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

Tese de Doutorado

Proteção da Informação Quântica Contra a Ocorrência de Erros Computacionais e de Apagamentos

Gilson Oliveira dos Santos

Francisco Marcos de Assis
Orientador

Campina Grande – PB

Março - 2012

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

Proteção da Informação Quântica Contra a Ocorrência de Erros Computacionais e de Apagamentos

Gilson Oliveira dos Santos

Tese de Doutorado submetida 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.

Francisco Marcos de Assis
Orientador

Campina Grande – PB, Paraíba, Brasil

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG

S237p Santos, Gilson Oliveira dos.
Proteção da Informação Quântica Contra a Ocorrência de Erros Computacionais e de Apagamentos / Gilson Oliveira dos Santos. - Campina Grande, 2012.
130 f.: il.

Tese (Doutorado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática.
Orientador: Prof. Dr. Francisco Marcos de Assis
Referências.

1. Códigos Corretores de Erros Quânticos. 2. Decodificação Quântica. 3. Estados GHZ. I. Título.

CDU 530.145(043)

PROTEÇÃO DA INFORMAÇÃO QUÂNTICA CONTRA A OCORRÊNCIA DE ERROSCOMPUTACIONAIS E DE APAGAMENTOS

GILSON OLIVEIRA DOS SANTOS

Tese Aprovada em 30.03.2012

FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador

RENATO PORTUGAL, Ph.D., LNCC
Componente da Banca

GIULIANO GADIOLI LA GUARDIA, Dr., UEPG-PR
Componente da Banca

HÉLIO MAGALHÃES DE OLIVEIRA, Dr., UFPE
Componente da Banca

AÉRCIO FERREIRA DE LIMA, Dr., UFCG
Componente da Banca

BENEMAR ALENCAR DE SOUZA, D.Sc., UFCG
Componente da Banca

CAMPINA GRANDE – PB
MARÇO - 2012

Agradecimentos

A Deus que me permitiu aprender e progredir por meio do trabalho, perseverar mesmo diante dos obstáculos e encontrar suporte e colaboração de pessoas tão especiais, quanto as que cito aqui.

À minha esposa Carmen, por me apoiar e se fazer presente em todos os momentos desta minha trajetória. À minha filha Sarah Letícia, que com sua inocência e sensibilidade foi uma grande incentivadora para esta etapa de minha vida. A elas dedico este trabalho.

Ao Prof. Francisco M. de Assis com imensa gratidão por ter aceitado me orientar e por acreditar em meu potencial, bem como pela sua disponibilidade, paciência e atenção para comigo, formulando indagações e fornecendo sugestões as quais possibilitaram obter os resultados necessários para esta tese de doutorado.

Ao Prof. Aércio F. de Lima que colaborou decisivamente para o sucesso deste trabalho, tendo disponibilizando parte do seu tempo e atenção para tirar dúvidas e discutir indagações que surgiram ao longo deste trabalho.

Aos membros da banca pela apreciação do meu trabalho e pelas sugestões de melhoria.

Aos meus pais José Muniz dos Santos e Helena Oliveira dos Santos e aos queridos irmãos Givaldo, Ednaldo, Edivaldo, Eliane, Josinaldo e Luciana a quem também dedico este trabalho, pois eles são partes de mim, acreditam e me apoiam incondicionalmente. Aos amigos e familiares, pelas palavras de incentivo e credibilidade no meu profissionalismo.

À Elloá por sua amizade e também por dispor parte de seu tempo colaborando com inestimáveis sugestões e revisões dos textos produzidos ao longo deste doutorado.

Ao casal Vânio e Elizabete, pela amizade e apoio durante esta caminhada na cidade de Campina Grande.

Aos amigos da pós-graduação Christiane, Edmar Nascimento, Eline, Felipe, Heron, Marcos Vinícius, Rex e Rubem. Também aos amigos Gil, Valéria, Val, Tiago, Expedito entre outros que possibilitaram um convívio bastante agradável e relaxante na hora de almoço na cantina de D. Socorro. Amigos dessa longa caminhada que, mesmo diante de um trabalho tão solitário quanto o trabalho de tese, possibilitaram compartilhar ansiedades, conhecimentos e, principalmente, palavras de incentivo e perseverança.

Aos amigos do IFAL Adriana, Carmem, Heron, Lemberg, Nádia e Valéria pelo apoio e incentivo.

Aos professores Roland dos S. Gonçalves, José Carlos P. de Melo e Álvaro J. de Oliveira, pela sensibilidade e empenho dados para o afastamento das atividades do IFAL.

Aos professores Bernardo Lula Jr., Bruno Albert e Edmar Gurjão da UFCG pelo apoio e agradável convivência.

A todo o pessoal administrativo da UFCG/UAEE/COPELE, especialmente à Ângela e Pedro, pela eficiência no trato das questões burocráticas.

Ao IFAL pelo respaldo financeiro e apoio durante todo o período de doutorado.

À CAPES/PIQDTec pelo apoio financeiro e ao IQuanta pelo suporte geral.

Infelizmente não é possível mencionar todos, mas gostaria de dizer que por mais que a ajuda tenha sido por um detalhe pequeno, seu valor só é entendido quando faço uma analogia com as partículas fundamentais: sozinhas, isoladas, elas são apenas partes insignificantes, mas juntas, elas dão origem a muitas coisas importantes. Portanto, tenho que agradecer e muito, a todas essa pequenas, mas importantes ajudas que vocês (aos que não pude lembrar) me proporcionaram.

“Estou convencido das minhas próprias limitações - e esta convicção é minha força.”

—MAHATMA GANDHI

Resumo

Erros computacionais e apagamentos quânticos são tipos de alterações que podem ocorrer naturalmente devido a interação entre os sistemas quânticos e o ambiente. O objetivo desta tese é propor um código capaz de realizar a proteção da informação contra a ocorrência desses tipos de alterações. Para tanto, primeiramente resolveu-se o problema de encontrar uma construção explícita que realize, de maneira eficiente, o cálculo da síndrome de erro para os códigos grafos quânticos (CGQ's). Isso foi conseguido mediante adaptação da transformada de Fourier quântica inversa. Com isso, apresentou-se uma descrição detalhada da operação de decodificação para os CGQ's não-degenerados. Em seguida, realizou-se o aprimoramento do código introduzido por Yang *et al.* [JETP Letters 79 (2004)] para caracterizar um esquema capaz de proteger a informação contra a ocorrência de múltiplos apagamentos quânticos utilizando-se estados Greenberger-Horne-Zeilinger (GHZ), que são estados maximamente emaranhados. A técnica desenvolvida neste esquema permite proteger k-qubit (do inglês, *quantum bit*) de informação, sendo $k \geq 3$, contra a ocorrência de $t = \lfloor k/2 \rfloor$ apagamentos quânticos. O esquema proposto faz uso de $(t + 1)$ blocos redundantes e possui a restrição de que cada apagamento deve ocorrer em blocos distintos. Visando cumprir o objetivo desta tese, propôs-se um esquema de concatenação em que o código externo é um código corretor de erros computacionais e o código interno é um código corretor de apagamentos quânticos que não realiza medição. Se esta construção for respeitada, o código concatenado resultante protege a informação contra a ocorrência de erros computacionais e de apagamentos quânticos. Por fim, os resultados obtidos são ilustrados por meio de um exemplo em que um qubit de informação é protegido contra a ocorrência de dois apagamentos e um erro computacional.

Palavras-chave: Códigos Corretores de Erros Quânticos, Códigos Grafos Quânticos, Decodificação Quântica, Transformada de Fourier Quântica Inversa, Códigos Corretores de Apagamentos Quânticos, Estados GHZ, Códigos Concatenados.

Abstract

Computational errors and quantum erasures are the types of changes that may occur naturally due to the interaction between quantum systems and the environment. The aim of this thesis is to propose a code capable of performing the information protection against the occurrence of these types of changes. To do this, first we solve the problem of finding an explicit construction that performs efficiently the calculation of the error syndrome for the quantum graphs codes (QGC's). This was achieved by means of an adjustment of the inverse quantum Fourier transform. With this, we present a detailed description of the decoding operation for non-degenerate QGC's. After that, we introduce an improvement of the code given by Yang *et al.* [JETP Letters 79 (2004)] to characterize a scheme able to protect the information against the occurrence of multiple quantum erasures using Greenberger-Horne-Zeilinger (GHZ) states. The technique developed in this scheme allows to protect k-qubit ($k \geq 3$) information against the occurrence of $t = \lfloor k/2 \rfloor$ quantum erasures. The proposed scheme makes use of $(t + 1)$ redundant blocks and has the restriction that each erasure must occur in different blocks. Aiming to fulfill the goals of this thesis, we propose a concatenation scheme in which the external code is a quantum error-correcting code and the internal code is quantum erasure-correcting code that does not perform measurements. If the requirements of this construction are met, the resulting concatenated code protects the information against the occurrence of computational errors and quantum erasures. Finally, we illustrate the results obtained in this work by means of an example in which one qbit of information is protected against the occurrence of two erasures and one computational error.

Keywords: Quantum Error-Correcting Codes, Quantum Graph Codes, Quantum Decoding, Inverse Quantum Fourier Transform, Quantum Erasure-Correcting Codes, GHZ States, Concatenated Codes.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

$\mathbb{C}$ Conjunto dos números complexos

$\mathbb{Z}$ Conjunto dos números inteiros

$\mathbb{Z}_N$ Grupo formado pelo conjunto $\{0, \cdots, N-1\}$ com soma módulo N

$\mathbb{F}_p$ Corpo finito de ordem p

$|B|$ Cardinalidade de um conjunto B

$\Gamma_{j,k}$ Elemento linha j e coluna k (indexado a partir de zero) de uma matriz Γ

$\Gamma_{m \times n}$ Matriz Γ qualquer, de dimensão $m \times n$

$\mathcal{H}$ Espaço de Hilbert

$|\cdot\rangle$ Vetor no espaço de Hilbert, em notação de Dirac, e. g., $|\psi_k\rangle$

$\langle\cdot|$ Vetor dual (transposto conjugado) na notação de Dirac, e. g., $\langle\psi_j|$

$(\cdot)^T$ Transposto, e. g., A^T, b^T

$(\cdot)^\dagger$ Transposto conjugado, e. g., $A^\dagger$, $b^\dagger$

$(\cdot)^*$ Complexo conjugado, e. g., A^*, z^*

$\lfloor\cdot\rfloor$ Maior número inteiro que seja menor ou igual a um número (*floor*)

$\perp$ Ortogonalidade entre vetores

$|\psi_k\rangle \otimes |\psi_j\rangle$ Produto tensorial entre $|\psi_k\rangle$ e $|\psi_j\rangle$

$|\psi_k\rangle\,|\psi_j\rangle$ Produto tensorial entre $|\psi_k\rangle$ e $|\psi_j\rangle$ (notação compacta)

$|\psi_k\psi_j\rangle$ Produto tensorial entre $|\psi_k\rangle$ e $|\psi_j\rangle$ (notação compacta)

$(\cdot)^{\otimes n}$ Produto tensorial repetido n vezes, e. g., $H^{\otimes s} \equiv \underbrace{H \otimes \ldots \otimes H}_{s}$

$\bigotimes_{d=1}^{n} |0^{\otimes k}\rangle_{(d)}$ Representa a sequência de produtos tensoriais $|0^{\otimes k}\rangle_{(1)} \otimes \ldots \otimes |0^{\otimes k}\rangle_{(n)}$

$\bigcirc_{j=1}^{n} G^{(j)}$ Representa a sequência de composições $G^{(1)} \circ \ldots \circ G^{(n)}$;

$|\psi_k\rangle \langle\psi_j|$ Produto externo entre $|\psi_k\rangle$ e $|\psi_j\rangle$

$\langle\psi_k|\psi_j\rangle$ Produto interno entre $|\psi_k\rangle$ e $|\psi_j\rangle$

$\langle\psi_k| \mathbf{A} |\psi_j\rangle$ Produto interno entre $|\psi_k\rangle$ e $\mathbf{A} |\psi_j\rangle$. Equivalente ao produto interno entre $\mathbf{A}^{\dagger} |\psi_k\rangle$ e $|\psi_j\rangle$

$\hat{\mathbf{H}}$ Operador hamiltoniano

$\mathcal{G}$ Representa um grupo finito

$\mathcal{E}$ Operador de interação

Ω Processo ruidoso

ρ Operador densidade

$Tr(\cdot)$ Traço de matriz

i Unidade imaginária, $\sqrt{-1}$

$\mathbf{log}$ Logaritmo na base dois

$\simeq$ Representa uma relação preservando isomorfismo entre dois objetos.

