Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Departamento de Engenharia Elétrica
Programa de Pós-Graduação em Engenharia Elétrica

Tese de Doutorado

Códigos Algébrico-Geométricos e suas Aplicações à Teoria de Códigos Quânticos

Francisco Revson Fernandes Pereira

Campina Grande – PB, Brasil
Novembro – 2019

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

Códigos Algébrico-Geométricos e suas Aplicações à Teoria de Códigos Quânticos

Francisco Revson Fernandes Pereira

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande como parte dos requisitos necessários para obtenção do grau de Doutor em Ciências, no domínio da Engenharia Elétrica.

Área de Concentração: Processamento da Informação.
Linha de Pesquisa: Eletrônica e Telecomunicações.

Prof. Francisco Marcos de Assis, Dr.
Prof. Giuliano Gadioli La Guardia, Dr.
Orientadores

Campina Grande – PB, Brasil
Novembro – 2019

P436c Pereira, Francisco Revson Fernandes.
Códigos algébrico-geométricos e suas aplicações à teoria de códigos quânticos / Francisco Revson Fernandes Pereira. – Campina Grande, 2019.
119 f. : il. color.

Tese (Doutorado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2019.
"Orientação: Prof. Dr. Francisco Marcos de Assis, Prof. Dr. Giuliano Gadioli La Guardia".
Referências.

1. Códigos Algébrico-Geométricos. 2. Códigos Estabilizadores. 3. Códigos Quânticos Assistidos por Emaranhamento. 4. Códigos Convolucionais Clássicos e Quânticos. I. Assis, Francisco Marcos de. II. La Guardia, Giuliano Gadioli. III. Título.

CDU 621.391(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA MARIA ANTONIA DE SOUSA CRB 15/398

"CÓDIGOS ALGÉBRICO-GOMÉTRICOS E SUAS APLICAÇÕES À TEORIA DE CÓDIGOS QUÂNTICOS
"

FRANCISCO REVSON FERNANDES PEREIRA

TESE APROVADA EM 26/11/2019

FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador(a)

GIULIANO GADIOLI LA GUARDIA, Dr., UEPG-PR
Orientador(a)

FERNANDO EDUARDO TORRES ORIHUELA, Dr., UNICAMP
Examinador(a)

WASHINGTON LUIZ ARAUJO NEVES, Ph.D., UFCG
Examinador(a)

LEOCARLOS BEZERRA DA SILVA LIMA, D.Sc., UFCG
Examinador(a)

SUELI IRENE RODRIGUES COSTA, Dr., UNICAMP
Examinador(a)

CAMPINA GRANDE - PB

Aos meus pais, Auxiliadora (Dorinha) e Francisco (Chico).

Agradecimentos

Um amigo uma vez me disse que o doutorado é como escalar uma montanha. Diversos altos e baixos surgem durante a subida. Em alguns momentos pensamos que estamos perdidos. Até que uma luz (ou uma corda, fazendo um paralelo com a escalada) aparece e conseguimos superar o obstáculo. E no sonhado topo da montanha, que almejamos desde o início, estão o aprendizado de ser pesquisador, a tese de doutoramento e as publicações vinculadas. Essa escalada seria impossível sem a presença de diversas pessoas e entidades. E é para elas que eu quero agradecer.

Primeiramente, mesmo não sendo uma pessoa muito religiosa, queria agradecer a Deus. Essa entidade espiritual que nos rodeia, nos dá força e perseverança nos momentos mais difíceis foi imprescindível nesses quatro anos.

Agradeço à minha família pelo apoio e ensinamentos. À mainha, por ter se virado e revirado a me dar o estudo que tenho e por me mostrar que com ele eu posso ir para onde quiser. Ao meu pai, homem de coração mais mole que conheço, por sempre estar de braços abertos e disposto a me ajudar seja no que for. À minha irmã Allyne, por me mostrar o quão longe uma pessoa pode chegar com esforço e motivação. Ao meu irmão Renê, por fazer parte dos momentos de lazer, fornecendo-me uma recarga de energia para continuar essa jornada.

Agradeço ao professor Francisco Marcos de Assis pelo suporte durante a execução desta tese de doutoramento e por ser um dos principais motivos de ter seguido a área de Teoria da Informação Clássica e Quântica. Agradeço por ter aceita as propostas mais sem pé nem cabeça que eu propunha. Minhas terças-feiras nunca mais serão as mesmas sem as reuniões e discussões do senhor.

Também agradeço ao professor Giuliano G. La Guardia por ter me mostrado as entrelinhas do que é fazer pesquisa. Sua paixão, seriedade e dedicação me mostrou que pesquisar é uma atividade gostosa, mas árdua, um bom pesquisador vive sua pesquisa. Além disso, sou grato pelas suas motivações a voar o mais alto que pudesse. Muito obrigado, meu amigo.

Agradeço ao professor Ruud Pellikaan por ter me aceitado à passar um ano na *Eindhoven University of Technology*. Também agradeço pelo suporte na construção da minha carreira através do estimulo a pesquisa e a apresentar trabalhos em diversos congressos. O senhor me mostrou o lado humano de um grande pesquisador, mostrou-me que simplicidade, companheirismo e respeito são os atributos mais importantes que qualquer profissional deve

ter. Eu espero trabalhar novamente com o senhor em um futuro próximo.

Agradeço ao professor e tio Pedro Dantas Fernandes por ser a pessoa mais íntegra e sábia que já conheci. O senhor é o modelo de ser humano que desejo ser para minha vida pessoal e profissional. Obrigado por ser meu ponto de apoio desde a graduação para qualquer coisa que acontecesse. Estarei em eterna dívida com o senhor.

Agradeço aos amigos que conquistei durante minha estadia na *Eindhoven University of Technology*, em especial a Gustavo, Leon, Lorenz, Andy, Simon, Daan, Alessandro, Stefan e Manos por ter me ajudado a tornar essa experiência longe de casa mais alegre e produtiva. Sentirei falta dos almoços, das cervejas da sexta-feira e das minhas tentativas de jogar pebolim.

Agradeço aos colegas de trabalho do IQuanta, sejam eles professores, alunos, e ex-alunos, dos quais tive apoio e com quem tive oportunidade de conviver e dividir conhecimento. Em especial à Elloá, por ter me introduzido na pesquisa durante minha graduação, e à Milena, Taciana, Micael e Juliana, pelas conversas descontraídas e debates científicos.

Agradeço ao professor e amigo Danieverton (Dani) Moretti por ter aceitado a ensinar Mecânica Quântica a um aluno sonhador mas bastante ingênuo. Além disso, por ter me dado suporte a procurar novos ares e pelos momentos de descontração.

Agradeço aos amigos que tenho desde a graduação, Joãozim, Serafa, Dudz, Lolo, Lalau, Roiben, Thaís e Túlio. Vocês tornaram o ambiente estressante da universidade em um local suportável e, algumas vezes, até agradável.

Agradeço a todos os funcionários do Departamento de Engenharia Elétrica, em especial à Ângela por ter me ajudado com quaisquer problemas de cunho administrativo que surgisse. Ao CNPq, à CAPES, e à COPELE, pelo suporte e financiamento.

Por fim, mas não menos importante, agradeço a minha futura esposa Paloma por estar sempre ao meu lado dando apoio e suporte. Você é a pessoa mais compreensiva que conheço. Obrigado por sempre estar ao meu lado, estando fisicamente próxima ou não. Sem você eu não tenho certeza se conseguiria terminar esta tese com todas minhas faculdades mentais.

“If I have seen further it is by standing
on the shoulders of Giants.”
(Isaac Newton)

Resumo

Nesta tese de doutorado são investigadas aplicações de códigos algébrico-geométricos na construção de códigos estabilizadores, códigos quânticos assistidos por emaranhamento e códigos convolucionais clássicos e quânticos. Uma análise comparativa dos códigos criados com os códigos presentes na literatura também é feita. O primeiro resultado mostrado é sobre a obtenção de novos códigos algébrico-geométricos a partir de considerações sobre divisores de corpos de funções. Posteriormente, para a classe de códigos estabilizadores, dois tipos de métodos de construções de códigos estabilizadores com comprimento finito, e um para análise assintótica de códigos derivados de uma torre de códigos algébrico-gemétricos, são apresentados. Essa análise assintótica é feita sobre expansão de códigos algébrico-geométricos, o que difere dos trabalhos anteriores da literatura. Partindo para os códigos quânticos assistidos por emaranhamento, é mostrado que a utilização de códigos algébrico-geométricos na construção de códigos quânticos assistidos por emaranhamento é possível através de um resultado mostrado também nesta tese. Com isso, são construídas três famílias de códigos quânticos assistidos por emaranhamento utilizando a construção euclidiana destes códigos quânticos, além de mais uma pela construção hermitiana. Também é mostrado a existência de uma família assintoticamente boa, em termos de taxa e emaranhamento relativo, de códigos quânticos assistidos por emaranhamento. Códigos cíclicos também são aplicados na construção de códigos quânticos assistidos por emaranhamento. Descrevendo códigos cíclicos via conjunto de definição é possível diminuir a complexidade de criação e descrição dos códigos quânticos criados. Duas famílias com parâmetros ótimos são construídas através da utilização de códigos cíclicos. Por fim, para a construção de códigos convolucionais clássicos via códigos de blocos, é utilizado o método de construção proposto inicialmente por Piret. Uma análise deste método é feita por meio da construção de uma matriz geradora na forma canônica controladora e pelo cálculo da identidade de MacWilliams. Aplicando códigos algébrico-geométricos ao método de Piret são criados novos códigos convolucionais com parâmetros melhores que os códigos convolucionais existentes na literatura. Também são construídos códigos convolucionais quânticos a partir de códigos algébrico-geométricos.

Palavras-Chave: Códigos Algébrico-Geométricos, Códigos Estabilizadores, Códigos Quânticos Assistidos por Emaranhamento e Códigos Convolucionais Clássicos e Quânticos.

Abstract

In this thesis, applications of algebraic geometry codes in the construction of stabilizer codes, entanglement-assisted quantum error correcting codes, and classical and quantum convolutional codes are investigated. A comparative analysis of the codes created with the codes present in the literature is also made. The first result shown is about obtaining new algebraic geometry codes from considering divisors from algebraic function field with some properties. In the following, for the class of stabilizer code, two types of finite-length stabilizer code are constructed and a asymptotic analysis of codes derived from a tower of algebraic geometry are presented. This asymptotic analysis is made from the expansion of algebraic geometry codes, which differs from previous works in the literature. In the area of entanglement-assisted quantum codes, it is shown that the use of algebraic geometry codes in the construction of entanglement-assisted quantum codes is possible through a result also shown in this thesis. Applying this result, three families of entanglement-assisted quantum codes are constructed using the Euclidean construction of these quantum codes, and one more by the Hermitian construction. It is shown the existence of an asymptotically good family, in terms of rate and relative entanglement, of quantum codes assisted by entanglement. Cyclic codes are also applied in the construction of entanglement-assisted quantum codes. By describing cyclic codes via the defining set, it is possible to easily create and describe the quantum codes created. Two families with optimal parameters are constructed using cyclic codes. Finally, for the construction of classical convolutional codes via block codes, the method proposed by Piret is used. An analysis of this method is made by constructing a generating matrix in the controller canonical form and by computing the MacWilliams identity. As shown, applying algebraic geometry codes to the Piret method create new convolutional codes with better parameters than existing ones in the literature. Quantum convolutional codes are also constructed from algebraic geometry codes.

Key-Words: Algebraic Geometry Codes, Stabilizer Codes, Entanglement-Assisted Quantum Error Correcting Codes, and Classical and Quantum Convolutional Codes.

Lista de Figuras

Lista de Tabelas

Lista de Símbolos e Terminologia

$\mathcal{C}$	Código Clássico Linear
$:=$	Definição
$\mathbb{F}_q$	Corpo Finito com q Elementos
$R(\mathcal{C})$	Taxa de Informação do Código $\mathcal{C}$
$d(\mathcal{C})$	Distância Mínima do Código $\mathcal{C}$
$[n, k, d]_q$	Parâmetros de um Código Linear Definido sobre $\mathbb{F}_q$
$\langle \mathbf{u}, \mathbf{v} \rangle$	Produto Interno Euclidiano entre os Vetores $\mathbf{u}$ e $\mathbf{v}$
$\langle \mathbf{u}, \mathbf{v} \rangle_s$	Produto Interno Simplético entre os Vetores $\mathbf{u}$ e $\mathbf{v}$
$\langle \mathbf{u}, \mathbf{v} \rangle_a$	Produto Interno Alternante entre os Vetores $\mathbf{u}$ e $\mathbf{v}$
$\mathcal{C}^{\perp}$	Dual Euclidiano do Código Linear $\mathcal{C}$
$\mathcal{C}^{\perp_h}$	Dual Hermitiano do Código Linear $\mathcal{C}$
$\mathbb{F}_q[x]$	Anel de Polinômios na Variável x
R	Anel Quociente
$g(x)$	Polinômio Gerador
$\mathbb{C}_i$	Classe Lateral Ciclotômica Contendo o Elemento i
$Z(\mathcal{C})$	Conjunto de Definição do Código Cíclico $\mathcal{C}$
$\equiv \mod m$	Congruência Módulo m
BCH	Código de Bose-Chaudhuri-Hocquenghem
RS	Código de Reed-Solomon
AG	Código Algébrico-Geométrico
$F/\mathbb{F}_q$	Corpo de Função Algébrica
g	Gênero da Curva
$\deg(D)$	Grau de um Divisor D
$G \cup H$	União dos Divisores G e H
$G \cap H$	Interseção dos Divisores G e H
$\mathcal{L}(G)$	Espaço de Riemann-Roch associado ao Divisor G
ω ou η	Diferencial de Weil de um Corpo de Funções
$H(Q)$	Semigrupo de Weierstrass do Divisor Q
$\mathcal{T}(F_1, F_2, \ldots)$	Torre de Corpos Funções
B	Base de um Espaço Vetorial

$\mathcal{H}_q$ ou $\mathbb{C}^q$	Espaço de Hilbert Complexo com dimensão q
$\|\psi\rangle$	Vetor Complexo do Espaço de Hilbert
$\langle\psi\|$	Vetor Complexo do Espaço de Hilbert Dual a $\|\psi\rangle$
E	Operador de Erro
$\{I, X, Z, Y\}$	Conjunto das Matrizes de Pauli
$\mathcal{E}$	Conjunto dos Operadores de Erro
G_n	Grupo de Erro do Espaço $\mathcal{H}_q^n$
$\mathcal{S}$	Estabilizador de Código Quântico
$\mathcal{S} \leq G_n$	$\mathcal{S}$ é um Subgrupo de G_n
$C_{G_n}(\mathcal{S})$	Centralizador de $\mathcal{S}$ em G_n
$Z(G_n)$	Centro de G_n
$\mathcal{Q}$	Código Quântico
$[[n, k, d]]_q$	Parâmetros de um Código Quântico Definido sobre $\mathcal{H}_q$
$A \setminus B$	Conjuntos dos Elementos de A que não Pertencem a B
$\mathbb{N}_0$	Conjunto dos Número Inteiros Não-negativos
$(\mathbf{u}\|\mathbf{v})$	Concatenação dos Vetores $\mathbf{u}$ e $\mathbf{v}$
swt$((\mathbf{u}\|\mathbf{v}))$	Peso Simplético do Vetor Concatenado $(\mathbf{u}\|\mathbf{v})$
wt(E)	Peso do Operador E
Tr(E)	Traço da matriz A
$\text{tr}_{q/p}(\alpha)$	Traço do Elemento $\alpha \in \mathbb{F}_q$ Relativo à Extensão $\mathbb{F}_p \subseteq \mathbb{F}_q$
$\mathcal{N}$	Canal de Comunicação Ruidoso
$\mathcal{D}$	Processo de Decodificação
$[[n, k, d; c]]_q$	Parâmetros de um Código Quântico Assistidos por Emaranhamento
rank(A)	Posto da matriz A
$\mathcal{V}_\mathcal{C}$	Código Convolucional Clássico
$\mathcal{V}_\mathcal{Q}$	Código Convolucional Quântico
QCC	*Quantum Convolutional Code*
$G(D)$	Matriz Geradora Polinomial de um Código Convolucional
$H(D)$	Matriz Verificadora de Paridade Polinomial de um Código Convolucional
$\mathcal{H}(P)$	Matriz P-MacWilliams

Sumário

CAPÍTULO 1

Introdução

1.1 – Motivação e Contextualização

Singularidades são eventos que mudam totalmente o meio em que estão inseridas. Estas impõem mudanças nos meios social, comercial e tecnológico que são, muitas vezes, imprevisíveis. Isso também ocorre nas esferas científicas. O artigo de Claude Elwood Shannon, publicado em 1948, com certeza foi uma dessas singularidades [1]. Publicado no *Bell System Technical Journal*, e contendo alguns dos resultados da sua pesquisa durante a Segunda Guerra Mundial, esse artigo é o marco histórico da criação da Teoria da Informação. Claude Shannon apresentou no artigo diversas medidas de informação que são utilizadas até hoje, tais como entropia, informação mútua e capacidade de canal. Além disso, ele demonstrou o Teorema de Codificação de Canal Ruidoso, no qual diz que, para qualquer nível de contaminação do ruído sobre um canal, é possível transmitir informação de forma confiável por meio de uma codificação de canal. Entretanto, no referido artigo ele não mostra como construir tais códigos para canal; este trabalho vem sendo realizado por outros pesquisadores também historicamente importantes.

A Teoria de Códigos para canal (também denominada de códigos para correção e/ou controle de erros) teve como trabalho pioneiro o artigo de Richard W. Hamming, publicado em 1950 [2]. Esse trabalho de Hamming fundamentou várias ideias, tais como a de distância entre palavras-código e equivalência entre códigos, além de propor o código que leva seu nome, o código de Hamming. Posteriormente, foram introduzidos na literatura o código de Reed-Solomon (RS) [3], o código Bose-Chaudhuri-Hocquenghem (BCH) [4, 5], os códigos de Goppa [6], entre outros. A procura por códigos com bons parâmetros sempre estimulou diversos trabalhos na literatura. Assim, Goppa notou que códigos derivados de curvas algébricas forneciam uma fonte consistente para códigos com parâmetros (assintoticamente) bons, o que fez com que surgisse os códigos algébrico-geométricos (AG, do inglês *algebraic geometric codes*) [7, 8].

Códigos AG formam uma subclasse da família de códigos lineares. Tais códigos utilizam

técnicas e recursos de Álgebra e Geometria Algébrica para a construção de códigos com diversas propriedades e características. Muitas das técnicas utilizadas na criação de códigos AG são matematicamente elegantes; porém, exigem um conhecimento bastante aprofundado da matemática em que se baseiam. Em poucas palavras, os códigos AG utilizam as ideias relacionadas às curvas algébricas, tais como pontos racionais, divisores e gênero. O interesse científico abrangente por essa classe de códigos ocorreu quando M. Tsfasman, S. G. Vladuts e T. Zink mostraram [9], em 1982, a existência de famílias infinitas de códigos AG que excedem o limitante de Gilbert-Varshamov [10, 11]. Esse foi o primeiro momento em que uma classe de códigos obteve tal feito. Além da área de comunicações, códigos AG podem ser utilizados nas áreas de Criptografia de Chave Pública [12, 13] e de Computação e Informação Quânticas [14–16].

O nível de miniaturização dos dispositivos de comunicação e de computação fez com que surgisse uma nova *singularidade científica*, a criação das áreas de computação e informação quânticas. Teoria da Informação Quântica possui uma subárea que é denominada codificação quântica para canal. O surgimento de códigos para correção de erros quânticos (ou códigos quânticos, por simplicidade) ocorreu devido à necessidade de proteger computadores quânticos da ação de ruídos internos e externos, pois esse é o único método para construir computadores quânticos de médio e grande porte, com altos níveis de confiabilidade. O primeiro desses códigos foi desenvolvido por Peter Shor, em 1995 [17] e por Steane, em 1996 [18]. Porém, foi somente com a criação dos códigos CSS feita por R. Calderbank, P. Shor e A. Steane [19] e sua generalização, denominada códigos estabilizadores quânticos (ou somente códigos estabilizadores), por Daniel Gottesman [20], que a área teve um avanço significativo. Diversos trabalhos acadêmicos que vieram posteriormente empenharam-se na aplicação de tais métodos de construção para a criação de novos códigos quânticos [21–23]. A utilização de códigos AG para construir códigos estabilizadores também é encontrada na literatura [24–33]. Entretanto, esses artigos lidam com códigos AG de 1 ou 2 lugares racionais. Assim sendo, uma generalização para códigos AG de t-lugares racionais e de lugares não-racionais não existia, além da construção de códigos estabilizadores assintoticamente bons derivados de códigos AG com certas propriedades.

Códigos estabilizadores possuem propriedades úteis e práticas de forma a que possam ser eficientemente utilizados em computadores quânticos e sistemas de comunicações quânticas. Entretanto, sua capacidade de correção pode ser melhorada se pares de estados emaranhados forem compartilhados entre o transmissor e receptor antes do processo de comunicação. Códigos quânticos que utilizam tais pares de estados emaranhados são denominados códigos quânticos assistidos por emaranhamento (códigos QUENTA[1]). Além dessa melhoria de capacidade de correção, esses códigos atingem o limitante *hashing* [34, 35] e violam o limitante quântico de Hamming [36]. O primeiro código QUENTA foi proposto por Bowen [37], seguido

[1]Também é possível encontrar na literatura a denominação códigos EAQEC. Porém, por motivos de fonética do acrônimo anterior, optou-se por códigos QUENTA.

pelo artigo de Fattal, *et al.* [38]. O formalismo estabilizador para códigos QUENTA foi criado por Brun *et al.* [39], em que foi mostrado que para a criação de códigos QUENTA não há a necessidade da hipótese de auto-dualidade como é presente em códigos estabilizadores [40]. Wilde e Brun [41] propuseram dois métodos de criação de códigos QUENTA a partir de códigos lineares, os quais são denominados métodos de construção euclidiano e hermitiano. A generalização do formalismo estabilizador para códigos quânticos definidos sobre qudits foi recentemente apresentada à academia por meio do trabalho de Galindo, *et al.* [42] Esse trabalho mostra que ainda há muito a ser produzido na área de códigos QUENTA. Depois desses trabalhos de Brun *et al.*, diversos artigos focaram na construção de códigos QUENTA com base em códigos lineares [41, 43–46]. Entretanto, análises de códigos QUENTA q-ários foram feitas somente recentementes [43, 45–52]. Em particular, não havia trabalhos com a utilização explícita de códigos algébrico-geométricos, o que fornece uma oportunidade de criação de códigos que tenham comprimentos grandes, quando comparados sobre o mesmo corpo finito, e sejam assintoticamente bons.

Sobre o paradigma da Mecânica Quântica, existe outra classe de códigos corretores de erros, os quais são denominados códigos convolucionais quânticos. Tais códigos podem ser utilizados em comunicações quânticas, pois seus processos de codificação e decodificação podem ser feitos *online*. Um dos primeiros trabalhos a ter relevância na área foi o de H. Ollivier e J.-P. Tillich [53]. Diversas pesquisas vieram posteriormente [54–57]. Em 2007, Aly, *et al.* generalizaram o método proposto por Piret [58], o qual consiste em construir códigos convolucionais clássicos a partir de códigos de bloco [59]. Vários trabalhos existentes na literatura utilizam essa construção de Piret para obter novos códigos convolucionais clássicos e quânticos [22, 32, 60, 61]. Entretanto, não existiam, na época, trabalhos utilizando códigos AG para a construção de códigos convolucionais quânticos. Além disso, a construção de códigos convolucionais pelo método de Piret utilizando códigos AG também não existia na literatura.

Códigos estabilizadores, assistidos ou não por emaranhamento, e códigos convolucionais clássicos e quânticos são essenciais tanto para o desenvolvimento de computadores quânticos quanto para a área de comunicações quânticas. Assim, esta tese almeja a ampliação das ferramentas fundamentais para esse desenvolvimento. O objetivo aqui é dar suporte a mais nova singularidade científica de Teoria da Informação, a qual já está mudando o mundo ao nosso redor.

1.2 – Objetivos

Com base no que foi apresentado, os objetivos gerais desta tese de doutorado são

1. Desenvolver métodos de construção de códigos algébrico-geométricos de forma a gerar propriedades atratíveis para a construção de códigos de outras áreas de codificação, tais como códigos quânticos e convolucionais.

2. Generalizar alguns resultados sobre códigos estabilizadores utilizando códigos algébrico-geométricos.

3. Aplicar a descrição de conjunto de definição de códigos cíclicos de forma a simplificar a descrição dos parâmetros dos códigos assistidos por emaranhamento construídos a partir destes códigos cíclicos. Análise comparativa dos códigos contruídos com os existentes na literatura.

4. Criar, pela primeira vez na literatura, códigos quânticos assistidos por emaranhamento a partir de códigos algébrico-geométricos. Fazer uma análise para códigos com comprimento finito e uma análise assintótica.

5. Construir um codificador na forma canônica controladora e calcular a identidade de MacWilliams para o os códigos convolucionais derivados do método de construção proposto por Piret.

6. Utilizar códigos algébrico-geométricos no método de construção de códigos convolucionais de Piret para obter códigos com distância livre superior aos da literatura. Aplicar puncionamento, extensão, expansão e produto a códigos algébrico-geométricos para construir códigos convolucionais com uma maior diversidade de parâmetros.

7. Gerar famílias de códigos quânticos convolucionais utilizando códigos algébrico-geométricos e comparar os parâmetros de tais códigos com os existentes na literatura.

1.3 – Organização do Trabalho

Nesta tese, a aplicação de códigos algébrico-geométricos na construção de novos códigos pertencentes às classes de códigos estabilizadores, quânticos assistidos por emaranhamento e convolucionais clássicos e quânticos é feita. Os Capítulos 2 e 3 apresentam uma mescla entre a fundamentação teórica necessária para o entendimento da pesquisa efetuada e alguns resultados obtidos relacionados a códigos algébrico-geométricos e estabilizadores. Os Capítulos 4 e 5 utilizam essa fundamentação teórica para firmar a construção de novos códigos quânticos assistidos por emaranhamento e convolucionais clássicos e quânticos, respectivamente. Por fim, o Capítulo 6 apresenta as considerações finais e os possíveis trabalhos futuros a serem feitos a partir desta tese. O detalhamento da organização desta tese é apresentado a seguir:

Capítulo 2: A teoria de códigos lineares, códigos cíclicos e códigos algébrico-geométricos é construída e explanada. São apresentados limitantes inferiores e superiores para estes códigos que serão utilizados ou generalizados nos capítulos seguintes. Por fim, são descritas três novas construções de códigos algébrico-geométricos;

Capítulo 3: Apresenta o formalismo estabilizador para os códigos quânticos utilizados nesta tese. É feita uma generalização dos limitantes apresentados no capítulo anterior para códigos quânticos estabilizadores. Em seguida, são expostos novos códigos quânticos estabilizadores via códigos algébrico-geométricos para situações de comprimento finito e análise assintótica;

Capítulo 4: Por meio de uma motivação exemplificativa, é construído intuitivamente o formalismo estabilizador para códigos quânticos quando estes utilizam emaranhamento como fonte auxiliar aos processos de codificação e decodificação. Dois métodos gerais de construção de códigos quânticos assistidos por emaranhamento são mostrados. Utilizando esses métodos em códigos cíclicos e códigos algébrico-geométricos, é criada uma variedade de códigos quânticos com parâmetros bons. No final do capítulo, é demonstrada a existência de códigos quânticos assistidos por emaranhados assintoticamente bons em termos de taxa, distância relativa e emaranhamento relativo;

Capítulo 5: Códigos convolucionais são descritos via matrizes geradora e de verificação de paridade. É apresentado o método de construção de códigos convolucionais a partir de códigos de bloco de Piret. Uma análise deste método é feita por meio da construção de uma matriz geradora na forma canônica controladora e pelo cálculo da identidade de MacWilliams. Com a utilização de códigos algébrico-geométricos são construídas várias famílias de códigos convolucionais clássicos e quânticos;

Capítulo 6: É encerrada a tese com considerações sobre os resultados obtidos e sobre trabalhos futuros em potencial.

1.4 – Lista de Publicações

1.4.1 – Publicações e Submissões em Revistas

- Francisco Revson F. Pereira, Giuliano G. La Guardia, and Francisco M. de Assis. "Classical and Quantum Convolutional Codes Derived from Algebraic Geometry Codes," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 73–82, Jan. 2019. Veja a Ref. [62];

- Giuliano G. La Guardia, Francisco Revson F. Pereira, "Good and asymptotically good quantum codes derived from algebraic geometry codes," *Quantum Information Processing*, vol. 16, no. 6, article no. 165, June 2017. Veja a Ref. [63];

- Francisco Revson F. Pereira, Ruud Pellikaan, Giuliano G. La Guardia, Francisco M. de Assis, "Entanglement-assisted Quantum Codes from Algebraic Geometry Codes," arXiv:1907.06357, July 2019. (Submetido para *IEEE Transactions on Information Theory*). Veja a Ref. [64];

- Francisco Revson F. Pereira, "Entanglement-assisted Quantum Codes from Cyclic Codes," arXiv:1911.06384, Nov. 2019. (Submetido para *International Journal of Quantum Information*). Veja a Ref. [65].

1.4.2 – Publicações em Eventos

- Francisco Revson F. Pereira, Ruud Pellikaan, Giuliano G. La Guardia, Francisco M. de Assis, "Application of Complementary Dual AG Codes to Entanglement-Assisted Quantum Codes," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 2559–2563, Paris, France, 2019;

- Francisco Revson F. Pereira, Ruud Pellikaan, Giuliano G. La Guardia, Francisco M. de Assis, "Entanglement-assisted Quantum Codes from Algebraic Geometry Codes," in *Proceedings of the WCC 2019: The Eleventh International Workshop on Coding and Cryptography*, Saint-Jacut-de-la-Mer, France, 2019;

- Francisco Revson F. Pereira, Giuliano G. La Guardia, "Códigos Convolucionais Quânticos Derivados de Códigos Algébrico-Geométricos," in *Proceedings of the XXXVI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, Campina Grande, Brasil, 2018;

- Francisco Revson F. Pereira, Giuliano G. La Guardia, "Novos Códigos Convolucionais Derivados de Códigos Algébrico-Geométricos," in *Proceedings of the XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, São Pedro, Brasil, 2017.

CAPÍTULO 2

Códigos de Bloco Lineares

Este capítulo apresenta, caracteriza e quantifica códigos de bloco. Inicialmente são descritos a estrutura e parâmetros dos códigos de bloco e, em particular, de códigos lineares. Relações existentes entre matrizes geradora e de verificação de paridade são relembradas. Posteriormente, apresentamos exemplos concretos de códigos cíclicos, tais como os códigos Bose-Chaudhuri-Hocquenghem (BCH, por simplicidade), Reed-Solomon e algébrico-geométrico. O foco deste capítulo é direcionado para o estudo dos códigos algébrico geométricos. Por este motivo, são mostrados detalhes da estrutura algébrica necessária na construção destes códigos, tais como a definição de lugar, divisores e espaço de Riemann-Roch, além das relações entre os parâmetros de um código algébrico-geométrico e de seu respectivo dual euclidiano. Por fim, novos resultados sobre a construção de códigos algébrico-geométricos a partir de códigos algébrico-geométricos já existentes são apresentados no Teorema 2.6 e Proposições 2.14 e 2.15. O Teorema 2.6 está contido na publicação [62] e as Proposições 2.14 e 2.15 estão na publicação [64], ambas tendo o autor desta tese como um dos co-autores. Para o leitor que desejar se aprofundar em códigos lineares e, em particular, em códigos algébrico-geométricos, recomendamos as Refs. [66–71].

2.1 – Códigos de Bloco Clássicos

2.1.1 – Conceitos Introdutórios

Definição 2.1 *Um código q-ário de comprimento n é um subconjunto $\mathcal{C} \subseteq A^n$, em que A é um conjunto com q elementos denominado alfabeto. Os elementos de $\mathcal{C}$ são denominados palavras-código.*

Geralmente, considera-se que o conjunto A é o corpo finito (ou campo de Galois) $\mathbb{F}_q$.

Definição 2.2 *Seja $\mathcal{C}$ um código de comprimento n. A taxa de informação é definida por*

$$R(\mathcal{C}) := \frac{\log_q |\mathcal{C}|}{n}. \tag{2.1}$$

Exemplo 2.1 *Sejam* $\mathbf{v}_1 = (1,0,0,0,1,1,1)$, $\mathbf{v}_2 = (0,1,0,0,1,0,1)$, $\mathbf{v}_3 = (0,0,1,0,1,1,0)$ *e* $\mathbf{v}_4 = (0,0,0,1,0,1,1)$ *vetores linearmente independentes de* $\mathbb{F}_2^7$. *O código formado por todas combinações lineares (em* $\mathbb{F}_q$*) destes vetores é conhecido como código de Hamming em dimensão* 7. *A cardinalidade de* $\mathcal{C}$ *é* $2^4 = 16$, *o que torna* $\mathcal{C}$ *um código com taxa* $R(\mathcal{C}) = \frac{\log_2 16}{7} = \frac{4}{7}$. *Uma possível palvra-código é o vetor* $\mathbf{c} = \mathbf{v}_1 + \mathbf{v}_3 = (1,0,1,0,0,0,1)$.

Definição 2.3 *Um código* $\mathcal{C}$ *será denominado código linear se for um subespaço vetorial de* $\mathbb{F}_q^n$.

Assim, se $\mathcal{C}$ é um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão k, então $|C| = q^k$, em que $|\cdot|$ denota a cardinalidade do conjunto em questão. Aplicando esse resultado na fórmula da taxa de informação obtêm-se $R(\mathcal{C}) = k/n$, o que é normalmente encontrado em livros-texto. Se $\{\mathbf{c}_0, \ldots, \mathbf{c}_{k-1}\}$ é uma base de $\mathcal{C}$, então toda palavra-código pode ser escrita de maneira única como combinação linear dos elementos da base, ou seja,

$$a_0\mathbf{c}_0 + \cdots + a_{k-1}\mathbf{c}_{k-1}, \tag{2.2}$$

em que $a_0, \ldots, a_{k-1} \in \mathbb{F}_q$.

A capacidade de correção de erros de um código depende do tipo do canal ao qual a palavra-código será enviada e do algoritmo de decodificação utilizado. Entretanto, para os casos mais comuns, tais como quando o canal é aditivo e o algoritmo de decodificação é o de decodificação única, existe uma relação direta entre a capacidade de decodificação e a distância mínima do código. Essa distância mínima é geralmente definida mediante a métrica de Hamming.

Definição 2.4 *Sejam* $\mathbf{x} = (x_0, \ldots, x_{n-1})$ *e* $\mathbf{y} = (y_0, \ldots, y_{n-1})$ *dois vetores de* $\mathbb{F}_q^n$. *Então a métrica de Hamming é definida como sendo*

$$d_{\textit{Hamming}}(\mathbf{x}, \mathbf{y}) := |\{i \colon x_i \neq y_i,\ 0 \leq i \leq n-1\}|. \tag{2.3}$$

Neste trabalho, ao invés de adotarmos a notação $d_{\text{Hamming}}(\cdot,\cdot)$ preferiremos a notação $d(\cdot,\cdot)$.

Definição 2.5 *Seja* $\mathcal{C}$ *um código. A distância mínima de* $\mathcal{C}$ *é dada por*

$$d_{\min}(\mathcal{C}) = d(\mathcal{C}) := \min\{d(\mathbf{x}, \mathbf{y}) \colon \mathbf{x}, \mathbf{y} \in \mathcal{C},\ \mathbf{x} \neq \mathbf{y}\}. \tag{2.4}$$

Seja $\mathbf{x} \in \mathbb{F}_q^n$ um vetor. Então seu peso de Hamming é dado pelo número de coordenadas não-nulas. Se $\mathcal{C}$ é um código linear, então é possível mostrar que

$$d(\mathcal{C}) = \text{wt}(\mathcal{C}), \tag{2.5}$$

em que $\text{wt}(\mathcal{C})$ é o menor peso de todas as palavras-código de $\mathcal{C}$ a menos do vetor nulo.

A partir deste momento é possível definir a notação amplamente utilizada para códigos lineares e seus parâmetros.

Definição 2.6 *Sejam $\mathbb{F}_q$ um corpo finito e $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear. Os parâmetros do código linear $\mathcal{C}$ são descritos pela terna de inteiros positivos $[n, k, d]_q$, em que n é o comprimento do código, k é a dimensão de $\mathcal{C}$ sobre $\mathbb{F}_q$ e d representa a distância mínima de $\mathcal{C}$.*

Exemplo 2.2 *Seja $\mathcal{C}$ o código do Exemplo 2.1, gerado pelos vetores $\mathbf{v_1}$, $\mathbf{v}_2$, $\mathbf{v}_3$ e $\mathbf{v}_4$. Então, $\mathcal{C}$ é um código linear, pois soma de vetores do código e multiplicação por constantes fornecem vetores que também são combinações lineares dos vetores $\mathbf{v_1}$, $\mathbf{v}_2$, $\mathbf{v}_3$ e $\mathbf{v}_3$. Tome, por exemplo, as palavras-código $\mathbf{c}_1 = \mathbf{v}_1 + \mathbf{v}_2$ e $\mathbf{c}_2 = \mathbf{v}_2 + \mathbf{v_3}$, então tem-se que $\mathbf{c}_3 = \mathbf{c}_1 + \mathbf{c}_2 = \mathbf{v}_1 + \mathbf{v}_3 \in \mathcal{C}$. Os parâmetros de $\mathcal{C}$ podem ser facilmente obtidos pela observação de alguns fatos. Primeiramente, como $\mathcal{C}$ é gerado por quatro vetores e não há um conjunto de geradores com cardinalidade menor que produza $\mathcal{C}$, tem-se que a dimensão de $\mathcal{C}$ é $k = 4$. Por outro lado, comparando as possíveis palavras-código de $\mathcal{C}$, vê-se que a distância mínima entre duas palavras-código é 3. Isso faz com que $\mathcal{C}$ seja um código $[7, 4, 3]_2$.*

2.1.2 – Propriedades de Códigos Lineares

Códigos lineares para correção de erros são os mais estudados na literatura. A razão disso é a facilidade de extração dos seus parâmetros, tais como dimensão e distância mínima, e a existência de métodos práticos para codificação e decodificação, principalmente por causa da existência de uma transformação linear que os descreve. Essa transformação linear é descrita por meio de uma matriz geradora do código.

Definição 2.7 *Os códigos lineares podem ser obtidos como imagem de uma transformação linear injetiva*

$$\Phi \colon \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n \tag{2.6}$$

$$(a_0, \ldots, a_{k-1}) \mapsto (a_0, \ldots, a_{k-1}) \cdot G_{k\times n}, \tag{2.7}$$

em que $G_{k\times n}$ é uma matriz com posto k formada por elementos de $\mathbb{F}_q$. Essa matriz é denominada matriz geradora. Uma matriz geradora de um código $[n, k]$ é chamada de sistemática se tiver k colunas que são, em alguma ordem, as k colunas da matriz identidade I_k. Além disso, o código também pode ser definido como sendo o núcleo de uma outra transformação linear

$$\Theta \colon \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n-k}, \tag{2.8}$$

em que $\Phi(\mathbb{F}_q^k) = Núcleo(\Theta)$.

Exemplo 2.3 *Seja $\mathcal{C}$ o código linear do Exemplo 2.1. Uma vez que qualquer palavra-código pode ser gerada dos vetores $\mathbf{v}_1 = (1, 0, 0, 0, 1, 1, 1)$, $\mathbf{v}_2 = (0, 1, 0, 0, 1, 0, 1)$, $\mathbf{v}_3 = (0, 0, 1, 0, 1, 1, 0)$ e $\mathbf{v}_4 = (0, 0, 0, 1, 0, 1, 1)$, temos que uma matriz geradora para este código linear é dada por*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}. \tag{2.9}$$

Como é possível notar, ela está na forma sistemática e, mais especificamente, na forma padrão, pois ela é da forma $G = (I|P)$, com I sendo a matriz identidade.

Relacionado à aplicação Θ, é possível descrever outra matriz, que será denominada de matriz de verificação de paridade.

Definição 2.8 *Seja $\mathcal{C}$ um código linear com matriz geradora G. A matriz de verificação de paridade H é a matriz que tem seu núcleo dado pelos vetores do código $\mathcal{C}$, ou seja,*

$$H\mathbf{c}^T = \mathbf{0} \in \mathbb{F}_q^{n-k} \iff \mathbf{c} \in \mathcal{C} \subset \mathbb{F}_q^n. \tag{2.10}$$

Além disso, tem-se que $GH^T = 0_{k\times(n-k)}$.

Assim sendo, a representação matricial da aplicação Θ é a matriz de verificação de paridade H. O mesmo pode ser dito da aplicação Φ e matriz geradora G. É claro que tais matrizes não são únicas.

Exemplo 2.4 *Continuemos com o código de Hamming do Exemplo 2.1. Utilizando-se a matriz geradora para $\mathcal{C}$ dada no Exemplo 2.3 é possível construir uma matriz de verificação de paridade. Primeiramente, note que $G = (I_{4\times4}|P_{4\times3})$, em que $I_{4\times4}$ é a matriz identidade de tamanho 4×4. Da propriedade de que $GH^T = 0_{4\times3}$, temos que a matriz de verificação de paridade pode ser descrita por $H = (-P_{3\times4}^T|I_{3\times3})$. Assim,*

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{2.11}$$

Agora será definido o dual euclidiano de um código $\mathcal{C}$. Porém, antes é necessário relembrar o produto interno euclidiano entre dois vetores de $\mathbb{F}_q^n$.

Definição 2.9 *Sejam $\mathbf{a} = (a_0, \ldots, a_{n-1})$ e $\mathbf{b} = (b_0, \ldots, b_{n-1})$ dois vetores de $\mathbb{F}_q^n$. O produto interno euclidiano entre eles é dado por*

$$\langle \mathbf{a}, \mathbf{b} \rangle := \sum_{i=0}^{n-1} a_i b_i, \tag{2.12}$$

em que a multiplicação e soma é feita no corpo $\mathbb{F}_q$.

Definição 2.10 *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear. O dual euclidiano de $\mathcal{C}$, denotado por $\mathcal{C}^\perp$, é definido como sendo*

$$\mathcal{C}^\perp := \{\mathbf{u} \in \mathbb{F}_q^n \colon \langle \mathbf{u}, \mathbf{c} \rangle = 0 \text{ para todo } \mathbf{c} \in \mathcal{C}\}. \tag{2.13}$$

É possível mostrar que se $\mathcal{C}$ é um código linear com parâmetros $[n, k]$, então seu dual terá parâmetros $[n, n-k]$ e, além disso, $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. Em particular, a dimensão de um código auto-dual de comprimento n é igual a $n/2$.

Se o corpo tiver cardinalidade q^2, em que q é potência de primo (ou seja, $\mathbb{F}_{q^2}$), então é possível definir o dual hermitiano de um código linear.

Definição 2.11 *Seja $\mathcal{C}$ um código linear definido sobre o corpo finito $\mathbb{F}_{q^2}$. O dual hermitiano de $\mathcal{C}$ é definido como sendo*

$$\mathcal{C}^{\perp_h} := \{\ \mathbf{u} \in \mathbb{F}_{q^2}^n \colon \langle \mathbf{u}, \mathbf{c}^q \rangle = 0 \text{ para todo } \mathbf{c} \in \mathcal{C}\ \}, \tag{2.14}$$

em que $\mathbf{c}^q = (c_0^q, \ldots, c_{n-1}^q)$.

Exemplo 2.5 *Seja $\mathcal{C}$ o código linear sobre $\mathbb{F}_{2^2}$ gerado pelos vetores $\mathbf{v_1} = (1,0,0,1,1,1)$, $\mathbf{v_2} = (0,1,0,1,\alpha,\alpha+1)$ e $\mathbf{v_3} = (0,0,1,1,\alpha+1,\alpha)$, com $\alpha^2 = \alpha + 1$. Então temos que o código $\mathcal{C}^2$ é gerado pelos vetores $\mathbf{v'_1} = \mathbf{v_1}^2 = (1,0,0,1,1,1)$, $\mathbf{v'_2} = \mathbf{v_2}^2 = (0,1,0,1,\alpha+1,\alpha)$ e $\mathbf{v'_3} = \mathbf{v_3}^2 = (0,0,1,1,\alpha,\alpha+1)$.*

2.1.3 – Códigos Cíclicos

Códigos cíclicos são um subconjunto dos códigos lineares. Tais códigos têm a vantagem de serem descritos por meio de um polinômio, além de possuírem um algoritmo de decodificação bastante eficiente em termos do número de operações realizadas.

Definição 2.12 *Seja $\mathcal{C} \subseteq F_q^n$ um código linear. $\mathcal{C}$ será dito cíclico se, para todo $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$, o vetor $\mathbf{c}' = (c_{n-1}, c_0, \ldots, c_{n-2})$ também pertencer ao $\mathcal{C}$.*

Consideremos uma palavra-código $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$. Podemos associar $\mathbf{c}$ a um polinômio por meio da seguinte transformação linear

$$\phi \colon \mathbb{F}_q^n \rightarrow \mathbb{F}_q[x]/I =: R_n \tag{2.15}$$

$$(c_0, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} = c(x) \tag{2.16}$$

em que $I = \langle x^n - 1 \rangle \subset \mathbb{F}_q[x]$ e R_n é o anel dos polinômios em $\mathbb{F}_q$ de grau menor ou igual a $n-1$.

Com esta observação, podemos descrever as palavras-código de um código cíclico por meio de vetores em $\mathbb{F}_q^n$ ou por meio de polinômios pertencentes ao anel R_n, via a imagem de ϕ sobre o código.

Proposição 2.1 *[67, Teorema 1, Capítulo 6] Seja $\mathcal{C}$ um código linear com parâmetros $[n, k]$. Então $\mathcal{C}$ é um código cíclico se, e somente se, $\phi(\mathcal{C})$ é um ideal de R_n.*

Será mostrado que, uma vez que $\mathcal{C}$ seja cíclico, é possível definí-lo unicamente por meio de um polinômio, denominado polinômio gerador do código.

Proposição 2.2 *[67, Teorema 1, Capítulo 6] Seja $\mathcal{C}$ um código cíclico com parâmetros $[n, k]$. Afirma-se que*

1. *Se $g(x)$ é um polinômio mônico de menor grau pertencente a $\phi(\mathcal{C})$, então $g(x)$ é determinado unicamente em $\phi(\mathcal{C})$ e*

$$\mathcal{C} = \{\phi^{-1}(q(x)g(x)) \colon q(x) \in \mathbb{F}_q[x] \text{ tem grau menor que } n - r\}, \tag{2.17}$$

   em que $r = \deg(g(x))$. Particularmente, $\mathcal{C}$ tem dimensão igual a $k = n - r$.

2. *O polinômio $g(x)$ divide $x^n - 1$ em R_n e é denominado polinômio gerador de $\mathcal{C}$.*

O motivo da existência de um polinômio gerador é o seguinte. Uma vez que todo código cíclico é um ideal no anel principal R_n (ou seja, todo ideal de R_n é gerado por um único elemento), então tem-se que o gerador do ideal que representa o código é o polinômio gerador.

Também é possível mostrar relações entre o polinômio gerador e o polinômio verificador de paridade e as correspondentes matrizes geradora e de paridade. Veja a definição e as duas proposições a seguir.

