{(i)}$, onde

$$\begin{aligned} i \in C = \{&48, 97, 146, 195, 244, 293, 331, 332, 333, 334, \\ &335, 337, 342, 440, 489, 538, 587, 674, 675, 676, \\ &677, 678, 880, 929, 978, 1018, 1019, 1020, 1021, 1027, \\ &1223, 1272, 1321, 1362, 1363, 1364, 1370, 1615, 1664, \\ &1706, 1707, 1713, 2001, 2008, 2050, 2057\}, \end{aligned}$$

onde C pode ser escrito da forma $C = \{48 + 49j : j = 0, 1, \cdots, 41\}$.

Note que ${C_2}^{\perp}$ possui uma seqüência de pelo menos 46 números naturais consecutivos, a saber, os números 2317 *até o número* 2363 *como raízes. A dimensão deste código quântico é* $2400 - 274 = 2126$*. Evidentemente, $C_2 \subset C_1$. Além disso, tanto C_1 quanto ${C_2}^{\perp}$ corrigem* 23 *erros.*

Então, pelo Teorema 3.2.6 e pela Observação 3.2.8, o código $CSS(C_1, C_2)$ possui parâmetros $[[2400, 2126, d \geq 47]]_7$ e corrige erros em 23 *qudits.*

Observação 3.2.9 *É conveniente ressaltar que, no exemplo anterior, utilizamos as idéias contidas no Teorema 3.2.6 e também escolhemos classes laterais específicas relacionadas ao código ${C_2}^{\perp}$ para garantir a existência de pelo menos uma seqüência de 46 ou mais números naturais consecutivos.*

Exemplo 3.2.8 *Considere os códigos cíclicos C_1, C_2 e ${C_2}^{\perp}$ sobre o corpo F_3, com comprimento* 26*, dados pelos produto de polinômios minimais:*

$$C_1 = \langle g_1(x) \rangle = \langle M^{(0)} M^{(1)} M^{(2)} \rangle,$$

C_2 gerado pelo produto de polinômios minimais

$$C_2 = \langle g_2(x) \rangle = \langle M^{(0)} M^{(1)} M^{(2)} M^{(4)} M^{(7)} M^{(8)} M^{(17)} \rangle$$

e

$${C_2}^{\perp} = \langle g_2(x) \rangle = \langle M^{(5)} M^{(13)} M^{(14)} \rangle.$$

Como as classes laterais ciclotômicas $\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_5, \mathbb{C}_{14}$ *possuem três elementos e as classes laterais* $\mathbb{C}_0$ *e* $\mathbb{C}_{13}$ *possuem somente um elemento, segue que a dimensão do código quântico* $CSS(C_1, C_2)$ *é igual a* 12.

Então, pelo Teorema 3.2.6 e pela Observação 3.2.8, o código quântico $CSS(C_1, C_2)$ *possui parâmetros* $[[26, 12, d \geq 5]]_3$ *e corrige erros quânticos arbitrários em* 2 *qudits.*

Exemplo 3.2.9 *Sejam* C_1*,* C_2 *e* ${C_2}^{\perp}$ *códigos cíclicos sobre o corpo* F_5*, com comprimento* 124*, dados pelos produto de polinômios minimais:*

$$C_1 = \langle g_1(x) \rangle = \langle M^{(31)} M^{(32)} M^{(33)} M^{(34)} M^{(7)} \rangle,$$

C_2 *gerado pelo produto de todos os polinômios minimais, exceto os polinômios*

$$M^{(62)},\ M^{(63)},\ M^{(64)},\ M^{(13)}\ e\ M^{(38)},$$

e

$${C_2}^{\perp} = \langle g_2(x) \rangle = \langle M^{(62)} M^{(63)} M^{(64)} M^{(13)} M^{(38)} \rangle.$$

Construímos, então, o código $CSS(C_1, C_2)$ *com parâmetros* $[[124, 98, d \geq 7]]_5$.

3.2.3 Método de construção III - *CSS* q-ários com comprimento $n = q^2 - 1$

A principal contribuição desta subseção é o Teorema 3.2.10. Este afirma que podemos construir bons códigos quânticos, melhores do que a maioria dos códigos existentes na literatura. A idéia principal de tal construção é o fato de desenvolvermos um método diferenciado no qual não precisaremos utilizar os Lemas 3.2.6 e 3.2.7.

Esses dois lemas, assim como o Teorema 3.1.3 para o caso binário, limitam bastante o processo e construção. Em outras palavras, para grandes valores do número natural $n \geq 1$, onde q é uma potência de primo tal que $\text{mdc}(n, q) = 1$, o limitante superior para o número de classes laterais ciclotômicas distintas são baixos. Devido a esses fatos, desenvolveremos o método de construção três, denominado *Construção Especial*, que gera bons códigos quânticos. Demonstraremos inicialmente que existem bons códigos quânticos p-ários de comprimento $p^2 - 1$, onde p é um primo maior ou igual a 5, e depois generalizaremos naturalmente este teorema para o caso q-ário de comprimento $q^2 - 1$, onde q é uma potência de primo maior ou igual a 5.

Iniciaremos o método de construção acima referido, demonstrando o Lema 3.2.13.

Lema 3.2.13 *Seja p um primo, $p \geq 5$, e $n = p^2 - 1$. Considere as primeiras $2p-2$ classes laterais ciclotômicas dadas por*

$$\begin{aligned}
\mathbb{C}_0 &= \{0\},\\
\mathbb{C}_1 &= \{1, p\},\\
\mathbb{C}_2 &= \{2, 2p\},\\
\mathbb{C}_3 &= \{3, 3p\}, \cdots,\\
\mathbb{C}_{p-2} &= \{p-2, (p-2)p\},\\
\mathbb{C}_{p+1} &= \{p+1, p(p+1) = 1+p\},\\
\mathbb{C}_{p+2} &= \{p+2, p(p+2) = 1+2p\}, \cdots,\\
\mathbb{C}_{2p-1} &= \{2p-1, (2p-1)p = 1+(p-1)p\}.
\end{aligned}$$

Então, todas essas classes laterais ciclotômicas são distintas e possuem dois elementos, exceto as classes laterais $\mathbb{C}_0$ e $\mathbb{C}_{p+1}$, que possuem somente um elemento cada.

Demonstração: Primeiramente, iremos demonstrar que são verdadeiras as seguintes desigualdades: $p^2 - 1 > 1 + (p-1)p$ e $p^2 - 1 > (p-2)p$.

Caso 1: Como $p \geq 5$, segue que $2 - p \leq -3$. Então, temos que $p^2 > 2 - p + p^2$ e assim, é verdadeira a desigualdade $p^2 - 1 > 1 + (p-1)p$.

Caso 2: Como $(p-2)p = p^2 - 2p$ e $2p \geq 10$, concluímos que $p^2 - 1 > (p-2)p$.

Demonstraremos, agora, que todas essas classes laterais são distintas.

Caso 1: Suponha que $1 \leq l, k \leq p-1$, onde $1 + lp = kp$. Assim, deduzimos que $p \mid 1$, um absurdo, pois p é um número primo.

Caso 2: Similarmente, se $1 + lp = 1 + kp$, como $1 + lp = 1 + kp < p^2 - 1$, então segue que $l = k$.

Caso 3: Além disso, se $kp = lp$, como a desigualdade $kp = lp < p^2 - 1$ é verdadeira, deduzimos que $l = k$.

Caso 4: Se $p + j = kp$ onde $1 \leq k, j \leq p-1$, obtemos $p(k-1) = j$, e assim $p \mid j$, uma contradição, pois $j < p$.

Caso 5: Se $p+j = lp+1$ onde $1 \leq l, j \leq p-1$, como $1+lp < p^2-1$ então $p(l-1) = j-1$, e assim $p \mid j-1$, uma contradição, pois $j - 1 < p$.

Caso 6: É claro que as classes laterais $\mathbb{C}_0$ $\mathbb{C}_{p+1}$ são distintas entre si e distintas das outras classes laterais.

Provaremos, agora, que, com exceção das classes laterais $\mathbb{C}_0$ e $\mathbb{C}_{p+1}$, todas as outras classes laterais possuem exatamente dois elementos.

Caso 1: Se $l = lp$, como $l = lp < p^2 - 1$ então $p = 1$, o que é um absurdo, pois p é um número primo.

Caso 2: Além disso, suponha que $p+l = 1+lp$, onde $2 \leq l \leq p-1$ é um número inteiro. Então, segue que $l - 1 = lp - p$, e assim $l - 1 = p(l - 1)$. Como $p + l = 1 + lp < p^2 - 1$ e $l - 1 \neq 0$, deduzimos que $p = 1$, um absurdo.

Conseqüentemente, todas as classes laterais ciclotômicas, exceto as classes laterais $\mathbb{C}_0$ e $\mathbb{C}_{p+1}$, contém exatamente dois elementos.

Por verificação imediata concluímos que as classes laterais ciclotômicas $\mathbb{C}_0$ e $\mathbb{C}_{p+1}$ contém somente um elemento cada. Assim, segue o resultado. □

Com a ajuda do Lema 3.2.13, provaremos o Teorema 3.2.10.

Teorema 3.2.10 *Seja p um número primo, $p \geq 5$ e $n = p^2 - 1$. Então, existem códigos quânticos* CSS *com parâmetros $[[p^2 - 1, p^2 - 4p + 5, d \geq p]]_p$. Além disso, os códigos cíclicos envolvidos em tais construções são gerados pelos polinômios*

$$C_1 = \langle M^{(0)} M^{(1)} M^{(2)} M^{(3)} \cdots M^{(p-2)} \rangle,$$

$$C_2{}^{\perp} = \langle M^{(p+1)} M^{(p+2)} \cdots M^{(2p-1)} \rangle$$

e

$$C_2 = \langle M^{(0)} M^{(1)} M^{(2)} M^{(3)} \cdots M^{(p-2)} \cdot \prod_i M^{(i)} \rangle,$$

onde $M^{(i)}$ são todos os polinômios minimais tais que

$$i \notin \{p + 1, p + 2, \cdots, 2p - 1\},$$

e i percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod p^2-1.

Note que o código C_1 é um código *BCH*.

Demonstração:

Cada um dos conjuntos de definição dos códigos C_1 e $C_2{}^{\perp}$ possui $p - 1$ classes laterais ciclotômicas distintas. Além disso, pelo Lema 3.2.13, todas tais classes, exceto as classes laterais $\mathbb{C}_0$ (de C_1) e $\mathbb{C}_{p+1}$ (de $C_2{}^{\perp}$), possuem dois elementos.

A equação (3.1) significa que o grau do polinômio minimal $M^{(i)}(x)$ é igual à cardinalidade da respectiva classe lateral C_s, e assim, o grau do polinômio gerador de um código cíclico é igual à cardinalidade de seu conjunto de definição.

Como C_1 é um código cíclico, sua dimensão, k_1, é dada por $k_1 = n - \partial(g_1(x))$, onde $n = p^2 - 1$ é o comprimento da palavra-código. Ainda, pela equação (3.1), $\partial(g_1(x))$ é igual à cardinalidade do conjunto de definição do código C_1. Além disso, pelo Lema 3.2.13, o conjunto de definição do código C_1 tem $2(p-2)+1 = 2p-3$ elementos, e assim

$$k_1 = p^2 - 1 - 2p + 3 = p^2 - 2p + 2.$$

Similarmente, a dimensão do código cíclico C_2, a saber k_2, é igual a

$$k_2 = p^2 - 1 - {k_2}^{\perp} = p^2 - 1 - (p^2 - 1 - 2p + 3) = 2p - 3,$$

onde ${k_2}^{\perp}$ é a dimensão do código ${C_2}^{\perp}$.

Então

$$k_1 - k_2 = p^2 - 2p + 2 - 2p + 3 = p^2 - 4p + 5,$$

e assim, a dimensão do código quântico $CSS(C_1, C_2)$ é igual a $p^2 - 4p + 5$.

Por construção, existem duas seqüências de $p-1$ números inteiros positivos consecutivos, onde uma pertence ao conjunto de definição do código C_1 e a outra está contida no conjunto de definição do código ${C_2}^{\perp}$. Assim, C_1 e ${C_2}^{\perp}$ têm distância mínima pelo menos p. Além disso, por construção, é válida a inclusão $C_2 \subsetneq C_1$.

Conseqüentemente, são geradas novas famílias de códigos quânticos *CSS* com parâmetros

$$[[p^2 - 1, p^2 - 4p + 5, d \geq p]]_p.$$

□

Corolário 3.2.1 *Pelo mesmo método de construção apresentado no Teorema 3.2.10, podemos gerar bons códigos* CSS *com parâmetros* $[[p^2 - 1, p^2 - 4c + 5, d \geq c]]_p$*, onde* $c < p$*,* p *primo. Os códigos cíclicos clássicos considerados em tais construções são gerados pelos polinômios*

$$C_1 = \langle M^{(0)} M^{(1)} M^{(2)} M^{(3)} \cdots M^{(c-2)} \rangle,$$

$$C_2{}^{\perp} = \langle M^{(p+1)} M^{(p+2)} \cdots M^{(p+(c-1))} \rangle$$

e

$$C_2 = \langle M^{(0)} M^{(1)} M^{(2)} M^{(3)} \cdots M^{(c-2)} \cdot \prod_i M^{(i)} \rangle,$$

onde $M^{(i)}$ *são todos os polinômios minimais tais que*

$$i \notin \{p+1, p+2, \cdots, p+(c-1)\},$$

e i *percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod* $p^2 - 1$.

Demonstração: Da mesma forma como foi feito na demonstração do teorema anterior, existem $2c-2$ classes laterais ciclotômicas distintas, dos códigos C_1 e ${C_2}^{\perp}$. Todas estas contém dois elementos cada, exceto as classes $\mathbb{C}_0$ e $\mathbb{C}_{p+1}$, que contém somente um elemento cada.

Como C_1 é um código cíclico sua dimensão, k_1, é dada por $k_1 = n - \partial(g_1(x))$, onde $n = p^2 - 1$ é o comprimento da palavra-código. Ainda, pela equação (3.1), $\partial(g_1(x))$ é igual à cardinalidade do conjunto de definição do código C_1. Além disso, pelo Lema 3.2.13, o conjunto de definição do código C_1 tem $2(c-2)+1 = 2c-3$ elementos, e assim

$$k_1 = p^2 - 1 - 2c + 3 = p^2 - 2c + 2.$$

Similarmente, a dimensão do código cíclico C_2, a saber k_2, é igual a

$$k_2 = p^2 - 1 - {k_2}^{\perp} = p^2 - 1 - (p^2 - 1 - 2c + 3) = 2c - 3,$$

onde ${k_2}^{\perp}$ é a dimensão do código ${C_2}^{\perp}$.

Então

$$k_1 - k_2 = p^2 - 2c + 2 - 2c + 3 = p^2 - 4c + 5,$$

e assim, a dimensão do código quântico $CSS(C_1, C_2)$ é igual a $p^2 - 4c + 5$.

Por construção, observamos que existem duas seqüências de $c-1$ elementos consecutivos, contidas nos conjuntos de definição dos códigos C_1 e ${C_2}^{\perp}$. Assim, os códigos C_1 e ${C_2}^{\perp}$ corrigem erros em, pelo menos, c qudits. Além disso, ainda por construção, segue que $C_2 \subsetneq C_1$.

Portanto, o método de construção gera outras famílias de bons códigos quânticos com parâmetros

$$[[p^2 - 1, p^2 - 4c + 5, d \geq c]]_p.$$

□

Aplicando o mesmo método de construção descrito no Teorema 3.2.10 ao corpo F_{q^2}, onde q é um potência de primo, generalizamos naturalmente o Teorema 3.2.10:

Teorema 3.2.11 *Seja q uma potência de primo, $q \geq 5$, e $n = q^2 - 1$. Então, existem códigos quânticos* CSS *com parâmetros $[[q^2 - 1, q^2 - 4q + 5, d \geq q]]_q$. Além disso, os códigos cíclicos envolvidos em tais construções são gerados pelos polinômios*

$$C_1 = \langle M^{(0)} M^{(1)} M^{(2)} M^{(3)} \cdots M^{(q-2)} \rangle,$$

$$ {C_2}^{\perp} = \langle M^{(q+1)} M^{(q+2)} \cdots M^{(2q-1)} \rangle$$

e

$$C_2 = \langle M^{(0)} M^{(1)} M^{(2)} M^{(3)} \cdots M^{(q-2)} \cdot \prod_i M^{(i)} \rangle,$$

onde $M^{(i)}$ *são todos os polinômios minimais tais que*

$$i \notin \{q+1, q+2, \cdots, 2q-1\},$$

e i *percorre o conjunto dos representantes de todas as classes laterais ciclotômicas mod* q^2-1.

Demonstração: Análoga à demonstração do Teorema 3.2.10. □

Para calcular a taxa das novas famílias de códigos *CSS* geradas a partir do Método de Construção III, seja $f(p) : \mathbb{Z}^+ \longrightarrow \mathbb{R}$ a aplicação dada por

$$f(q) = \frac{q^2 - 4q + 5}{q^2 - 1},$$

onde $\mathbb{Z}^+$ e $\mathbb{R}$ são o conjunto dos números inteiros positivos e o conjunto dos números reais, respectivamente, $n = q^2 - 1$ é o comprimento da palavra-código, $k = q^2 - 4q + 5$ é a dimensão e d é a distância mínima do código.

Calculando o limite de $f(q)$ quando q tende ao infinito deduzimos que

$$\lim_{q \longrightarrow \infty} f(q) = 1.$$

Assim, para grandes valores para variável q, a taxa das novas famílias de códigos *CSS* tende ao valor 1.

3.2.4 Método de construção IV - *CSS* ternários

As principais contribuições dessa subseção são o Lema 3.2.18 e o Teorema 3.2.12. O Teorema 3.2.12 afirma que é possível a construção de famílias de bons códigos quânticos *CSS* ternários. Em outras palavras, é gerada uma família de códigos *CSS* ternários com parâmetros $[[3^m - 1, k \geq 3^m - 8m - 3, d \geq 8]]_3$, onde m é um inteiro positivo $m \geq 3$. Além disso, são propostas construções de novas famílias de códigos *CSS* com parâmetros $[[n, k \geq n - 2m - 2, d \geq 3]]_3$ $[[n, k \geq n - 4m, d \geq 4]]_3$, $[[n, k \geq n - 4m - 2, d \geq 5]]_3$ e $[[n, k \geq n - 6m - 2, d \geq 6]]_3$, respectivamente, onde $n = 3^m - 1$.

Iniciaremos a subseção demonstrando vários lemas que são essenciais na demonstração do Teorema 3.2.12.

Lema 3.2.14 *Seja* $n = 3^m - 1$, *onde* m *é um inteiro positivo* $m \geq 3$. *Então a classe lateral* $\mathbb{C}_{(\frac{3^m-1}{2})}$ *possui somente o elemento* $\frac{3^m-1}{2}$.

Demonstração: Sabemos que os elementos da classe lateral $\mathbb{C}_{\left(\frac{3^m-1}{2}\right)}$ são descritos por $\frac{3^m-1}{2}.3^t$, onde $t \in \{1, 2, \cdots, m-1\}$.

Calculando a expressão $\left(\frac{3^m-1}{2}\right).3^t$ obtemos

$$\left(\frac{3^m-1}{2}\right)3^t = \frac{3^m-1}{2} + (3^t-1)\left(\frac{3^m-1}{2}\right).$$

Como $3^t - 1$ é par, segue que

$$(3^t-1)\left(\frac{3^m-1}{2}\right) = l(3^m-1),$$

onde l é um inteiro, e assim

$$\left(\frac{3^m-1}{2}\right)3^t \equiv \frac{3^m-1}{2} \ mod\ (3^m-1),$$

donde segue o lema. □

A seguir, demonstraremos os Lemas 3.2.15, 3.2.16 e 3.2.17.

Lema 3.2.15 *Considere $n = 3^m - 1$, onde m é um inteiro positivo $m \geq 3$. Então, a classe lateral $\mathbb{C}_{(\frac{3^m-1}{2}-1)}$ contém o elemento $\frac{3^m-1}{2} - 3$.*

Demonstração: É suficiente demonstrar que

$$(\frac{3^m-1}{2} - 1).3 \equiv \frac{3^m-1}{2} - 3 \ mod\ (3^m-1).$$

De fato,

$$\left(\frac{3^m-1}{2} - 1\right).3 \equiv$$
$$\equiv \frac{3^m-1}{2} - 1 + 3^m - 1 - 2 \equiv$$
$$\equiv \frac{3^m-1}{2} - 3 \ mod\ (3^m-1),$$

donde

$$\left(\frac{3^m-1}{2} - 1\right).3 \equiv \frac{3^m-1}{2} - 3 \ mod\ (3^m-1).$$

□

Lema 3.2.16 *Seja $n = 3^m - 1$, onde m é um inteiro positivo $m \geq 3$. Então, a classe lateral $\mathbb{C}_{(\frac{3^m-1}{2}+1)}$ contém o elemento $\frac{3^m-1}{2} + 3$.*

Demonstração: Análoga à demonstração anterior □

Lema 3.2.17 *Se $n = 3^m - 1$, onde m é um inteiro positivo $m \geq 3$, então as classes laterais $\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_4, \mathbb{C}_5$ são distintas e cada uma destas contém m elementos.*

Demonstração: Aplicando os Lemas 3.2.7 e 3.2.6, como $5 \leq 3^{\lceil m/2 \rceil}$, o resultado segue diretamente. □

O Lema 3.2.18, dado a seguir, é um resultado importante para a demonstração do Teorema 3.2.12.

Lema 3.2.18 *Seja $n = 3^m - 1$, $m \geq 4$. Então, as classes laterais $\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_4, \mathbb{C}_5$ são distintas das classes laterais $\mathbb{C}_{(\frac{3^m-1}{2})}, \mathbb{C}_{(\frac{3^m-1}{2}+1)}, \mathbb{C}_{(\frac{3^m-1}{2}+2)}, \mathbb{C}_{(\frac{3^m-1}{2}-1)}, \mathbb{C}_{(\frac{3^m-1}{2}-2)}$.*

Demonstração: Adotaremos, para essa demonstração, l como sendo um inteiro positivo tal que $1 \leq l \leq m-1$, e que a operação considerada é a operação módulo $3^m - 1$.

É claro que a classe lateral $\mathbb{C}_{(\frac{3^m-1}{2})}$ é distinta das classes $\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_4, \mathbb{C}_5$.

Caso 1: Provaremos que a classe lateral $\mathbb{C}_{(\frac{3^m-1}{2}-1)}$ é distinta das classes laterais mencionadas anteriormente.

De fato, se $(\frac{3^m-1}{2} - 1).3^l \equiv 1$, temos que

$$(3^m - 1).3^l - 2.3^l \equiv 2 \Longrightarrow 2.3^l \equiv -2.$$

Como $2.3^l < 3^m - 1$ e $2.3^l + 2 < 3^m - 1$, é suficiente demonstrar que a equação $2.3^l = -2$ não possui solução. Como a equação $2.3^l = -2$ não é satisfeita, segue que a classe lateral $\mathbb{C}_{(\frac{3^m-1}{2}-1)}$ é distinta da classe $\mathbb{C}_1$.

Similarmente, se $(\frac{3^m-1}{2} - 1).3^l \equiv 2$, sabemos que

$$(3^m - 1).3^l - 2.3^l \equiv 4 \Longrightarrow 2.3^l \equiv -4.$$

Como $2.3^l < 3^m - 1$ e $2.3^l + 4 < 3^m - 1$, precisamos apenas demonstrar que a equação $2.3^l = -4$ não possui solução, mas isso é óbvio. Assim, a classe lateral $\mathbb{C}_{(\frac{3^m-1}{2}-1)}$ é diferente da classe $\mathbb{C}_2$.

Para provar que a classe $\mathbb{C}_{(\frac{3^m-1}{2}-1)}$ é diferente da classe $\mathbb{C}_4$, assuma $(\frac{3^m-1}{2} - 1).3^l \equiv 4$. Então,

$$(3^m - 1).3^l - 2.3^l \equiv 8 \Longrightarrow 2.3^l \equiv -8.$$

Como a equação $2.3^l = -8$ não é verdadeira, o resultado está demonstrado. Analogamente, podemos demonstrar que a classe $\mathbb{C}_{(\frac{3^m-1}{2}-1)}$ é diferente da classe $\mathbb{C}_5$.

Caso 2: A classe lateral $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ é distinta das classes laterais mencionadas anteriormente.