$\mathbf{O}(\cdot)$ Complexidade computacional no pior caso: diz-se $f(x) = O(g(x))$ se existe um C e um x_0 tal que $|f(x)| < Cg(x), \forall x > x_0$

$\oplus$ Soma módulo dois, e. g., $a \oplus b \equiv a + b \ (mod\ 2)$

CAPÍTULO 1

Introdução

Ao longo das últimas décadas, a Ciência da Informação Quântica tem emergido para buscar respostas para a pergunta: pode-se ganhar alguma vantagem armazenando, transmitindo e processando informação codificada em sistemas que exibem unicamente propriedades quânticas? Hoje entende-se que a resposta é sim e muitos grupos de pesquisa ao redor do mundo estão trabalhando em direção a uma meta altamente ambiciosa tecnologicamente - aquela de construir um computador quântico, o qual poderá melhorar drasticamente o poder computacional para tarefas específicas. Além disso, muitas pesquisas também estão sendo desenvolvidas em Comunicação Quântica, a qual possibilitará o compartilhamento de segredos com segurança garantida pelas leis da física [3].

A informação em computadores tradicionais ou clássicos, é representada por uma sequência de 0's e 1's denominados bits. A informação quântica, por sua vez, usa *bits quânticos* ou *qubits*. Um qubit (do inglês quantum bit) é um sistema quântico que tem duas configurações distinguíveis correspondendo aos valores dos bits 0 e 1. Mas, sendo um sistema quântico, o princípio da superposição se aplica: o estado do qubit pode ser qualquer combinação ou superposição das duas configurações. Da mesma forma, uma sequência de qubits pode estar em qualquer superposição de suas configurações de qubits. Isto permite que a interferência quântica possa ser explorada, enriquecendo grandemente o tipo de informação que pode ser representada [4].

Um dos mais importantes obstáculos em processamento da informação quântica é um fenômeno conhecido como *descoerência* [5, 6]. A utilização de sistemas quânticos de modo eficiente nas diversas aplicações da computação e do processamento da informação está condicionada à mitigação dos efeitos da descoerência, que pode pode ser visto como uma consequência do emaranhamento entre o sistema quântico e o ambiente. Uma das implicações da descoerência é a ocorrência de perda de informação quântica [7, 8].

Para minimizar os efeitos da descoerência nas aplicações dos sistemas quânticos utilizam-se *códigos corretores de erros quânticos* (CCEQ's). Estes códigos têm sido integrados a vários

esquemas de Computação e Comunicação Quânticas e, por esta razão, têm recebido muita atenção no decorrer dos últimos anos.

Shor [9] propôs um algoritmo quântico para um problema extremamente importante - o de encontrar os fatores primos de um inteiro - mostrando um ganho exponencial sobre o melhor algoritmo clássico conhecido. Este resultado atraiu grande interesse não somente devido a crença de que este problema não tem uma solução eficiente em computadores clássicos, mas também porque forneceu fortes evidências de que os computadores quânticos são mais poderosos que os computadores clássicos.

A construção de códigos quânticos é diferente da construção dos códigos clássicos, pois leva em conta as restrições impostas pela Mecânica Quântica [8]. Essas restrições impedem que os resultados obtidos para os códigos clássicos sejam diretamente estendidos para o domínio quântico sem uma análise prévia, a fim de verificar se as restrições quânticas não estão sendo violadas.

Nos sistemas clássicos, os códigos corretores de erros são projetados para proteger a informação de determinados tipos de erros, os quais são representados por um modelo de canal. Analogamente, nos sistemas quânticos, os erros também são modelados por um canal, que pode representar tanto um canal de comunicação físico, a passagem do tempo para um conjunto de qubits interagindo com o ambiente ou ainda o resultado de uma operação com uma porta quântica ruidosa em um computador quântico [10].

Um tipo de efeito causado pela descoerência no estado quântico pode ser caracterizado como sendo composto por alterações que são consistentes com as condições estabelecidas por Knill-Laflamme [11]. Tais alterações são representadas pelas matrizes de Pauli σ_X, σ_Y e σ_Z. Estas atuam no que se denomina de *espaço computacional* [8] e por isso são chamadas de *erros computacionais* [12]. Um dos modelos de canais que descreve este tipo de efeito é, por exemplo, o de *despolarização* [8, 13].

Para a correção de erros quânticos, vários resultados merecem destaque, pois constituem a base do que hoje é conhecido como a teoria quântica para a correção de erros [14]. Um dos resultados teóricos importantes são as condições necessárias e suficientes para que um CCEQ seja capaz de corrigir um determinado conjunto de erros. Tais condições foram provadas independentemente por Bennett *et al.* [15] e por Knill-Laflamme [11].

O primeiro CCEQ, considerado como um análogo quântico do código de repetição clássico, foi proposto por Shor em 1995 [5]. O primeiro código quântico MDS (do inglês *Maximum-Distance-Separable*) que codifica um qubit de informação, o código de cinco qubits, foi descoberto por Laflamme *et al.* [16] e independentemente por Bennett *et al.* [15].

O desenvolvimento da teoria quântica para a correção de erros então tornou-se sistemático. Uma construção de Calderbank, Shor e Steane [17, 18] mostrou que era possível construir códigos quânticos a partir de códigos clássicos lineares - os códigos CSS. Além disso, Gottesman [10, 19] desenvolveu o *formalismo estabilizador*, que foi utilizado por ele para definir

uma ampla classe de códigos quânticos, os *códigos estabilizadores*. Nessa visão, CCEQ's são auto-espaços simultâneos de um grupo de operadores de comutação, o estabilizador.

Recentemente, vários tipos novos de códigos quânticos, tais como códigos Bose-Chaudhuri-Hocquenghem (BCH) quânticos [20, 21], códigos Reed-Solomon quânticos [22], códigos convolucionais quânticos [23, 24], códigos Low-Density Parity-Check (LDPC) quânticos [25–27] e códigos quânticos de subsistemas [28], têm sido estudados. Entretanto, essas construções demandam um grande esforço para a verificação das condições de Knill-Laflamme [11].

Para minimizar esta dificuldade, Schlingemann e Werner [1] fizeram uso da teoria dos grafos para apresentar uma nova maneira de construir códigos estabilizadores de tal forma que as condições necessárias e suficientes para a correção de erros sejam diretamente "visíveis" da estrutura de um grafo. Com isso, eles adaptaram as condições de Knill e Laflamme [11] e estabeleceram as condições necessárias e suficientes para um grafo gerar um CCEQ. Os códigos construídos dessa forma são denominados de *códigos grafos quânticos* (CGQ's) [1,29]. Usando esse método, novos códigos quânticos foram construídos [30–32].

Embora diversos autores proponham esquemas de codificação para códigos quânticos, a caracterização de esquemas de decodificação não tem sido extensivamente explorada. Isso possivelmente ocorre devido a dificuldade em se conseguir construir um procedimento para calcular a síndrome de erro para os códigos quânticos.

Schlingemann [33] mostrou que a operação de decodificação para um CGQ pode ser realizada em modelos de computador *one-way* e também provou que, para qualquer síndrome de erro calculada para um CGQ, existe uma operação de correção local apropriada. Entretanto, até o presente momento, não são encontrados na literatura trabalhos que apresentem como realizar o cálculo da síndrome de erro para um CGQ.

Uma das contribuições desta tese é a construção explícita de um operador que possibilita calcular a síndrome de erro para os CGQ's. Com isso, apresenta-se aqui uma descrição detalhada de como deve ser a operação de decodificação para os CGQ's não-degenerados.[1] Na construção desse operador, considerou-se as condições que um grafo deve satisfazer para corrigir um número de e erros [33], bem como a adaptação da *transformada de Fourier quântica inversa* (TFQI) para os CGQ's. A adoção da TFQI no cálculo da síndrome de erro favorece a implementação eficiente da operação de decodificação proposta para os CGQ's em computadores quânticos [8].

Além das alterações mencionadas (erros computacionais), existe uma outra fonte significante de erro – a perda (ou apagamento) de qubits em Computação Quântica (CQ). O qubit é o elemento básico de informação em CQ. A definição exata dos qubits pressupõe isolamento perfeito. Nessas situações, o qubit poderia ser definido como sendo formado pelo espaço do sistema quântico com exatamente dois estados ortonormais. Em situações menos idealizadas, o qubit faria parte de um subespaço de um sistema com muitos níveis. A ausência de isolamento do subespaço dos qubits é uma possível origem das fontes de erros ocasionadas pela transição

[1] Em um código *não-degenerado* os erros são vistos diferentemente quando agindo no subespaço de codificação.

desses estados (do subespaço) para outros níveis a ele acessíveis, fazendo com que o qubit seja perdido [34]. Este problema é comum em implementações com vários qubits candidatos, tais como junções de Josephson [35], átomos neutros em reticulados ópticos [36] e, mais notoriamente, em fótons isolados que podem ser perdidos durante o processamento ou podem ter a perda atribuída ao uso de fontes e/ou detectores ineficientes [37, 38].

Grassl *et al.* [39] ao considerarem a situação na qual a posição dos qubits errôneos (perdidos) é conhecida, chamaram esse modelo de *canal de apagamento quântico* (*quantum erasure channel* - QEC, em inglês). Assim, um código que trata esse tipo de alteração é denominado de *código corretor de apagamentos quânticos* (CCAQ). Alguns cenários físicos nos quais a posição de um qubit de erro é sinalizada, tal como emissão espontânea, foram apresentados em [39].

Embora transições estimuladas sejam mais frequentes que transições espontâneas na faixa de micro-ondas (frequência $\sim 2 \times 10^{10}$Hz), as transições espontâneas são mais frequentes que transições estimuladas no domínio óptico (frequência $\sim 6 \times 10^{14}$Hz) [40]. Deve-se frisar que atualmente a óptica é o domínio amplamente adotado para a Comunicação Quântica, o que faz com que a ocorrência de apagamentos seja relevante para este tipo de comunicação. Além disso, é muito frequente a perda de fótons (apagamento) em uma linha de transmissão, sendo esse considerado o principal obstáculo para a sobrevivência da coerência quântica em comunicações [41]. Como consequência, a construção de um CCAQ é vista como uma nova ferramenta para o estabelecimento da coerência da óptica quântica em longas distâncias.

Considerando as preocupações em relação ao cenário descrito para apagamento quântico, Yang *et al.* [42] apresentaram um CCAQ que protege três qubits de informação contra a ocorrência de um apagamento, usando estados GHZ [43]. Durante este trabalho de pesquisa foi realizada uma extensão deste código a fim de proteger cinco qubits de informação (ver [44]), e depois disso foi realizada uma generalização para proteger $k \geq 3$ qubits de informação [45]. Embora a generalização proposta para este esquema seja para um número arbitrário de qubits, verificou-se que só há proteção contra a ocorrência de um único apagamento.

Do ponto de vista de algumas aplicações, tais como as que lidam com vários qubits [35, 36] ou para resolver os efeitos da atenuação em linha de transmissão em óptica quântica [41], ou ainda para compartilhamento de segredo quântico [46], a ocorrência de apagamento dificilmente está restrita a apenas um qubit.

Lassen *et al.* [41] apresentaram uma primeira realização experimental de um aparato capaz de fazer a proteção contra a ocorrência de apagamentos quânticos. Entretanto, tal aparato foi desenvolvido para *sistemas quânticos com variáveis contínuas* (do inglês *continuous-variable systems*). Um modelo de sistema para o qual se aplica variáveis contínuas é o oscilador harmônico quântico. Sistemas quânticos como este são de dimensão infinita e têm coordenadas canônicas correspondentes à posição e *momentum*. Estes fatores observáveis não têm um conjunto discreto de autovalores, mas um espectro contínuo deles. Daí, o termo "sistemas de variáveis contínuas" ter sido cunhado para descrever este tipo de situação [47]. Uma limitação

em se trabalhar com esses sistemas é que não se tem controle completo sobre falhas que venham a ocorrer nas operações realizadas. Essa dificuldade decorre devido ao fato de que o espaço de Hilbert subjacente a estes possui dimensão infinita.

Nesta tese caracteriza-se um esquema que tem um conjunto discreto de autovalores para proteger a informação contra a ocorrência de múltiplos apagamentos quânticos pelo aprimoramento do código dado por Yang *et al.* [42]. A técnica desenvolvida neste esquema permite proteger k-qubits ($k \geq 3$) de informação contra a ocorrência de $t = \lfloor k/2 \rfloor$ apagamentos quânticos. O esquema proposto faz uso de $(t + 1)$ blocos redundantes e possui a restrição de que cada apagamento deve ocorrer em blocos distintos. Com relação a restrição mencionada, uma estratégia de implementação que pode ser utilizada é o envio dos blocos por meio de canais diferentes, tendo em vista que trabalhos experimentais relatam o processo de detecção da ocorrência de apagamentos quânticos através de canais distintos [41, 48].

Uma característica especial do esquema proposto é que nenhuma operação de medição é requerida, pois a informação sobre a ocorrência de apagamento quântico é disponibilizada naturalmente pelo sistema (por exemplo, via emissão espontânea). Por isso, a operação de restauração usada no referido esquema consiste apenas de operadores unitários.