Definição 2.13 *Seja $g(x)$ o polinômio gerador do código cíclico $\mathcal{C}$. Então é possível definir o polinômio de verificação de paridade da seguinte forma:*

$$g(x)h(x) = x^n - 1. \tag{2.18}$$

Proposição 2.3 *[67, Corolário 2 do Capítulo 6] Seja $\mathcal{C}$ um código cíclico com polinômio gerador $g(x) = \sum_{i=0}^{r} g_i x^i$. Então uma matriz geradora do código é dada por*

$$G = \begin{pmatrix} \phi^{-1}(g(x)) \\ \phi^{-1}(xg(x)) \\ \vdots \\ \phi^{-1}(x^{n-r}g(x)) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{pmatrix}. \tag{2.19}$$

Proposição 2.4 *[67, Teorema 3 do Capítulo 6] Seja $\mathcal{C}$ um código cíclico com polinômio verificador de paridade dado por $h(x) = \sum_{i=0}^{k} h_i x^i$. Então uma matriz de paridade de $\mathcal{C}$ é dada por*

$$H = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}. \tag{2.20}$$

Um método de caracterização dos parâmetros de um código cíclico é mediante o polinômio gerador e do seu conjunto de definição. Para a descrição desse conjunto, considere o seguinte: sejam $m = ord_n(q)$, α um gerador do grupo multiplicativo $\mathbb{F}_{q^m}^*$, e assuma que $\beta = \alpha^{\frac{q^m-1}{n}}$; i.e., β é uma n-ésima raiz primitiva da unidade. Então, o conjunto de zeros de $\mathcal{C}$, o qual é denotado por $Z(\mathcal{C})$, é definido como sendo $Z(\mathcal{C}) := \{i \in \mathbb{Z}_n : c(\beta^i) = 0 \text{ para todo } c(x) \in \mathcal{C}\}$. É possível mostrar que esse conjunto tem uma relação intrínseca com o polinômio gerador do código. Para códigos BCH e Reed-Solomon, os quais são casos particulares dos código cíclicos, tem-se que o conjunto de definição (ou seu polinômio gerador) possui algumas propriedades adicionais. Veja as Definições 2.14 e 2.16.

Códigos BCH

Definição 2.14 *Sejam $b \geq 0$, $\delta \geq 1$ e $\alpha \in \mathbb{F}_{q^m}$, em que $m = ord_n(q)$. Um código cíclico $\mathcal{C}$ de comprimento n sobre $\mathbb{F}_q$ é denominado código BCH com distância de projeto δ se*

$$g(x) = mmc\{m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)\},$$

em que $m_i(x)$ é o polinômio minimal de α^i sobre $\mathbb{F}_q$. Se $n = q^m - 1$ então o código BCH é chamado de primitivo. Por outro lado, se $b = 1$ ele é denominado narrow sense.

Antes de relacionar os parâmetros de um código BCH com seu conjunto de definição, será introduzida a ideia de classe lateral ciclotômica. Esta ferramenta surge da observação de que o polinômio minimal $m_i(x)$ de α^i pode ser o polinômio minimal de outras potências de α. A razão disso é que α pertence a uma extensão de $\mathbb{F}_q$, enquanto que o polinômio $m_i(x) \in \mathbb{F}_q[x]$. O conjunto de todos os zeros de $m_i(x)$ no corpo $\mathbb{F}_{q^m}$ é denotado pela classe lateral ciclotômica de i. Assim, o conjunto de definição é a união das classes ciclotômicas de $b, b+1, \ldots, b+\delta-2$. A seguinte definição descreve classe lateral ciclotômica.

Definição 2.15 *A classe lateral ciclotômica q-ária $\mod n$ contendo o elemento i é definido como*

$$\mathbb{C}_i := \{i, iq, iq^2, iq^3, \ldots, iq^{m_i-1}\}, \tag{2.21}$$

em que m_i é o menor inteiro positivo tal que $iq^{m_i} \equiv i(\mod n)$.

Para os parâmetros de um código BCH, pode ser mostrado que a sua dimensão é igual a $n - |Z(\mathcal{C})|$ e sua distância mínima é limitada inferiormente por δ (quantidade que normalmente é denominada cota BCH) [69]. Desta forma, podemos ver que a quantificação de um código BCH pode ser obtida por meio do seu conjunto de definição. A mesma afirmação pode ser feita sobre o dual euclidiano e hermitiano de um código cíclico; em particular, para códigos BCH e Reed-Solomon. As Proposições 2.5 e 2.6 focam neste aspecto.

Proposição 2.5 *[69, Proposição 4.3.8] Seja $\mathcal{C}$ um código cíclico de comprimento n e conjunto de definição $Z(\mathcal{C})$. Então o conjunto de definição de $\mathcal{C}^{\perp}$ é dado por*

$$Z(\mathcal{C}^{\perp}) = \mathbb{Z}_n \setminus \{-i | i \in Z(\mathcal{C})\}$$

Para códigos BCH, o polinômio gerador do dual euclidiano é dado pelo mínimo múltiplo comum dos polinômios minimais sobre $\mathbb{F}_q$ dos elementos α^j tais que $j \in Z(\mathcal{C}^{\perp})$.

Proposição 2.6 *Seja $\mathcal{C}$ um código cíclico sobre $\mathbb{F}_{q^2}$ com conjunto de definição $Z(\mathcal{C})$. Então*

$$Z(\mathcal{C}^{\perp_h}) = \mathbb{Z}_n \setminus \{-i | i \in qZ(\mathcal{C})\}.$$

Demonstração: Seja $c \in \mathbb{F}_{q^2}^n$ uma palavra-código de $\mathcal{C}$. Escrevendo c^q como polinômio, tem-se que $c^{(q)}(x) = c_0^q + c_1^q x + \cdots + c_{n-1}^q x^{n-1}$. Para $i \in \mathbb{Z}_n$ pertence a $Z(\mathcal{C}^q)$ tem-se que

$$\begin{aligned} c^{(q)}(\alpha^i) = 0 \quad &\iff \quad c_0^q + c_1^q \alpha^i + \cdots + c_{n-1}^q \alpha^{i(n-1)} = 0 \\ &\iff \quad (c_0^q + c_1^q \alpha^i + \cdots + c_{n-1}^q \alpha^{i(n-1)})^q = 0 \\ &\iff \quad c_0 + c_1 \alpha^{iq} + \cdots + c_{n-1} \alpha^{iq(n-1)} = 0 \\ &\iff \quad iq \in Z(C). \end{aligned}$$

Isto mostra que $Z(\mathcal{C}^q) = qZ(\mathcal{C})$. Uma vez que $\mathcal{C}^{\perp_h} = (\mathcal{C}^q)^{\perp}$, tem-se da Proposição 2.5 que $Z(\mathcal{C}^{\perp_h}) = \mathbb{Z}_n \setminus \{-i | i \in qZ(\mathcal{C})\}$. ∎

Exemplo 2.6 *Seja α um elemento primitivo de $\mathbb{F}_{16}$, tal que $1 + \alpha + \alpha^4 = 0$, e $n = 15$. Os polinômios minimais para α, α^3, α^4 sobre $\mathbb{F}_2$ são $m_1(x) = 1 + x + x^4$, $m_3(x) = 1 + x + x^2 + x^3 + x^4$ e $m_5(x) = 1 + x + x^2$. Como pode ser verificado, pelo cálculo do classe lateral ciclotômica de 1, $m_1(x)$ também é o polinômio minimal de α^2, α^4 e α^8. Da mesma forma obtem-se que $m_3(x)$ é o polinômio minimal para α^3, α^6, α^9 e α^{12}. Dito isso, podemos construir um código BCH seguindo a Definição 2.14. Sejam $b = 1$ e $\delta = 5$. O código BCH construído com os parâmetros mencionados tem polinômio gerador*

$$g(x) = mmc\{m_1(x), m_2(x), m_3(x), m_4(x)\} = m_1(x)m_3(x) = 1 + x^4 + x^6 + x^7 + x^8 \quad (2.22)$$

e dimensão igual a $k = n - \deg g(x) = 7$. *Consequentemente, tal código tem parâmetros* $[15, 7, 5]_2$. *Por fim, tem-se que* $Z(\mathcal{C}) = \{1, 2, 3, 4, 6, 8, 9, 12\}$.

Códigos Reed-Solomon

Outra classe de códigos cíclicos utilizados nesta tese são os códigos Reed-Solomon. Eles podem ser vistos como uma subclasse dos códigos BCH[1]. Assim, uma descrição similar em termos do conjunto de definição pode ser feita, veja Definição 2.16 e Corolário 2.1. Uma propriedade dos códigos Reed-Solomon que justifica sua aplicabilidade em diversos casos é que tais códigos têm máxima distância de separação (MDS, do inglês *maximal distance separable*); i.e., para comprimento e dimensão fixos, os códigos Reed-Solomon tem como valor para a distância mínima o máximo possível. Será mostrado na Seção 4 que é possível obter códigos quânticos MDS por meio da utilização de códigos Reed-Solomon.

Definição 2.16 *Seja* $b \geq 0$, $n = q - 1$ *e* $1 \leq k \leq n$. *Um código cíclico* $RS_k(n, b)$ *de comprimento* n *sobre* $\mathbb{F}_q$ *é um código Reed-Solomon com distância mínima* $n - k + 1$ *se*

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdot \cdots \cdot (x - \alpha^{b+n-k-1}),$$

em que α *é um elemento primitivo de* $\mathbb{F}_q$.

Uma aplicação da Proposição 2.5 para códigos Reed-Solomon é feita no Corolário 2.1, em que os parâmetros e conjunto de definição do dual euclidiano de um código Reed-Solomon é mostrado. Esse resultado também pode ser encontado na Proposição 5.1.2 da Ref. [69].

Corolário 2.1 *Seja* $RS_k(n, b)$ *um código Reed-Solomon. Então seu dual euclidiano pode ser descrito como sendo*

$$RS_k(n, b)^{\perp} = RS_{n-k}(n, n - b + 1)$$

Em particular, o conjunto de definição de $RS_k(n, b)^{\perp}$ *é dado por* $Z(RS_k(n, b)^{\perp}) = \{n - b + 1, n - b + 2, \ldots, n - b + k\}$.

Como será mostrado na Seção 4, um parâmetro importante de um código quântico assistido por emaranhamento pode ser calculado a partir da dimensão da interserção de dois códigos. Assim sendo, a última proposição desta subseção é designada a esse tópico.

Proposição 2.7 *[68, Exercício 239, Capítulo 4] Sejam* C_1 *e* C_2 *códigos cíclicos com conjunto de definição* $Z(C_1)$ *e* $Z(C_2)$, *respectivamente. Então o conjunto de definição de* $C_1 \cap C_2$ *é dado por* $Z(C_1) \cup Z(C_2)$. *Em particular,* $\dim(C_1 \cap C_2) = n - |Z(C_1) \cup Z(C_2)|$.

Observe que o resultado apresentado pode ser aplicado a qualquer tipo de código cíclico, donde, em particular, para os códigos BCH e Reed-Solomon.

[1]Também é possível fazer a caracterização inversa, i.e., mostrar que para qualquer código BCH existe um código Reed-Solomon que o contém.

Exemplo 2.7 *Suponha que se deseje construir um código Reed-Solomon sobre* $\mathbb{F}_8$*, o qual tem como elemento primitivo* α *que satisfaz* $\alpha^3 + \alpha + 1 = 0$*. Considere o polinômio gerador* $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = x^4+\alpha^3x^3+x^2+\alpha x+\alpha$*. Então tem-se que o código Reed-Solomon construído é um* $RS_3(7,1)$*, com distância mínima igual a* $d = n - k + 1 = 5$*. Além disso, seu conjunto de definição é* $Z(RS_3(7,1)) = \{1,2,3,4\}$.

2.1.4 – Limitantes sobre Códigos Clássicos

Dentre os diversos limitantes que existem na literatura, foram escolhidos dois deles para análise dos parâmetros dos códigos construídos nesta tese. O primeiro deles é o limitante de Singleton, o qual apresenta um cota superior para os parâmetros do código. Vale a pena salientar que este limitante não leva em consideração a cardinalidade do corpo sobre o qual o código é definido, fazendo com que tenha pouca utilidade para análise dos parâmetros de códigos algébrico-geométricos ou derivados dos mesmos.

Por fim, o limitante de Edgar Gilbert e Rom Varshamov (ou, por simplicidade, limitante de Gilbert-Varshamov) é mostrado. Cotas inferiores para os parâmetros dos códigos são obtidas deste limitante; ou seja, o limitante de Gilbert-Varshamov descreve parâmetros de códigos que existem. Esse limitante pode ser utilizado para caracterização e comparação de códigos em situações de comprimento finito ou análise assintótica. Os primeiros códigos a obter parâmetros superiores aos que o limitante de Gilbert-Varshamov garantia existir foram os códigos algébrico-geométricos [9].

Proposição 2.8 *[69, Teorema 2.2.1](Limitante de Singleton) Seja* $\mathcal{C}$ *um código linear com parâmetros* $[n,k,d]_q$*. Então tem-se que*

$$d \leq n - k + 1. \tag{2.23}$$

Esse limitante superior para a distância mínima é denominado limitante de Singleton. Posteriormente será apresentado generalizações desse limitante para os casos de códigos quânticos estabilizadores, assistidos ou não por emaranhamento, e códigos convolucionais clássicos e quânticos.

Definição 2.17 *Um código linear será chamado de MDS (do inglês* Maximum Distance Separable*) se valer a igualdade para o limitante de Singleton, ou seja,* $d = n - k + 1$.

O limitante de Gilbert-Varshamov é um dos limitantes mais importantes da Teoria da Codificação. Ele só foi superado em 1978 quando Tsfasman, Vladuts e Zink utilizaram a Teoria de Curvas Modulares na construção de códigos algébrico-geométricos [9]. Esse feito foi e é um dos motivos para o estudo de códigos algébrico-geométricos, tanto no paradigma clássico quanto no quântico.

Proposição 2.9 *[69, Teorema 2.3.15](Limitante Asintótico de Gilbert-Varshamov) Seja*

$$h_q(x) := x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x). \tag{2.24}$$

Sendo C um código com parâmetros $[n,k,d]_q$, com taxa $R(C) = k/n$, então, para qualquer q e $\delta \in [0, 1-1/q]$, existe uma família infinita de códigos C's sobre $\mathbb{F}_q$ com taxa

$$R_q^C(\delta) \geq 1 - h_q(\delta). \tag{2.25}$$

2.2 – Códigos Algébrico-Geométricos

Nesta seção são apresentados os objetos matemáticos sobre os quais os códigos algébrico-geométricos são definidos, o método de construção desses códigos e suas propriedades. A maioria das demonstrações deste capítulo serão omitidas para que o trabalho fique mais sucinto. Para o leitor que deseje se aprofundar mais no assunto, recomenda-se os livros de Henning Stichtenoth [71], de Tsfasman, Vladut e Nogin [70] e de Pretzel [72].

2.2.1 – Corpo de Funções Algébricas

Antes de tudo, assuma que K é um corpo arbitrário, que posteriormente será substituído pelo corpo finito $\mathbb{F}_q$, em que $q = p^m$ com p primo e $m \geq 1$ um número. A seguir, apresentamos algumas definições e resultados que serão úteis posteriormente.

Definição 2.18 *Um corpo de funções algébricas F/K de uma variável sobre K é uma extensão de corpos $F \supset K$ tal que F é uma extensão algébrica de $K(x)$, em que $x \in F \backslash K$ é um elemento transcendente sobre K.*

Existem diversos tipos de corpos de funções. Os mais utilizados na literatura são os corpos de funções racionais, elípticas, hiperelípticas e hermitianas. Para o leitor interessado no aprofundamento desse assunto, recomenda-se o Capítulo 6 da Ref. [71]. Em seguida continuaremos com a fundamentação dos objetos matemáticos utilizados em códigos algébrico-geométricos.

Definição 2.19 *Seja $\mathcal{O} \subset F$ um anel de F, então ele é chamado anel de valorização de F/K se satisfaz as as seguintes condições:*

1. *$K \subsetneq \mathcal{O} \subsetneq F$,*
2. *Para todo $z \in F$ tem-se $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$*

Proposição 2.10 *[71, Proposição 1.1.5] Seja $\mathcal{O}$ um anel de valorização do corpo de funções algébricas F/K. Então são válidas*

1. *$\mathcal{O}$ possui um único ideal maximal $P = \mathcal{O} \setminus \mathcal{O}^*$, em que*

$$\mathcal{O}^* := \{z \in \mathcal{O} \colon \exists w \in \mathcal{O} \text{ com } zw = 1\} \tag{2.26}$$

   é o grupo das unidades de $\mathcal{O}^*$;

2. *Seja $0 \neq x \in F$, então $x \in P \iff x^{-1} \notin \mathcal{O}$;*

3. *Tem-se que $\tilde{K} \subseteq \mathcal{O}$ e $\tilde{K} \cap P = \{0\}$, em que $\tilde{K}$ é o corpo das constantes de F/K.*

Teorema 2.1 *[71, Proposição 1.1.6] Sejam $\mathcal{O}$ um anel de valorização do corpo de funções algébricas F/K e P seu único ideal maximal. Então, tem-se que*

1. *P é um ideal principal;*

2. *se $P = t\mathcal{O}$, então cada $0 \neq z \in F$ tem uma única representação na forma $z = t^n u$, em que $n \in \mathbb{Z}$ e $u \in \mathcal{O}^*$. Nesse caso, diz-se que t é um elemento primo para P;*

3. *$\mathcal{O}$ é um domínio de ideais principais. Mais precisamente, se $P = t\mathcal{O}$ e $\{0\} \neq I \subset \mathcal{O}$ é um ideal, então $I = t^n\mathcal{O}$ para algum $n \in \mathbb{Z}$.*

Definição 2.20 *Um lugar geométrico, ou simplesmente lugar, P de um corpo de funções F/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ de F/K e $\mathbb{P}_{F/K}$ é o conjunto de todos os lugares de F/K.*

Como $\mathcal{O}$ é unicamente determinado por P, então se escreve $\mathcal{O}_P$ ao invés de $\mathcal{O}$.

Definição 2.21 *Uma valorização de F/K é uma função $v \colon F \to \mathbb{Z} \cup \infty$ tal que*

1. *$\exists\, z \in F$ tal que $v(z) = 1$;*

2. *$v(a) = 0$ para todo $a \in K \setminus \{0\}$;*

3. *$v(x) = \infty \iff x = 0$;*

4. *$v(xy) = v(x) + v(y)$ para todo $x, y \in F$;*

5. *$v(x + y) \geq \min\{v(x), v(y)\}$ para todo $x, y \in F$.*

Definição 2.22 *Seja $P \in \mathbb{P}_{F/K}$, então define-se $v_P \colon F \to \mathbb{Z} \cup \{\infty\}$ da seguinte forma: se t é um elemento primo para P e $z = t^n u$, com $u \in \mathcal{O}^*$ e $n \in \mathbb{Z}$, então $v_P(z) = n$ e $v_P(0) = \infty$.*

Definição 2.23 *Para um lugar $P \in \mathbb{P}_{F/K}$, define-se o corpo das classes laterais no lugar P por $F_P := \mathcal{O}_P/P$. O homomorfismo canônico de $\mathcal{O}_P$ em F_P é chamado de aplicação da classe lateral com relação a P. Por fim, tem-se que $\deg(P) := [F_P\colon K]$ é o grau de P.*

Observe que F_P é corpo, pois P é um ideal maximal, e, por isso, faz sentido falar de grau de P.

Definição 2.24 *Sejam $z \in F$, $m \in \mathbb{N}$ e $P \in \mathbb{P}_{F/K}$. Diz-se que P é um polo de ordem m de z se $v_P(z) = -m < 0$, e que P é um zero de ordem m de z se $v_P(z) = m > 0$.*

Proposição 2.11 *[71, Corolário 1.1.20] Se $z \in F$ é transcendental sobre K, então z tem pelo menos um polo e um zero.*

Definição 2.25 *Um divisor D do corpo de funções algébricas F/K é uma soma formal*

$$D = \sum_{P \in \mathbb{P}_{F/K}} n_P P, \tag{2.27}$$

em que $n_P \in \mathbb{Z}$ e é igual a zero para quase todo P.

O conjunto dos divisores de F/K, denotado por $Div(F)$, é um grupo abeliano livre. O suporte de um divisor D é definido como sendo $supp(D) := \{P \in \mathbb{P}_{F/K} | n_P \neq 0\}$. Um divisor da forma $D = P$, em que P é um lugar, é denominado divisor primo. Para qualquer lugar P' de F/K e $D = \sum n_P P$ um divisor, define-se $v_{P'}(D) = n_{P'}$.

É possível definir um ordenamento parcial em $Div(F)$ da seguinte forma:

$$D_1 \leq D_2 \iff v_P(D_1) \leq v_P(D_2), \text{ para todo } P \in \mathbb{P}_{F/K}. \tag{2.28}$$

Um divisor satisfazendo $D \geq 0$ é denotado por divisor efetivo.

Por fim, o grau de um divisor D é dado por

$$\deg(D) := \sum_{P \in \mathbb{P}_{F/K}} v_p(D) \deg(P). \tag{2.29}$$

Definição 2.26 *Para um elemento não-nulo $x \in F$, denote por Z o conjunto dos zeros de x e por N o conjunto dos polos. Com isso, define-se*

$$(x)_0 := \sum_{P \in Z} v_P P, \tag{2.30}$$

o divisor de zeros de x,

$$(x)_\infty := \sum_{P \in N} v_P P, \tag{2.31}$$

o divisor de polos de x e, por fim,

$$(x) := (x)_0 - (x)_\infty = \sum_{P \in \mathbb{P}_{F/K}} v_P P, \tag{2.32}$$

o divisor de x.

Um divisor é dito principal se é o divisor de algum elemento $x \in F$.

Dois divisores D, D' *pertencentes a* $Div(F)$ *são ditos equivalentes, denotado por* $D \sim D'$ *ou* $D \equiv D'$, *se* $D = D' + (x)$, *para algum* $x \in F \setminus \{0\}$.

Definição 2.27 *Seja* $A \in Div(F)$, *então define-se o espaço de Riemann-Roch sobre* K *associado ao divisor* A *por*

$$\mathcal{L}(A) := \{x \in F \colon (x) \geq -A\} \cup \{0\}. \tag{2.33}$$

Adota-se por $l(A)$ *como sendo a dimensão de* $\mathcal{L}(A)$.

Proposição 2.12 *[71, Observação 1.4.5, Lema 1.4.6 e Lema 1.4.7] Seja* $A \in Div(F)$, *então*

1. $\mathcal{L}(A) \neq \{0\} \iff \exists A' \in Div(F)$ *que é equivalente a* A *e* $A' \geq 0$;
2. *Se* A' *é equivalente a* A, *então* $\mathcal{L}(A)$ *é isomorfo, como espaço vetorial, a* $\mathcal{L}(A')$;
3. $\mathcal{L}(0) = K$;
4. *Se* $A < 0$, *então* $\mathcal{L}(A) = \{0\}$.

As seguintes definições serão ferramentas importantes para o cálculo da dimensão do espaço de Riemann-Roch e dos códigos algébrico-geométricos associados a ele.

Definição 2.28 *Um adele de* F/K *é uma aplicação descrita por*

$$\alpha : \begin{cases} \mathbb{P}_{F/K} & \to F, \\ P & \mapsto \alpha_P \end{cases} \tag{2.34}$$

tal que $\alpha_P \in \mathcal{O}_P$ *para quase todo* $P \in \mathbb{P}_{F/K}$.

Definimos ainda $\mathcal{A}_F := \{\alpha \colon \alpha$ *é um adele de* $F/K\}$ *e*

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \colon v_P(\alpha) \geq v_P(A), \text{ para todo } P \in \mathbb{P}_{F/K}\}, \tag{2.35}$$

em que $v_P(\alpha) = v_P(\alpha_P)$.

Definição 2.29 *Um diferencial de Weil de* F/K *é uma aplicação* $\omega \colon \mathcal{A}_F \to K$ *que se anula em* $\mathcal{A}_F(A) + F$ *para algum* $A \in Div(F)$. *De forma similar aos adeles, define-se* $\Omega_F := \{\omega \colon \omega$ *é um diferencial de Weil de* $F/K\}$ *e*

$$\Omega_F(A) := \{\omega \in \Omega_F \colon \omega \text{ se anula em } \mathcal{A}_F(A) + F\}. \tag{2.36}$$

Definição 2.30 *Um divisor (ω) de um diferencial de Weil é o único divisor de F/K que possui as seguintes propriedades*

1. *ω se anula em $\mathcal{A}_F((\omega)) + F$;*
2. *se ω se anula em $\mathcal{A}_F(A) + F$, então $A \leq (\omega)$.*

Definição 2.31 *Um divisor W é dito canônico se existe algum diferencial $\omega \in \Omega_F$ tal que $W = (w)$.*

Com essa última definição é possível apresentar o que é o gênero de um corpo de funções algébricas e a dimensão do espaço de Riemann-Roch associado a um divisor.

Definição 2.32 *O gênero g do corpo de funções algébricas F/K é definido como sendo*

$$g := \max\{\deg(A) - l(A) + 1 \colon A \in Div(F)\}. \tag{2.37}$$

Note que o gênero está bem definido pois, como é mostrado na Proposição 1.4.14 [71], existe uma constante $\gamma \in \mathbb{Z}$ tal que, para todo $A \in Div(F)$, tem-se $\deg(A) - l(A) \leq \gamma$.

O teorema a seguir oferece um método para calcular a dimensão do espaço de Riemann-Roch associado a um divisor. Tal teorema será extensivamente utilizado no cálculo dos parâmetros dos códigos algébrico-geométricos apresentados posteriormente.

Teorema 2.2 *[71, Teorema 1.5.15] Para qualquer divisor $A \in Div(F)$ tem-se*

$$l(A) = \deg(A) + 1 - g + l(W - A), \tag{2.38}$$

em que W é um divisor canônico de F/K.

Corolário 2.2 *Se $A \in Div(F)$ satisfaz $\deg(A) \geq 2g - 1$, então*

$$l(A) = \deg(A) + 1 - g. \tag{2.39}$$

Semigrupo de Weierstrass

O semigrupo de Weierstrass é apresentado a seguir. Tal conceito está ligado com a dimensão do espaço de Riemann-Roch e, por conseguinte, com a dimensão de códigos algébrico-geométricos.

Definição 2.33 *Seja $n \geq 0$ um número inteiro. Então n é denominado não-lacuna em $Q \in \mathbb{P}_{F/K}$ se existe um elemento $x \in F$ tal que $(x)_\infty = nQ$. Caso contrário, n é chamado de lacuna em Q.*

Note que n será não-lacuna se, e somente se, $l(nQ) > l((n-1)Q)$. Além disso, tem-se que n é não-lacuna para todo $n \geq 2g$, sendo g o gênero do corpo de funções algébricas F/K. Para ver isso, note que como $l((n-1)Q) = (n-1)\deg Q + 1 - g$ e $l(nQ) = n \deg Q + 1 - g$, então $\mathcal{L}((n-1)Q) \subsetneq \mathcal{L}(nQ)$.

Teorema 2.3 *[71, Teorema 1.6.8] Seja F/K um corpo de funções algébricas com gênero g e $Q \in \mathbb{P}_{F/K}$ um lugar de grau um. Então existem g lacunas $i_1 < \cdots < i_g$ em Q tais que $i_1 = 1$ e $i_g \leq 2g - 1$.*

Por fim, é definido o semigrupo de Weierstrass de um lugar racional.

Definição 2.34 *Seja Q um lugar racional do corpo de funções algébricas F/K. Denota-se por $H(Q) = \{0 = \rho_0 < \rho_1 < \cdots < \infty\} \subset \mathbb{N}$ o conjunto de não-lacunas em Q. Como $H(Q)$ é um semigrupo de $\mathbb{N}$ com relação a adição, então $H(Q)$ é chamado de semigrupo de Weierstrass de Q.*

2.2.2 – Códigos Algébrico-Geométricos

Como foi mencionado anteriormente, um dos primeiros atrativos dos códigos algébrico-geométricos surgiu quando Tsfasman, Vladuts e Zink mostraram que podia utilizá-los para obter códigos com parâmetros que superavam o limitante de Gilbert e Varshamov [9]. O método de construção desses códigos é sedimentado nos aspectos expostos anteriormente, por isso, são revistas algumas definições.

Seja $F/\mathbb{F}_q$ um corpo de funções algébricas com gênero g. Assuma que $P_1, \ldots, P_n$ são lugares de grau 1, distintos dois a dois, de $F/\mathbb{F}_q$, $D = P_1 + \cdots + P_n$ e G um divisor tal que $\sup(G) \cap \sup(D) = \emptyset$. Com isso, é possível definir códigos algébrico-geométricos.

Definição 2.35 *O código algébrico-geométrico (AG) associado com os divisores D e G, denotado por $\mathcal{C}_{\mathcal{L}}(D, G)$, é dado como sendo a imagem da seguinte aplicação*

$$\alpha \colon f \in \mathcal{L}(G) \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n. \tag{2.40}$$

Inicialmente, note que dizer que os lugares $P_1, \ldots, P_n$ são de grau 1 significa que $[F_{P_i} : \mathbb{F}_q] = 1$, para $i = 1, \ldots, n$. Além disso, como $\sup(G) \cap \sup(D) = \emptyset$, então tem-se que $v_{P_i}(f) \geq 0$, para qualquer $f \in \mathcal{L}(G)$ e $i \in \{1, \ldots, n\}$. Dessas duas informações chega-se à conclusão de que $f(P_i) \in \mathbb{F}_q$, para $i = 1, \ldots, n$, e, assim, a aplicação α está bem definida.

A seguir são apresentados um teorema e um corolário que relacionam os parâmetros de um código AG e espaços de Riemann-Roch relacionados aos operadores que definem o código.

Teorema 2.4 *[71, Teorema 2.2.2] Seja $\mathcal{C}_{\mathcal{L}}(D,G)$ um código AG com parâmetros $[n,k,d]_q$, então*

$$k = \dim \mathcal{L}(G) - \dim \mathcal{L}(G-D) \tag{2.41}$$

e

$$d \geq n - \deg(G). \tag{2.42}$$

Corolário 2.3 *Se $\deg(G) < n$, então*

1. *A aplicação α é injetiva e os parâmetros do código $\mathcal{C}_{\mathcal{L}}(D,G)$ são dados por*

$$k = \dim \mathcal{L}(G) = \deg(G) + 1 - g \tag{2.43}$$

e

$$d \geq n - \deg(G). \tag{2.44}$$

Portanto, $k + d \geq n + 1 - g$;

2. *Se, além disso, $2g - 2 < \deg(G)$, então $k = \deg(G) + 1 - g$;*

3. *Se $\{f_1, \ldots, f_k\}$ é uma base de $\mathcal{L}(G)$, então a matriz geradora do código $\mathcal{C}_{\mathcal{L}}(D,G)$ é dada por*

$$M = \begin{pmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{pmatrix}. \tag{2.45}$$

Relacionado à dimensão do código $\mathcal{C}_{\mathcal{L}}(D,G)$ é possível construir uma quantidade que está relacionada com o semigrupo de Weierstrass de $H(G)$. Essa quantidade será denotada por H^* e pode ser utilizada para o cálculo de um limitante melhor que o limitante de Goppa para a distância mínima de $\mathcal{C}_{\mathcal{L}}(D,G)$; veja a Definição 2.36 dada a seguir.

Definição 2.36 *Seja $\mathcal{C}_{\mathcal{L}}(D,G)$ o código AG da Definição 2.35 com $G = mQ$. Então considere o seguinte conjunto:*

$$H^* = H^*(D,G) := \{m \in \mathbb{N}_0 \colon \mathcal{C}_{\mathcal{L}}(D,mQ) \neq \mathcal{C}_{\mathcal{L}}(D,(m-1)Q)\}. \tag{2.46}$$

Conhecer H^* é equivalente a saber a dimensão de $\mathcal{C}_{\mathcal{L}}(D,mQ)$ para todo $m \in \mathbb{N}_0$. Além disso, é possível notar que H^* consiste de n elementos, $H^* \subset H(Q)$ e que, para $m < n$, tem-se que $m \in H^*$ se, e somente se, $m \in H(Q)$. Escreve-se $H^* = \{m_1, \ldots, m_n\}$.

Além do código $\mathcal{C}_{\mathcal{L}}(D,G)$, é possível construir outro código algébrico-geométrico, que é o código dual euclidiano do código $\mathcal{C}_{\mathcal{L}}(D,G)$. Sua definição, tanto quanto a caracterização dos seus parâmetros, é feita no teorema a seguir.

Teorema 2.5 *[71, Teorema 2.2.7] Seja $\mathcal{C}_{\mathcal{L}}(D,G)$ código AG anteriormente descrito. Seja η um diferencial de Weil tal que $\nu_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$, para todo $i = 1,\ldots,n$. Então, $\mathcal{C}_{\Omega}(D,G) := \mathcal{C}_{\mathcal{L}}(D,G)^{\perp} = \mathcal{C}_{\mathcal{L}}(D,G^{\perp})$, com $G^{\perp} = D - G + (\eta)$. Os parâmetros do código $\mathcal{C}_{\Omega}(D,G)$ são os seguintes*

$$k' = i(G-D) - i(G) \tag{2.47}$$

e

$$d' \geq \deg(G) - 2g + 2. \tag{2.48}$$

Além disso, se $\deg(G) > 2g-2$, então $k' = i(G-D) \geq n + g - 1 - \deg(G)$. Se, além disso, $\deg(G) < n$, então tem-se a igualdade no valor de k'.

Exemplo 2.8 *Seja $F/\mathbb{F}_{q^2}$, em que q é uma potência de primo, o corpo de funções hermitianas definido pela equação*

$$y^q + y = x^{q+1}. \tag{2.49}$$

É possível mostrar que este corpo de funções tem q^3+1 lugares racionais (de grau 1), em que um deles é o lugar no infinito Q, e gênero $g = q(q-1)/2$. Sejam $P_1,\ldots,P_n$ lugares racionais dois a dois distintos e diferentes do lugar no infinito. Adote $D = P_1 + \cdots + P_n$ e $G = mQ$. Para $q = 2$ e $m = 3$, tem-se que uma base para o espaço de Riemann-Roch $\mathcal{L}(G)$ é o conjunto $B = \{1, x, y\}$ [71]. Os lugares geométricos $P_1,\ldots,P_8$ são os seguintes:

$$\left[\begin{array}{c|cccccccc} & P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 \\ \hline x & 0 & 0 & 1 & \alpha & \alpha+1 & 1 & \alpha & \alpha+1 \\ y & \alpha & \alpha+1 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right] \tag{2.50}$$

com $\alpha^2 = \alpha + 1$. Aplicando as funções da base B nos lugares $P_1,\ldots,P_8$, contrói-se a seguinte matriz geradora

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \alpha+1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & \alpha & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \tag{2.51}$$

Este código é um código $[8,3,5]_4$.

2.2.3 – Códigos Algébrico-Geométricos Asintoticamente Bons

Uma torre de corpos de função (veja [73, Definição 1.3]) sobre $\mathbb{F}_q$ é uma sequência $\mathcal{T} = (F_1, F_2, \ldots)$ de corpos de função $F_i/\mathbb{F}_q$ com as seguintes propriedades:

(1) $F_1 \subseteq F_2 \subseteq F_3 \cdots$.

(2) Para cada $n \geq 1$, a extensão F_{n+1}/F_n é separável de grau $[F_{n+1} : F_n] > 1$.

(3) $g(F_j) > 1$, para algum $j > 1$.

Pela fórmula para o gênero de Hurwitz, a condição (3) implica que $g(F_n) \to \infty$ para $n \to \infty$. A torre é dita ser assintoticamente boa se $\lambda(\mathcal{T}) = \limsup_{i\to\infty}, N(F_i)/g(F_i) > 0$, com $N(F_i)$ e $g(F_i)$ denotando o número de pontos racionais em $\mathbb{F}_q$ e o gênero de F_i, respectivamente. Para o caso de torre de corpos de função, pode-se trocar $\limsup_{i\to\infty} N(F_i)/g(F_i)$ por $\lim_{i\to\infty} N(F_i)/g(F_i)$, pois a sequência $(N(F_i)/g(F_i))_{i\geq 1}$ é convergente. Diz-se que uma torre $\mathcal{T}$ (sobre $\mathbb{F}_q$) atinge o limitante de Drinfeld-Vladut se $\lambda(\mathcal{T}) = \limsup_{i\to\infty} N(F_i)/g(F_i) = \sqrt{q} - 1$. Por simplicidade, a notação que será usada é $N(F_i) = N_i$ e $g(F_i) = g_i$.

2.3 – Construção de Novos Códigos Algébrico-Geométricos a Partir de Antigos

São mostrados nesta seção métodos de construção de códigos algébrico-geométricos a partir de códigos algébrico-geométricos já existentes. Esses métodos se estendem desde a existência de uma matriz geradora na forma simplética à interseção e união de códigos algébrico-geométricos.

O Teorema 2.6, dado a seguir, utiliza o semigrupo de Weierstrass de Q e considera $G = mQ$, com $m \in \mathbb{N}_0$, para a construção de uma matriz na forma sistemática dependendo apenas do $\deg(G)$. Esse resultado pertence a Ref. [62], tendo o autor desta tese como um dos autores do artigo. Antes desta publicação, não era óbvio se a construção de uma matriz geradora na forma sistemática para códigos algébrico-geométricos era possível sem a consideração de curvas específicas.

Teorema 2.6 *Seja G um divisor de um corpo de funções $F/\mathbb{F}_q$ com $\deg(G) \in H(Q)$ suficientemente grande, então existe um código AG $C_{\mathcal{L}}(D, G)$ com matriz geradora na forma sistemática.*

Demonstração: Seja $J = \{j_1, \ldots, j_k\}$, com $j_1, \ldots, j_k \in \{1, \ldots, n\}$ dois a dois distintos e $k = \ell(G)$, e $\overline{J_i} = J \setminus \{j_i\}$. Assuma que $X_{j_i} := \{a_1 + a_2 + \cdots + a_{j_i-1} + a_{j_i+1} + \cdots + a_n | a_l \in \mathbb{N}$ para $l \in \overline{J_i}$ ou $a_l \in \mathbb{N}_0$ caso contrário$\}$, para $j_i \in J$. Será mostrado que, para $\deg(G) \in X_{j_1} \cap \cdots \cap X_{j_k} \cap S(Q)$, existe um código AG com matriz geradora na forma sistemática. Para isso, considere $x_i = a_1P_1 + \cdots + a_{j_i-1}P_{j_i-1} + a_{j_i+1}P_{j_i+1} + \cdots + a_nP_n - \deg(G)Q$, com $i = 1, \ldots, k$. Uma vez que $\{x_i\}$ são dois a dois distintos em termos de suas valorizações, então eles formam uma base de $\mathcal{L}(G)$. A matriz geradora consistindo desses elementos da base tem k colunas, em que cada uma delas tem apenas um elemento não nulo. Além disso, em tais colunas, a posição desses elementos é diferente, i.e., os elementos estão em linhas distintas. Dividindo cada linha por tal elemento, obtêm-se uma matriz geradora na forma sistemática. ■

A descrição feita para espaços de Riemann-Roch mostra que os elementos advindos destes espaços são funções que obedecem certas regras descritas pelo divisor que define o espaço. Uma questão natural a ser levantada é se existe um método para descrever a interseção de dois espaços de Riemann-Roch por meio dos divisores que definem tais espaços. Este resultado foi mostrado por Munuera e Pellikaan [74]. Antes de apresentá-lo, é necessário definir a interseção e união de dois divisores, o que é feito logo a seguir.

Definição 2.37 *Sejam G e H divisores sobre $F/\mathbb{F}_q$. Se $G = \sum_{P\in\mathbb{P}_F} \nu_P(G)P$ e $H = \sum_{P\in\mathbb{P}_F} \nu_P(H)P$, em que $P \in \mathbb{P}_F$ é um lugar, então a interseção $G \cap H$ de G e H sobre $F/\mathbb{F}_q$ é definido como sendo*

$$G \cap H = \sum_{P\in\mathbb{P}_F} \min\{\nu_P(G), \nu_P(H)\}P. \tag{2.52}$$

De forma similar, definimos a união por

$$G \cup H = \sum_{P\in\mathbb{P}_F} \max\{\nu_P(G), \nu_P(H)\}P. \tag{2.53}$$

Proposição 2.13 *[74, Lema 2.6] Sejam G e H dois divisores sobre $F/\mathbb{F}_q$. Então $\mathcal{L}(G) \cap \mathcal{L}(H) = \mathcal{L}(G \cap H)$.*

No Capítulo 4 é mostrado que para a utilização de códigos lineares na construção de códigos quânticos assistidos por emaranhamento faz-se necessário o cálculo da dimensão da interseção de dois códigos. Para o caso da utilização de códigos AG, é possível associar essa quantidade com a dimensão da interseção dos espaços de Riemann-Roch que definem os códigos AG, uma vez que os divisores atendam certas restrições, veja Proposição 2.14. Outro resultado também é derivado. Mostramos que a união de códigos AG também fornece um código AG, veja Proposição 2.15. Este resultado não é óbvio, pois somas usuais de espaços vetoriais nem sempre fornece um espaço vetorial. Esses resultados pertencem a Ref. [64], tendo o autor desta tese como um dos autores do artigo.

Proposição 2.14 *Sejam $F/\mathbb{F}_q$ um corpo de funções de gênero g e D um divisor como na Definição 2.35. Se G_1 e G_2 são dois divisores tais que $\mathrm{supp}(G_1) \cap \mathrm{supp}(D) = \varnothing$, resp. $\mathrm{supp}(G_2) \cap \mathrm{supp}(D) = \varnothing$, e $\deg(G_1 \cup G_2) < n$, então $C_{\mathcal{L}}(D, G_1) \cap C_{\mathcal{L}}(D, G_2) = C_{\mathcal{L}}(D, G_1 \cap G_2)$.*

Demonstração: Primeiramente, suponha que $\mathbf{c} \in C_{\mathcal{L}}(D, G_1) \cap C_{\mathcal{L}}(D, G_2)$. Então existe $g_1 \in \mathcal{L}(G_1)$ e $g_2 \in \mathcal{L}(G_2)$ tais que $\mathbf{c} = ev_D(g_1) = ev_D(g_2)$, o que implica que $ev_D(g_1 - g_2) = 0$. Uma vez que $g_1 - g_2 \in \mathcal{L}(G_1 \cup G_2)$ e $\deg(G_1 \cup G_2) < n$, então $g_1 = g_2 \in \mathcal{L}(G_1 \cap G_2)$ pela Proposição 2.13. Consequentemente, $\mathbf{c} \in C_{\mathcal{L}}(D, G_1 \cap G_2)$. A outra inclusão segue diretamente da Proposição 2.13. ■

Proposição 2.15 *Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g e D um divisor como na Definição 2.35. Se G_1 e G_2 são dois divisores tais que* $\mathrm{supp}(G_1) \cap \mathrm{supp}(D) = \varnothing$ *e* $\mathrm{supp}(G_2) \cap \mathrm{supp}(D) = \varnothing$*, respectivamente,* $\deg(G_1 \cap G_2) > 2g - 2$ *e* $\deg(G_1 \cup G_2) < n$*, então* $C_{\mathcal{L}}(D, G_1) + C_{\mathcal{L}}(D, G_2) = C_{\mathcal{L}}(D, G_1 \cup G_2)$.

Demonstração: Considere inicialmente a inclusão $C_{\mathcal{L}}(D, G_1)+C_{\mathcal{L}}(D, G_2) \subseteq C_{\mathcal{L}}(D, G_1 \cup G_2)$. Uma vez que $G_i \leq G_1 \cup G_2$, para $i = 1, 2$, então $C_{\mathcal{L}}(D, G_i) \subseteq C_{\mathcal{L}}(D, G_1 \cup G_2)$, para $i = 1, 2$. Assim, $C_{\mathcal{L}}(D, G_1) + C_{\mathcal{L}}(D, G_1) \subseteq C_{\mathcal{L}}(D, G_1 \cup G_2)$. Por outro lado, é possível notar que $\ell(G_1) + \ell(G_2) = \ell(G_1 \cap G_2) + \ell(G_1 \cup G_2)$, uma vez que $\deg(G_1 \cap G_2) > 2g - 2$. Isto implica em $\mathcal{L}(G_1 \cup G_2) = \mathcal{L}(G_1) + \mathcal{L}(G_2)$ pela Proposição 2.13. Por fim, a demonstração da inclusão remanescente segue da hipótese que $\deg(G_1 \cup G_2) < n$ e da Proposição 2.14. ■

CAPÍTULO 3

Códigos Quânticos Estabilizadores

São apresentados neste capítulo os códigos quânticos e, em particular, códigos quânticos estabilizadores. Uma modelagem dos tipos de erros que esses códigos podem corrigir é apresentada, tanto quanto uma explanação sobre o que caracteriza os erros corrigíveis ou não. A partir dessa caracterização, são construídos os códigos quânticos estabilizadores e é mostrado que tais códigos têm a capacidade de correção requerida. Alguns limitantes, similares aos limitantes para códigos clássicos anteriormente expostos, são mostrados. Esses limitantes serão utilizados neste e em capítulos posteriores para quantificar a qualidade dos códigos e fornecer um método de comparação com os existentes na literatura. Por fim, três tipos distintos de novos códigos estabilizadores são construídos e uma análise comparativa dos mesmos com os códigos quânticos presentes na literatura é feita. Esses resultados estão presentes nas Seções 3.4 e 3.5 e podem ser encontrados na Ref. [63]. Para o leitor que desejar se aprofundar em códigos quânticos, recomendamos as Refs. [19, 40, 75, 76].

3.1 – Códigos Quânticos Estabilizadores

No que segue, consideramos que a informação é quantizada em dígitos quânticos q-ários, também denominados de *qudits* (do inglês, *quantum digits*). Para o caso em que $q = 2$, chamamos os dígitos quânticos de qubits. O estado quântico com um único qudit é um vetor não-nulo e unitário $|\psi\rangle$ pertencente ao espaço de Hilbert $\mathcal{H}_q$[1] [19]. Esse espaço vetorial possui uma base ortonormal com elementos denotados por $|x\rangle$, em que x é um elemento do corpo finito $\mathbb{F}_q$. Em um sistema com n qudits, o estado quântico é um vetor em $\mathcal{H}_q^n = \mathcal{H}_q \otimes \cdots \otimes \mathcal{H}_q$. De forma similar ao caso clássico, um código quântico é um subespaço vetorial de $\mathcal{H}_q^n$. Quando um código quântico codifica k qudits lógicos de informação em n qudits físicos ele será denotado por $[[n, k, d]]_q$, em que d é a distância mínima entre as palavras do código quântico. Note o

[1] Quando não há a necessidade de ser feito uma análise mais funcional dos entes matemáticos utilizados, é possível adotar que o código quântico é definido sobre o corpo dos complexos $\mathbb{C}^q$. Essa hipótese é comumente encontrada na literatura de códigos quânticos e será assumida aqui. Por esse motivo, o produto interno de estados quânticos é assumido como sendo o usual sobre $\mathbb{C}^q$.

uso de duplos colchetes para diferenciação entre códigos lineares clássicos. Uma outra forma mais geral de denotar códigos quânticos é $((n, K, d))_q$, em que essa notação enfatiza que o código quântico é um subespaço com cardinalidade K e possui a capacidade de corrigir até $t = \lfloor (d-1)/2 \rfloor$ erros. Essa última informação sobre t também se mantém para a notação dada anteriormente.