Se $(\frac{3^m-1}{2}+2).3^l \equiv 1$ então

$$(3^m-1).3^l + 4.3^l \equiv 2 \Longrightarrow 4.3^l \equiv 2.$$

Se $1 \leq l \leq m-2$, as desigualdades $4.3^l < 3^m - 1$ e $4.3^l - 2 < 3^m - 1$ são verdadeiras, e assim, é suficiente demonstrar que a equação $4.3^l = 2$ não é válida. Como a equação $4.3^l = 2$ não possui solução, as classes $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ e $\mathbb{C}_1$ são distintas.

Por outro lado, se $l = m-1$, segue que

$$\left(\frac{3^m-1}{2}+2\right).3^{m-1} \equiv 1 \Longrightarrow$$
$$\Longrightarrow (3^m-1).3^{m-1} + 4.3^{m-1} \equiv 2.$$

Sabemos que $(3^m-1).3^{m-1} + 4.3^{m-1} \equiv 4.3^{m-1}$. Continuando com as manipulações algébricas resulta em

$$4.3^{m-1} = (3^m-1) + 3^{m-1} + 1 \equiv 3^{m-1} + 1.$$

Como $3^{m-1} + 1 < 3^m - 1$ e como a equação $3^{m-1} + 1 = 2$ possui somente a solução $m = 1$, concluímos que as classes $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ e $\mathbb{C}_1$ são diferentes.

Considerando $(\frac{3^m-1}{2}+2).3^l \equiv 2$, deduzimos que

$$(3^m-1).3^l + 4.3^l \equiv 4 \Longrightarrow 4.3^l \equiv 4.$$

Se $1 \leq l \leq m-2$, então $4.3^l - 4 < 3^m - 1$. Como $4.3^l = 4$ possui somente a solução $l = 0$ (e assim $m = 1$), deduzimos que as classes $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ e $\mathbb{C}_2$ são distintas.

Considere $l = m-1$. Sabemos que

$$4.3^{m-1} = (3^m-1) + 3^{m-1} + 1 \equiv 3^{m-1} + 1.$$

Como $3^{m-1} + 1 < 3^m - 1$ e como a equação $3^{m-1} + 1 = 4$ possui somente a solução $m = 2$, as classes laterais $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ e $\mathbb{C}_2$ são distintas.

Se $(\frac{3^m-1}{2}+2).3^l \equiv 4$, obtemos

$$(3^m-1).3^l + 4.3^l \equiv 8 \Longrightarrow 4.3^l \equiv 8.$$

Se $1 \leq l \leq m-2$, então $4.3^l - 8 < 3^m - 1$, e assim, é suficiente verificar se a equação $4.3^l = 8$ é válida. Mas como tal equação não possui solução, as classes laterais $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ e $\mathbb{C}_4$ são distintas.

Se $l = m-1$, como $3^{m-1}+1 < 3^m - 1$ e como a equação $3^{m-1}+1 = 8$ não possui solução, deduzimos que $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ e $\mathbb{C}_4$ são distintas.

Em relação ao caso $(\frac{3^m-1}{2}+2).3^l \equiv 5$, segue que

$$(3^m-1).3^l + 4.3^l \equiv 10 \Longrightarrow 4.3^l \equiv 10.$$

Se $1 \leq l \leq m-2$, então $4.3^l - 10 < 3^m - 1$ e assim, a equação $4.3^l = 10$ não é satisfeita. Então, $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ e $\mathbb{C}_5$ são diferentes.

Se $l = m-1$, como $3^{m-1}+1 < 3^m - 1$, a classe lateral $\mathbb{C}_{(\frac{3^m-1}{2}+2)}$ é distinta da classe lateral $\mathbb{C}_5$.

Para demonstrar que as classes laterais $\mathbb{C}_{(\frac{3^m-1}{2}+1)}$ e $\mathbb{C}_{(\frac{3^m-1}{2}-2)}$ são distintas das classes laterais $\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_4, \mathbb{C}_5$, é suficiente proceder de forma análoga aos Casos 1 e 2. □

Teorema 3.2.12 *Seja $n = 3^m - 1$, onde $m \geq 3$. então, existem códigos quânticos* CSS *com parâmetros* $[[n, k \geq n - 8m - 2, d \geq 8]]_3$.

Demonstração: Seja C_1 o código clássico *BCH* gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(4)}M^{(5)},$$

e seja ${C_2}^{\perp}$ o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(a-2)}M^{(a-1)}M^{(a)}M^{(a+1)}M^{(a+2)},$$

onde $a = \frac{3^m-1}{2}$.

Ainda, considere C_2 como sendo o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(4)}M^{(5)}M^{(7)} \cdot \prod_i M^{(i)},$$

onde $M^{(i)}$ são os polinômios minimais tais que

$$i \notin \{a-2,\ a-1,\ a,\ a+1,\ a+2\}$$

e i percorre os representantes das classes laterais mod $3^m - 1$. Então, $C_2 \subset C_1$. Aplicando os Lemas 3.2.14 ao 3.2.18 concluímos que cada um dos códigos C_1 e ${C_2}^{\perp}$ possuem distância mínima $d \geq 8$.

Procedendo como na demonstração do Teorema 3.2.6 e utilizando a construção *CSS* são gerados códigos quânticos com parâmetros $[[n, k \geq n - 8m - 2, d \geq 8]]_3$, como desejado. □

Calculando as taxas dos códigos construídos no Teorema 3.2.12 temos que

$$f(m) = \frac{3^m - 8m - 3}{3^m - 1},$$

$$\lim_{m \longrightarrow \infty} f(m) = 1.$$

Assim, como foi demonstrado nos métodos de construção anteriores, quando m tende ao infinito, a taxa de tais códigos quânticos também tende para 1.

Exemplo 3.2.10 *Seja C_1 o código* BCH *com comprimento* 80 *sobre F_3, e ${C_2}^{\perp}$ o código cíclico sobre F_3, com comprimento* 80*, dados, respectivamente, pelo produto dos polinômios minimais*

$$C_1 = \langle g_1(x) \rangle = \langle M^{(0)} M^{(1)} M^{(2)} M^{(4)} M^{(5)} \rangle,$$

e

$${C_2}^{\perp} = \langle g_2(x) \rangle = \langle M^{(22)} M^{(13)} M^{(14)} M^{(40)} M^{(41)} \rangle.$$

Então, o código $CSS(C_1, C_2)$ possui parâmetros $[[80, 46, d \geq 8]]_3$.

Em seguida, serão demonstrados resultados diretos da aplicação do Teorema 3.2.12. Mais precisamente, em tais corolários são construídos novos códigos *CSS* com distâncias mínimas iguais a $3, 4, 5$ e 6, respectivamente.

Corolário 3.2.2 *Seja $n = 3^m - 1$, onde m é um inteiro positivo $m \geq 3$. Então, existem códigos* CSS *com parâmetros $[[n, k \geq n - 2m - 2, d \geq 3]]_3$ e $[[n, k \geq n - 4m, d \geq 4]]_3$.*

Demonstração: Sem perda de generalidade, demonstraremos somente a construção dos novos códigos quânticos com parâmetros $[[n, k \geq n - 4m, d \geq 4]]_3$, pois a demonstração da construção dos códigos com parâmetros $[[n, k \geq n - 2m - 2, d \geq 3]]_3$ é análoga à primeira.

É suficiente considerar C_1 como sendo o código clássico *BCH* gerado pelo produto dos polinômios minimais

$$M^{(1)} M^{(2)},$$

${C_2}^{\perp}$ o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(a-2)} M^{(a-1)},$$

onde $a = \frac{3^m-1}{2}$ e C_2 o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(4)} \cdot \prod_i M^{(i)},$$

onde $M^{(i)}$ são os polinômios minimais tais que $i \notin \{a-2,\ a-1\}$, e i percorre os representantes das classes laterais módulo $3^m - 1$.

Posteriormente, basta proceder como na demonstração do Teorema 3.2.6, aplicar os Lemas 3.2.14–3.2.18 e utilizar a construção *CSS*. □

Corolário 3.2.3 *Seja $n = 3^m - 1$, onde m é um inteiro positivo $m \geq 3$. Então, existem códigos quânticos* CSS *com parâmetros* $[[n, k \geq n - 4m - 2, d \geq 5]]_3$.

Demonstração: Seja C_1 o código *BCH* gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)},$$

$C_2{}^{\perp}$ o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(a-2)}M^{(a-1)}M^{(a)},$$

onde $a = \frac{3^m-1}{2}$ e C_2 o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(4)} \cdot \prod_i M^{(i)},$$

onde $M^{(i)}$ são os polinômios minimais tais que

$$i \notin \{a-2,\ a-1,\ a\}$$

e i percorre os representantes das classes laterais módulo $3^m - 1$. Assim, como já foi demonstrado anteriormente, segue o resultado. □

Exemplo 3.2.11 *O código $CSS(C_1, C_2)$ com parâmetros $[[80, 62, d \geq 5]]_3$ é um exemplo de código gerado pela aplicação do Corolário 3.2.3.*

Corolário 3.2.4 *Seja $n = 3^m - 1$, onde m é um inteiro positivo tal que $m \geq 3$. Então, existem códigos quânticos* CSS *com parâmetros* $[[n, k \geq n - 6m - 2, d \geq 6]]_3$.

Demonstração: Seja C_1 gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(4)},$$

${C_2}^{\perp}$ gerado pelo produto dos polinômios minimais

$$M^{(a-2)}M^{(a-1)}M^{(a)}M^{(a+1)},$$

onde $a = \frac{3^m-1}{2}$ e C_2 o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(4)} \cdot \prod_i M^{(i)},$$

onde $M^{(i)}$ são os polinômios minimais tais que

$$i \notin \{a-2,\ a-1,\ a,\ a+1\}$$

e i percorre os representantes das classes laterais módulo $3^m - 1$. Similarmente como já foi demonstrado anteriormente, o resultado é verdadeiro. □

Exemplo 3.2.12 *Pelo Corolário 3.2.4 podemos construir códigos quânticos* CSS *com parâmetros* $[[80, 54, d \geq 6]]_3$ *e* $[[242, 210, d \geq 6]]_3$*, por exemplo.*

3.2.5 Método de construção V - *CSS* p-ários com comprimento $n = p^3 - 1$

O Teorema 3.2.13 é a principal contribuição dessa subseção; este produz uma nova família de bons códigos *CSS* p-ários, com parâmetros $[[p^3 - 1, p^3 - 21, d \geq 5]]_p$.

Teorema 3.2.13 *Seja* $p \geq 5$ *um primo e* $n = p^3 - 1$*. Então, existem códigos quânticos* CSS *com parâmetros* $[[p^3 - 1, p^3 - 21, d \geq 5]]_p$.

Demonstração: Começaremos a demonstração provando que a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2})}$ possui somente o elemento $\left(\frac{p^3-1}{2}\right)$.

Pelo Teorema 3.1.1, sabemos que cada classe lateral possui 1 ou 3. elementos. Além disso,

$$\left(\frac{p^3-1}{2}\right)p = \left(\frac{p^3-1}{2}\right) + (p-1)\left(\frac{p^3-1}{2}\right).$$

Como p é ímpar, $p-1$ é par, donde

$$\left(\frac{p^3-1}{2}\right) + (p-1)\left(\frac{p^3-1}{2}\right) = \left(\frac{p^3-1}{2}\right) + l(p^3-1) \equiv \left(\frac{p^3-1}{2}\right),$$

onde l é um inteiro.

Analogamente,

$$\left(\frac{p^3-1}{2}\right)p^2 = \left(\frac{p^3-1}{2}\right) + (p^2-1)\left(\frac{p^3-1}{2}\right).$$

Como p é ímpar, p^2 é ímpar, e assim p^2-1 é par, donde

$$\left(\frac{p^3-1}{2}\right) + (p^2-1)\left(\frac{p^3-1}{2}\right) = \left(\frac{p^3-1}{2}\right) + r(p^3-1) \equiv \left(\frac{p^3-1}{2}\right),$$

onde r é um inteiro, concluindo a demonstração.

Em seguida, demonstramos que as classes laterais $\mathbb{C}_{(\frac{p^3-1}{2})}$, $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$, $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$ e $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$ são distintas das classes laterais $\mathbb{C}_1$, $\mathbb{C}_2$ e $\mathbb{C}_3$.

Consideraremos, no decorrer dessa demonstração, que $i = 1, 2$ e que o símbolo $\equiv$ denota a operação módulo p^3-1.

Claramente a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2})}$ é distinta de tais classes.

Caso 1: Considere as classes laterais $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$. Se $(\frac{p^3-1}{2}+1)p^i \equiv 1$, então

$$(p^3-1)p^i + 2p^i \equiv 2 \Longrightarrow (p^3-1)p^i + 2p^i \equiv 2p^i \equiv 2.$$

Como $2p^i - 2 < p^3-1$ e como a equação $2p^i = 2$ é válida somente quando $i = 0$, concluímos que a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$ é diferente da classe lateral $\mathbb{C}_1$.

Se $(\frac{p^3-1}{2}+1)p^i \equiv 2$, temos que

$$(p^3-1)p^i + 2p^i \equiv 4 \Longrightarrow (p^3-1)p^i + 2p^i \equiv 2p^i \equiv 4.$$

Como $2p^i - 4 < p^3-1$ e como a equação $2p^i = 4$ não possui solução, a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$ é diferente da classe lateral $\mathbb{C}_2$.

Se $(\frac{p^3-1}{2}+1)p^i \equiv 3$, obtemos

$$(p^3-1)p^i + 2p^i \equiv 6 \Longrightarrow (p^3-1)p^i + 2p^i \equiv 2p^i \equiv 6.$$

Como $2p^i - 6 < p^3-1$ e como a equação $2p^i = 6$ não possui solução, a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$ é diferente da classe lateral $\mathbb{C}_3$.

Caso 2: Considere a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$. Se $(\frac{p^3-1}{2}+2)p^i \equiv 1$, então

$$(p^3-1)p^i + 4p^i \equiv 2 \Longrightarrow (p^3-1)p^i + 4p^i \equiv 4p^i \equiv 2.$$

Como $4p^i - 2 < p^3-1$ e como a equação $4p^i = 2$ não é satisfeita, as classes laterais $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$ e $\mathbb{C}_1$ são distintas.

Se $(\frac{p^3-1}{2}+2)p^i \equiv 2$, deduzimos que

$$(p^3-1)p^i + 4p^i \equiv 4 \Longrightarrow (p^3-1)p^i + 4p^i \equiv 4p^i \equiv 4.$$

Como a equação $4p^i = 4$ possui somente a solução $i = 0$, as classes laterais $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$ e $\mathbb{C}_2$ são distintas.

Se $(\frac{p^3-1}{2} + 2)p^i \equiv 3$, sabemos que

$$(p^3 - 1)p^i + 4p^i \equiv 6 \Longrightarrow (p^3 - 1)p^i + 4p^i \equiv 4p^i \equiv 6.$$

Como $4p^i = 6$ não possui solução, as classes laterais $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$ e $\mathbb{C}_6$ são distintas.

Caso 3: Considere a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$. Se $(\frac{p^3-1}{2} + 3)p^i \equiv 1$, temos que

$$(p^3 - 1)p^i + 6p^i \equiv 2 \Longrightarrow (p^3 - 1)p^i + 6p^i \equiv 6p^i \equiv 2.$$

Se $p \geq 7$, $6p^i - 2 < p^3 - 1$ e então, a demonstração é idêntica à anterior. Se $p = 5$, $6p^i \not\equiv 2$ e assim, a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$ é distinta da classe lateral $\mathbb{C}_1$.

Se $(\frac{p^3-1}{2} + 3)p^i \equiv 2$, segue que

$$(p^3 - 1)p^i + 6p^i \equiv 4 \Longrightarrow (p^3 - 1)p^i + 6p^i \equiv 6p^i \equiv 4.$$

Se $p \geq 7$ então $6p^i - 4 < p^3 - 1$, e assim a demonstração é idêntica à anterior. Se $p = 5$ sabemos que $6p^i \not\equiv 4$, e assim, a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$ é diferente da classe $\mathbb{C}_2$.

Se $(\frac{p^3-1}{2} + 3)p^i \equiv 3$, deduzimos que

$$(p^3 - 1)p^i + 6p^i \equiv 6 \Longrightarrow (p^3 - 1)p^i + 6p^i \equiv 6p^i \equiv 6.$$

Se $p \geq 7$ então $6p^i - 6 < p^3 - 1$, e assim, a demonstração é idêntica à anterior. Se $p = 5$ então $6p^i \not\equiv 6$, e assim, a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$ é distinta da classe $\mathbb{C}_3$.

Aplicando os Lemas 3.2.7 e 3.2.6, como $4 \leq p^{\lceil 3/2 \rceil}$ sabemos que as classes $\mathbb{C}_1$, $\mathbb{C}_2$ e $\mathbb{C}_3$ são distintas e possuem 3 elementos.

Demonstraremos, agora, que cada uma das classes laterais $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$, $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$ e $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$ são distintas.

Caso 4: Se

$$\left(\frac{p^3 - 1}{2} + 1\right) \equiv \left(\frac{p^3 - 1}{2} + 2\right) p^i,$$

concluímos que

$$p^3 - 1 + 2 \equiv (p^3 - 1)p^i + 4p^i \Longrightarrow 4p^i \equiv 2.$$

Como a inequação $4p^i - 2 < p^3 - 1$ e a equação $4p^i = 2$ não são satisfeitas, a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$ é distinta da classe $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$.

Caso 5: Para demonstrar que a classe $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$ é diferente da classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$, considere a seguinte equação:

$$\left(\frac{p^3-1}{2}+1\right) \equiv \left(\frac{p^3-1}{2}+3\right) p^i.$$

Assim, temos que

$$p^3-1+2 \equiv (p^3-1)p^i + 6p^i \Longrightarrow 6p^i \equiv 2.$$

Como a equivalência $6p^i \equiv 2$ não é satisfeita, o resultado segue.

Caso 6: Suponha que

$$\left(\frac{p^3-1}{2}+2\right) \equiv \left(\frac{p^3-1}{2}+3\right) p^i.$$

Então,

$$p^3-1+4 \equiv (p^3-1)p^i + 6p^i \Longrightarrow 6p^i \equiv 4.$$

Como a equivalência $6p^i \equiv 4$ não possui solução, a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$ é distinta da classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$.

Agora, provaremos que cada uma das classes laterais $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$, $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$ e $\mathbb{C}_{(\frac{p^3-1}{2}+3)}$ possui três elementos.

Caso 7: Mostraremos que a classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+1)}$ possui três elementos. Por simples manipulação algébrica temos que

$$\left(\frac{p^3-1}{2}+1\right) p = \frac{p^3+1}{2} + (p-1)\left(\frac{p^3-1}{2}\right) + p - 1.$$

Como $p-1$ é par, segue que

$$(p-1)\left(\frac{p^3-1}{2}\right) \equiv 0$$

e então

$$\left(\frac{p^3-1}{2}+1\right) p = \left(\frac{p^3-1}{2}+1\right) + p - 1.$$

Além disso,

$$\left(\frac{p^3-1}{2}+1\right) p^2 = \frac{p^3+1}{2} + (p^2-1)\left(\frac{p^3-1}{2}\right) + p(p-1).$$

Como p^2-1 é par,

$$(p^2-1)\left(\frac{p^3-1}{2}\right) \equiv 0,$$

e assim

$$\left(\frac{p^3-1}{2}+1\right)p^2 = \left(\frac{p^3-1}{2}+1\right) + p(p-1).$$

Caso 8: A classe lateral $\mathbb{C}_{(\frac{p^3-1}{2}+2)}$ possui três elementos. Considere

$$\left(\frac{p^3-1}{2}+2\right)p = \frac{p^3+3}{2} + (p-1)\left(\frac{p^3-1}{2}\right) + 2(p-1).$$

Similarmente ao Caso 7 temos que

$$\left(\frac{p^3-1}{2}+2\right)p = \left(\frac{p^3-1}{2}+2\right) + 2(p-1).$$

Analogamente,

$$\left(\frac{p^3-1}{2}+2\right)p^2 = \left(\frac{p^3-1}{2}+2\right) + 2p(p-1).$$

Caso 9: Como

$$\left(\frac{p^3-1}{2}+3\right)p = \frac{p^3+5}{2} + (p-1)\left(\frac{p^3-1}{2}\right) + 3(p-1),$$

então

$$\left(\frac{p^3-1}{2}+3\right)p^2 = \left(\frac{p^3-1}{2}+3\right) + 3(p-1).$$

Similarmente,

$$\left(\frac{p^3-1}{2}+3\right)p^2 = \left(\frac{p^3-1}{2}+3\right) + 3p(p-1).$$

Considere C_1 o código clássico *BCH* code gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(1)}M^{(3)},$$

${C_2}^{\perp}$ o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(b)}M^{(b+1)}M^{(b+2)}M^{(b+3)},$$

onde $b = \frac{p^3-1}{2}$. Além disso, seja C_2 o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(3)}M^{(4)} \cdot \prod_i M^{(i)},$$

onde $M^{(i)}$ são os polinômios minimais tais que

$$i \notin \{b,\ b+1,\ b+2,\ b+3\},$$

e i percorre os representantes das classes laterais ciclotômicas mod $p^3 - 1$.

Procedendo como na demonstração do Teorema 3.2.6 e utilizando a construção *CSS* segue o resultado. □

Exemplo 3.2.13 *Aplicando o Teorema 3.2.13, construímos códigos com parâmetros* $[[124, 104, d \geq 5]]_5$, $[[342, 322, d \geq 5]]_7$, $[[1330, 1310, d \geq 5]]_{11}$, *e assim por diante.*

Procedendo como no Teorema 3.2.13 obtemos códigos quânticos com distâncias mínimas 3 e 4:

Corolário 3.2.5 *Seja* $p \geq 5$ *um primo e* $n = p^3 - 1$. *Então, existem códigos quânticos* CSS *com parâmetros* $[[p^3 - 1, p^3 - 9, d \geq 3]]_p$ *e* $[[p^3 - 1, p^3 - 15, d \geq 4]]_p$, *respectivamente.*

Demonstração: Para a primeira construção, considere C_1 como sendo o código *BCH* gerado pelo produto de polinômios minimais

$$M^{(0)}M^{(1)},$$

${C_2}^{\perp}$ o código cíclico gerado pelo produto de polinômios minimais

$$M^{(b)}M^{(b+1)},$$

onde $b = \frac{p^3-1}{2}$, e C_2 o código cíclico gerado pelo produto de polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)} \cdot \prod_i M^{(i)},$$

onde $M^{(i)}$ são os polinômios minimais tais que

$$i \notin \{b,\ b+1\},$$

e i percorre os representantes das classes laterais mod (p^3-1).

Para a segunda construção, considere C_1 como sendo o código *BCH* gerado pelo produto de polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)},$$

${C_2}^{\perp}$ o código cíclico gerado pelo produto de polinômios minimais

$$M^{(b)}M^{(b+1)}M^{(b+2)},$$

onde $b=\frac{p^3-1}{2}$, e C_2 o código cíclico gerado pelo produto de polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(3)}\cdot\prod_i M^{(i)},$$

onde $M^{(i)}$ são os polinômios minimais tais que

$$i\notin\{b,\ b+1,\ b+2\}$$

e i percorre os representantes das classes laterais mod (p^3-1).

Procedendo como na demonstração do Teorema 3.2.6 e utilizando a construção *CSS* segue o resultado. □

Exemplo 3.2.14 *Aplicando o Corolário 3.2.5 geramos códigos quânticos com parâmetros* $[[124,116,d\geq 3]]_5$, $[[124,110,d\geq 4]]_5$, $[[342,334,d\geq 3]]_7$, $[[342,328,d\geq 4]]_7$, $[[1330,1322,d\geq 3]]_{11}$, $[[1330,1316,d\geq 4]]_{11}$ *e assim por diante.*

3.2.6 Método de construção VI - *CSS* não primitivos

Nesta subseção construímos códigos quânticos *CSS* a partir de códigos cíclicos (incluindo códigos *BCH* não primitivos). A principal contribuição é o Teorema 3.2.16. Este produz novas famílias de códigos *CSS*, como veremos em seguida.

Antes de continuarmos, é apropriado relembrar o conceito de *corpo de decomposição*. Para maiores detalhes referimos ao leitor [33].