Erros computacionais e apagamentos quânticos são tipos de alterações que podem ocorrer naturalmente devido a interação entre os sistemas quânticos e o ambiente. Diante da impossibilidade de ignorar a existência de tais alterações, existem relatos na literatura que destacam a importância prática do desenvolvimento de códigos que sejam capazes de proteger a informação contra esses dois tipos de alterações [13, 49].

Para reforçar o que foi mencionado anteriormente, tem-se que, enquanto a perda de fótons (apagamento) irá certamente ser uma importante fonte de ruído em alguns modelos de implementações práticas, outras fontes de ruído, tal como defasamento (erro computacional), estarão também presentes. Além disso, resultados conhecidos na teoria de correção de erros quânticos asseguram que possuindo a habilidade para proteger contra despolarização, será também assegurada a habilidade para proteger contra outros tipos de ocorrências de ruído, incluindo, defasamento, amortecimento de amplitude, etc. [49]. Devido a isso, o ruído de despolarização é usado como um representante geral para todos os tipos de ruídos locais que não a perda de qubits. Dessa forma, é interessante se considerar um modelo de ruído que envolva tanto a ocorrência de erros computacionais quanto a ocorrência de apagamentos quânticos.

Em geral, é possível manipular códigos existentes para construir um novo código adequado para um modelo de erro mais geral. Um dos artifícios que pode ser usado para isso é a *concatenação*, que possibilita a criação de um novo código por meio de códigos existentes. Embora esta técnica já tenha sido aplicada a vários cenários no processamento da informação quântica [13, 50–54], não foi encontrada nenhuma referência na literatura em que houvesse a concatenação de um CCEQ com um CCAQ.

Objetivando fechar esta lacuna, como outra contribuição, esta tese mostra que se pode concatenar um CCEQ com um CCAQ. Para isso, é exigido que o código externo da concate-

nação seja um CCEQ, enquanto que o código interno seja um CCAQ em que não se realiza medição. Se esta construção for respeitada, o código concatenado resultante protege a informação contra erros computacionais bem como apagamentos quânticos.

Este documento está organizado sob a forma de sete capítulos e três apêndices. O Capítulo 2 introduz alguns conceitos e definições da Mecânica Quântica adequados ao entendimento dos conteúdos tratados neste documento, bem como alguns princípios necessários para a correção de erros quânticos. O Capítulo 3 apresenta uma descrição geral dos CGQ's, incluindo a relação destes códigos com os códigos estabilizadores e as condições de correção de erro. O Capítulo 4 apresenta o primeiro resultado: a construção de um operador para calcular a síndrome de erro para os CGQ's. Neste Capítulo também são dadas descrições dos erros e de uma proposta de operação de decodificação para os CGQ's não-degenerados. O Capítulo 5 apresenta o segundo resultado: a caracterização de um esquema para proteger a informação contra a ocorrência de múltiplos apagamentos quânticos. O Capítulo 6 apresenta o terceiro resultado: uma proposta de concatenação capaz de proteger a informação contra a ocorrência de erros computacionais e apagamentos quânticos. O Capítulo 7 apresenta as conclusões deste trabalho. No apêndice A é apresentada a lista de artigos produzidos. No apêndice B são abordados alguns tópicos inerentes ao processamento da informação quântica. Por fim, no apêndice C é dado uma breve introdução a Caracteres de Grupo.

CAPÍTULO 2

Preliminares

Neste capítulo introduz-se alguns conceitos e definições da Mecânica Quântica adequados ao entendimento dos conteúdos tratados neste documento bem como alguns princípios para correção de erros quânticos. Alguns tópicos fundamentais para o processamento da informação quântica também são apresentados no apêndice B. Especificamente, aborda-se neste capítulo os seguintes tópicos: os postulados da mecânica quântica, uma visão geral sobre estados GHZ, uma descrição do canal de apagamento quântico e fundamentos para a correção de erros quânticos.

2.1 Postulados da Mecânica Quântica

A mecânica quântica é uma estrutura matemática para o desenvolvimento de teorias físicas [8]. Matematicamente falando, a mecânica quântica é uma teoria, pois é regida por um conjunto de postulados (axiomas). Esses postulados fornecem a conexão entre o mundo físico e o formalismo matemático da mecânica quântica. Esses postulados são descritos e comentados a seguir.

2.1.1 Primeiro Postulado – Espaço de Hilbert

Todos os eventos que ocorrem durante a evolução dos estados em um sistema quântico são modelados matematicamente no espaço de Hilbert das funções de ondas (que é usado para modelagens de sistemas infinitos). No entanto, para a compreensão da comunicação e computação quânticas, é necessário somente o conhecimento de sistemas quânticos finitos. Em outras palavras, não é necessário modelar sistemas quânticos no espaço de Hilbert das funções de ondas [55]. Considera-se somente os *espaços vetoriais complexos* de dimensão finita munidos de produto interno.[1] Espaços de Hilbert que sejam assim tem a vantagem de não precisar se preocupar com funções de onda. Dessa forma, segue o primeiro postulado da mecânica quântica.

[1] Um *espaço vetorial complexo* é um espaço vetorial cujos vetores possuem coordenadas descritas por números complexos.

Postulado 2.1. *[8] Associado a qualquer sistema físico isolado existe um espaço vetorial complexo com produto interno (espaço de Hilbert) conhecido como espaço de estados do sistema. O sistema é completamente descrito por seu vetor de estado, que é um vetor unitário no espaço de estados do sistema.*

O sistema quântico mais simples é o qubit (ou bit quântico), um sistema quântico com um espaço de estados com duas dimensões. O estado $|\psi\rangle$ associado com um qubit pode ser qualquer vetor unitário no espaço vetorial bidimensional gerado por $|0\rangle$ e $|1\rangle$ sobre os números complexos [56]. Usando a notação de Dirac, um qubit pode ser representado como

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \tag{2.1}$$

sendo que $|0\rangle$ e $|1\rangle$ formam uma base ortonormal para o espaço de estados do sistema conhecida como a *base computacional* e a e b são números complexos arbitrários restringidos somente pela necessidade que $|\psi\rangle$, como $|0\rangle$ e $|1\rangle$, seja um vetor unitário no espaço vetorial complexo, isto é, que satisfaçam a relação de normalização $|a|^2 + |b|^2 = 1$. O estado $|\psi\rangle$ é dito ser uma *superposição* dos estados $|0\rangle$ e $|1\rangle$ com *amplitudes* a e b. Assim, o qubit $|\psi\rangle$ pode colapsar para o estado $|0\rangle$ com probabilidade $|a|^2$, ou para o estado $|1\rangle$ com probabilidade $|b|^2$.

Sistemas quânticos de dimensões maiores que dois são comumente chamados de *qudits* (do inglês *quantum digits*).

Como um estado geral de um único qubit é qualquer superposição normalizada (2.1) de dois estados possíveis, o estado geral $|\psi\rangle$ que a natureza permite que seja associada com dois qubits é qualquer superposição normalizada de quatro estados ortogonais

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{2.2}$$

com amplitudes complexas restritas somente pela condição de normalização

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1. \tag{2.3}$$

Isto generaliza de modo óbvio para n qubits, no qual o estado geral $|\psi\rangle$ pode ser qualquer superposição de 2^n estados diferentes, com amplitudes nas quais as somas das magnitudes ao quadrado seja a unidade:

$$|\psi\rangle = \sum_{0\leq x<2^n} \alpha_x\,|x\rangle_n\,, \tag{2.4}$$

e

$$\sum_{0\leq x<2^n} |\alpha_x|^2 = 1. \tag{2.5}$$

Na definição anterior de qubit, nada é dito sobre o meio físico em que as bases do qubit são construídas. A base $\{|0\rangle, |1\rangle\}$ pode ser fisicamente codificada como *spin-up* e *spin-down* de uma partícula, direção vertical e horizontal de polarização, etc ... Felizmente, para que se possa entender como ocorre o processamento da comunicação e computação quânticas, não se faz necessária a abordagem dos aspectos físicos envolvidos na criação destes. Ou seja, a definição de qubit dada em (2.1) é uma abstração da implementação física, mas nem por isso deixa de ser menos significativa ou dificulta o entendimento dos conceitos envolvidos na comunicação e computação quânticas.

Um qubit pode ser geometricamente visualizado em três dimensões, como na Figura 2.1. Essa representação geométrica é chamada de esfera de Bloch. Devido à restrição de normalização (i.e, a norma do vetor no espaço de Hilbert deve ser igual a 1), pode-se expressar genericamente o estado de um qubit como $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\mathrm{sen}(\theta/2)\,|1\rangle$, em que os ângulos θ e ϕ definem um ponto na esfera. Todas as transformações que ocorrem num qubit são, na verdade, rotações do vetor $|\psi\rangle$ na esfera de Bloch.

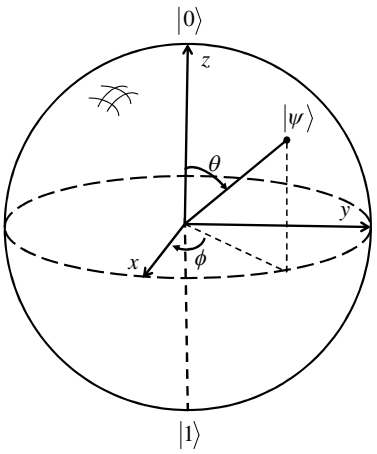

Figura 2.1 Esfera de Bloch: representação 3D do qubit.

Além da representação utilizando-se vetores de estado indicada no Postulado 2.1, existe uma outra representação que as vezes é mais conveniente. Nessa representação, o sistema quântico é descrito por um operador densidade denotado por ρ. O operador densidade permite descrever sistemas quânticos cujo estado não é completamente conhecido, devido principalmente às incertezas na sua preparação. Para um sistema quântico que pode estar em um dentre muitos estados $|\psi_i\rangle$ com probabilidade p_i, o operador densidade é definido por:

$$\rho \equiv \sum_i p_i \,|\psi_i\rangle \,\langle\psi_i|\,. \tag{2.6}$$

Um sistema quântico cujo vetor de estado $|\psi\rangle$ é conhecido exatamente é dito estar em um *estado puro*. Nesse caso, o operador densidade é dado por $\rho = |\psi\rangle\,\langle\psi|$. Quando o estado

não é puro, ele se encontra em uma mistura de estados. O qubit representado em (2.1) é um exemplo de estado puro com operador densidade dado por:

$$\rho = |a|^2 |0\rangle \langle 0| + ab^\dagger |0\rangle \langle 1| + a^\dagger b |1\rangle \langle 0| + |b|^2 |1\rangle \langle 1| = \begin{bmatrix} |a|^2 & ab^\dagger \\ a^\dagger b & |b|^2 \end{bmatrix}. \tag{2.7}$$

2.1.2 Segundo Postulado – Evolução Dinâmica

O princípio fundamental na mudança de estados em um sistema quântico são as transformações unitárias. Uma transformação unitária é uma transformação linear que é inversível e cuja inversa é igual a sua conjugada transposta. Ou seja, a matriz U é unitária se

$$UU^\dagger = U^\dagger U = I, \tag{2.8}$$

onde $U^\dagger$ é a conjugada transposta de U e I é a matriz identidade. As transformações unitárias são inerentes a qualquer sistema quântico dinâmico, i.e., sistemas que sofrem mudanças em seus estados. As transformações unitárias podem ser vistas como uma característica da mecânica quântica, devido à sua grande importância em todas operações modificadoras de um sistema. Assim sendo, o postulado a seguir dá uma prescrição de como o estado $|\psi\rangle$ de um sistema quântico muda com o tempo.

Postulado 2.2. *[8] A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Ou seja, o estado $|\psi\rangle$ do sistema no tempo t_1 está relacionado ao estado $|\psi'\rangle$ do sistema no tempo t_2 por um operador unitário U o qual depende somente dos tempos t_1 e t_2,*

$$|\psi'\rangle = U |\psi\rangle . \tag{2.9}$$

O Postulado 2.2 requer que o sistema descrito seja fechado. Ou seja, que ele de nenhuma maneira interaja com outros sistemas.

Intuitivamente falando, a transformação unitária corresponde a uma rotação no espaço vetorial que preserva o mesmo comprimento do vetor e a mesma quantidade de informação do sistema. A preservação do comprimento do vetor garante que a probabilidade total de um conjunto de estados sempre permaneça a mesma (igual a 1 se considerado o qubit normalizado) e que a norma do vetor não extrapole os limites da esfera de Bloch. A preservação de informação reflete o princípio universal da conservação com relação a sistemas físicos quânticos, que estabelece que todas as mudanças em nível microscópico preservam a informação. Em outras palavras, o estado quântico (vetor de amplitudes) de um sistema isolado pode determinar (probabilisticamente) a qualquer momento o estado quântico do sistema no passado e no futuro.