Exemplo 3.1 *Seja $\mathcal{H}_3^4$ um espaço de Hilbert. Um possível vetor pertencente a este espaço é $|\psi\rangle = \frac{1}{\sqrt{4}}\{|1000\rangle + |0200\rangle + |0010\rangle + |0002\rangle\}$. O fator $\frac{1}{\sqrt{4}}$ existe por motivo de normalização do vetor $|\psi\rangle$; ou seja, ele é incluído de forma que $\sqrt{\langle\psi|\psi\rangle} = 1$. Uma possível base para $\mathcal{H}_3^4$ é o conjunto*

$$
\begin{aligned}
\{ \quad & |0000\rangle, |1000\rangle, |2000\rangle, |0100\rangle, |1100\rangle, |2100\rangle, |0200\rangle, |1200\rangle, |2200\rangle, \\
& |0010\rangle, |1010\rangle, |2010\rangle, |0110\rangle, |0210\rangle, |1110\rangle, |1210\rangle, |2110\rangle, |2210\rangle, \\
& |0020\rangle, |1020\rangle, |2020\rangle, |0120\rangle, |0220\rangle, |1120\rangle, |1220\rangle, |2120\rangle, |2220\rangle, \\
& |0001\rangle, |1001\rangle, |2001\rangle, |0101\rangle, |0201\rangle, |1101\rangle, |1201\rangle, |2101\rangle, |2201\rangle, \\
& |0011\rangle, |1011\rangle, |2011\rangle, |0111\rangle, |0211\rangle, |1111\rangle, |1211\rangle, |2111\rangle, |2211\rangle, \\
& |0021\rangle, |1021\rangle, |2021\rangle, |0121\rangle, |0221\rangle, |1121\rangle, |1221\rangle, |2121\rangle, |2221\rangle, \\
& |0002\rangle, |1002\rangle, |2002\rangle, |0102\rangle, |0202\rangle, |1102\rangle, |1202\rangle, |2102\rangle, |2202\rangle, \\
& |0012\rangle, |1012\rangle, |2012\rangle, |0112\rangle, |0212\rangle, |1112\rangle, |1212\rangle, |2112\rangle, |2212\rangle, \\
& |0022\rangle, |1022\rangle, |2022\rangle, |0122\rangle, |0222\rangle, |1122\rangle, |1222\rangle, |2122\rangle, |2222\rangle, \quad \}.
\end{aligned}
$$

Da complexidade relacionada à base desse espaço de Hilbert, nota-se que descrever códigos quânticos via uma base para seu espaço vetorial é inviável.

Um exemplo prático do que é mostrado no exemplo anterior pode ser feito para o código quântico $[[7, 1, 3]]_2$ de Steane [18]. Uma descrição em termos de elementos da base é a seguinte:

$$
\begin{aligned}
|0_L\rangle &= \frac{1}{\sqrt{8}}\Big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\Big), \\
|1_L\rangle &= \frac{1}{\sqrt{8}}\Big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\Big). \qquad (3.1)
\end{aligned}
$$

Aqui foi utilizado o subíndice L para indicar que os vetores $|0_L\rangle$ e $|1_L\rangle$ representam os bits lógicos zero e um, respectivamente. Outra maneira de descrever códigos quânticos, que é utilizada neste trabalho, é por meio de operadores unitários que atuam sobre o espaço de Hilbert $\mathcal{H}_q^n$. Operadores são transformações lineares que levam vetores de $\mathcal{H}_q^n$ a vetores de $\mathcal{H}_{q'}^m$, em

que q e q' (tanto quanto n e m) não precisam ser idênticos. Entretanto, neste trabalho são considerados apenas operadores que atuam de $\mathcal{H}_q^n$ para $\mathcal{H}_q^n$.

Seja E um operador que representa um erro advindo de um canal quântico. Considere que os erros em cada qudit sejam independentes, então o operador de erro E pode ser decomposto em $E = E_1 \otimes \cdots \otimes E_n \in \mathcal{H}_q^n$. Além disso, a linearidade da mecânica quântica permite que apenas um conjunto discreto de erros precisem ser levados em consideração (para essa demonstração veja o livro do Nielsen e Chuang [19]). O código quântico que será considerado neste trabalho pode ser descrito como a interseção de autoespaços de um subgrupo abeliano de operadores de erro. Este subgrupo de operadores de erro é chamado de estabilizador do código, pois seus elementos não alteram os estados pertencentes ao código, e o código é chamado de código estabilizador. Nas próximas subseções serão descritos o grupo de erros e os códigos estabilizadores em detalhes.

3.1.1 – Base de Erro

Seja $\mathcal{P}$ o conjunto das matrizes de Pauli para qubits dado por $\mathcal{P} = \{I, X, Z, Y\}$ [19]. É possível generalizar o conceito de matrizes de Pauli para qudits. Desse forma, pode-se escrever qualquer erro como a combinação linear do erro de amplitude, X, e do erro de fase, Z. Considere agora a e b elementos de $\mathbb{F}_q$ e q uma potência do número primo p. Define-se a ação dos operadores unitários $X(a)$ e $Z(b)$ sobre $\mathcal{H}_q$, que generalizam os operadores de Pauli X e Z para o caso q-ário, como

$$X(a)|x\rangle := |x + a\rangle, \tag{3.2}$$
$$Z(b)|x\rangle := \beta^{tr(bx)}|x\rangle, \tag{3.3}$$

em que a soma é operada no corpo $\mathbb{F}_q$, $tr(\cdot)$ denota a operação de traço de $\mathbb{F}_q$ para $\mathbb{F}_p$ e $\beta := \exp(2\pi i/p)$ é uma p-ésima raiz primitiva da unidade.

Exemplo 3.2 *Seja $|\psi\rangle = |1\rangle$ um vetor de $\mathcal{H}_3$. Os resultados das operações $X(2)$ e $Z(1)$ sobre o vetor $|\psi\rangle$ são*

$$\begin{aligned} X(2)|\psi\rangle &= |1 + 2 \mod 3\rangle = |0\rangle \\ Z(1)|\psi\rangle &= \beta^{tr(1)}|1\rangle = \beta|1\rangle = e^{2\pi i/3}|1\rangle. \end{aligned}$$

Seja $\mathcal{E} := \{X(a)Z(b)|a, b \in \mathbb{F}_q\}$ o conjunto dos operadores de erro. Os operadores de erro em $\mathcal{E}$ formam uma base do conjunto das matrizes $q \times q$ com entrada complexa, uma vez que o traço $Tr(A^\dagger B) = 0$ para quaisquer elementos A e B distintos de $\mathcal{E}$. Além disso, observe que

$$X(a)Z(b)X(a')Z(b') = \beta^{tr(ba')}X(a + a')Z(b + b'). \tag{3.4}$$

A base de erro para um sistema quântico q-ário de dimensão n pode ser obtida pela aplicação do produto tensorial da base de erro de cada um dos sistemas individuais. Sejam $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$. Defina $X(\mathbf{a}) := X(a_1) \otimes \cdots \otimes X(a_n)$ e $Z(\mathbf{b}) := Z(b_1) \otimes \cdots \otimes Z(b_n)$. Então, tem-se o seguinte resultado, cuja demonstração segue das definições de $X(\mathbf{a})$ e $Z(\mathbf{b})$.

Lema 3.1 *[76, Lema 1] O conjunto definido por $\mathcal{E}_n := \{X(\mathbf{a})Z(\mathbf{b})\colon \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ é uma base de erro sobre o espaço vetorial complexo $\mathcal{H}_q^n$.*

Exemplo 3.3 *Seja $|\psi\rangle$ o vetor de $\mathcal{H}_3^4$ do Exemplo 3.1. Assuma que $\mathbf{a} = (1, 0, 0, 2)$ e $\mathbf{b} = (2, 0, 1, 0)$ são vetores de $\mathbb{F}_3$. Com isso, a ação de $X(\mathbf{a})$ e $Z(\mathbf{b})$ sobre o vetor $|\psi\rangle$ é dada por*

$$
\begin{aligned}
X(\mathbf{a})|\psi\rangle &= \frac{1}{\sqrt{4}} X(\mathbf{a})\{|1000\rangle + |0200\rangle + |0010\rangle + |0002\rangle\} && (3.5)\\
&= \frac{1}{\sqrt{4}}\{|2002\rangle + |1202\rangle + |1012\rangle + |1001\rangle\} && (3.6)\\
Z(\mathbf{b})|\psi\rangle &= \frac{1}{\sqrt{4}} Z(\mathbf{b})\{|1000\rangle + |0200\rangle + |0010\rangle + |0002\rangle\} && (3.7)\\
&= \frac{1}{\sqrt{4}}\{e^{4\pi i/3}|1000\rangle + |0200\rangle + e^{2\pi i/3}|0010\rangle + |0002\rangle\}. && (3.8)
\end{aligned}
$$

3.1.2 – Códigos Estabilizadores

A descrição do código quântico que será feita logo a seguir é baseada no conjunto de base de erro que foi apresentado. Considere o grupo de erros G_n definido como

$$G_n = \{\beta^c X(\mathbf{a})Z(\mathbf{b})\colon \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}. \tag{3.9}$$

Ou seja, G_n é um grupo finito gerado pelas matrizes na base de erro $\mathcal{E}_n$. Note também que G_n não é um grupo abeliano.

Seja $\mathcal{S}$ o maior subgrupo abeliano do grupo de erro G_n que fixa todo elemento no código quântico $\mathcal{Q}$. Ou seja, considere $S \in \mathcal{S}$, então tem-se que $S|\psi\rangle = (+1)|\psi\rangle$ para todo $|\psi\rangle \in \mathcal{Q}$. Como será visto a seguir, a propriedade de comutatividade dos elementos do grupo estabilizador garante que se possa medir simultaneamente os elementos do grupo e a propriedade de estabilizar os elementos do código fornece um método de caracterização dos parâmetros do código, tais como a dimensão e a sua capacidade de correção. Dito isso, agora é possível descrever um código estabilizador. O código estabilizador $\mathcal{Q}$ associado ao grupo estabilizador $\mathcal{S}$ é o subespaço não nulo de $\mathcal{H}_q^n$ definido por

$$\mathcal{Q} = \bigcap_{S \in \mathcal{S}} \{|\psi\rangle \in \mathcal{H}_q^n\colon S|\psi\rangle = |\psi\rangle\}. \tag{3.10}$$

Dizendo de outra forma, $\mathcal{Q}$ é a interseção de autoespaços com autovalor $+1$ do subgrupo estabilizador $\mathcal{S}$.

3.1.3 – Estabilizador e Correção de Erros

Devido às propriedades de vetores e da detecção no paradigma da Mecânica Quântica, há três tipos de erros de interesse para um código estabilizador $\mathcal{Q}$. Um que deixa o estado imutável ou atua resultando em apenas uma multiplicação escalar do vetor do código, caso em que o erro não afeta a informação codificada. Outro que mapeia o estado do código para um estado pertencendo ao complemento ortogonal de $\mathcal{Q}$, caso em que o erro pode ser detectado por processo de medida. Em formulação matemática, diz-se que o código estabilizador $\mathcal{Q}$ consegue "detectar" um erro E do grupo G_n se, e somente se, a condição $\langle c_1|E|c_2\rangle = \lambda_E\langle c_1|c_2\rangle$ é válida para todo $|c_1\rangle, |c_2\rangle \in \mathcal{Q}$ [76]. Por último, há erros que levam uma palavra-código para uma sobreposição de palavras-código e, assim, o código não é capaz nem de detectar, muito menos de corrigir tais tipos de erros.

O problema agora é associar os erros que o código estabilizador $\mathcal{Q}$ é capaz de corrigir e o grupo estabilizador $\mathcal{S}$ que o define. Será mostrado a seguir que $\mathcal{Q}$ pode detectar todos os erros de G_n que são ou múltiplos escalares de elementos em $\mathcal{S}$ ou que não comutam com algum elemento de $\mathcal{S}$, veja Lema 3.2. Em particular, um erro em G_n é detectável se não comutar com algum dos elementos de $\mathcal{S}$. Seja $\mathcal{S} \leq G_n$ e $C_{G_n}(\mathcal{S})$ denote o centralizador de $\mathcal{S}$ em G_n, ou seja,

$$C_{G_n}(\mathcal{S}) = \{E \in G_n \colon ES = SE, \text{ para todo } S \in \mathcal{S}\}. \tag{3.11}$$

Além disso, denote por $\mathcal{S}Z(G_n)$ o grupo gerado por $\mathcal{S}$ e o centro $Z(G_n)$. Com isso, pode-se apresentar o lema a seguir.

Lema 3.2 *[76, Lema 11] Seja $\mathcal{S} \leq G_n$ um grupo estabilizador de um código estabilizador $\mathcal{Q}$ de dimensão $\dim \mathcal{Q} > 1$. Um erro E em G_n é detectável pelo código $\mathcal{Q}$ se, e somente se, ou E é um elemento de $\mathcal{S}Z(G_n)$ ou E não pertence ao centralizador $C_{G_n}(\mathcal{S})$.*

Demonstração: Inicialmente, suponha que $E \in \mathcal{S}Z(G_n)$. Assim, E é um múltiplo escalar de um elemento do grupo estabilizador e sua ação sobre um estado de $\mathcal{Q}$ é apenas a de multiplicação escalar sobre o mesmo. Daí segue que esse erro é detectável.

Agora, assuma que E é um erro de G_n que não comuta com algum elemento F do grupo estabilizador. Segue que $EF = \lambda FE$, para algum $\lambda \neq 1$. Para todo par de vetores $|u\rangle$ e $|v\rangle$ de $\mathcal{Q}$ segue que

$$\langle u|E|v\rangle = \langle u|EF|v\rangle = \lambda\langle u|FE|v\rangle = \lambda\langle u|E|v\rangle. \tag{3.12}$$

Ou seja, $\langle u|E|v\rangle = 0$ e segue que E é um erro detectável.

Por fim, considere o caso em que E é um elemento de $C_{G_n}(\mathcal{S}) \setminus \mathcal{S}Z(G_n)$. Por absurdo, assuma que E é um erro detectável. Isso implica que existe um escalar complexo λ_E tal que

$E|v\rangle = \lambda_E|v\rangle$ para todo $|v\rangle \in \mathcal{Q}$. Observe que λ_E não pode ser nulo, pois isso faria com que E não pertencesse a $C_{G_n}(\mathcal{S})$. Seja $\mathcal{S}^\star$ o grupo abeliano gerado por $\lambda_E^{-1}E$ e pelos elementos de S. A intersecção de autoespaço de $\mathcal{S}^\star$ com autovalor $+1$ tem dimensão $q^n/|\mathcal{S}^\star| < \dim(\mathcal{Q}) = q^n/|\mathcal{S}|$. Isso implica que nem todos os vetores em $\mathcal{Q}$ permanecem invariantes sobre $\lambda_E^{-1}E$, o que é uma contradição à hipótese inicial. ■

Com o lema anterior podemos categorizar os tipos de erros em três classes:

- *Good*: São os erros pertencentes ao grupo $\mathcal{S}Z(G_n)$. Esses erros deixam o estado inalterado ou apenas atuam como uma multiplicação escalar sobre eles. Assim sendo, em termos práticos, são erros que deixam o estado imutável;

- *Bad*: São erros pertencentes a $G_n \setminus C_{G_n}(\mathcal{S})$. Esses erros levam o estado do código quântico para um espaço ortogonal ao espaço do código. Com isso, é possível efetuar medidas sobre o estado com erro, detectá-lo e corrigí-lo.

- *Ugly*: Esses erros pertencem ao conjunto $C_{G_n}(\mathcal{S}) \setminus \mathcal{S}Z(G_n)$. A ação desses erros é levar o estado para outro vetor, diferente do inicial, que também pertence ao código. Uma vez que esses erros comutam com qualquer elemento de $\mathcal{S}$, tem-se que a ação dos mesmos não pode ser detectada e, consequentemente, corrigida.

Por meio desta descrição, quando é feito o cálculo da distância mínima de um código quântico, mede-se o peso mínimo, em termos de uma medida que será definida posteriormente, dos operadores presentes no conjunto $C_{G_n}(\mathcal{S}) \setminus \mathcal{S}Z(G_n)$.

Exemplo 3.4 *Será apresentado o código quântico proposto por Steane [18]. Seja*

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{3.13}$$

a matriz de verificação de paridade do código de Hamming (Exemplo 2.4) apresentado no Capítulo 2. O grupo estabilizador do código quântico $[[7, 1, 3]]_2$ *proposto por Steane é construído a partir dessa matriz. A matriz estabilizadora para o código é*

$$H_{\mathcal{S}} = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix}. \tag{3.14}$$

Dessa matriz é possível caracterizar a existência dos operadores X *e* Z *no grupo estabilizador. Para cada* 1 *presente na metade esquerda da matriz, tem-se a presença do operador* X*. Por outro lado, para cada* 1 *presenta na metade direita da matriz, tem-se a presença do operador* Z *na respectiva coordenada. Elementos iguais a* 0 *representam a existência da matriz identidade.*

Assim sendo, os elementos do grupo estabilizador $\mathcal{S}$ do código $[[7,1,3]]_2$ são

$$\begin{aligned} S_1 &= X\otimes X\otimes X\otimes I\otimes X\otimes I\otimes I \\ S_2 &= X\otimes I\otimes X\otimes X\otimes I\otimes X\otimes I \\ S_3 &= X\otimes X\otimes I\otimes X\otimes I\otimes I\otimes X \\ S_4 &= Z\otimes Z\otimes Z\otimes I\otimes Z\otimes I\otimes I \\ S_5 &= Z\otimes I\otimes Z\otimes Z\otimes I\otimes Z\otimes I \\ S_6 &= Z\otimes Z\otimes I\otimes Z\otimes I\otimes I\otimes Z. \end{aligned}$$

Como o grupo estabilizador tem 6 elementos, o código tem comprimento 7 e é definido sobre qubits, então tem-se que o número de elementos em $C_{G_n}(\mathcal{S})\setminus\mathcal{S}$ é $2^{7-6}=2$. É fácil verificar que estes operadores são $E_1 = X\otimes X\otimes X\otimes X\otimes X\otimes X\otimes X$ e $E_2 = Z\otimes Z\otimes Z\otimes Z\otimes Z\otimes Z\otimes Z$, visto que eles comutam com qualquer elemento em $\mathcal{S}$. Utilizando este código é possível corrigir qualquer tipo de erro, seja de inversão de bit ou de fase (ou combinação dos dois). Na Seção 3.2 é mostrado como generalizar este resultado por meio da utilização de códigos clássicos e seu dual (euclidiano ou hermitiano).

Como pode ser visto no Lema 3.2 e na discussão que se seguiu, a detectabilidade de erros está bastante associada com a relação de comutação entre os erros detectáveis e o grupo estabilizador do código. Assim, para cálculos práticos, pode vir a ser necessário saber quando dois operadores de erro comutam. Essa condição está associada com o traço simplético de dois vetores em $\mathbb{F}_q^{2n}$. Suponha que $(\mathbf{a}|\mathbf{b})$ e $(\mathbf{a}'|\mathbf{b}')$ são vetores em $\mathbb{F}_q^{2n}$, em que $(\mathbf{a}|\mathbf{b})$ representa a concatenação dos vetores $\mathbf{a}$ e $\mathbf{b}$ pertencentes a $\mathbb{F}_q^n$. Então o produto interno simplético desses dois vetores é dado por

$$\langle(\mathbf{a}|\mathbf{b}),(\mathbf{a}'|\mathbf{b}')\rangle_s := tr_{q/p}(\mathbf{b}\cdot\mathbf{a}'-\mathbf{b}'\cdot\mathbf{a}). \tag{3.15}$$

Com a introdução desse produto interno, podemos apresentar a condição para a qual dois operadores de G_n comutam.

Lema 3.3 *[76, Lema 5] Dois elementos quaisquer $E, E'\in G_n$ podem ser escritos como $E=\beta^c X(\mathbf{a})Z(\mathbf{b})$ e $E'=\beta^{c'}X(\mathbf{a}')Z(\mathbf{b}')$. A relação de comutação leva a ter $EE'=\beta^{tr(\mathbf{b}\cdot\mathbf{a}'-\mathbf{b}'\cdot\mathbf{a})}E'E$, ou seja, E e E' comutam se, e somente se, o traço na forma simplética é zero.*

Demonstração: Segue direto da Eq. 3.4. ∎

Agora será definida a distância mínima de um código quântico $\mathcal{Q}$. Para que isso seja feito, é necessário apresentar o peso simplético de um vetor $(\mathbf{a}|\mathbf{b})$ em $\mathbb{F}_q^{2n}$, em que $(\mathbf{a}|\mathbf{b})$ representa a concatenação dos vetores $\mathbf{a}$ e $\mathbf{b}$ pertencentes a $\mathbb{F}_q^n$. Esse peso será denotado por swt (abreviação do inglês *sympletic weight*) e é definido como

$$\text{swt}((\mathbf{a}|\mathbf{b})) = |\{k|(a_k, b_k) \neq (0,0)\}|, \tag{3.16}$$

em que a_k e b_k são as k-ésimas coordenadas do vetores $\mathbf{a}$ e $\mathbf{b}$, respectivamente. Com isso, pode-se definir o peso de um elemento $E = \beta^c X(\mathbf{a})Z(\mathbf{b}) = \beta^c E_1 \otimes \cdots \otimes E_n$ no grupo de erro G_n, o qual é dado por

$$\text{wt}(E) := |\{E_i \neq I\}| = \text{swt}((\mathbf{a}|\mathbf{b})). \tag{3.17}$$

Um código quântico $\mathcal{Q}$ é dito ter distância mínima d se, e somente se, pode detectar todos os erros em G_n de peso menor que d, mas não pode detectar algum erro de peso d. Ou seja, um código quântico estabilizador tem distância mínima d se $d = \min\{\text{wt}(E)\colon E \in C_{G_n}(\mathcal{S}) \setminus \mathcal{S}Z(G_n)\}$. Um código com distância mínima d também corrige todos os erros de peso $t = \lfloor (d-1)/2 \rfloor$ ou menor. Com isso, diz-se que $\mathcal{Q}$ é um código $((n, K, d))_q$ se, e somente se, $\mathcal{Q}$ é um subespaço de $\mathcal{H}_q^n$ com dimensão K e tem distância mínima d. Um código $((n, q^k, d))_q$ também é denotado por $[[n, k, d]]_q$. Devido à linearidade da Mecânica Quântica, um código quântico que detecta um conjunto $\mathcal{E}$ de erros também detecta todos os erros no espaço linear gerado por $\mathcal{E}$.

Por fim, é dito que um código quântico $\mathcal{Q}$ é puro para t se, e somente se, seu grupo estabilizador $\mathcal{S}$ não contêm operadores de erro não-escalares de peso menor que t. Um código quântico $[[n, k, d]]_q$ é chamado de puro se, e somente se, é puro para sua distância mínima d. Um código impuro também é chamado de código degenerado. A importância de códigos puros é quantificada no Corolário 3.1.

Corolário 3.1 *[76, Corolário 12] Se um código estabilizador $\mathcal{Q}$ tem distância mínima d e é puro para t, então todos os erros $E \in G_n$ com $1 \leq wt(E) < \min\{t, d\}$ satisfazem $\langle u|E|v\rangle = 0$, para todo $|u\rangle, |v\rangle \in \mathcal{Q}$.*

Demonstração: Por hipótese, como o peso de E é menor que a distância mínima do código estabilizador $\mathcal{Q}$, então ele é detectável. Entretanto, E não é um elemento de $\mathcal{S}Z(G_n)$, visto que o código é puro para $t > wt(E)$. Além disso, como E também não pertence a $C_{G_n}(\mathcal{S})$, tem-se que a afirmação segue da Eq. 3.12. ∎

Para códigos puros, têm-se que erros que levem um estado do código quântico para um espaço que seja ortogonal ao espaço do código é um erro detectável. Além disso, esses espaços são degenerados; ou seja, erros distintos levam o estado para espaços distintos.

3.2 – Construção de Códigos Quânticos a partir de Códigos Clássicos Auto-ortogonais

Nesta seção será apresentada a relação entre códigos estabilizadores e códigos clássicos. A ideia central dessa relação é que a detecção de um erro de fase global é irrelevante. Isso significa

que é possível descartar o fator da fase global e definir uma aplicação sobrejetora que vai de $G_n/Z(G_n)$ para $\mathbb{F}_q^{2n}$ e estudar as imagens dessa aplicação sobre $\mathcal{S}$ e $C_{G_n}(\mathcal{S})$.

Usando essa conexão entre o grupo quociente $G_n/Z(G_n)$ e vetores em $\mathbb{F}_q^{2n}$, é demonstrado que a construção de um código estabilizador $\mathcal{Q}$ se reduz à construção de códigos clássicos auto-ortogonais euclidianos ou hermitianos sobre $\mathbb{F}_q$ ou $\mathbb{F}_{q^2}$, respectivamente.

3.2.1 – Códigos sobre $\mathbb{F}_q$

Como foi dito anteriormente, será criada um aplicação de G_n para $\mathbb{F}_q^{2n}$ que será útil para o desenvolvimento de uma relação entre códigos estabilizadores e códigos clássicos. Assim, defina

$$\begin{aligned} \xi\colon G_n &\rightarrow \mathbb{F}_q^{2n} && (3.18)\\ \beta^c X(\mathbf{a})Z(\mathbf{b}) &\mapsto (\mathbf{a}|\mathbf{b}). && (3.19) \end{aligned}$$

Com isso, nota-se que a aplicação ξ leva o grupo $SZ(G_n)$ no código aditivo

$$\mathcal{C} = \{(\mathbf{a}|\mathbf{b})\colon \beta^c X(\mathbf{a})Z(\mathbf{b}) \in \mathcal{S}Z(G_n)\} = \mathcal{S}Z(G_n)/Z(G_n). \tag{3.20}$$

A aditividade do código $\mathcal{C}$ pode ser vista pelo fato de que o grupo estabilizador $\mathcal{S}$ é fechado sobre multiplicação.

O traço na forma simplética introduzido na seção anterior pode ser utilizado para definir o dual simplético do código aditivo $\mathcal{C}$. Seja $\mathcal{C}^{\perp_s}$ o dual de $\mathcal{C}$ relacionado ao traço simplético, ou seja,

$$\mathcal{C}^{\perp_s} = \{\mathbf{x} \in \mathbb{F}_q^{2n}\colon \langle \mathbf{x}, \mathbf{c}\rangle_s = 0 \textit{ para todo } \mathbf{c} \in \mathcal{C}\}. \tag{3.21}$$

Por definição, o centralizador $C_{G_n}(\mathcal{S})$ contém todos os elementos de G_n que comutam com cada um dos elementos de S. Assim, veja Lema 3.3, tem-se que ξ mapeia sobrejetivamente $C_{G_n}(S)$ em $\mathcal{C}^{\perp_s}$,

$$\mathcal{C}^{\perp_s} = \{(\mathbf{a}|\mathbf{b})\colon \beta^c X(\mathbf{a})Z(\mathbf{b}) \in C_{G_n}(S)\}. \tag{3.22}$$

A conexão que foi mencionada algumas vezes anteriormente, entre códigos estabilizadores e códigos clássicos, é finalmente apresentada no Teorema 3.1 a seguir.

Teorema 3.1 *[76, Teorema 13] Um código estabilizador $((n, K, d))_q$ existe se, e somente se, existe um código aditivo $\mathcal{C} \in \mathbb{F}_q^{2n}$ de tamanho $|\mathcal{C}| = q^n/K$ tal que $\mathcal{C} \leq \mathcal{C}^{\perp_s}$ e $swt(\mathcal{C}^{\perp_s} \setminus \mathcal{C}) = d$ se $K > 1$ (ou $swt(\mathcal{C}^{\perp_s}) = d$ se $K = 1$).*

Demonstração: Suponha que exista um código estabilizador $\mathcal{Q}$ com parâmetros $((n, K, d))_q$. Isso implica que existe um subgrupo $\mathcal{S}$ de G_n com ordem $|\mathcal{S}| = q^n/K$ tal que $\mathcal{Q}$ é a interseção

de autoespaços de $\mathcal{S}$ com autovalor $+1$. O grupo $\mathcal{S}$ é abeliano e satisfaz $\mathcal{S} \cap Z(G_n) = I$, veja o Lema 10 de trabalho de Ketkar, *et al.* [76]. O quociente $\mathcal{C} \approx \mathcal{S}Z(G_n)/Z(G_n)$ é um subgrupo aditivo de $\mathbb{F}_q^{2n}$ tal que $|\mathcal{C}| = |\mathcal{S}| = q^n/K$. Tem-se que $\mathcal{C}^{\perp_s} = C_{G_n}(\mathcal{S})/Z(G_n)$ pelo Lema 3.3. Como $\mathcal{S}$ é um grupo abeliano, tem-se que $\mathcal{S}Z(G_n) \leq C_{G_n}(\mathcal{S})$ e, assim, $\mathcal{C} \leq \mathcal{C}^{\perp_s}$. Se $K = 1$, então $\mathcal{Q}$ é um código estabilizador puro, fazendo com que $\text{wt}(C_{G_n}(S)) = \text{swt}(\mathcal{C}^{\perp_s}) = d$. Se $K > 1$, então os elementos de $C_{G_n}(S) \setminus \mathcal{S}Z(G_n)$ tem peso pelo menos d pelo Lema 3.2, o que leva a $\text{swt}(\mathcal{C}^{\perp_s} \setminus \mathcal{C}) = d$.

Por outro lado, suponha que $\mathcal{C}$ é um subgrupo aditivo de $\mathbb{F}_q^{2n}$ tal que $|\mathcal{C}| = q^n/K$, $\mathcal{C} \leq \mathcal{C}^{\perp_s}$ e $\text{swt}(\mathcal{C}^{\perp_s} \setminus \mathcal{C}) = d$ se $K > 1$ (e $\text{swt}(\mathcal{C}^{\perp_s}) = d$ se $K = 1$). Seja $N = \{\beta^c X(\mathbf{a})Z(\mathbf{b})\colon c \in \mathbb{F}_p \text{ e } (\mathbf{a}|\mathbf{b}) \in \mathcal{C}\}$. Note que N é um subgrupo abeliano normal de G_n, pois é a pré-imagem de $\mathcal{C} = N/Z(G_n)$. Escolha a característica ξ de N tal que $\xi(\beta^c I) = \beta^c$. Então

$$P_N = \frac{1}{|N|} \sum_{E \in N} \xi(E^{-1})E \tag{3.23}$$

é um projetor ortogonal sobrejetor no espaço vetorial $\mathcal{Q}$, visto que P_n é idempotente no grupo $C_{G_n}(S)$, veja o trabalho de Klappenecker e Rötteler [77]. Assim tem-se

$$\dim \mathcal{Q} = \text{Tr}(P_n) = |Z(G_n)|q^n/|N| = q^n/|\mathcal{C}| = K. \tag{3.24}$$

Cada classe lateral de N módulo $Z(G_n)$ contém exatamente uma matriz E tal que $E|v\rangle = |v\rangle$, para todo $|v\rangle \in \mathcal{Q}$. Com isso, o conjunto $\mathcal{S} = \{E \in N\colon E|v\rangle = |v\rangle \text{ para todo } |v\rangle \in \mathcal{Q}\}$ está bem definido. $\mathcal{S}$ é um subgrupo abeliano de G_n de ordem $|\mathcal{S}| = |\mathcal{C}| = q^n/K$. É possível notar que $\mathcal{Q}$ é a interseção de autoespaços com autovalor $+1$ de $\mathcal{S}$ e tem $\dim \mathcal{Q} = q^n/|\mathcal{S}| = K$. Um elemento $\beta^c X(\mathbf{a})Z(\mathbf{b})$ em $C_{G_n}(\mathcal{S}) \setminus SZ(G_n)$ não pode ter peso menor que d, pois isso implicaria que $(\mathbf{a}|\mathbf{b}) \in \mathcal{C}^{\perp_s} \setminus \mathcal{C}$ tem peso menor que d, o que é impossível por hipótese. Pela mesma razão, se $K = 1$, então todos os elementos do centralizador $C_{G_n}(\mathcal{S})$ diferentes da identidade devem ter peso igual a d ou maior. Assim, $\mathcal{Q}$ é um código estabilizador com parâmetros $((n, K, d))_q$. ∎

Utilizando o Teorema 3.1 pode-se extrair o método de construção CSS de códigos estabilizadores proposto por Calderbank, Shor [78] e Steane [18] em 1996.

Lema 3.4 *(Construção CSS de Códigos Estabilizadores) Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ dois códigos lineares clássicos com parâmetros $[n, k_1, d_1]_q$ e $[n, k_2, d_2]_q$, respectivamente, tais que $\mathcal{C}_2^{\perp} \leq \mathcal{C}_1$. Então existe um código estabilizador $[[n, k_1 + k_2 - n, d]]_q$ com distância mínima $d = \min\{wt(\mathbf{c})|\mathbf{c} \in (\mathcal{C}_1 \setminus \mathcal{C}_2^{\perp}) \cup (\mathcal{C}_2 \setminus \mathcal{C}_1^{\perp})\}$ que é puro para $\min\{d_1, d_2\}$.*

Demonstração: Seja $\mathcal{C} = \mathcal{C}_1^{\perp} \times \mathcal{C}_2^{\perp} \leq \mathbb{F}_q^{2n}$. É possível ver que $\mathcal{C} \leq \mathcal{C}_2 \times \mathcal{C}_1$, pois $\mathcal{C}_2^{\perp} \leq \mathcal{C}_1$ por hipótese. Se $(\mathbf{c_1}|\mathbf{c_2}) \in \mathcal{C}$ e $(\mathbf{c_1'}|\mathbf{c_2'}) \in \mathcal{C}_2 \times \mathcal{C}_1$, então observa-se que $tr(\mathbf{c_2} \cdot \mathbf{c_1'} - \mathbf{c_2'} \cdot \mathbf{c_1}) = tr(0 - 0) = 0$. Assim, $\mathcal{C} \leq \mathcal{C}_2 \times \mathcal{C}_1 \leq \mathcal{C}^{\perp_s}$. Uma vez que $|\mathcal{C}| = q^{2n-k_1-k_2}$, $|\mathcal{C}^{\perp_s}| = q^{2n}/|\mathcal{C}| = q^{k_1+k_2} = |\mathcal{C}_2 \times \mathcal{C}_1|$. Consequentemente, $\mathcal{C}^{\perp_s} = \mathcal{C}_2 \times \mathcal{C}_1$. Pelo Teorema 3.1

tem-se que existe um código estabilizador $((n, K, d))_q$ com $K = q^n/|\mathcal{C}| = q^{k_1+k_2-n}$. A afirmação sobre a distância mínima e pureza seguem, também, do Teorema 3.1. ■

Corolário 3.2 *Seja $\mathcal{C}$ um código linear clássico $[n, k, d]_q$ contendo seu dual, $\mathcal{C}^\perp \leq \mathcal{C}$, então existe um código estabilizador $[[n, 2k - n, \geq d]]_q$ que é puro para d.*

3.2.2 – Códigos sobre $\mathbb{F}_{q^2}$

Será mostrado agora que também é possível criar uma relação entre códigos estabilizadores e códigos sobre $\mathbb{F}_{q^2}$. Para isso, primeiramente é necessário apresentar o tipo da operação traço que é utilizado aqui. Seja $\{\beta, \beta^q\}$ uma base normal de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$. Define-se o traço na forma alternante de dois vetores $\mathbf{v}$ e $\mathbf{w}$ em $\mathbb{F}_{q^2}^n$ por

$$\langle \mathbf{v}, \mathbf{w} \rangle_a := tr_{q/p}\Big(\frac{\mathbf{v} \cdot \mathbf{w}^q - \mathbf{v}^q \cdot \mathbf{w}}{\beta^{2q} - \beta^2}\Big) \tag{3.25}$$

Seja $\phi\colon \mathbb{F}_q^{2n} \to \mathbb{F}_{q^2}^n$ uma aplicação descrita por $(\mathbf{a}|\mathbf{b}) \to \beta\mathbf{a} + \beta^q\mathbf{b}$. A aplicação ϕ é uma isometria no sentido que o peso simplético de $(\mathbf{a}|\mathbf{b})$ é igual ao peso de Hamming de $\phi((\mathbf{a}|\mathbf{b}))$. Se $\mathcal{C} \leq \mathbb{F}_{q^2}^n$, então denota-se o seu dual com relação ao traço na forma alternante por $\mathcal{C}^{\perp_a} := \{\mathbf{v} \in \mathbb{F}_{q^2}^n\colon \langle \mathbf{v}, \mathbf{w} \rangle_a = 0 \text{ para todo } \mathbf{w} \in \mathcal{C}\}$. Essa aplicação permite transformar a dualidade relacionada ao traço na forma simplética para uma dualidade no traço na forma alternante.

Lema 3.5 *Suponha que $\mathbf{c}$ e $\mathbf{d}$ são dois vetores de $\mathbb{F}_q^{2n}$. Então*

$$\langle \mathbf{c}, \mathbf{d} \rangle_s = \langle \phi(\mathbf{c}), \phi(\mathbf{d}) \rangle_a. \tag{3.26}$$

Em particular, $\mathbf{c}$ e $\mathbf{d}$ são ortogonais com respeito ao traço na forma simplética se, e somente se, $\phi(\mathbf{c})$ e $\phi(\mathbf{d})$ são ortogonais com respeito ao traço na forma alternante.

Demonstração: Sejam $\mathbf{c} = (\mathbf{a}|\mathbf{b})$ e $\mathbf{d} = (\mathbf{a}'|\mathbf{b}')$. Então, tem-se

$$\langle \phi(\mathbf{c}), \phi(\mathbf{d})^q \rangle = \beta^{q+1}\mathbf{a} \cdot \mathbf{a}' + \beta^2 \mathbf{a} \cdot \mathbf{b}' + \beta^{2q}\mathbf{b} \cdot \mathbf{a}' + \beta^{q+1}\mathbf{b} \cdot \mathbf{b}' \tag{3.27}$$

$$\langle \phi(\mathbf{c})^q, \phi(\mathbf{d}) \rangle = \beta^{q+1}\mathbf{a} \cdot \mathbf{a}' + \beta^{2q}\mathbf{a} \cdot \mathbf{b}' + \beta^2 \mathbf{b} \cdot \mathbf{a}' + \beta^{q+1}\mathbf{b} \cdot \mathbf{b}'. \tag{3.28}$$

Assim, o traço na forma alternante de $\phi(\mathbf{c})$ e $\phi(\mathbf{d})$ é dado por

$$\langle \phi(\mathbf{c}), \phi(\mathbf{d}) \rangle_a = tr_{q/p}\Big(\frac{\phi(\mathbf{c}) \cdot \phi(\mathbf{d})^q - \phi(\mathbf{c})^q \cdot \phi(\mathbf{d})}{\beta^{2q} - \beta^2}\Big) = tr_{q/p}(\mathbf{b} \cdot \mathbf{a}' - \mathbf{a} \cdot \mathbf{b}'), \tag{3.29}$$

que é precisamente o traço na forma simplética $\langle \mathbf{c}, \mathbf{d} \rangle_s$. ■

Com isso, é possível reformular o Teorema 3.1 para o caso em que se utilize o traço na forma alternante. Veja Teorema 3.2.

Teorema 3.2 *[76, Teorema 15] Um código estabilizador $((n, K, d))_q$ existe se, e somente se, existe um código aditivo $\mathcal{C} \leq F_{q^2}^n$ de tamanho $|\mathcal{C}| = q^n/K$ tal que $\mathcal{C} \leq \mathcal{C}^{\perp_a}$ e $swt(\mathcal{C}^{\perp_a} \setminus \mathcal{C}) = d$ se $K > 1$ (ou $swt(\mathcal{C}^{\perp_a}) = d$ se $K = 1$).*

Demonstração: Segue diretamente da construção da aplicação ϕ e do Teorema 3.1. ■

Caso se trabalhe com códigos lineares, em vez da formulação geral mostrada para códigos apenas aditivos, então a utilização do produto interno hermitiano para a construção dos códigos estabilizadores é mais útil. Como foi mostrado no Capítulo 2, o produto interno hermitiano entre dois $\mathbf{v}, \mathbf{w} \in \mathbb{F}_{q^2}^n$ é dado por

$$\langle \mathbf{v}, \mathbf{w} \rangle_h = \langle \mathbf{v}^q, \mathbf{w} \rangle, \tag{3.30}$$

em que $\mathbf{v}^q = (v_1^q, \ldots, v_n^q)$. Da definição de traço na forma alternante é claro que se dois vetores são ortogonais com respeito ao produto interno hermitiano, então eles também serão ortogonais com respeito ao traço na forma alternante. Consequentemente, se $\mathcal{C} \leq \mathbb{F}_{q^2}^n$, então $\mathcal{C}^{\perp_h} \leq \mathcal{C}^{\perp_a}$, onde $\mathcal{C}^{\perp_h} = \{\mathbf{v} \in \mathbb{F}_{q^2}^n : \langle \mathbf{v}, \mathbf{w} \rangle_h = 0 \text{ para todo } \mathbf{w} \in \mathcal{C}\}$.

Assim, quaisquer códigos auto-ortogonais com respeito ao produto interno hermitiano também serão auto-ortogonais com relação ao traço na forma alternante. No caso geral, $\mathcal{C}^{\perp_h}$ e $\mathcal{C}^{\perp_a}$ são diferentes, mas acontece que quando os códigos são $\mathbb{F}_{q^2}$-lineares, então esses dois espaços duais coincidem.

Lema 3.6 *Suponha que $\mathcal{C} \leq \mathbb{F}_{q^2}^n$ é $\mathbb{F}_{q^2}$-linear, então $\mathcal{C}^{\perp_h} = \mathcal{C}^{\perp_a}$.*

Demonstração: Seja $q = p^m$, em que p é um número primo. Se $\mathcal{C}$ é um subespaço de dimensão k de $\mathbb{F}_{q^2}^n$, então $\mathcal{C}^{\perp_h}$ é também um subespaço de $\mathbb{F}_{q^2}^n$ mas com dimensão $n - k$. É possível também ver $\mathcal{C}$ como um subespaço de $\mathbb{F}_p^{2mn}$ com dimensão $2mk$ e seu dual com relação ao traço alternante $\mathcal{C}^{\perp_a}$ como um subespaço de $\mathbb{F}_p^{2mn}$ com dimensão $2m(n - k)$. Visto que $\mathcal{C}^{\perp_h} \subseteq \mathcal{C}^{\perp_a}$ e os dois subespaços tem a mesma cardinalidade; então, tem-se que eles são iguais. ■

Corolário 3.3 *Se existe um código C que é $\mathbb{F}_{q^2}$ linear e $\mathcal{C}^{\perp_h} \leq \mathcal{C}$, então existe um código estabilizador $[[n, 2k - n, \geq d]]_q$ que é puro para d.*

Demonstração: Notando que $\mathcal{C}$ pode ser visto como um espaço vetorial com dimensão $2mk$, onde $q = p^m$, e utilizando o Teorema 3.2, o corolário segue. ■

Ref. [63].r-Laflamme de um código estabilizador. Para ver isso, assuma que $C \leq \mathbb{F}_q^{2n}$ denota um código aditivo associado com o código estabilizador Q. Defina os pesos simpléticos de C e $C^{\perp_s}$, respectivamente, por

3.3 – Limitantes sobre Códigos Quânticos

Será apresentado diversos limitantes, tais como limitantes computacionais para os pesos simpléticos e distância mínima. Inicialmente será mostrado alguns resultados de limitantes relacionados com pesquisa computacional.

Teorema 3.3 *[76, Teorema 25] Seja $\mathcal{Q}$ um código estabilizador com parâmetros $((n, K, d))_q$ em que $K > 1$, então existe uma solução para o seguinte problema de otimização: minimize $\sum_{j=1}^{d-1} A_j$ sujeito as restrições*

1. $A_0 = 1$ *e* $A_j \geq 0$ *para todo* $1 \leq j \leq n$*;*
2. $\sum_{j=0}^{n} A_j = q^n/K$*;*
3. $B_j = \frac{K}{q^n} \sum_{r=0}^{n} K_j(r) A_r$ *se mantem para todo* $0 \leq j \leq n$*;*
4. $A_j = B_j$ *para todo* $0 \leq j < d$ *e* $A_j \leq B_j$ *para todo* $d \leq j \leq n$*;*
5. $(p-1)$ *divide* A_j *para todo* $1 \leq j \leq n$*.*

Para o caso em que é utilizado códigos sobre $\mathbb{F}_{q^2}$ para construir códigos estabilizadores, então a condição 5. do Teorema 3.3 tem, em vez de "$(p-1)$ divide A_j", "$q^2 - 1$ dividindo A_j".

O próximo limitante também se baseia em busca computacional e será utilizado posteriormente na demonstração do limitante de Singleton.

Teorema 3.4 *[76, Teorema 27] Seja $\mathcal{Q}$ um código estabilizador com parâmetros $((n, K, d))_q$ em que $K > 1$. Suponha que S é um subconjunto não-vazio de $\{0, \ldots, d-1\}$ e $N = \{0, \ldots, n\}$. Seja*

$$f(x) = \sum_{i=0}^{n} f_i K_i(x) \tag{3.31}$$

satisfazendo as condições:

1. $f_x > 0$ *para todo* $x \in S$ *e* $f_x \geq 0$ *caso contrário;*
2. $f(x) \leq 0$ *para todo* $x \in N \setminus S$*.*

Então

$$K \leq \frac{1}{q^n} \max_{x \in S} \frac{f(x)}{f_x}. \tag{3.32}$$

Corolário 3.4 *[79, Lema 1.3](Limitante de Singleton Quântico) Seja $\mathcal{Q}$ um código quântico com parâmetros $((n, K, d))_q$ em que $K > 1$. Então, tem-se que*

$$K \leq q^{n-2d+2}. \tag{3.33}$$

Demonstração: Seja $S = \{0, \ldots, d-1\}$. Assuma que

$$f(x) = q^{n-d+1} \prod_{j=d}^{n} \Big(1 - \frac{x}{j}\Big). \tag{3.34}$$

É possível expressar o polinômio $f(x) = \sum_{i=0}^{n} f_i K_i(x)$, em que

$$f_i = q^{-2n} \sum_{x=0}^{n} f(x) K_x(i) = q^{1-d-n} \sum_{x=0}^{n} K_x(i) \binom{n-x}{n-d+1} \Big/ \binom{n}{n-d+1}. \tag{3.35}$$

Como é mostrado no trabalho de Levenshtein [80] que $\sum_{x=0}^{n} K_x(i) \binom{n-x}{n-d+1} = \binom{n-i}{d-1} q^{2(d-1)}$, então a expressão anterior pode ser resumida para

$$f_i = q^{d-1-n} \binom{n-i}{d-1} \Big/ \binom{n}{n-d+1} > 0. \tag{3.36}$$

Se $r(x) := f(x)/f_x$, então

$$r(x) = \frac{f(x)}{f_x} = q^{2n-2d+2} \binom{n-x}{n-d+1} \Big/ \binom{n-x}{d-1}. \tag{3.37}$$

Além disso, tem-se que

$$\frac{r(x)}{r(x+1)} = \frac{n-x-d+1}{d-x-1}. \tag{3.38}$$

A partir de agora será efetivamente demonstrado o corolário em questão. Por absurdo, assuma que exista um código estabilizador com parâmetros $((n, K, d))_q$ tal que $2d \geq n+2$. Com isso se terá $r(x)/r(x+1) \leq 1$, tendo valor máximo para $r(x)$ quando $x = d-1$, quando $x \in \{0, \ldots, d-1\}$. Pelo Teorema 3.4 tem-se que $K \leq r(d-1)/q^n = q^{n-2d+2} / \binom{n-d+1}{d-1}$, o que é uma contradição, pois $K \binom{n-d+1}{d-1} \leq q^{n-2d+2} \leq 1$ e, por hipótese, $K > 1$.