É bem conhecido que o polinômio gerador de um código cíclico com comprimento n sobre F_q deve ser um fator de x^n-1. Suporemos sempre que n e q são relativamente primos, ou seja, $\mathrm{mdc}(n,q)=1$. Então, existe um menor inteiro m tal que $n\mid(q^m-1)$, denominado *ordem multiplicativa* de q *módulo* n. Assim, os zeros do polinômio x^n-1, denotados *raízes n-ésimas da unidade*, pertence ao corpo F_{q^m} e não pertence a nenhum corpo de menor cardinalidade.

Como x^n-1 possui zeros distintos, a saber, $\alpha_0, \alpha_1, \cdots, \alpha_{n-1} \in F_{q^m}$, então $x^n-1 = \prod_{i=0}^{n-1}(x-\alpha_i)$ e F_{q^m} é denominado *corpo de decomposição* de $x^n - 1$.

Por outro lado, é possível fatorar $x^n - 1$ sobre o corpo F_q considerando as classes laterais ciclotômicas módulo n sobre F_q:

$$\mathbb{C}_s = \{s, sq, sq^2, sq^3, \cdots, sq^{m_s-1}\},$$

onde m_s é o menor inteiro positivo tal que $q^{m_s}s \equiv s \ mod \ n$.

Baseados em tais conceitos estamos aptos a prosseguir com nosso trabalho.

Lema 3.2.19 *Se n é um inteiro positivo, então $n \mid [(n-1)^2 - 1]$ e $n \mid [(n+1)^2 - 1]$. Em particular se $q = p^m$ então $q \mid [(q-1)^2 - 1]$ e $q \mid [(q+1)^2 - 1]$.*

Demonstração: A verificação é imediata. □

Seguem os Teoremas 3.2.14 e 3.2.15, que são resultados importantes desta subseção:

Teorema 3.2.14 *Seja $n > q-1$ um inteiro tal que $n \mid [(q-1)^2 - 1]$, onde $q-1 = p^m \geq 7$ é uma potência de primo. Suponha também que $mdc(n, q) = 1$. Então, códigos quânticos* CSS *com parâmetros $[[n, k, d]]_{q-1}$ podem ser construídos. Em particular, códigos quânticos com parâmetros $[[q, k, d]]_{q-1}$ podem ser construídos.*

Demonstração: Por hipótese, $n \geq 8$ e $\text{mdc}(n, q) = 1$. Como cada classe possui um ou dois elementos, existem, no mínimo, cinco classes laterais distintas sobre F_{q-1}. Escolha C_1 como sendo o código cíclico gerado pelo polinômio minimal $M^{(0)}$, ${C_2}^{\perp}$ gerado pelo polinômio minimal $M^{(1)}$ e C_2 gerado pelo produto dos polinômios minimais $\prod_{i \neq 1} M^{(i)}$, onde i percorre o conjunto dos representantes módulo n. Sabemos que $M^{(0)}$ é distinto de $M^{(1)}$ e $C_2 \subset C_1$. Aplicando, então, a construção *CSS*, obtemos um código quântico com parâmetros $[[n, n-3, d \geq 2]]_{q-1}$. □

Teorema 3.2.15 *Assuma que q e $q+1$ são potências de primos. Então códigos quânticos $q+1$-ários MDS podem ser construídos.*

Demonstração: Claramente $\text{mdc}(q+1, q) = 1$. Além disso, pelo Lema 3.2.19, $q \mid [(q+1)^2 - 1]$. É fácil ver que todas as classes laterais possuem somente um elemento, quando

consideradas sobre F_{q+1}, onde a operação é a operação mod q. Conseqüentemente, escolhendo $C_1 = \prod_{i<\lfloor \frac{n}{2} \rfloor -1} M^{(i)}$ e ${C_2}^{\perp} = \prod_{i>\lfloor \frac{n}{2} \rfloor +1} M^{(i)}$, aplicando a construção *CSS* obtemos códigos quânticos MDS sobre F_{q+1}. □

Observação 3.2.1 *As famílias de códigos construídos a partir do Teorema 3.2.15 foram descobertas por Grassl* et al.*, [27]. Entretanto, temos construído tais famílias de um modo diferenciado.*

Alguns exemplos de códigos quânticos construídos a partir dos Teoremas 3.2.14 e 3.2.15 são apresentados em seguida.

Exemplo 3.2.15 *Sabemos que* $mdc(8,9) = 1$ *e* $9 \mid (8^2 - 1)$*. Além disso, tanto* 8 *quanto* 9 *são potências de primos. Assim, podemos construir um código quântico com parâmetros* $[[9, 4, d \geq 3]]_8$*.*

Para isso, considere as classes laterais mod 9*:*

$$\mathbb{C}_0 = \{0\},\ \mathbb{C}_1 = \{1, 8\},\ \mathbb{C}_2 = \{2, 7\},\ \mathbb{C}_3 = \{3, 6\},\ \mathbb{C}_4 = \{4, 5\}.$$

Se C_1 *é o código* BCH *gerado pelo produto dos polinômios minimais* $M^{(0)}M^{(1)}$ *e* ${C_2}^{\perp}$ *é o código cíclico gerado por* $M^{(4)}$*, o resultado segue, como desejado.*

Exemplo 3.2.16 *Sabemos que* $17 \mid (16^2 - 1)$ *e* $mdc(16, 17) = 1$*. Como* 17 *e* 16 *são potências de primos, podemos construir um código quântico com parâmetros* $[[17, 6, d \geq 5]]_{16}$*. Basta considerar* C_1 *como sendo o código* BCH *gerado pelo produto dos polinômios minimais* $M^{(0)}M^{(1)}M^{(2)}M^{(3)}$ *e* ${C_2}^{\perp}$ *como sendo o código cíclico gerado pelo produto dos polinômios minimais* $M^{(7)}M^{(8)}$*.*

Similarmente podemos construir um código quântico com parâmetros $[[17, 2, d \geq 6]]_{16}$*.*

Exemplo 3.2.17 *Como* $mdc(8, 21) = 1$ *e* $21 \mid (8^2 - 1)$ *podemos gerar códigos quânticos com parâmetros* $[[21, 15, d \geq 3]]_8$ *e* $[[21, 9, d \geq 5]]_8$*, por exemplo. Além disso, como* $32 \mid (31^2 - 1)$ *também existe um código quântico com parâmetros* $[[32, 6, d \geq 10]]_{31}$*.*

Exemplo 3.2.18 *Considerando* $q = 31$*, segue que* $31 \mid (32^2 - 1)$ *e* $mdc(31, 32) = 1$*. Pelo Teorema 3.2.15, existem códigos quânticos MDS com parâmetros* $[[31, 23, d \geq 5]]_{32}$*,* $[[31, 21, d \geq 6]]_{32}$*,* $[[31, 19, d \geq 7]]_{32}$*,* $[[31, 17, d \geq 8]]_{32}$*, e assim por diante.*

Utilizando o Lema 3.2.20, podemos construir mais códigos *CSS*:

Lema 3.2.20 *Seja q uma potência de primo e n um inteiro positivo tal que $mdc(q,n)=1$. Assuma também que $(q-1) \mid n$, $n \mid (q^2-1)$ e $n > q-1$. Então cada uma das classes laterais $\mathbb{C}_{lr}$, onde r é tal que $n = r(q-1)$ e $1 \leq l \leq q-2$ é um inteiro, possui somente um elemento.*

Demonstração: Como $n \mid (q^2-1)$, cada classe lateral possui um ou dois elementos. Na classe lateral $\mathbb{C}_{lr}$, onde $1 \leq l \leq q-1$, considere o elemento $(lr)q$. Então,

$$n = rq - r \Longrightarrow rq = n + r.$$

Conseqüentemente,

$$(lr)q = l(n+r) = ln + lr \equiv lr \ mod \ n,$$

donde cada classe lateral $\mathbb{C}_{lr}$ possui somente um elemento, a saber, o elemento lr. □

O Teorema 3.2.16 é o resultado principal dessa subseção, a principal contribuição, que gera códigos quânticos não primitivos:

Teorema 3.2.16 *Seja q uma potência de primo e $n > q-1$ um inteiro tal que $mdc(q,n)=1$. Assuma que $(q-1) \mid n$ e $n \mid (q^2-1)$, onde $m = 2$ é a ordem multiplicativa de q mod n. Então, existem códigos quânticos com parâmetros $[[n, n-[4(r-1)-2], d \geq r]]_q$.*

Demonstração: Seja C_1 o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}\cdots M^{(r-3)}M^{(r-2)},$$

$C_2{}^{\perp}$ o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(r)}M^{(r+1)}\cdots M^{(2r-3)}M^{(2r-2)}$$

e C_2 gerado pelo produto dos polinômios minimais

$$\prod_i M^{(i)},$$

onde $i \notin \{r, r+1, \cdots, 2r-2\}$ e i percorre o conjunto dos representantes mod n. Sabemos que o conjunto de definição do código C_1 é disjunto do conjunto de definição do código $C_2{}^{\perp}$. Além disso, por construção, $C_2 \subset C_1$.

Procedendo como na demonstração do Teorema 3.2.6 e utilizando a construção *CSS* segue o resultado. □

Observação 3.2.2 *Obviamente podemos construir códigos quânticos com distâncias mínimas maiores. Para isso, é suficiente que o número r, definido anteriormente, seja suficientemente grande de forma a permitir que o código quântico corrija mais erros. Esse fato será enfatizado nos exemplos.*

Corolário 3.2.6 *Assuma que as hipóteses do Teorema 3.2.16 sejam válidas. Então existem códigos quânticos com parâmetros* $[[n, n-[4(c-1)-2], d \geq c]]_q$.

Demonstração: Seja C_1 o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}\cdots M^{(c-3)}M^{(c-2)},$$

${C_2}^{\perp}$ o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(r)}M^{(r+1)}\cdots M^{(2c-3)}M^{(2c-2)}$$

e C_2 o código cíclico gerado pelo produto dos polinômios minimais

$$\prod_i M^{(i)},$$

onde $i \notin \{r, r+1, \cdots, 2c-2\}$ e i percorre o conjunto dos representantes mod n.

Procedendo como na demonstração do Teorema 3.2.6 e utilizando a construção *CSS* segue o resultado. □

Exemplo 3.2.19 *Considere $q = 9$ e $n = 40$. Então $mdc(9, 40) = 1$ e $40 \mid (9^2 - 1)$. Nesse caso $r = 5$. O Teorema 3.2.16 afirma que existe um código quântico com parâmetros* $[[40, 26, d \geq 5]]_9$. *As respectivas classes laterais associadas são:*

$$\begin{aligned}
\mathbb{C}_0 = \{0\},\ \ \mathbb{C}_1 = \{1,9\},\ \ \mathbb{C}_2 = \{2,18\},\\
\mathbb{C}_3 = \{3,27\},\ \ \mathbb{C}_4 = \{4,36\},\ \ \mathbb{C}_5 = \{6,14\}\cdots\\
\cdots\ \mathbb{C}_6 = \{6,14\},\ \ \mathbb{C}_7 = \{7,23\},\ \ \mathbb{C}_8 = \{8,32\},\\
\mathbb{C}_{10} = \{10\},\ \ \mathbb{C}_{23} = \{11,19\},\ \ \mathbb{C}_{12} = \{12,28\},\\
\mathbb{C}_{13} = \{13,37\},\ \ \mathbb{C}_{15} = \{15\},\ \ \mathbb{C}_{16} = \{16,24\},\cdots,
\end{aligned}$$

e assim por diante.

Entretanto, como r é suficientemente grande, é possível construir códigos quânticos com distâncias mínimas maiores, ou seja, escolhendo C_1 como sendo o código cíclico gerado pelo produto dos polinômios minimais

$$M^{(0)}M^{(1)}M^{(2)}M^{(3)}M^{(4)}M^{(5)},$$

e $C_2{}^{\perp}$ *o código cíclico gerado pelo produto dos polinômios minimais*

$$M^{(6)}M^{(10)}M^{(11)}M^{(12)}M^{(13)}M^{(15)},$$

obtemos um código quântico com parâmetros $[[40, 20, d \geq 7]]_9$

Exemplo 3.2.20 *Considere* $q = 11$ *e* $n = 20$*; então* $mdc(11, 20) = 1$*,* $20 \mid (11^2 - 1)$ *e* $r = 2$*. Procedendo da mesma forma como no exemplo anterior, construímos um código quântico com parâmetros* $[[20, 6, d \geq 6]]_{11}$*.*

Exemplo 3.2.21 *Considerando* $q = 11$ *e* $n = 30$ *sabemos que* $mdc(11, 30) = 1$*,* $30 \mid (11^2 - 1)$ *e* $r = 3$*. Escolhendo* C_1 *como sendo o código cíclico gerado pelo produto dos polinômios minimais*

$$M^{(0)}M^{(1)}M^{(2)}M^{(3)}M^{(4)}M^{(5)}M^{(6)},$$

e $C_2{}^{\perp}$ *o código cíclico gerado pelo produto dos polinômios minimais*

$$M^{(7)}M^{(10)}M^{(15)}M^{(16)}M^{(18)}M^{(19)}M^{(21)},$$

obtemos um código quântico com parâmetros $[[30, 7, d \geq 8]]_{11}$*.*

3.3 Parâmetros de alguns Códigos Novos

Apresentamos algumas tabelas contendo novos códigos quânticos construídos pelos métodos propostos neste capítulo. Nas tabelas, n é o comprimento da palavra-código, k é a dimensão e d é a distância mínima do código.

3.4 Comparações

A Tabela 3.7 mostra os parâmetros de alguns códigos quânticos q-ários construídos pelos métodos propostos em comparação aos parâmetros de bons códigos quânticos q-ários disponíveis na literatura. Os códigos apresentados em [5, 26] são os melhores códigos quânticos quaternários conhecidos até o presente momento. Podemos ver que, baseado no Método de Construção II, podemos reproduz os parâmetros dos códigos construídos em [26]. Além disso, este método proposto gera códigos melhores que os apresentados em [5].

Outro fato que deve ser observado é que devido ao fato da teoria da codificação quântica ser uma teoria recente, existem na literatura pouquíssimos códigos quânticos q-ários, $q \neq 2$. Além disso, alguns destes possuem parâmetros muito diferentes dos códigos gerados pelos métodos de construção propostos neste trabalho, o que dificulta as comparações.

Tabela 3.1: Construção I, $p = 2$

$[[n, k, d]]_q$
$[[255, 239, \geq 3]]$
$[[255, 223, \geq 5]]$
$[[255, 207, \geq 7]]$
$\vdots$
$[[255, 143, \geq 15]]$
$[[511, 475, \geq 5]]$
$[[511, 457, \geq 7]]$
$[[511, 439, \geq 9]]$
$[[511, 421, \geq 11]]$
$\vdots$
$[[511, 331, \geq 21]]$
$\vdots$
$[[511, 241, \geq 31]]$
$[[1023, 983, \geq 5]]$
$[[1023, 963, \geq 7]]$
$\vdots$
$[[1023, 912, \geq 12]]$
$[[1023, 903, \geq 13]]$
$[[1023, 883, \geq 15]]$
$[[1023, 863, \geq 17]]$
$\vdots$
$[[1023, 723, \geq 31]]$

Tabela 3.2: Construção II, para $p = 4, 5, 7$

$[[n, k, d]]_q$
$[[21, 13, 3]]_4$
$[[21, 7, 4]]_4$
$[[63, 43, \geq 6]]_4$
$[[85, 69, 4]]_4$
$[[85, 61, 5]]_4$
$[[85, 53, 7]]_4$
$[[124, 98, \geq 7]]_5$
$[[124, 72, \geq 12]]_5$
$[[124, 64, \geq 13]]_5$
$[[624, 503, \geq 19]]_5$
$[[2400, 2126, \geq 47]]_7$

Tabela 3.3: Construção III, para $p = 4, 5, 7, 8, 9, 11, 13, 16, 17, 19$

$[[q^2-1, q^2-4q+5, d \geq q]]_q$
$[[q^2-1, q^2-4c+5, d \geq c]]_q$
$[[15, 9, \geq 3]]_4$
$[[15, 5, \geq 4]]_4$
$[[24, 18, \geq 3]]_5$
$[[24, 10, \geq 5]]_5$
$[[48, 42, \geq 3]]_7$
$[[48, 34, \geq 5]]_7$
$[[48, 26, \geq 7]]_7$
$[[63, 57, \geq 3]]_8$
$[[63, 49, \geq 5]]_8$
$[[63, 41, \geq 7]]_8$
$[[63, 37, \geq 8]]_8$
$[[80, 74, \geq 3]]_9$
$[[80, 70, \geq 4]]_9$
$[[80, 66, \geq 5]]_9$
$[[80, 50, \geq 9]]_9$
$[[120, 114, \geq 3]]_{11}$
$[[120, 106, \geq 5]]_{11}$
$[[120, 98, \geq 7]]_{11}$
$[[120, 90, \geq 9]]_{11}$
$[[120, 82, \geq 11]]_{11}$
$[[168, 162, \geq 3]]_{13}$
$[[168, 154, \geq 5]]_{13}$
$[[168, 146, \geq 7]]_{13}$
$[[168, 138, \geq 9]]_{13}$
$[[168, 130, \geq 11]]_{13}$
$[[168, 122, \geq 13]]_{13}$
$[[256, 198, \geq 16]]_{16}$
$[[288, 282, \geq 3]]_{17}$
$[[288, 274, \geq 5]]_{17}$
$[[288, 266, \geq 7]]_{17}$
$[[288, 258, \geq 9]]_{17}$
$[[288, 250, \geq 11]]_{17}$
$[[288, 242, \geq 13]]_{17}$
$[[288, 234, \geq 15]]_{17}$
$[[288, 226, \geq 17]]_{17}$
$[[360, 354, \geq 3]]_{19}$
$[[360, 346, \geq 5]]_{19}$
$[[360, 338, \geq 7]]_{19}$
$[[360, 330, \geq 9]]_{19}$
$[[360, 322, \geq 11]]_{19}$
$[[360, 314, \geq 13]]_{19}$
$[[360, 306, \geq 15]]_{19}$
$[[360, 298, \geq 17]]_{19}$
$[[360, 290, \geq 19]]_{19}$

Tabela 3.4: Construção IV, $p = 3$ e $n = 3^m - 1$

$[[n, k \geq n - 2m - 2, d \geq 3]]_3$
$[[n, k \geq n - 4m, d \geq 4]]_3$
$[[n, k \geq n - 4m - 2, d \geq 5]]_3$
$[[n, k \geq n - 6m - 2, d \geq 6]]_3$
$[[n, k \geq n - 8m - 2, d \geq 8]]_3$
$[[26, 18, \geq 3]]_3$
$[[26, 12, \geq 5]]_3$
$[[80, 70, \geq 3]]_3$
$[[80, 64, \geq 4]]_3$
$[[80, 62, \geq 5]]_3$
$[[80, 54, \geq 6]]_3$
$[[80, 46, \geq 8]]_3$
$[[242, 230, \geq 3]]_3$
$[[242, 222, \geq 4]]_3$
$[[242, 220, \geq 5]]_3$
$[[242, 210, \geq 6]]_3$
$[[242, 200, \geq 8]]_3$

Tabela 3.5: Construção V, para $p = 5, 7, 11$

$[[p^3 - 1, p^3 - 9, d \geq 3]]_p$
$[[p^3 - 1, p^3 - 15, d \geq 4]]_p$
$[[p^3 - 1, p^3 - 21, d \geq 5]]_p$
$[[124, 116, \geq 3]]_5$
$[[124, 110, \geq 4]]_5$
$[[124, 104, \geq 5]]_5$
$[[342, 334, \geq 3]]_7$
$[[342, 328, \geq 4]]_7$
$[[342, 322, \geq 5]]_7$
$[[1330, 1322, \geq 3]]_{11}$
$[[1330, 1316, \geq 4]]_{11}$
$[[1330, 1310, \geq 5]]_{11}$

Tabela 3.6: Construção VI, para $q = 8, 9, 11, 16, 31$

$[[n, k, d]]_q$
$[[9, 4, \geq 3]]_8$
$[[10, 2, \geq 4]]_9$
$[[17, 6, \geq 5]]_{16}$
$[[17, 2, \geq 6]]_{16}$
$[[20, 6, \geq 6]]_9$
$[[20, 6, \geq 6]]_{11}$
$[[21, 15, \geq 3]]_8$
$[[21, 9, \geq 5]]_8$
$[[30, 7, d \geq 8]]_{11}$
$[[32, 6, \geq 10]]_{31}$
$[[40, 20, \geq 7]]_9$
$[[40, 26, \geq 5]]_9$

Ainda, chamamos a atenção para o seguinte fato: os parâmetros dos códigos $[[124, 94, d \geq 7]]_5$, $[[124, 100, d \geq 5]]_5$, $[[124, 64, d \geq 13]]_5$ e $[[26, 8, \geq 5]]_3$, construídos em [16], são parâmetros de códigos que os autores demonstraram a existência mas não apresentaram as construções explícitas.

3.5 Considerações Finais

Foram apresentados seis novos métodos de construção que geram novas famílias de bons códigos quânticos *CSS* q-ários, ou seja, as novas famílias de códigos construídas pelos métodos propostos possuem taxa de codificação tendendo para o valor 1. Além disso, reproduzimos muitos dos códigos apresentados em [26] e, principalmente, conseguimos construir códigos melhores que aqueles apresentados em [5, 14, 16, 18].

Tabela 3.7: Comparação entre Códigos

Artigo	Códigos do Artigo	Códigos Construídos pelos Métodos Propostos
[14]	$[[144, 94, 6]]_{13}$	$[[168, 146, \geq 7]]_{13}$
[14]	$[[256, 158, 8]]_{17}$	$[[288, 262, \geq 8]]_{17}$
[5]	$[[21, 12, 3]]_4$	$[[21, 13, 3]]_4$
[5]	$[[63, 39, 6]]_4$	$[[63, 43, \geq 6]]_4$
[5]	$[[85, 69, 4]]_4$	$[[85, 69, 4]]_4$
[5]	$[[85, 61, 5]]_4$	$[[85, 61, 5]]_4$
[5]	$[[85, 53, 7]]_4$	$[[85, 53, 7]]_4$
[18]	$[[256, 126, 12]]_2$	$[[255, 159, \geq 13]]_2$
[18]	$[[512, 336, 12]]_2$	$[[511, 403, \geq 13]]$
[16]	$[[124, 94, \geq 7]]_5$	$[[124, 98, \geq 7]]_5$
[16]	$[[124, 100, \geq 5]]_5$	$[[124, 104, \geq 5]]_5$
[16]	$[[124, 64, \geq 13]]_5$	$[[124, 64, \geq 13]]_5$
[16]	$[[26, 8, \geq 5]]_3$	$[[26, 12, \geq 5]]_3$
[26]	$[[15, 5, 4]]_4$	$[[15, 5, 4]]_4$
[26]	$[[15, 9, 3]]_4$	$[[15, 9, 3]]_4$
[26]	$[[85, 69, 4]]_4$	$[[85, 69, 4]]_4$
[26]	$[[85, 61, 5]]_4$	$[[85, 61, 5]]_4$
[26]	$[[85, 53, 7]]_4$	$[[85, 53, 7]]_4$

Capítulo 4

CSS Derivados de Códigos Reed-Muller e Resíduos Quadráticos

Assim como nos capítulos anteriores, os métodos de construção de códigos *CSS*, propostos neste capítulo, também serão realizados a partir de dois códigos clássicos distintos, não necessariamente auto-ortogonais, devido às vantagens que tal método apresenta. O primeiro método de construção sendo proposto utiliza dois códigos clássicos *Reed-Muller* (RM) e o segundo método utiliza dois códigos clássicos do tipo *Resíduos Quadráticos* (RQ).

O capítulo está organizado como segue. Na Seção 4.1, apresentamos uma revisão da teoria dos códigos *Reed-Muller* e *Resíduos Quadráticos*. Nas Seções 4.2 e 4.3, explicitamos as contribuições do capítulo, ou seja, os métodos de construção de códigos *CSS* baseados em códigos clássicos *Reed-Muller* e *Resíduos Quadráticos*, respectivamente, e na Seção 4.4, descrevemos as considerações finais do capítulo.

4.1 Conceitos Preliminares

Esta seção tem por objetivo apresentar uma breve revisão dos conceitos sobre os códigos *Reed-Muller* e *Resíduos Quadráticos*, necessários para o desenvolvimento deste trabalho. Para maiores detalhes sobre esses conceitos, sugerimos a referência [33].