A relação temporal existente entre os estados $|\psi\rangle$ e $|\psi'\rangle$ no Postulado 2.2 é melhor observada através da equação de Schrödinger:

$$\frac{d}{dt}\left|\psi(t)\right\rangle = -i\hat{\mathrm{H}}\left|\psi(t)\right\rangle . \tag{2.10}$$

Na equação (2.10), $\hat{\mathrm{H}}$ é um operador auto-adjunto chamado de Hamiltoniano do sistema fechado. A equação (2.9) representa o equivalente discreto da equação de Schrödinger, obtida considerando-se quantidades infinitesimais dt, resultando em:

$$\left|\psi(t)\right\rangle = e^{-it\hat{\mathrm{H}}}\left|\psi(0)\right\rangle = U(t)\left|\psi(0)\right\rangle . \tag{2.11}$$

2.1.3 Terceiro Postulado – Medida

Foi postulado que sistemas quânticos fechados se transformam de acordo com uma evolução unitária. Entretanto, se um sistema físico externo observa o sistema quântico para tentar saber o que está havendo dentro deste sistema, então haverá uma interação que fará com que o sistema não seja totalmente fechado, e portanto não necessariamente sujeito à evolução unitária. Para explicar o que ocorre quando isso é feito, introduz-se a seguir um postulado que fornece um meio para descrever os efeitos das medidas em sistemas quânticos.

Postulado 2.3. *[8] As medidas quânticas são descritas por uma coleção $\{M_m\}$ de operadores de medida. Esses operadores atuam no espaço de estados do sistema que está sendo medido. O índice m se refere aos efeitos das medidas que podem ocorrer em um experimento. Se o estado do sistema quântico for $|\psi\rangle$ imediatamente antes da medida, então a probabilidade de um resultado m ocorrer é dada por*

$$p(m) = \left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle , \tag{2.12}$$

e o estado do sistema depois da medida será

$$\frac{M_m\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle}}. \tag{2.13}$$

Os operadores de medida satisfazem a equação de completude,

$$\sum_m M_m^\dagger M_m = I. \tag{2.14}$$

Relacionado ao Postulado 2.3 está o conceito de *observável*. Um observável é definido como uma propriedade de um sistema físico que, em princípio, pode ser medida, tal como a posição ou a velocidade de uma partícula. Na mecânica quântica, um observável é representado por um operador autoadjunto, ou seja, um operador $\mathbf{A}$ tal que $\mathbf{A} = \mathbf{A}^\dagger$. Um operador autoadjunto em um espaço de Hilbert $\mathcal{H}$ possui uma representação espectral, ou seja, os seus

autoestados formam uma base ortonormal completa em $\mathcal{H}$. Um operador autoadjunto $\mathbf{A}$ pode ser então expresso como:

$$\mathbf{A} = \sum_n \lambda_n \mathbf{P}_n, \tag{2.15}$$

em que λ_n é um autovalor de $\mathbf{A}$ e $\mathbf{P}_n$ é a projeção ortogonal correspondente no espaço dos autovetores com autovalor λ_n. Se os autovalores λ_n são não degenerados ($\lambda_n \neq \lambda_m, n \neq m$) então $\mathbf{P}_n = |n\rangle \cdot |n\rangle^\dagger = |n\rangle \langle n|$ é a projeção no autovetor indicado por $|n\rangle$. Os projetores $\mathbf{P}_n$ verificam as relações:

$$\mathbf{P}_n \mathbf{P}_m = \delta_{n,m} \mathbf{P}_n, \tag{2.16}$$

$$\mathbf{P}_n^\dagger = \mathbf{P}_n. \tag{2.17}$$

As medidas quânticas obtidas por meio de projetores $\mathbf{P}_n$ são conhecidas como medidas projetivas, ortogonais ou de Von Neumann. Ao medir um sistema quântico, a saída numérica do processo de medição de um observável $\mathbf{A}$ é um autovalor de $\mathbf{A}$. O estado do sistema é modificado de modo que, logo após a medição, o estado quântico passa a ser um autoestado do observável $\mathbf{A}$ correspondente ao autovalor medido. De acordo com o Postulado 2.3, se o estado quântico imediatamente antes da medida for $|\psi\rangle$, então a saída λ_n é obtida com probabilidade

$$P(\lambda_n) = \langle\psi| \mathbf{P}_n |\psi\rangle = \| \mathbf{P}_n |\psi\rangle \|^2 . \tag{2.18}$$

Se a saída λ_n é obtida, o estado normalizado pós-medição é

$$|\psi'\rangle = \frac{\mathbf{P}_n |\psi\rangle}{\| \mathbf{P}_n |\psi\rangle \|} = \frac{\langle n|\psi\rangle |n\rangle}{\| \langle n|\psi\rangle |n\rangle \|} = \frac{|n\rangle}{\| |n\rangle \|}. \tag{2.19}$$

Uma medida projetiva realizada em um espaço de Hilbert de dimensão D_S resulta no máximo em D_S resultados possíveis. Esse tipo de medida não é a medida quântica mais geral, mas é a de mais fácil implementação prática e é suficiente no estudo dos códigos quânticos.

A medida quântica mais geral é a POVM (do inglês *Positive Operator Valued Measure*). As medidas POVM são especialmente úteis nos casos em que o estado do sistema quântico, após a realização da medida, é de pouco interesse sendo mais importante a obtenção de estatísticas da medida. A forma tradicional de construção de um POVM com $N \geq D_S$ elementos é por meio do aumento da dimensão do espaço de Hilbert, mediante a inserção de qubits auxiliares, para uma dimensão no mínimo igual a N para, em seguida, realizar uma medida projetiva no sistema aumentado.

2.1.4 Quarto Postulado – Sistemas Compostos e Produto Tensorial

Suponha que se esteja interessado em sistemas quânticos compostos feitos com base em dois ou mais sistemas físicos distintos. O postulado a seguir descreve como o espaço de estados de um sistema composto é construído com base no espaço de estados dos sistemas que o compõem.

Postulado 2.4. *[8] O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas físicos que o compõem. Além disso, se houver sistemas numerados de 1 até n, e o sistema número i for preparado no estado $|\psi_i\rangle$, então o estado do sistema composto será $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.*

Apresenta-se uma heurística que algumas vezes é usada para explicar o que é declarado no Postulado 2.4. O *princípio da superposição da mecânica quântica*, o qual declara que se $|x\rangle$ e $|y\rangle$ são dois estados de um sistema quântico, então qualquer superposição $a\,|x\rangle + b\,|y\rangle$ pode também ser um estado permitido de um sistema quântico, em que $|a|^2 + |b|^2 = 1$. Para sistemas compostos, vê-se que se $|A\rangle$ é um estado do sistema A, e $|B\rangle$ é um estado do sistema B, então pode haver algum estado correspondente, no qual se possa denotar $|A\rangle\,|B\rangle$, do sistema composto AB. Aplicando o princípio da superposição para o produto de estados desta forma, chega-se ao postulado do produto tensorial dado acima. Isto não é uma derivação, já que o princípio da superposição não é utilizado como parte fundamental dessa descrição da mecânica quântica, mas ele dá o sentimento das várias maneiras de como essas ideias são algumas vezes reformuladas [8].

Para explicitar melhor o que diz o Postulado 2.4, considere Q_1 e Q_2 como sendo sistemas quânticos. Imagine que esses dois sistemas foram configurados separadamente nos estados $|\psi_1\rangle$ e $|\psi_2\rangle$, respectivamente, e depois foram unidos sem que houvesse interação entre eles. Devido aos sistemas Q_1 e Q_2 terem sido separadamente configurados sem que houvesse interação, seus estados $|\psi_1\rangle$ e $|\psi_2\rangle$ estão em espaços de Hilbert distintos $\mathcal{H}_1$ e $\mathcal{H}_2$, respectivamente. Portanto, qualquer alteração em algum dos estados não irá afetar a configuração do outro estado.

O sistema quântico global Q, que consiste dos sistemas quânticos Q_1 e Q_2, como descritos acima, é então um sistema composto pela justaposição dos sistemas quânticos Q_1 e Q_2.

O estado $|\psi\rangle$ de Q pode ser representado como:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2. \tag{2.20}$$

Em geral, os estados quânticos são descritos através do produto tensorial, denotado pelo símbolo $\otimes$, e estados não quânticos (i.e., da computação clássica) são descritos através do produto cartesiano. Compreender mais profundamente as diferenças entre os produtos cartesiano e tensorial é fundamental para o entendimento dos conceitos envolvidos na computação quântica.

Sejam V e W dois espaços vetoriais complexos de duas dimensões, com bases $\beta_1 = \{v_1, \ldots, v_n\}$ e $\beta_2 = \{w_1, \ldots, w_l\}$, respectivamente. Os elementos de $V \otimes W$ são combinações lineares finitas de elementos de $V \otimes W$, isto é,

$$\sum_{i=1}^{n} v_i \otimes w_i, \tag{2.21}$$

em que $v_i \in V$ e $w_i \in W$. O produto cartesiano desses dois espaços tem como base a união das bases de V e W, $\{v_1, \ldots, v_n, w_1, \ldots, w_l\}$. Note que a ordem das bases foi escolhida arbitrariamente e que a dimensão do espaço cresce linearmente, pois $dim(V \times W) = dim(V) + dim(W)$. Por outro lado, o produto tensorial de V e W tem como base $\{v_1 \otimes w_1, \ldots, v_1 \otimes w_l, \ldots, v_n \otimes w_1, \ldots, v_n \otimes w_l\}$. Novamente a escolha da ordem das bases pode ser feita arbitrariamente. No entanto, a dimensão do novo espaço agora é dada por $dim(V \otimes W) = dim(V) \times dim(W)$ [55]. Caso se tenha três qubits, utilizando-se a base para o espaço de estados de um qubit $\{|0\rangle, |1\rangle\}$, e se queira colocá-los juntos no mesmo espaço de Hilbert, então o novo espaço terá como base $\{|0\rangle \otimes |0\rangle \otimes |0\rangle ; |0\rangle \otimes |0\rangle \otimes |1\rangle ; |0\rangle \otimes |1\rangle \otimes |0\rangle ; |0\rangle \otimes |1\rangle \otimes |1\rangle ; |1\rangle \otimes |0\rangle \otimes |0\rangle ; |1\rangle \otimes |0\rangle \otimes |1\rangle ; |1\rangle \otimes |1\rangle \otimes |0\rangle ; |1\rangle \otimes |1\rangle \otimes |1\rangle\}$, que pode ser escrito de uma forma mais compacta como $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$.

De uma forma mais genérica, escreve-se $|x\rangle$ como sendo $|b_n b_{n-1} \cdots b_0\rangle$, em que b_i são os dígitos binários do número natural x.

Para exemplificar um sistema composto, seja $\mathcal{H}$ um espaço de Hilbert, e seja $\{|0\rangle, |1\rangle\}$ uma base ortonormal selecionada arbitrariamente. Sejam $\mathcal{H}_{n-1}, \mathcal{H}_{n-2}, \cdots, \mathcal{H}_0$ espaços de Hilbert bidimensionais distintos, cada um com as seguintes bases ortonormais:

$$\{|0_{n-1}\rangle, |1_{n-1}\rangle\}, \{|0_{n-2}\rangle, |1_{n-2}\rangle\}, \cdots, \{|0_0\rangle, |1_0\rangle\}, \tag{2.22}$$

respectivamente.