Já para $2d < n+2$, então $r(x)/r(x+1) > 1$ e o máximo de $r(x)$ acontece quando $x = 0$, uma vez que $x \in \{0, \ldots, d-1\}$. Como $r(0) = q^{2n-2d+2}$, então o Teorema 3.4 implica que

$$K \leq q^{-n} \max_{0 \leq x < d} \frac{f(x)}{f_x} = q^{n-2d+2}. \tag{3.39}$$

■

Um código quântico que atinge o limitante de Singleton quântico é denominado de código quântico com máxima distância de separação ou MDS (do inglês, *Maximum Distance Separable*).

A seguir será apresentado o análogo quântico do limitante de Hamming. A utilização desse limitante é normalmente feita para analisar códigos estabilizadores que tem faixa de parâmetros onde não é possível construir códigos estabilizadores MDS.

Teorema 3.5 *[79, Lema 1.2](Limitante de Hamming Quântico) Seja $\mathcal{Q}$ um código*

estabilizador com parâmetros $((n, K, d))_q$ *em que* $K > 1$. *Então, tem-se que*

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q^2-1)^i \leq \frac{q^n}{K}. \tag{3.40}$$

Um código quântico que atinge o limitante de Hamming quântico é chamado de código quântico perfeito. Por último será mostrado a generalização do limitante de Gilbert-Varshamov mostrado na Proposição 2.9 para código quânticos.

Teorema 3.6 *[79, Teorema 1.4](Limitante de Gilbert-Varshamov) Seja* $h_q(x)$ *a função entropia* q*-ária da Eq. 2.24 e* $\mathcal{Q}$ *um código quântico com parâmetros* $[[n, k, d]]_q$*, com taxa* $R(\mathcal{Q}) = k/n$. *Então, para qualquer* q *e* $\delta \in [0, 1 - 1/q]$*, existem códigos quânticos* $\mathcal{Q}$*'s com taxa*

$$R_q^{\mathcal{Q}}(\delta) \geq 1 - h_q(\delta) - \delta \log_q(q+1). \tag{3.41}$$

3.4 – Códigos Algébrico-Geométricos Quânticos

Esta seção é dividida em três partes. A primeira trata sobre a construção de códigos AG quânticos com t-lugares; na segunda serão construídos códigos AG os quais possuem o divisor G como sendo uma soma de lugares não racionais e, na terceira parte, constrói-se uma sequência códigos AG quânticos assintoticamente bons, no sentido que será apresentado. Todos os resultados dessa seção são de co-autoria do autor desta tese e estão contidos na Ref. [63].

3.4.1 – Códigos Algébrico-Geométricos Quânticos com t-lugares

O primeiro resultado baseia-se na utilização de códigos AG com t-lugares para a derivação de códigos quânticos com bons parâmetros.

Teorema 3.7 *(Construção Geral de* t*-lugares) Seja* q *uma potência de um número primo e* $F/\mathbb{F}_q$ *um corpo de funções de gênero* g *com* $(n+t)$*-lugares racionais. Assuma que* a_i, b_i*,* $i = 1, \ldots, t$*, são inteiros positivos tais que* $a_i \leq b_i$ *para todo* i *e* $2g - 2 < \sum_{i=1}^{t} a_i < \sum_{i=1}^{t} b_i < n$. *Então existe um código quântico com parâmetros* $[[n, k, d]]_q$*, com* $k = \sum_{i=1}^{t} b_i - \sum_{i=1}^{t} a_i$ *e* $d \geq \min\left\{ n - \sum_{i=1}^{t} b_i, \sum_{i=1}^{t} a_i - (2g-2) \right\}$.

Demonstração: Seja $\{P_1, P_2, \ldots, P_n, P_{n+1}, \ldots, P_{n+t}\}$ o conjunto de lugares de $F/\mathbb{F}_q$ de grau um. Assuma que $D = P_1 + \cdots + P_n$ é um divisor de $F/\mathbb{F}_q$. Além disso, considere que G_1 e G_2 são dois divisores de $F/\mathbb{F}_q$ dados, respectivamente, por $G_1 = a_1 P_{n+1} + \cdots + a_t P_{n+t}$ e $G_2 = b_1 P_{n+1} + \cdots + b_t P_{n+t}$, com $a_i \leq b_i$, para todo $i = 1, \ldots, t$ e $2g-2 < \sum_{i=1}^{t} a_i < \sum_{i=1}^{t} b_i < n$.

Por construção, $\operatorname{supp} G_1 \cap \operatorname{supp} D = \emptyset$ e $\operatorname{supp} G_2 \cap \operatorname{supp} D = \emptyset$. Como $G_1 < G_2$ tem-se que $\mathcal{L}(G_1) \subset \mathcal{L}(G_2)$, o que leva a $C_{\mathcal{L}}(D, G_1) \subset C_{\mathcal{L}}(D, G_2)$. Do Teorema 2.4, o código $C_1 := C_{\mathcal{L}}(D, G_1)$ tem parâmetros $[n, k_1, d_1]_q$, com $d_1 \geq n - \sum_{i=1}^{t} a_i$ e $k_1 = \sum_{i=1}^{t} a_i - g + 1$ e $C_2 := C_{\mathcal{L}}(D, G_2)$ tem parâmetros $[n, k_2, d_2]_q$, com $d_2 \geq n - \sum_{i=1}^{t} b_i$ e $k_2 = \sum_{i=1}^{t} b_i - g + 1$. Por outro lado, do Teorema 2.5, o código dual $C_1^{\perp} = C_{\Omega}(D, G_1)$ de C_1 tem parâmetros $[n, k_1^{\perp}, d_1^{\perp}]_q$, com $d_1^{\perp} \geq \sum_{i=1}^{t} a_i - (2g-2)$ e $k_1^{\perp} = n + g - 1 - \sum_{i=1}^{t} a_i$, e o código dual $C_2^{\perp} = C_{\Omega}(D, G_2)$ de C_2 tem parâmetros $[n, k_2^{\perp}, d_2^{\perp}]_q$ com $d_2^{\perp} \geq \sum_{i=1}^{t} b_i - (2g-2)$ e $k_2^{\perp} = n + g - 1 - \sum_{i=1}^{t} b_i$.

Aplicando a construção CSS, Lema 3.4, aos códigos C_1 e C_2, obtêm-se um código quântico com os parâmetros mencionados. ■

Observação 3.1 *Fazendo uma comparação com os códigos na literatura, nota-se que nos trabalhos Chen,* et al. *[25] e Kim e Walker[81] são utilizados códigos AG com um lugar para construir códigos quânticos bons ou assintoticamente bons. Em [26], os autores aplicam códigos AG de dois-lugares para derivar códigos quânticos bons ou assintoticamente bons. No Teorema 3.7 é feito uma generalização natural dessas construções de códigos de um e dois lugares para a construção de códigos com t-lugares, com* $t \geq 1$.

Corolário 3.5 *(Códigos de Um-lugares) Existe um código quântico com parâmetros* $[[q(1 + (q-1)m), b-a, d]]_{q^2}$, *com* $(q-1)(m-1) - 2 < a < b < q(1 + (q-1)m)$, $m|(q+1)$ *e* $d \geq \min\{q(1 + (q-1)m) - b, a - (q-1)(m-1) + 2\}$.

Demonstração: Seja $F/\mathbb{F}_q$ o corpo de funções definido pela equação $y^q + y = x^m$ e $m|(q+1)$. Sabe-se que o gênero de $F/\mathbb{F}_q$ é $g = (q-1)(m-1)/2$ e o número de lugares de grau 1 é $N = 1 + q(1 + (q-1)m)$ (veja [71, Exemplo 6.4.2]). Seja $\{P_1, P_2, \ldots, P_n, P_{n+1}, \ldots, P_N\}$ o conjunto com todos esses lugares. Sem perda de generalidade, assuma que $D = P_1 + \cdots + P_{N-1}$ e $G_1 = aP_N$ e $G_2 = bP_N$ são dois divisores tais que $\operatorname{supp} G_1 \cap \operatorname{supp} D = \emptyset$ e $\operatorname{supp} G_2 \cap \operatorname{supp} D = \emptyset$, com $(q-1)(m-1) - 2 < a < b < q(1 + (q-1)m)$. Pelo Teorema 3.7, existe um código quântico com parâmetros $[[q(1 + (q-1)m), b-a, d]]_{q^2}$, em que $d \geq \min\{q(1 + (q-1)m) - b, a - (q-1)(m-1) + 2\}$. Assim, a demonstração está completa.

■

Observação 3.2 *Note que a curva de Hermite definida por* $y^q + y = x^{q+1}$, *sobre* $\mathbb{F}_{q^2}$, *é um caso particular da curva* $y^q + y = x^m$ *considerado na demonstração do Corolário 3.5.*

Corolário 3.6 *(Códigos de Dois-lugares) Existe um código quântico com parâmetros* $[[q(1 + (q-1)m) - 1, b_1 + b_2 - a_1 - a_2, d]]_{q^2}$, *com* $a_i \leq b_i$ *para* $i = 1, 2$, $(q-1)(m-1) - 2 <$

$a_1 + a_2 < b_1 + b_2 < q(1 + (q-1)m) - 1$, $m|(q+1)$ *e* $d \geq \min\{q(1 + (q-1)m) - b_1 - b_2 - 1, a_1 + a_2 - (q-1)(m-1) + 2\}$.

Demonstração: Seja $D = P_1 + \cdots + P_{N-2}$ um divisor e $G_1 = a_1 P_{N-2} + a_2 P_{N-1}$ e $G_2 = b_1 P_{N-2} + b_2 P_{N-1}$ outros dois divisores com $\operatorname{supp} G_1 \cap \operatorname{supp} D = \emptyset$ e $\operatorname{supp} G_2 \cap \operatorname{supp} D = \emptyset$, com $(q-1)(m-1) - 2 < a_1 + a_2 < b_1 + b_2 < q(1 + (q-1)m) - 1$. Do Teorema 3.7, existe um código quântico com parâmetros $[[q(1 + (q-1)m) - 1, b_1 + b_2 - a_1 - a_2, d]]_{q^2}$, tendo $d \geq \min\{q(1 + (q-1)m) - 1 - b_1 - b_2, a_1 + a_2 - (q-1)(m-1) + 2\}$. ■

Corolário 3.7 *(Códigos de t-lugares) Existe um código quântico com parâmetros* $[[q(1 + (q-1)m) - t + 1, b_1 + \cdots + b_t - (a_1 + \cdots + a_t), d]]_{q^2}$, *com* $a_i \leq b_i$ *para* $i = 1, \ldots t$, $(q-1)(m-1) - 2 < a_1 + \cdots + a_t < b_1 + \cdots + b_t < q(1 + (q-1)m) - t + 1$, $m|(q+1)$ *e* $d \geq \min\{q(1 + (q-1)m) - (b_1 + \cdots + b_t) - t + 1, a_1 + \cdots + a_t - (q-1)(m-1) + 2\}$.

Demonstração: Similar à demonstração do Corolário 3.6. ■

3.4.2 – Códigos Algébrico-Geométricos Quânticos com Divisores não-Racionais

Esta subseção trata da construção de códigos quânticos a partir de códigos AG que possuem divisores que são múltiplos de um lugar não-racional. O primeiro resultado é dado logo a seguir.

Teorema 3.8 *(Construção Geral) Seja q uma potência de um número primo e $F/\mathbb{F}_q$ um corpo de funções com gênero g e tendo n lugares racionais. Assuma que existem lugares $Q_1, \ldots, Q_t$ de $F/\mathbb{F}_q$ com grau $\alpha_i \geq 2$, respectivamente, $i = 1, 2, \ldots, t$. Para todos os inteiros positivos $a_i \leq b_i$, $i = 1, \ldots, t$, tais que $2g - 2 < a_1\alpha_1 + \cdots + a_t\alpha_t < b_1\alpha_1 + \cdots + b_t\alpha_t < n$, existem um código quântico com parâmetros $[[n, k, d]]_q$, com $k = (b_1 - a_1)\alpha_1 + \cdots + (b_t - a_t)\alpha_t$ e $d \geq \min\{n - (b_1\alpha_1 + \cdots + b_t\alpha_t), (a_1\alpha_1 + \cdots + a_t\alpha_t) - (2g-2)\}$.*

Demonstração: A prova é similar à do Teorema 3.7. ■

Corolário 3.8 *Seja q uma potência de um número primo e $F/\mathbb{F}_q$ um corpo de funções hiperelíptica de gênero g com n lugares racionais. Então existe um código quântico com parâmetros $[[n, 2(t_2 - t_1), d]]_q$, com t_1, t_2 sendo inteiros positivos tais que $2g-2 < t_1 < t_2 < n$ e $d \geq \min\{n - 2t_2, 2t_1 - 2g + 2\}$.*

Demonstração: Uma vez que $F/\mathbb{F}_q$ é um corpo de funções hiperelípticas, então existe um lugar G de grau dois (veja [71, Lema 6.2.2(a)]). Seja $D = P_1 + \cdots + P_n$ um divisor, com P_i sendo todos os lugares racionais de $F/\mathbb{F}_q$. Assuma que $G_2 = t_2 G$ e $G_1 = t_1 G$, com $2g - 2 < 2t_1 < 2t_2 < n$. Então, aplicando as ideias contidas na demonstração do Teorema 3.7, obtêm-se o resultado. ■

Exemplo 3.5 *Seja $F/\mathbb{F}_q$ o corpo de funções definido pela equação $y^q + y = x^m$, com $m = 2$ e $q = 5$ (ou seja, $m|(q+1)$). Como o gênero de $F/\mathbb{F}_q$ é $g = 2$, então $F/\mathbb{F}_q$ é um corpo de funções hiperelípticas (veja [71, Lema 6.2.2(b)]) e, consequentemente, o Corolário 3.8 pode ser aplicado. Isso leva a existência de códigos quânticos com parâmetros $[[46, 2(t_2 - t_1), d]]_{25}$, em que t_1, t_2 são inteiros positivos tais que $1 < t_1 < t_2 < 23$ e $d \geq \min\{46 - 2t_2, 2t_1 - 2\}$.*

3.4.3 – Exemplos e Comparação dos Novos Códigos Quânticos

São apresentados na Tabela 4.4 alguns códigos quânticos bons obtidos dos Corolários 3.5 e 3.6. Todos os códigos da Tabela 4.4 são novos, no sentido de que não há códigos na literatura com os mesmos parâmetros. Note que o novo código $[[26, 16, d \geq 3]]_9$ é melhor que o código $[[26, 14, 3]]_9$ apresentado no endereço eletrônico de Edel [82] e, além disso, o código $[[26, 14, d \geq 4]]_9$ tem parâmetros superiores aos do código $[[26, 4, 4]]_9$ também mostrado em [82].

Quando o alfabeto é grande, é difícil encontrar códigos na literatura que tenham parâmetros comparáveis. Por isso, a análise dos códigos criados aqui é baseada sobre o limitante de Singleton quântico. Como foi mostrado em seções anteriores deste capítulo, um código quântico com parâmetros $[[n, k, d]]_q$ deve satisfazer a $k + 2d \leq n + 2$. Note que os códigos quânticos apresentado na Tabela 4.4 de comprimento 46 tem *Singleton defect* iguais a 2. Além disso, todos os novos códigos quânticos de comprimento $n = 26$ e $n = 27$ exibidos na Tabela 4.4 tem *Singleton defect* igual a 3. É também importante notar que o código de comprimento $n = 175$ da Tabela 4.4 tem *Singleton defect* igual a 9. Por exemplo, o novo código $[[175, 31, d \geq 64]]_{49}$ tem distância mínima maior ou igual a 64 e, consequentemente, o seu *Singleton defect* é 9, enquanto os códigos $[[165, 99, 18]]_9$ e $[[194, 144, 8]]_9$ disponíveis na Ref. [82], de comprimento similar, têm distâncias mínimas iguais a 18 e 8, respectivamente, e, como pode ser calculado, *Singleton defect* iguais a 16 e 18, respectivamente. Além disso, note que os novos códigos $[[27, 3, d \geq 10]]_9$, $[[27, 5, d \geq 9]]_9$, $[[65, 9, d \geq 25]]_{25}$, $[[175, 31, d \geq 64]]_{49}$ e $[[175, 1, d \geq 79]]_{49}$ têm distâncias mínimas comparativamente superiores aos da literatura.

Tabela 3.1 – Exemplos de novos códigos algébrico-geométricos quânticos

Novos Códigos do Corolário 3.5	q	m	a	b
$[[27, 17, d \geq 3]]_9$	3	4	7	24
$[[27, 15, d \geq 4]]_9$	3	4	8	23
$[[27, 13, d \geq 5]]_9$	3	4	9	22
$[[27, 11, d \geq 6]]_9$	3	4	10	21
$[[27, 9, d \geq 7]]_9$	3	4	11	20
$[[27, 7, d \geq 8]]_9$	3	4	12	19
$[[27, 5, d \geq 9]]_9$	3	4	13	18
$[[27, 3, d \geq 10]]_9$	3	4	14	17
$[[27, 1, d \geq 11]]_9$	3	4	15	16
$[[64, 48, d \geq 3]]_{16}$	4	5	13	61
$[[64, 46, d \geq 4]]_{16}$	4	5	14	60
$[[64, 44, d \geq 5]]_{16}$	4	5	15	59
$[[64, 24, d \geq 15]]_{16}$	4	5	25	49
$[[64, 4, d \geq 25]]_{16}$	4	5	35	39
$[[64, 2, d \geq 26]]_{16}$	4	5	36	38
$[[65, 53, d \geq 3]]_{25}$	5	3	9	62
$[[65, 51, d \geq 4]]_{25}$	5	3	10	61
$[[65, 49, d \geq 5]]_{25}$	5	3	11	60
$[[65, 9, d \geq 25]]_{25}$	5	3	31	40
$[[175, 153, d \geq 3]]_{49}$	7	4	19	172
$[[175, 151, d \geq 4]]_{49}$	7	4	20	171
$[[175, 149, d \geq 5]]_{49}$	7	4	21	170
$[[175, 109, d \geq 25]]_{49}$	7	4	41	150
$[[175, 31, d \geq 64]]_{49}$	7	4	80	111
$[[175, 1, d \geq 79]]_{49}$	7	4	95	96
Novos Códigos do Corolário 3.6	q	m	$a_1 - a_2$	$b_1 - b_2$
$[[26, 16, d \geq 3]]_9$	3	4	$3-4$	$7-16$
$[[26, 14, d \geq 4]]_9$	3	4	$3-5$	$7-15$
$[[26, 12, d \geq 5]]_9$	3	4	$3-6$	$7-14$
$[[26, 4, d \geq 9]]_9$	3	4	$3-10$	$7-10$
$[[26, 2, d \geq 10]]_9$	3	4	$4-10$	$6-10$
Novos Códigos do Exemplo 3.5	q	m	t_1	t_2
$[[46, 36, d \geq 4]]_{25}$	5	2	3	21
$[[46, 32, d \geq 6]]_{25}$	5	2	4	20
$[[46, 28, d \geq 8]]_{25}$	5	2	5	19
$[[46, 4, d \geq 20]]_{25}$	5	2	11	13

3.5 – Códigos Algébrico-Geométricos Quânticos Assintoticamente Bons

Será proposta a construção de um sequência de códigos quânticos assintoticamente bons derivados de códigos AG. Todos os resultados dessa seção são de co-autoria do autor desta tese e estão contidos na Ref. [63].

Seja $(\mathcal{Q}_i)_{i\geq 1}$ uma sequência de códigos quânticos sobre $\mathcal{H}_q$ com parâmetros $[[n_i, k_i, d_i]]_q$, respectivamente. Diz-se que $(\mathcal{Q}_i)_{i\geq 1}$ é assintoticamente boa se $\limsup_{i\to\infty} k_i/n_i > 0$ e $\limsup_{i\to\infty} d_i/n_i > 0$. Com isso, tem-se o seguinte resultado.

Teorema 3.9 *(Códigos Quânticos Assintoticamente bons de Dois-lugares) Assuma que a torre $\mathcal{T} = (F_1, F_2, \ldots)$ do corpo de funções sobre $\mathbb{F}_q$ atinge o limitante de Drinfeld-Vladut. Então, existe uma sequência $(\mathcal{Q}_i)_{i\geq 1}$ de códigos quânticos assintoticamente bons sobre $\mathcal{H}_q$ derivados dos códigos AG clássicos de dois-lugares.*

Demonstração:
Para cada F_i, considere o conjunto dos lugares racionais $P_1(i), \ldots, P_{N_i-2}(i), P_{N_i-1}(i), P_{N_i}(i)$ de F_i. Assuma que $D(i) = P_1(i) + \cdots + P_{N_i-2}(i)$, $G_1(i) = a_1(i)P_{N_i-1}(i) + a_2(i)P_{N_i}(i)$ e $G_2(i) = b_1(i)P_{N_i-1}(i) + b_2(i)P_{N_i}(i)$, com $a_1(i) \leq b_1(i)$ e $a_2(i) \leq b_2(i)$ uma vez que $2g_i - 2 < a_1(i) + a_2(i) < b_1(i) + b_2(i) < N_i - 2$. Considere $C_1(i) = C_{\mathcal{L}}[D(i), G_1(i)]$ e $C_2(i) = C_{\mathcal{L}}[D(i), G_2(i)]$ códigos AG de dois-lugares sobre $\mathbb{F}_q$ correspondendo a $G_1(i)$ e $G_2(i)$, respectivamente; assim $C_1(i) \subset C_2(i)$. O código $C_1(i)$ tem parâmetros $[N_i - 2, a_1(i) + a_2(i) - g_i + 1, d_1(i)]_q$, com $d_1(i) \geq N_i - 2 - (a_1(i) + a_2(i))$ e o código $C_2(i)$ tem parâmetros $[N_i - 2, b_1(i) + b_2(i) - g_i + 1, d_2(i)]_q$, com $d_2(i) \geq N_i - 2 - (b_1(i) + b_2(i))$. O correspondente código quântico tem parâmetros $[[N_i - 2, K_i = b_1(i) + b_2(i) - (a_1(i) + a_2(i)), D_i]]_q$, tendo $D_i \geq \min\{N_i - 2 - (b_1(i) + b_2(i)), a_1(i) + a_2(i) - (2g_i - 2)\}$. Sabe-se que K_i assume todos os valores de 1 a $N_i - 2g_i - 2$, i.e. $0 < K_i \leq N_i - 2g_i - 2$. Para cada um dos K_i coloca-se $b_1(i)+b_2(i) = \lfloor (N_i+2g_i+K_i-4)/2 \rfloor$; assim segue que $N_i-2-(b_1(i)+b_2(i)) \geq a_1(i)+a_2(i)-(2g_i-2)$, com $a_1(i)+a_2(i)-(2g_i-2) \geq (N_i-K_i-2g_i-1)/2$. A sequência de inteiros positivos $(K_i)_{i\geq 1}$ satisfaz $0 < \limsup_{i\to\infty} \frac{K_i}{N_i-2} \leq \limsup_{i\to\infty} N_i/(N_i-2) - \limsup_{i\to\infty} 2g_i/(N_i-2) + \limsup_{i\to\infty} - 2/(N_i-2) = 1 - 2/(\sqrt{q}-1)$, onde é usado na última igualdade o fato que $\limsup_{i\to\infty} N_i/g_i = \sqrt{q} - 1$. Para cada $0 < c < 1 - 2/(\sqrt{q}-1)$, pode-se escolher convenientes valores de K_i tais que $\lim_{i\to\infty} K_i/N_i = c$. Assim, $\limsup_{i\to\infty} K_i/(N_i - 2) = c > 0$. Além disso, tem-se que $\limsup_{i\to\infty}(N_i - K_i - 2g_i - 1)/2(N_i - 2) = 1/2\left[1 - 2/(\sqrt{q}-1) - c\right] > 0$. Consequentemente, existe uma sequência $(\mathcal{Q}_i)_{i\geq 1}$ de códigos quânticos assintoticamente bons sobre $\mathcal{H}_q$. ∎

Teorema 3.10 *(Códigos Quânticos Assintoticamente Bons de t-lugares) Assuma que a torre $\mathcal{T} = (F_1, F_2, \ldots)$ de corpos de funções sobre $\mathbb{F}_q$ atinge o limitante de Drinfeld-Vladut. Então,*

existe uma sequência $(\mathcal{Q}_i)_{i\geq 1}$ de códigos quânticos assintoticamente bons sobre $\mathcal{H}_q$ derivados de códigos AG de t-lugares.

Demonstração: Assuma a mesma notação da demonstração do Teorema 3.9. Para cada F_i, considere o conjunto dos lugares racionais $P_1(i), \ldots, P_{n_i}(i), P_{n_i+1}(i), \ldots, P_{n_i+t}(i)$ de F_i, com $N_i = n_i + t$. Adote $D(i) = P_1(i) + \cdots + P_{n_i}(i)$, $G_1(i) = a_1(i)P_{n_i+1}(i) + \cdots + a_t(i)P_{n_i+t}(i)$ e $G_2(i) = b_1(i)P_{n_i+1}(i) + \cdots + b_t(i)P_{n_i+t}(i)$, com $a_j(i) \leq b_j(i)$ para todo $j = 1, \ldots, t$ com $2g_i - 2 < \sum_{j=1}^{t} a_j(i) < \sum_{j=1}^{t} b_j(i) < N_i - t$. Considere o seguinte código AG de t-lugares $C_1(i) = C_{\mathcal{L}}[D(i), G_1(i)]$ e $C_2(i) = C_{\mathcal{L}}[D(i), G_2(i)]$. Segue que $C_1(i) \subset C_2(i)$, e $C_1(i)$ tem parâmetros $\left[N_i - t, \sum_{j=1}^{t} a_j(i) - g_i + 1, d_1(i)\right]_q$, com $d_1(i) \geq N_i - t - \sum_{j=1}^{t} a_j(i)$, e $C_2(i)$ tem parâmetros $\left[N_i - t, \sum_{j=1}^{t} b_j(i) - g_i + 1, d_2(i)\right]_q$, com $d_2(i) \geq N_i - t - \sum_{j=1}^{t} b_j(i)$.

Colocando $\sum_{j=1}^{t} b_j(i) = \lfloor (N_i + 2g_i + K_i - t - 2)/2 \rfloor$ e proceguindo da mesma forma que na demonstração do Teorema 3.9, o resultado segue. ∎

Seja q uma potência de um número inteiro primo. Adote que $\mathcal{C}$ é um código linear $[n, k, d]_{q^m}$ e B uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Assuma também que $B^{\perp}$ é uma base dual de B. Seja $C^{\perp}$ o dual euclidiano de C. Então tem-se que $[B(C)]^{\perp} = B^{\perp}(C^{\perp})$ (veja os trabalhos de Grassl, *et al.* e La Guardia [21, 83]).

Teorema 3.11 *Para qualquer inteiro primo p, existe uma sequência $(\mathcal{Q}_i)_{i\geq 1}$ de códigos quânticos assintoticamente bons sobre $\mathcal{H}_p$.*

Demonstração: Seja $q^2 = p^{2r}$ com p primo. Considere a torre de corpos de funções $\mathcal{T} = (F_1, F_2, \ldots)$ sobre $\mathbb{F}_{q^2}$, mostrada em no trabalho de Garcia e Stichtenoth [73], definida por $F_t = \mathbb{F}_{q^2}(x_1, \ldots, x_t)$, com $x_{i+1}^q + x_{i+1} = x_i^q/(x_i^{q-1} + 1)$, para $i = 1, \ldots t-1$. Essa torre atinge o limitante de Drinfeld-Vladut. Expandindo os códigos $C_1(i)$ e $C_2(i)$ mostrados na demonstração do Teorema 3.9 com respeito à base B de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_p$ obtêm-se, desta forma, os códigos $B(C_1(i))$ e $B(C_2(i))$, ambos sobre $\mathbb{F}_p$, com parâmetros $[2r(N_i-2), 2r(a_1(i)+a_2(i)-g_i+1), \geq d_1^*(i)]_p$, tendo $d_1^*(i) \geq d_1(i) \geq N_i - 2 - (a_1(i) + a_2(i))$, e $[2r(N_i - 2), 2r(b_1(i) + b_2(i) - g_i + 1), d_2^*(i)]_p$, tendo $d_2^*(i) \geq d_2(i) \geq N_i - 2 - (b_1(i) + b_2(i))$, respectivamente. Por $B(C_1(i)) \subset B(C_2(i))$, é possível aplicar a construção CSS sobre esses códigos, obtendo-se, assim, um código quântico $[[2r(N_i - 2), 2rK_i, D_i]]_p$, com $D_i \geq \min\{N_i - 2 - (b_1(i) + b_2(i)), a_1(i) + a_2(i) - (2g_i - 2)\}$ (note que como $[B(C_1(i))]^{\perp} = B^{\perp}(C_1(i))^{\perp}$, então a distância mínima de $[B(C_1(i))]^{\perp}$ é pelo menos $a_1(i) + a_2(i) - (2g_i - 2)$). Procedendo de forma similar à demonstração do Teorema 3.9 obtêm-se $N_i - 2 - (b_1(i) + b_2(i)) \geq a_1(i) + a_2(i) - (2g_i - 2) \geq (N_i - K_i - 2g_i + 1)/2$. Consequentemente, é obtido $\limsup_{i\to\infty} 2rK_i/2r(N_i - 2) > 0$ e $\limsup_{i\to\infty}(N_i - K_i - 2g_i + 1)/4r(N_i - 2) = 1/4r\,[1 - 2/(p^r - 1) - c] > 0$, como desejado.

∎

Observação 3.3 *Fazendo uma comparação da construção apresentada com a literatura, é possível observar alguns fatos. Os resultados dos Teoremas 3.9 e 3.11 são similares às contidas nos trabalhos de Chen,* et al. *e Kim e Walker [25, 81], entretanto, tem-se que o caso aqui apresentado utiliza códigos AG de t-lugares ($t \geq 2$), enquanto que nos referidos trabalhos, os autores utilizam códigos AG de apenas um lugar. Outra diferença é que nas Refs. [25, 81] os autores utilizam códigos concatenados para obter códigos sobre os corpos de base e aqui é usado expansão de códigos.*

CAPÍTULO 4

Códigos Quânticos Assistidos por Emaranhamento

A construção de códigos sobre o paradigma quântico fornece ferramentas inexistentes para o caso clássico. Uma dessas ferramentas é o emaranhamento. Como foi mostrado no capítulo anterior, é possível criar códigos quânticos que não utilizem explicitamente emaranhamento nos processos de codificação e decodificação. Entretanto, como é exposto neste capítulo, esta ferramenta fornece um método de criação de códigos quânticos a partir de códigos clássicos sem a existência da restrição de que um dos códigos esteja contido no outro. Tais códigos são denotados por códigos quânticos assistidos por emaranhamentos. Isso faz com que qualquer código clássico possa ser utilizado no processo de construção, o que implica em maior variedade de parâmetros.

É apresentada neste capítulo uma motivação sobre a construção via estabilizadores dos códigos quânticos assistidos por emaranhamento. Em seguida, uma caracterização dos parâmetros dos códigos quânticos por meio dos parâmetros dos códigos clássicos é feita, além da apresentação do limitante de Singleton quântico para códigos quânticos assistidos por emaranhamento. Ademais, é detalhada a construção de várias famílias de códigos quânticos assistidos por emaranhamento construídas a partir de duas classes de códigos, códigos cíclicos e códigos algébrico-geométricos. Os códigos contruídos utilizando códigos cíclicos são descritos na Seção 4.2 e podem ser encontrados na Ref. [65]. A construção de códigos quânticos assistidos por emaranhamento a partir de códigos algébrico-geométricos é feita na Seção 4.3 e podem ser encontrados na Ref. [64]. Ambas publicações têm o autor desta tese como um dos co-autores. Como é mostrado nas referidas seções, várias famílias ótimas são construídas, tanto pela utilização de códigos cíclicos quanto algébrico-geométricos, quando comparadas com o limitante de Singleton. Por fim, na Seção 4.4, códigos quânticos assistidos por emaranhamento assintoticamente bons são criados e uma análise dos parâmetros dos mesmos por meio do limitante de Gilbert-Varshamov é feita. Esse resultado também está contigo na Ref. [64].

4.1 – Formalismo Estabilizador para Códigos Quânticos Assistidos por Emaranhamento

Como a formulação matemática via estabilizadores para códigos quânticos assistidos por emaranhamentos é similar à formulação do Capítulo 3, não atentaremos ao desenvolvimento desta descrição. O que será feito é o desenvolvimento de uma motivação que justifique a caracterização dos parâmetros dos códigos quânticos. Para o leitor que deseje ver a descrição mais detalhada do formalismo estabilizador para estes códigos, recomendamos as Refs. [39, 41, 42, 84].

Suponha que se queira construir códigos quânticos estabilizadores a partir do grupo $\mathcal{S}$ gerado pelos elementos

$$S_1 = Z \otimes X \otimes Z \otimes I, \tag{4.1}$$
$$S_2 = Z \otimes Z \otimes I \otimes Z, \tag{4.2}$$
$$S_3 = Y \otimes X \otimes X \otimes Z, \tag{4.3}$$
$$S_4 = Z \otimes Y \otimes Y \otimes X. \tag{4.4}$$

Como pode ser notado, os dois primeiros geradores anticomutam, ou seja, o grupo $\mathcal{S}$ não é comutativo e, consequentemente, não é possível usar a construção do capítulo anterior. Mediante uma trasformação unitária, é possível transformar S_1, S_2, S_3 e S_4 no seguinte conjunto de geradores

$$\tilde{S}_1 = X \otimes I \otimes I \otimes I, \tag{4.5}$$
$$\tilde{S}_2 = Z \otimes I \otimes I \otimes I, \tag{4.6}$$
$$\tilde{S}_3 = I \otimes Z \otimes I \otimes I, \tag{4.7}$$
$$\tilde{S}_4 = I \otimes I \otimes Z \otimes I. \tag{4.8}$$

Assim sendo, $\mathcal{S} = \langle S_1, S_2, S_3, S_4 \rangle \approx \langle \tilde{S}_1, \tilde{S}_2, \tilde{S}_3, \tilde{S}_4 \rangle = \tilde{\mathcal{S}}$ em termos de transformações unitárias. Uma passo chave é feito agora para transformar $\tilde{\mathcal{S}}$ em um grupo abeliano. Esse passo corresponde à adesão de um novo elemento em cada um dos geradores de forma que todos eles comutem. Para o caso específico, o novo grupo de geradores depois dessa adesão será

$$\hat{S}_1 = X \otimes I \otimes I \otimes I \otimes \boldsymbol{X}, \tag{4.9}$$
$$\hat{S}_2 = Z \otimes I \otimes I \otimes I \otimes \boldsymbol{Z}, \tag{4.10}$$
$$\hat{S}_3 = I \otimes Z \otimes I \otimes I \otimes \boldsymbol{I}, \tag{4.11}$$
$$\hat{S}_4 = I \otimes I \otimes Z \otimes I \otimes \boldsymbol{I}. \tag{4.12}$$

Agora, o grupo $\hat{\mathcal{S}} = \langle \hat{S}_1, \hat{S}_2, \hat{S}_3, \hat{S}_4 \rangle$ é abeliano. Um autoestado para o estabilizador $\hat{\mathcal{S}}$ é o seguinte

$$|\mathbf{c}\rangle = \left|\Phi^+\right\rangle^{AB} |00\rangle^A |\psi\rangle^A, \tag{4.13}$$

em que $\left|\Phi^+\right\rangle^{AB} := \frac{|00\rangle^{AB} + |11\rangle^{AB}}{\sqrt{2}}$ é um estado maximamente emaranhado de Bell compartilhado entre o transmissor (representado pelo subíndice A) e o receptor (representado pelo subíndice B), $|00\rangle^A$ são *zero paddings* utilizados no processo de codificação e $|\psi\rangle^A$ são os qubits de informação que o transmissor deseja enviar. Efetuando a transformação unitária inversa para obter os estabilizadores globais de $\mathcal{S}$, obtém-se o seguinte:

$$S_1 = Z \otimes X \otimes Z \otimes I \otimes \boldsymbol{X}, \tag{4.14}$$

$$S_2 = Z \otimes Z \otimes I \otimes Z \otimes \boldsymbol{Z}, \tag{4.15}$$

$$S_3 = Y \otimes X \otimes X \otimes Z \otimes \boldsymbol{I}, \tag{4.16}$$

$$S_4 = Z \otimes Y \otimes Y \otimes X \otimes \boldsymbol{I}. \tag{4.17}$$

Em resumo, suponha que se tenha o grupo $\mathcal{S}$ não abeliano com $2c$ elementos que não comutam entre si. Então, é adicionado um produto tensorial de c operadores em cada um dos geradores do grupo estabilizador de forma que o mesmo se torne, agora, abeliano. Estes c elementos adicionados correspondem ao número de pares de estados maximamente emaranhados utilizados pelo codificador.

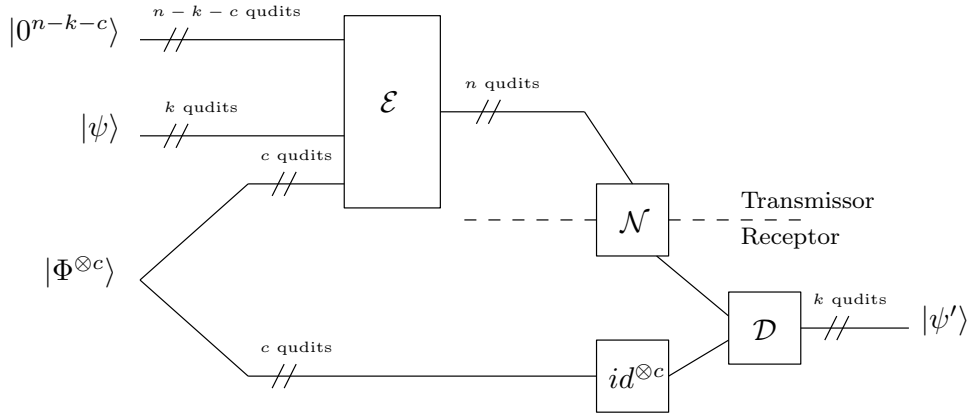


Figura 4.1 – Esquema de comunicação utilizando códigos quânticos assistidos por emaranhamento. Os elementos $\mathcal{E}$ e $\mathcal{D}$ representam os processos de codificação e o decodificação, respectivamente, $\mathcal{N}$ descreve o canal de comunicação quântico e $id^{\otimes n}$ reflete a hipótese de que não há ruído sobre os pares de estados emaranhados compartilhados entre o transmissor e o receptor.

O exemplo anterior pode ser generalizado para a seguinte construção: Seja $\mathcal{S}$ um grupo não abeliano de G_n. Pelo teorema fundamental da geometria simplética, veja a Ref. [85], é possível reescrever $\mathcal{S}$ de forma a ser particionado em dois subgrupos: o subgrupo isotrópico $\mathcal{S}_I$ e o subgrupo emaranhado $\mathcal{S}_E$. O subgrupo $\mathcal{S}_I$ é o subgrupo abeliano de $\mathcal{S}$. Os elementos do subgrupo emaranhado $\mathcal{S}_E$ vêm em pares que anticomutam mas comutam com os restantes; ou seja, suponha que $\mathcal{S}_E = \langle \overline{Z}_{a+1}, \ldots, \overline{Z}_{a+c}, \overline{X}_{a+1}, \ldots, \overline{X}_{a+c} \rangle$, então $[\overline{Z}_{a+i}, \overline{X}_{a+j}] = 0$ para

$i \neq j$, $\{\overline{Z}_{a+i}, \overline{X}_{a+i}\} = 0$, para $i, j = 1, \ldots c$, e $[\overline{X}_{a+i}, \overline{X}_{a+j}] = [\overline{Z}_{a+i}, \overline{Z}_{a+j}] = 0$ para todo i, j. Assuma que o número de geradores de $\mathcal{S}_I$ e $\mathcal{S}_E$ são $a = n - k$ e $2c$, respectivamente. Então, o código quântico assistido por emaranhamento dado pelos estados estabilizados por $\mathcal{S} = \mathcal{S}_I \cup \mathcal{S}_E$ tem parâmetros $[n, k, d; c]$, com c sendo o número de estados maximamente emaranhados inicialmente compartilhados pelo transmissor e receptor e $d = \min\{\text{wt}(E) \colon E \in C_{G_n}(\mathcal{S}) \setminus \mathcal{S}Z(G_n)\}$.

Definição 4.1 *Um código quântico $\mathcal{Q}$ é chamado de código quântico assistido por emaranhamento (QUENTA) com parâmetros $[[n, k, d; c]]_q$ se codifica k qudits lógicos em n qudits físicos usando c cópias de um estado maximamente emaranhado e pode corrigir $\lfloor (d-1)/2 \rfloor$ erros quânticos. A taxa de um código QUENTA é dada por k/n, a distância relativa por d/n e o emaranhamento relativo por c/n. Por último, um código QUENTA é chamado de maximamente emaranhado quando $c = n - k$.*

Como será mostrado na subseção a seguir, o método de construção de códigos quânticos assistidos por emaranhamento é bastante similar ao do Capítulo 3, com a diferença que, agora, não há mais a necessidade de termos um dos códigos contido no outro. Isso facilita na escolha dos códigos clássicos a serem utilizados. Porém, cria-se também uma dificuldade. O parâmetro do código relacionado com a quantidade de emaranhamento está ligado ao cálculo da dimensão da interseção entre dois códigos. Esta tarefa não é simples. Entretanto, por meio da apresentação e criação de novas ferramentas matemáticas, é possível efetuar esse cálculo sobre códigos cíclicos e algébrico-geométricos.

4.1.1 – Construção CSS e Limitante de Singleton

O formalismo estabilizador para códigos QUENTA fornece um método de criação de códigos via códigos clássicos. Wilde e Brun foram os primeiros a desenvolver este formalismo para códigos QUENTA que utilizem qubits [41]. A generalização para qudits foi apresentada somente recentemente em um trabalho de Galindo, *et al.* [42]. É essa generalização que é apresentada a seguir. Ela fornece dois métodos de criação de códigos QUENTA, que são denominadas de método euclidiano e método hermitiano.

Proposição 4.1 *[42, Teorema 4](Método de Construção Euclidiana) Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ dois códigos lineares sobre $\mathbb{F}_q$ com parâmetros $[n, k_1, d_1]_q$ e $[n, k_2, d_2]_q$, com matrizes de verificação de paridade H_1 e H_2, respectivamente. Então, existe um código QUENTA com parâmetros $[[n, k_1 + k_2 - n + c, d; c]]_q$, sendo $d = \min\{d_{\min}(\mathcal{C}_1 \setminus (\mathcal{C}_1 \cap \mathcal{C}_2^{\perp})), d_{\min}(\mathcal{C}_2 \setminus (\mathcal{C}_1^{\perp} \cap \mathcal{C}_2))\}$, e*

$$c = \operatorname{rank}(H_1 H_2^T) = \dim \mathcal{C}_1^{\perp} - \dim(\mathcal{C}_1^{\perp} \cap \mathcal{C}_2) \tag{4.18}$$

é o número de estados maximamente emaranhados utilizado pelo código.

Proposição 4.2 *[42, Proposição 3 e Corolário 1](Método de Construção Hermitiana) Sejam $\mathcal{C}$ um código linear sobre $\mathbb{F}_{q^2}$ com parâmetros $[n, k, d]_q$, H é a matriz de verificação de paridade de $\mathcal{C}$ e H^* a q-ésima potência da matriz transposta de H. Então, existe um código QUENTA com parâmetros $[[n, 2k - n + c, d'; c]]_q$, com $d' = d_{\min}(\mathcal{C} \setminus (\mathcal{C} \cap \mathcal{C}^{\perp_h}))$ e*

$$c = \operatorname{rank}(HH^*) = \dim \mathcal{C}^{\perp_h} - \dim(\mathcal{C}^{\perp_h} \cap \mathcal{C}) \tag{4.19}$$

é o número de estados maximamente emaranhados utilizado pelo código.

Uma medida quantitativa de qualidade para um código QUENTA é o limitante de Singleton quântico para estes códigos. Seja $[[n, k, d; c]]_q$ um código QUENTA, então o limitante de Singleton quântico é dado por [42]

$$d \leq \left\lfloor \frac{n - k + c}{2} \right\rfloor + 1. \tag{4.20}$$

A diferença entre o limitante de Singleton quântico e a distância mínina d do código é denominada de *Singleton defect* (quântico). Quando o *Singleton defect* é igual a zero (resp. um), o código é chamado de código quântico com máxima distância de separação (resp. código quântico com *almost* máxima distância de separação) e é denominado código quântico MDS (resp. código quântico *almost* MDS).

4.2 – Códigos Quânticos Assistidos por Emaranhamento Derivados de Códigos Cíclicos

Na presente seção é apresentada a construção de códigos quânticos assistidos por emaranhamento (QUENTA) a partir dos códigos cíclicos descritos anteriormente. Será aplicado os métodos de construção euclidiano e hermitiano, os quais fornecem códigos com parâmetros diferentes quando comparados sobre o mesmo corpo finito.

4.2.1 – Construção Euclidiana de Códigos Quânticos Assistidos por Emaranhamento

Uma aplicação direta de códigos cíclicos à Proposição 4.1 via conjunto de definição produz os resultados mostrados no Teorema 4.1 e Corolário 4.1.