4.1.1 Códigos Reed-Muller

Definição 4.1.1 *[33] Uma função booleana é uma função $f(v) = f(v_1, \cdots, v_m)$ que assume valores* 0 *ou* 1*. Tal função pode ser especificada por uma tabela verdade, que mostra os valores de f em todos os seus 2^m argumentos.*

Por exemplo, quando $m = 3$, uma função booleana é especificada pela Tabela-
-Verdade 4.1.

v_3	00001111
v_2	00110011
v_1	01010101
f	00011000

Tabela 4.1: Tabela-Verdade

A última linha da tabela fornece os valores assumidos por f, que é um vetor de comprimento $n = 2^m$, denotado por **f**. As operações lógicas usuais podem ser aplicadas às funções booleanas. Ou seja,

$$f \text{ OU EXCLUSIVO } g = f \oplus g,$$
$$f \text{ E } g = fg,$$
$$f \text{ OU } g = f \oplus g \oplus fg,$$
$$\text{NÃO } f = \overline{f} = 1 \oplus f.$$

A função booleana, estabelecida na Tabela-Verdade 4.1, pode ser escrita da seguinte maneira:

$$f = v_1 v_2 \overline{v_3} \text{ OU } \overline{v_1 v_2} v_3.$$

Com todos esses conceitos em mente, enunciamos a seguir, a definição do código *Reed-Muller* (RM).

Definição 4.1.2 *[33] Seja* $\boldsymbol{f}$ *o vetor de comprimento* 2^m *obtido a partir de uma função booleana* $f(v_1, \cdots, v_m)$. *O código binário Reed-Muller, ou* $\mathcal{R}(r, m)$, *de ordem* r *e comprimento* $n = 2^m$, *para* $0 \leq r \leq m$ *é o conjunto de todos os vetores* $\boldsymbol{f}$, *onde* $f(v_1, \cdots, v_m)$ *é uma função booleana, que, por sua vez, é um polinômio de grau no máximo* r.

Segue um exemplo para melhor entendimento do texto.

Exemplo 4.1.1 *O código* $\mathcal{R}(1, 3)$, *de comprimento* 8, *consiste de* 16 *palavras-código*

$$a_0 \boldsymbol{1} + a_1 \boldsymbol{v}_1 + a_2 \boldsymbol{v}_2 + a_3 \boldsymbol{v}_3,$$

onde $a_i = 0$ *ou* $a_i = 1$, *e o vetor* $\boldsymbol{1} = (1, 1, \cdots, 1)$. *A Tabela 4.2 mostra todos os* 16 *vetores.*

$\mathbf{0}$	00000000
$\mathbf{v}_3$	00001111
$\mathbf{v}_2$	00110011
$\mathbf{v}_1$	01010101
$\mathbf{v}_2 + \mathbf{v}_3$	00111100
$\mathbf{v}_1 + \mathbf{v}_3$	01011010
$\mathbf{v}_1 + \mathbf{v}_2$	01100110
$\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3$	01101001
$\mathbf{1}$	11111111
$1 + \mathbf{v}_3$	11110000
$1 + \mathbf{v}_2$	11001100
$1 + \mathbf{v}_1$	10101010
$1 + \mathbf{v}_2 + \mathbf{v}_3$	11000011
$1 + \mathbf{v}_1 + \mathbf{v}_3$	10100101
$1 + \mathbf{v}_1 + \mathbf{v}_2$	10011001
$1 + \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3$	10010110

Tabela 4.2: Tabela

A Proposição 4.1.1 permite calcular a dimensão do código $\mathcal{R}(r, m)$.

Proposição 4.1.1 *[33] A dimensão de um código* Reed-Muller $\mathcal{R}(r, m)$ *é dada por*

$$k = 1 + \left(\begin{array}{c} m \\ 1 \end{array} \right) + \left(\begin{array}{c} m \\ 2 \end{array} \right) + \cdots + \left(\begin{array}{c} m \\ r \end{array} \right).$$

Em seguida, enunciaremos dois teoremas e uma proposição que serão utilizadas na construção dos códigos quânticos deste capítulo.

Teorema 4.1.1 *[33] O código Reed-Muller $\mathcal{R}(r, m)$ possui distância mínima, denotada por d_{min}, igual a 2^{m-r}.*

Teorema 4.1.2 *[33] O código Reed-Muller $\mathcal{R}(m - r - 1, m)$ é o código dual do código $\mathcal{R}(r, m)$, para $0 \leq r \leq m - 1$.*

Proposição 4.1.2 *[33] Vale a seguinte inclusão: $\mathcal{R}(r, m) \subset \mathcal{R}(r + 1, m)$.*

O próximo passo é a introdução da classe dos códigos clássicos do tipo *Resíduos Quadráticos.*

Definição 4.1.3 *[33] Se a congruência $x^2 \equiv n \bmod p$ possui solução, então n é chamado resíduo quadrático módulo p, onde n é um número natural e p é um número primo.*

Os códigos do tipo *Resíduos Quadráticos* (RQ) têm comprimento p primo e são construídos sobre F_l, onde l é um outro número primo, também resíduo quadrático *mod* p. Consideraremos $l = 2$, o que, de acordo com [33], implica que p é da forma $p = 8k + 1$ ou da forma $p = 8k - 1$.

Seja $\mathcal{Q}$ o conjunto de resíduos quadráticos *mod* p, $\mathcal{N}$ o conjunto de não resíduos e R o anel $F_2[x]/(x^p - 1)$.

Definição 4.1.4 *[33] Os códigos do tipo* RQ $\mathcal{Q}$, $\mathcal{Q}^*$, $\mathcal{N}$ *e* $\mathcal{N}^*$ *são códigos cíclicos de* R, *com polinômios geradores* $q(x)$, $(x-1)q(x)$, $n(x)$, $(x-1)n(x)$, *respectivamente, onde*

$$q(x) = \prod_{r \in \mathcal{Q}} (x - \alpha^r), \quad n(x) = \prod_{n \epsilon N} (x - \alpha^n)$$

e α *é uma* p*-ésima raiz primitiva da unidade em algum corpo contendo* F_2.

Salientamos que $q(x)$ e $n(x)$ têm coeficientes em F_2, $\mathcal{Q} \supset \mathcal{Q}^*$ e $\mathcal{N} \supset \mathcal{N}^*$. Além disso, $\mathcal{Q}$ e $\mathcal{N}$ são códigos equivalentes e têm dimensão $\frac{1}{2}(p+1)$; $\mathcal{Q}^*$ e $\mathcal{N}^*$ também são códigos equivalentes e possuem dimensão $\frac{1}{2}(p-1)$ [33].

Enunciaremos, em seguida, dois teoremas que serão fundamentais para a construção de códigos *CSS* a partir de códigos clássicos do tipo RQ.

Teorema 4.1.3 *[33] Se* $d_{min} = d$ *é a distância mínima do código* $\mathcal{Q}$ *ou* $\mathcal{N}$ *(que são do tipo* RQ*), então* $d^2 \geq p$. *Além disso, se* $p = 4k - 1$, *então* $d^2 - d + 1 \geq p$.

Teorema 4.1.4 *[33] Se* $p = 4k - 1$, *então* $\mathcal{Q}^\perp = \mathcal{Q}^*$ *e* $\mathcal{N}^\perp = \mathcal{N}^*$. *Se* $p = 4k + 1$, *então* $\mathcal{Q}^\perp = \mathcal{N}^*$ *e* $\mathcal{N}^\perp = \mathcal{Q}^*$.

4.2 Construção de Códigos *CSS* a Partir de Códigos Reed-Muller

Iniciaremos esta seção com a construção de alguns códigos quânticos *CSS*, e a posteriori, generalizaremos o procedimento pelo método dedutivo.

Exemplo 4.2.1 *(Código* CSS *construído a partir de códigos* Reed-Muller*, que corrige erros arbitrários em* 3 *qubits) De acordo com a Proposição 4.1.2, vale a inclusão* $\mathcal{R}(2,6) \subset \mathcal{R}(3,6)$.

Considerando $C_1 = \mathcal{R}(3,6)$ *e* $C_2 = \mathcal{R}(2,6)$, *sabemos que* $C_2 \subset C_1$. *Pela Proposição 4.1.1, a dimensão de* C_1 *é igual a*

$$k_1 = 1 + \begin{pmatrix} 6 \\ 1 \end{pmatrix} + \begin{pmatrix} 6 \\ 2 \end{pmatrix} + \begin{pmatrix} 6 \\ 3 \end{pmatrix} = 42$$

e a dimensão de C_2 *é igual a*

$$k_2 = 1 + \left(\begin{array}{c} 6 \\ 1 \end{array} \right) + \left(\begin{array}{c} 6 \\ 2 \end{array} \right) = 22.$$

Assim, a dimensão do código $CSS(C_1, C_2)$ *será* $k = k_1 - k_2 = 20$.

O comprimento deste código será $n = 2^6 = 64$. *Calculemos agora, a distância mínima do código* $CSS(C_1, C_2)$.

Pelo Teorema 4.1.1, a distância mínima de C_1 *é igual a* $d = 2^{6-3} = 8$. *Utilizando o Teorema 4.1.2 com* $m = 6$ *e* $r = 2$, *o código dual* ${C_2}^{\perp}$ *possui parâmetros* $(m - r - 1, 6) = (6 - 2 - 1, 6) = (3, 6)$. *Ainda, pelo Teorema 4.1.1, a distância mínima de* ${C_2}^{\perp}$ *também é igual a* 8.

Aplicando a construção CSS, *podemos concluir que o código* $CSS(C_1, C_2)$ *possui parâmetros* $[[64, 20, d = 8]]$ *e corrige erros arbitrários em* 3 *qubits.*

Exemplo 4.2.2 *Neste exemplo, apresentaremos a construção de um código* CSS, *a partir de códigos* RM, *com capacidade de correção de* 7 *erros quânticos arbitrários.*

Utilizando novamente a Proposição 4.1.2, vale a inclusão $\mathcal{R}(3, 8) \subset \mathcal{R}(4, 8)$. *Considere* $C_1 = \mathcal{R}(4, 8)$ *e* $C_2 = \mathcal{R}(3, 8)$. *Então* $C_2 \subset C_1$. *Pela Proposição 4.1.1, a dimensão de* C_1 *é igual a*

$$k_1 = 1 + \left(\begin{array}{c} 8 \\ 1 \end{array} \right) + \left(\begin{array}{c} 8 \\ 2 \end{array} \right) + \left(\begin{array}{c} 8 \\ 3 \end{array} \right) + \left(\begin{array}{c} 8 \\ 4 \end{array} \right) = 163$$

e a dimensão de C_2 *é igual a*

$$k_2 = 1 + \left(\begin{array}{c} 8 \\ 1 \end{array} \right) + \left(\begin{array}{c} 8 \\ 2 \end{array} \right) + \left(\begin{array}{c} 8 \\ 3 \end{array} \right) = 93.$$

Portanto, a dimensão do código $CSS(C_1, C_2)$ *será* $k = k_1 - k_2 = 70$.

Calculando o comprimento deste código temos que $n = 2^8 = 256$. *A distância mínima do código* $CSS(C_1, C_2)$ *será calculada a seguir.*

Pelo Teorema 4.1.1, a distância mínima de C_1 *é* $d = 2^{8-4} = 16$. *Aplicando o Teorema 4.1.2 com* $m = 8$ *e* $r = 3$, *o código dual* ${C_2}^{\perp}$ *possui parâmetros* $(8 - 3 - 1, 8) = (4, 8)$. *Ainda, pelo Teorema 4.1.1, a distância mínima de* ${C_2}^{\perp}$ *também é igual a* 16. *Utilizando-se a construção* CSS, *podemos concluir que o código* $CSS(C_1, C_2)$ *possui parâmetros* $[[256, 70, d = 16]]$ *e corrige erros arbitrários em* 7 *qubits.*

Com isso estamos aptos a realizar a construção generalizada. Construiremos códigos quânticos *CSS* capazes de corrigir erros quânticos arbitrários em

$$\left\lfloor \frac{2^s - 1}{2} \right\rfloor \ qubits,$$

onde $\lfloor x \rfloor$ denota o maior inteiro menor ou igual a x.

Observe que é verdadeiro o seguinte esquema:

$$d_{min} = 2^3 \longrightarrow C_1 = \mathcal{R}(3,6) \supset \mathcal{R}(2,6) = C_2,$$

$$d_{min} = 2^4 \longrightarrow C_1 = \mathcal{R}(4,8) \supset \mathcal{R}(3,8) = C_2,$$

$$d_{min} = 2^5 \longrightarrow C_1 = \mathcal{R}(5,10) \supset \mathcal{R}(4,10) = C_2.$$

Conseqüentemente,

$$d_{min} = 2^s \longrightarrow C_1 = \mathcal{R}(s,2s) \supset \mathcal{R}(s-1,2s) = C_2,$$

onde d_{min} é a distância mínima do código.

Pelo Teorema 4.1.2, segue que ${C_2}^{\perp} = \mathcal{R}(2l-(s-1)-1,2s) = \mathcal{R}(s,2s)$. Portanto, $C_2 \subset C_1$, $d_{min}(C_1) = 2^s$ e $d_{min}({C_2}^{\perp}) = 2^{2s-s} = 2^s$. Calcularemos agora, a dimensão do código *CSS* gerado a partir destes dois códigos.

Sabemos que a dimensão do código C_1 é igual a

$$k_1 = 1 + \left(\begin{array}{c} 2s \\ 1 \end{array} \right) + \cdots + \left(\begin{array}{c} 2s \\ s-1 \end{array} \right) + \left(\begin{array}{c} 2s \\ s \end{array} \right)$$

e a dimensão de C_2 é igual a

$$k_2 = 1 + \left(\begin{array}{c} 2s \\ 1 \end{array} \right) + \cdots + \left(\begin{array}{c} 2s \\ s-1 \end{array} \right),$$

donde

$$k = k_1 - k_2 = \left(\begin{array}{c} 2s \\ s \end{array} \right).$$

Analisando os resultados, concluímos que os códigos quânticos *CSS*, construídos neste capítulo, possuem parâmetros

$$[[n,k,d]] = [[2^{2s}, \left(\begin{array}{c} 2s \\ s \end{array} \right), 2^s]].$$

4.3 Construção de Códigos *CSS* a Partir de Códigos Resíduos Quadráticos

Fixadas as notações e estabelidos os pré-requisitos, propomos, então, a construção de um código *CSS* com parâmetros $[[31,1,5]]$.

Construiremos um código *CSS*, onde C_1 e C_2 são códigos clássicos resíduos quadráticos *mod* p, com $p = 31$ e $l = 2$. Como a equação modular $x^2 \equiv 2 \; mod \; 31$ possui uma solução para $x = 8$, escolhemos $p = 31$.

Pelo Teorema 4.1.3, como p é da forma $4k - 1$, segue que

$$d^2 - d + 1 \geq 31 \Longrightarrow d \geq 6.$$

Além disso, pelo Teorema 4.1.4, como $p = 4k - 1$, concluímos que $\mathcal{Q}^{\perp} = \mathcal{Q}^*$.

Considerando $C_1 = \mathcal{Q}$ e $C_2 = \mathcal{Q}^{\perp} = \mathcal{Q}^*$, segue que $C_2 \subset C_1$ e ${C_2}^{\perp} = (\mathcal{Q}^{\perp})^{\perp} \supset \mathcal{Q} = C_1$. A distância mínima de C_1 é maior ou igual a 6 e a distância mínima de ${C_2}^{\perp}$ também é maior ou igual a 6, donde o código $CSS(C_1, C_2)$ corrige erros arbitrários em até 2 qubits. A dimensão de C_1 é $\frac{1}{2}(31 + 1) = 16$ e a dimensão de C_2 é $\frac{1}{2}(31 - 1) = 15$.

Assim, o código $CSS(C_1, C_2)$ possui parâmetros $[[31, 1, 5]]$ e corrige erros arbitrários em 2 qubits.

4.4 Considerações Finais

Neste capítulo foram propostos métodos de construção de códigos quânticos *CSS*, derivados de códigos clássicos *Reed-Muller* e *Resíduos Quadráticos*. Enfatizamos que a primeira família de códigos já foi apresentada anteriormente por Zang and Fuzz [31], porém, a construção de tal família foi realizada por um método de construção diferente do apresentado neste capítulo.

Capítulo 5

Construção de Códigos *CSS* Derivados de Códigos Produto

Neste capítulo, a partir do produto tensorial de dois códigos clássicos *Reed-Solomon*, propomos um método de construção de códigos *CSS* . Apesar das vantagens que tal processo proporciona, como já foi mencionado nos capítulos anteriores, a construção sendo proposta não gera códigos com bons parâmetros, devido ao fato do comprimento das palavras-código aumentarem muito rapidamente à medida que o produto tensorial é aplicado aos códigos clássicos *Reed-Solomon*. Entretanto, motivados pela geração de novos códigos quânticos que são facilmente construídos e com o intuito de gerar códigos quânticos atuando nos qudits de forma desigual (proteção desigual), justifica-se a proposta de construção realizada no decorrer do capítulo. Relembremos que se considerarmos um único código clássico auto-ortogonal no processo de construção *CSS* não é possível a construção de códigos quânticos atuando de forma desigual na proteção contra erros quânticos.

O capítulo está organizado como segue. Na Seção 5.1, apresentamos uma revisão de códigos produto. Na Seção 5.2, apresentamos as contribuições do capítulo, ou seja, o método de construção proposto. Na Seção 5.3, exibimos uma tabela com alguns códigos gerados pelo método proposto, e na Seção 5.4, relatamos as considerações finais do capítulo.

5.1 Revisão de Código Produto

Nesta seção, apresentaremos alguns resultados já conhecidos sobre códigos produto, que serão fundamentais para a construção sendo proposta. Os próximos três resultados podem ser encontrados em [14].

Lema 5.1.1 *[14] Sejam $C_1 = [n_1, k_1, d_1]_q$ e $C_2 = [n_2, k_2, d_2]_q$ códigos lineares sobre o corpo F_q, (onde $q = p^m$, p primo) com matrizes geradoras $G^{(1)}$ e $G^{(2)}$, respectivamente. Então, o*

código produto $C_\pi := C_1 \otimes C_2$ *é o código linear* $C_\pi := [n_1 n_2,\ k_1 k_2,\ d_1 d_2]_q$, *gerado pela matriz* $G := G^{(1)} \otimes G^{(2)}$, *onde* $\otimes$ *denota o produto de Kronecker:*

$$G = \begin{bmatrix} g_{11}^{(1)} G^{(2)} & g_{12}^{(1)} G^{(2)} & \cdots & g_{1,n_1}^{(1)} G^{(2)} \\ g_{21}^{(1)} G^{(2)} & g_{22}^{(1)} G^{(2)} & \cdots & g_{2,n_1}^{(1)} G^{(2)} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k_1,1}^{(1)} G^{(2)} & g_{k_1,2}^{(1)} G^{(2)} & \cdots & g_{k_1,n_1}^{(1)} G^{(2)} \end{bmatrix}.$$

Teorema 5.1.1 *[14] Sejam* $C_1 = [n_1, k_1]$ *e* $C_2 = [n_2, k_2]$ *códigos lineares cíclicos com polinômios geradores* $g_1(X)$ *e* $g_2(Y)$, *respectivamente. Então* $C_\pi := C_1 \otimes C_2$ *é o código bicíclico gerado por* $g_1(X)g_2(Y)$. *As palavras-código de* C_π *correspondem a todos os polinômios de duas variáveis da forma* $c(X,Y) = i(X,Y)g_1(X)g_2(Y)$ *módulo o ideal gerado por* $X^{n_1} - 1$ *e* $Y^{n_2} - 1$, *onde* $i(X,Y) \in F_{p^m}[X,Y]$ *é um polinômio arbitrário de duas variáveis. O código dual Euclidiano* $(C_1 \otimes C_2)^\perp$ *do código produto* $C_1 \otimes C_2$ *consiste de todos os polinômios que são múltiplos de* $h_1(X)$ *ou* $h_2(Y)$, *onde* $h_1(X)$ *e* $h_2(Y)$ *são os polinômios geradores dos códigos duais* ${C_1}^\perp$ *e* ${C_2}^\perp$, *respectivamente.*

Teorema 5.1.2 *[14] O código produto de dois códigos* Reed-Solomon $C_1 = [p^m - 1, p^m - \delta_1,\ \delta_1]_{p^m}$ *e* $C_2 = [p^m - 1, p^m - \delta_2,\ \delta_2]_{p^m}$ *sobre o corpo* F_{p^m} *é o código*

$$C_1 \otimes C_2 = [(p^m - 1)^2, (p^m - \delta_1)(p^m - \delta_2),\ \delta_1\delta_2]_{p^m}.$$

O código dual Euclidiano,

$$(C_1 \otimes C_2)^\perp = [(p^m - 1)^2, K^\perp, d^\perp]_{p^m},$$

possui parâmetros

$$K^\perp = p^m(\delta_1 + \delta_2 - 2) - \delta_1\delta_2 + 1,$$

e

$$d^\perp = \min(p^m - \delta_1, p^m - \delta_2),$$

onde δ_1 *e* δ_2 *são as distâncias mínimas dos códigos* C_1 *e* C_2, *respectivamente.*

Além disso, o código produto é auto-ortogonal se C_1 *ou* C_2 *são auto-ortogonais.*

5.2 Códigos *CSS* Derivados de Códigos Produto

Nesta seção, apresentaremos nossas contribuições. O resultado principal deste capítulo é o Teorema 5.2.1.

Seja p um número primo. O primeiro passo deste método de construção consiste em encontrar o menor número natural m satisfazendo

$$p^m \geq \lceil \sqrt{2t+1} \rceil + 1 + 2t + 1 = \lceil \sqrt{2t+1} \rceil + 2t + 2,$$

onde $\lceil y \rceil$, $y \in \mathbb{R}$, denota o menor inteiro maior ou igual a y. Iniciaremos o processo de construção encontrando o menor número inteiro m que satisfaça esta condição.

Pelo Princípio do Menor Inteiro, é claro que existem esses números (o Princípio do Menor Inteiro afirma que cada subconjunto não vazio do conjunto dos números inteiros possui um elemento mínimo). Uma questão natural se origina com respeito a este fato. Por que escolhemos este limitante?

Para que possamos construir códigos quânticos que corrijam erros quânticos arbitrários em t qudits, para todo $t \geq 2$, devemos considerar espaços suficientemente amplos. A raiz quadrada que aparece na desigualdade está diretamente relacionada com o valor da distância mínima, a saber, d_{min}, do código C_1, antes da aplicação da construção dos códigos produto. Mais especificamente, se sabemos que d_{min} deve ser igual a a, devemos considerar o valor real $\sqrt{a}$, visto que, quando aplicarmos a construção dos códigos produto, teremos $d_{min} = (\sqrt{a})^2 = a$.

O outro valor, a saber, o valor $2t + 2$, está relacionado com o valor do d_{min} do código dual $(C_2 \otimes C_2)^{\perp}$. De fato, pelo Teorema 5.1.2, concluímos que a distância mínima do código $(C_2 \otimes C_2)^{\perp}$ é igual a $p^m - \delta_2$, onde δ_2 é a distância mínima do código C_2.

Assim, através deste passo, é possível construir códigos *Reed-Solomon* C_1 e C_2, sobre o corpo F_{p^m}, de tal modo que a distância mínima dos respectivos códigos C_1 e C_2 satisfaçam as condições impostas pela construção dos códigos *CSS*, quando aplicadas aos códigos produto. Note que os códigos C_1 e C_2 terão comprimentos $n = p^m - 1$, p primo.

O segundo passo já é a construção explícita.

Seja C_1 o código *Reed-Solomon* sobre o corpo F_{p^m}, gerado pelo polinômio

$$g_1(x) = (x-1)(x-\alpha^1)(x-\alpha^2)\cdots(x-\alpha^{(\lceil \sqrt{d} \rceil - 2)}),$$

onde α é um elemento primitivo do corpo F_{p^m} e $d = 2t + 1$ é a suposta distância mínima que o código $C_1 \otimes C_1$ deverá ter para corrigir erros quânticos arbitrários em t qudits.

Sabemos que $\partial g_1(x) = \lceil \sqrt{d} \rceil - 1$, onde ∂ denota o grau do polinômio $g_1(x)$, e que a distância mínima do código C_1 é igual a $\lceil \sqrt{d} \rceil$. Assim, os parâmetros do código C_1 são:

$$[p^m - 1, p^m - (\lceil \sqrt{d} \rceil), \lceil \sqrt{d} \rceil]_{p^m}.$$

Aplicando o Teorema 5.1.2 e utilizando o fato de que o código C_1 é um código *Reed-Solomon*, sabemos que a distância mínima do código $C_1 \otimes C_1$ é, no mínimo, igual a d, ou seja, $(\lceil \sqrt{d} \rceil)^2 \geq d$. Assim, o código $C_1 \otimes C_1$ corrige, no mínimo, t erros.