Considere n qubits $Q_{n-1}, Q_{n-2}, ..., Q_0$ configurados separadamente nos estados

$$\frac{1}{\sqrt{2}}\big(|0_{n-1}\rangle + |1_{n-1}\rangle\big), \frac{1}{\sqrt{2}}\big(|0_{n-2}\rangle + |1_{n-2}\rangle\big), \cdots, \frac{1}{\sqrt{2}}\big(|0_0\rangle + |1_0\rangle\big), \tag{2.23}$$

respectivamente. Q denota o sistema quântico global que consiste dos qubits $Q_{n-1}, Q_{n-2}, ..., Q_0$ configurados separadamente (sem interação entre eles). Então, o estado $|\psi\rangle$ de Q é o produto tensorial:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|0_{n-1}\rangle + |1_{n-1}\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|0_{n-2}\rangle + |1_{n-2}\rangle\big) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\big(|0_0\rangle + |1_0\rangle\big). \tag{2.24}$$

Utilizando as propriedades do produto tensorial, é equivalente a:

$$|\psi\rangle = \Big(\frac{1}{\sqrt{2}}\Big)^n \big(|0_{n-1}0_{n-2}\cdots 0_1 0_0\rangle + |0_{n-1}0_{n-2}\cdots 0_1 1_0\rangle + \cdots + |1_{n-1}1_{n-2}\cdots 1_1 1_0\rangle \big). \quad (2.25)$$

que está no espaço de Hilbert $\mathcal{H}$:

$$\mathcal{H} = \mathcal{H}_{n-1} \otimes \mathcal{H}_{n-2} \otimes \cdots \otimes \mathcal{H}_0. \quad (2.26)$$

Então, o sistema global Q, que consiste da justaposição dos n qubits $Q_{n-1}, Q_{n-2}, \cdots, Q_0$, está no estado

$$|\psi\rangle = \Big(\frac{1}{\sqrt{2}}\Big)^n \big(|00\cdots 00\rangle + |00\cdots 01\rangle + \cdots + |11\cdots 11\rangle \big). \quad (2.27)$$

A interação de dois ou mais sistemas quânticos pode criar uma correlação não local entre eles. Essas correlações não locais ocorrem somente quando o estado quântico do sistema não pode ser representado como um produto tensorial dos estados quânticos dos subsistemas que o formam. Essas correlações, que não existem nos sistemas clássicos, são chamadas de emaranhamento ou entrelaçamento. Um estado $|\psi\rangle$ definido em um espaço de Hilbert $\mathcal{H}_E \otimes \mathcal{H}_F$ é considerado emaranhado se este não puder ser escrito como um produto de estados $|\phi\rangle \in \mathcal{H}_E$ e $|\chi\rangle \in \mathcal{H}_F$, ou seja, se $|\psi\rangle \neq |\phi\rangle \otimes |\chi\rangle$. Caso contrário, ele é considerado não emaranhado. Assim como foi mencionado anteriormente, a interação de um sistema quântico com o ambiente (sistema externo) pode resultar no emaranhamento indesejável entre eles. Por outro lado, o emaranhamento é usado como recurso nos esquemas de codificação a fim de proporcionar proteção contra erros.

2.2 Estados GHZ – Uma visão geral

No rápido desenvolvimento dos campos da comunicação quântica e do processamento da informação quântica, o conceito de emaranhamento quântico é considerado como sendo de grande importância prática [57]. Emaranhamento entre muitas partículas é o aspecto mais importante para muitos protocolos de computação e comunicação quânticas [58, 59]. Muitas aplicações importantes - tais como compartilhamento de segredo [60], teleportação de destinação aberta [61], computação tolerante a falhas [62, 63] e outros [8] - dependem grandemente da habilidade em se poder gerar estados emaranhados multipartites. Este é especialmente o caso

dos estados Greenberger-Horne-Zeilinger (GHZ), também conhecidos como estados do "gato" (veja, por exemplo, [64]), os quais - de acordo com muitas medidas de emaranhamento - são maximamente emaranhados [8]. Eles foram introduzidos por Daniel M. Greenberger, Michael A. Horne e Anton Zeilinger [43] como um novo modo de provar o teorema de Bell [65].

No espaço de Hilbert 2^n-dimensional existem 2^n estados GHZ independentes, tendo a forma

$$|GHZ\rangle^n = \frac{1}{\sqrt{2}}\left(\left|b_1 b_2 \ldots b_n\right\rangle \pm \left|\hat{b}_1 \hat{b}_2 \ldots \hat{b}_n\right\rangle\right), \tag{2.28}$$

em que $|b_m\rangle$ e $|\hat{b}_m\rangle$ representam dois estados ortogonais do qubit m, sendo $\hat{b}_m = 1 - b_m$ e $b_m \in \{0, 1\}$.

Uma das mais notáveis propriedades dos estados GHZ está no fato de que, realizando o traço somente em uma parte (operação traço parcial), destrói-se completamente o emaranhamento do estado e o transforma em um estado misturado, que é completamente separável:

$$Tr_k\Big(\, |GHZ\rangle^n \langle GHZ|^n \,\Big) = I_{n\backslash k} \tag{2.29}$$

em que $I_{n\backslash k}$ é uma matriz diagonalizável de dimensão 2^{n-k} com traço unitário.

Para entender o que é a operação traço parcial, considere que se tenha um estado puro sobre dois subsistemas A e B,

$$\left|\psi^{AB}\right\rangle = \sum_i \alpha_i \left|\psi_i^A\right\rangle \left|\psi_i^B\right\rangle, \tag{2.30}$$

mas se gostaria de descrever o estado apenas do subsistema A. Matematicamente, este procedimento é conhecido como obtendo o *traço parcial* sobre o subsistema B,

$$\rho_A = Tr_B\big(\, \left|\psi^{AB}\right\rangle \left\langle\psi^{AB}\right| \,\big) = \sum_i \langle i^B|\psi^{AB}\rangle\langle\psi^{AB}|i^B\rangle, \tag{2.31}$$

em que $\left|i^B\right\rangle$ pode ser qualquer base completa sobre o subsistema B. A matriz densidade reduzida ρ_A é uma descrição útil capaz de determinar os resultados das ações aplicadas somente ao subsistema A. A operação traço parcial é considerada também o primeiro passo para quantificar a quantidade de emaranhamento compartilhada entre dois subsistemas [66, p. 340].

Por exemplo, se um sistema está num estado GHZ puro de 3 qubits e qualquer um dos três qubits é perdido ou medido na base computacional $\{|0\rangle, |1\rangle\}$, então o subsistema consistindo dos dois qubits restantes está definitivamente em um produto de estados. Um reflexo

disso, é que quando se faz o traço sobre um dos três sistemas, por exemplo no terceiro sistema, obtém-se

$$Tr_3\Big[\Big(\,|000\rangle + |111\rangle\,\Big)\Big(\,\langle 000| + \langle 111|\,\Big)\Big] = |00\rangle\langle 00| + |11\rangle\langle 11| \tag{2.32}$$

que é um estado misturado não emaranhado. Este estado obtido em (2.32) certamente tem correlações de duas partículas (qubits), mas essas são de natureza clássica.

Por outro lado, se for medido um dos subsistemas, de tal modo que a medição distingue entre os estado $|0\rangle$ e $|1\rangle$, será deixado para trás $|00\rangle$ ou $|11\rangle$ e o processo resultará num estado não emaranhado [58].

Sabe-se que estados GHZ maximizam emaranhamentos monotônicos[2] e, portanto, podem ser chamados de maximamente emaranhados no sentido multipartite.

De acordo com a classificação de estado dada por meio de operações locais estocásticas assistida por comunicação clássica (do inglês *stochastic local operations assisted by classical communication* - SLOCC), existem de fato somente duas classes de estados de três qubits que são verdadeiramente emaranhamentos tripartite, que correspondem aos estados GHZ e aos chamados estados W, respectivamente [67].

Além disso, definindo-se a decomposição de Schmidt generalizada como sendo [68, p. 890]

$$|\psi\rangle_{A_1\ldots A_n} := \sum_{i=1}^{min\{dim(A_1),\ldots,dim(A_n)\}} a_i \left|u^i\right\rangle_{A_1} \otimes \ldots \otimes \left|u^i\right\rangle_{A_n} \tag{2.33}$$

para um estado puro $|\psi\rangle_{A_1\ldots A_n}$ de n-partículas representado no espaço de Hilbert $\mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_n$, em que $\{A_j\}$ são subsistemas arbitrários, $dim(A_j)$ é a dimensão do subsistema A_j ($j = 1, \ldots, n$), a_i são os coeficientes de Schmidt e $|u^i\rangle_{A_1}, \ldots, |u^i\rangle_{A_n}$ são as bases em $\mathcal{H}_1, \ldots, \mathcal{H}_n$, respectivamente. Entretanto, isto não pode ser realizado tão facilmente no caso multipartite, pois muito raramente estados puros multipartites admitem a decomposição de Schmidt generalizada. Pode-se verificar que os estados GHZ admitem a decomposição de Schmidt generalizada [67–69].

Em geral, um estado admite a decomposição de Schmidt se, realizando o traço em qualquer subsistema, o resto do sistema está em um estado completamente separado. Isto é realmente verdade para os estado GHZ, enquanto que não é assegurado para os estados W que, de fato, não admitem a decomposição de Schmidt [68, 69].

[2] Uma quantidade $M(|\psi\rangle\langle\psi|)$ é um emaranhamento monotônico se, e somente se, o seu valor esperado não aumentar sob a ação de cada operação local ([67] - Teorema 2, p. 3).

2.3 Canal de Apagamento Quântico

O modelo de canal de apagamento quântico (do inglês *quantum erasure channel* - QEC),[3] foi primeiro considerado por Grassl e outros em [39]. Neste modelo é considerada uma situação na qual a posição dos qubits errôneos é conhecida.

Admite-se que toda informação é fisicamente representável e, portanto, todos os qubits representando-a são codificados em estados de sistemas físicos [70]. Os qubits irão ter dois estados distinguíveis que serão denominados "zero" e "um". Eles estarão em contato com um ambiente que pode ser modelado como um reservatório de calor a uma temperatura fixa T. Haverá também um parâmetro externo que permite fazer uma operação sobre o qubit. Este parâmetro externo será o meio com o qual se irá apagar o qubit. Em todos os casos admitir-se-á ter um grande número de qubits, mas estes serão apagados individualmente, um por um. Ver-se-á o grande número de qubits como um conjunto (*an ensemble*, em inglês). Para ter uma visão mais clara de todo o processo se poderia pensar, por exemplo, no qubit como sendo uma partícula de spin-$1/2$ e do parâmetro externo como sendo um campo magnético que se pode alterar. Isto mostra que tudo que se precisa é de um reservatório de calor e um parâmetro externo para apagamento. Não é necessário reservatórios de calor adicionais ou parâmetros externos adicionais. Apagamento é uma operação de *reset*. Ela pode ser definida como "restaurar para um" ou como "restaurar para zero". De qualquer forma, segue-se de dois estados possíveis do qubit para um estado possível.

Em seu artigo seminal de 1961 [71], Landauer argumenta que como o apagamento é uma função lógica que não tem um inverso de valor único, ele deve ser associado com a irreversibilidade física e, portanto, requer a dissipação de calor. Ele argumenta que um qubit tem um grau de liberdade e a dissipação de calor deve ser da ordem de $k_B T$, em que k_B é a constante de Boltzmann e T é a temperatura na qual o apagamento ocorre. Mais precisamente, desde que antes do apagamento um qubit pode estar em qualquer um dos dois possíveis estados e depois do apagamento ele pode estar somente em um estado, isso implica em uma mudança na entropia da informação de $-k\ln(2)$. Uma vez que a entropia não pode diminuir (decrescer) este (apagamento) deve aparecer, argumenta Landauer, em algum outro lugar como calor. Implícito neste argumento é a suposição essencial que a entropia da informação se traduz em entropia física.

Em geral, a corrupção do dado não é, *a priori*, óbvia para o observador, que deve codificar o dado de modo especial para detectar tal corrupção. Sobre alguns modelos físicos entretanto, é imediatamente conhecido quando algum operador de erro tiver sido aplicado. Considerando a situação em que erros são acompanhados pela emissão de *quanta*[4] eles podem, em princípio, serem detectados [39]. Por exemplo, se os qubits são representados por átomos, uma importante fonte de erros é a emissão espontânea. Um elétron pode passar espontaneamente de uma órbita para outra de energia menor e, com isso, o átomo correspondente emite um fóton

[3] Outros canais quânticos são apresentados no Apêndice B.2.

[4] plural de *quantum*.

numa direção qualquer. O fóton emitido tem energia igual à energia do estado inicial menos a energia do estado final. Esse processo é chamado de emissão espontânea ou decaimento espontâneo. Fótons espontâneos podem ser observados pelas técnicas de fotodetecção. Para ilustrar, considere as seguintes situações:

- seja um sistema físico consistindo de um átomo no qual a informação é apropriadamente codificada em dois níveis de energia. Esses níveis constituem o espaço computacional $\mathcal{H}_{comp}$. Uma transição que leva um estado do sistema para fora do espaço computacional é chamada um transição não ressonante, sendo denotada por $\mathcal{H}_{comp}^{\perp}$. A manipulação do sistema é realizada por meio de técnicas que permitem identificar a população desses níveis de trabalho, usando um laser sintonizado na diferença de energia entre esses dois estados (transição ressonante). Se uma transição é sinalizada pela emissão de um fóton, por exemplo, e a medida da população do nível previsto não indica variação, pode-se concluir que aquela foi uma transição não ressonante. O estado foi, portanto, levado para fora do espaço computacional. Este fato caracteriza o canal de apagamento quântico [42];

- similarmente, se bits quânticos são armazenados em forma de cavidades quantizadas, um fóton de cavidade detectado indica um erro [72]. Tome um átomo excitado passando completamente por dupla fenda, como representado pela Figura 2.2 [6]. Se nada está entre as fendas e a tela coletora no final, bordas podem ser observadas no padrão de interferência. Mas, se for colocada uma sonda, consistindo de duas cavidades ressonantes (identificadas por 1 e 2 na Figura 2.2) que são compostas por detector e espelhos removíveis, então as bordas de interferência desaparecem, desde que o átomo, enquanto relaxando para seu estado fundamental, libere um fóton em uma das duas cavidades, dependendo da fenda em que ele passou completamente. Este fato é usualmente interpretado como a sonda mantendo uma trilha de qual é a forma da informação sobre a trajetória do átomo, de tal modo que uma informação pode ser, em princípio, extraída pelo experimentador. Experimentalmente, isto pode ser realizado depois da passagem do átomo pelas cavidades, removendo simultaneamente ambos os espelhos na Figura 2.2, de tal modo que o detector entre as duas cavidades seja acoplado com o estado simétrico da radiação dentro delas. Então, separando os dois sub-efeitos dos eventos correspondendo aos resultados das medidas, é possível recuperar as bordas de interferência originais.