Teorema 4.1 *Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ dois códigos cíclicos com parâmetros $[n, k_1, d_1]_q$ e $[n, k_2, d_2]_q$, respectivamente. Então, existe um código QUENTA com parâmetros $[[n, k_1 - |Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)|, \min\{d_1, d_2\}; n - k_2 - |Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)|]]_q$.*

Demonstração: Da Proposição 2.7 tem-se que $\dim(\mathcal{C}_1^{\perp} \cap \mathcal{C}_2) = n - |Z(\mathcal{C}_1^{\perp}) \cup Z(\mathcal{C}_2)| = n - |Z(\mathcal{C}_2)| - |Z(\mathcal{C}_1^{\perp})| + |Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)| = k_2 - k_1 + |Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)|$. Assim, a quantidade de emaranhamento usado pelo código QUENTA construído desses dois códigos cíclicos pode

ser calculado da Proposição 4.1, o que fornece $c = n - k_2 - |Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)|$. Substituindo este valor de c nos parâmetros do código QUENTA da Proposição 4.1, obtemos um código QUENTA com parâmetros $[[n, k_1 - |Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)|, \min\{d_1, d_2\}; n - k_2 - |Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)|]]_q$. ■

Corolário 4.1 *Seja $\mathcal{C}$ um código cíclico LCD com parâmetros $[n, k, d]_q$. Então existe um código QUENTA maximamente emaranhado com parâmetros $[[n, k, d; n - k]]_q$. Em particular, se $\mathcal{C}$ é MDS, então o código QUENTA derivado dele também será.*

Demonstração: Seja $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}$ no Teorema 4.1. Uma vez que $\mathcal{C}$ é LCD, então $|Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)| = 0$. Do Teorema 4.1 vemos que existe um código QUENTA com parâmetros $[[n, k, d; n - k]]_q$. ■

Teorema 4.2 *Sejam $\mathcal{C}_1 = RS_{k_1}(n, b_1)$ e $\mathcal{C}_2 = RS_{k_2}(n, b_2)$ dois códigos Reed-Solomon sobre $\mathbb{F}_q$ com $0 \leq b_1 \leq k_1$, $b_2 \geq 0$, e $b_1 + b_2 \leq k_1 + 1$. Então, tem-se dois possíveis casos:*

1. *Para $k_1 - b_1 \geq b_2$, existe um código QUENTA com parâmetros*

$$[[n, b_1 + b_2 - 1, n - \min\{k_1, k_2\} + 1; n + b_1 + b_2 - k_1 - k_2 - 1]]_q;$$

2. *Para $k_1 - b_1 < b_2$, existe um código QUENTA com parâmetros*

$$[[n, k_1, n - \min\{k_1, k_2\} + 1; n - k_2]]_q.$$

Demonstração: Pelo Corolário 2.1, tem-se que $Z(\mathcal{C}_1^{\perp}) = \{n - b_1 + 1, n - b + 2, \ldots, n - b_1 + k_1\}$. Primeiramente note que a restrição $b_1 + b_2 \leq k_1 + 1$ implica que o primeiro elemento no conjunto de definição de $Z(\mathcal{C}_1^{\perp})$ vem depois do último elemento em $Z(\mathcal{C}_2)$. Uma vez que $0 \leq b_1 \leq k_1$, temos que $n - b_1 + k_1 \geq n$, o que implica no conjunto de definição para $\mathcal{C}_1^{\perp}$ ser igual a $Z(\mathcal{C}_1^{\perp}) = \{n - b_1 + 1, n - b + 2, \ldots, n - 1, 0, 1, \ldots, k_1 - b_1\}$. Assim, $Z(\mathcal{C}_1^{\perp})$ intersecta com $Z(\mathcal{C}_2)$ se, e somente se, $k_1 - b_1 \geq b_2$. No caso que intersecta, a interseção é igual a $Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2) = k_1 - (b_1 + b_2) + 1$. As demais afirmações são obtidas usando o Teorema 4.1. ■

Corolário 4.2 *Seja $\mathcal{C} = RS_k(n, b)$ um código Reed-Solomon sobre $\mathbb{F}_q$ com $0 < b \leq (k + 1)/2$ e $0 < k < n \leq q$. Então, existe um código QUENTA MDS com parâmetros $[[n, 2b - 1, n - k + 1; n + 2b - 2k - 1]]_q$. Em particular, para $b = (k + 1)/2$, existe um código QUENTA MDS maximamente emaranhado.*

Demonstração: Sejam $\mathcal{C}_1 = \mathcal{C}_2 = RS_k(n, b)$ no Teorema 4.2. Assumindo que $0 \leq b < (k + 1)/2$, temos que o código clássico atende ao primeiro caso do Teorema 4.2; e para

$b = (k+1)/2$, o código atende ao segundo caso do Teorema 4.2. Consequentemente, substituindo os valores de k_1, k_2 e b_1, b_2 por k e b, respectivamente, o resultado segue. ■

De forma similar aos resultados para códigos Reed-Solomon, podemos usar códigos BCH para construir códigos QUENTA. O ganho em utilizar códigos BCH é a obtenção de um código que não é mais limitado pela cardinalidade do corpo finito utilizado. Entretanto, criar códigos clássicos ou quânticos a partir de códigos BCH que sejam MDS é uma tarefa árdua. Os resultados que se seguem baseiam-se na utilização de dois códigos BCH, os quais são descritos pelos seus conjuntos de definição, para construir códigos QUENTA. Além disso, é mostrado que tal construção pode ser utilizada para obter códigos QUENTA maximamente emaranhados. Para tal objetivo, será mostrado algumas propriedades atrativas das classes laterais ciclotômicas quando $n = q^2 - 1$.

Lema 4.1 *Seja $n = q^2 - 1$ com $q > 2$. Então, a classe lateral ciclotômicas q-ário $\mathbb{C}_0$ tem apenas um elemento e $\mathbb{C}_i = \{i, iq\}$ para qualquer $1 \leq i \leq q-1$.*

Demonstração: A primeira afirmação é trivial. Para a segunda, note que $iq^2 \equiv i \mod (q^2-1)$. Assim, o único elemento em $\mathbb{C}_i$ são i e iq, para $1 \leq i \leq q-1$. ■

Do Lema 4.1, podemos construir códigos QUENTA com comprimento $n = q^2 - 1$. Veja o Teorema 4.3.

Teorema 4.3 *Seja $n = q^2 - 1$ com $q > 2$. Assuma que a, b são inteiros tais que $0 \leq a \leq q-1$ e $1 \leq b \leq q$. Então existe um código QUENTA com parâmetros*

- $[[n, 2(q-b)-1, b+1; 2(q-a-1)]]_q$, *se $a \geq q-b$ e $b < q$;*
- $[[n, 2a+1, b+1; 2b - \lfloor \frac{b}{q} \rfloor]]_q$, *se $a < q-b$.*

Demonstração: Primeiramente, assuma que $\mathcal{C}_1^{\perp}$ tem conjunto de definição dado por $Z(\mathcal{C}_1^{\perp}) = \cup_{i=0}^{a}\mathbb{C}_i$ e o conjunto de definição de $\mathcal{C}_2$ é igual a $Z(\mathcal{C}_2) = \cup_{i=1}^{b}\mathbb{C}_{q-i}$. Do Lema 4.1 tem-se que $|Z(\mathcal{C}_1^{\perp})| = 2a+1$ e $|Z(\mathcal{C}_2)| = 2b - \lfloor \frac{b}{q} \rfloor$. Assim, a dimensão de $\mathcal{C}_1$ e $\mathcal{C}_2$ é igual a $k_1 = |Z(\mathcal{C}_1^{\perp})| = 2a+1$ e $k_2 = n - |Z(\mathcal{C}_2)| = n - 2b + \lfloor \frac{b}{q} \rfloor$, respectivamente. Para o cálculo de $|Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)|$, tem-se que considerar dois casos. Se $a \geq q-b$, então temos que $Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2) = \cup_{i=q-b}^{a}\mathbb{C}_i$, o qual tem cardinalidade igual a $|Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)| = (a-(q-b)+1)2 - \lfloor \frac{b}{q} \rfloor$, visto que $|\mathbb{C}_0| = 1$. Por outro lado, se $a < q-b$, então $|Z(\mathcal{C}_1^{\perp}) \cap Z(\mathcal{C}_2)| = 0$. Por último, uma vez que $a, b \leq q$ e $n = q^2 - 1$ com $q > 2$, é possível notar que $d_1 > d_2 = b+1$. Agora, aplicando esses resultados ao Teorema 4.1, temos que existe um código QUENTA com parâmetros $[[n, 2(q-b) - 1 + \lfloor \frac{b}{q} \rfloor, b+1; 2(q-a-1)]]_q$, se $a \geq q-b$, ou um código QUENTA com parâmetros $[[n, 2a+1, b+1; 2b - \lfloor \frac{b}{q} \rfloor]]_q$, caso contrário. ■

4.2.2 – Construção Hermitiana de Códigos Quânticos Assistidos por Emaranhamento

De forma similar ao que foi feito na seção anterior, é mostrado a aplicação de códigos cíclicos na construção de códigos QUENTA a partir do método de construção hermitiana da Proposição 4.2. Veja o teorema a seguir.

Teorema 4.4 *Seja $\mathcal{C}$ um código cíclico com parâmetros $[n,k,d]_{q^2}$. Então existe um código QUENTA com parâmetros $[[n, k-|Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})|, d; n-k-|Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})|]]_q$.*

Demonstração: Primeiramente, da Proposição 2.7 é possível ver que $\dim(\mathcal{C}^{\perp}\cap\mathcal{C}) = n - |Z(\mathcal{C}^{\perp})\cup Z(\mathcal{C})| = n - |Z(\mathcal{C})| - |Z(\mathcal{C}^{\perp_h})| + |Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})| = k - k + |Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})| = |Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})|$. Assim, $c = \dim(\mathcal{C}^{\perp_h}) - \dim(\mathcal{C}^{\perp}\cap\mathcal{C}) = n-k-|Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})|$. Usando um código $[n,k,d]_{q^2}$ para construir um código QUENTA via Proposição 4.2, deriva-se o código QUENTA com parâmetros $[[n, k-|Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})|, d; n-k-|Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})|]]_q$. ■

Corolário 4.3 *Seja $\mathcal{C}$ um código cíclico LCD com parâmetros $[n,k,d]_{q^2}$. Então existe um código QUENTA maximamente emaranhado com parâmetros $[[n,k,d;n-k]]_q$.*

Demonstração: Da demonstração do Teorema 4.4, temos que $\dim(\mathcal{C}^{\perp_h}\cap\mathcal{C}) = |Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})|$. Uma vez que $\mathcal{C}$ é LCD, $|Z(\mathcal{C}^{\perp_h})\cap Z(\mathcal{C})| = 0$ e o resultado segue do Teorema 4.4. ■

Diferentemente da construção euclidiana de códigos QUENTA usando código cíclicos, a construção hermitiana pode ser mais delicada de se trabalhar, até mesmo para códigos Reed-Solomon. Mesmo assim, será mostrado que é possível construir códigos QUENTA utilizando códigos Reed-Solomon e alguns códigos cíclicos, uma vez que seus parâmetros atendam certas restrições.

Teorema 4.5 *Seja q uma potência de um número primo e assuma que $\mathcal{C} = RS_k(n,0)$ é um código Reed-Solomon sobre $\mathbb{F}_{q^2}$ com $k = qt + r < q^2$, em que $t \geq 1$, $0 \leq r \leq q-1$, e $n = q^2$. Então tem-se o seguinte:*

- *Se $t \geq q - r - 1$, então existe um código QUENTA MDS com parâmetros*

$$[[q^2, (t+1)^2 - 2(q-r) + 1, q(q-t) - r + 1; (q-t-1)^2 + 1]]_q.$$

- *Se $t < q - r - 1$, então existe um código QUENTA MDS com parâmetros*

$$[[q^2, t^2 - 1, q(q-t) - r + 1; (q-t)^2 - 2r - 1)]]_q.$$

Demonstração: Uma vez que $\mathcal{C} = RS_k(n,0)$, temos que $Z(\mathcal{C}) = \{0,1,2,\ldots,n-k-1\}$. Da demonstração do Teorema 2.6, também temos que $Z(\mathcal{C}^{\perp_h}) = qZ(\mathcal{C}^{\perp}) = \{q, 2q, \ldots, kq\}$. De $n = q^2$ e $k = qt + r$, é possível reescrever estes dois conjuntos de definição como

$Z(\mathcal{C}) = \{qi+j | 0 \leq i \leq q-t-2, 0 \leq j \leq q-1\} \cup \{(q-t-1)q+j | 0 \leq j \leq q-r-2\}$ e $Z(\mathcal{C}^{\perp_h}) = \{qi+j | 0 \leq i \leq q-1, 0 \leq j \leq t-1\} \cup \{qi+t | 0 \leq i \leq r\}$. Usando esta descrição, calculamos $|Z(\mathcal{C}) \cap Z(\mathcal{C}^{\perp_h})|$. Para fazer isso, temos que considerar dois casos separadamente, $t \geq q-r-1$ and $t < q-r-1$. Para o primeiro caso, a interseção é dada pelo seguinte conjunto $Z(\mathcal{C}) \cap Z(\mathcal{C}^{\perp_h}) = \{qi+j | 0 \leq i \leq q-t-2, 0 \leq j \leq t\} \cup \{(q-t-1)q+j | 0 \leq j \leq q-r-2\}$. Assim, $|Z(\mathcal{C}) \cap Z(\mathcal{C}^{\perp_h})| = (q-t-1)(t+1)+q-r-1$. Similarmente para o caso $t < q-r-1$, temos que $Z(\mathcal{C}) \cap Z(\mathcal{C}^{\perp_h}) = \{qi+j | 0 \leq i \leq q-t-1, 0 \leq j \leq t-1\} \cup \{qi+t | 0 \leq i \leq r\}$, o qual implica em $|Z(\mathcal{C}) \cap Z(\mathcal{C}^{\perp_h})| = (q-t)t+r+1$. Aplicando os cálculos anteriores e usando o fato que C tem parâmetros $[q^2, k, q^2-k+1]_{q^2}$ no Teorema 4.4, tem-se que existe um código QUENTA com parâmetros

- $[[q^2, (t+1)^2 - 2(q-r)+1, q(q-t)-r+1; (q-t-1)^2+1]]_q$, para $t \geq q-r-1$; e
- $[[q^2, t^2-1, q(q-t)-r+1; (q-t)^2-2r-1)]]_q$, para $t < q-r-1$.

■

Teorema 4.6 *Seja $n = q^4 - 1$ e $q \geq 3$ uma potência de um número primo. Então existe um código QUENTA com parâmetros $[[n, n-4(a-1)-3, d \geq a+1; 1]]_q$, em que $2 \leq a \leq q^2-1$.*

Demonstração: Seja $\mathcal{C}_a$ um código cíclico com conjunto de definição $Z(\mathcal{C}_a) = \mathbb{C}_0 \cup \mathbb{C}_{q^2+1} \cup (\cup_{i=2}^{a} \mathbb{C}_{q^2+a})$, para $2 \leq a \leq q^2-1$. Da Referência [86], tem-se que $\mathbb{C}_{q^2+1} = \{q^2+1\}$ e $\mathbb{C}_{q^2+a} = \{q^2+a, 1+aq^2\}$. É trivial mostrar que $\mathbb{C}_0 = \{0\}$. De $-qZ(\mathcal{C}_a) \cap Z(\mathcal{C}_a) = \mathbb{C}_0$ [86], podemos ver que $Z(\mathcal{C}_a^{\perp_h}) \cap Z(\mathcal{C}_a) = Z(\mathcal{C}_a) \setminus \mathbb{C}_0$. Consequentemente, $|Z(\mathcal{C}_a^{\perp_h}) \cap Z(\mathcal{C}_a)| = 2(a-1)+1$. Da hipótese do conjunto de definição, a dimensão e distância mínima do código linear são $k = n-2(a-1)-2$ e $d \geq a+1$, respectivamente. Assim, aplicando estas quantidades ao Teorema 4.4, temos que existe um código QUENTA com parâmetros $[[n, n-4(a-1)-3, d \geq a+1; 1]]_q$. ■

Dois fatos importantes podem ser ditos sobre o Teorema 4.6. Comparando os limitantes dados pela distância mínima para os códigos criados e o limitante de Singleton para códigos QUENTA da Eq. 4.20, vemos que a diferença entre estes dois valores é igual a $a-1$. Consequentemente, para valores de a pequenos, tais como $a = 2$ ou $a = 3$, os códigos QUENTA têm distância mínima próxima da ótima; e.g., se $a = 2$ (ou $a = 3$), a família de códigos QUENTA é *almost* MDS (ou *almost near* MDS). O segundo ponto é que os códigos no Teorema 4.6 podem ser vistos como uma generalização dos resultados apresentados por Qian e Zhang [87].

No teorema a seguir é feito o uso de códigos cíclicos LCD à construção de códigos QUENTA maximamente emaranhados.

Teorema 4.7 *Seja q uma potência de número primo, $m \geq 2$ e $2 \leq \delta \leq q^{2\lceil \frac{m}{2} \rceil}+1$. Então,*

1. *Para m ímpar, $\kappa = q^{2m} - 2 - 2(\delta - 1 - \lfloor \frac{\delta-1}{q^2} \rfloor)m$ e $1 \leq u \leq q-1$, tem-se que existe um código QUENTA maximamente emaranhado com parâmetros $[[q^{2m}-1, k, d \geq \delta + 1 + \lfloor \frac{\delta-1}{q} \rfloor; q^{2m} - 1 - k]]_q$, em que*

$$k = \begin{cases} \kappa, & \text{se } 2 \leq \delta \leq q^m - 1; \\ \kappa + u^2 m, & \text{se } uq^m \leq \delta \leq (u+1)(q^m-1); \\ \kappa + (u^2 + 2v + 1)m, & \text{se } \delta = (u+1)(q^m-1) + v + 1 \text{ para } 0 \leq v \leq u-1; \\ \kappa + q^2 m, & \text{se } \delta = q^{m+1} \text{ or } q^{m+1} + 1. \end{cases} \tag{4.21}$$

2. *Para m par, tem-se que existe um código QUENTA maximamente emaranhado com parâmetros*

$$[[q^{2m} - 1, \kappa, d \geq \delta + 1 + \lfloor \frac{\delta - 1}{q} \rfloor; 2(\delta - 1 - \lfloor \frac{\delta - 1}{q^2} \rfloor)m + 1]]_q. \tag{4.22}$$

Demonstração: Li [88] mostrou que existem códigos cíclicos LCD com parâmetros $[q^{2m} - 1, k, \delta + 1 + \lfloor \frac{\delta-1}{q} \rfloor]_{q^2}$, em que k possui a mesma faixa de valores que os das Eqs. 4.21 e 4.22 para m ímpar e par, respectivamente. Assim, aplicando estes códigos LCD ao Corolário 4.3 obtemos os códigos QUENTA mencionados. ■

4.2.3 – Exemplos

É apresentado na Tabela 4.1 alguns códigos QUENTA MDS obtidos dos Teoremas 4.2 e 4.5. Os códigos na primeira coluna são obtidos da construção euclidiana e os da segunda da construção hermitiana. Como pode ser visto, os os parâmetros dos códigos exibidos na segunda coluna têm comprimentos maiores quando comparados sobre o mesmo corpo finito. Assim sendo, eles podem ser usados em aplicações em que o sistema quântico não possui muitos graus de liberdade. Por outro lado, os parâmetros dos códigos exibidos na primeira coluna podem atingir maior diversidade de valores em comparação à construção hermitiana. Consequentemente, essas duas classes de códigos QUENTA são sutis a aplicações específicas fazendo com que sua construção seja de motivação direta.

Na seção anterior foi apresentado uma família de códigos QUENTA a partir de códigos BCH, veja o Teorema 4.3. Alguns exemplos numéricos destes códigos são mostrados na Tabela 4.2. Como pode ser visto na Tabela 1 da Referência [89] (e as referencias continas neste trabalho), os códigos QUENTA construídos no Teorema 4.3 têm parâmetros novos quando comparados com os códigos QUENTA da literatura. Uma característica presente nos códigos do Teorema 4.3 que não está presente nos da literatura é que eles foram construídos com o uso de dois códigos BCH ao invés de apenas um, o que é tradicionalmente encontrado na literatura. Esta propriedade fornece uma maior faixa de parâmetros possíveis quando comparado com os da literatura. Veja a Tabela 4.2 para alguns exemplos numéricos.

Tabela 4.1 – Códigos QUENTA MDS maximamente emaranhados derivados de códigos Reed-Solomon

Novos códigos QUENTA – Corolário 4.2 $[[n, 2b-1, n-k+1; n+2b-2k-1]]_q$ $0 < b \leq (k+1)/2$ e $0 < k < n \leq q$	Novos códigos QUENTA – Teorema 4.5 $[[q^2, t^2-1, q(q-t)-r+1; (q-t)^2-2r-1)]]_q$ $qt + r < q^2$, em que $1 \leq t < q-r-1$ e $0 \leq r \leq q-1$
Exemplos	
$[[3, 1, 3; 2]]_3$	$[[16, 3, 9; 3]]_4$
$[[4, 3, 2; 1]]_4$	$[[64, 35, 17; 3]]_8$
$[[7, 3, 5; 4]]_7$	$[[64, 15, 31; 11]]_8$
$[[8, 5, 4; 3]]_8$	$[[256, 196, 33; 3]]_{16}$
$[[11, 9, 3; 2]]_{11}$	$[[256, 120, 78; 18]]_{16}$
$[[13, 9, 5; 4]]_{13}$	$[[1024, 784, 129; 15]]_{32}$
$[[16, 13, 3; 2]]_{16}$	$[[1024, 624, 220; 38]]_{32}$

Tabela 4.2 – Códigos QUENTA criados de códigos BCH

Novos códigos QUENTA – Teorema 4.3 $[[q^2-1, 2a+1, b+1; 2b-\lfloor \frac{b}{q} \rfloor]]_q$ $1 \leq b \leq q$ e $0 \leq a < q-b$
Exemplos
$[[15, 5, 2; 2]]_4$
$[[48, 9, 3; 4]]_7$
$[[63, 7, 5; 8]]_8$
$[[80, 13, 3; 4]]_9$
$[[255, 19, 7; 12]]_{16}$

Os códigos QUENTA remanescentes a serem apresentados são os derivados de códigos cíclicos que não são nem Reed-Solomon e nem BCH. Duas tais famílias foram criadas a partir da construção hermitiana. Alguns exemplos de parâmetros que estes códigos podem atingir estão presentes na Tabela 4.3. Os códigos na primeira coluna são *almost* MDS ou *almost near* MDS; i.e., o *Singleton defect*, o qual é dado pela diferença entre o limitante de Singleton para códigos QUENTA mostrado na Eq. 4.20 e o limitante inferior para a distância mínima do código, é igual a uma ou duas unidades. Por fim, é apresentado na segunda coluna da Tabela 4.3 alguns códigos do Teorema 4.7. Todos os códigos no Teorema 4.7 são maximamente emaranhados. Assim, eles podem ser usados para se atingir o limitante hashing [36]. Tendo comprimento proporcional ao um potência superior a dois da cardinalidade do corpo finito, é esperado atingir baixa taxas de erros usando estes códigos. Comparando-os com os presentes na literatura [48, 90–92], nota-se que eles são novos.

Tabela 4.3 – Códigos QUENTA derivados de códigos cíclicos via construção hermitiana

Novos códigos QUENTA – Teorema 4.6	Novos códigos QUENTA – Teorema 4.7
Exemplos	
$[[80, 73, 3; 1]]_3$	$[[80, 42, 14; 38]]_3$
$[[80, 69, 4; 1]]_3$	$[[80, 50, 10; 30]]_3$
$[[255, 248, 3; 1]]_4$	$[[255, 193, 20; 62]]_4$
$[[255, 244, 4; 1]]_4$	$[[255, 237, 7; 18]]_4$

4.3 – Códigos Quânticos Assistidos por Emaranhamento Derivados de Códigos Algébrico-Geométricos

4.3.1 – Construção Euclidiana de Códigos Quânticos Assistidos por Emaranhamento

Na Proposição 4.1, a conexão entre o emaranhamento utilizado em códigos QUENTA e a dimensão da interseção entre dois códigos clássicos foi mostrado. Entretando, o cálculo desta interseção pode ser complexo em alguns casos, mas como será mostrado no Teorema 4.8, é possível obtê-lo através da utilização da Proposição 2.14.

Teorema 4.8 *Seja $P_1, \ldots, P_n$ lugares racionais dois-a-dois distintos de $F/\mathbb{F}_q$ e $D = P_1 + \cdots + P_n$. Escolha divisores G_1, G_2 de $F/\mathbb{F}_q$ tais que $\mathrm{supp}(G_i) \cap supp(D) = \varnothing$ e $2g - 2 < \deg(G_i) < n$, para $i = 1, 2$. Sejam $\mathcal{C}_1 = C_{\mathcal{L}}(D, G_1)$ e $\mathcal{C}_2 = C_{\mathcal{L}}(D, G_2)$. Se $\deg(G_1^{\perp} \cup G_2) < n$, então existe um código QUENTA com parâmetros $[[n, \deg(G_1 + G_2) - 2g + 2 - n + c, d; c]]_q$, em que $d \geq n - \max\{\deg(G_1), \deg(G_2)\}$ e $c = n + g - 1 - \deg(G_1) - \ell(G_1^{\perp} \cap G_2)$.*

Demonstração: Primeiramente, note que os parâmetros dos códigos AG $C_{\mathcal{L}}(D, G_1)$ e $C_{\mathcal{L}}(D, G_2)$ são $[n, \deg(G_1) - g + 1, d_1 \geq n - \deg(G_1)]_q$ e $[n, \deg(G_2) - g + 1, d_2 \geq n - \deg(G_2)]_q$, respectivamente, e a dimensão do dual euclidiano de $C_{\mathcal{L}}(D, G_1)$ é $n + g - 1 - \deg(G_1)$, pela Proposição 2.5. Da Proposição 2.14 tem-se que $\dim(\mathcal{C}_1^{\perp} \cap \mathcal{C}_2)) = \ell(G_1^{\perp} \cap G_2)$. Consequentemente, usando a Proposição 4.1 obtemos os parâmetros mencionados para o código QUENTA. ■

Corolário 4.4 *Seja $P_1, \ldots, P_n$ lugares racionais dois-a-dois distintos de $F/\mathbb{F}_q$ e $D = P_1 + \cdots + P_n$. Escolha divisores G_1, G_2 de $F/\mathbb{F}_q$ tais que $\mathrm{supp}(G_i) \cap \mathrm{supp(D)} = \varnothing$ e $2g - 2 < \deg(G_i) < n$, para $i = 1, 2$. Se $\deg(G_1^{\perp} \cup G_2) < n$ e $\deg(G_1^{\perp} \cap G_2) < 0$, então existe um código QUENTA com parâmetros $[[n, \deg(G_2) - g + 1, d; c]]_q$, em que $d \geq n - \max\{\deg(G_1), \deg(G_2)\}$ e $c = n + g - 1 - \deg(G_1)$. Em particular, se $G_1 = G_2 = G$, então existe um código QUENTA com parâmetros $[[n, \deg(G) - g + 1, d; n + g - 1 - \deg(G)]]_q$, em que $d \geq n - \deg(G)$.*

O Teorema 4.8 e seu corolário fornecem um meio para a utilização de códigos AG derivados de qualquer corpo de funções na construção de códigos QUENTA. Em particular,

é possível utilizar códigos AG para construir códigos quânticos MDS e famílias de códigos quânticos assintoticamente boas. A primeira descrição explícita de família de códigos QUENTA construídos nesta seção é mostrado a seguir. O corpo de funções racionais $\mathbb{F}_q(z)/\mathbb{F}_q$ é usado para derivar a família construída.

Teorema 4.9 *Seja q um potência de um número primo. Considere que a_1, a_2, b_1, b_2 são inteiros positivos tais que $b_1 \leq a_2$ e $b_2 \leq q-2-a_2$, com $a_1+a_2 < q-1$ e $b_1+b_2 < q-1$; então, tem-se o seguinte:*

- *Se $b_2 \geq a_1+1$, então existem códigos QUENTA com parâmetros*

$$[[q-1, a_1+b_1-1, \geq q-1-\max\{a_1+a_2, b_1+b_2\}; q-2-(a_2+b_2)]]_q.$$

- *Se $b_2 < a_1+1$, então existem códigos QUENTA com parâmetros*

$$[[q-1, b_1+b_2+1, \geq q-1-\max\{a_1+a_2, b_1+b_2\}; q-2-(a_1+a_2)]]_q.$$

Demonstração: Seja $\mathbb{F}_q(z)/\mathbb{F}_q$ o corpo de funções racionais. O diferencial de Weil $\eta = \frac{1}{x^q-x}dx$ satisfaz as hipóteses do Teorema 2.5 e tem divisor dado por $(\eta) = (q-2)P_\infty - P_0 - D$, em que P_∞ e P_0 são os lugares no infinito e na origem, respectivamente, e $D = \sum_{i=1}^{q-1} P_i$, com P_i sendo os lugares racionais restantes. Assuma que $G_1 = a_1P_0 + a_2P_\infty$, $G_2 = b_1P_0 + b_2P_\infty$, $C_1 = C_{\mathcal{L}}(D, G_1)$ e $C_2 = C_{\mathcal{L}}(D, G_2)$. Uma vez que $b_2 \leq q-2-a_2$, temos que $\deg(G_1^\perp \cup G_2) = b_1+q-2-a_2 < q-1$, pela hipótese $b_1 \leq a_2$ e por $G_1^\perp \cap G_2 = (-1-a_1)P_0 + b_2P_\infty$. Assim, é possível usar o Teorema 4.8. Para o primeiro caso, tem-se que $c = q-1-1-(a_1+a_2)-(b_2-a_1) = q-2-(a_2+b_2)$, uma vez que $\deg(G_1^\perp \cap G_2) \geq 0$. Para o segundo, quando $b_2 < a_1+1$, tem-se que $\deg(G_1^\perp \cap G_2) < 0$, o qual implica em $\ell(G_1^\perp \cap G_2) = 0$ e $c = q-2-(a_1+a_2)$. As afirmações restantes são derivadas do Teorema 4.8 e da observação de que $\deg(G_1) = a_1+a_2$ e $\deg(G_2) = b_1+b_2$. ■

Corolário 4.5 *Suponha que $b_1 \leq a_2$, $b_2 \leq \min\{q-2-a_2, a_1\}$, com $a_1+a_2 = b_1+b_2 < q-1$, então existem códigos QUENTA* almost *maximamente emaranhados MDS com parâmetros $[[q-1, b_1+b_2+1, \geq q-1-(a_1+a_2); q-2-(a_1+a_2)]]_q$. Em particular, se $a_1 \leq q-2-a_2$, então existem códigos QUENTA $[[q-1, a_1+a_2+1, \geq q-1-(a_1+a_2); q-2-(a_1+a_2)]]_q$ que são maximamente emaranhados e MDS.*

Demonstração: As hipóteses feitas se encaixam no segundo caso no Teorema 4.9. O resultado segue da considerando $a_1+a_2 = b_1+b_2 < e-2$. ■

É mostrado no seguinte teorema a construção de códigos QUENTA derivados do corpo de funções hermitianas. Em seguida, o corpo de funções elípticas será usado para obter códigos QUENTA maximamente emaranhados com *Singleton defect* no máximo igual a um.

Teorema 4.10 *Seja q uma potência de um número primo e a_1, a_2, b_1, b_2 inteiros positivos tais que $b_1 \leq a_2 - q(q-1)$, $b_2 \leq q^3 + q(q-1) - 2 - a_2$, com $b_1 + b_2 < q^3 - 1$ e $a_1 + a_2 < q^3 - 1$. Então, tem-se os seguintes resultados:*

- *Se $b_2 \geq a_1 + 1$, então existe um código QUENTA com parâmetros*

$$[[q^3 - 1, a_1 + b_1 + 1, \geq q^3 - 1 - \max\{a_1 + a_2, b_1 + b_2\}; q^3 - 2 + q(q-1) - (a_2 + b_2)]]_{q^2}.$$

- *Se $b_2 < a_1 + 1$, então existe um código QUENTA com parâmetros*

$$[[q^3 - 1, b_1 + b_2 + 1 - \frac{q(q-1)}{2}, \geq q^3 - 1 - \max\{a_1 + a_2, b_1 + b_2\}; q^3 - 2 + \frac{q(q-1)}{2} - (a_1 + a_2)]]_{q^2}.$$

Demonstração: Seja $F/\mathbb{F}_{q^2}$ o corpo de funções hermitianas definido pela equação

$$y^q + y = x^{q+1}.$$

Então $F/\mathbb{F}_{q^2}$ tem $1 + q^3$ lugares racionais e gênero $g = q(q-1)/2$. Assuma que $D = P_1 + \cdots + P_{q^3-1}$, $G_1 = a_1 P_0 + a_2 P_\infty$, e $G_2 = b_1 P_0 + b_2 P_\infty$, em que P_∞ e P_0 são os lugares racionais no infinito e na origem, respectivamente. Assim, um possível diferencial de Weil satisfazendo o Teorema 2.35 é $\eta = \frac{1}{x^{q^2} - x} dx$, o qual tem divisor $(\eta) = -D - P_0 + (q^3 + q(q-1) - 2)P_\infty$. A hipótese que $b_2 \leq q^3 + q(q-1) - 2 - a_2$ implica em $G_1^\perp \cup G_2 = b_1 P_0 + (q^3 + q(q-1) - 2 - a_2)P_\infty$. De forma similar, da hipótese $b_1 \leq a_2 - q(q-1)$ temos que $\deg(G_1^\perp \cup G_2) < q^3 - 1$, o que permite a utilização do Teorema 4.8. Deste teorema, derivamos o resultado $G_1^\perp \cap G_2 = (-1 - a_1)P_0 + b_2 P_\infty$. Assim, se $b_2 \geq a_1 + 1$ tem-se que $\deg(G_1^\perp \cap G_2) \geq 0$, o que implica em $c = q^3 - 1 + \frac{q(q-1)}{2} - 1 - (a_1 + a_2) - (b_2 - a_1) + \frac{q(q-1)}{2} = q^3 - 2 + q(q-1) - (a_2 + b_2)$. Por outro lado, se $b_2 < a_1 + 1$ tem-se $\deg(G_1^\perp \cap G_2) < 0$, implicando em $\ell(G_1^\perp \cap G_2) = 0$ e $c = q^3 - 2 + \frac{q(q-1)}{2} - (a_1 + a_2)$. Uma vez que $\deg(G_1) = a_1 + a_2$ e $\deg(G_1) = b_1 + b_2$, usando o Teorema 4.8 e os valores para c calculados, obtêm-se os parâmetros mencionados para os códigos QUENTA. ■

Teorema 4.11 *Seja $q = 2^s$, com $s \geq 1$ sendo um número inteiro. Seja $F/\mathbb{F}_q$ o corpo de funções elípticas com e lugares racionais e gênero $g = 1$ definido pela equação*

$$y^2 + y = x^3 + bx + c, \tag{4.23}$$

em que $b, c \in \mathbb{F}_q$. Assuma que a_1, a_2, b_1, e b_2 são inteiro positivos tais que $b_1 \leq a_2$ e $b_2 \leq e - 1 - a_2$, com $a_1 + a_2 < e - 2$ e $b_1 + b_2 < e - 2$. Então, tem-se o seguinte resultado:

- *Se $b_2 \geq a_1 + 1$, então existem códigos QUENTA com parâmetros*

$$[[e - 2, a_1 + b_1 + 1, \geq e - 2 - \max\{a_1 + a_2, b_1 + b_2\}; e - 1 - (a_2 + b_2)]]_q.$$

- *Se $b_2 < a_1 + 1$, então existem códigos QUENTA com parâmetros*

$$[[e-2, b_1+b_2, \geq e-2-\max\{a_1+a_2, b_1+b_2\}; e-2-(a_1+a_2)]]_q.$$

Demonstração: Antes de tudo, assuma $S = \{\alpha \in \mathbb{F}_q | \text{existe } \beta \in \mathbb{F}_q \text{ tal que } \beta^2+\beta = \alpha^3 + b\alpha + c\}$. Para cada $\alpha \in S$, existem dois $\beta \in \mathbb{F}_q$ satisfazendo a expressão $\beta^2+\beta = \alpha^3+b\alpha+c$. Consequentemente, para cada $\alpha \in S$, existem dois lugares racionais relacionados a x igual a α. Assim, o conjunto de todos os lugares racionais é dado por estes valores de x e y mais o lugar no infinito, P_∞. O número de lugares racionais é denotado por e. Então $e = |S| + 1$. Agora, adote $D = \sum_{i=1}^{e-2} P_i$, $G_1 = a_1P_0 + a_2P_\infty$, e $G_2 = b_1P_0 + b_2P_\infty$, em que $P_0, P_1, \ldots, P_{e-1}$ são lugares racionais dois-a-dois distintos. Além disso, seja $\eta = \frac{dx}{\prod_{\alpha_i \in S}(x+\alpha_i)}$, então tem-se que o divisor do diferencial de Weil η é dado por $(\eta) = (e-1)P_\infty - P_0 - D$. Da hipótese $b_2 \leq e-1-a_2$ tem-se que $G_1^\perp \cup G_2 = b_1P_0 + (e-1-a_2)P_\infty$. Já a hipótese $b_1 \leq a_2$ implica em $\deg(G_1^\perp \cup G_2) < e-2$, o que possibilita o uso do Teorema 4.8. Por este teorema, derivamos $G_1^\perp \cap G_2 = (-1-a_1)P_0 + b_2P_\infty$. Consequentemente, se $b_2 \geq a_1+1$ tem-se que $\deg(G_1^\perp \cap G_2) \geq 0$, o que implica em $c = e-1-(a_2+b_2)$. Por outro lado, se $b_2 < a_1+1$ tem-se $\deg(G_1^\perp \cap G_2) < 0$, implicando em $\ell(G_1^\perp \cap G_2) = 0$ e $c = e-2-(a_1+a_2)$. Uma vez que $\deg(G_1) = a_1+a_2$ e $\deg(G_1) = b_1+b_2$, pelo uso do Teorema 4.8 e dos valores de c anteriormente calculados, obtemos os parâmetros mencionados para o códigos QUENTA. ■

Corolário 4.6 *Suponha que exista uma curva elíptica com e lugares racionais. Então, para $b_1 \leq a_2$, $b_2 \leq \min\{e-1-a_2, a_1\}$, com $a_1+a_2 = b_1+b_2 < e-2$, existem códigos QUENTA $[[e-2, b_1+b_2, \geq e-2-(a_1+a_2); e-2-(a_1+a_2)]]_q$ que são maximamente emaranhados e* almost *MDS.*

Demonstração: Considere o segundo caso do Teorema 4.11. Da hipótese $a_1+a_2 = b_1+b_2 < e-2$, o resultado segue. ■

É mostrado na Tabela 4.4 o número de lugares racionais para diversas curvas elípticas em função do valor de s, o grau da extensão $\mathbb{F}_{2^s}$ [93].

Observação 4.1 *Nesta seção, foi utilizado códigos AG de dois lugares. O motivo para isso é que os códigos QUENTA derivados de códigos AG de um lugar têm parâmetros triviais; i.e., eles possuem ou emaranhamento igual a zero, o que os torna códigos quânticos ordinários (como os do Capítulo 3) e não é esse o objetivo aqui, ou dimensão nula, o que também não é atrativo para a literatura de códigos quânticos.*

4.3.2 – Construção Hermitiana de Códigos Quânticos Assistidos por Emaranhamento

Como foi dito na seção anterior, o uso do método de construção hermitiana para códigos QUENTA normalmente tem que ser feito de forma mais cautelosa, principalmente para códigos

Tabela 4.4 – Algumas curvas elípticas sobre $\mathbb{F}_q$ ($q = 2^s$) e o número de lugares racionais

Curva elíptica	s	Número de lugares racionais (e)
$y^2 + y = x^3$	s ímpar	$q+1$
	$s \equiv 0 \mod 4$	$q+1-2\sqrt{q}$
	$s \equiv 0 \mod 2$	$q+1+2\sqrt{q}$
$y^2+y = x^3+x$	$s \equiv 1,7 \mod 8$	$q+1+\sqrt{2q}$
	$s \equiv 3,5 \mod 8$	$q+1-\sqrt{2q}$
$y^2+y = x^3+x+1$	$s \equiv 1,7 \mod 8$	$q+1-\sqrt{2q}$
	$s \equiv 3,5 \mod 8$	$q+1+\sqrt{2q}$
$y^2 + y = x^3 + \delta x$ $(Tr(\delta) = 1)$	s par	$q+1$
$y^2 + y = x^3 + \delta$ $(Tr(\delta) = 1)$	$s \equiv 0 \mod 4$	$q+1+2\sqrt{q}$
	$s \equiv 2 \mod 4$	$q+1-2\sqrt{q}$

AG, pois não existe uma fórmula genérica que caracterize o dual hermitiano de um código AG. Entretanto, descrevendo códigos AG por meio de uma base com características que serão apresentadas a seguir, é possível construir códigos QUENTA usando o dual hermitiano de um código AG. Antes de apresentar este resultado, será demonstrado algumas ferramentas que serão utilizadas no resultado principal dessa seção.

Proposição 4.3 *Seja $\mathcal{C}$ um código linear sobre $\mathbb{F}_{q^2}$ com comprimento n e $\mathcal{C}^{\perp_h}$ seu dual hermitiano. Então* $\dim(\mathcal{C} \cap \mathcal{C}^{\perp_h}) = \dim(\mathcal{C}^{\perp} \cap \mathcal{C}^q)$.

Demonstração: Considere $\mathbf{x} \in \mathcal{C}^{\perp_h}$, então se tem o seguinte:

$$\begin{aligned}
\mathbf{x} \in \mathcal{C}^{\perp_h} \quad &\iff \mathbf{x} \cdot \mathbf{c}^q = 0, && \forall \mathbf{c} \in C, \\
&\iff \textstyle\sum_{i=1}^{n} x_i c_i^q = 0, && \forall \mathbf{c} \in C, \\
&\iff \textstyle\sum_{i=1}^{n} x_i^q c_i = 0, && \forall \mathbf{c} \in C, \text{ uma vez que } c_i^{q^2} = c_i \\
&\iff \mathbf{x}^q \in \mathcal{C}^{\perp}, \\
&\iff \mathbf{x} \in (\mathcal{C}^{\perp})^q.
\end{aligned}$$

Assim, podemos ver que

$$\begin{aligned}
\dim(\mathcal{C} \cap \mathcal{C}^{\perp_h}) &= \dim(\mathcal{C} \cap (\mathcal{C}^{\perp})^q) \\
&= \dim(\mathcal{C}^q \cap \mathcal{C}^{\perp}).
\end{aligned}$$

Consequentemente, temos $\dim(\mathcal{C} \cap \mathcal{C}^{\perp_h}) = \dim(\mathcal{C}^{\perp} \cap \mathcal{C}^q)$. ∎

É apresentado na Proposição 4.3 um novo método de cálculo da dimensão de $\mathcal{C} \cap \mathcal{C}^{\perp_h}$. Para ser possível utilizá-lo para códigos AG, é necessário descrever o código linear $\mathcal{C}^q$. A

Proposição 4.4 aborda esse tópico mostrando que é possível calcular uma base para $\mathcal{C}^q$ a partir de uma base de $\mathcal{C}$. E é descrito no Teorema 4.2 como calcular a interseção de dois espaços vetoriais (em particular, códigos lineares) quando as bases são subconjuntos de um conjunto maior o qual é base de $\mathbb{F}_{q^2}^n$.

Proposição 4.4 *Seja $\mathcal{C}$ um código linear sobre $\mathbb{F}_{q^2}$ com comprimento n e dimensão k. Se $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ é uma base de $\mathcal{C}$, então uma base para $\mathcal{C}^q$ é dado pelo conjunto $\{\mathbf{x}_1^q, \ldots, \mathbf{x}_k^q\}$.*

Demonstração: Primeiramente, note que para qualquer $\mathbf{c}' \in \mathcal{C}^q$ existe um único $\mathbf{c} \in \mathcal{C}$ tal que $\mathbf{c}' = \mathbf{x}^q$. Uma vez que $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ é uma base para $\mathcal{C}$, então $\mathbf{c} = \sum_{i=1}^k c_i \mathbf{x}_i$, com $c_i \in \mathbb{F}_{q^2}$. Assim, $\mathbf{c}' = \mathbf{c}^q = \sum_{i=1}^k c_i^q \mathbf{x}_i^q = \sum_{i=1}^k c_i' \mathbf{x}_i^q$. Como $\mathcal{C}$ e $\mathcal{C}^q$ são isomorfos, então eles têm a mesma dimensão, o que implica que $\{\mathbf{x}_1^q, \ldots, \mathbf{x}_k^q\}$ é uma base de $\mathcal{C}^q$. ∎

Por completeza, será apresentado o lema a seguir.

Lema 4.2 *Seja B uma base para $\mathbb{F}_{q^2}^n$ sobre $\mathbb{F}_{q^2}$. Assuma que B_1 e B_2 são dois subconjuntos de B. Denotando por V_1 e V_2 os subespaços gerados por B_1 e B_2, respectivamente, tem-se que $\dim(V_1 \cap V_2) = |B_1 \cap B_2|$.*

Demonstração: A afirmação de que qualquer elemento em $B_1 \cap B_2$ fornece um vetor em $V_1 \cap V_2$ é trivial. Denote os elementos de B_1, B_2 e $B_1 \cap B_2$ por $\mathbf{v}_{1i}, \mathbf{v}_{2i}$ e $\mathbf{v}_{0i}$, respectivamente. Para demonstrar a inclusão reversa, considere $\mathbf{v} \in V_1 \cap V_2$. Assim, podemos representá-lo por

$$\mathbf{v} = \sum_{\mathbf{v}_{0i} \in B_1 \cap B_2} c_{0i}\mathbf{v}_{0i} + \sum_{\mathbf{v}_{1i} \in B_1 \setminus (B_1 \cap B_2)} c_{1i}\mathbf{v}_{1i} \quad \text{e} \quad \mathbf{v} = \sum_{\mathbf{v}_{0i} \in B_1 \cap B_2} d_{0i}\mathbf{v}_{0i} + \sum_{\mathbf{v}_{2i} \in B_2 \setminus (B_1 \cap B_2)} d_{2i}\mathbf{v}_{2i},$$

o que implica que

$$\sum_{\mathbf{v}_{0i} \in B_1 \cap B_2} (c_{0i} - d_{0i})\mathbf{v}_{0i} + \sum_{\mathbf{v}_{1i} \in B_1 \setminus (B_1 \cap B_2)} c_{1i}\mathbf{v}_{1i} - \sum_{\mathbf{v}_{2i} \in B_2 \setminus (B_1 \cap B_2)} d_{2i}\mathbf{v}_{2i} = 0.$$

Uma vez que $\mathbf{v}_{0i}, \mathbf{v}_{1i}$ e $\mathbf{v}_{2i}$ pertencem à base B, temos que os coeficientes na equação anterior precisam ser iguais a zero, o que resulta em $\mathbf{v} = \sum_{\mathbf{v}_{0i} \in B_1 \cap B_2} c_{0i}\mathbf{v}_{0i}$ e a inclusão reversa está demonstrada. ∎

Agora estamos prontos para descrever a utilização da construção hermitiana para códigos QUENTA utilizando códigos AG. Para tal objetivo, será aplicado o Lema 4.2 à códigos AG derivados do corpo de funções racionais. Veja o Teorema 4.12.