Os parâmetros do código $C_1 \otimes C_1$ são:

$$C_1 \otimes C_1 = [(p^m-1)^2, (p^m - \lceil\sqrt{d}\rceil)^2,\ (\lceil\sqrt{d}\rceil)^2]_{p^m},$$

onde $(\lceil\sqrt{d}\rceil)^2 \geq d = 2t+1$.

Considere, agora, todas as potências de α ordenadas em ordem crescente:

$$\alpha^0 = 1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{(p^m-2)}.$$

Sabemos que o conjunto das unidades do corpo F_{p^m} (exceto as raízes de $g_1(x)$) é o conjunto

$$NRg_1 = \{\alpha^{(\lceil\sqrt{d}\rceil-1)}, \alpha^{(\lceil\sqrt{d}\rceil)}, \alpha^{(\lceil\sqrt{d}\rceil+1)}, \cdots, \alpha^{(p^m-2)}\}.$$

Considere o conjunto das últimas $2t+1$ unidades do corpo F_{p^m} cujas potências estão ordenadas em ordem crescente, a saber:

$$A = \{\alpha^{[p^m-(2t+2)]}, \alpha^{[p^m-(2t+1)]}, \alpha^{(p^m-2t)}, \alpha^{[p^m-(2t-1)]}, \alpha^{[p^m-(2t-2)]}, \cdots, \alpha^{(p^m-3)}, \alpha^{p^m-2}\}.$$

Seja C_2 o código *Reed-Solomon* gerado pelo polinômio

$$g_2(x) = (x-1)(x-\alpha)\cdots(x-\alpha^{(\lceil\sqrt{d}\rceil)})\cdots(x-\alpha^{(p^m-2t-3)}).$$

Por construção, temos que $C_2 \subset C_1$. Além disso, os parâmetros do código C_2 são dados por

$$[p^m-1,\ 2t+1,\ p^m-2t-1]_{p^m}.$$

Conseqüentemente, os parâmetros do código $C_2 \otimes C_2$ são dados por

$$C_2 \otimes C_2 = [(p^m-1)^2,\ (2t+1)^2,\ (p^m-2t-1)^2]_{p^m}.$$

O terceiro passo da construção generalizada é dado a seguir.

Considere o código produto $(C_2 \otimes C_2)^{\perp}$. Pelo Teorema 5.1.2, este código tem parâmetros

$$(C_2 \otimes C_2)^{\perp} = [(p^m-1)^2,\ p^{2m}-2p^m-4t^2-4t,\ 2t+1]_{p^m}.$$

Demonstraremos, agora, o Lemma 5.2.1, que afirma sobre a veracidade da inclusão $C_2 \otimes C_2 \subset C_1 \otimes C_1$, requerida para a construção dos códigos *CSS*.

Lema 5.2.1 *Sejam C_1 e C_2 dois códigos clássicos lineares com parâmetros $[n, k_1, d_1]_{p^m}$ e $[n, k_2, d_2]_{p^m}$, respectivamente, tal que $C_2 \subset C_1$. Então, o código produto $C_1 \otimes C_1$ contém o código $C_2 \otimes C_2$.*

Demonstração: Seja $C_1 = \langle g_1(X)\rangle$. Como $C_2 \subset C_1$, existe um polinômio $b(X)$ tal que $C_2 = \langle b(X)g_1(X)\rangle$. Pelo Teorema 5.1.1, o código $C_1 \otimes C_1$ é o código bicíclico gerado pelo polinômio $\langle p_1(X,Y)\rangle = \langle g_1(X)g_1(Y)\rangle$. Além disso, aplicando novamente o Teorema 5.1.1, temos o código bicíclico $C_2 \otimes C_2$, gerado pelo polinômio $\langle p_2(X,Y)\rangle = \langle b(X)g_1(X)b(Y)g_1(Y)\rangle$.

Como o polinômio $p_1(X,Y)$ divide o polinômio $p_2(X,Y)$, vale a inclusão $C_2 \otimes C_2 \subset C_1 \otimes C_1$. □

Combinando todos esses fatos, obtém-se ferramentas necessárias para a demonstração do resultado principal deste capítulo, a saber, o Teorema 5.2.1.

Teorema 5.2.1 *Sejam* $C_1 = [p^m - 1, p^m - (\lceil\sqrt{d}\rceil), \lceil\sqrt{d}\rceil]_{p^m}$ *e* $C_2 = [p^m - 1, 2t + 1, p^m - 2t - 1]_{p^m}$ *códigos* Reed-Solomon *clássicos construídos anteriormente. Considere os códigos produto*

$$C_1 \otimes C_1 = [(p^m - 1)^2, (p^m - \lceil\sqrt{d}\rceil)^2, (\lceil\sqrt{d}\rceil)^2]_{p^m},$$

$$C_2 \otimes C_2 = [(p^m - 1)^2, (2t + 1)^2, (p^m - 2t - 1)^2]_{p^m}$$

e

$$(C_2 \otimes C_2)^{\perp} = [(p^m - 1)^2, p^{2m} - 2p^m - 4t^2 - 4t, 2t + 1]_{p^m}.$$

Então, os códigos quânticos $CSS(C_1 \otimes C_1, C_2 \otimes C_2)$ *possuem parâmetros* $[[(p^m - 1)^2, (p^m - \lceil\sqrt{d}\rceil)^2 - (2t + 1)^2, D \geq 2t + 1]]_{p^m}$, *taxa* $p^{2m} - 2p^m d/(p^m - 1)^2$ *e corrigem erros quânticos arbitrários em* t *qudits, para todo* $t \geq 2$.

Demonstração: Aplique o Teorema 5.1.2 e todas as construções realizadas anteriormente. □

Façamos, agora, um sumário do processo de construção.

Passo 1) Escolha um número primo p apropriado.

Passo 2) Construa os códigos clássicos *Reed-Solomon* q-ários, ($q = p^m$, p primo) C_1 e C_2 sobre o corpo F_{p^m}, onde m é o menor número natural satisfazendo a desigualdade $p^m \geq \lceil\sqrt{2t+1}\rceil + 2t + 2$.

Passo 3) Construa os códigos clássicos q-ários $C_1 \otimes C_1$, $C_2 \otimes C_2$ e $(C_2 \otimes C_2)^{\perp}$.

Passo 4) Aplique a construção dos códigos *CSS*.

Observação 5.2.1 *Baseado neste método de construção sendo proposto, podemos deduzir que o Teorema 5.2.1 pode ser generalizado, se considerarmos o produto de n códigos* Reed-Solomon ${C_1}^{\otimes n}$ *e também o produto de n códigos* Reed-Solomon ${C_2}^{\otimes n}$*, onde n são os números* $\{2, 4, 8, \cdots\}$*. Isto significa que devemos considerar somente os casos* $C_1 \otimes C_1$*,* $(C_1 \otimes C_1) \otimes (C_1 \otimes C_1)$*,* $(C_1 \otimes C_1) \otimes (C_1 \otimes C_1) \otimes (C_1 \otimes C_1) \otimes (C_1 \otimes C_1)$*,* $\cdots$*, pois somente nestes casos podemos aplicar o Teorema 5.1.2.*

Estabelecemos o Teorema 5.2.2, que é a generalização do Teorema 5.2.1. Para simplificar a notação consideraremos o caso de se ter apenas dois produtos tensoriais dos códigos C_1 e C_2.

Escolha um número primo p apropriado. A seguir, encontre um o menor natural m que satisfaça a condição

$$p^m \geq \lceil \sqrt[4]{2t+1} \rceil + 1 + 2t + 1 = \lceil \sqrt{2t+1} \rceil + 2t + 2,$$

onde $\lceil y \rceil$, $y \in \mathbb{R}$, denota o menor número inteiro maior ou igual a y.

Teorema 5.2.2 *Sejam*

$$C_1 \otimes C_1 = [(p^m - 1)^2, [p^m - (\lceil \sqrt{d} \rceil)]^2, (\lceil \sqrt{d} \rceil)^2]_{p^m}$$

e

$$C_2 = [(p^m - 1)^2, (2t+1)^2, (p^m - d)^2]_{p^m}$$

códigos produto derivados dos códigos RS*. Considere os códigos produto*

$$(C_1 \otimes C_1) \otimes (C_1 \otimes C_1) = [(p^m - 1)^4, (p^m - \lceil \sqrt{d} \rceil)^4, (\lceil \sqrt{d} \rceil)^4]_{p^m},$$

$$(C_2 \otimes C_2) \otimes (C_2 \otimes C_2) = [(p^m - 1)^4, (2t+1)^4, (p^m - 2t - 1)^4]_{p^m}$$

e

$$(C_2 \otimes C_2) \otimes (C_2 \otimes C_2)^{\perp}$$
$$= [(p^m - 1)^4, (2p^m - 1)(p^m - d)^2 - 2p^m - 1, p^m - (p^m - d)^2]_{p^m}.$$

Então, o código quântico $CSS({C_1}^{\otimes 4}, {C_2}^{\otimes 4})$ *construído desta forma possui parâmetros*

$$[[(p^m - 1)^4, (p^m - \lceil \sqrt{d} \rceil)^4 - (2t+1)^4, D \geq p^m - (p^m - d)^2]]_{p^m}$$

e corrige erros quânticos arbitrários em $\min\{p^m - (p^m - d)^2, (\lceil \sqrt{d} \rceil)^4\}$ *qudits.*

Demonstração: Veja a Observação 5.2.1. □

A seguir, são apresentados alguns exemplos para ilustrar a construção proposta.

Exemplo 5.2.1 *(*CSS *que corrige erros quânticos arbitrários em* 4 *qubits) Escolha* $p = 5$. *Calculando o valor de* m, *temos que* $\lceil\sqrt{2t+1}\rceil + 2t + 2 = 13 \leq 5^2$. *Disso segue que os códigos* C_1 *e* C_2 *serão construídos sobre o corpo* F_{5^2} *e terão comprimento* 24.

Seja α *um elemento primitivo do corpo* F_{5^2} *e considere*

$$C_1 = \langle g_1(x)\rangle = (x-1)(x-\alpha)$$

e

$$C_2 = \langle g_2(x)\rangle = (x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)\cdots(x-\alpha^{14}).$$

Sejam $C_1 \otimes C_1$, $C_2 \otimes C_2$ *e* $(C_2 \otimes C_2)^{\perp}$ *os códigos produto com parâmetros*

$$C_1 \otimes C_1 = [24^2, 22^2, 3^2]_{25},$$

$$C_2 \otimes C_2 = [24^2, 9^2, 16^2]_{25}$$

e

$$(C_2 \otimes C_2)^{\perp} = [24^2, 25(2.16-2) - 16^2 + 1, 9]_{25}.$$

Pelo Teorema 5.2.1, o código resultante $CSS(C_1 \otimes C_1,\ C_2 \otimes C_2)$ *possui parâmetros* $[[576, 403, 9]]_{25}$ *e corrige erros quânticos arbitrários em* 4 *qudits.*

Exemplo 5.2.2 *(*CSS *que corrige erros quânticos arbitrários em* 6 *qudits) Escolha* $p = 3$. *Calculando o valor de* m, *segue que* $\lceil\sqrt{2t+1}\rceil + 2t + 2 = 18 \leq 3^3$. *Assim, os códigos* C_1 *e* C_2 *serão construídos sobre o corpo* F_{3^3} *e terão comprimento* 26.

Seja α *um elemento primitivo do corpo* F_{3^3} *e considere*

$$C_1 = \langle g_1(x)\rangle = (x-1)(x-\alpha)(x-\alpha^2)$$

e

$$C_2 = \langle g_2(x)\rangle = (x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)\cdots(x-\alpha^{12}).$$

Considere os códigos produto

$$C_1 \otimes C_1 = [676, 529, 16]_{27},$$

$$C_2 \otimes C_2 = [676, 169, 225]_{27}$$

e

$$(C_2 \otimes C_2)^{\perp} = [676, 507, 13]_{27}.$$

Então, pelo Teorema 5.2.1, temos que o código quântico $CSS(C_1 \otimes C_1, C_2 \otimes C_2)$ *possui parâmetros* $[[676, 360, 13]]_{27}$ *e corrige erros quânticos arbitrários em* 6 *qudits.*

Exemplo 5.2.3 *(*CSS *que corrige erros quânticos arbitrários em* 8 *qudits) Escolha* $p = 2$. *Um possível valor para o número* m *é* $\lceil\sqrt{2t+1}\rceil + 2t + 2 = 23 \leq 2^5$.

Sabemos que os códigos C_1 *e* C_2 *serão construídos sobre o corpo* F_{2^5}. *O comprimento da palavra-código é* 31. *Considere os códigos*

$$C_1 = \langle g_1(x)\rangle = (x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)$$

e

$$C_2 = \langle g_2(x)\rangle = (x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)\cdots(x-\alpha^{13}).$$

Considere também os códigos

$$C_1 \otimes C_1 = [961, 729, 25]_{32},$$

$$C_2 \otimes C_2 = [961, 289, 225]_{32}$$

e

$$(C_2 \otimes C_2)^{\perp} = [961, 672, 17]_{32}.$$

Pelo Teorema 5.2.1, o código $CSS(C_1 \otimes C_1, C_2 \otimes C_2)$ *possui parâmetros* $[[961, 440, 17]]_{32}$ *e corrige erros quânticos arbitrários em* 8 *qudits.*

5.3 Parâmetros dos Novos Códigos *CSS*

Na Tabela 5.1, n é o comprimento da palavra-código do código quântico *CSS*, k é a dimensão, d_{min} é a distância mínima e t é o número de qudits que o código *CSS* é capaz de corrigir.

n	k	d_{min}	t
576	403	9	4
676	360	13	6
961	440	17	8

Tabela 5.1: Parâmetros de Códigos Construídos pelo Método Proposto

5.4 Considerações Finais

Neste capítulo, foi construída uma nova família de códigos quânticos *CSS* baseados no produto tensorial de códigos *Reed-Solomon*. Destacamos que esses códigos são facilmente construídos. Essa família de códigos *CSS* não possui taxa de codificação k/n alta, devido ao fato do comprimento da palavra-código crescer muito rapidamente à medida que se aplica o produto tensorial dos códigos clássicos envolvidos no processo de construção do código *CSS*. Entretanto, podemos utilizar tais códigos no caso de processos quânticos que necessitem de proteção desigual aplicados aos qudits.

Capítulo 6

Códigos Cíclicos MDS Clássicos e Quânticos

A classe dos códigos MDS (máxima distância de separação) é uma classe importante e amplamente estudada, pois a distância mínima de tais códigos é máxima. As famílias mais conhecidas de códigos MDS clássicos e quânticos são as famílias de códigos *Reed-Solomon* e *Reed-Solomon* estendidos (veja [33, 35, 36]).

Os códigos cíclicos são exaustivamente estudados na literatura não somente no caso clássico bem como no caso quântico, veja, por exemplo, [4, 6, 7, 13, 16, 19, 20, 29, 30, 37–44].

A maioria dos trabalhos disponíveis na literatura tratam da existência de certas famílias de códigos clássicos (quânticos) MDS. Mais precisamente, para o caso clássico é bem conhecido que existem códigos cíclicos MDS, sobre F_q, com parâmetros $[q+1, k, q-k+2]$, para todo k, onde $1 \leq k \leq q+1$, [33]. Em [44], Roth e Seroussi provam que um código cíclico C, de comprimento q, sobre o corpo F_q, é um código MDS se, e somente se, q é um número primo, e nesse caso C é equivalente, a menos de permutações de coordenadas, a um código Reed-Solomon estendido; ou C é um código trivial de dimensão $k \in \{1, q-1, q\}$. Então, existe um código cíclico não-trivial *Reed-Solomon* estendido, de comprimento q, sobre F_q se, e somente se, q é um número primo. Em [45], Georgiades prova que se n, onde n é um divisor de $q+1$, for um número par, então códigos cíclicos MDS com parâmetros $[n, k]$ não existem se k é par.

No caso quântico, os trabalhos mais relevantes são [27] e [29]. Em [27], Grassl, Beth e Rötteler construíram códigos quânticos MDS com parâmetros $[[n, n-2d+2, d]]_q$, para todo $3 \leq n \leq q+1$ e $1 \leq d \leq n/2+1$, onde q é uma potência de primo. Em [29], Sarvepalli e Klappenecker fornecem uma resposta parcial sobre a existência de códigos quânticos q-ários MDS de comprimento n, onde $q \leq n \leq q^2-1$, por meio da construção *CSS*, utilizando, para isso, códigos clássicos *Reed-Muller* generalizados. Todos os trabalhos disponíveis na literatura tratam da existência e construção de tais códigos.

Neste capítulo, propomos novos critérios que possibilitam caracterizar códigos clássicos

(quânticos) cíclicos MDS. Desta forma, generalizamos as construções anteriores, não somente para o caso clássico mas também para o caso quântico.

No caso clássico, provamos que, se a união das classes laterais ciclotômicas de um determinado código cíclico, denominada conjunto de definição, é igual a uma seqüência de $d-1$ números inteiros positivos consecutivos, então C é MDS e possui distância mínima igual a d.

Para o caso quântico, provamos um resultado análogo: dado um código quântico cíclico $CSS(C_1, C_2)$, se o conjunto de definição do código C_1 e do código ${C_2}^{\perp}$ são iguais a conjuntos de seqüências disjuntas de números inteiros não-negativos consecutivos com $d-1$ elementos cada, e se é adicionada uma hipótese conveniente, então o código quântico $CSS(C_1, C_2)$ é MDS com distância mínima igual a d. Reciprocamente provamos que, se um código clássico cíclico C é MDS com distância mínima d, então seu conjunto de definição possui exatamente $d-1$ elementos. Além disso, para o caso quântico, demonstraremos que, se $CSS(C_1, C_2)$ é MDS com distância mínima D e adicionando uma hipótese conveniente, então cada conjunto de definição dos códigos C_1 e ${C_2}^{\perp}$ possui exatamente $D-1$ elementos.

O objetivo deste capítulo é propor novos critérios para classificar códigos clássicos (quânticos) cíclicos MDS. Reciprocamente, dado um código quântico (clássico) cíclico MDS, podemos determinar a cardinalidade do conjunto de definição. Além disso, demonstramos um análogo quântico ao Teorema do Limitante do *BCH* para códigos cíclicos *CSS*.

O capítulo está organizado como segue. Na Seção 6.1, apresentamos nossas contribuições para o caso clássico. Mais especificamente, fornecemos condições sob as quais um código cíclico se torna MDS. Reciprocamente, calculamos o número de elementos do conjunto de definição dos códigos clássicos cíclicos MDS. Na Seção 6.2, apresentamos nossas contribuições para o caso quântico: estabelecemos condições para que um código cíclico quântico seja um código MDS. Da mesma forma que no caso clássico, calculamos o número de elementos do conjunto de definição dos códigos quânticos cíclicos MDS. Ainda, generalizamos o Teorema do Limitante do *BCH* para códigos quânticos cíclicos *CSS*. As considerações finais do capítulo estão contidas na Seção 6.3.

6.1 Códigos Clássicos Cíclicos MDS

Nesta seção, apresentamos nossas contribuições para o caso clássico. O resultado principal dessa seção é o Teorema 6.1.2. Este afirma que, se o conjunto de definição de um código cíclico C é igual a uma seqüência de $d-1$ números inteiros não-negativos consecutivos, então C é um código MDS com distância mínima igual a d.

Descrevemos abaixo, o Teorema do Limitante de Singleton (clássico), que é válido para todo código linear sobre qualquer corpo.

Teorema 6.1.1 *[33](Limitante Clássico de Singleton) Se C é um código $[n, k, d]$, então $d \leq n - k + 1$.*

Segue a definição dos códigos MDS.

Definição 6.1.1 *[33] Seja C um código clássico com parâmetros $[n, k, d]$. Se C atinge o limitante de Singleton, i. e., $d = n - k + 1$, então C é denominado código com máxima distância de separação, ou código MDS.*

Aqui, apresentamos o resultado principal dessa seção, a saber, o Teorema 6.1.2. Denotaremos por $M^{(i_j)}$, $j = 1, \cdots, r$, o conjunto dos polinômos minimais de $\alpha^j \in F_{p^m}$, onde α é um elemento primitivo do corpo em questão.

Teorema 6.1.2 *(Códigos MDS Clássicos) Seja p um número primo e $C = [n = p^m - 1, k, d^*]$ o código cíclico gerado pelo produto dos polinômios minimais dados por $g(x) = M^{(i_1)}(x)M^{(i_2)}(x)\cdots M^{(i_r)}(x)$. Além disso, sejam $x_k \geq 0$ números inteiros não-negativos tais que $x_{k+1} = x_k + 1$, para todo $1 \leq k \leq d - 1$, e $\mathbb{C}_s$ as classes laterais ciclotômicas com representantes $s \in S$, onde $S = \{i_1, i_2, \cdots, i_r\}$. Se $\bigcup_{s\in S} \mathbb{C}_s = \{x_k\}_{k=1}^{d-1}$, então C é MDS e $d = d^*$.*

Demonstração: Observe que é suficiente demonstrar que as equações $d^* = d$ e $d = n-k+1$ são verdadeiras, i. e., o código atinge o limitante de Singleton.

Seja $C = [p^m - 1, k, d^*]$ o código cíclico gerado pelo polinômio

$$g(x) = M^{(i_1)}(x)M^{(i_2)}(x)\cdots M^{(i_r)}(x),$$

onde $M^{(i_j)}(x)$ são os respectivos polinômios minimais dos elementos $\alpha^j \in F_{p^m}$. Note que, por hipótese, existe um elemento primitivo α. Além disso, considere $\mathbb{C}_s$ a classe ciclotômica onde s é seu respectivo representante. É bem conhecido que, se $i \in \mathbb{C}_s$ então

$$M^{(i)}(x) = \prod_{j\in C_s} (x - \alpha^j). \tag{6.1}$$

Pela equação (6.1), deduzimos que o número total de elementos na união das classes ciclotômicas (conjunto de definição), do código cíclico $C = \langle g(x)\rangle$, é igual ao grau do polinômio $g(x)$.

De fato, como os números $n = p^m - 1$ e p são relativamente primos, todas as raízes do polinômio $x^{p^m-1} - 1$ são distintas. Conseqüentemente, existe uma bijeção entre as potências

do elemento primitivo α (do corpo F_{p^m}) e os elementos α^i, $1 \leq i \leq p^m - 2$, dada por $i \longrightarrow \alpha^i$. Como todos os polinômios da forma $x - \alpha^j$ na equação (6.1) possuem grau 1, e como as classes ciclotômicas são disjuntas, concluímos que o número total de elementos no conjunto de definição do código $C = \langle g(x) \rangle$ é igual ao grau do polinômio $g(x)$.

Retornando à demonstração, observe que, por hipótese

$$\bigcup_{s \in S} \mathbb{C}_s = \{x_k\}_{k=1}^{d-1}.$$

Assim, temos que

$$\partial(g(x)) = \mid \bigcup_{s \in S} \mathbb{C}_s \mid = d - 1,$$

onde $\mid . \mid$ denota a cardinalidade do conjunto. Ainda, a dimensão k do código C é igual a $k = n - r$, onde $r = \partial(g(x))$. Então $k = n - (d - 1)$.

Considere o Teorema do Limitante de Singleton:

$$d^* \leq n - k + 1.$$

Substituindo os valores encontrados previamente, deduzimos que

$$n - k + 1 = n - [n - (d - 1)] + 1 = d$$

e assim, segue que $d^* \leq d$.

De outra forma, como C é um código cíclico, pelo Teorema do Limitante do *BCH* e por hipótese, sabemos que $d^* \geq d$, donde $d^* = d$. Como $d^* = d$ e $n - k + 1 = d$, concluímos que

$$d^* = n - k + 1.$$

Conseqüentemente, o código C é MDS e $d = d^*$, demonstrando o resultado. □

O Teorema 6.1.2 é uma ferramenta útil na procura por códigos cíclicos MDS. Em seguida, provamos alguns corolários do Teorema 6.1.2.