É usualmente admitido que o espaço do sistema $\mathcal{H}_{sys}$ seja um produto tensorial de espaços bidimensionais $\mathcal{H}_2$ (qubits), i. e.,

$$\mathcal{H}_{sys} = \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_2. \tag{2.34}$$

Entretanto, isto é uma aproximação [39]. Por exemplo, átomos usualmente tem muitos níveis que podem ser corrompidos; isso é atribuído a uma evolução dinâmica não desejada do

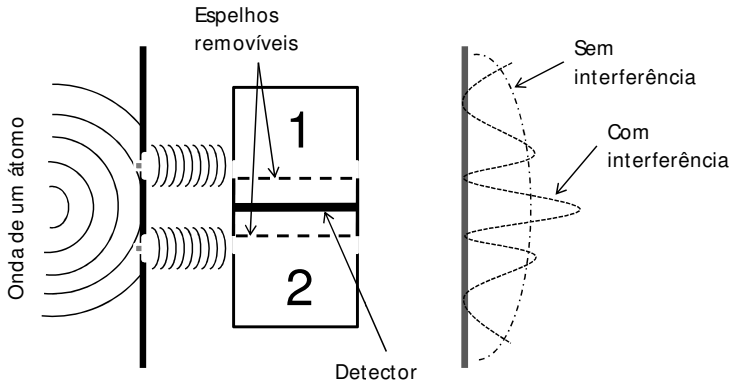

Figura 2.2 A figura ilustra um esquema para detecção de apagamento quântico.

sistema. Portanto, o espaço de Hilbert do sistema $\mathcal{H}_{sys}$, é um produto tensorial de espaços multidimensionais em que subespaços bidimensionais são usados para computação:

$$\mathcal{H}_{sys} = \mathcal{H}_k \otimes \ldots \otimes \mathcal{H}_k, \tag{2.35}$$

$$\mathcal{H}_{comp} = \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_2, \tag{2.36}$$

em que $\mathcal{H}_{comp}$ é o subespaço dos estados computacionais permitidos. Cada espaço bidimensional $\mathcal{H}_2$ é um subespaço de $\mathcal{H}_k$, mas não necessariamente um fator tensorial de $\mathcal{H}_k$ (assume-se, por simplificação, que as dimensões de todos os fatores tensoriais sejam iguais). Com isso, o espaço do sistema $\mathcal{H}_{sys}$ pode somente ser decomposto como uma soma direta de subespaços

$$\mathcal{H}_{sys} = \mathcal{H}_{comp} \oplus \mathcal{H}_{comp}^{\perp} \tag{2.37}$$

e, geralmente, não como um produto tensorial. Durante as computações livres de apagamento o sistema permanece em $\mathcal{H}_{comp}$. Qualquer população encontrada em $\mathcal{H}_{comp}^{\perp}$ é uma sinalização de apagamento.

O QEC, com probabilidade ϵ, substitui o estado do qubit que entra por um "estado apagado" $|2\rangle$ ortogonal a $|0\rangle$ e $|1\rangle$, assim, tanto apaga o qubit quanto informa ao receptor que o mesmo foi apagado.

2.4 Fundamentos para a Correção de Erros Quânticos

O processamento de informação quântica é frequentemente descrito como uma série de operações unitárias e de medidas em algum sistema físico. Imperfeições nestas operações e interações com o meio ambiente circundante são inevitáveis tanto no processamento de informação

clássica quanto quântica. O acúmulo de erros será prejudicial em qualquer processamento de informação de larga escala.

Portanto, para que a computação quântica funcione na prática, tem-se um grande obstáculo a superar: proteger a informação quântica de erros. Sem esta proteção um computador quântico, por exemplo, certamente irá falhar. Qualquer estratégia efetiva para impedir que erros ocorram em um computador quântico deve proteger contra pequenos erros em portas unitárias em um circuito quântico, bem como contra erros de descoerência.

Contra os erros de descoerência foi desenvolvida a teoria dos códigos corretores de erros quânticos. Quanto aos erros operacionais, intrínsecos às portas lógicas, foi desenvolvida a teoria quântica de tolerância a falhas (ver por exemplo [8]).

Assim, uma estratégia útil para defender a coerência do processamento quântico contra ruídos do ambiente é o uso de CCEQ's, em que, fazendo analogia com a teoria da informação clássica, a informação quântica é estabilizada utilizando-se codificação redundante e medidas.

Mas, existem algumas diferenças importantes entre a informação clássica e a informação quântica que exigem a introdução de novas ideias para que a construção de CCEQ's seja possível. Relembra-se as quatro grandes dificuldades que devem ser superadas [8, 73]:

1. Os *erros* de fase não têm análogo clássico.

2. Os *erros são contínuos*: um *continuum* de diferentes erros pode ocorrer em um qubit. Determinar qual erro ocorreu para que se possa fazer a correção parece requerer precisão infinita.

3. *Não é possível clonar a informação quântica*: poder-se-ia tentar implementar o código de repetição no contexto quântico por meio de duplicação do estado quântico três vezes ou mais. Mas, isto é proibido pelo teorema da não clonagem. Mesmo se a clonagem fosse possível, não seria possível medir e comparar os três estados quânticos na saída do canal.

4. *A medida destrói a informação quântica*: na correção de erros clássicos se observa a saída do canal para decidir qual procedimento de decodificação se deve adotar. Sabe-se da mecânica quântica que as observações em geral destroem o estado quântico sob observação e tornam impossível a recuperação do estado original.

A informação quântica é convenientemente representada por vetores do espaço de Hilbert $\mathbb{C}^m$ (em que $\mathbb{C}$ é o corpo dos números complexos e m é um inteiro positivo representando a dimensão do espaço) [74]. De acordo com a mecânica quântica, dois vetores do espaço $\mathbb{C}^m$ são completamente distinguíveis por uma medida se e somente se eles forem ortogonais. Em $\mathbb{C}^2$ existe uma base ortogonal, identificada aqui por v_0 e v_1, a qual se pode associar $|0\rangle$ lógico a v_0 e $|1\rangle$ lógico a v_1. Esta base é chamada de *base computacional*. O espaço $\mathbb{C}^2$ permite codificar um bit de informação e é chamado qubit (bit quântico). Desta forma, o estado de um qubit arbitrário normalizado pode ser escrito como

$$|\psi\rangle = a|0\rangle + b|1\rangle, \tag{2.38}$$

em que $|a|^2+|b|^2 = 1$, com $a, b \in \mathbb{C}$. A base conjugada é definida como $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$.

Caso se deseje preparar n qubits de informação, necessita-se do espaço $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$, em que $\otimes$ é o produto tensorial. Em $(\mathbb{C}^2)^{\otimes n}$ pode-se escolher 2^n vetores ortogonais do espaço que permitam preparar n qubits de informação. Pode-se escolher como uma base ortonormal para este espaço os estados nos quais cada qubit tem um valor definido, $|0\rangle$ ou $|1\rangle$. Desta forma, um vetor geral normalizado pode ser escrito nesta base como

$$|\psi\rangle = \sum_{x=0}^{2^n-1} a_x|x\rangle, \tag{2.39}$$

em que é associado a cada símbolo x o número natural que ela representa na notação binária, um valor entre 0 e $2^n - 1$. Os coeficientes a_x são números complexos satisfazendo a relação $\sum_x |a_x|^2 = 1$.

Um CCEQ pode ser visto como um mapeamento de k qubits em n qubits, em que $n > k$. Os k qubits são os qubits lógicos que se deseja proteger de erros. Os n qubits são os qubits físicos resultantes da codificação. Os $n - k$ qubits adicionais permitem armazenar os k qubits lógicos de uma forma redundante tal que os n qubits físicos não sejam facilmente alterados [73].

Assim, um código para codificar k qubits em n qubits irá ter 2^k palavras-código correspondendo à base composta dos estados originais. Qualquer combinação linear dessas palavras-código é também uma palavra código. O espaço das palavras-código válidas (o espaço de codificação) é portanto um espaço de Hilbert, um subespaço do espaço de Hilbert 2^n-dimensional.

A notação $[[n, k]]$ refere-se a um conjunto de 2^k palavras-código, cada uma de comprimento n e tendo a propriedade de ser um código linear. Isso significa que, se a operação ou-exclusivo é realizada bit a bit entre quaisquer duas palavras código, então a palavra resultante é também um membro do código.

No processo de transmissão sobre um canal, a informação pode ser alterada por um erro. Uma importante mudança é que o erro quântico pode ser contínuo. Por exemplo, uma provável fonte de erro é a rotação: um estado $a\,|0\rangle + b\,|1\rangle$ pode tornar-se $a\,|0\rangle + be^{i\phi}\,|1\rangle$, mas ao invés disso torna-se $a\,|0\rangle + be^{i(\phi+\delta)}\,|1\rangle$. Este último estado é muito próximo do estado correto, mas ainda não é o estado desejado. Caso não se faça alguma coisa a respeito, pequenos erros serão formados ao longo do percurso da computação e, eventualmente, tornar-se-ão um grande erro [75].

Além do mais, estados quânticos são intrinsecamente delicados: uma interação indesejada (observação) pode fazer com que ele colapse, ou seja, $a\,|0\rangle + b\,|1\rangle$ pode tornar-se $|0\rangle$ com probabilidade $|a|^2$ ou $|1\rangle$ com probabilidade $|b|^2$. O ambiente está constantemente tentando

"observar" o estado, um processo conhecido como *descoerência*. Um dos objetivos da correção de erros quânticos será o de impedir o ambiente de realizar a observação dos dados.

Para a correção de erros quânticos, precisa-se sustentar a fase correta bem como corrigir troca de bits. Mas, também existe outro problema. Considere o código clássico mais simples, o código de repetição:

$$0 \rightarrow 000 \tag{2.40}$$

$$1 \rightarrow 111 \tag{2.41}$$

Ele corrigirá um estado tal como 010 pelo valor da maioria (tornando-se 000 neste caso).

Poder-se-ia pensar na construção de um código de repetição quântico:

$$|\psi\rangle = |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle \,. \tag{2.42}$$

Entretanto, tal código não existe devido ao Teorema da Não-Clonagem [76]:

Teorema 2.1 (Não-Clonagem - [75])**.** *Não existe uma operação quântica que mapeie um estado* $|\psi\rangle$ *e leve para* $|\psi\rangle \otimes |\psi\rangle$*, para qualquer estado arbitrário* $|\psi\rangle$*.*

Demonstração: Este fato é uma simples consequência da linearidade da mecânica quântica. Será assumido que o Teorema seja falso e mostrado que isso leva a uma contradição. Suponha que haja tal operação e que $|\psi\rangle$ e $|\phi\rangle$ sejam estados distintos. Então, por definição da operação, segue-se que

$$|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \tag{2.43}$$

$$|\phi\rangle \rightarrow |\phi\rangle \otimes |\phi\rangle \tag{2.44}$$

$$|\psi\rangle + |\phi\rangle \rightarrow (|\psi\rangle + |\phi\rangle) \otimes (|\psi\rangle + |\phi\rangle). \tag{2.45}$$

(Aqui, e frequentemente a seguir, fatores de normalização serão omitidos.)

Mas, por linearidade,

$$|\psi\rangle + |\phi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle \,. \tag{2.46}$$

Isto difere de (2.45) quando realizando o cruzamento dos termos, ou seja,

$$|\psi\rangle \otimes |\phi\rangle + |\phi\rangle \otimes |\psi\rangle \tag{2.47}$$

o que contradiz a suposição inicial. Portanto, conclui-se que tal operação não existe.

□

O Teorema 2.1 não impede a construção de uma operação que possa copiar um conjunto particular de estados quânticos ortonormais. O que o Teorema 2.1 regula, entretanto, é a expectativa de sempre construir uma operação que possa tomar um estado quântico arbitrário como entrada e produzir uma cópia exata dele.

Pode-se considerar um erro quântico como um operador linear arbitrário $\mathcal{E}$ que transfere um estado quântico para um estado corrompido. Os $\mathcal{E}$ são chamados de operadores de interação. Um *superoperador* é definido por qualquer família de operadores $\mathcal{E}$ que satisfaça

$$\sum_j \mathcal{E}_j^\dagger \mathcal{E}_j = I, \tag{2.48}$$

em que I é a matriz identidade.