Teorema 4.12 *Seja q uma potência de um número primo e m um inteiro o qual pode ser escrito como $m = qt + r < q^2$, em que $t \geq 1$ e $0 \leq r \leq q - 1$. Então, tem-se:*

- *Se $t \geq q - r - 1$, então existem códigos QUENTA MDS com parâmetros*

$$[[q^2, (t+1)^2 + 2r + 1 - 2q, \geq q^2 - (qt + r); (q - t - 1)^2]]_q.$$

- *Se $t < q - r - 1$, então existem códigos QUENTA MDS com parâmetros*

$$[[q^2, t^2 - 1, \geq q^2 - (qt + r); (q - t)^2 - 2(r + 1)]]_q.$$

Demonstração: Seja $F(z)/\mathbb{F}_{q^2}$ o corpo de funções racionais, $D = \sum_{i=0}^{q^2-1} P_i$ e $G = mP_\infty$, em que $m = qt + r$. Seja $C_{\mathcal{L}}(D, G)$ o código AG derivado de D e G com parâmetros $[q^2, m + 1, q^2 - m]_q$. Considere $\boldsymbol{x^i} = ev_D(x^i)$. Assuma que $B = \{\boldsymbol{x^i} | 0 \leq i \leq n - 1\}$. Então B é uma base para $\mathbb{F}_{q^2}^n$. Uma base para $C_{\mathcal{L}}(D, G)$ é dada pelo subconjunto $B' = \{\boldsymbol{x^i} | 0 \leq i \leq m\}$. Consequentemente, uma base de $C_{\mathcal{L}}(D, G)^q$ pode ser descrita como $B_1 = \{\boldsymbol{x^{qi}} | 0 \leq i \leq m\}$. Agora, note que $\boldsymbol{x^{q^2+a}} = \boldsymbol{x^{a+1}}$ para todo $a \geq 0$. Assim,

$$B_1 = \{\boldsymbol{x^{qi+j}} | 0 \leq i \leq q - 1, 0 \leq j \leq t - 1\} \cup \{\boldsymbol{x^{qi+t}} | 0 \leq i \leq r\}.$$

Por outro lado, uma base de $C_{\mathcal{L}}(D, G)^\perp$ pode ser descrita pelo conjunto

$$\begin{aligned} B_2 &= \{\boldsymbol{x^i} | 0 \leq i \leq q^2 - 2 - m\} \\ &= \{\boldsymbol{x^{qi+j}} | 0 \leq i \leq q - t - 2, 0 \leq j \leq q - 1\} \cup \{\boldsymbol{x^{(q-t-1)q+j}} | 0 \leq j \leq q - r - 2\}. \end{aligned}$$

Dessa forma, expoentes para $\boldsymbol{x}$ nas bases B_1 e B_2 podem ser representados pelos conjuntos

$$\begin{Bmatrix} 0 & 1 & 2 & \cdots & t-1 & t \\ q & q+1 & q+2 & \cdots & q+t-1 & q+t \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ rq & rq+1 & rq+2 & \cdots & rq+t-1 & rq+t \\ \vdots & \vdots & \vdots & \cdots & \vdots & \\ (q-1)q & (q-1)q+1 & (q-1)q+2 & \cdots & (q-1)q+t-1 & \end{Bmatrix}$$

e

$$\begin{Bmatrix} 0 & 1 & \cdots & q-r-2 & \cdots & q-1 \\ q & q+1 & \cdots & q+q-r-2 & \cdots & 2q-1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ (q-t-2)q & (q-t-2)q+1 & \cdots & (q-t-2)q+q-r-2 & \cdots & (q-t-2)q+q-1 \\ (q-t-1)q & (q-t-1)q+1 & \cdots & (q-t-1)q+q-r-2 & & \end{Bmatrix},$$

respectivamente. Usando esta descrição, vemos que estas bases satisfazem a hipótese necessária para a utilização do Lema 4.2, o que faz possível o cálculo da interseção dos códigos relacionados com B_1 e B_2 via o cálculo da interseção destes conjuntos. Para isso, é necessário considerar dois casos separadamente, $t \geq q - r - 1$ e $t < q - r - 1$. Para o primeiro caso, a

interseção é dada pelo seguinte conjunto

$$B_1 \cap B_2 = \{\boldsymbol{x}^{\boldsymbol{qi+j}} | 0 \leq i \leq q-t-2, 0 \leq j \leq t\} \cup \{\boldsymbol{x}^{\boldsymbol{(q-t-1)q+j}} | 0 \leq j \leq q-r-2\}.$$

Assim, $\dim(C_{\mathcal{L}}(D,G)^q \cap C_{\mathcal{L}}(D,G)^{\perp}) = |B_1 \cap B_2| = (q-t-1)(t+1)+q-r-1$. Usando a mesma descrição para o caso em que $t < q-r-1$, vemos que

$$B_1 \cap B_2 = \{\boldsymbol{x}^{\boldsymbol{qi+j}} | 0 \leq i \leq q-t-1, 0 \leq j \leq t-1\} \cup \{\boldsymbol{x}^{\boldsymbol{(qi+t}} | 0 \leq i \leq r\},$$

o que implica em $\dim(C_{\mathcal{L}}(D,G)^q \cap C_{\mathcal{L}}(D,G)^{\perp}) = |B_1 \cap B_2| = (q-t)t+r+1$. Aplicando os cálculos anteriores e o fato que $C_{\mathcal{L}}(D,G)$ tem parâmetros $[q^2, m+1, q^2-m]_q$, tem-se, pela Proposição 4.2, que existem códigos QUENTA com parâmetros

- $[[q^2, (t+1)^2+2r+1-2q, \geq q^2-(qt+r); (q-t-1)^2]]_q$, para $t \geq q-r-1$; e
- $[[q^2, t^2-1, \geq q^2-(qt+r); (q-t)^2-2(r+1)]]_q$, para $t < q-r-1$.

■

4.3.3 – Exemplos

Nas Tabelas 4.5 e 4.6, é apresentado alguns códigos QUENTA ótimos, em termos do limitante de Singleton, obtidos dos Teoremas 4.9, 4.11 e 4.12. Os códigos QUENTA derivados da construção euclidiana estão expostos na Tabela 4.5. Foi utilizado códigos AG obtidos da linha projetiva e da curva elíptica para construir estes códigos. Como pode ser visto, os códigos da primeira coluna da Tabela 4.5 são MDS e os da segunda são *almost* MDS. Para a Tabela 4.6, códigos QUENTA são derivados da construção hermitiana, em que códigos AG racionais foram usados como a contra-partida clássica. Estes códigos também possuem uma combinação ótima de parâmetros, uma vez que são MDS. Além disso, desde que códigos QUENTA utilizam emaranhamento, podemos concluir que os códigos das Tabelas 4.5 e 4.6 têm distância mínima melhor ou igual à qualquer código quântico estabilizador [19].

Os códigos QUENTA que faltam ser comparados com os da literatura são aqueles derivados da curva de Hermite. A primeira análise de qualidade dos códigos construídos é via o *Singleton defect*, o qual é a diferença entre o limitante de Singleton para códigos QUENTA mostrado na Eq. 4.20 e a distância mínima do código. Relembrando que um código quântico $[[n,k,d;c]]_q$ satisfaz $k+2d \leq n+c+2$. Tem-se que os códigos construídos no Teorema 4.10 tem máximo *Singleton defect* igual a $q(q-1)/2$. Alguns exemplos de parâmetros possíveis destes códigos são $[[7,2,4;3]]_4$, $[[26,10,11;10]]_9$ e $[[63,19,32;31]]_{16}$, os quais possuem *Singleton defect* igual a 1, 3 e 6, respectivamente. Comparando estes exemplos com códigos quânticos estabilizadores, vê-se que os exemplos numéricos apresentados possuem distância mínima inalcançáveis, para o mesmo comprimento e dimensão, por códigos estabilizadores. De fato, usando o limitante de Singleton para códigos estabilizadores esta conclusão pode facilmente ser obtida. Assim,

Tabela 4.5 – Exemplos de códigos maximamente emaranhados (*almost*) MDS obtidos pela construção euclidiana

Novos códigos QUENTA – Teorema 4.9 $[[q-1, a_1+a_2+1, q-1-(a_1+a_2); q-2-(a_1+a_2)]]_q$ $a_1+a_2 \leq q-2$	Novos códigos QUENTA – Teorema 4.11 $[[e-2, a_1+a_2, e-2-(a_1+a_2); e-2-(a_1+a_2)]]_q$ $a_1+a_2 < e-2$, e e como na Tabela 4.4
Exemplos	
$[[3,2,2;1]]_4$	$[[7,5,2;2]]_4$
$[[4,2,3;2]]_5$	$[[11,6,5;5]]_8$
$[[6,4,3;2]]_7$	$[[11,8,3;3]]_8$
$[[7,4,4;3]]_8$	$[[23,13,10;10]]_{16}$
$[[10,7,4;3]]_{11}$	$[[23,18,5;5]]_{16}$
$[[12,7,6;5]]_{13}$	$[[39,25,14;14]]_{32}$
$[[15,10,6;5]]_{16}$	$[[39,18,11;11]]_{32}$

Tabela 4.6 – Exemplos de códigos QUENTA MDS obtidos pela construção hermitiana

Novos códigos QUENTA – Teorema 4.12 $[[q^2, (t+1)^2+2r+1-2q, q^2-(qt+r); (q-t-1)^2]]_q$ $m = qt+r < q^2$, $t \geq q-r-1$ e $0 \leq r \leq q-1$
Exemplos
$[[16,6,6;1]]_4$
$[[49,25,13;1]]_7$
$[[49,11,24;9]]_7$
$[[64,29,20;4]]_8$
$[[64,25,22;4]]_8$
$[[81,33,29;9]]_9$
$[[81,16,41;16]]_9$
$[[256,141,66;16]]_{16}$

mesmo não sendo possível construir códigos MDS por meio do Teorema 4.10, é possível utilizá-los para obter códigos com parâmetros superiores aos dos códigos quânticos estabilizadores. Assumindo que o *entanglement defect* é dado pela diferença entre o valor de emaranhamento utilizado por um código QUENTA e $n-k$, com n sendo o comprimento do código e k sua dimensão, nota-se que o *entanglement defect* nesta família de códigos QUENTA code é igual a $2g$, com g sendo o gênero do corpo de funções hermitianas. Por fim, a Tabela 4.7 mostra alguns exemplos de códigos QUENTA que possuem taxas superior às taxas de códigos derivadas do limitantes assintótico de Gilbert-Varshamov mostrado na Seção 4.4.

Tabela 4.7 – Exemplos de novos códigos QUENTA obtidos da curva de Hermite pela construção euclidiana

Novos códigos QUENTA – Teorema 4.10
$[[q^3-1, b_1+b_2+1-q(q-1)/2, q^3-1-\max\{a_1+a_2, b_1+b_2\};$ $q^3+q(q-1)/2-(a_1+a_2)-2]]_{q^2}$
$b_1 \leq a_2-q(q-1)$, $b_2 \leq \min\{q^3+q(q-1)-2-a_2, a_1\}$, and $a_1+a_2, b_1+b_2 < q^3-1$
Exemplos
$[[26, 15, 6; 5]]_9$
$[[64, 39, 11; 10]]_{16}$
$[[125, 51, 54; 53]]_{25}$
$[[343, 179, 122; 121]]_{49}$

4.4 – Existência de Famílias Asintoticamente Boas de Códigos QUENTA Maximamente Emaranhados

Nesta seção é mostrado que é possível construir uma família de códigos QUENTA maximamente emaranhados e assintoticamente boa a partir de qualquer família de códigos (clássicos) AG assintoticamente boa. Isto é um consequência do uso de um resultado de Carlet, *et al.* [94] aplicado ao Corolário 4.1. Antes de apresentá-lo, é necessário mostrar o resultado de de Carlet, *et al.*.

Proposição 4.5 *[94, Corolário 14] Sejam $q > 3$ uma potência de um número primo e $A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}$, em que $N_q(g)$ denota o número máximo de lugares racionais que um corpo de funções de gênero g com corpo das constantes $\mathbb{F}_q$ pode ter. Então existe uma família de códigos LCD com*

$$\alpha_q^{LCD}(\delta) \geq 1-\delta-\frac{1}{A(q)}, \text{ para } \delta \in [0,1]. \tag{4.24}$$

Teorema 4.13 *Sejam $q > 3$ um potência de um número primo e $A(q)$ definido como na Proposição 4.5. Então, existe uma família de códigos QUENTA MDS maximamente emaranhados e assintoticamente boa com parâmetros $[[n_t, k_t, d_t; c_t]]_q$, tal que*

$$\lim_{t\to\infty}\frac{d_t}{n_t} \geq \delta, \qquad \lim_{t\to\infty}\frac{k_t}{n_t} \geq 1-\delta-\frac{1}{A(q)},$$

e

$$\lim_{t\to\infty}\frac{c_t}{n_t} \in [\delta, \delta+1/A(q)].$$

para todo $\delta \in [0, 1-1/A(q)]$.

Demonstração: Seja $\mathcal{F}_{\mathcal{C}} = \{C_1, C_2, \ldots\}$ uma família de códigos LCD assintoticamente boa como as da Proposição 4.5, em que cada C_t tem parâmetros $[n_i, k_i, d_i]_q$. Se aplicarmos a

família $\mathcal{F}_{\mathcal{C}}$ para construir códigos QUENTA, segue do Corolário 4.1 que os códigos QUENTA construídos têm máximo emaranhamento e parâmetros $[[n_t, k_t, d_t; c_t]]_q$, tais que

$$\lim_{t\to\infty}\frac{d_t}{n_t}=\lim_{i\to\infty}\frac{d_i}{n_i}\geq\delta, \qquad \lim_{t\to\infty}\frac{k_t}{n_t}=\lim_{i\to\infty}\frac{k_i}{n_i}\geq 1-\delta-\frac{1}{A(q)}.$$

Além disso, tem-se

$$\lim_{t\to\infty}\frac{c_t}{n_t}=\lim_{i\to\infty}\frac{n_i-k_i}{n_i}=\lim_{i\to\infty}1-\frac{k_i}{n_i}\leq\delta+\frac{1}{A(q)}$$

and

$$\lim_{t\to\infty}\frac{c_t}{n_t}=\lim_{i\to\infty}\frac{n_i-k_i}{n_i}\geq\lim_{i\to\infty}\frac{d_i-1}{n_i}\geq\delta,$$

para $\delta\in[0,1-1/A(q)]$. Consequentemente, uma vez que as famílias da Proposição 4.5 são assintoticamente boas e LCD; então, tem-se que a família de códigos QUENTA também será assintoticamente boa e terá máximo emaranhamento. ■

Observação 4.2 *Se q é um quadrado, então $A(q)=\sqrt{q}-1$ por [9, 95].*

Observação 4.3 *Foi mostrado recentemente por Galindo,* et al. *[42] o limitante de Gilbert-Varschamov para códigos QUENTA. Usando códigos AG derivados de uma torre de corpos de funções que atinge o limitante de Drinfeld-Vladut [71] e o teorema anterior, é possível mostrar que existe uma família de códigos QUENTA com parâmetros que excedem o limitante mencionado (veja Figura 4.2).*

Na Fig. 4.2 é mostrado uma comparação entre os parâmetros dos códigos QUENTA construídos via o Teorema 4.13 e os códigos que o limitante de Gilbert-Varshamov da Ref. [42] garantem existir. Essa comparação é feita sobre a taxa e emaranhamento relativo dos códigos QUENTA quando $q=64$. Como é possível notar, para distâncias relativas maiores que $\delta=0.1$, é obtido códigos QUENTA superiores aos do limitante de Gilbert-Varshamov. Isso expõe quantitativamente a qualidade dos códigos aqui apresentados.

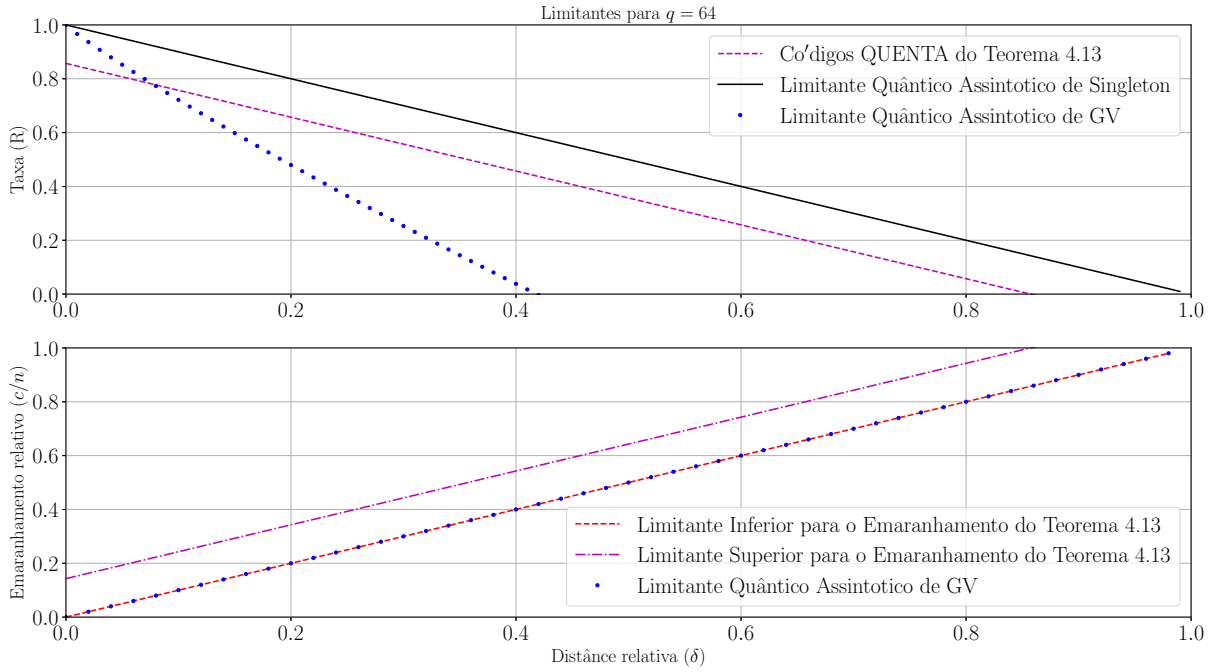


Figura 4.2 – Comparação entre os códigos QUENTA derivados do Teorema 4.13 e o limitante quântico de Gilbert-Varshamov via análise da taxa e emaranhamento relativo quando $q = 64$.

CAPÍTULO 5

Códigos Convolucionais Clássicos e Quânticos

Códigos convolucionais são amplamente utilizados nos sistemas de comunicações atuais e é sobre esse assunto que este capítulo contempla. Trataremos de códigos convolucionais clássicos, bem como de códigos convolucionais no paradigma quântico. Para o caso clássico, as matrizes geradoras, tanto polinomial quanto semi-infinita, são mostradas. O dual euclidiano e hermitiano são apresentados e esses são utilizados, posteriormente, para fazer a conexão entre códigos convolucionais clássicos e quânticos. De forma similar ao caso anterior, é mostrado uma matriz geradora para o código convolucional quântico e a conexão com seu grupo estabilizador. Por fim, o limitante de Singleton generalizado é exposto.

5.1 – Revisão de Códigos Convolucionais Clássicos

5.1.1 – Estrutura Algébrica de Códigos Convolucionais

Um código convolucional com parâmetros (n, k) é o conjunto de todas as sequências produzidas por uma função linear que mapeia uma sequência de entrada $\mathbf{u} = (\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2, \ldots)$ de k-uplas em uma sequência de saída $\mathbf{v} = (\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \ldots)$ de n-uplas, $k \leq n$, em que cada bloco de n-uplas $\mathbf{v}_l$, produzido no tempo l, depende do correspondente bloco de k-uplas de entrada, $\mathbf{u}_l$, e de alguns μ blocos de k-uplas de entrada anteriores, $\mathbf{u}_{l-1}$, $\mathbf{u}_{l-2}$, …, $\mathbf{u}_{l-\mu}$. O parâmetro μ é chamado de memória do codificador.

Para uma definição mais formal, considere o seguinte:

Definição 5.1 *Um código convolucional clássico $\mathcal{V}_\mathcal{C}$ é um submódulo de $\mathbb{F}_q[D]^n$ gerado pela matriz invertível à direita $G(D) = (g_{ij}) \in \mathbb{F}_q[D]^{k\times n}$,*

$$\mathcal{V}_\mathcal{C} := \{\mathbf{u}(D)G(D) \colon \mathbf{u}(D) \in \mathbb{F}_q[D]^k\}. \tag{5.1}$$

O elemento D representa a memória do código convolucional. Uma matriz geradora de um código convolucional é denominada de minimal se tiver o menor número possível de elementos de memória. O grau do código convolucional $\mathcal{V}_\mathcal{C}$ é dado por

$$\delta := \max\{\deg\gamma : \gamma \textit{ é um determinante de uma submatriz } k\times k \textit{ de } G(D)\} = \sum_{i=1}^{k}\nu_i, \quad (5.2)$$

em que $\nu_i := \max_{1\leq j\leq n}\{\deg g_{ij}\}$. O peso wt$(v(D))$ de um polinômio $v(D)$ em $\mathbb{F}_q[D]$ é dado pelo número de coeficientes não-nulos de $v(D)$, enquanto que para um elemento $\mathbf{u}(D)\in\mathbb{F}_q[D]^n$ tem-se wt$(\mathbf{u}(D)) := \sum_{i=0}^{n-1}$ wt$(u_i(D))$. A distância livre d_f de $\mathcal{V}_\mathcal{C}$ é definida como $d_f :=$ wt$(\mathcal{V}_\mathcal{C}) = \min\{wt(\mathbf{c}(D))\colon \mathbf{c}(D)\in\mathcal{V}_\mathcal{C}, \mathbf{c}(D)\neq\mathbf{0}\}$. Um código convolucional $(n,k,\delta)_q$ com memória μ e distância livre d_f é denotado por $(n,k,\delta;\mu,d_f)_q$.

Seja $\mathbb{N}_0$ o conjunto dos inteiros não-negativos. Além disso, denote por

$$\Gamma_q := \{f:\mathbb{N}_0\to\mathbb{F}_q\colon \text{a menos de um conjunto finito, todos elementos na imagem de } f \text{ são } 0\}. \quad (5.3)$$

É possível ver $f\in\Gamma_q$ como uma sequência infinita $(f_i = f(i))_{i\geq 0}$ de suporte finito. Com isso, Γ_q descreve um módulo vetorial considerando soma sobre $\mathbb{F}_q$ e convolução de sequências. De agora em diante, será essa a descrição feita para elementos de Γ_q. Defina o isomorfismo de espaços vetoriais $\vartheta\colon\mathbb{F}_q[D]^n\to\mathbb{F}_q[D]$, que mapeia um elemento $\mathbf{u}(D) = (u_0(D),\ldots,u_{n-1}(D))$ de $\mathbb{F}[D]^n$ ao polinômio $\sum_{i=0}^{n-1}D^i u_i(D^n)\in\mathbb{F}_q[D]$ (veja o Exemplo 5.1). Além disso, defina a composição de isomorfismos $\sigma\colon\mathbb{F}_q[D]^n\to\Gamma_q$ como sendo $\sigma=\zeta\circ\vartheta$, com $\zeta\colon\mathbb{F}_q[D]\to\Gamma_q$ sendo o isomorfismo trivial entre esses módulos vetoriais. Será referido à imagem $\sigma(\mathcal{V}_\mathcal{C}) := \{\sigma(\mathbf{c})\colon\mathbf{c}\in\mathcal{V}_\mathcal{C}\}$ de um código convolucional também como $\mathcal{V}_\mathcal{C}$.

Exemplo 5.1 *Seja $\mathbf{u}(D) = (1+D, 1+D^2, D+D^4, D, 1+D^5)$ um elemento de $\mathbb{F}_2[D]^5$. Com isso, tem-se*

$$\begin{aligned}\vartheta(\mathbf{u}(D)) &= \sum_{i=0}^{4}D^i u_i(D^5) &(5.4)\\ &= 1+D^5+D+D^{11}+D^7+D^{22}+D^8+D^4+D^{24} &(5.5)\\ &= 1+D+D^4+D^5+D^7+D^8+D^{11}+D^{22}+D^{24}. &(5.6)\end{aligned}$$

Aplicando ζ a $\vartheta(\mathbf{u}(D))$ é obtido a sequência

$$\zeta(\vartheta(\mathbf{u}(D))) = (1,1,0,0,1,1,0,1,1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,1,0,1,0,0,0,...), \quad (5.7)$$

o que também pode ser descrito como $\sigma(\mathbf{u}(D))$.

Seja $G(D) = G_0 + G_1D + \cdots + G_\mu D^\mu$, em que $G_i\in\mathbb{F}_q^{k\times n}$, para $0\leq i\leq\mu$. Associa-se à

matriz geradora $G(D)$ uma matriz semi-infinita dada por

$$G = \begin{pmatrix} G_0 & G_1 & \cdots & G_\mu & & \\ & G_0 & G_1 & \cdots & G_\mu & \\ & & \ddots & \ddots & & \ddots \end{pmatrix}. \tag{5.8}$$

Produtos Internos Euclidianos e Hermitianos

O produto interno euclidiano de duas sequências u e v em Γ_q é definido como sendo $\langle u, v\rangle := \sum_{i\in\mathbb{N}_0} u_i v_i$. O dual euclidiano de um código convolucional $\mathcal{V}_\mathcal{C}$ é dado por $\mathcal{V}_\mathcal{C}^\perp := \{u \in \Gamma_q \colon \langle u, v\rangle = 0 \text{ para todo } v \in \mathcal{V}_\mathcal{C}\}$. Um código convolucional $\mathcal{V}_\mathcal{C}$ é chamado de auto-ortogonal se $\mathcal{V}_\mathcal{C} \subseteq \mathcal{V}_\mathcal{C}^\perp$. É fácil notar que um código convolucional $\mathcal{V}_\mathcal{C}$ é auto-ortogonal se, e somente se, $GG^T = 0$ [96].

Agora considere que as palavras-código sejam definidas sobre $\mathbb{F}_{q^2}$. O produto interno hermitiano de duas sequências u e v em Γ_{q^2} é definido como $\langle u, v\rangle_h = \sum_{i\in\mathbb{N}_0} u_i v_i^q$. Assim, $\mathcal{V}_\mathcal{C}^{\perp_h} := \{u \in \Gamma_{q^2} \colon \langle u, v\rangle_h = 0 \text{ para todo } v \in \mathcal{V}_\mathcal{C}\}$. Tem-se que $\mathcal{V}_\mathcal{C} \subseteq \mathcal{V}_\mathcal{C}^{\perp_h}$ se, e somente se, $GG^\dagger = 0$, em que $G^\dagger$ representa a transposta hermitiana de G.

5.2 – Códigos Convolucionais Quânticos

Um código convolucional quântico codifica uma sequência de qudits que, em princípio, tem comprimento desconhecido pelo codificador. Assim, a ideia é impor uma estrutura ao código que simplifique essa codificação e decodificação *online*. A ideia chave para a construção dessa estrutura é notar que restringindo um código convolucional (quântico) estabilizador a comprimentos finitos, obtem-se o código estabilizador do Capítulo 3. Consequentemente, como será mostrado posteriormente, a exigência de auto-ortogonalidade sobre o código clássico será mantida, tanto quanto a existência de um estabilizador para o código e a descrição dos erros corrigíveis ou não. Para uma caracterização mais prática, assuma que n e m sejam inteiros positivos. A cada passo de processamento do codificador convolucional será processado $n + \mu$ qudits, em que μ qudits serão guardados para o passo de codificação seguinte e n qudits são os que irão para o canal de comunicação.

De forma similar ao que foi apresentado no Capítulo 3, assuma o grupo de Pauli $G_{(t+1)n+\mu} = \langle E \colon E \in \mathcal{E}_{(t+1)n+\mu}\rangle$, com $t \in \mathbb{N}_0$. Para $i, j \in \mathbb{N}_0$, com $i \leq j$, defina o isomorfismo inclusivo $\iota_{ij} \colon G_{(i+1)n+\mu} \hookrightarrow G_{(j+1)n+\mu}$ por $\iota_{ij}(E) = E \otimes I^{\otimes n(j-i)}$. Tem-se que $\iota_{ii}(E) = E$ e $\iota_{ik} = \iota_{jk} \circ \iota_{ij}$, para $i \leq j \leq k$. Assim, existe o grupo

$$G_\infty = \varinjlim (G_{(i+1)n+\mu}, \iota_{ij}), \tag{5.9}$$

que é o limite direto do grupo $G_{(i+1)n+\mu}$ sobre o conjunto com ordenamento total $(\mathbb{N}_0, \leq)$. Para cada inteiro não-negativo i, existe um homomorfismo $\iota_i \colon G_{(i+1)n+\mu} \to G_\infty$ dado por

$\iota_i(E_i) = E_i \otimes I^{\otimes\infty}$, para $E_i \in G_{(i+1)n+\mu}$, tanto quanto a composição $\iota_i = \iota_j \circ \iota_{ij}$, para todo $i \leq j$. Por fim, tem-se que $G_\infty = \cup_{i=0}^{\infty}\iota_i(G_{(i+1)n+\mu})$, ou seja, G_∞ consiste de todos os infinitos produtos tensoriais de matrizes em $\langle E\colon M \in \mathcal{E}\rangle$ tal que, a menos de um número finito, todas as componentes são iguais a I.

O estabilizador do código convolucional quântico será definido por meio desse limite direto. Assim, seja $\mathcal{S}_{n+\mu}$ um subgrupo abeliano de $G_{n+\mu}$. Para um inteiro positivo t, defina recursivamente o subgrupo $\mathcal{S}_{(t+1)n+\mu}$ de $G_{(t+1)n+\mu}$ como sendo $\mathcal{S}_{(t+1)n+\mu} := \langle E \otimes I^{\otimes n}, I^{\otimes tn} \otimes E'\colon E \in \mathcal{S}_{tn+\mu}, E' \in \mathcal{S}_{n+\mu}\rangle$. Seja $Z(G_{(t+1)n+\mu})$ o centro do grupo $G_{(t+1)n+\mu}$, então será assumido que

(P_1) $I^{\otimes tn} \otimes E$ e $E' \otimes I^{\otimes tn}$ comuta para todo $E, E' \in \mathcal{S}_{n+\mu}$ e t é um inteiro positivo;

(P_2) $\mathcal{S}_{(t+1)n+\mu}Z(G_{(t+1)n+\mu})/Z(G_{(t+1)n+\mu})$ é gerada por $(t+1)(n-k)$ operadores;

(P_3) $\mathcal{S}_{(t+1)n+\mu} \cap Z(G_{(t+1)n+\mu})$ contém apenas a identidade.

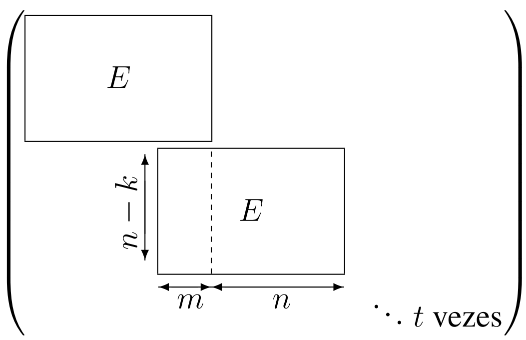
Para que essas considerações sejam melhor compreendidas, observe que a primeira delas garante que $\mathcal{S}_{(t+1)n+\mu}$ é um subgrupo abeliano de $G_{(t+1)n+\mu}$, a segunda implica que $\mathcal{S}_{(t+1)n+\mu}$ é gerado por $t+1$ versões deslocadas de $n-k$ geradores de $\mathcal{S}_{n+\mu}$ e que esses $(t+1)(n-k)$ geradores são independentes e, por fim, a terceira garante que o autoespaço de $\mathcal{S}_{(t+1)n+\mu}$ é não-trivial desde que $k < n$.

O subgrupo abeliano $\mathcal{S}_{(t+1)n+\mu}$ de $G_{(t+1)n+\mu}$ define um grupo abeliano

$$\mathcal{S}_\infty := \lim_{\longrightarrow}(\mathcal{S}_{(i+1)n+\mu}, \iota_{ij}) = \langle \iota_t(I^{\otimes tn} \otimes E)\colon t \geq 0, E \in \mathcal{S}_{n+\mu}\rangle \tag{5.10}$$

gerado pelas versões deslocadas dos elementos de $\mathcal{S}_{n+\mu}$.

$\mathcal{S}_\infty =$



. (5.11)

Definição 5.2 *Seja $\mathcal{S}_{n+\mu}$ um subgrupo abeliano de $G_{n+\mu}$ tal que as propriedades (P_1), (P_2) e (P_3) são satisfeitas. Então o autoespaço com autovalor $+1$ de $\mathcal{S}_\infty = \lim_{\longrightarrow}(\mathcal{S}_{(i+1)n+\mu}, \iota_{ij})$ em $\otimes_{i=0}^{\infty}\mathcal{H}_q$ define um código convolucional (quântico) estabilizador $\mathcal{V}_Q$ com parâmetros $[(n,k,\mu)]_q$.*

Observe que o código estabilizador somente terá taxa igual a k/n quanto t for para infinito. De fato, para t finito, tem-se $\mathcal{S}_{(t+1)n+\mu}$ define um código estabilizador com parâmetros $[[(t+1)n+\mu, (t+1)k+\mu]]_q$.

Diz-se que um erro E em G_∞ é detectável por um código convolucional estabilizador com estabilizador $\mathcal{S}_\infty$ se, e somente se, um múltiplo escalar de E está contido em $\mathcal{S}_\infty$ ou se E não comuta com algum elemento de $\mathcal{S}_\infty$. O peso wt de um elemento em G_∞ é definido como o número de componentes que compõem seu produto tensorial que são diferentes da identidade. Um código convolucional estabilizador é dito ter distância livre d_f se, e somente se, pode detectar todos os erros com peso menor que d_f, mas não detecta algum erro de peso d_f. Denote por $Z(G_\infty)$ o centro de G_∞ e por $C_{G_\infty}(\mathcal{S}_\infty)$ o centralizador de $\mathcal{S}_\infty$ em G_∞. Então, a distância livre é dada por $d_f = \min\{\text{wt}(E)\colon E \in C_{G_\infty}(\mathcal{S}_\infty) \setminus \mathcal{S}_\infty Z(G_\infty)\}$.

Um fato importante a ser comentado é que a relação de comutação entre dois elementos de G_∞ segue a mesma regra apresentada no Capítulo 3. Isso posibilita criar códigos convolucionais quânticos a partir de códigos convolucionais clássicos de maneira similar ao caso de códigos quânticos estabilizadores. Em particular, também existe o método de construção CSS para códigos convolucionais estabilizadores. Antes de apresentar tais métodos, é preciso introduzir um mapa que facilitará a conexão entre os códigos convolucionais nos paradigmas clássicos e quânticos.

Seja (β, β^q) uma base normal de $\mathbb{F}_{q^2}/\mathbb{F}_q$. Defina o mapa $\tau\colon G_\infty \to \Gamma_{q^2}$ por

$$\tau(\omega^c X(a_0)Z(b_0) \otimes X(a_1)Z(b_1) \otimes \cdots) = (\beta a_0 + \beta^q b_0, \beta a_1 + \beta^q b_1, \ldots). \tag{5.12}$$

Note que τ leva operadores de G_∞ a sequências infinitas sobre $\mathbb{F}_{q^2}$ de suporte finito. Como é mostrado no lema a seguir e na construção CSS para códigos convolucionais estabilizadores, é possível concluir que existe um código convolucional estabilizador se, e somente se, existe um código convolucional clássico com certos parâmetros. A demonstração destas afirmações é com a utilização do mapa τ e o isomorfismo σ.

Lema 5.1 *Seja $\mathcal{V}_\mathcal{Q}$ um código convolucional estabilizador com parâmetros $[(n,k,m)]_q$ e $\mathcal{S}_\infty$ seu estabilizador. Então existe um código convolucional clássico $\mathcal{V}_\mathcal{C}$ sobre $\mathbb{F}_{q^2}$ que pode ser descrito como $\mathcal{V}_\mathcal{C} = \sigma^{-1}\tau(\mathcal{S}_\infty)$. Além disso, $\mathcal{V}_\mathcal{C}$ tem parâmetros $(n, (n-k)/2; \mu \leq \lceil m/n \rceil)_{q^2}$, é gerado por $\sigma^{-1}\tau(\mathcal{S}_{n+m})$ e é auto-ortogonal, $\mathcal{V}_\mathcal{C} \subseteq \mathcal{V}_\mathcal{C}^{\perp_h}$.*

Demonstração: Como foi mostrado anteriormente, $\sigma\colon \mathbb{F}_{q^2}[D]^n \to \Gamma_{q^2}$ mapeia um elemento $\mathbf{u}(D)$ de $\mathbb{F}_{q^2}[D]^n$ para uma sequência infinita de suporte finito em Γ_{q^2}. Esse mapa é invertível, e assim, $\sigma^{-1}\tau(E) = \sigma^{-1} \circ \tau(E)$ é bem definido para qualquer $E \in G_\infty$. Como $\mathcal{S}_\infty$ é gerado pela versão deslocada de $\mathcal{S}_{n+m}$, segue que $\mathcal{V}_\mathcal{C} = \sigma^{-1}\tau(\mathcal{S}_\infty)$ é gerado pela expansão sobre $\mathbb{F}_{q^2}$ de $\sigma^{-1}\tau(\mathcal{S}_{n+m})$ e seus deslocamentos, ou seja, $D^l\sigma^{-1}\tau(\mathcal{S}_{n+m})$, em que $l \in \mathbb{N}$. Como $\mathcal{V}_\mathcal{Q}$ é um código convolucional estabilizador com parâmetros $[(n,k,m)]_q$, então $\mathcal{S}_{n+m}$ define um código estabilizador $[[n+m, k+m]]_q$ com $(n-k)$ geradores. Como os mapas σ e τ são lineares, então $\sigma^{-1}\tau(\mathcal{S}_{n+m})$ será $\mathbb{F}_{q^2}$-linear. Como $\sigma^{-1}\tau(E)$ pertence a $\mathbb{F}_{q^2}[D]^n$ e o código quântico é definido sobre $\mathcal{C}_q$, então uma matriz geradora polinomial para $\mathcal{V}_\mathcal{C}$ é uma matriz $(n-k)/2 \times n$. Como

é possível considerar que existe uma matriz geradora polinomial inversível a direita, então concluímos que $\mathcal{V}_\mathcal{C}$ é um código convolucional com parâmetros $(n, (n-k)/2; m)_{q^2}$. Desde que $\mathcal{V}_\mathcal{Q}$ é estabilizador, tem-se que $\mathcal{V}_\mathcal{C} \subseteq \mathcal{V}_\mathcal{C}^{\perp_h}$. Finalmente, observando que o grau máximo de um elemento em $\sigma^{-1}\tau(\mathcal{S}_{n+m})$ é $\lceil m/n \rceil$, por causa de σ, e junto com o Lema 14.3.8 do livro de Huffman e Pless [68], tem-se que a memória de $\sigma^{-1}\tau(S)$ deve ser $\mu \leq \lceil m/n \rceil$. ■

5.2.1 – Construção CSS

Primeiramente, a notação que será usada para um código quântico convolucional $[(n, k, \mu)]_q$ com distância livre d_f e grau δ, com $\delta = \sigma^{-1}\tau(\mathcal{S}_\infty)$, é dada por $[(n, k, \mu; \delta, d_f)]_q$. É importante salientar que a notação para os códigos convolucionais clássicos e quânticos é diferente, não apenas na apresentação de seus parâmetros mas também no significado dos mesmos.

Corolário 5.1 *[97, Corolário 144] A existência de um código convolucional quântico $\mathcal{V}_\mathcal{Q}$ com parâmetros $[(n, k, \mu; \delta, d_f)]_q$ implica na existência de um código convolucional clássico $\mathcal{V}_\mathcal{C}$ com parâmetros $(n, (n-k)/2; \delta)_{q^2}$ e $d_f = wt(\mathcal{V}_\mathcal{C}^{\perp_h} \setminus \mathcal{V}_\mathcal{C})$.*

Demonstração: Seja $\mathcal{V}_\mathcal{C} = \sigma^{-1}\tau(\mathcal{S}_\infty)$, pela relação de comutação dos elementos em G_∞ é possível concluir que $\sigma^{-1}\tau(C_{G_\infty}(\mathcal{S}_\infty)) \subseteq \mathcal{V}_\mathcal{C}^{\perp_h}$. Assim, um erro não-detectável é mapeado para um elemento em $\mathcal{V}_\mathcal{C}^{\perp_h} \setminus \mathcal{V}_\mathcal{C}$. Note que mesmo τ sendo injetivo em $\mathcal{S}_\infty$, não será em $C_{G_\infty}(\mathcal{S}_\infty)$. Entretanto, se $\mathbf{c}(D)$ pertence a $\mathcal{V}_\mathcal{C}^{\perp_h} \setminus \mathcal{V}_\mathcal{C}$, então a sobrejetividade de τ sobre $C_{G_\infty}(\mathcal{S}_\infty)$ implicará na existência de um erro E em $C_{G_\infty}(\mathcal{S}_\infty) \setminus \mathcal{S}_\infty Z(G_\infty)$ tal que $\tau(E) = \sigma(\mathbf{c}(D))$. Como τ e σ são isométricos, então E é um erro não-detectável com peso $\mathrm{wt}(\mathbf{c}(D))$. Consequentemente, pode-se concluir que $d_f = \mathrm{wt}(\mathcal{V}_\mathcal{C}^{\perp_h} \setminus \mathcal{V}_\mathcal{C})$. Combinando análise com o lema anterior, o corolário está demonstrado. ■

De forma similar ao que foi definido para o caso de códigos estabilizadores, diz-se que um código $[(n, k, \mu; \delta, d_f)]_q$ é puro se não existem erros de peso menor que d_f no estabilizador do código. O corolário anterior implica que $d_f = \mathrm{wt}(\mathcal{V}_\mathcal{C}^{\perp_h} \setminus \mathcal{V}_\mathcal{C}) = \mathrm{wt}(\mathcal{V}_\mathcal{C}^{\perp_h})$ para esse caso.

Teorema 5.1 *[97, Teorema 145] Seja $\mathcal{V}_\mathcal{C}$ um código convolucional clássico com parâmetros $(n, (n-k)/2, \delta; \mu)_{q^2}$ tal que $\mathcal{V}_\mathcal{C} \subseteq \mathcal{V}_\mathcal{C}^{\perp_h}$. Então, existe um código convolucional estabilizador com parâmetros $[(n, k, n\mu; \delta, d_f)]_q$, em que $d_f = wt(\mathcal{V}_\mathcal{C}^{\perp_h} \setminus \mathcal{V}_\mathcal{C})$. Ele será puro se $d_f = wt(\mathcal{V}_\mathcal{C}^{\perp_h})$.*

O mesmo segue para códigos convolucionais que são auto-ortogonais euclidianos.

Corolário 5.2 *[97, Corolário 146] Seja $\mathcal{V}_\mathcal{C}$ um código convolucional clássico com parâmetros $(n, (n-k)/2, \delta; \mu)_q$ tal que $\mathcal{V}_\mathcal{C} \subseteq \mathcal{V}_\mathcal{C}^{\perp}$. Então existe um código convolucional estabilizador com parâmetros $[(n, k, n\mu; \delta, d_f)]_q$, em que $d_f = wt(\mathcal{V}_\mathcal{C}^{\perp} \setminus \mathcal{V}_\mathcal{C})$. Ele será puro se $wt(\mathcal{V}_\mathcal{C}^{\perp} \setminus \mathcal{V}_\mathcal{C}) = wt(\mathcal{V}_\mathcal{C}^{\perp})$.*

5.2.2 – Construção de Códigos Convolucionais a partir de Códigos de Bloco

O método apresentado aqui é uma generalização do método de criação de códigos convolucionais a partir de códigos de bloco apresentada por Piret [58] feita por Aly, *et al.* [59].

Seja H uma matriz de verificação de paridade de um código de bloco com parâmetros $[n, k, d]_q$. Se a matriz H for dividida um $\mu + 1$ submatrizes H_i, cada uma de comprimento n, da seguinte forma

$$H = \begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ H_\mu \end{pmatrix}, \tag{5.13}$$

então, pode-se construir uma matriz polinomial dada por

$$H(D) = \tilde{H}_0 + \tilde{H}_1 D + \cdots + \tilde{H}_\mu D^\mu, \tag{5.14}$$

em que o número de linhas de $H(D)$ é igual ao número de linhas da submatriz H_j que tem o maior número de linhas entre todas as submatrizes H_i, com $0 \leq i \leq \mu$, esse número será denotado por κ. A matriz $\tilde{H}_i$ é obtida da matriz H_i pela adição de linhas nulas na parte inferior de H_i de tal forma que $\tilde{H}_i$ tenha κ linhas no total. Com essa definição, $H(D)$ gera um código convolucional. Agora será apresentado o resultado de Aly, *et al.* [59].

Teorema 5.2 *[59, Teorema 3] Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código linear com parâmetros $[n, k, d]_q$ e matriz de verificação de paridade $H \in \mathbb{F}_q^{(n-k)\times n}$. Assuma que H é particionada nas submatrizes $H_0, H_1, \ldots, H_\mu$ como na Eq. 5.13 de tal forma que $\kappa = rkH_0$ e $rkH_i \leq \kappa$, para $1 \leq i \leq \mu$. Defina a matriz polinomial*

$$H(D) = \tilde{H}_0 + \tilde{H}_1(D) + \cdots + \tilde{H}_\mu D^\mu, \tag{5.15}$$

em que $\tilde{H}_i$ é obtida da matriz H_i pelo método anteriormente descrito. Então, é possível concluir que

- *A matriz $H(D)$ é uma matriz geradora reduzida e básica;*
- *Se o código $\mathcal{C}$ contém seu dual euclidiano $\mathcal{C}^\perp$, ou seu dual hermitiano $\mathcal{C}^{\perp_h}$, então o código convolucional $\mathcal{V}_\mathcal{C} = \{\mathbf{v}(D)H(D) \colon \mathbf{v}(D) \in \mathbb{F}_q[D]^{n-k}\}$ estará contido no seu dual $\mathcal{V}_\mathcal{C}^\perp$, ou $\mathcal{V}_\mathcal{C}^{\perp_h}$, respectivamente;*
- *Sejam d_f e $d_f^\perp$ as distâncias livres de $\mathcal{V}_\mathcal{C}$ e $\mathcal{V}_\mathcal{C}^\perp$, respectivamente. Suponha que d_i é a distância mínima do código $\mathcal{C}_i = \{\mathbf{v} \in \mathbb{F}_q^n \colon \mathbf{v}\tilde{H}_i^t = 0\}$ e $d^\perp$ a distância mínima de $\mathcal{C}^\perp$. Então, as distâncias livre de $\mathcal{V}_\mathcal{C}$ e $\mathcal{V}_\mathcal{C}^\perp$ são limitadas por $d_f \geq d^\perp$ e $\min\{d_0 + d_\mu, d\} \leq d_f^\perp \leq d$, respectivamente.*

Se aplicarmos o Teorema 5.2 nos resultados apresentados no Teorema 5.1 e no Corolário 5.2, pode-se construir códigos convolucionais estabilizadores a partir de códigos de bloco clássicos. Isto é feito na Seção 5.3 para códigos algébrico-geométricos.

5.2.3 – Codificador na Forma Canônica Controladora e um Método para o Cálculo da Identidade de MacWilliams

Inicialmente, será apresentado como construir uma matriz geradora na forma controladora para o método de Piret. Essa forma é utilizada para descrever o processo de codificação no espaço de estados do sistema. Posteriormente, um método de cálculo da identidade de MacWilliams para o mesmo método também é fornecido.