Corolário 6.1.1 *Suponha que sejam válidas todas as hipóteses do Teorema 6.1.2. Então o código $C^\perp$ é MDS.*

Corolário 6.1.2 *Seja $C = [N = p^m - 1, K, D]$ um código Reed-Solomon. Então $C = [N = p^m - 1, K, D]$ é MDS.*

Tabela 6.1: Classes laterais sobre a multiplicação por 32 módulo 33

{ 0}	
{ 1, 32 }	{ 9, 24 }
{ 2, 31 }	{ 10, 23 }
{ 3, 30 }	{ 11, 22 }
{ 4, 29 }	{ 12, 21 }
{ 5, 28 }	{ 13, 20 }
{ 6, 27 }	{ 14, 19 }
{ 7, 26 }	{ 15, 18 }
{ 8, 25 }	{ 16, 17 }

Demonstração: Seja $C = [N = p^m - 1, K, D]$ um código Reed-Solomon. Sabemos que todas as classes ciclotômicas dos códigos Reed-Solomon contêm exatamente um elemento. Como tais códigos possuem $D-1$ classes ciclotômicas e como o conjunto de definição possui uma seqüência de $D-1$ números inteiros não negativos consecutivos, concluímos que

$$\bigcup_{s \in S} \mathbb{C}_s = \{y_k\}_{k=1}^{D-1},$$

onde $y_k \geq 0$ e $y_{k+1} = y_k + 1$, para todo $1 \leq k \leq D-1$. Aplicando o Teorema 6.1.2, segue que o código $C = [N = p^m - 1, K, D]$ é MDS. □

Corolário 6.1.3 *Os códigos MDS construídos em [44] satisfazem as hipóteses do Teorema 6.1.2, e assim essas famílias de códigos MDS são casos particulares dos códigos gerados pelo Teorema 6.1.2.*

Exemplo 6.1.1 *Considere as classes laterais sobre a multiplicação por 2^m módulo $2^m + 1$. Se $2^m + 1 = 33$, as classes laterais são dadas na Tabela 6.1. Construa códigos cíclicos tendo respectivos conjuntos de definição dados por: $D_1 = \mathbb{C}_{15} \cup \mathbb{C}_{16}$, $D_2 = \mathbb{C}_{14} \cup \mathbb{C}_{15} \cup \mathbb{C}_{16}$, $D_3 = \mathbb{C}_{13} \cup \mathbb{C}_{14} \cup \mathbb{C}_{15} \cup \mathbb{C}_{16}$, $D_4 = \mathbb{C}_{12} \cup \mathbb{C}_{13} \cup \mathbb{C}_{14} \cup \mathbb{C}_{15} \cup \mathbb{C}_{16}$, etc. Como esses conjuntos de definição satisfazem as hipóteses do Teorema 6.1.2, concluímos que tais códigos cíclicos são MDS.*

A distância de projeto é um parâmetro útil de um código cíclico, pois é um limitante inferior para a distância mínima real de tais códigos. Embora seja um parâmetro útil, geralmente este não coincide com a valor da distância mínima real. Por essa razão, não podemos provar a recíproca do Teorema 6.1.2. De qualquer modo, demonstramos uma variação mais fraca para a recíproca desse teorema.

Teorema 6.1.3 *Assim como no Teorema 6.1.2, seja p primo e considere* $C = [n = p^m - 1, k, d]$ *o código cíclico gerado pelo produto dos polinômios minimais*

$$g(x) = M^{(i_1)}(x)M^{(i_2)}(x)\cdots M^{(i_r)}(x).$$

Se C é MDS, então seu conjunto de definição $\bigcup_{s\in S} \mathbb{C}_s$ *contém exatamente* $d-1$ *elementos.*

Demonstração: Por hipótese, sabemos que

$$d = n - k + 1, \tag{6.2}$$

ou seja, o código atinge o limitante de Singleton. Além disso, como C é um código cíclico, segue que $k = n - \partial(g(x))$.

Substituindo os valores da dimensão k na equação (6.2), concluímos que $\partial(g(x)) = d-1$. Ainda, pela equação (6.1) e se raciocinarmos como na demonstração do Teorema 6.1.2, verificamos que o conjunto $\bigcup_{s\in S} \mathbb{C}_s$ contém exatamente $d-1$ elementos. □

Observação 6.1.1 *Ressaltamos que os Teoremas 6.1.2 e 6.1.3 também são válidos se substituirmos o valor* $n = p^m - 1$ *por um valor de* n^* *o qual é relativamente primo com q; neste caso o corpo considerado é o corpo* F_q*. Além disso, se o corpo* F_{q^m} *é o corpo de decomposição do polinômio* $x^n - 1$*, então os Teoremas 6.1.2 e 6.1.3 também são válidos. De fato, podemos demonstrar tais afirmações pelos mesmos métodos adotados anteriormente na demonstração do Teorema 6.1.2.*

6.2 Códigos Quânticos Cíclicos MDS

As principais contribuições dessa seção são os Teoremas 6.2.2, 6.2.3 e 6.2.5. Mais explicitamente, os Teoremas 6.2.2 e 6.2.5 produzem critérios para que os códigos quânticos cíclicos se tornem códigos MDS, e o Teorema 6.2.3 é uma generalização do Teorema do Limitante do *BCH* para códigos *CSS* cíclicos quânticos.

O limitante quântico de Singleton e a definição de códigos quânticos MDS são descritos na seqüência:

Teorema 6.2.1 *[27](Limitante Quântico de Singleton) Se C é um código quântico* $[[n, k, d]]_q$*, então* $k + 2d \leq n + 2$.

Definição 6.2.1 *[27] Seja* $C = [[n, k, d]]_q$ *um código quântico. Se C atinge o limitante quântico de Singleton, i. e.,* $k + 2d = n + 2$*, C é denominado código quântico com máxima distância de separação ou código MDS. Assim, os códigos MDS possuem parâmetros* $[[n, n - 2d + 2, d]]_q$.

Provaremos, agora, o Teorema 6.2.2, que é uma versão similar do Teorema 6.1.2. No Teorema 6.2.2 utilizamos a mesma notação que a adotada no Teorema 6.1.2: $\bigcup_{s_1 \in S_1} \mathbb{C}_{s_1}$ e $\bigcup_{s_2{}^{\perp} \in S_2{}^{\perp}} \mathbb{C}_{s_2{}^{\perp}}$ são os conjuntos de definição dos códigos C_1 e $C_2{}^{\perp}$, respectivamente.

Considere $q = p^m$, p primo e $\mathrm{mdc}(n, p) = 1$, i. e., n e p são relativamente primos, onde n é o comprimento da palavra-código. Suponha que $C_1 = [n, k_1, d_1]_q$ e $C_2 = [n, k_2, d_2]_q$ sejam códigos cíclicos clássicos. Além disso, assuma que $C_2 \subset C_1$. É bem conhecido o fato de que é possível gerar códigos quânticos através da construção $CSS(C_1, C_2)$ baseada em dois códigos lineares clássicos C_1 e C_2. Motivados por essa classe de códigos, que é a classe mais estudada dentre as classes de códigos quânticos, definimos o que será entendido neste trabalho, por códigos quânticos cíclicos:

Definição 6.2.2 *Sejam $C_1 = [n, k_1, d_1]_q$ e $C_2 = [n, k_2, d_2]_q$ códigos cíclicos clássicos tais que $C_2 \subset C_1$. Então, o código quântico $CSS(C_1, C_2)$ com parâmetros $[[n, k_1 - k_2, D]_q$, onde D é dado pela construção* CSS*, será denominado código cíclico quântico.*

Baseado em todas essas asserções, estamos aptos a demonstrar o Teorema 6.2.2. No Teorema 6.2.2 consideramos o conjunto A como sendo o conjunto $A = (C_1 \backslash C_2) \cup (C_2{}^{\perp} \backslash C_1{}^{\perp})$.

Teorema 6.2.2 *(Códigos MDS Quânticos) Seja $CSS(C_1, C_2)$ um código quântico cíclico construído através de dois códigos clássicos cíclicos $C_1 = [n = p^m - 1, k_1, d_1]$ e $C_2{}^{\perp} = [n = p^m - 1, k_2{}^{\perp}, d_2{}^{\perp}]$, onde C_1 e $C_2{}^{\perp}$ são gerados pelos polinômios $g_1(x)$ e $g_2{}^{\perp}(x)$, respectivamente, como no Teorema 6.1.2. Ainda, suponha que $x_k \geq 0$ e $y_j \geq 0$ sejam números inteiros tais que $x_{k+1} = x_k + 1$, para todo $1 \leq k \leq d - 1$, e $y_{j+1} = y_j + 1$, para todo $1 \leq j \leq d - 1$, onde esses conjuntos, a saber, $\{x_k\}_{k=1}^{d-1}$ e $\{y_j\}_{j=1}^{d-1}$ são disjuntos. Suponha também que exista uma palavra-código $c \in A$ tal que $wt(c) = d$. Se $\bigcup_{s_1 \in S_1} \mathbb{C}_{s_1} = \{x_k\}_{k=1}^{d-1}$, e se $\bigcup_{s_2{}^{\perp} \in S_2{}^{\perp}} \mathbb{C}_{s_2{}^{\perp}} = \{y_j\}_{j=1}^{d-1}$, então $CSS(C_1, C_2)$ é um código quântico MDS com parâmetros $[[n = p^m - 1, K = k_1 - k_2, d]]$, onde $k_2 = n - k_2{}^{\perp}$.*

Demonstração: Para provar que o código $CSS(C_1, C_2)$ é MDS com parâmetros dados na hipótese do teorema, utilizaremos basicamente o Teorema 6.1.2.

A idéia principal desta demonstração é aplicar o Teorema 6.1.2 para os códigos cíclicos C_1 e $C_2{}^{\perp}$. Identificaremos o código dual $C_2{}^{\perp}$ com o dual do código cíclico $C_2 = \langle g_2(x) \rangle$, gerado pelo polinômio

$$g_2(x) = (x^{p^m - 1} - 1)/g_2{}^{\perp}(x).$$

Suponha que $n = p^m - 1$, onde p é um número primo. Considere o código C_1. Note que, por hipótese, podemos garantir, baseados no Teorema 6.1.2, que o código clássico C_1 é MDS com parâmetros $C_1 = [n, k_1 = n - d + 1, d]$. Por outro lado, aplicando novamente o Teorema 6.1.2 ao código ${C_2}^{\perp}$, verificamos que este código também é MDS com parâmetros ${C_2}^{\perp} = [n, {k_2}^{\perp} = n - d + 1, d]$.

Seja C_2 o código gerado pelo polinômio

$$g_2(x) = (x^{p^m-1} - 1)/{g_2}^{\perp}(x).$$

É claro que C_2 é cíclico. Por definição, concluímos que este possui parâmetros dados por

$$C_2 = [n, k_2 = n - {k_2}^{\perp}, d_2].$$

Sabemos que

$$k_1 = n - d + 1 \tag{6.3}$$

e

$${k_2}^{\perp} = n - d + 1. \tag{6.4}$$

Considere esses três códigos C_1, C_2 e ${C_2}^{\perp}$. Por hipótese, sabemos que os conjuntos $\{x_k\}_{k=1}^{d-1}$ e $\{y_j\}_{j=1}^{d-1}$ são disjuntos. Logo, os códigos C_1 e ${C_2}^{\perp}$ não possuem raízes comuns. Pela construção *CSS*, segue que $C_2 \subset C_1$. Por conveniência, podemos supor que o corpo em que os códigos estão sendo construídos tenha cardinalidade suficientemente grande, donde $C_2 \subsetneqq C_1$. Além disso, aplicando novamente o Teorema 6.1.2 aos códigos C_1 e ${C_2}^{\perp}$, concluímos que ambos possuem distâncias mínimas iguais a d.

Provaremos, agora, que o código quântico $CSS(C_1, C_2)$ é MDS, i. e., que este atinge o limitante de Singleton $K = n - 2D + 2$, onde D é a distância mínima do código $CSS(C_1, C_2)$.

Primeiramente, observe que por hipótese, existe uma palavra-código $c \in A$ tal que $wt(c) = d$. Então, d é o menor valor para os pesos das palavras-código contidas no conjunto $A = (C_1 \backslash C_2) \cup ({C_2}^{\perp} \backslash {C_1}^{\perp})$. Como a distância mínima D de $CSS(C_1, C_2)$ é $D = \min\{wt(c) \mid c \in A\}$, deduzimos que $D \leq d$. Por outro lado, como d é o menor valor para os pesos das palavras-código contidas no conjunto A, segue que $d \leq D$, donde $D = d$.

Verificaremos que o código $CSS(C_1, C_2)$ satisfaz a igualdade no Teorema do Limitante (quântico) de Singleton. De fato, pela equação (6.4) e como $D = d$, sabemos que

$$k_2 = n - {k_2}^{\perp} = n - (n - d + 1) = d - 1.$$

Assim, segue que

$$K = k_1 - k_2 = n - d + 1 - (d - 1) = n - 2d + 2,$$

donde $K = n - 2d + 2$. Conseqüentemente, o código $CSS(C_1, C_2)$ é MDS com parâmetros

$$[[n = p^m - 1, K = k_1 - k_2, d]].$$

□

Observação 6.2.1 *Assim como no caso clássico, ressaltamos que o Teorema 6.2.2 também é válido se substituírmos $n = p^m - 1$ por um número inteiro n^* relativamente primo com p. Ainda, se o corpo F_{q^m} é o corpo de decomposição do polinômio $x^n - 1$, então o Teorema 6.2.2 também é válido. De fato, tais asserções são facilmente verificadas pelo mesmo método utilizado na demonstração do Teorema 6.2.2.*

Corolário 6.2.1 *Seja $\mathcal{C} = [[N = p^m - 1, K, D]]_q$ um código Reed-Solomon quântico gerado pelo método proposto do Capítulo 2. Então $\mathcal{C}$ é um código MDS.*

Demonstração: Pelo método de construção proposto do Capítulo 2, verificamos diretamente que os conjuntos de definição dos códigos C_1 e ${C_2}^{\perp}$, respectivamente, são disjuntos e dados por

$$\bigcup_{s_1 \in S_1} \mathbb{C}_{s_1} = \{x_k\}_{k=1}^{d-1}$$

e

$$\bigcup_{s_2{}^{\perp} \in S_2{}^{\perp}} \mathbb{C}_{s_2{}^{\perp}} = \{y_j\}_{j=1}^{d-1}.$$

Assim, aplicando o Teorema 6.2.2, concluímos o resultado. □

Assumiremos, ao longo deste capítulo, que os conjuntos de definição dos códigos C_1 e ${C_2}^{\perp}$ são disjuntos e que α é um elemento primitivo do corpo F_q.

O Teorema 2.1.5 (Limitante do *BCH*) é uma ferramenta poderosa para se calcular um limitante inferior para a distância mínima de um código cíclico. Assim, como no caso clássico, provaremos um teorema análogo ao Teorema 2.1.5 para o caso de códigos cíclicos quânticos *CSS*.

Teorema 6.2.3 *(Teorema do Limitante do* BCH *Quântico) Seja $CSS(C_1, C_2)$ um código cíclico quântico com parâmetros $[[N, K, D]]_q$. Assuma que o código C_1 possua uma seqüência de $\delta_1 - 1$ potências de α como zeros, e que o código ${C_2}^{\perp}$ possua uma seqüência de ${\delta_2}^{\perp} - 1$ potências de α como zeros. Então, a distância mínima D do código quântico $CSS(C_1, C_2)$ é, no mínimo,* $\min\{\delta_1, {\delta_2}^{\perp}\}$.

Demonstração: Sejam d_1 e ${d_2}^{\perp}$ as respectivas distâncias mínimas dos códigos cíclicos C_1 e ${C_2}^{\perp}$. Então, pelo Teorema (clássico) do Limitante do *BCH*, segue que

$$d_1 \geq \delta_1; \qquad {d_2}^{\perp} \geq {\delta_2}^{\perp}.$$

Pela construção *CSS*, sabemos que

$$D = \min\{wt(c) \mid c \in (C_1 \backslash C_2) \cup ({C_2}^{\perp} \backslash {C_1}^{\perp})\}.$$

Analisemos essa situação.

Se $c \in (C_1 \backslash C_2)$, então $wt(c) \geq d_1$. De outra forma, se $c \in ({C_2}^{\perp} \backslash {C_1}^{\perp})$, temos que $wt(c) \geq {d_2}^{\perp}$. Sabemos que $D \geq \min\{d_1, {d_2}^{\perp}\}$. Como são válidas as desigualdades $d_1 \geq \delta_1$ e ${d_2}^{\perp} \geq {\delta_2}^{\perp}$, segue que

$$D \geq \min\{\delta_1, {\delta_2}^{\perp}\},$$

concluindo a demonstração. □

Teorema 6.2.4 *(A Dimensão do Código Cíclico Quântico* CSS*) Seja $CSS(C_1, C_2)$ um código cíclico quântico com parâmetros $[[N, K, D]]_q$, onde $C_1 = [N, k_1, d_1]_q$ e $C_2 = [N, k_2, d_2]_q$ são os códigos cíclicos clássicos utilizados na construção do mesmo. Então, $K = N - (\partial(g_1(x)) + \partial({g_2}^{\perp}(x))$, onde $g_1(x)$ e ${g_2}^{\perp}(x)$ são os polinômios geradores dos códigos C_1 e ${C_2}^{\perp}$, respectivamente.*

Demonstração: Como C_1 e C_2 são códigos cíclicos, temos

$$k_1 = N - \partial(g_1(x));$$
$$k_2 = N - \partial(g_2(x)).$$

Pela construção *CSS*, segue que $K = k_1 - k_2$. Logo,

$$K = \partial(g_2(x)) - \partial(g_1(x)).$$

Como

$$\partial(g_2(x)) = N - \partial({g_2}^{\perp}(x)),$$

deduzimos que

$$K = N - (\partial(g_1(x)) + \partial({g_2}^{\perp}(x)).$$

□

Similarmente ao caso clássico, não podemos demonstrar a recíproca do Teorema 6.2.2. Entretanto, provaremos uma variação mais fraca para sua recíproca. No Teorema 6.2.5, consideramos que C_1 possui conjunto de definição $\bigcup_{s_1 \in S_1} \mathbb{C}_{s_1}$, e que o código ${C_2}^{\perp}$ possui conjunto de definição $\bigcup_{{s_2}^{\perp} \in {S_2}^{\perp}} \mathbb{C}_{{s_2}^{\perp}}$. Além disso, o conjunto A será dado por $A = (C_1 \backslash C_2)$, o conjunto B dado por $B = ({C_2}^{\perp} \backslash {C_1}^{\perp})$ e o conjunto P igual a $P = \{wt(c) \mid c \in (C_1 \backslash C_2) \cup ({C_2}^{\perp} \backslash {C_1}^{\perp})\}$.

Teorema 6.2.5 *Seja $CSS(C_1, C_2) = [[N, K, D]]_q$ o código cíclico quântico gerado a partir dos códigos cíclicos $C_1 = [N, k_1, d_1]_q$ e $C_2 = [N, k_2, d_2]_q$. Assuma que os conjuntos de definição dos códigos C_1 e ${C_2}^{\perp}$ sejam disjuntos. Se $CSS(C_1, C_2)$ é MDS e se existem palavras-código $c_1 \in A$ com $wt(c_1) = d_1$ e $c_2 \in B$ com $wt(c_2) = {d_2}^{\perp}$, então cada conjunto de definição dos códigos C_1 e ${C_2}^{\perp}$ contém exatamente $D - 1$ elementos.*

Demonstração: Como o código dual de um código cíclico também é cíclico, segue que ${C_2}^{\perp}$ é cíclico.

Por hipótese, sabemos que

$$K = k_1 - k_2 = N - 2D + 2, \tag{6.5}$$

i. e., o código quântico $CSS(C_1, C_2)$ atinge o limitante de Singleton. Como C_1 e ${C_2}^{\perp}$ são cíclicos, segue que

$$k_1 = N - \partial(g_1(x)) \tag{6.6}$$

e também que

$$k_2 = N - {k_2}^{\perp} = N - [N - \partial({g_2}^{\perp}(x))], \tag{6.7}$$

$$k_2 = \partial({g_2}^{\perp}(x)), \tag{6.8}$$

onde os polinômios $g_1(x)$ e ${g_2}^{\perp}(x)$ são polinômios geradores dos códigos C_1 e ${C_2}^{\perp}$, respectivamente.

Substituindo (6.6) e (6.8) em (6.5), deduzimos que

$$N - 2D + 2 = N - \partial(g_1(x)) - \partial({g_2}^{\perp}(x)),$$

e assim,

$$\partial(g_1(x)) + \partial({g_2}^{\perp}(x)) = 2(D - 1).$$

Por hipótese, o conjunto de definição dos códigos C_1 e ${C_2}^{\perp}$ são disjuntos. Logo, aplicando a equação (6.1) e procedendo como na demonstração do Teorema 6.1.2, concluímos que o conjunto dado por

$$(\bigcup_{s_1 \in S_1} \mathbb{C}_{s_1}) \bigcup (\bigcup_{{s_2}^{\perp} \in {S_2}^{\perp}} \mathbb{C}_{{s_2}^{\perp}})$$

possui exatamente $2(D-1)$ elementos.

Como próxima etapa, demonstraremos que cada conjunto de definição dos códigos C_1 e ${C_2}^{\perp}$ possui exatamente $D-1$ elementos.

Utilizando o limitante (clássico) de Singleton para C_1 e ${C_2}^{\perp}$, segue que

$$d_1 \leq N - k_1 + 1 \tag{6.9}$$

e

$$ {d_2}^{\perp} \leq N - {k_2}^{\perp} + 1. \tag{6.10}$$

Como C_1 e ${C_2}^{\perp}$ são cíclicos, deduzimos que

$$k_1 = N - \partial(g_1(x)) \tag{6.11}$$

e

$$ {k_2}^{\perp} = N - \partial({g_2}^{\perp}(x)). \tag{6.12}$$

Combinando as equações (6.9), (6.10), (6.11) e (6.12) temos que

$$d_1 \leq N - [N - \partial(g_1(x))] + 1 \Longrightarrow d_1 \leq \partial(g_1(x)) + 1. \tag{6.13}$$

Pela equação (6.1) e repetindo a demonstração do Teorema 6.1.2, concluímos que o conjunto de definição do código C_1 possui $\partial(g_1(x))$ elementos, i. e.,

$$| \bigcup_{s_1 \in S_1} \mathbb{C}_{s_1} | = \partial(g_1(x)), \tag{6.14}$$

onde | . | denota a cardinalidade do conjunto.

Suponha que o conjunto de definição do código C_1 possua menos que $D-1$ elementos. Por (6.14), segue que $\partial(g_1(x)) < D-1$. Por hipótese, existe uma palavra-código $c_1 \in A$ tal que $wt(c_1) = d_1$. Assim, concluímos que

$$\min P \leq d_1 < D,$$

e esse fato contradiz a construção *CSS*. Conseqüentemente, o conjunto de definição de C_1 possui $D-1$ ou mais elementos.

Substituindo o código C_1 pelo código ${C_2}^{\perp}$, existe uma palavra-código $c_2 \in B$ tal que $wt(c_2) = {d_2}^{\perp}$. Analogamente, supondo que o conjunto de definição de ${C_2}^{\perp}$ possua menos que $D-1$ elementos, temos que ${d_2}^{\perp} < D$, onde ${d_2}^{\perp}$ é a distância mínima do código ${C_2}^{\perp}$. Assim, segue que

$$D = \min P \leq {d_2}^{\perp} < D, \tag{6.15}$$

um absurdo.

Então, o conjunto de definição do código ${C_2}^{\perp}$ também possui $D-1$ ou mais elementos. Conseqüentemente, cada um dos conjuntos de definição possui $D-1$ ou mais elementos.

Sabemos que a união dos conjuntos de definição de C_1 e ${C_2}^{\perp}$ possui $2(D-1)$ elementos. Como cada um destes possui $D-1$ ou mais elementos e tais conjuntos são disjuntos, concluímos que cada conjunto de definição possui exatamente $D-1$ elementos, provando o teorema. □

6.3 Considerações Finais

Foram determinadas condições sob as quais códigos cíclicos clássicos (quânticos) são códigos MDS. Além disso, demonstramos que a cardinalidade do conjunto de definição dos códigos cíclicos clássicos (quânticos) MDS são naturalmente determinados. Ainda, generalizamos a noção de distância de projeto para códigos estabilizadores do tipo *CSS*.