Se não existe conhecimento *a priori* dos operadores de interação que corrompem um estado codificado, não é possível recuperar $|\psi\rangle$ consistentemente. Entretanto, em muitos sistemas físicos os $\mathcal{E}$ são de uma forma restrita. Por exemplo, uma aproximação razoável para sistemas de qubits é que a interação com o ambiente é independente para cada qubit. Neste caso, os operadores de interação são produtos tensoriais de operadores de interação de um qubit. Para taxas de erros pequenas, pode ser que um dos operadores de interação de um qubit, chamado $\mathcal{E}_0$, seja próximo da identidade. Pode-se então definir o número de erros de uma interação pela contagem do número de operadores no produto tensorial que sejam diferentes de $\mathcal{E}_0$.

Em geral não se conhece exatamente qual ruído está afligindo um sistema quântico. Poderia ser útil se um código quântico específico C_Q e uma operação de correção de erro $\mathcal{R}$ pudessem ser usados para proteger contra uma classe completa de processos ruidosos. Este tipo de proteção é garantida pelo teorema a seguir.

Teorema 2.2. *(Discretização dos erros - [8, p. 438]) Suponha que C_Q seja um código quântico e $\mathcal{R}$ seja uma operação de correção de erro para realizar a recuperação de um processo ruidoso Ω com elementos de operação $\{\mathcal{E}_i\}$. Suponha que $\mathcal{F}$ seja uma operação quântica com elementos de operação $\{F_j\}$ o qual é uma combinação linear de $\mathcal{E}_i$, isto é, $F_j = \sum_i m_{ji}\mathcal{E}_i$ para alguma matriz m_{ji} de números complexos. Então a operação de correção de erro $\mathcal{R}$ também corrige efeitos de processos ruidosos $\mathcal{F}$ no código C_Q.*

Este resultado habilita a introdução de uma linguagem mais poderosa para descrever CCEQ's. Ao invés de falar a respeito de uma classe de processos de erros Ω corrigível por um código C_Q e uma operação de correção de erro $\mathcal{R}$, pode-se falar a respeito de um conjunto de *operadores de erros* (ou simplesmente *erros*) $\{\mathcal{E}_i\}$ os quais são corrigíveis. Resumindo, é possível *discretizar* erros quânticos de tal maneira que para combater o contínuo de erros possíveis em um único qubit é meramente suficiente tratar um conjunto finito de erros.

Existem muitos modelos de canais, como apresentado no Apêndice B.2. Aqui será considerado o canal completamente despolarizado. Nesse modelo, um estado pode ser representado por um vetor $|v\rangle \in \mathbb{C}^2$ e este pode ser alterado por um dos seguintes operadores de erros:

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Z = \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ e } Y = iXZ = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{2.49}$$

O operador de erro $\mathcal{E}$ tem a seguinte forma:

$$\mathcal{E} = \sigma_1 \otimes \sigma_2 \otimes \ldots \otimes \sigma_n \tag{2.50}$$

em que $\sigma_i \in \{I_2, X, Z, Y\}, i = 1, \ldots, n$.

A seguir será apresentada uma definição de peso para códigos quânticos.

Definição 2.1. *[74] O número de matrizes diferentes da matriz identidade no produto tensorial (*2.50) é chamado o **peso** de $\mathcal{E}$ e é denotado por $\mathbf{w}_q(\mathcal{E})$.

Como exemplo da definição acima considere $\mathcal{E} = X \otimes I \otimes I \otimes Z \otimes X \otimes I \otimes I$. Neste caso o peso é igual a 3, isto é, $\mathbf{w}_q(\mathcal{E}) = 3$.

Se um vetor $|v\rangle$ é afetado por um erro $\mathcal{E}$, então o resultado é $|w\rangle = \mathcal{E}|v\rangle$.

Por exemplo, considere

$$\mathcal{E} = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix};\ \text{e}\ |v\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

então,

$$|w\rangle = \mathcal{E}|v\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle.$$

Definição 2.2. *[74] Um código quântico C_Q de comprimento n e dimensão k, denotado por $[[n, k]]$, é um subespaço k-dimensional do espaço $(\mathbb{C}^2)^{\otimes n}$.*

Diz-se que um erro $\mathcal{E}$ é detectável se quaisquer dois vetores ortogonais do código permanecerem ortogonais (isto é, distinguíveis) depois de um deles ter sido alterado por $\mathcal{E}$. Em outras palavras, tem-se a seguinte definição.

Definição 2.3. *[74] $\mathcal{E}$ é detectável se, e somente se,*

$$\langle v|\mathcal{E}|w\rangle = 0 \tag{2.51}$$

para todos os vetores ortogonais $|v\rangle$ e $|w\rangle$ do código C_Q.

Definição 2.4. *[74] A distância mínima de um código quântico C_Q é o maior inteiro d tal que qualquer erro $\mathcal{E}$, $\mathbf{w}_q(\mathcal{E}) \leq d - 1$, seja detectável.*

Knill e Laflamme [11] e Bennett *et al.* [15] estabeleceram as condições necessárias e suficientes para que um CCEQ seja capaz de corrigir um determinado conjunto de erros. Dado um conjunto de erros $\Omega = \{\mathcal{E}_i\}$, as seguintes condições devem ser satisfeitas:

$$\langle v_k|\mathcal{E}_i^\dagger\mathcal{E}_j|v_l\rangle = 0, \text{ para } (v_k \neq v_l) \text{ e } \langle v_k|v_l\rangle = 0 \tag{2.52}$$

$$\langle v_k|\mathcal{E}_i^\dagger\mathcal{E}_j|v_k\rangle = \langle v_l|\mathcal{E}_i^\dagger\mathcal{E}_j|v_l\rangle. \tag{2.53}$$

A primeira dessas condições estabelece que dois erros distintos $\mathcal{E}_i$ e $\mathcal{E}_j$, atuando sobre duas palavras-código distintas e ortogonais $|v_k\rangle$ e $|v_l\rangle$, respectivamente, devem ser sempre distinguíveis, ou seja, $\mathcal{E}_i|v_k\rangle$ e $\mathcal{E}_j|v_l\rangle$ são ortogonais. A segunda condição leva em conta o fato de que ao se fazer uma medição para obter informação sobre o erro, não se deve obter informação sobre as palavras do código, pois isso causaria perturbação no estado quântico codificado. Caso não houvesse a igualdade na equação (2.53), para um mesmo tipo de erro, poder-se-ia obter informação sobre as palavras-código fazendo-se uma medida projetiva na base do código.

Uma condição também relatada em [11], é que a equação (2.53) é zero se $\mathcal{E}_i$ e $\mathcal{E}_j$ forem diferentes. Isso implica que cada erro mapeia o estado inicial para subespaços ortogonais. Obviamente isto permite a recuperação do estado original pela projeção naqueles subespaços. A equação (2.53) permite que dois erros diferentes sejam mapeados no mesmo subespaço. Esta possibilidade é permitida pelo princípio da superposição da mecânica quântica, mas não pode ocorrer na correção clássica de erro.

Estes argumentos mostram que se existe alguma base para o espaço de erros de tal forma que as equações (2.52) e (2.53) são asseguradas, então os estados v_k e v_l geram um CCEQ. Tratando aquelas duas equações juntas e generalizando para múltiplos qubits codificados, obtém-se o seguinte teorema, sendo $|\psi\rangle$ um estado arbitrário:

Teorema 2.3. *[11, 15, 75] Suponha que Ω seja um subgrupo do grupo de erros $\mathcal{G}_n$ agindo no espaço de Hilbert $\mathcal{H}$. Então, um subespaço C de $\mathcal{H}$ forma um CCEQ corrigindo os erros em Ω se, e somente se,*

$$\langle\psi|\,\mathcal{E}^\dagger\mathcal{E}\,|\psi\rangle = C(\mathcal{E}) \tag{2.54}$$

para todo $\mathcal{E} \in \Omega$. A função $C(\mathcal{E})$ não depende do estado $|\psi\rangle$.

Demonstração: Suponha $\{\mathcal{E}_a\}$ seja uma base para Ω e $\{|\psi_j\rangle\}$ uma base para C. Escolhendo $\mathcal{E}$ e $|\psi\rangle$ igual aos elementos da base e a soma e diferença de dois elementos da base (com ou sem um fator de fase i), pode-se ver que (2.54) é equivalente a

$$\langle\psi_k|\,\mathcal{E}_a^\dagger\mathcal{E}_b\,|\psi_l\rangle = C_{ab}(\delta_{kl}), \tag{2.55}$$

em que C_{ab} é uma matriz hermitiana independente de k e l. Para ilustrar isso, considera-se

$\{\mathcal{E}_a = X, \mathcal{E}_b = Z\}$ como uma base para Ω e $\{|0\rangle, |1\rangle\}$ uma base para C. Seja $|\psi_0\rangle = \alpha_0 |0\rangle$ e $|\psi_1\rangle = \alpha_1 |1\rangle$ (estados normalizados), como também $C_{ab} = \langle 0| X^\dagger Z |0\rangle$ ou $C_{ab} = \langle 1| X^\dagger Z |1\rangle$. Avaliando-se inicialmente o produto interno em relação ao estado $|\psi_0\rangle$ tem-se:

$$\begin{aligned} \langle\psi_0| X^\dagger Z |\psi_0\rangle &= \alpha_0^* \langle 0| X^\dagger Z \alpha_0 |0\rangle \\ &= \alpha_0^* \alpha_0 \langle 0| X^\dagger Z |0\rangle \\ &= |\alpha_0|^2 C_{ab} \\ &= C_{ab}. \end{aligned} \tag{2.56}$$

Realizando-se agora a avaliação do produto interno em relação ao estado $|\psi_1\rangle$ tem-se:

$$\begin{aligned} \langle\psi_1| X^\dagger Z |\psi_1\rangle &= \alpha_1^* \langle 1| X^\dagger Z \alpha_1 |1\rangle \\ &= \alpha_1^* \alpha_1 \langle 1| X^\dagger Z |1\rangle \\ &= |\alpha_1|^2 C_{ab} \\ &= C_{ab}. \end{aligned} \tag{2.57}$$

Observando (2.56) e (2.57) nota-se claramente que C_{ab} não depende de $|\psi_0\rangle$ e de $|\psi_1\rangle$.[5]

Suponha que a equação (2.55) seja assegurada. Pode-se diagonalizar C_{ab}. Isto envolve escolher uma nova base $\{\mathcal{F}_a\}$ para Ω, e o resultado são as equações (2.52) e (2.53). Os argumentos anteriores ao teorema mostram que se pode medir o erro, determiná-lo unicamente (em uma nova base) e invertê-lo (no espaço de codificação). Portanto, tem-se um CCEQ.

Agora suponha que se tenha um CCEQ, e tome $|\psi\rangle$ e $|\phi\rangle$ como sendo duas palavras-código distintas. Então, deve-se ter

$$\langle\psi| \mathcal{E}^\dagger \mathcal{E} |\psi\rangle = \langle\phi| \mathcal{E}^\dagger \mathcal{E} |\phi\rangle \tag{2.58}$$

para todo $\mathcal{E}$. Isto é, (2.54) deve ser assegurada. Caso contrário, $\mathcal{E}$ muda o tamanho de $|\psi\rangle$ em relação ao tamanho de $|\phi\rangle$. Para deixar isso mais claro, considere $\mathcal{E}|\psi\rangle = |\mu_\psi\rangle$ e $\mathcal{E}|\phi\rangle = |\mu_\phi\rangle$. Sendo assim, $C_\psi(\mathcal{E}) = \langle\psi| \mathcal{E}^\dagger \mathcal{E} |\psi\rangle = \langle\mu_\psi|\mu_\psi\rangle$ e $C_\phi(\mathcal{E}) = \langle\phi| \mathcal{E}^\dagger \mathcal{E} |\phi\rangle = \langle\mu_\phi|\mu_\phi\rangle$. Dessa maneira, caso $C_\psi(\mathcal{E})$ seja diferente de $C_\phi(\mathcal{E})$ implica que eles têm tamanhos diferentes. Sejam $|\psi\rangle + |\phi\rangle$ e $|\psi\rangle + c|\phi\rangle$ palavras-código, e

$$\mathcal{E}(|\psi\rangle + |\phi\rangle) = N(|\psi\rangle + c|\phi\rangle), \tag{2.59}$$

[5]Chegar-se-ia a mesma conclusão caso fossem considerados $|\psi_0\rangle$ e $|\psi_1\rangle$ como sendo uma combinação linear da base de C.

em que N é um fator de normalização e

$$c = \langle\psi|\,\mathcal{E}^{\dagger}\mathcal{E}\,|\psi\rangle \,/\, \langle\phi|\,\mathcal{E}^{\dagger}\mathcal{E}\,|\phi\rangle\,. \tag{2.60}$$

O erro $\mathcal{E}$ mudará o estado codificado, que é uma falha do código, a menos que $c = 1$.