Definição 5.3 *Seja* $G(D) \in \mathbb{F}_q[D]^{k\times n}$ *uma matriz geradora básica e minimal com* constraint length $\nu_1, \nu_2, \ldots, \nu_r > 0 = \nu_{r+1} = \cdots = \nu_k$ *e* $\delta = \sum_{i=1}^{k} \nu_i$. *Considere que* $G(D)$ *tem linhas* $g_i = \sum_{j=0}^{\nu_i} g_{ij} D^j$, $i = 1, \ldots, k$, *com* $g_{ij} \in \mathbb{F}_q^n$. *Para* $i = 1, \ldots, r$, *define-se as matrizes*

$$A_i = \begin{bmatrix} 0 & 1 & & \\ & & \ddots & \\ & & & 1 \\ & & & 0 \end{bmatrix} \in \mathbb{F}_q^{\nu_i \times \nu_i}, \tag{5.16}$$

$$B_i = \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix} \in \mathbb{F}_q^{\nu_i}, \tag{5.17}$$

$$C_i = \begin{bmatrix} g_{i1} \\ g_{i2} \\ \vdots \\ g_{i\gamma_i} \end{bmatrix} \in \mathbb{F}_q^{\nu_i \times n}. \tag{5.18}$$

Então, a forma controladora de $G(D)$ *é definida como a quádrupla de matrizes* $(A, B, C, E) \in \mathbb{F}_q^{\delta\times\delta} \times \mathbb{F}_q^{k\times\delta} \times \mathbb{F}_q^{\delta\times n} \times \mathbb{F}_q^{k\times n}$, *com*

$$A = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{bmatrix},\ B = \begin{bmatrix} \overline{B} \\ 0 \end{bmatrix},\ C = \begin{bmatrix} C_1 \\ \vdots \\ C_r \end{bmatrix},\ E = \begin{bmatrix} g_{10} \\ \vdots \\ g_{k0} \end{bmatrix} = G(0). \tag{5.19}$$

em que

$$\overline{B} = \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_r \end{bmatrix}. \tag{5.20}$$

Proposição 5.1 *[98, Proposição 2.1 e Teorema 2.3] Sabe-se que* $G(D) = B(D^{-1}I - A)^{-1}C + E$. *Assim, se* $\mathbf{v}(D) = \mathbf{u}(D)G(D)$, *com* $\mathbf{u}(D) = \sum_i \mathbf{u}_i D^i$ *e* $\mathbf{v}(D) = \sum_j \mathbf{v}_j D^j$, *então segue que*

$$\begin{cases} \mathbf{x}_{t+1} & = \mathbf{x}_t A + \mathbf{u}_t B \\ \mathbf{v}_t & = \mathbf{x}_t C + \mathbf{u}_t E, \end{cases} \tag{5.21}$$

para todo $t \geq 0$, *com* $\mathbf{x}_0 = \mathbf{0}$.

Aplicando a forma canônica controlada de $G(D)$ para o código convolucional mostrado no Teorema 5.2, e assumindo que o código convolucional tem memória unitária, então o seguinte segue:

Proposição 5.2 *Seja* $G(D) \in \mathbb{F}_q[D]^{k\times n}$ *uma matriz básica e minimal do Teorema 5.2 com* $\mu = 1$. *Então a forma canônica controlada de* $G(D)$ *é definida pela quádrupla de matrizes* $(A, B, C, E) \in \mathbb{F}_q^{rkH_1\times rkH_1} \times \mathbb{F}_q^{\kappa\times rkH_1} \times \mathbb{F}_q^{rkH_1\times n} \times \mathbb{F}_q^{\kappa\times n}$ *como sendo*

$$A = \begin{bmatrix} 0 & & \\ & \ddots & \\ & & 0 \end{bmatrix},\ B = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & 0 \\ & & \vdots \\ & & 0 \end{bmatrix},\ C = H_1,\ E = H_0. \tag{5.22}$$

A identidade de MacWilliams para códigos convolucionais é apresentada em diversos trabalhos [98–100]. Como será mostrado, a Proposição 5.2 pode ser utilizada para encontrar a identidade de MacWilliams para o código convolucional de memória unitária do Teorema 5.2. Primeiramente, será definido a matriz de peso adjacente (WAM, do inglês *Weight Adjacency Matrix*) e a matriz P-MacWilliams de um código convolucional.

Definição 5.4 *Seja* $\mathcal{F} := \mathbb{F}_q^\delta \times \mathbb{F}_q^\delta$ *e* $\mathbb{F}_q[W]_{\leq n}$ *o espaço de polinômios sobre* $\mathbb{F}_q$ *de grau no máximo* n. *Uma WAM* $\Lambda(M) = (\lambda_{X,Y}) \in \mathbb{F}_q[W]^{q^\delta \times q^\delta}$ *de um código convolucional com forma canônica controlada dada pela quádrupla* (A, B, C, E) *é definida pela matriz indexada por* $(X, Y) \in \mathcal{F}$ *com as entradas dadas por*

$$\lambda_{X,Y} := wt(\{XC + \mathbf{u}E | \mathbf{u} \in \mathbb{F}_q^k \text{ e } Y = XA + \mathbf{u}B\}) \tag{5.23}$$

em $\mathbb{F}_q[W]_{\leq n}$, *com* $wt(\mathbf{d})$ *sendo o peso de enumeração de um* $\mathbf{d} \subseteq \mathbb{F}_q^n$. *Um par de estados* $(X, Y) \in \mathcal{F}$ *é chamado de conectado se* $\lambda_{X,Y} \neq 0$; *caso contrário é chamado de desconectado. O conjunto de todos os pares conectados é denotado por* $\Delta \subseteq \mathcal{F}$.

Definição 5.5 *Sejam q uma potência de p, com p sendo primo, e $\zeta \in \mathbb{F}_q^*$ uma p-ésima raiz primitiva da unidade. Para $P \in GL_\delta(\mathbb{F}_q)$, com $\delta \in \mathbb{N}_0$ e $GL_\delta(\mathbb{F}_q)$ sendo o grupo linear geral de grau δ sobre $\mathbb{F}_q$, definimos a matriz P-MacWilliams como*

$$\mathcal{H}(P) := q^{\frac{-\delta}{2}}(\zeta^{\tau(\beta(X,YP^T))})_{(X,Y)\in\mathcal{F}} \in \mathbb{F}_q^{q^\delta \times q^\delta}, \tag{5.24}$$

com τ sendo o traço usual e β a forma canônica bilinear sobre $\mathbb{F}_q^\delta$.

Devido à simplicidade da forma canônica controlada apresentada na Proposição 5.2, para mostrar que dois pares são conectados, é suficiente mostrar que existe um $\mathbf{u} \in \mathbb{F}_q^k$ tal que $Y = \mathbf{u}B$.

Teorema 5.3 *Seja $\mathbf{H}\colon \mathbb{F}_q[W]_{\leq n} \to \mathbb{F}_q[W]_{\leq n}$ a transformação de MacWilliams e $\mathcal{H} = \mathcal{H}(I) \in \mathbb{F}_q^{q^\delta \times q^\delta}$ a matriz P-MacWilliams matriz da identidade. Se a forma canônica controlada do código dual $\mathcal{V}_\mathcal{C}^\perp$ é dada pela quádrupla de matrizes $(\hat{A}, \hat{B}, \hat{C}, \hat{E})$, então $P := -\hat{C}E^tB \in GL_\delta(\mathbb{F})$, e, para todo $(X, Y) \in \mathcal{F}$, tem-se*

$$\hat{\lambda}_{X,Y} = q^{-k}\mathbf{H}((\mathcal{H}\Lambda^t\mathcal{H}^{-1})_{XP,YP}), \tag{5.25}$$

com Λ sendo a WAM do código convolucional $\mathcal{V}_\mathcal{C}$.

Demonstração: Segue da aplicação do Teorema V.10 do trabalho de Luerssen [99] e da Proposição 5.2. ∎

5.2.4 – Limitante de Singleton para Códigos Quânticos Convolucionais

Primeiramente será mostrado o limitante de Singleton generalizado para códigos convolucionais clássicos, devido a Smarandache, *et al.* [101]. Como será visto, a obtenção do limitante de Singleton para códigos convolucionais estabilizadores puros é a mera utilização do resultado anterior.

Lema 5.2 *[101, Teorema 2.4](Limitante de Singleton Generalizado) Seja $\mathcal{V}_\mathcal{C}$ um código convolucional com parâmetros $(n, k, m; \delta, d_f)_q$. Então a distância livre de $\mathcal{V}_\mathcal{C}$ é limitada superiormente por*

$$d_f \leq (n-k)\Big(\Big\lceil\frac{\delta}{k}\Big\rceil + 1\Big) + \delta + 1. \tag{5.26}$$

Proposição 5.3 *(Limitante de Singleton Quântico Generalizado) Seja $\mathcal{V}_\mathcal{Q}$ um código convolucional com parâmetros $[(n, k, m; \delta, d_f)]_q$. Com isso, tem-se que a distância livre de $\mathcal{V}_\mathcal{Q}$ é limitada superiormente por*

$$d_f \leq \frac{n-k}{2}\Big(\Big\lceil \frac{2\delta}{n+k} \Big\rceil + 1\Big) + \delta + 1. \tag{5.27}$$

Demonstração: Pelo Corolário 5.1, existe um código convolucional clássico $\mathcal{V}_{\mathcal{C}}$ com parâmetros $(n, (n-k)/2, \delta)_{q^2}$ e $d_f = \text{wt}(\mathcal{V}_{\mathcal{C}}^{\perp_h} \setminus \mathcal{V}_{\mathcal{C}}) = \text{wt}(\mathcal{V}_{\mathcal{C}}^{\perp_h})$, pela hipótese inicial de pureza. Como é mostrado no Teorema 2.66 em [96], os códigos duais $\mathcal{V}_{\mathcal{C}}^{\perp}$ e $\mathcal{V}_{\mathcal{C}}^{\perp_h}$ possuem o mesmo grau. Assim, $\mathcal{V}_{\mathcal{C}}^{\perp_h}$ é um código convolucional com parâmetros $(n, (n+k)/2, \delta)_{q^2}$ e distância livre d_f. Pelo limitante de Singleton generalizado do Lema 5.2, tem-se que

$$d_f \leq (n-(n+k)/2)\Big(\Big\lceil \frac{\delta}{(n+k)/2} \Big\rceil + 1\Big) + \delta + 1. \tag{5.28}$$

■

A demonstração da Proposição 5.3 também pode ser encontrada na Ref. [97].

5.3 – Códigos Convolucionais Clássicos e Quânticos Derivados de Códigos AG

Nesta seção são construídas famílias de novos códigos convolucionais clássicos e quânticos. Os códigos convolucionais clássicos são derivados de códigos AG. Além disso, mais famílias são obtidas por meio de puncionamento, extensão, expansão e pelo produto direto de códigos AG. Adicionalmente, utilizando-se dos novos códigos convolucionais clássicos construídos aqui, obtêm-se novos códigos convolucionais quânticos. Os parâmetros desses códigos são bons no sentido que sua distância livre difere do limitante de Singleton por um fator linearmente proporcional ao gênero da curva utilizada na construção dos códigos AG. Mais precisamente, no caso clássico tem-se uma família com códigos cujas distâncias mínimas diferem do limitante de Singleton de, no máximo, duas unidades. Com respeito ao caso quântico, é construído uma família de códigos MDS. Todos os resultados dessa seção são de co-autoria do autor desta tese e estão contidos na Ref. [62].

5.3.1 – Códigos Convolucionais Clássicos derivados de AG

É apresentado aqui um método geral para a construção de códigos convolucionais advindos de códigos AG. Mais precisamente, obtêm-se códigos convolucionais com bons parâmetros, os quais têm matrizes geradoras derivadas do código AG $C_{\Omega}(D, G)$. O primeiro resultado é apresentado a seguir:

Teorema 5.4 *Seja $F/\mathbb{F}_q$ um corpo de funções de gênero g. Considere o código AG $C_{\Omega}(D, G)$ como no Teorema 2.5. Então existe um código convolucional de memória unitária com parâmetros $(n, k-l, l; 1, d_f \geq d)_q$, em que $l \leq k/2$, $k = \ell(G) - \ell(G-D)$ e $d \geq n - \deg(G)$.*

Demonstração: Considere o código AG $C_\Omega(D,G)$ definido sobre $F/\mathbb{F}_q$ com matriz verificado de paridade dada por

$$H_\Omega = \begin{bmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \cdots & x_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{bmatrix}, \tag{5.29}$$

em que $\{x_1,\ldots,x_k\}$ é uma base de $\mathcal{L}(G)$. Seja $C_\mathcal{L}(D,G)$ o código dual (euclidiano) do código $C_\Omega(D,G)$. Uma matriz geradora de $C_\mathcal{L}(D,G)$ é a matriz H_Ω. Sabe-se que $C_\mathcal{L}(D,G)$ é um código AG com parâmetros $[n, k=\ell(G)-\ell(G-D), d\geq n-\deg(G)]_q$, em que $n=\deg(D)$. Defina um código convolucional com matriz gerado dada por

$$G(D) = H_0 + \widetilde{H}_1 D,$$

em que H_0 é a submatriz de H_Ω consistindo das primeiras $k-l$ linhas e $\widetilde{H}_1$ é a matriz consistindo das últimas l linhas de H_Ω com adição de linhas nulas abaixo, de tal forma que a matriz $\widetilde{H}_1$ tenha $k-l$ linhas no total. Por hipótese, segue que $\mathrm{rk}\, H_0 \geq \mathrm{rk}\, \widetilde{H}_1$. Do Teorema 5.2, a matriz $M(D)$ é uma matriz básica reduzida. O código convolucional gerado por $M(D)$ é um código de memória unitária com dimensão $k-l$, grau l e distância livre d_f. Do Teorema 5.2, segue que $d_f \geq d$. Assim, existe um código convolucional com parâmetros $(n, k-l, l; 1, d_f)$, em que $d_f \geq d$. ■

Corolário 5.3 *Assuma que todas as hipóteses do Teorema 5.4 sejam satisfeitas. Se* $2g-2 < \deg(G) < n$*, então existe um código convolucional com parâmetros* $(n, k-l, l; 1, d_f \geq d)_q$*, em que* $n=\deg(D)$*,* $k=\deg(G)+1-g$*,* $l \leq k/2$ *e* $d \geq n-\deg(G)$*.*

Demonstração: Seja G o divisor utilizado para construir o código AG $\mathcal{C}_\Omega(D,G)$ com $2g-2 < \deg(G) < n$. Utilizando os resultados da Subseção 2.2.2 e o Teorema 5.4, o resultado segue. ■

Corolário 5.4 *Assuma que todas as hipóteses do Teorema 5.4 sejam satisfeitas. Então, existe um código convolucional com parâmetros* $(n, k-1, 1; 1, d_f \geq d)_q$*, em que* $k=\deg(G)+1-g$ *e* $d \geq n-\deg(G)$*.*

Demonstração: É suficiente considerar $l=1$ no Corolário 5.3. ■

Observação 5.1 *Pelo Corolário 5.4, aplicando o limitante de Singleton generalizado, segue que a distância livre do código convolucional construído é limitado por* $d_f \leq n-k+3$ *(em que* n *e* k *são os parâmetros de* $C_\mathcal{L}(D,G)$*). Além disso,* $d_f \geq n-deg(G) = n-(k+g-1) = n-k+1-g$*; então, tem-se que a distância livre* d_f *é limitada por* $n-k+1-g \leq d_f \leq n-k+3$*. Em particular, para corpos de funções* $F/\mathbb{F}_q$ *com* $g=0$*, o novo código convolucional tem distância limitado por* $n-k+1 \leq d_f \leq n-k+3$*. Nesse caso, esses códigos são* almost

near *MDS ou* near *MDS ou MDS. Em outras palavras, o Singleton* defect *é no máximo duas unidades. Consequentemente, tais códigos convolucionais tem bons parâmetros.*

Corolário 5.5 *Seja* $F = \mathbb{F}_q(z)$ *o corpo de funções racionais. Então, existe um código convolucional com parâmetros* $(q, r, 1; 1, d_f \geq q - m)_q$*, em que* $1 \leq r \leq q - 1$.

Demonstração: Sejam $\beta \in \mathbb{F}_q$, P_β o zero de $z - \beta$ e P_∞ o polo de z em $\mathbb{F}_q(z)$. Considere o código AG $C_{\mathcal{L}}(D, G)$ com $D = \sum_{\beta \in \mathbb{F}_q} P_\beta$ e $G = rP_\infty$, em que $1 \leq r \leq q - 1$. Sabe-se que $C_{\mathcal{L}}(D, G)$ tem parâmetros $n = q$, $k = r + 1$ e $d \geq n - r$. Aplicando o Corolário 5.4 ao código AG $C_{\mathcal{L}}(D, G)^{\perp}$, obtêm-se um código convolucional com os parâmetros desejados. ∎

É mostrado na Tabela 5.1 alguns exemplos de códigos convolucionais derivados do Corolário 5.5.

Tabela 5.1 – Exemplos de novos códigos convolucionais *almost near* MDS ou *near* MDS ou MDS

Novos Códigos Convolucionais – Corolário 5.5 $(q, r, 1; 1, d_f \geq q - r)_q$ $1 \leq r \leq q - 1$
Exemplos
$(n, k, \gamma; m, d_f)$
$(8, 2, 1; 1, d_f \geq 6)_8$
$(37, 17, 1; 1, d_f \geq 20)_{37}$
$(71, 68, 1; 1, d_f \geq 3)_{71}$
$(128, 64, 1; 1, d_f \geq 64)_{128}$
$(256, 128, 1; 1, d_f \geq 128)_{256}$

Teorema 5.5 *Seja* $q = 2^t$*, em que* $t \geq 1$ *é um inteiro. Então existe um código convolucional com parâmetros* $(2q^2, r - q/2, 1; 1, d_f \geq 2q^2 - r)_{q^2}$*, em que* $q - 2 < r < 2q^2$.

Demonstração: O resultado segue do fato de que do corpo de função $F = \mathbb{F}_q(x, y)$, definido pela equação $y^2 + y = x^{q+1}$, é possível construir um código AG com parâmetros $[2q^2, r - q/2 + 1, d \geq 2q^2 - r]_{q^2}$, com $q - 2 < r < 2q^2$ (veja os trabalhos de Stichtenoth e Jin [102, 103]). ∎

A utilização de códigos AG na construção de códigos convolucionais implica na criação de um problema na análise comparativa entre os códigos criados e os códigos da literatura. O motivo disso é a faixa de valores que os novos códigos convolucionais possui. De fato, a maioria dos novos códigos convolucionais não tem contra-partida na literatura (veja a Tabela 5.2). Mesmo assim, é feito uma comparação para alguns códigos (veja a Tabela 5.2). Os códigos mostrados na Tabela 5.2 são obtidos dos Teoremas 5.5 e 5.6.

Considere o novo código convolucional com parâmetros $(32, 15, 1; 1, d_f \geq 15)_{16}$; esse código tem parâmetros melhores que o código the $(32, 15, 10; \mu, d_f \geq 9)_3$ mostrado na Ref. [104], no sentindo que eles têm o mesmo comprimento e dimensão mas tem distância

Tabela 5.2 – Comparação dos códigos convolucionais criados com os da literatura

Novos Códigos Convolucionais Teoremas 5.5 e 5.6	Códigos na Ref. [104]	Códigos na Ref. [59]
$(32, 15, 1; 1, d_f \geq 15)_{16}$	$(32, 15, 10; \mu, d_f \geq 9)_3$	$(32, 16, \gamma; 1, d_f \geq 5)_3$
$(32, 1, 1; 1, d_f \geq 29)_{16}$	–	–
$(128, 64, 1; 1, d_f \geq 60)_{64}$	$(128, 64, 35; \mu, d_f \geq 17)_7$	$(128, 64, \gamma; 1, d_f \geq 8)_7$
$(176, 64, 1; 1, d_f \geq 105)_{64}$	–	–
$(512, 128, 1; 1, d_f \geq 376)_{256}$	–	–
$(512, 256, 1; 1, d_f \geq 248)_{256}$	–	–
$(2048, 1024, 1; 1, d_f \geq 1008)_{1024}$	–	–
$(3008, 1024, 1; 1, d_f \geq 1953)_{1024}$	–	–

livre maior. Entretanto, o novo código convolucional é definido sobre um alfabeto maior. Mesmo podendo ser impróprio, foi necessário negligenciar este fato para poder fazer a análise comparativa do código construído. Além disso, adotando o mesmo critério de comparação, é possível ver que o novo código convolucional com parâmetros $(128, 64, 1; 1, d_f \geq 60)_{64}$ é melhor que os códigos $(128, 64, 35; \mu, d_f \geq 17)_7$, apresentado na Ref. [104], e $(128, 64, \gamma; 1, d_f \geq 8)_7$, presente na Ref. [59]. Consequentemente, concluímos que para o mesmo comprimento e dimensão, os novos códigos criados têm distância livre maiores que as dos códigos presentes nas Refs. [59] e [104]. Este ganho vem com um custo: os novos códigos convolucionais são definidos sobre corpos finitos de cardinalidade maior, o que implica em uma maior complexidade para os processos de codição de decodificação, uma vez que essas operações são feitas sobre estes corpos finitos.

Teorema 5.6 *Seja $q = 2^t$, em que $t \geq 1$ é um inteiro ímpar. Então, existe um código convolucional $(3q^2 - 2q, r - q + 1, 1; 1, d_f \geq 3q^2 - 2q - r)_{q^2}$, em que $2q - 4 < r < 3q^2 - 2q$.*

Demonstração: Seja F o corpo de função sobre $\mathbb{F}_{q^2}$ definido pela equação

$$y^q + y = x^3.$$

O gênero de F é igual a $g = q - 1$ e o número de lugares racionais é igual a $3q^2 - 2q + 1$ (veja o trabalho de Jin [103]). Seja $D = P_1 + \ldots + P_n$ um divisor, $n = 3q^2 - 2q$ e $G = rP_{3q^2-2q+1} = mP_\infty$, com $2g - 2 < r < n$ e tendo $\{P_1, \cdots, P_{3q^2-2q+1}\}$ como o conjunto de lugares racionais dois a dois distintos. Considere o código AG $C_{\mathcal{L}}(D, G)$; os parâmetros de $C_{\mathcal{L}}(D, G)$ são $[3q^2 - 2q, r + 1 - g, d \geq n - r]_q$, em que $2q - 4 < r < 3q^2 - 2q$. Aplicando o Corolário 5.5, obtêm-se um código convolucional com parâmetros $(3q^2-2q, r-q+1, 1; 1, d_f \geq 3q^2-2q-r)_q$, em que $2q - 4 < r < 3q^2 - 2q$. ■

Foi aplicado o Teorema 5.4 às curvas utilizadas nos Teoremas 5.5 e 5.6 pois elas são curvas maximais, i.e., são curvas com o número de pontos racionais igual a $N = q + 1 + 2g\sqrt{q}$ e, além disso, elas têm gênero proporcional a q. Consequentemente, os seus correspondentes códigos convolucionais têm *Singleton defect* também proporcional a q. Entretanto, outras curvas

poderiam ser utilizadas, tais como a curva Suzuki ou Ree [105, 106], isso não foi feito pois elas possuem gênero proporcional a potências maiores de q, fazendo com que o *Singleton defect* dos códigos convolucionais construídos com elas sejam maiores que o dos códigos convolucionais nos Teoremas 5.5 e 5.6 para o mesmo q.

Os próximos resultados são derivados do Teorema 5.4 quando é considerado puncionamento, extensão, expansão e produto dos códigos AG.

Teorema 5.7 *Assuma a notação do Teorema 5.4 com* $2g-2 < \deg(G) < n-1$ *e suponha que as palavras-código de* $C_{\mathcal{L}}(D,G)$ *com peso mínimo tenham a* j*-ésima coordenada nula. Então há um código convolucional com parâmetros* $(n-1, k-l, l; 1, d_f)_q$*, em que* $d_f \geq d$*,* $k = \deg(G)+1-g$*,* $l \leq k/2$ *e* $d \geq n - \deg(G)$*.*

Demonstração: Seja $C_{\mathcal{L}}(D,G)$ o código AG com parâmetros $[n,k,d]_q$ considerado no Teorema 5.4, em que $D = P_1 + \cdots + P_n$. Agora, assuma que $D' = D - P_j$. Define-se o código puncionado como sendo o código $C_{\mathcal{L}}(D',G)$ derivado de $C_{\mathcal{L}}(D,G)$, o qual também é um código AG (veja o trabalho de Pellikaan, *et al.* [107]). Note que o suporte de D' e G são disjuntos, i.e., a definição de $C_{\mathcal{L}}(D',G)$ faz sentido. Da hipótese (veja [68, Teorema 1.5.1, pg. 13]), $C_{\mathcal{L}}(D',G)$ tem parâmetros $[n-1,k,d]_q$. Aplicando a mesma construção do Teorema 5.4, é possível obter um código convolucional $\mathcal{V}_{\mathcal{C}}$ com parâmetros $(n-1, k-l, l; 1, d_f)_q$, em que $d_f \geq d$. Uma matriz geradora $G^*(D)$ para $\mathcal{V}_{\mathcal{C}}$ é dada por

$$G^*(D) = \begin{bmatrix} x_1(P_1)+x_{k-l+1}(P_1)D & \cdots & x_1(P_{j-1})+x_{k-l+1}(P_{j-1})D & x_1(P_{j+1})+x_{k-l+1}(P_{j+1})D & \cdots & x_1(P_n)+x_{k-l+1}(P_n)D \\ x_2(P_1)+x_{k-l+2}(P_1)D & \cdots & x_2(P_{j-1})+x_{k-l+2}(P_{j-1})D & x_2(P_{j+1})+x_{k-l+2}(P_{j+1})D & \cdots & x_2(P_n)+x_{k-l+2}(P_n)D \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ x_l(P_1)+x_k(P_1)D & \cdots & x_l(P_{j-1})+x_k(P_{j-1})D & x_l(P_{j+1})+x_k(P_{j+1})D & \cdots & x_l(P_n)+x_k(P_n)D \\ x_{l+1}(P_1) & \cdots & x_{l+1}(P_{j-1}) & x_{l+1}(P_{j+1}) & \cdots & x_{l+1}(P_n) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ x_{k-l}(P_1) & \cdots & x_{k-l}(P_{j-1}) & x_{k-l}(P_{j+1}) & \cdots & x_{k-l}(P_n) \end{bmatrix}.$$

■

Teorema 5.8 *Assuma a mesma notação do Teorema 5.4. Então, existe um código convolucional* $(n+1, k-l, l; 1, d_f \geq d^e)_q$*, em que* $d^e = d$ *ou* $d^e = d+1$*, uma vez que* $k = \deg(G)+1-g$*,* $l \leq k/2$ *e* $d \geq n - \deg(G)$*.*

Demonstração: Considere $C_{\mathcal{L}}(D,G)$ como sendo o código AG $[n,k,d]_q$ considerado no Teorema 5.4. Construa um novo código $C^e_{\mathcal{L}}(D,G)$ pela extensão do código $C_{\mathcal{L}}(D,G)$. Esse novo código tem parâmetros $[n+1,k,d^e]_q$, com $d^e = d$ ou $d^e = d+1$. Aplicando o método utilizado na demonstração do Teorema 5.4, obtêm-se um código convolucional $(n+1, k-l, l; 1, d_f \geq d^e)_q$ e, assim, o resultado segue. ■

Teorema 5.9 *Seja* $F/\mathbb{F}_{q^m}$ *um corpo de funções com gênero* g *e* $n+1$ *lugares racionais. Sejam* $P_1, \ldots, P_n, P_\infty$ *lugares racionais dois-a-dois distintos. Adote* $D = P_1 + \cdots + P_n$*,*

$G = \deg(G)P_\infty$ *e* $C_{\mathcal{L}}(D,G)$ *o código AG derivado destes divisores, com* $2g-2 < \deg(G) < n$. *Então, existe um código convolucional* $(mn, mk-l, l; 1, d_f \geq d)_q$, *em que* $k = \deg(G)+1-g$, $l \leq k/2$ *e* $d \geq n - \deg(G)$.

Demonstração: Considere que $C_{\mathcal{L}}(D,G)$ é um código AG sobre $\mathbb{F}_{q^m}$, com parâmetros $[n,k,d]_{q^m}$. Seja $B = \{b_1, \ldots, b_m\}$ uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Expandindo o código $C_{\mathcal{L}}(D,G)$ com respeito a base B, gera-se o código $B(C_{\mathcal{L}}(D,G))$ sobre $\mathbb{F}_q$ com parâmetros $[mn, mk, d^* \geq d]_q$. Uma matriz verificadora de paridade H de $[B(C_{\mathcal{L}}(D,G))]^\perp$ é uma matriz geradora de $B(C_{\mathcal{L}}(D,G))$.

Seja V o código convolucional gerado pela matriz mínima e básica

$$G(D) = H_0 + \tilde{H}_1 D, \tag{5.30}$$

em que H_0 é uma submatriz de H consistindo das primeiras $mk-l$ linhas de H e $\tilde{H}_1$ é a matriz consistindo das últimas linhas de H e mais $mk-2l$ linhas nulas. Assim, constrói-se um código convolucional $\mathcal{V}_{\mathcal{C}}$ que tem parâmetros $(mn, mk-l, l; 1, d_f \geq d)_q$, como desejado. ∎

Teorema 5.10 *Assuma que a mesma notação do Teorema 5.4. Então existe um código convolucional* $(n^2, k^2-l, l; 1, d_f \geq d^2)_q$, *com* $k = \deg(G)+1-g$, $l \leq k/2$ *e* $d \geq n - \deg(G)$.

Demonstração: Seja $C_{\mathcal{L}}(D,G)$ o código convolucional do Teorema 5.4 sobre $\mathbb{F}_q$, com parâmetros $[n,k,d]_q$. Construa o produto de código $(C_{\mathcal{L}}(D,G) \otimes C_{\mathcal{L}}(D,G))$. Esse código tem parâmetros $[n^2, k^2, d^2]_q$. De forma similar à demonstração do Teorema 5.4, é possível construir um código convolucional $(n^2, k^2-l, l; 1, d_f \geq d^2)$, como desejado. ∎

5.3.2 – Códigos Convolucionais Quânticos derivados de AG

Nesta subseção são construídas várias famílias de códigos convolucionais quânticos (QCC, do inglês *quantum convolutional codes*) derivados de códigos algébrico-geométricos. Em particular, as famílias de códigos convolucionais quânticos construídas pelo Teorema 5.12 são MDS.

Teorema 5.11 *Seja* $C_\Omega(D,G)$ *um código AG auto-ortogonal com parâmetros* $[n,k,d]_q$ *e com matriz verificadora de paridade* M. *Seguindo o método de construção do Teorema 5.4, sendo* d_1 *a distância mínima do código com matriz verificadora de paridade* $\tilde{M}_1$ *e* $C_{\mathcal{L}}(D,G')$ *um código AG gerado pelo divisor* G', *em que* $\dim(\mathcal{L}(G')) = k-l$, *então existe um código convolucional quântico derivado de* $C_{\mathcal{L}}(D,G)$ *com parâmetros* $[(n, n-2(k-l), 1; l, d_f)]_q$, *em que* $d_f \geq \min\{d(C_{\mathcal{L}}(D,G'))+d_1, d(C_\Omega(D,G))\}$. *Em particular, se* $2g-2 \leq \deg(G) \leq n/2+g$ *então* $d_f \geq \deg(G) - (2g-2)$.

Demonstração: Seja $H(Q) = \{0 = \rho_1 < \rho_2 < \ldots\}$ o semigrupo de Weierstrass de Q. Construa a *base de Weierstrass* do espaço de Riemann-Roch $\mathcal{L}(rQ)$, $r \geq 0$, com dimensão

$\ell(rQ) = k$ da seguinte forma. O primeiro elemento da base de $\mathcal{L}(rQ)$ é um vetor $x_1 \in F/\mathbb{F}_q$ tal que $\nu_Q(x_1) = \rho_1 = 0$. A escolha do segundo vetor segue a mesma ideia; i.e., tome $x_2 \in F/\mathbb{F}_q$ com $\nu_Q(x_2) = \rho_2$, e assim por diante. Por construção, segue que cada um desses vetores tem valorização diferente no lugar Q, isso implica que o conjunto $\{x_1, x_2, \ldots, x_k\}$ contém k vetores linearmente independentes. Além disso, esses vetores pertencem ao espaço $\mathcal{L}(rQ)$. Em outras palavras, $\{x_1, x_2, \ldots, x_k\}$ é uma base de $\mathcal{L}(rQ)$ e será chamada de *base de Weierstrass* de $\mathcal{L}(rQ)$. Assim, o conjunto $\{x_1, x_2, \ldots, x_{k-1}\}$ também é uma base do espaço de Riemann-Roch $\mathcal{L}(r'Q)$, com $\mathcal{L}(r'Q) \subset \mathcal{L}(rQ)$ e $\ell(r'Q) = k - 1$. Agora é possível construir o código convolucional quântico e calcular seus parâmetros.

Seja $C_{\mathcal{L}}(D, G)$ um código AG auto-ortogonal com parâmetros $[n, k, d]_q$, tendo matriz geradora M com linhas $\{m_1, \ldots, m_k\}$. Seja $\{x_1, \ldots, x_k\}$ a base de Weierstrass de $\mathcal{L}(G)$ apresentada anteriormente. Aplicando o Teorema 5.4, o código convolucional correspondente também será auto-ortogonal e tem parâmetros $(n, k - l, l; 1, d_f \geq d(C_{\mathcal{L}}(D, G)))_q$. Aplicando o Teorema 5.1 para este código, e como os vetores $\{x_1, \ldots, x_{k-l}\}$ geram outro espaço de Riemann-Roch associado ao divisor $G' = \rho_{k-l}Q$, sendo ρ_{k-l} o $(k - l)$-ésimo elemento de $H(Q)$, então é possível construir um código convolucional quântico com parâmetros $[(n, n - 2(k - l), 1; l, d_f)]$, com $d_f \geq \min\{d(C_\Omega(D, G')) + d_1, d(C_\Omega(D, G))\}$. ■

Observação 5.2 *Note que aplicando o limitante de Singleton quântico generalizado no Teorema 5.11 segue que a distância livre do código convolucional quântico construído aqui é limitado superiormente por* $d_f \leq \deg(G) - g + 2$. *Além disso,* $d_f \geq \deg(G) - 2g + 2$*; então, a distância livre* d_f *é limitada por* $\deg(G) - 2g + 2 \leq d_f \leq \deg(G) - g + 2$. *Em outras palavras, o* Singleton defect *dos novos QCC's é no máximo igual ao gênero da curva utilizada para construir o código AG (clássico). Em particular, para corpos de funções* $F/\mathbb{F}_q$ *com* $g = 0$*, os novos códigos convolucionais são MDS.*

Teorema 5.12 *Assuma todas as hipóteses do Teorema 5.11 e seja* $F = \mathbb{F}_q(z)$ *é um corpo de funções racionais. Então, existe um QCC MDS com parâmetros* $[(q, q - 2r, 1; 1, d_f)]_q$*, com* $1 \leq r \leq (q - 2)/2$ *e* $d_f = r + 2$.

Demonstração: Prosseguindo da mesma forma que no Corolário 5.5, o corpo de funções racionais é utilizado para construir um código convolucional. Para $r \leq (q - 2)/2$ tem-se que os códigos AG construídos desse corpo de funções é auto-ortogonal (veja o livro de Stichtenoth [71]); assim, o código convolucional derivado desse código também será auto-ortogonal. Aplicando o Teorema 5.11, obtêm-se o código desejado. Note que os parâmetros desses códigos atingem o limitante de Singleton quântico generalizado e, consequentemente, esse código é MDS. ■

É mostrado na Tabela 5.3 alguns exemplos de códigos convolucionais estabilizadores derivados do Teorema 5.12. Uma vez que esses códigos são MDS, pode-se concluir que têm *Singleton defect* igual a zero e, consequentemente, são ótimos.

Tabela 5.3 – Exemplo de novos códigos convolucionais estabilizadores MDS

Novos Códigos Convolucionais Estabilizadores – Teorema 5.12 $[(q, q-2r, 1; 1, d_f = r+2)]_q$ $1 \leq r \leq (q-2)/2$
Exemplos
$[(4, 2, 1; 1, d_f = 3)]_4$
$[(5, 3, 1; 1, d_f = 3)]_5$
$[(7, 3, 1; 1, d_f = 4)]_7$
$[(8, 4, 1; 1, d_f = 4)]_8$
$[(9, 3, 1; 1, d_f = 5)]_9$
$[(13, 3, 1; 1, d_f = 7)]_{13}$
$[(17, 11, 1; 1, d_f = 5)]_{17}$

Se restringirmos os parâmetros dos códigos AG usados na construção dos códigos convolucionais clássicos do Teorema 5.5 e Teorema 5.6 para termos códigos convolucionais auto-duais e aplicarmos o Teorema 5.11, é possível criar novas famílias de códigos convolucionais estabilizadores. Isso é feito nos Teoremas 5.13 e 5.13. Exemplos são mostrados na Tabela 5.4.

Teorema 5.13 *Seja* $(2q^2, r - q/2, 1; 1, d_f \geq 2q^2 - r)_{q^2}$ *o código convolucional construído no Teorema 5.5, com* $q = 2^t$ *e* $t \geq 3$*. Se* $q - 2 \leq r \leq q^2 + q/2 - 1$*, então existe um código QCC com parâmetros* $[(2q^2, 2q^2 + q - 2r, 1; 1, d_f)]_{q^2}$*, tendo* $d_f \geq r - q + 2$*. Por outro lado, se* $q - 2 \leq r \leq 2q - 2$*, também é possível construir um código QCC com parâmetros* $[(2q^2, 2q^2 + q - 2r, 1; 1, d_f)]_q$*, tendo* $d_f \geq r - q + 2$*.*

Demonstração: Seja $F/\mathbb{F}_q$ o corpo de funções do Teorema 5.5. Para $q-2 \leq r \leq q^2+q/2-1$, o código AG construído sobre $F/\mathbb{F}_q$ é auto-ortogonal euclidiano, e para $r \leq 2q-2$ ele será auto-ortogonal hermitiano (veja o trabalho de Jin [103]). Assim, aplicando o Teorema 5.11, é possível obter os códigos QCC's com parâmetros $[(2q^2, 2q^2 + q - 2r, 1; 1, d_f)]_{q^2}$ e $[(2q^2, 2q^2 + q - 2r, 1; 1, d_f)]_q$. ■

Teorema 5.14 *Seja* $(3q^2 - 2q, r - q + 1, 1; 1, d_f \geq 3q^2 - 2q - r)_q$ *o código convolucional construído pela aplicação do Teorema 5.6, com* $q = 2^t$ *e* $t \geq 3$ *sendo um inteiro ímpar. Se* $2q - 4 \leq r \leq \frac{3q^2}{2} - 2$*, então existe um código QCC com parâmetros* $[(3q^2 - 2q, 3q^2 - 2(r+1), 1; 1, d_f)]_{q^2}$*, tendo* $d_f \geq r - 2q + 4$*. Por outro lado, para* $2q - 4 \leq r \leq 3q - 4$*, é possível também construir um outro QCC com parâmetros* $[(3q^2 - 2q, 3q^2 - 2(r+1), 1; 1, d_f)]_q$*, tendo* $d_f \geq r - 2q + 4$*.*

Demonstração: Seja $F/\mathbb{F}_q$ o corpo de funções do Teorema 5.6. Para $r \leq \frac{3q^2}{2} - 2$, o correspondente código AG definido sobre $F/\mathbb{F}_q$ é auto-ortogonal euclidiano e, para $r \leq 3q-4$, ele será auto-ortogonal hermitiano (veja [103]). Aplicando o Teorema 5.11 o resultado segue. ■

Tabela 5.4 – Exemplos de códigos convolucionais estabilizadores

Novos Códigos Convolucionais Estabilizadores – Teorema 5.13 $[(2q^2, 2q^2+q-2r, 1; 1, d_f \geq r-q+2)]_q$ $q-2 \leq r \leq 2q-2$ and $q=2^t$ with $t \geq 3$	
Examples	Singleton defect
$[(128, 118, 1; 1, d_f \geq 3)]_8$	4
$[(128, 114, 1; 1, d_f \geq 5)]_8$	4
$[(128, 108, 1; 1, d_f \geq 8)]_8$	4
$[(512, 494, 1; 1, d_f \geq 3)]_{16}$	8
$[(512, 482, 1; 1, d_f \geq 9)]_{16}$	8
$[(512, 468, 1; 1, d_f \geq 16)]_{16}$	8

Fazendo uma comparação entre os códigos derivados dos Teoremas 5.12 e 5.13, nota-se que os códigos do Teorema 5.13 têm maior taxa, mesmo não possuindo *Singleton defect* nulo. Por outro lado, os códigos convolucionais estabilizadores do Teorema 5.12 são códigos MDS.

Observação 5.3 *Como existem poucos trabalhos na literatura tratando sobre construção de códigos convolucionais estabilizadores, os parâmetros dos novos códigos convolucionais estabilizadores apresentados têm faixa de valores diferentes dos da literatura. Consequentemente, é impossível comparar seus correspondentes parâmetros "...for large q, it is difficult to find explicit known codes to compare with ours since there are no suitable tables for reference" (veja p. 3 da Ref. [103]). Esse problema é agravado pelo fato de que não há na literatura trabalhos utilizando códigos AG para construir códigos estabilizadores quânticos. Mais precisamente, uma vez que os parâmetros dos códigos AG têm parâmetros bastante distintos de outras classes de códigos de bloco, tais como códigos BCH e Reed-Solomon, tem-se que os correspondentes códigos convolucionais estabilizadores tem faixa de parâmetros muito discrepantes dos códigos convolucionais estabilizadores da literatura, o que impossibilita em uma comparação justa dos nossos códigos e os da literatura.*

Exemplo 5.2 *Do Teorema 5.13 é possível construir novos QCC's que tem parâmetros* $[(128, 120, 1; 1, d_f \geq 2)]_8$ *e* $[(128, 2, 1; 1, d_f \geq 61)]_8$ *para* $q = 8$. *Por outro lado, aplicando o Teorema 5.14, obtêm-se os seguintes novos QCC's:* $[(176, 158, 1; 1, d_f \geq 4)]_8$ *e* $[(176, 2, 1; 1, d_f \geq 82)]_8$, *para* $q = 8$.

CAPÍTULO 6

Considerações Finais e Proposta de Trabalhos Futuros

Neste trabalho de tese foram apresentadas quatro aplicações de códigos algébrico-geométricos na criação de códigos pertencentes a outras classes. Para o melhor entendimento dos resultados, foi feita uma fundamentação teórica de códigos lineares e códigos quânticos. Estas fundamentações estão presentes nos Capítulos 2 e 3, respectivamente. No Capítulo 2 também são apresentadas contribuições na área de códigos algébrico-geométricos. A primeira aplicação de códigos algébrico-geométricos na construção de códigos pertencentes a outras classes de códigos é mostrada no Capítulo 3, em que são construídas famílias códigos estabilizadores de comprimento finito e é feita uma análise assintótica mostrando a existência de famílias assintoticamente boas de códigos estabilizadores. No Capítulo 4 é aplicada a teoria de códigos estabilizadores para fundamentar a construção de códigos quânticos que utilizam emaranhamento como ferramenta adicional aos processos de codificação e decodificação. O uso de códigos algébrico-geométricos para a construção dessa classe também deriva códigos quânticos com parâmetros interessantes para a literatura de códigos. Por fim, como última contribuição desta tese, trata-se da construção de códigos convolucionais clássicos e quânticos a partir de códigos de bloco no Capítulo 5. Ambas construções utilizam códigos algébrico-geométricos e, como é mostrado, obtêm-se códigos com parâmetros novos ou superiores aos dos códigos presentes na literatura.

O Capítulo 2 inicia com a apresentação da teoria de códigos lineares. Essa teoria aborda códigos lineares, códigos BCH, códigos Reed-Solomon e códigos algébrico-geométricos. A descrição de códigos cíclicos, tais como os códigos BCH e Reed-Solomon, é através do seu conjunto de definição. Com ele é feita uma caracterização dos parâmetros dos códigos. Por outro lado, como a principal aplicação desta tese é através de códigos algébrico-geométricos, um maior detalhamento é feito para estes. É construída a teoria de corpos de função e apresentados alguns entes matemáticos dela, tais como lugar geométrico, divisores, espaços de Riemann-Roch e diferencial de Weil. Após essa descrição, é possível caracterizar o que é

um código algébrico-geométrico e seus parâmetros, tanto quanto para o seu dual euclidiano. Por fim, a primeira contribuição desta tese é descrita. Tomando divisores que tenham certas propriedades, mostra-se como construir uma matriz geradora para um código algébrico-geométrico que possua forma canônica. Em seguida, demonstramos que interseção e união de códigos algébrico-geométricos também resultam em códigos algébrico-geométricos. Estes resultados são utilizados em capítulos seguintes de forma a ser possível quantizar os parâmetros dos novos códigos construídos.

No Capítulo 3 é descrita a teoria sobre a qual códigos estabilizadores são definidos e descritos. Uma motivação sobre a impossibilidade de descrever códigos estabilizadores no mesmo formato que é feito para códigos lineares é dada via um exemplo. Em seguida, uma descrição dos tipos de erros considerados nesta tese e a relação de comutação entre eles é apresentada. Observando a existência de três tipos distintos de erros, é construída a ideia de estabilizador de um código quântico. Com esta descrição, quantizam-se os erros corrigíveis por um código estabilizador e os parâmetros do código. Isso abre a possibilidade de apresentar a construção de códigos estabilizadores mais amplamente utilizada na literatura, a construção CSS. Duas construções são mostradas, uma que considera a utilização do dual euclidiano e outra do dual hermitiano de um código linear. Alguns limitantes para códigos estabilizadores são expostos, tais como o limitante de Hamming e o limitante de Singleton quânticos. Em seguida, três importantes contribuições para esta tese são apresentadas. A primeira trata da utilização de códigos algébrico-geométricos de multi-lugares, o que foi denominado de construção de t-lugares, na obtensão de códigos estabilizadores. Estes códigos generalizam resultados anteriores que utilizavam códigos com um ou dois lugares. A segunda aplicação é através da utilização de códigos algébrico-geométricos que tenham um dos seus divisores definido sobre um lugar que não seja racional. Por fim, a terceira construção utiliza torres de códigos algébrico-geométricos assintoticamente boas para construir torres de códigos estabilizadores também assintoticamente boas. Diferentemente das construções presentes na literatura, é utilizada expansão de códigos algébrico-geométricos na construção da torre de códigos quânticos, em vez de concatenação de códigos.

No Capítulo 4 é tratada a construção de códigos quânticos assistidos por emaranhamento via códigos algébrico-geométricos. Utilizando um exemplo no início do capítulo, é mostrado como ampliar a teoria de códigos estabilizadores para códigos quânticos que utilizem emaranhamento como um recurso adicional aos processos de codificação e decodificação. Com isso, mostra-se que a construção CSS deste tipo de código quântico não necessita da hipótese de auto-ortogonalidade ou que um dos códigos esteja contido no dual de outro. A análise de grande parte dos códigos quânticos é feita através do limitante de Singleton quântico para estes códigos e, por isso, este limitante é descrito neste capítulo. As construções fundamentam-se na utilização de códigos cíclicos, códigos BCH e Reed-Solomon, e códigos algébrico-geométricos. Através da utilização de códigos cíclicos, é mostrado como conectar o conjunto de definição e os parâmetros dos códigos quânticos assistidos por emaranhamento. Códigos MDS

e maximamente emaranhados são construídos a partir de códigos cíclicos. Em seguida é feita a aplicação de códigos algébrico-geométricos na construção de códigos quânticos assistidos com emaranhamento. Esta aplicação só é possível por meio da utilização do resultado do Capítulo 2 que mostra que a interseção de códigos algébrico-geométricos é também um códigos algébrico-geométrico. Fez-se uso dos corpos de funções racionais, elípticas e hermitianas para construir os códigos quânticos deste capítulo via a construção euclidiana de códigos quânticos assistidos por emaranhamento. Para a construção hermitiana, por motivo de complexidade ao trabalhar com o dual hermitiano de códigos algébrico-geométrico, foram utilizados apenas códigos algébrico-geométricos advindos do corpo de funções racionais. O capítulo finaliza com a construção de torres assintoticamente boas de códigos quânticos assistidos por emaranhamento a partir de códigos algébrico-geométricos. Uma comparação com o limitante de Gilbert-Varshamov é exposta.