Capítulo 7

Conexões entre Matróides e Códigos Quânticos

Em seu artigo seminal sobre teoria de matróides, [46], Hassler Whitney chamou atenção para o problema de caracterizar matróides representáveis sobre um dado corpo. A conexão entre códigos lineares sobre corpos e matróides representáveis sobre estes é bem conhecido e foi apresentado em [47], onde foi demonstrado que a função enumeradora de peso de um código linear clássico pode ser avaliada a partir do polinômio de Tutte de seu matróide associado. Outras caracterizações entre matróides representáveis e códigos corretores de erros, seguindo essa proposta, podem ser encontradas em [48–50]. Nos artigos [48, 51], os matróides são associados às matrizes geradoras dos respectivos códigos através de conceitos tais como o polinômio de Tutte ou suporte de vetor.

O objetivo principal deste capítulo é demonstrar que a função enumeradora de pesos de um código quântico *CSS* é uma avaliação do polinômio de Tutte do matróide soma direta dos códigos clássicos envolvidos na construção do mesmo, estendendendo o resultado demonstrado por Greene em [47], para códigos quânticos *CSS*. Acreditamos que tais conexões sejam as primeiras entre a teoria de matróides e a teoria de códigos quânticos *CSS*.

O capítulo está organizado como segue. Na Seção 7.1, enunciamos os conceitos básicos da teoria de matróides. Na Seção 7.2, faremos uma breve revisão da teoria dos códigos de bloco lineares. Na Seção 7.3, apresentamos nossos resultados relativos à novas conexões entre teoria de matróides e a teoria dos códigos quânticos *CSS* e, na Seção 7.4, relatamos as considerações finais do capítulo.

7.1 Teoria de Matróides

Nesta seção, apresentamos conceitos e teoremas sobre a teoria de matróides que serão necessários para o desenvolvimento do capítulo. Todos os resultados listados em seguida são encontrados em [52].

Definição 7.1.1 *[52] Um matróide M é um par ordenado $(E, \mathcal{I})$ consistindo de um conjunto finito E e uma coleção $\mathcal{I}$ de subconjuntos de E satisfazendo as seguintes condições:*

1. $\emptyset \in \mathcal{I}$.
2. *Se $I \in \mathcal{I}$ e $I' \subset I$, então $I' \in \mathcal{I}$.*
3. *Se I_1, $I_2 \in \mathcal{I}$ e $\mid I_1 \mid < \mid I_2 \mid$, então existe um elemento $e \in I_2 - I_1$ tal que $I_1 \cup e \in \mathcal{I}$, onde $\mid . \mid$ denota a cardinalidade do conjunto.*

Se M é o matróide $(E, \mathcal{I})$, então M é denominado *matróide em* E. Os membros de $\mathcal{I}$ são denominados *conjuntos independentes de* M, e E é o *conjunto base de* M. Escreveremos freqüentemente $\mathcal{I}(M)$ para $\mathcal{I}$ e $E(M)$ para E, particularmente quando vários matróides estão sendo considerados. Um subconjunto de E que não pertence a $\mathcal{I}$ é denominado *dependente*. Um multiconjunto é um conjunto que contém ou pode conter elementos repetidos.

O teorema a seguir é folclórico na literatura; é fundamental para o desenvolvimento deste capítulo.

Teorema 7.1.1 *Seja E o conjunto de rótulos de cada coluna de uma matriz $A_{m\times n}$ sobre o corpo F, e seja $\mathcal{I}$ o conjunto de subconjuntos X de E para os quais o multiconjunto de colunas rotuladas por X é linearmente independente (LI) no espaço vetorial m-dimensional sobre o corpo F, denotado por $V(m, F)$. Então $(E, \mathcal{I})$ é um matróide.*

Um matróide obtido a partir da matriz A será denotado por $M[A]$ e denominado *matróide vetorial de* A. Dizemos que dois matróides M_1 e M_2 são *isomorfos*, isto é, $M_1 \cong M_2$, se existe uma bijeção ψ de $E(M_1)$ para $E(M_2)$ tal que, para todo $X \subseteq E(M_1)$, $\psi(X)$ é independente em M_2 se, e somente se, X é independente em M_1. Se um matróide é isomorfo a um matróide vetorial de uma matriz D sobre um corpo F, então M é dito ser *representável sobre* F ou *F-representável*. D é dito ser uma representação para M sobre o corpo F. Conjuntos dependentes minimais são conjuntos dependentes cujos subconjuntos próprios são conjuntos independentes. Um conjunto dependente minimal em um matróide arbitrário M será denominado circuito de M e o conjunto de todos os circuitos de M será denotado por $\mathcal{C}$ ou $\mathcal{C}(M)$. Um conjunto independente é maximal se a inclusão de qualquer elemento no conjunto resulta em um outro conjunto dependente. Denominaremos um conjunto independente maximal em um matróide M de *base* de M. O conjunto de todas as bases de M será denotado por $\mathcal{B}$. Os membros de $\mathcal{B}$ são equicardinais, ou seja, contém o mesmo número de elementos. Seja $M = (E, \mathcal{I})$ um matróide e suponha que $X \subseteq E$. Seja $\mathcal{I} \mid X = \{I \subseteq X : I \in \mathcal{I}\}$. Então o par $(X, \mathcal{I}|X)$ é um matróide e será denotado por $M|X$. Como $M \mid X$ é um matróide, todas as suas bases são equicardinais. Definimos o *posto* de X como sendo o comprimento de uma base B de $M \mid X$ e denominaremos o conjunto B uma *base* de X. A função posto

de M é uma função $r : 2^E \longrightarrow \mathbb{Z}^+$ tal que, para todo $X \subseteq E$, associa um número $r(X)$. Tal função será denotada por r ou r_M. Evidentemente, $r(M)$ é igual ao comprimento de uma (e portanto, de todas as) base de M.

Seja r a função posto de M. O *operador fecho*, de M, denotado por cl, é uma aplicação $cl : 2^E \longrightarrow 2^E$, definida para todo $X \subseteq E$, como sendo $cl(X) = \{x \in E : r(X \cup x) = r(X)\}$. Seja $M = (E, \mathcal{I})$ um matróide e $X \subseteq E$. Se $X = cl(X)$, dizemos que X é um flat de M. Enunciaremos agora, um teorema sobre soma direta de matróides. Soma direta de matróides comporta-se bem em relação à estrutura de seu código associado.

Teorema 7.1.2 *[52] Sejam M_1 e M_2 matróides em conjuntos disjuntos E_1 e E_2. Sejam ainda $E = E_1 \cup E_2$ e*

$$\mathcal{I} = \{I_1 \cup I_2 : I_1 \in \mathcal{I}(M_1), I_2 \in \mathcal{I}(M_2)\}.$$

Então $(E, \mathcal{I})$ é um matróide.

O matróide $(E, \mathcal{I})$, dado no Teorema 7.1.2, é denominado *soma direta* de M_1 e M_2 e será denotado por $M_1 \oplus M_2$. Mais geralmente, se consideramos n matróides e se procedermos como no teorema anterior, teremos a n-soma direta de matróides $M_1 \oplus M_2 \oplus \cdots \oplus M_n$. Em seguida enunciaremos o Teorema 7.1.3 que afirma que a soma direta de matróides comporta-se bem em relação à F-representabilidade:

Teorema 7.1.3 *[52] As classes de matróides F-representáveis são fechadas em relação à operação de soma direta.*

Dado um espaço vetorial V, considere o *espaço vetorial dual* $V^\perp$. Analogamente, dado um matróide M, existe um *matróide dual de M*, denotado por M^*:

Definição 7.1.2 *[52] Seja M um matróide. O conjunto*

$$\mathcal{B}^*(M) = \{E(M) - B : B \in \mathcal{B}(M)\}$$

é o conjunto das bases de um matróide M^* em $E(M)$.

Os conjuntos independentes, as bases e os circuitos de M^* são denominados *conjuntos coindependentes*, *cobases* e *cocircuitos* de M, respectivamente.

O Teorema 7.1.4 permite identificar a estrutura do matróide dual de um matróide vetorial. Essa estrutura coincide com a estrutura do código dual.

Teorema 7.1.4 *[52] Seja M um matróide vetorial da matriz $[I_r|D]$ sobre o corpo F. Então M^* é o matróide vetorial da matriz $[-D^T|I_{n-r}]$, onde D^T é a transposta da matriz $D_{r\times(n-r)}$, definida sobre o corpo F, e I_r é a matriz identidade $r \times r$, onde r é a cardinalidade de uma (e assim, de todas as) base de M.*

7.2 Códigos de Bloco

Supomos que o leitor esteja familiarizado com o teoria dos códigos de bloco lineares. Mais detalhes podem ser encontrados em [33,35,36]. Relembremos dois resultados básicos da teoria de códigos de bloco:

Corolário 7.2.1 *[36] Seja $C(n,k)$ um código de bloco linear com matriz verificação de paridade H. Então, $C(n,k)$ possui peso mínimo (e assim, distância mínima) no mínimo igual a d se, e somente se, cada combinação de $d-1$ ou menos colunas de H é linearmente independente.*

Corolário 7.2.2 *[36] Seja $C(n,k)$ um código de bloco linear com matriz verificação de paridade H. O peso mínimo (e então, a distância mínima) de $C(n,k)$ é igual ao menor número de colunas linearmente dependentes de H.*

7.3 Matróides e Códigos *CSS*

Nesta seção, apresentamos nossas contribuições. Enunciaremos e demonstramos novos resultados relativos à conexão entre códigos clássicos e quânticos e a teoria de matróides.

O Teorema 7.3.1 é bem conhecido na literatura; é uma aplicação do Teorema 7.1.1.

Teorema 7.3.1 *Seja $C(n,k)$ um código de bloco linear com matriz verificação de paridade $H_{n-k,n}$. Seja $E = \{1, 2, \cdots, n\}$ o conjunto de rótulos das n colunas da matriz H e seja $\mathcal{I}$ o conjunto de rótulos de colunas de H tal que os respectivos vetores são linearmente independentes no espaço vetorial $V(n-k, F_q)$. Então, o par ordenado $(E, \mathcal{I})$ é um matróide vetorial da matriz H sobre o corpo F_q. Reciprocamente, se M é um matróide F_q-representável da matriz $A_{m\times n}$, tal que as linhas de A são vetores linearmente independentes em $V(n, F_q)$, então o matróide M dá origem a uma matriz verificação de paridade de um código de bloco linear $C(n, n-m)$.*

O matróide derivado do código $C(n,k)$ será denotado por M_C e, reciprocamente, o código $C(n,k)$ derivado do matróide M será denotado por C_M.

Observação 7.3.1 *Dado o código $C(n,k)$, seu matróide associado M_C não depende da escolha da matriz verificação de paridade H. Porém, existem propriedades de códigos que não são determinadas por seu matróide vetorial M_C, como por exemplo, o raio de recobrimento do código (veja, [53]).*

Observação 7.3.2 *Podemos sempre supor que as linhas da matriz $A_{m\times n}$, que geram o matróide vetorial $M[A]$, são linearmente independentes. Isso vale devido ao fato que as operações elementares com linhas e colunas da matriz A tornam invariante o matróide vetorial $M[A]$ (veja [52] §2.2, propriedades 2.2.1 - 2.2.6).*

Ilustraremos o Teorema 7.3.1 apresentando um exemplo, no qual geramos um matróide M_C a partir do código de Hamming $(7, 4)$.

Exemplo 7.3.1 *Considere o código de Hamming* $(7, 4)$*, cuja matriz verificação de paridade é dada por*

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

Considerando os rótulos das colunas de H como sendo os números 1 *até* 7*, temos* $E = \{1, 2, 3, 4, 5, 6, 7\}$*. Os elementos do conjunto $\mathcal{I}$ são rótulos de vetores-coluna linearmente independentes em $V(3, F_q)$, ou seja,*

$$\begin{aligned} \mathcal{I} = \{&\{1\},\{2\},\{3\},\{4\},\{5\},\{6\},\{7\},\{1,2\},\\ &\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{1,7\},\\ &\{2,3\},\{2,4\},\{2,5\},\{2,6\},\{2,7\},\\ &\{3,4\},\{3,5\},\{3,6\},\{3,7\},\{4,5\},\\ &\{4,6\},\{4,7\},\{5,6\},\{5,7\},\{6,7\},\\ &\{1,2,3\},\{1,2,5\},\{1,2,6\},\{1,2,7\},\\ &\{1,3,4\},\{1,3,5\},\{1,3,6\},\{1,4,5\},\\ &\{1,4,6\},\{1,4,7\},\{1,5,7\},\{2,3,4\},\\ &\{2,3,6\},\{2,3,7\},\{2,4,5\},\{2,4,6\},\\ &\{2,4,7\},\{2,5,6\},\{2,5,7\},\{3,4,5\},\\ &\{3,4,7\},\{3,5,6\},\{3,5,7\},\{3,6,7\},\{4,5,6\},\\ &\{4,6,7\},\{5,6,7\}\}. \end{aligned}$$

O conjunto das bases deste matróide é dado por

$$\begin{aligned} \mathcal{B} = \{&\{1,2,3\},\{1,2,5\},\{1,2,6\},\{1,2,7\},\\ &\{1,3,4\},\{1,3,5\},\{1,3,6\},\{1,4,5\},\\ &\{1,4,6\},\{1,4,7\},\{1,5,7\},\{2,3,4\},\\ &\{2,3,6\},\{2,3,7\},\{2,4,5\},\{2,4,6\},\\ &\{2,4,7\},\{2,5,6\},\{2,5,7\},\{3,4,5\},\\ &\{3,4,7\},\{3,5,6\},\{3,5,7\},\{3,6,7\},\\ &\{4,5,6\},\{4,6,7\},\{5,6,7\}\}. \end{aligned}$$

É claro que, utilizando a notação dual de M_C, conceitos tais como polinômio de Tutte são facilmente calculados através de conceitos existentes na literatura; para esse propósito, veja por exemplo, [51](Equação (7)).

A primeira contribuição deste capítulo é o Teorema 7.3.2. É um método alternativo para se calcular a distância mínima de um código de bloco linear, sem o uso de conceitos tais como polinômio de Tutte e suporte de vetor.

Teorema 7.3.2 *Seja $C(n,k)$ um código de bloco com matriz verificação de paridade H e seja M_C o matróide derivado do código $C(n,k)$. Suponha que o circuito $\mathbf{C}$ do matróide M_C tenha o menor número de elementos (ou seja, menor comprimento) dentre todos os circuitos de M_C, $|\boldsymbol{C}| = c$. Então, a distância mínima do código $C(n,k)$ é igual a c.*

Demonstração: Pelo Teorema 7.3.1, o código $C(n,k)$ origina um matróide vetorial da matriz H. Como o comprimento do menor circuito $\mathbf{C}$ é igual a c, então todo conjunto contendo menos do que c elementos é necessariamente um conjunto independente. Em outras palavras, todo conjunto contendo menos que c elementos, origina um conjunto de vetores linearmente independentes em $V(n-k, F_q)$. Pelo Corolário 7.2.1, podemos garantir que a distância mínima do código $C(n,k)$ é, pelo menos, c. Entretanto, existe um conjunto dependente contendo c elementos, por exemplo, o conjunto $\mathbf{C}$. Então, existe um conjunto contendo c vetores linearmente dependentes em $V(n-k, F_q)$. Como o menor número de colunas linearmente dependentes da matriz H é c, segue, pelo Corolário 7.2.2, que a distância mínima do código $C(n,k)$ é exatamente igual a c. □

Pelo Teorema 7.3.2, é possível calcular a distância mínima de um código linear $C(n,k)$ através do comprimento do menor circuito dentre todos os circuitos de seu matróide associado M_C. Conseqüentemente, fornece um método alternativo para, não somente calcular a distância mínima de um código linear $C(n,k)$, mas também para investigar o comprimento do menor circuito derivado do matróide M_C.

Enunciamos, agora, o Teorema 7.3.3, que conecta o código dual com seu repectivo matróide dual. Este teorema é bem conhecido na literatura.

Teorema 7.3.3 *Seja $C(n,k)$ um código de bloco linear com matriz geradora G e matriz verificação de paridade H. Então, o respectivo matróide vetorial e seu dual possuem matrizes que preservam as estruturas existentes entre G e H.*

A soma direta de matróides é um matróide que possui estrutura que nos permite calcular a distância mínima do respectivo código gerado por este. Em outras palavras, o Teorema 7.3.4 afirma que a soma direta de dois matróides gera um código linear com parâmetros $C(n_1 + n_2, m_1 + m_2, min\{d_1, d_2\})$.

Teorema 7.3.4 *Sejam M_1 e M_2 matróides representáveis sobre F_q com matrizes de representação $A_{m_1\times n_1}$ e $B_{m_2\times n_2}$, respectivamente, onde A e B possuem linhas linearmente independentes em $V(n_1, F_q)$ e $V(n_2, F_q)$, respectivamente, definidos em conjuntos disjuntos. Então o matróide $M_1 \oplus M_2$ gera um código linear $C(n_1+n_2, m_1+m_2)$ cuja distância mínima é igual a $min\{c_1, c_2\}$, onde c_1 e c_2 são os menores comprimentos dentre todos os circuitos de M_1 e M_2, respectivamente.*

Demonstração: Pelo Teorema 7.1.3, $M_1 \oplus M_2$ é F_q-representável. Além disso, a matriz

$$H = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right]$$

é uma representação deste matróide (veja [52], §21, exercício 6). Considere que esta matriz H seja a matriz verificação de paridade de um código linear $C(n_1+n_2, m_1+m_2)$. Analisemos a matriz H. Considerando a submatriz

$$H_1 = \left[\begin{array}{c} A \\ 0 \end{array}\right],$$

temos que, pelo Teorema 7.3.2, o menor número de colunas linearmente dependentes de H_1 é igual a c_1. Similarmente, considerando a submatriz

$$H_2 = \left[\begin{array}{c} 0 \\ B \end{array}\right],$$

concluímos novamente pelo Teorema 7.3.2, que o menor número de colunas linearmente dependentes de H_2 é igual a c_2. Claramente, a matriz H possui todas as linhas linearmente independentes. Além disso, a matriz H satisfaz a seguinte propriedade: o menor número de colunas linearmente dependentes de H é igual a c_1, se $c_1 \leq c_2$ ou o menor número de colunas linearmente dependentes de H é igual a c_2, se $c_2 \leq c_1$. Isso ocorre pela aplicação do Teorema 7.3.2 e pela estrutura de H. Assim, segue que a distância mínima do código $C(n_1+n_2, m_1+m_2)$, com matriz verificação de paridade H, é igual a $min\{c_1, c_2\}$. □

Observação 7.3.3 *Analogamente ao caso de dois matróides, o teorema anterior também é válido quando são considerados um número finito de matróides F_q-representáveis. De fato, podemos demonstrar esta afirmação pelo mesmo método de demonstração utilizado no Teorema 7.3.4.*

Teorema 7.3.5 *Considerando as mesmas hipóteses do Teorema 7.3.4, considere n matróides F_q-representáveis $M_1, M_2, \cdots, M_n$ definidos em conjuntos disjuntos. Então o matróide $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ gera um código linear cuja distância mínima é igual a $min\{c_1, c_2, \cdots, c_n\}$, onde c_i, $i = 1, \cdots, n$, são os menores comprimentos dentre todos os circuitos de $M_1, M_2, \cdots, M_n$, respectivamente.*

Na seqüência, demonstramos o Teorema 7.3.6. Estamos supondo que os códigos clássicos que geram o código *CSS* são códigos de bloco.

Teorema 7.3.6 *Seja $CSS(C_1, C_2)$ um código* CSS *com parâmetros $[[n, k = k_1 - k_2]]_q$, onde q é uma potência de primo. Então, existe um par de matróides F_q-representáveis $M_1 = (E_1, \mathcal{I}_1)$ e $M_2{}^{\perp} = (E_2{}^{\perp}, \mathcal{I}_2{}^{\perp})$ tal que o código $CSS(C_1, C_2)$ é gerado pela soma direta $M_2{}^{\perp} \oplus M_1$ dos matróides $M_2{}^{\perp}$ e M_1. Reciprocamente, assuma que existam matróides $M_1 = (E_1, \mathcal{I}_1)$ e $M_2 = (E_2, \mathcal{I}_2)$, representáveis sobre F_q, cujas matrizes de representação são A_1 e A_2, respectivamente. Suponha que o espaço linha de A_2 esteja contido no espaço linha de A_1. Então, existe um código quântico* CSS *representado pela matriz H, onde H é uma F_q-representação de $M_2{}^{\perp} \oplus M_1$, onde $M_2{}^{\perp}$ é o matróide dual de M_2.*

Demonstração: ($\Longrightarrow$) Sejam C_1 e C_2 códigos de bloco lineares q-ários que geram o código $CSS(C_1, C_2)$. Considere a matriz verificação de paridade $H(C_1)$ e $H(C_2{}^{\perp})$ dos códigos C_1 e $C_2{}^{\perp}$, respectivamente. Pelo Teorema 7.3.4, sabemos que existem matróides $M_1 = (E_1, \mathcal{I}_1)$ e $M_2{}^{\perp} = (E_2{}^{\perp}, \mathcal{I}_2{}^{\perp})$ que são matróides vetoriais das matrizes $H(C_1)$ e $H(C_2{}^{\perp})$, respectivamente, sobre F_q. Além disso, pelo processo de construção *CSS* (veja Eq. 10.106 em [1]), segue que o código $CSS(C_1, C_2)$ possui matriz verificação de paridade

$$H = \left[\begin{array}{c|c} H(C_2{}^{\perp}) & 0 \\ \hline 0 & H(C_1) \end{array}\right].$$

Além disso, a soma direta $M_2{}^{\perp} \oplus M_1$ dos matróides M_1 e $M_2{}^{\perp}$ é F_q-representável, cuja matriz de representação é a matriz

$$H = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right],$$

onde A e B são F_q-representações de M_1 e $M_2{}^{\perp}$, respectivamente. Considerando $A = H(C_1)$ e $B = H(C_2{}^{\perp})$, concluímos que a matriz verificação de paridade do código quântico $CSS(C_1, C_2)$ é a matriz H, onde H é uma F_q-representação do matróide soma direta $M_1 \oplus M_2$, concluindo a demonstração.

($\Longleftarrow$) Como, por hipótese, os matródes $M_1 = (E_1, \mathcal{I}_1)$ e $M_2 = (E_2, \mathcal{I}_2)$ são representáveis sobre F_q, a soma direta $M_2{}^{\perp} \oplus M_1$ também é F_q-representável. Suponha, sem perda de generalidade, que as matrizes A_1 e A_2 possuam todas as linhas linearmente independentes. Pelo Teorema 7.3.4, sabemos que existem códigos (clássicos) de bloco C_1 e C_2 cujas matrizes verificação de paridade são as matrizes A_1 e A_2, respectivamente. Como o espaço linha de A_2 está contido no espaço linha de A_1, temos que $C_2 \subset C_1$. Aplicando o processo de construção *CSS*, geramos um código $CSS(C_1, C_2)$ cuja matriz verificação de paridade é a matriz

$$H = \left[\begin{array}{c|c} A_2{}^{\perp} & 0 \\ \hline 0 & A_1 \end{array}\right],$$

onde ${A_2}^{\perp}$ é a matriz verificação de paridade do código
${C_2}^{\perp}$. Como H é uma F_q-representação do matróide ${M_2}^{\perp} \oplus M_1$, o resultado segue diretamente. □

Observação 7.3.4 *O Teorema 7.3.6 estabelece uma nova conexão entre matróides e códigos quânticos* CSS *como veremos a seguir. De fato, geramos a função enumeradora de pesos do código* CSS *por meio da avaliação do polinômio de Tutte do matróide soma correspondente aos códigos clássicos utilizados na construção do código* CSS*, como explicitado no Teorema 7.3.6.*

Definição 7.3.1 *O* polinômio de Tutte $T_M(x, y)$ *de um matróide $M = (E, \mathcal{I})$, com função posto r, é definido como sendo*

$$T_M(x,y) = \sum_{A \subseteq E} (x-1)^{r(M)-r(A)} (y-1)^{|A|-r(A)}, \tag{7.1}$$

onde $r(M)$ é o comprimento de uma (e portanto de todas as) base(s) do matróide M, $r(A)$ é o comprimento de uma (e, portanto, todas as) base(s) contida no subconjunto $A \subset E$ e $|\,.\,|$ denota a cardinalidade do conjunto.

Tal polinômio possui, entre outras, as seguintes propriedades:

1. $T_M(x, y) = T_{M^*}(y, x)$;
2. $T_{M_1 \oplus M_2}(x, y) = T_{M_1}(x, y) T_{M_2}(x, y)$;

onde M^* é o matróide dual de M e $M_1 \oplus M_2$ é a soma direta dos matróides M_1 e M_2.