Códigos convolucionais clássicos e quânticos são tratados no Capítulo 5. Este capítulo inicia com a formulação matemática de códigos convolucionais clássicos via módulo vetorial e matrizes geradora e de verificação de paridade. O método de construção de códigos convolucionais a partir de códigos de bloco, proposto inicialmente por Piret, é explicado. Para códigos convolucionais quânticos, a formulação estabilizadora via limite direto é mostrada, tanto quanto a relação entre os parâmetros dos códigos e seu grupo estabilizador. Limitantes de Singleton para ambos os códigos convolucionais são apresentados. A primeira contribuição deste capítulo refere-se à análise do método de Piret em outra perspectiva por meio da construção de uma matriz geradora na forma canônica controladora e pelo cálculo da identidade de MacWilliams. Em seguida, códigos algébrico-geométricos são utilizados na derivação de códigos convolucionais clássicos. Utilizando diversos corpos de funções, tais como os corpos de funções racionais e hiperelípticas, foi obtido códigos convolucionais com parâmetros melhores que os códigos convolucionais existentes na literatura. A faixa de possíveis parâmetros para códigos convolucionais utilizando códigos algébrico-geométricos é ampliada por meio da utilização das técnicas de puncionamento, extensão, expansão e produto de códigos. O capítulo termina com a construção de códigos convolucionais quânticos derivados de códigos algébrico-geométricos com parâmetros inéditos na literatura.

6.1 – Proposta de Trabalhos Futuros

Como possíveis propostas trabalhos futuros em potencial decorrentes da pesquisa realizada podemos citar:

1. Criar um algoritmo eficiente, em termos de número de operações, que calcule a interseção entre um códigos algébrico-geométrico e seu dual hermitiano para curvas diversas, tais como curva hermitiana, Suzuki e GK. Esse ponto fornece uma primeira abordagem à questão sobre a utilização de códigos algébrico-geométricos na construção de códigos quânticos assistidos por emaranhamento através da construção hermitiana;

2. Construir códigos quânticos definidos a partir de curvas algébricas sobre o corpo dos números complexos. Analisar condições sobre a curva utilizada de forma que o código criado seja estabilizador. Gerar limitantes para os parâmetros do código quântico;

3. Desenvolver uma teoria para o dual hermitiano de um código algébrico-geométrico via *Weil descent*. Feito isso, aplicá-la à construção de códigos quânticos assistidos por emaranhamento. Essa teoria e os códigos derivados da mesma podem responder diversos questionamentos sobre o dual hermitiano de códigos algébrico-geométricos e abrir novas portas para pesquisas futuras;

4. Criar algoritmos de decodificação eficientes para os códigos quânticos apresentados nesta tese. Por parte do autor, não é conhecido algoritmos de decodificação algébricos para códigos quânticos e tal elucidação é bastante interessante para aplicações práticas de códigos quânticos.

Referências Bibliográficas

[1] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, July 1948.

[2] R. W. Hamming, "Error detecting and error correcting codes," *The Bell System Technical Journal*, vol. 29, pp. 147–160, Apr. 1950.

[3] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, pp. 300–304, June 1960.

[4] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, 1959.

[5] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79, Mar. 1960.

[6] V. D. Goppa, "A new class of linear error correcting codes," *Problems of Information Transmission*, vol. 6, no. 3, pp. 207–212, 1970.

[7] V. D. Goppa, "Codes associated with divisors," *Problems of Information Transmission*, vol. 13, no. 1, pp. 22–27, 1977.

[8] V. D. Goppa, "Algebraico-geometric codes," *Mathematics of the USSR-Izvestiya*, vol. 21, no. 1, pp. 75–91, 1983.

[9] M. A. Tsfasman, S. G. Vladuts, and T. Zink, "Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound," *Mathematische Nachrichten*, vol. 109, no. 1, pp. 21–28, 1982.

[10] E. N. Gilbert, "A comparison of signalling alphabets," *The Bell System Technical Journal*, vol. 31, pp. 504–522, May 1952.

[11] R. R. Varshamov, "Estimate of the number of signals in error correcting codes," *Doklady Akademii Nauk SSSR*, vol. 117, pp. 739–741, 1957.

[12] H. Janwa and O. Moreno, "McEliece public key cryptosystems using algebraic-geometric codes," *Designs, Codes and Cryptography*, vol. 8, pp. 293–307, June 1996.

[13] R. P. Irene Marquez-Corbella, Edgar Martinez-Moro, "Evaluation of public-key cryptosystems based on algebraic geometry codes," in *Proceedings of the Third International Castle Meeting on Coding Theory and Applications* (J. Borges and M. Villanueva, eds.), pp. 199–204, Servei de Publicacions de la Universitat Autònoma de Barcelona, 2011.

[14] K. Feng, S. Ling, and C. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," *IEEE Transactions on Information Theory*, vol. 52, pp. 986–991, Mar. 2006.

[15] L. F. Jin and C. P. Xing, "Euclidean and hermitian self-orthogonal algebraic geometry codes and their application to quantum codes," *IEEE Transactions on Information Theory*, vol. 58, pp. 5484–5489, Aug. 2012.

[16] G. G. L. Guardia and F. R. F. Pereira, "Good and asymptotically good quantum codes derived from algebraic geometry," *Quantum Information Processing*, vol. 16, p. 165, May 2017.

[17] P. Shor, "Scheme for reducing decoherence in quantum memory," *Physical Review A*, vol. 52, pp. 2493–2496, Oct. 1995.

[18] A. M. Steane, "Error correcting codes in quantum theory," *Physical Review Letters*, vol. 77, pp. 793–797, July 1996.

[19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2 ed., 2010.

[20] D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, Caltech, 1997.

[21] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed-Solomon codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (M. Fossorier, H. Imai, S. Lin, and A. Poli, eds.), (Berlin, Heidelberg), pp. 231–244, Springer Berlin Heidelberg, 1999.

[22] G. G. L. Guardia, "On classical and quantum MDS-convolutional BCH codes," *IEEE Transactions on Information Theory*, vol. 60, pp. 304–312, Jan. 2014.

[23] G. G. L. Guardia, "On the construction of nonbinary quantum BCH codes," *IEEE Transactions on Information Theory*, vol. 60, pp. 1528–1535, Mar. 2014.

[24] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Physical Review A*, vol. 63, pp. 032311–1–032311–5, Feb. 2001.

[25] H. Chen, S. Ling, and C. Xing, "Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound," *IEEE Transactions on Information Theory*, vol. 47, pp. 2055–2058, July 2001.

[26] H. Chen, "Some good quantum error-correcting codes from algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 47, pp. 2059–2061, July 2001.

[27] R. Matsumoto, "Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes," *IEEE Transactions on Information Theory*, vol. 48, pp. 2122–2124, July 2002.

[28] J.-L. Kim and G. L. Matthews, *Quantum Error-Correcting Codes from Algebraic Curves*, vol. 5 of *Series on Coding Theory and Cryptology*, ch. 12, pp. 419–444. Word Scientific, Hackensack, 2008.

[29] A. Elezi and T. Shaska, "Quantum codes from superelliptic curves." arXiv:1305.3941.

[30] C. Munuera, W. Tenório, and F. Torres, "Quantum error-correcting codes from algebraic geometry codes of Castle type," *Quantum Information Processing*, vol. 15, pp. 4071–4088, Oct. 2016.

[31] D. Bartoli, M. Montanucci, and G. Zini, "AG codes and AG quantum codes from the GGS curve," *Designs, Codes and Cryptography*, vol. 86, pp. 2315–2344, Oct. 2018.

[32] M. Montanucci, M. Timpanella, and G. Zini, "AG codes and AG quantum codes from cyclic extensions of the Suzuki and Ree curves," *Journal of Geometry*, vol. 109, p. 23, Mar. 2018.

[33] F. Hernando, G. McGuire, F. Monserrat, and J. J. Moyano-Fernández, "Quantum codes from a new construction of self-orthogonal algebraic geometry codes." arXiv:1907.05645.

[34] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Transactions on Information Theory*, vol. 60, pp. 1203–1222, Feb. 2014.

[35] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Dualities and identities for entanglement-assisted quantum codes," *Quantum Information Processing*, vol. 13, pp. 957–990, Apr. 2014.

[36] R. Li, L. Guo, and Z. Xu, "Entanglement-assisted quantum codes achieving the quantum singleton bound but violating the quantum Hamming bound," *Quantum Information & Computation*, vol. 14, pp. 1107–1116, Oct. 2014.

[37] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Physical Review A*, vol. 66, pp. 052313–1–052313–8, Nov. 2002.

[38] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, "Entanglement in the stabilizer formalism." arXiv:quant-ph/0406168, June 2004.

[39] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, pp. 436–439, Oct. 2006.

[40] D. A. Lidar and T. A. Brun, eds., *Quantum Error Correction*. Cambridge University Press, 2013.

[41] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Physical Review A*, vol. 77, pp. 064302–1–064302–4, June 2008.

[42] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Entanglement-assisted quantum error-correcting codes over arbitrary finite fields," *Quantum Information Processing*, vol. 18, pp. 1–18, Apr. 2019.

[43] J. Chen, Y. Huang, C. Feng, and R. Chen, "Entanglement-assisted quantum MDS codes constructed from negacyclic codes," *Quantum Information Processing*, vol. 16, p. 303, Nov. 2017.

[44] L. Lu, R. Li, and L. Guo, "Entanglement-assisted quantum codes from quaternary codes of dimension five," *International Journal of Quantum Information*, vol. 15, p. 1750017, April 2017.

[45] K. Guenda, S. Jitman, and T. A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes," *Designs, Codes and Cryptography*, vol. 86, pp. 121–136, Jan. 2018.

[46] X. Liu, L. Yu, and P. Hu, "New entanglement-assisted quantum codes from k-Galois dual codes," *Finite Fields and Their Applications*, vol. 55, pp. 21–32, Jan. 2019.

[47] J. Fan, H. Chen, and J. Xu, "Constructions of q-ary entanglement-assisted quantum MDS codes with minimum distance greater than $q + 1$," *Quantum Information and Computation*, vol. 16, no. 5&6, pp. 423–434, 2016.

[48] L. Lu, W. Ma, R. Li, Y. Ma, Y. Liu, and H. Cao, "Entanglement-assisted quantum MDS codes from constacyclic codes with large minimum distance," *Finite Fields and Their Applications*, vol. 53, pp. 309 – 325, Sept. 2018.

[49] X. Chen, S. Zhu, and X. Kai, "Entanglement-assisted quantum MDS codes constructed from constacyclic codes," *Quantum Information Processing*, vol. 17, p. 273, Oct. 2018.

[50] X. Liu, H. Liu, and L. Yu, "Entanglement-assisted quantum codes from Galois LCD codes." arXiv:1809.00568, Sept. 2018.

[51] K. Guenda, T. A. Gulliver, S. Jitman, and S. Thipworawimon, "Linear ℓ-intersection pairs of codes and their applications." arXiv:1810.05103, Oct. 2018.

[52] M. E. Koroglu, "New entanglement-assisted MDS quantum codes from constacyclic codes," *Quantum Information Processing*, vol. 18, p. 44, Feb. 2019.

[53] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Physical Review Letters*, vol. 91, pp. 177902–1–177902–4, Oct. 2003.

[54] A. C. A. de Almeida and R. P. Jr., "A concatenated $[(4, 1, 3)]$ quantum convolutional code," in *Information Theory Workshop*, pp. 28–33, IEEE, Oct. 2004.

[55] J. J. Kong and K. K. Parhi, "Quantum convolutional codes design and their encoder architectures," in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, vol. 1, pp. 1131–1135, IEEE, Nov. 2004.

[56] H. Ollivier and J.-P. Tillich, "Trellises for stabilizer codes: deflnition and uses," *Physical Review A*, vol. 74, pp. 032304–1–032304–4, Sept. 2006.

[57] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 53, pp. 865–880, Mar. 2007.

[58] P. Piret, "A convolutional equivalent to Reed-Solomon codes," *Philips Journal of Research*, vol. 43, pp. 441–458, Jan. 1988.

[59] S. A. Aly, M. Grassl, A. Klappenecker, M. Rotteler, and P. K. Sarvepalli, "Quantum convolutional BCH codes," in *10th Canadian Workshop on Information Theory*, pp. 180–183, IEEE, June 2007.

[60] G. G. L. Guardia, "On negacyclic MDS-convolutional codes," *Linear Algebra and its Applications*, vol. 448, pp. 85–96, May 2014.

[61] G. G. L. Guardia, "On optimal constacyclic codes," *Linear Algebra and its Applications*, vol. 496, pp. 594–610, May 2016.

[62] F. R. Fernandes Pereira, G. G. La Guardia, and F. M. de Assis, "Classical and quantum convolutional codes derived from algebraic geometry codes," *IEEE Transactions on Communications*, vol. 67, pp. 73–82, Jan. 2019.

[63] G. G. L. Guardia and F. R. F. Pereira, "Good and asymptotically good quantum codes derived from algebraic geometry," *Quantum Information Processing*, vol. 16, p. 165, May 2017.

[64] F. R. F. Pereira, R. Pellikaan, G. G. L. Guardia, and F. M. de Assis, "Entanglement-assisted quantum codes from algebraic geometry codes." arXiv:1907.06357, 2019.

[65] F. R. F. Pereira, "Entanglement-assisted quantum codes from cyclic codes." arXiv:1911.06384, 2019.

[66] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library, 1 ed., 1977.

[67] A. Hefez and M. L. T. Villela, *Códigos Corretores de Erros*. IMPA, 1 ed., 2008.

[68] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 1 ed., 2003.

[69] R. Pellikaan, X.-W. Wu, S. Bulygin, and R. Jurrius, *Codes, Cryptology and Curves with Computer Algebra*. Cambridge University Press, 1 ed., 2017.

[70] M. Tsfasman, S. Vladut, and D. Nogin, *Algebraic Geometric Codes: Basic Notions*. American Mathematical Society, 1 ed., 2007.

[71] H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer-Verlag Berlin Heidelberg, 2 ed., 2009.

[72] O. Pretzel, *Codes and Algebraic Curves*. Clarendon Press, 1 ed., 1998.

[73] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," *Journal of Number Theory*, vol. 61, pp. 248–273, Dec. 1996.

[74] C. Munuera and R. Pellikaan, "Equality of geometric Goppa codes and equivalence of divisors," *Journal of Pure and Applied Algebra*, vol. 90, pp. 229–252, Dec. 1993.

[75] F. Gaitan, *Quantum Error Correction and Fault Tolerant Quantum Computing*. CRC Press, 1 ed., 2008.

[76] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, vol. 52, pp. 4892 – 4914, Nov. 2006.

[77] A. Klappenecker and M. Rötteler, "Beyond stabilizer codes II: Clifford codes," *IEEE Transactions on Information Theory*, vol. 48, pp. 2396–2399, Aug. 2002.

[78] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, pp. 1098–1105, Aug. 1996.

[79] K. Feng and Z. Ma, "A finite Gilbert-Varshamov bound for pure stabilizer quantum codes," *IEEE Transactions on Information Theory*, vol. 50, pp. 3323–3325, Dec. 2004.

[80] V. I. Levenshtein, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces," *IEEE Transactions on Information Theory*, vol. 41, pp. 1303–1321, Sept. 1995.

[81] J.-L. Kim and J. Walker, "Nonbinary quantum error-correcting codes from algebraic curves," *Discrete Mathematics*, vol. 308, pp. 3115–3124, July 2008.

[82] Y. Edel, "Table of quantum twisted codes." https://www.mathi.uni-heidelberg.de/ yves/Matritzen/QTBCH/QTBCHIndex.html.

[83] G. G. L. Guardia, "Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes," *Quantum Information Processing*, vol. 11, pp. 591–604, Apr. 2012.

[84] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Catalytic quantum error correction," *IEEE Transactions on Information Theory*, vol. 60, pp. 3073–3089, June 2014.

[85] A. C. da Silva, *Lectures on Symplectic Geometry*. Springer, 2 ed., 2008.

[86] G. G. L. Guardia, "Constructions of new families of nonbinary quantum codes," *Physical Review A*, vol. 80, pp. 042331–1–042331–11, Oct. 2009.

[87] J. Qian and L. Zhang, "Constructions of new entanglement-assisted quantum MDS and almost MDS codes," *Quantum Information Processing*, vol. 18, p. 71, Jan. 2019.

[88] C. Li, "Hermitian LCD codes from cyclic codes," *Designs, Codes and Cryptography*, vol. 86, pp. 2261–2278, Oct. 2018.

[89] G. Luo and X. Cao, "Two new families of entanglement-assisted quantum MDS codes from generalized Reed-Solomon codes," *Quantum Information Processing*, vol. 18, p. 89, Feb. 2019.

[90] L. Guo, Q. Fu, R. Li, and L. Lu, "Maximal entanglement entanglement-assisted quantum codes of distance three," *International Journal of Quantum Information*, vol. 13, pp. 1550002–1–1550002–7, Feb. 2015.

[91] L. Lu, R. Li, L. Guo, and Q. Fu, "Maximal entanglement entanglement-assisted quantum codes constructed from linear codes," *Quantum Information Processing*, vol. 14, pp. 165–182, Jan. 2015.

[92] L. Lv, R. Li, Q. Fu, X. Li, and X. Li, "Maximal entanglement entanglement-assisted quantum codes from quaternary BCH codes," in *Proceedings of IEEE Advanced Information Technology, Electronic and Automation Control Conference*, 2015.

[93] A. Menezes, *Elliptic Curve Public Key Cryptosystems*. The Springer International Series in Engineering and Computer Science, Springer, 1 ed., 1993.

[94] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, "Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$," *IEEE Transactions on Information Theory*, vol. 64, pp. 3010–3017, Apr. 2018.

[95] Y. Ihara, "Some remarks on the number of rational points of algebratic curves over finite fields," *Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics*, vol. 28, pp. 721–724, 1981.

[96] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. Wiley-IEEE Press, 2 ed., 2015.

[97] S. A. A. A. Ahmed, *Quantum Error Control Codes*. PhD thesis, Texas A&M University, May 2008.

[98] H. Gluesing-Luerssen, "On the weight distribution of convolutional codes," *Linear Algebra and its Applications*, vol. 408, pp. 298–326, Oct. 2005.

[99] H. Gluesing-Luerssen and F.-L. Tsang, "A matrix ring description for cyclic convolutional codes," *Advances in Mathematics of Communications*, vol. 2, no. 1, pp. 55–81, 2008.

[100] H. Gluesing-Luerssen and G. Schneider, "A MacWilliams identity for convolutional codes: The general case," *IEEE Transactions on Information Theory*, vol. 55, pp. 2920–2930, July 2009.

[101] R. Smarandache, H. G.-Luerssen, and J. Rosenthal, "Constructions of MDS-convolutional codes," *IEEE Transactions on Information Theory*, vol. 47, pp. 2045–2049, July 2001.

[102] H. Stichtenoth, "Self-dual Goppa codes," *Journal of Pure and Applied Algebra*, vol. 55, pp. 199–211, Nov. 1988.

[103] L. Jin, "Quantum stabilizer codes from maximal curves," *IEEE Transactions on Information Theory*, vol. 60, pp. 313–316, Jan. 2014.

[104] G. G. L. Guardia, "Nonbinary convolutional codes derived from group character codes," *Discrete Mathematics*, vol. 313, pp. 2730–2736, Dec. 2013.

[105] J. P. Hansen and H. Stichtenoth, "Group codes on certain algebraic curves with many rational points," *Applicable Algebra in Engineering, Communication and Computing*, vol. 1, pp. 67–77, Mar. 1990.

[106] J. P. Hansen, "Deligne-Lusztig varieties and group codes," in *Coding Theory and Algebraic Geometry* (H. Stichtenoth and M. A. Tsfasman, eds.), (Berlin, Heidelberg), pp. 63–81, Springer, 1992.

[107] R. Pellikaan, B.-Z. Shen, and G. J. M. van Wee, "Which linear codes are algebraic-geometric?," *IEEE Transactions on Information Theory*, vol. 37, pp. 583–602, May 1991.

[108] A. Garcia and Y. Lequain, *Elementos de Álgebra*. IMPA, 6 ed., 2018.

[109] I. N. Herstein, *Topics in Algebra*. John Wiley & Sons, 2 ed., 1975.

[110] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, 2 ed., 1996.

[111] D. J. Griffiths and D. F. Schroeter, *Introduction to Quantum Mechanics*. Cambridge University Press, 2018.

[112] J. J. Sakurai and J. Napolitano, *Modern Quantum Mechanics*. Cambridge University Press, 2 ed., 2017.

[113] W. Heisenberg, "Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik," *Zeitschrift für Physik*, vol. 43, pp. 172–198, Mar. 1927.

[114] H. P. Robertson, "The uncertainty principle," *Physical Review*, vol. 34, pp. 163–164, July 1929.

APÊNDICES

APÊNDICE A

Fundamentos de Álgebra

É apresentado neste apêndice algumas definições e resultados que são úteis para um melhor entendimento das ferramentas utilizadas advindas da Álgebra. Para o leitor que deseje se apronfundar no assunto, recomendamos as Refs. [108–110].

A.1 – Grupos e Anéis

Definição A.1 *Seja G um conjunto não-vazio munido da operação binária $* : G \times G \to G$. Dizemos que o par $(G, *)$ é um* grupo *se são válidas as seguintes propriedades:*

a. $a * (b * c) = (a * b) * c, \quad \forall a, b, c \in G.$

b. $\exists e \in G$ tal que $a * e = e * a = a, \quad \forall a \in G.$

c. $\forall a \in G, \exists b \in G$ tal que $a * b = b * a = e$ e este elemento b é dito inverso de a.

Um subconjunto H de um grupo G que também é um grupo sobre a mesma operação é chamado de subgrupo de G. Representamos essa relação por $H \leq G$.

Definição A.2 *Seja G um grupo. Um subgrupo N de G é chamado de subgrupo normal em G se, e somente se, $gng^{-1} \in N$ para todo $g \in G$ e $n \in N$. Em particular, tem-se $gN = Ng$, para todo $g \in G$ e N subgrupo normal em G.*

Associado com a ideia de subgrupo normal, é possível definir dois novos conjuntos chamados de centro e centralizador do grupo.

Definição A.3 *Sejam G um grupo e S um subconjunto de G. O centro de G é definido como o conjunto*

$$Z(G) := \{z \in G \colon zg = gz, \text{ para todo } g \in G\}. \tag{A.1}$$

Além disso, define-se o centralizador de S em G por

$$C_G(S) := \{g \in G \colon gs = sg, \text{ para todo } s \in S\}. \tag{A.2}$$

O centro e centralizador são usados no Cap. 3 na construção de códigos estabilizadores.

Definição A.4 *Um anel é um conjunto não-vazio A munido de duas operações binárias*

$$\begin{array}{rcl} +: A \times A & \to & A \\ (a,b) & \mapsto & a+b \end{array} \quad e \quad \begin{array}{rcl} \cdot : A \times A & \to & A \\ (a,b) & \mapsto & a \cdot b \end{array} \tag{A.3}$$

chamadas, respectivamente, de adição e multiplicação. Essas operações possuem as seguintes propriedades:

1. *Existe um elemento neutro, denotado por 0, tal que $a+0=0+a=a$, $\forall a \in A$;*
2. *Dado $a \in A$, existe um elemento chamado inverso (ou simétrico) de a, denotado por $-a$, tal que $a+(-a)=-a+a=0$;*
3. $(a+b)+c=a+(b+c), \quad \forall a,b,c \in A$;
4. $a+b=b+a, \quad \forall a,b \in A$;
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c), \quad \forall a,b,c \in A$;
6. $a \cdot (b+c) = a \cdot b + a \cdot c$ *e* $(b+c) \cdot a = b \cdot a + c \cdot a, \quad \forall a,b,c \in A$;

Um anel A munido das operações $+$ e $\cdot$ é comumente denotado por $(A,+,\cdot)$.

Seja $(A,+,\cdot)$ um anel, se existe um elemento denotado por $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$, $\forall a \in A$ diremos que A é um anel com unidade 1.

Se um anel $(A,+,\cdot)$ satisfaz $a \cdot b = b \cdot a$, $\forall a,b \in A$ é dito anel comutativo.

Exemplo A.1 *Como exemplos de anéis, temos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ munidos com as operações de adição e multiplicação usuais.*

Um anel comutativo com unidade A será chamado de domínio de integridade se satisfaz a seguinte condição:

$$\forall a,b \in A, \quad a \neq 0 \ \ e \ \ b \neq 0 \Rightarrow a \cdot b \neq 0.$$

Exemplo A.2 *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ munidos com as operações de adição e multiplicação usuais são domínios de integridade.*

Definição A.5 *Seja $(A,+,\cdot)$ é um anel com unidade. Um elemento $a \in A$ é dito invertível se existir um elemento $b \in A$ tal que $a \cdot b = 1$. Dizemos que b é inverso de a.*

Exemplo A.3 *Em $\mathbb{Z}$, os únicos elementos invertíveis são 1 e -1.*

Definição A.6 *Um anel comutativo com unidade onde todo elemento não nulo é invertível é chamado de corpo.*

Um corpo F que contém um corpo K, tal que as operações de F, quando restritas a K, coincidam com as operações de K, é chamado de *extensão* de K. Neste caso, dizemos que K é um *subcorpo* de F. Denotaremos por F/K ou pelo diagrama

$$\begin{array}{c} F \\ | \\ K \end{array} \tag{A.4}$$

Neste caso, K é dito corpo base ou corpo fundamental da extensão.

Exemplo A.4 *Considere a seguinte sequência de conjuntos $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Com isso, temos que $\mathbb{C}$ é uma extensão de $\mathbb{R}$, $\mathbb{C}$ é uma extensão de $\mathbb{Q}$ e $\mathbb{R}$ é uma extensão de $\mathbb{Q}$.*

A.2 – Classes Residuais

Uma relação R entre pares de elementos de um conjunto A é dita relação de equivalência, se ela é reflexiva, simétrica e transitiva, ou seja, dados $a, b, c \in A$ devemos ter:

1. aRa;
2. Se aRb, então bRa;
3. Se aRb e bRc, então aRc.

Uma relação de equivalência é denotada por $\sim$.

Definição A.7 *Seja $\sim$ uma relação de equivalência em um conjunto A e $a \in A$. Definimos a classe de equivalência $\overline{a}$ do elemento a em relação a $\sim$ como o conjunto $\overline{a} := \{b \in A; a \sim b\}$. Sejam A um anel e $a, b, m \in A$, diremos que* a *é* congruente *a* b *módulo* m*, se $m|(b-a)$ e denotaremos por*

$$a \equiv b \mod m. \tag{A.5}$$

Proposição A.1 *Sejam $a, b, c, d \in A$ e $(A, +, \cdot)$ um anel. Então:*

1. *$a \equiv a$ mod m.*
2. *Se $a \equiv b$ mod m, então $b \equiv a$ mod m.*
3. *Se $a \equiv b$ mod m e $b \equiv c$ mod m, então $a \equiv c$ mod m.*
4. *Se $a \equiv c$ mod m e $b \equiv d$ mod m, então $a + b \equiv c + d$ mod m e $a \cdot b \equiv c \cdot d$ mod m.*

As propriedades $1, 2,$ e 3 mostram que a relação de congruência é uma relação de equivalência e a propriedade 4 nos mostra que esta relação é compatível com as operações de adição e multiplicação do anel A.

A classe lateral de um elemento *a* $\in A$, módulo *m*, é o conjunto

$$\overline{a} := \{b \in A; b \equiv a \bmod m\} = \{a + m\lambda; \lambda \in A\}. \tag{A.6}$$

Podemos definir $m \cdot A = \{m \cdot \lambda; \lambda \in A\}$ e assim temos:

$$\overline{a} = a + mA. \tag{A.7}$$

O elemento a é chamado de representante da classe residual $\overline{a}$.

Vamos denotar por A_m o conjunto de todas as classes laterais em A módulo m.

O conjunto A_m munido das operações $\overline{a} + \overline{b} = \overline{a + b}(\bmod m)$ e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}(\bmod m)$ é um anel, com $\overline{0}$ e $\overline{1}$, respectivamente, os elementos neutros para a adição e multiplicação.

A.3 – Ideais de um anel

Definição A.8 *Um subconjunto I não vazio de um anel A é um ideal de A se:*

i. $\forall a, b \in I, a + b \in I$*;*

ii. $\forall a \in I$ *e* $\forall c \in A$*,* $ca \in I$ *e* $ac \in I$*.*

Note que um ideal I sempre contém o elemento zero de A, pois dado um elemento qualquer não nulo $a \in I$, temos $0 = 0a \in I$. Também é possível observar que $I = 0$ e $I = A$ são ideais de A, denominados ideais triviais.

Definição A.9 *Seja A um anel comutativo com unidade e $a \in A$, então o conjunto $I(a) = \{ca; c \in A\}$ é um ideal de A, chamado de ideal principal gerado por a; ou seja, um ideal principal é um ideal gerador por somente um ideal.*

Para o caso de domínios de integridades, diz-se que ele é um domínio de ideais principais se todo ideal é principal. Como todo anel é um domínio de integridade, a mesma denominação é utilizada para anéis.

A.4 – Corpos Finitos

A maioria dos códigos encontrados na literatura são definidos sobre corpos finitos []. Por isso, é de grande importância definir corpos finitos e suas propriedades a fim de melhor compreender a estrutura dos códigos corretores de erros.

Definição A.10 *Seja K um corpo finito (ou campo de Galois) com elemento unidade 1. Considere o conjunto*

$$\Lambda_K := \{n \in \mathbb{N}:\ n \cdot 1 = 0\} \subset \mathbb{N}.$$

A característica do corpo finito K é definida como o inteiro positivo λ

$$\lambda := \min \Lambda_K = \min\{n \in \mathbb{N};\ n \cdot 1 = 0\}. \tag{A.8}$$

Proposição A.2 *Seja K um corpo finito, então λ é um número primo.*

Definição A.11 *Seja $\alpha \in K^*$, onde $K^* = K \setminus \{0\}$ e K é um corpo finito. Define-se a ordem do elemento α como sendo o menor inteiro n tal que $\alpha^n = 1$.*

Definição A.12 *Sejam A e B dois anéis (ou corpos). Uma função $f : A \to B$ será chamada homomorfismo se, para todos os elementos $a, b \in A$, valem as seguintes condições:*

(i) $f(a + b) = f(a) + f(b)$.

(ii) $f(a \cdot b) = f(a) \cdot f(b)$.

(iii) $f(1) = 1$.

Definição A.13 *Um homomorfismo bijetor de anéis (ou corpos) será chamado de isomorfismo. Dois anéis (ou corpos) são ditos isomorfos se existir um isomorfismo entre eles.*

Teorema A.1 *Seja K um corpo finito com característica $\lambda = p$, onde p é um número primo. Então, K contém um subcorpo isomorfo a $\mathbb{Z}_p$ (que ainda denotaremos por $\mathbb{Z}_p$). Por outro lado, para todo p primo e $m \geq 1$ inteiro, tem-se que existe um corpo finito com p^m elementos.*

O corpo finito com $q = p^m$, com p sendo um número primo e $m \geq 1$ inteiro, é denotado por $\mathbb{F}_q$.

Teorema A.2 *Seja α um elemento não-nulo do corpo finito $\mathbb{F}_q$. Então $\alpha^{q-1} = 1$.*

Teorema A.3 *Seja α um elemento não-nulo do corpo finito $\mathbb{F}_q$. Seja n a ordem de α. Então n divide $q - 1$.*

Definição A.14 *Seja o corpo finito $\mathbb{F}_q$, um elemento não-nulo α de $\mathbb{F}_q$ é dito primitivo se a ordem de α for $q - 1$, ou seja, se $GF(q)^* = \langle\alpha\rangle = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$.*

Portanto, as potências do elemento primitivo geram todos os elementos não-nulos de $\mathbb{F}_q$. É possível mostrar que todo corpo finito possui elementos primitivos.

Vejamos alguns exemplos ilustrativos desses conceitos.

Exemplo A.5 *Considere o corpo finito $\mathbb{F}_7$ com as operações definidas como soma e multiplicação módulo 7. Se tomarmos potências do elemento 3, notamos a seguinte sequência:*

$$3^1 = 3 \mod 7, \tag{A.9}$$
$$3^2 = 2 \mod 7, \tag{A.10}$$
$$3^3 = 6 \mod 7, \tag{A.11}$$
$$3^4 = 4 \mod 7, \tag{A.12}$$
$$3^5 = 5 \mod 7, \tag{A.13}$$
$$3^6 = 1 \mod 7. \tag{A.14}$$

Portanto, a ordem do elemento 3 é 6. Como $q = 7$, temos $n = q - 1 \Rightarrow 6 = 7 - 1$. Isso implica em 3 ser um elemento primitivo do $\mathbb{F}_7$.

A.5 – Anéis de Polinômios

Definição A.15 *Sejam A um anel e X uma indeterminada. Definimos o polinômio $P(X)$ com coeficientes em A na indeterminada X como*

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + \cdots + a_n X^n \tag{A.15}$$

em que $n \in \mathbb{Z}^+$ e $a_i \in A$, para todo $i = 0, 1, \ldots, n$.

Dados os polinômios $P(X) = a_0 + a_1 X + \cdots + a_n X^n$ e $Q(X) = b_0 + b_1 X + \cdots + b_m X^m$, podemos dizer que $P(X) = Q(X)$ se $a_i = b_i$, para todo i. Seja $A[X] = \{P(X)\colon\ a_i \in A, \forall i = 1, \ldots, n\}$, ou seja, $A[X]$ é o conjunto de todos os polinômios na indeterminada X com coeficientes em A. Note que $A \subset A[X]$. Considere $P(X)$ e $Q(X)$ definidos acima, podemos definir as seguintes operações:

$$P(X) + Q(X) = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) X^i, \tag{A.16}$$
$$P(X) \cdot Q(X) = \sum_{i=0}^{n+m} c_i X^i, \tag{A.17}$$

em que $c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j} X^i$. Como é possível notar, o conjunto $A[X]$ munido das operações definidas acima é um anel.

Se $P(X) = 0 + 0X + 0X^2 + \ldots + 0X^n$ indicaremos $P(X) \equiv 0$ e dizemos que o polinômio é identicamente nulo sobre A. Se $P(X) = a$, com $a \in A$, então $P(X)$ é o polinômio constante

a. Se $P(X) \in A[X]$ tal que $a_n \neq 0$ e $a_j = 0$, para todo $j > n$, dizemos que n é o grau de $P(X)$ e denotaremos por $\deg P(X) = n$.

Note que não está definido o grau do polinômio identicamente nulo e que $\deg$ pode ser interpretada como uma função de $A[X]$ em $\mathbb{N}$ da seguinte forma

$$\begin{array}{rccc} \deg\colon & A[X]-\{0\} & \to & \mathbb{N} \\ & P(X) & \mapsto & \deg P(X) \end{array} \tag{A.18}$$

Seja K um corpo e $K[X]$ o domínio dos polinômios sobre K na indeterminada X. Sejam $F(X), G(X) \in K[X]$. Suponha que o grau de $G[X]$ é diferente de zero, efetuando a divisão de $F(X)$ por $Q(X)$ obtemos um único par de polinômios sobre $Q(X), R(X) \in K[X]$, chamados de quociente e resto, respectivamente, tais que:

$$F(X) = Q(X) \cdot G(X) + R(X) \tag{A.19}$$

onde ou $R(X) = 0$ ou $\deg R(X) < \deg G(X)$. Esta expressão é conhecida como Algoritmo de Euclides da Divisão.

Definição A.16 *Seja K um corpo e $P(X) \in K[X]$ tal que $\deg P(X) \geq 1$. Dizemos que $P(X)$ é um polinômio irredutível sobre K se, toda vez que $P(X) = G(X)H(X)$, tal que $G(X), H(X) \in K[X]$, então temos $G(X) = a$, uma constante em K, ou $H(X) = b$, uma constante em K. Se $P(X)$ não for irredutível sobre K, dizemos que $P(X)$ é redutível sobre K.*

Definição A.17 *Seja K um corpo e $K[X]$ o anel dos polinômios sobre K. Dado $P(X) \in K[X]$. Dizemos que $P(X)$ é mônico quando o coeficiente do termo de mais alto grau for $1 \in K$.*

Podemos definir as classes laterais de $A = K[X]$ módulo um polinômio não constante e mônico $m = P(X)$ de grau n da seguinte forma:

$$A_m = K[X]_{P(X)} := \{[R(X)]\colon R(X) \in K[X] \text{ com } R(X) = 0 \text{ ou } \deg R(X) < n\}. \tag{A.20}$$

Dados $R_1(X), R_2(X) \in K[X]$, com $\deg R_1(X) < n$ e $\deg R_2(X) < n$, tais que $R_1(X) \neq R_2(X)$, então $[R_1(X)] \neq [R_2(X)]$.

Teorema A.4 *O anel $K[X]_{P(X)}$ é um corpo se, e somente se, o polinômio $P(X)$ é irredutível.*

Este teorema nos fornece um método prático pra construir corpos finitos, como podemos observar no exemplo a seguir.

Exemplo A.6 *Sejam $K = \mathbb{F}_2$ e $P(X) = X^2+X+1$. $P(X)$ é um polinômio irredutível de grau 2 em $K[X]$. Podemos construir um corpo $\mathbb{F}_4$ dado por $\mathbb{F}_4 = K[X]_{P(X)} = \{[0], [1], [X], [1 + X]\}$. As operações neste corpo são a soma e multiplicação de polinômios módulo $P(X)$.*

A partir do Teorema A.4 temos um método para construir corpos finitos. Dados $K = \mathbb{F}_p$, onde p é um número primo positivo e $P(X) \in K[X]$ um polinômio irredutível com $\deg P(X) = n$, então $K[X]_{P(X)}$ é formado pelas classes de polinômios em $K[X]$ e o corpo $K[X]_{P(X)}$ tem p^n elementos.

APÊNDICE B

Fundamentos de Mecânica Quântica

Nesse apêndice será apresentada uma introdução aos fundamentos da Mecânica Quântica. O assunto aqui apresentado embasa os resultados apresentados no Cap. 3. Recomendamos as Refs. [19, 111, 112] para o leitor que deseje se aprofundar no assunto.

B.1 – Elementos de Mecânica Quântica

B.1.1 – Os Postulados da Mecânica Quântica

A Mecânica Quântica é construída sobre quatro postulados [19]:

- **Postulado 1** - Todo sistema físico tem a ele associado um espaço vetorial complexo chamado de espaço de Hilbert $\mathcal{H}_n$. Os elementos do espaço de Hilbert são vetores complexos $|\psi\rangle$, chamados de kets, e representam o estado físico do sistema. O complexo conjugado de um ket é chamado de bra, representado por $\langle\psi|$. Como esses elementos são vetores, então eles podem ser decompostos em uma base, por exemplo, considere a base $\mathcal{B} = \{|b_1\rangle, \ldots, |b_n\rangle\}$ de um espaço de Hilbert n dimensional, o vetor $|\psi\rangle$ é decomposto nessa base da seguinte forma

$$|\psi\rangle = b_1|b_1\rangle + \cdots + b_n|b_n\rangle, \tag{B.1}$$

  onde $b_i = \langle b_i|\psi\rangle$, para $i = 1, \cdots, n$, e $\sum_{i=1}^{n} |b_i|^2 = 1$. Para o caso em que o espaço de Hilbert tem dimensão $n = 2$, chamamos os vetores de qubits, e para o caso em que $n > 2$, chamamos os vetores complexos deste espaço de qudits. A noção de decomposição pode ser expandida para espaços de Hilbert com espectro contínuo.

- **Postulado 2** - A evolução temporal de um sistema quântico isolado, ou seja, que não interage com sua vizinhança[1], dá-se através de transformações unitárias:

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle, \tag{B.2}$$

onde $U^\dagger(t)U(t) = \mathcal{I}$, sendo $\mathcal{I}$ a matriz identidade. A relação do operador U com o hamiltoniano $\mathcal{H}$ do sistema é:

$$U(t) = \exp\Big(-\frac{i}{\hbar}\mathcal{H}t\Big). \tag{B.3}$$

Fisicamente, transformações unitárias representam processos temporalmente reversíveis. De fato, aplicando-se $U^\dagger(t)$ pela esquerda nos dois lados da Eq. B.2 obtém-se

$$|\psi(0)\rangle = U^\dagger(t)|\psi(t)\rangle. \tag{B.4}$$

Uma outra propriedade importante das transformações unitárias é a conservação do produto escalar, ou seja,

$$\langle\psi(0)|U^\dagger U|\psi(0)\rangle = \langle\psi(0)|\psi(0)\rangle = \langle\psi(t)|\psi(t)\rangle. \tag{B.5}$$

- **Postulado 3** - Medidas em Mecânica Quântica são representadas por um conjunto de operadores de medidas $\{M_m\}$, onde o índice m refere-se aos possíveis resultados da medida. A probabilidade de que o resultado m seja encontrado em uma medida feita em um sistema quântico preparado no estado $|\psi\rangle$ é dada por

$$p_M(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{B.6}$$

e o estado do sistema, após a medida com resultado m, será:

$$|\psi_m\rangle = \frac{M_m}{\sqrt{p_M(m)}}|\psi\rangle. \tag{B.7}$$

A normalização das probabilidades, $\sum_m p_M(m) = 1$, a hipótese de que $\langle\psi|\psi\rangle = 1$ e a Eq. (B.6) implicam na relação de completitude

$$\sum_m M_m^\dagger M_m = \mathcal{I}. \tag{B.8}$$

[1]Quando há a influência de um ambiente, tal como um reservatório térmico, o hamiltoniano $\mathcal{H}$ pode conter termos relacionados a interações entre partículas e/ou campos, por exemplo. Assim, o sistema não será isolado, de fato.

- **Postulado 4** - Os elementos do espaço de Hilbert de um sistema quântico composto AB é formado pelo produto tensorial dos kets dos espaços de Hilbert dos sistemas individuais:

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle. \tag{B.9}$$

  Esta regra pode ser estendida para N sistemas individuais.

B.1.2 – Princípio de Indeterminação

O princípio da indeterminação de Heisenberg consiste num enunciado da Mecânica Quântica, formulado inicialmente em 1927 por Werner Heisenberg [113], impondo restrições à precisão com que se podem efetuar medidas simultâneas de uma classe de pares de observáveis.

Em Mecânica Quântica, observáveis, tais como posição e *momentum*, são representados por operadores hermitianos. Quando se considera pares de observáveis, uma das quantidades mais importantes é o comutador. Para um par de observáveis A e B, define-se seu comutador como sendo

$$[A, B] := AB - BA. \tag{B.10}$$

Com essa definição, é possível mostrar que a relação de comutação entre a posição e o *momentum* é [112]

$$[x, p_x] = i\hbar. \tag{B.11}$$

O significado físico é que operadores que não comutam entre si não podem ser medidos com qualquer precisão simultaneamente, sempre ocorrendo um erro na medida dos observáveis.

A forma geral mais comum do princípio de indeterminação é a relação de indeterminação de Robertson [114]. Para um operador hermitiano arbitrário O, associa-se o desvio padrão como sendo

$$\Delta_O = \sqrt{\langle O^2\rangle - \langle O\rangle^2}, \tag{B.12}$$

onde $\langle O\rangle$ denota o valor médio[2]. Para um par de operadores A e B, a relação de indeterminação de Robertson é dada por

$$\Delta_A \Delta_B \geq \frac{1}{2}|\langle [A, B]\rangle|. \tag{B.13}$$

B.1.3 – Bits e Qubits

A unidade de informação clássica é o bit. Um bit pode ter os valores lógicos "0" ou "1". Nos computadores, bits são fisicamente representados pela presença ou não de correntes elétricas em componentes eletrônicos dentro dos chips: a presença da corrente indica o estado lógico 1 e a sua ausência o estado lógico 0. Obviamente que os dois valores lógicos de um bit clássico são mutuamente excludentes.

[2]Também é usado neste trabalho $\overline{O}$ para denotar o valor médio do operador O

Analogamente, a unidade de informação quântica é o bit quântico ou qubit. Um qubit pode ter os valores lógicos "0", "1" ou qualquer superposição deles. Fisicamente, qubits são representados por quaisquer objetos quânticos que possuam dois autoestados ortogonais. Os exemplos mais comuns são: estados de polarização de um fóton (horizontal ou vertical), elétrons em átomos de dois níveis (o que é uma aproximação), elétrons em poços quânticos, e *spins* nucleares [19].

Os estados de um qubit podem ser representados pelos seguintes kets

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{B.14}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{B.15}$$

O conjunto $\{|0\rangle, |1\rangle\}$ forma uma base no espaço de Hilbert de duas dimensões, chamada de base computacional. No caso de um *spin* $1/2$ representa-se o qubit como sendo $|0\rangle \equiv |\uparrow\rangle$ e $|1\rangle \equiv |\downarrow\rangle$.

O estado genérico de um qubit é representado por

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{B.16}$$

em que $|a|^2 + |b|^2 = 1$. Esse estado pode ser parametrizado por ângulos θ e ϕ fazendo-se $a \equiv \cos(\theta/2)$ e $b \equiv \exp(i\phi)\sin(\theta/2)$

$$|\psi\rangle = \cos(\theta/2)|0\rangle + \exp(i\phi)\sin(\theta/2)|1\rangle. \tag{B.17}$$

Essa representação permite que o estado de um qubit seja visualizado como um ponto sobre a superfície de uma esfera. Ela é chamada de esfera de Bloch.

B.1.4 – Aplicações dos Postulados

As matrizes de Pauli são importantes exemplos de transformações unitárias sobre 1 qubit:

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{B.18}$$

$$Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{B.19}$$

$$Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{B.20}$$

Uma outra operação unitária importante sobre 1 qubit é a transformação de Hadamard:

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{X+Z}{\sqrt{2}}. \tag{B.21}$$

Considere agora o seguinte conjunto de operadores de medida de 1 qubit:

$$M_0 = |0\rangle\langle 0| \tag{B.22}$$
$$M_1 = |1\rangle\langle 1|. \tag{B.23}$$

Note que M_0 e M_1 são Hermitianos mas não são unitários. Isto quer dizer que o processo de medida representado por esses operadores é irreversível. Segundo o Postulado 3,

$$p_M(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = |a|^2 \tag{B.24}$$
$$p_M(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = |b|^2. \tag{B.25}$$

Após a medida,

$$|\psi_0\rangle = \frac{a}{|a|}|0\rangle \tag{B.26}$$
$$|\psi_1\rangle = \frac{b}{|b|}|1\rangle. \tag{B.27}$$

Os fatores $a/|a|$ e $b/|b|$ são fases globais (não observáveis) e podem ser descartados. Esses operadores de medidas são exemplos de projetores.

Os vetores de um espaço de Hilbert com dois qubits são obtidos pelo produto tensorial dos vetores do espaço de Hilbert com apenas um qubit

$$\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}. \tag{B.28}$$

A representação matricial de cada um desses vetores da base computacional de dois qubits é:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{B.29}$$

$$|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{B.30}$$

$$|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{B.31}$$

$$|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{B.32}$$

A representação matricial das matrizes de Pauli e do operador de Hadamard nesta base pode ser obtida pelos produtos tensoriais correspondentes com a matriz identidade 2×2

$$O_A = O \otimes \mathcal{I}, \tag{B.33}$$

$$O_B = \mathcal{I} \otimes O, \tag{B.34}$$

em que $O = X, Y, Z, H$. Aqui, adota-se a convenção $|AB\rangle$ para os estados do sistema composto. Essas expressões podem ser facilmente generalizadas para um número arbitrário de qubits [19].