Greene [47] demonstrou que a função enumeradora de pesos $A_C(z)$ de um código linear q-ário $C(n, k)$ é uma avaliação especial do polinômio de Tutte de seu respectivo matróide $M(C)$, derivado a partir da matriz geradora de $C(n, k)$:

$$A_C(z) = (1-z)^k z^{n-k} T_{M(C)}\left(\frac{1+(q-1)z}{1-z}, \frac{1}{z}\right). \tag{7.2}$$

Tendo como base esse resultado, estamos aptos a demonstrar o Teorema 7.3.7 que generaliza, para códigos quânticos *CSS*, o resultado demonstrado por Greene [47] para códigos (de bloco) clássicos lineares.

Teorema 7.3.7 *Seja $C = [[n, K, D]]_q$ o código quântico* CSS *gerado pelos códigos clássicos $C_1 = [n, k_1]_q$ e $C_2 = [n, k_2]_q$. Então, a função enumeradora de pesos de C é dada por*

$$A_C(z) = (1-z)^{k_1} z^{n-k_1} T_{M(C_1)}\left(\frac{1+(q-1)z}{1-z}, \frac{1}{z}\right) \cdot (1-z)^{n-k_2} z^{k_2} T_{M({C_2}^{\perp})}\left(\frac{1+(q-1)z}{1-z}, \frac{1}{z}\right),$$

onde $M(C_1)$ e $M({C_2}^{\perp})$ são os respectivos matróides associados aos códigos $C_1 = [n, k_1]_q$ e ${C_2}^{\perp} = [n, n-k_2]_q$, respectivamente, e $T_{M(C_1)}$ e $T_{M({C_2}^{\perp})}$ são os polinômios de Tutte de $M(C_1)$ e $M({C_2}^{\perp})$, respectivamente.

Demonstração: Pelo Teorema 7.3.6, sabemos que o código $C = [[N, K, D]]_q$ é representado pela soma direta ${M_2}^{\perp} \oplus M_1$ de M_1 e ${M_2}^{\perp}$, onde M_1 é o matróide F_q-representável relacionado ao código C_1 e ${M_2}^{\perp}$ é o matróide F_q-representável relacionado ao código ${C_2}^{\perp}$. Pelo Item 2) e utilizando a equação (7.1), concluímos o resultado. □

Para ilustrar o Teorema 7.3.7 apresentamos um exemplo:

Considere $C = [[7, 1, 3]]_2$ o código quântico construído no Capítulo 3. Sabemos que $C_1 = \langle M^{(1)} = x^3 + x + 1\rangle$ é o código de Hamming $[7, 4, 3]$, ${C_2}^{\perp}$ é o código cíclico gerado pelo polinômio minimal $M^{(3)} = x^3 + x^2 + 1$, C_2 é o código cíclico gerado pelo produto dos polinômios minimais $M^{(0)}M^{(1)} = x^4 + x^3 + x^2 + 1$ e ${C_1}^{\perp}$ é o código simplex $[7, 3, 4]$. As matrizes geradoras para C_1 e ${C_2}^{\perp}$ são dadas, respectivamente, por

$$G(C_1) = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

e

$$G({C_2}^{\perp}) = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Tendo como base as Tabelas 7.1 e 7.2, verificamos que o polinômio enumerador de pesos de C_1 e de ${C_2}^{\perp}$ são dados por

$$A_{C_1}(z) = A_{{C_2}^{\perp}}(z) = 1 + 7z^3 + 7z^4 + z^7.$$

Calcularemos o polinômio enumerador de pesos do código C a partir do polinômio de Tutte de seu respectivo matróide soma direta.

código C_1
$A_0 = 1$
$A_3 = 7$
$A_4 = 7$
$A_7 = 1$

Tabela 7.1: Enumerador de Pesos de C_1

código ${C_2}^{\perp}$
$A_0 = 1$
$A_3 = 7$
$A_4 = 7$
$A_7 = 1$

Tabela 7.2: Enumerador de Pesos de ${C_2}^{\perp}$

Sabemos que $r(M_1) = r({M_2}^{\perp}) = 4$, $r(A) \in \{1,2,3,4\}$, para todo subconjunto $A \subset E_1$, onde $E_1 = \{1, \cdots, 7\}$, e $r(B) \in \{1,2,3,4\}$, para todo subconjunto $B \subset E_2$, onde $E_2 = \{1, \cdots, 7\}$. Os conjuntos E_1 e E_2 são os conjuntos base dos matróides M_1 e ${M_2}^{\perp}$, respectivamente. Além disso, $n = 7$, $k_1 = 4$, $k_2^{\perp} = 4$ e $q = 2$. Fazendo uso desses dados, calcularemos o polinômio enumerador de pesos do código quântico $C = [[7,1,3]]_2$.

Primeiramente calcularemos $A_{C_1}(z)$:

$$A_{C_1}(z) = (1-z)^k z^{n-k} T_{M(C_1)}\left(\tfrac{1+(q-1)z}{1-z}, \tfrac{1}{z}\right) \Longrightarrow A_{C_1}(z) = (1-z)^4 z^3 T_{M(C_1)}\left(\tfrac{1+z}{1-z}, \tfrac{1-z}{z}\right).$$

Substituindo a expressão $T_{M(C_1)}\left(\tfrac{1+z}{1-z}, \tfrac{1-z}{z}\right)$ na equação (7.1), segue que:

$$\begin{aligned} A_{C_1}(z) = (1-z)^4 z^3 &\left[\binom{7}{0}\left(\frac{2z}{1-z}\right)^4 + \binom{7}{1}\left(\frac{2z}{1-z}\right)^3 + \binom{7}{2}\left(\frac{2z}{1-z}\right)^2\right] \\ &+(1-z)^4 z^3 \left[\binom{7}{3}\left(\frac{2z}{1-z}\right)^1 + (35-7)\left(\frac{2z}{1-z}\right)^0\left(\frac{1-z}{z}\right)^0\right] \\ &+(1-z)^4 z^3 \left[\binom{7}{1}\left(\frac{2z}{1-z}\right)^1\left(\frac{1-z}{z}\right)^1 + \binom{7}{2}\left(\frac{1-z}{z}\right)^1\right] \\ &+(1-z)^4 z^3 \left[\binom{7}{1}\left(\frac{1-z}{z}\right)^2 + \binom{7}{0}\left(\frac{1-z}{z}\right)^3\right] \Longrightarrow \end{aligned}$$

$$A_{C_1}(z) = (1-z)^4 z^3 \left[\left(\frac{2z}{1-z} \right)^4 + 7 \left(\frac{2z}{1-z} \right)^3 + 21 \left(\frac{2z}{1-z} \right)^2 \right]$$

$$+(1-z)^4 z^3 \left[35 \left(\frac{2z}{1-z} \right)^1 + 28 \left(\frac{2z}{1-z} \right)^0 \left(\frac{1-z}{z} \right)^0 \right]$$

$$+(1-z)^4 z^3 \left[7 \left(\frac{2z}{1-z} \right)^1 \left(\frac{1-z}{z} \right)^1 + 21 \left(\frac{1-z}{z} \right)^1 \right]$$

$$+(1-z)^4 z^3 \left[7 \left(\frac{1-z}{z} \right)^2 + \left(\frac{1-z}{z} \right)^3 \right] =$$

$$= 16z^7 + 56(1-z)z^6 + 84(1-z)^2 z^5 + 70(1-z)^3 z^4$$

$$+42(1-z)^4 z^3 + 21(1-z)^5 z^2 + 7(1-z)^6 z + (1-z)^7 =$$

$$= 16z^7 + 56z^6 - 56z^7 + 84z^5 - 168z^6 + 84z^7 - 70z^7$$

$$+210z^6 - 210z^5 + 70z^4 + 42z^7 - 168z^6 + 252z^5 - 168z^4 +$$

$$+42z^3 - 21z^7 + 105z^6 - 210z^5 + 210z^4 - 105z^3 + 21z^2$$

$$+7z^7 - 42z^6 + 105z^5 - 140z^4 + 105z^3 - 42z^2 + 7z - z^7$$

$$+7z^6 - 21z^5 + 35z^4 - 35z^3 + 21z^2 - 7z + 1 =$$

$$1 + 7z^3 + 7z^4 + z^7.$$

Similarmente,

$$A_{C_2{}^\perp}(z) = 1 + 7z^3 + 7z^4 + z^7.$$

Aplicando o Teorema 7.3.7, segue que o polinômio enumerador de pesos do código C é dado por

$$A_C(z) = \left(1 + 7z^3 + 7z^4 + z^7\right)^2 =$$
$$z^{14} + 14z^{11} + 14z^{10} + 49z^8 + 100z^7 + 49z^6 + 14z^4 + 14z^3 + 1.$$

É conveniente enfatizarmos alguns fatos interessantes:

Definição 7.3.2 *Para a classe dos códigos estabilizadores q-ários, da qual os códigos* CSS *são parte integrante, define-se o* peso, $w(E)$, *de um elemento E pertencente ao grupo de erros do código como sendo*

$$w(E) = swt((\mathbf{a} \mid \mathbf{b})),$$

onde swt é o peso simplético *de um vetor $(\mathbf{a} \mid \mathbf{b}) \in F_q^{2n}$ dado por*

$$swt((\mathbf{a} \mid \mathbf{b})) = \mid \{k \mid (a_k, b_k) \neq (0,0)\} \mid .$$

A Definição 7.3.2 é um importante conceito para a generalização do processo de construção *CSS* binário para o processo de construção *CSS* q-ário. Tendo como base esses conceitos, podemos afirmar que o código $CSS(C_1, C_2)$ possui matriz verificação de paridade

$$H = \left[\begin{array}{c|c} H({C_2}^{\perp}) & 0 \\ \hline 0 & H(C_1) \end{array}\right].$$

De fato, tal interpretação já foi anteriormente mencionada e utilizada na demonstração do Teorema 7.3.6.

Observação 7.3.5 *Quando calculamos a função enumeradora de pesos do código $CSS(C_1, C_2)$ estamos considerando, na verdade, o peso de Hamming dos vetores pertencentes ao código originado de seu respetivo matróide soma direta. É claro que precisamos considerar o peso simplético correspondente às palavras-código do código $CSS(C_1, C_2)$. Porém, se a distribuição de pesos de Hamming do código é conhecida, o cálculo da função enumeradora simplética de pesos é apenas uma questão de ordenação das componentes dos vetores pertencentes ao código.*

Para ilustrar a observação anterior, apresentamos um exemplo:

Seja $C = [[7, 1, 3]]_2$ o código quântico considerado no Exemplo 1. Analisando sua função enumeradora (Hamming) de pesos, sabemos que tal código possui uma palavra-código com peso de Hamming igual a 14. Evidentemente, quando consideramos o peso simplético, tal palavra possui peso 7, conforme a Definição 7.3.2. Ainda, sabemos que tal código possui 14 palavras-código com peso de Hamming igual a 11. Conseqüentemente, $C = [[7, 1, 3]]_2$ possui pelo menos uma palavra-código com peso simplético igual a 6, e assim por diante.

7.4 Comentários Finais

Neste capítulo, foram apresentadas as primeiras conexões entre a teoria de matróides e a teoria de códigos quânticos *CSS*. Dentre tais conexões, demonstramos que a função enumeradora de pesos de um código quântico *CSS* é a avaliação do polinômio de Tutte do matróide soma direta dos códigos clássicos envolvidos na construção do mesmo. Além disso, acreditamos que, assim como foi demonstrado para códigos de bloco, também seja possível a generalização da função enumeradora de pesos para códigos *CSS* q-ários, derivados de códigos convolucionais clássicos.

Capítulo 8

Conclusões e Propostas de Trabalhos Futuros

Neste capítulo faremos um breve sumário dos assuntos abordados nesta tese.

No Capítulo 1, tratamos de definir e enunciar conceitos fundamentais da mecânica quântica e da teoria de codificação quântica, que foram necessários para o desenvolvimento desta tese. Foram apresentadas, também, algumas demonstrações alternativas para resultados importantes da teoria de codificação quântica, pois nenhuma dessas demonstrações foram encontradas na literatura.

No Capítulo 2, estabelecemos um novo método de construção para famílias de bons códigos quânticos *CSS*, derivados de códigos *Reed-Solomon* clássicos q-ários (q é potência de primo), distintos, não necessariamente auto-ortogonais. Demonstramos que, quando o comprimento da palavra-código tende ao infinito a taxa de codificação dos respectivos códigos quânticos tende ao valor 1, o que é um bom resultado. Além disso, tal método generaliza o método de construção apresentado em [3]. Ainda, baseado neste método proposto, conseguimos reproduzir algumas famílias de códigos quânticos MDS apresentadas em [27], bem como conseguimos estender uma (e possivelmente mais do que uma) família de códigos quânticos apresentada em [19].

No Capítulo 3, estabelecemos seis novos métodos de construção de códigos quânticos *CSS* derivados de códigos cíclicos clássicos. Esses métodos geram diversas famílias de bons códigos quânticos, ou seja, a taxa de codificação de tais famílias também tende ao valor 1. Esse é o capítulo mais importante da tese em nosso ponto de vista, pois conseguimos gerar métodos de construção eficientes e inovadores.

No Capítulo 4, fornecemos dois novos métodos de construção de códigos quânticos *CSS* derivados de códigos clássicos *Reed-Muller* e *Resíduos Quadráticos*, respectivamente. O primeiro método somente reproduz famílias já conhecidas de códigos quânticos. Entretanto, esse método de construção é mais sucinto e de fácil aplicação, quando comparado ao método apresentando por Zang and Fuzz [31].

No Capítulo 5, construímos uma nova família de códigos quânticos *CSS* baseados no produto tensorial de códigos *Reed-Solomon*. Destacamos que esses códigos são facilmente construídos. Entretanto, tal família não possui taxa de codificação k/n alta, devido ao fato do comprimento da palavra-código crescer muito rapidamente à medida que aplica-se o produto tensorial dos códigos clássicos envolvidos no processo de construção do código *CSS*. Mesmo assim, podemos utilizar tais códigos no caso de processos quânticos que necessitem de proteção desigual aplicados aos qudits.

No Capítulo 6, foram determinadas condições sob as quais códigos cíclicos clássicos (quânticos) são códigos MDS. Além disso, demonstramos que a cardinalidade do conjunto de definição dos códigos cíclicos clássicos (quânticos) MDS são naturalmente determinados. Ainda, generalizamos a noção de distância de projeto para códigos estabilizadores do tipo *CSS*.

No Capítulo 7, demonstramos que a função enumeradora de pesos de um código quântico *CSS* é uma avaliação do polinômio de Tutte do matróide soma direta dos códigos clássicos envolvidos na construção do mesmo, estendendendo o resultado demonstrado por Greene em [47], para códigos quânticos *CSS*. Tais conexões são as primeiras entre a teoria de matróides e a teoria de códigos quânticos *CSS*.

Tendo como base todos esses comentários inferimos que o objetivo principal deste trabalho de tese foi gerar novos métodos de construção de famílias de bons códigos quânticos *CSS*. A maioria dessas famílias possuem taxa de codificação tendendo ao valor 1, e muitos dos códigos contruídos pelos métodos propostos possuem palavras-código cujos comprimentos são próximos ao limitante quântico de Singleton.

Além disso, estabelecemos novas conexões entre a teoria de matróides e a teoria de códigos quânticos, onde a contribuição mais significativa foi demonstrar que a função enumeradora de pesos de um código quântico *CSS* é uma avaliação do polinômio de Tutte do matróide soma direta derivado dos códigos clássicos utilizados no processo de construção *CSS*.

Acreditamos, então, que os objetivos foram alcançados.

8.1 Propostas de Trabalhos Futuros

Como possíveis propostas de trabalhos futuros decorrentes da pesquisa realizada temos:

- Criação de novos métodos de construção para códigos quânticos *CSS* derivados de códigos (clássicos) sobre anéis;
- Generalização do processo de construção *CSS* para anéis finitos;
- Busca de outras conexões entre a teoria de matróides e a teoria dos códigos quânticos *CSS*;

- Possíveis conexões entre teoria de matróides e a teoria dos códigos convolucionais clássicos (quânticos).

Publicações

- Construção de códigos corretores de erros quânticos *CSS*, a partir de códigos *BCH*, *Reed-Solomon* e *Resíduos quadráticos*, 2º Workshop de Computação e Informação Quântica - WECIQ 2007, Campina Grande;

- Uma proposta de critério de separabilidade para estados quânticos com n qubits. 2º Workshop de Computação e Informação Quântica - WECIQ 2007, Campina Grande;

- Relações entre Matróides e Códigos de Bloco Lineares, Congresso Nacional de Matemática Aplicada e Computacional - XXX CNMAC 2007, Florianópolis.

Submissões

- Construction of New q-ary Quantum Reed-Solomon Codes - IEEE-IT.

Bibliografia

[1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[2] A. Ketkar, A. Klappenecker, S. Kumar, and P.K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inf. Theory*, 52(11):4892 – 4914, November 2006.

[3] M. Grassl, W. Geiselmann, and T. Beth. Quantum Reed-Solomon codes. *AAECC-13*, 1709:231–244, 1999.

[4] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Primitive quantum BCH codes over finite fields. In *Proc. Int. Symp. Inf. Theory (ISIT)*, pages 1114–1118, 2006.

[5] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Comb. Designs*, 8:174–188, 2000.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, January 1997.

[7] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098–1105, August 1996.

[8] H. Chen. Some good quantum error-correcting codes from algebric geometric codes. *IEEE. Trans. Inf. Theory*, 47(5):2059–2061, July 2001.

[9] H. Chen, S. Ling, and C. P. Xing. Quantum codes from concatenated algebraic geometric codes. *IEEE. Trans. Inf. Theory*, 51(8):2915 – 2920, august 2005.

[10] G.D. Cohen, S.B. Encheva, and S. Litsyn. On binary constructions of quantum codes. *IEEE Trans. Inf. Theory*, 45(7):2495–2498, July 1999.

[11] G. D. Forney, M. Grassl, and S. Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Trans. Inf. Theory*, 53(3):865–880, March 2007.

[12] M. Grassl. New binary codes from a chain of cyclic codes. *IEEE Trans. Inf. Theory*, 47(3):1178–1181, March 2001.

[13] M. Grassl and T. Beth. Quantum BCH codes. In *Proc. X Int. Symp. Theor. Elec. Eng.*, pages 207–212, Magdeburg, Germany, 1999. Available online: www.arXiv.org/quant-ph/9910060v1.

[14] M. Grassl and M. Rötteler. Quantum block and convolutional codes from self-orthogonal product codes. In *Proc. Int. Symp. Inf. Theory (ISIT)*, pages 1018–1022, 2005.

[15] R. Li and X. Li. Binary construction of quantum codes of minimum distances five and six. *Discrete Mathematics*, 308:1603–1611, 2008.

[16] A. Salah, A. Klappenecker, and P.K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inf. Theory*, 53(3):1183–1188, March 2007.

[17] A. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inf. Theory*, 45(7):2492–2495, November 1999.

[18] A. M. Steane. Quantum Reed-Muller codes. *IEEE Trans. Inf. Theory*, 45(5):1701–1703, July 1999.

[19] B. Sundeep and A. Thangaraj. Self-orthogonality of q-ary images of q^m-ary codes and quantum code construction. *IEEE Trans. Inf. Theory*, 53(7):2492–2495, July 2007.

[20] A. Thangaraj and S. McLaughlin. Quantum codes from cyclic codes over GF(4^m). *IEEE Trans. Inf. Theory*, 47(3):1176–1178, March 2001.

[21] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh. Graphical nonbinary quantum error-correcting codes. Technical report, Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China 2Physics Department, National University of Singapore, 2 Science Drive 3, Singapore 117542, 2008. Available online: www.arXiv.org/quant-ph/0801.0831.

[22] P. Lang and P. W. Shor. Nonadditive quantum error correcting codes adapted to the amplitude damping channel. Technical report, Department of Mathematics, MIT, Cambridge, MA02139, 2007. Available online: www.arXiv.org/quant-ph/0712.2586.

[23] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh. Nonadditive quantum error-correcting code. Technical report, Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics & Department of Modern Physics University of Science and Technology of China, Hefei 230026, P.R. China 2Department of Physics, National

University of Singapore, 10 Kent Ridge Crescent, Singapore 119260, 2007. Available online: www.arXiv.org/quant-ph/0704.2122.

[24] S. Yu, Q. Chen, and C. H. Oh. Graphical quantum error-correcting codes. Technical report, 1Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, P.R. China 2Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542, 2007. Available online: www.arXiv.org/quant-ph/0709.1780.

[25] M. S. Postol. A proposed quantum low density parity check code. Technical report, National Security Agency, Fort Meade, MD, August 2001. Available online: www.arXiv.org/quant-ph/0108131v1.

[26] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory*, 44(4):1369–1387, July 1998.

[27] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Int. J. Quan. Inf.*, 2(1):55–64, 2004.

[28] R. Li and X. Li. Binary construction of quantum codes of minimum distance three and four. *IEEE Trans. Inf. Theory*, 50:1331–1336, June 2004.

[29] P. K. Sarvepalli and A. Klappenecker. Nonbinary quantum Reed-Muller codes. In *Proc. Int. Symp. Inf. Theory (ISIT)*, 2005.

[30] L. Xiaoyan. Quantum cyclic and constacyclic codes. *IEEE Trans. Inf. Theory*, 50(3):547–549, March 2004.

[31] L. Zhang and I. Fuss. Quantum Reed-Muller codes. Technical report, Communications Division Defence Science and Technology Organisation P O Box 1500, Salisbury, South Australia 5108, 1997.

[32] Z. Li, L. J. Xing, and X. M. Wang. Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance-separable codes. *Phys. Rev. A*, 77:012308, 2008.

[33] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[34] S. T. J. Fenn, M. Benaissa, and D. Taylor. GF(2^m) multiplication and division over the dual basis. *IEEE Trans. Comp.*, 45(3):319 –327, March 1996.

[35] S. Lin and D. J. Costello Jr. *Error Control Coding, Fundamentals and Applications*. Prentice-Hall, 1983.

[36] W. W. Peterson and W. J. Weldon Jr. *Error-Correcting Codes*. MIT Press, 1972.

[37] G. Hughes. Constacyclic codes, cocycles and a $u + v|u - v$ construction. *IEEE Trans. Inf. Theory*, 46(2):674–680, March 2000.

[38] J. M. Jensen. A class of constacyclic codes. *IEEE Trans. Inf. Theory*, 40(3):951–954, May 1994.

[39] N. Kamiya. High-rate quasi-cyclic low-density parity-check codes derived from finite affine planes. *IEEE Trans. Inf. Theory*, 53(4):1444–1459, April 2007.

[40] A. Krishna and D. V. Sarwate. Pseudocyclic maximum-distance-separable codes. *IEEE Trans. Inf. Theory*, 36(4):880–884, July 1990.

[41] E. Louidor and R. M. Roth. Lowest density MDS codes over extension alphabets. *IEEE Trans. Inf. Theory*, 52(7):3186–3197, July 2006.

[42] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inf. Theory*, 45(6):1827–1832, September 1999.

[43] R. M. Roth and A. Lempel. On MDS codes via Cauchy matrices. *IEEE Trans. Inf. Theory*, 35(6):1314–1319, November 1989.

[44] R. M. Roth and G. Seroussi. On cyclic MDS codes of length q over gf(q). *IEEE Trans. Inf. Theory*, 32(2):284–285, March 1986.

[45] J. Georgiades. Cyclic $(q + 1, k)$-codes of odd order q are not optimal. *Atti. Sem. Mat. Fis. Univ. Mod.*, XXX:284–285, 1982.

[46] H. Whitney. On the abstract properties of linear dependence. *Amer. J. Math.*, 57:509–533, 1935.

[47] C. Greene. Weight enumeration and the geometry of linear codes. *Studies in Applied Mathematics*, 55:119–128, 1976.

[48] T. Britz. Extensions of the critical theorem. *Discrete Math.*, 305:55–73, 2005.

[49] N. Kashyap. A decomposition theory for binary linear codes. Submitted to IEEE Trans. Inform. Theory Nov. (2006).

[50] N. Kashyap. Matroid pathwidth and code trellis complexity. Submitted to SIAM Journal on Discrete Mathematics (2007).

[51] A. Barg. The matroid of supports of a linear code. *Applicable Algebra in Engineering, Communication and Computing*, 8(2):165–172, January 1997.

[52] J. G. Oxley. *Matroid Theory*. Oxford University Press, 1992.

[53] T. Britz. Higher support matroids. *Discrete Mathematics*, 307(17-18):2300–2308, August 2007.