□

Para um código de comprimento n que pode corrigir uma quantidade e de erros os operadores de erros $\{\mathcal{E}_i\}$ são de uma forma especial. Eles são todos operadores e-erro, isto é, operadores que diferem no máximo e dos fatores tensoriais de $\mathcal{H} = \mathcal{H}_2^{\otimes n}$ da identidade. Nas equações (2.52) e (2.53) é suficiente considerar bases da álgebra para operadores e-erro. As bases podem ser produtos tensoriais das bases locais, por exemplo, a identidade I_2 e as matrizes de Pauli $\{X, Z, Y\}$.

Para exemplificar, considere um código de cinco qubits que corrige um erro geral arbitrário, ou seja, $e = 1$. Colocando isso na forma de tabela, obtém-se:

Tabela 2.1 Operadores de um erro (X, Z ou Y) para um código de cinco qubits.

Posição do qubit	Erro X	Erro Z	Erro Y
1	$\mathcal{E}_{X1} = X \otimes I \otimes I \otimes I \otimes I$	$\mathcal{E}_{Z1} = Z \otimes I \otimes I \otimes I \otimes I$	$\mathcal{E}_{Y1} = Y \otimes I \otimes I \otimes I \otimes I$
2	$\mathcal{E}_{X2} = I \otimes X \otimes I \otimes I \otimes I$	$\mathcal{E}_{Z2} = I \otimes Z \otimes I \otimes I \otimes I$	$\mathcal{E}_{Y2} = I \otimes Y \otimes I \otimes I \otimes I$
3	$\mathcal{E}_{X3} = I \otimes I \otimes X \otimes I \otimes I$	$\mathcal{E}_{Z3} = I \otimes I \otimes Z \otimes I \otimes I$	$\mathcal{E}_{Y3} = I \otimes I \otimes Y \otimes I \otimes I$
4	$\mathcal{E}_{X4} = I \otimes I \otimes I \otimes X \otimes I$	$\mathcal{E}_{Z4} = I \otimes I \otimes I \otimes Z \otimes I$	$\mathcal{E}_{Y4} = I \otimes I \otimes I \otimes Y \otimes I$
5	$\mathcal{E}_{X5} = I \otimes I \otimes I \otimes I \otimes X$	$\mathcal{E}_{Z5} = I \otimes I \otimes I \otimes I \otimes Z$	$\mathcal{E}_{Y5} = I \otimes I \otimes I \otimes I \otimes Y$

Observe que na Tabela 2.1 $\mathcal{E}_{Xi}, \mathcal{E}_{Zi}, \mathcal{E}_{Yi}$, indicam a ocorrência de um único padrão de erro X, Z ou Y, respectivamente, nas posições i, sendo $i = 1, 2, 3, 4, 5$.

Considerando os erros para o código ilustrado na Tabela 2.1 e também que $\mathcal{E}_0 = I \otimes I \otimes I \otimes I \otimes I$, colocando-os no formato das condições estabelecidas pelas equações (2.52) e (2.53), tem-se que as verificações a serem realizadas para um código desse comprimento são as seguintes:

$$\begin{aligned}
\langle v_k|\mathcal{E}_1^{\dagger}\mathcal{E}_2|v_k\rangle &= \langle v_l|\mathcal{E}_1^{\dagger}\mathcal{E}_2|v_l\rangle, \qquad \langle v_k|\mathcal{E}_1^{\dagger}\mathcal{E}_2|v_l\rangle = 0;\\
\langle v_k|\mathcal{E}_1^{\dagger}\mathcal{E}_3|v_k\rangle &= \langle v_l|\mathcal{E}_1^{\dagger}\mathcal{E}_3|v_l\rangle, \qquad \langle v_k|\mathcal{E}_1^{\dagger}\mathcal{E}_3|v_l\rangle = 0;\\
\langle v_k|\mathcal{E}_1^{\dagger}\mathcal{E}_4|v_k\rangle &= \langle v_l|\mathcal{E}_1^{\dagger}\mathcal{E}_4|v_l\rangle, \qquad \langle v_k|\mathcal{E}_1^{\dagger}\mathcal{E}_4|v_l\rangle = 0;\\
\langle v_k|\mathcal{E}_1^{\dagger}\mathcal{E}_5|v_k\rangle &= \langle v_l|\mathcal{E}_1^{\dagger}\mathcal{E}_5|v_l\rangle, \qquad \langle v_k|\mathcal{E}_1^{\dagger}\mathcal{E}_5|v_l\rangle = 0;\\
\langle v_k|\mathcal{E}_2^{\dagger}\mathcal{E}_1|v_k\rangle &= \langle v_l|\mathcal{E}_2^{\dagger}\mathcal{E}_1|v_l\rangle, \qquad \langle v_k|\mathcal{E}_2^{\dagger}\mathcal{E}_1|v_l\rangle = 0;\\
\langle v_k|\mathcal{E}_2^{\dagger}\mathcal{E}_3|v_k\rangle &= \langle v_l|\mathcal{E}_2^{\dagger}\mathcal{E}_3|v_l\rangle, \qquad \langle v_k|\mathcal{E}_2^{\dagger}\mathcal{E}_3|v_l\rangle = 0;
\end{aligned}$$

$$
\begin{aligned}
&\langle v_k|\mathcal{E}_2^\dagger\mathcal{E}_4|v_k\rangle = \langle v_l|\mathcal{E}_2^\dagger\mathcal{E}_4|v_l\rangle, \qquad \langle v_k|\mathcal{E}_2^\dagger\mathcal{E}_4|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_2^\dagger\mathcal{E}_5|v_k\rangle = \langle v_l|\mathcal{E}_2^\dagger\mathcal{E}_5|v_l\rangle, \qquad \langle v_k|\mathcal{E}_2^\dagger\mathcal{E}_5|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_3^\dagger\mathcal{E}_1|v_k\rangle = \langle v_l|\mathcal{E}_3^\dagger\mathcal{E}_1|v_l\rangle, \qquad \langle v_k|\mathcal{E}_3^\dagger\mathcal{E}_1|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_3^\dagger\mathcal{E}_2|v_k\rangle = \langle v_l|\mathcal{E}_3^\dagger\mathcal{E}_2|v_l\rangle, \qquad \langle v_k|\mathcal{E}_3^\dagger\mathcal{E}_2|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_3^\dagger\mathcal{E}_4|v_k\rangle = \langle v_l|\mathcal{E}_3^\dagger\mathcal{E}_4|v_l\rangle, \qquad \langle v_k|\mathcal{E}_3^\dagger\mathcal{E}_4|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_3^\dagger\mathcal{E}_5|v_k\rangle = \langle v_l|\mathcal{E}_3^\dagger\mathcal{E}_5|v_l\rangle, \qquad \langle v_k|\mathcal{E}_3^\dagger\mathcal{E}_5|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_4^\dagger\mathcal{E}_1|v_k\rangle = \langle v_l|\mathcal{E}_4^\dagger\mathcal{E}_1|v_l\rangle, \qquad \langle v_k|\mathcal{E}_4^\dagger\mathcal{E}_1|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_4^\dagger\mathcal{E}_2|v_k\rangle = \langle v_l|\mathcal{E}_4^\dagger\mathcal{E}_2|v_l\rangle, \qquad \langle v_k|\mathcal{E}_4^\dagger\mathcal{E}_2|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_4^\dagger\mathcal{E}_3|v_k\rangle = \langle v_l|\mathcal{E}_4^\dagger\mathcal{E}_3|v_l\rangle, \qquad \langle v_k|\mathcal{E}_4^\dagger\mathcal{E}_3|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_4^\dagger\mathcal{E}_5|v_k\rangle = \langle v_l|\mathcal{E}_4^\dagger\mathcal{E}_5|v_l\rangle, \qquad \langle v_k|\mathcal{E}_4^\dagger\mathcal{E}_5|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_5^\dagger\mathcal{E}_1|v_k\rangle = \langle v_l|\mathcal{E}_5^\dagger\mathcal{E}_1|v_l\rangle, \qquad \langle v_k|\mathcal{E}_5^\dagger\mathcal{E}_1|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_5^\dagger\mathcal{E}_2|v_k\rangle = \langle v_l|\mathcal{E}_5^\dagger\mathcal{E}_2|v_l\rangle, \qquad \langle v_k|\mathcal{E}_5^\dagger\mathcal{E}_2|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_5^\dagger\mathcal{E}_3|v_k\rangle = \langle v_l|\mathcal{E}_5^\dagger\mathcal{E}_3|v_l\rangle, \qquad \langle v_k|\mathcal{E}_5^\dagger\mathcal{E}_3|v_l\rangle = 0;\\
&\langle v_k|\mathcal{E}_5^\dagger\mathcal{E}_4|v_k\rangle = \langle v_l|\mathcal{E}_5^\dagger\mathcal{E}_4|v_l\rangle, \qquad \langle v_k|\mathcal{E}_5^\dagger\mathcal{E}_4|v_l\rangle = 0,
\end{aligned}
\tag{2.61}
$$

em que $\mathcal{E}_i \equiv (\mathcal{E}_{Xi}\ ou\ \mathcal{E}_{Zi}\ ou\ \mathcal{E}_{Yi})$ e $\mathcal{E}_j \equiv (\mathcal{E}_{Xj}\ ou\ \mathcal{E}_{Zj}\ ou\ \mathcal{E}_{Yj})$, sendo $i \neq j$ e $i, j = 1, 2, 3, 4, 5$.

Assim, para um código que corrige uma quantidade e de erros, em (2.55), pode-se considerar somente $\mathcal{E}_a$ e $\mathcal{E}_b$ agindo em apenas e qubits. Isto leva a uma outra variação da condição:

$$\langle\psi|\,\mathcal{E}\,|\psi\rangle = C'(\mathcal{E}), \tag{2.62}$$

em que $\mathcal{E}$ é agora qualquer operador agindo em $2e$ qubits (isto é, ele substitui $\mathcal{E}_a^\dagger\mathcal{E}_b$ em (2.55)). Isto pode ser facilmente interpretado como dizendo que nenhuma medida em $2e$ qubits pode aprender informação sobre a palavra código. Alternativamente, significa que se pode detectar até $2e$ erros no código sem necessariamente estar apto a dizer o que aqueles erros são. Isto é, pode-se distinguir aqueles erros da identidade.

Se a matriz C_{ab} em (2.55) tem posto máximo, o código é chamado *não-degenerado*. Caso contrário, o código é dito *degenerado* [75]. Em um código degenerado, erros diferentes podem ser vistos como o mesmo erro no subespaço de codificação.

Para um código não-degenerado, pode-se configurar um limitante nos parâmetros do código simplesmente pela contagem de estados. Cada erro $\mathcal{E}$ agindo em cada palavra código da base $|\psi_i\rangle$ produz um estado linearmente independente. Todos aqueles estados devem se ajustar no espaço de Hilbert total de n qubits, o qual tem dimensão 2^n. Se o código codifica k qubits, e corrige erros em até e qubits, então

$$\left(\sum_{j=0}^{e} 3^j \binom{n}{j}\right) 2^k \leq 2^n. \tag{2.63}$$

A quantidade entre parenteses é o número de erros de peso e ou menos, sendo o peso como dado pela Definição 2.1. Esta desigualdade é chamada o *limitante quântico de Hamming*. Embora o limitante quântico de Hamming somente seja aplicado a códigos não-degenerados, não se tem conhecimento de código que não o obedeça [75].

Um limitante mais avançado, conhecido como o *limitante de Knill-Laflamme* [11] ou o *limitante quântico de Singleton*, aplica-se igualmente a códigos quânticos degenerados. Assim, este limitante estabelece que para um código quântico $[[n, k, d]]$, é válido

$$n - k \geq 2d - 2. \tag{2.64}$$

No próximo capítulo apresenta-se uma visão geral sobre os CGQ's, incluindo as condições necessárias e suficientes para detecção de erros nesses códigos.

CAPÍTULO 3

Códigos Corretores de Erros Quânticos Baseados em Grafos

3.1 Introdução

Códigos estabilizadores [10], também conhecidos como códigos quânticos aditivos [17], são uma importante classe de códigos quânticos para a qual a construção é análoga a de códigos lineares clássicos. Para a definição dos códigos estabilizadores, Gottesmann [10] desenvolveu o chamado *formalismo estabilizador*, um método poderoso para compreender uma ampla classe de operações em Mecânica Quântica. O poder do formalismo estabilizador vem do uso hábil da teoria de grupos, no qual vários conceitos foram devidamente adaptados para a teoria de códigos quânticos. Utilizando-se o formalismo estabilizador torna-se mais simples determinar quais erros de Pauli são detectáveis. Além disso, eles possibilitam fazer o uso das técnicas bem estabelecidas da teoria de códigos corretores de erros clássicos para construir bons códigos quânticos.

Um código estabilizador codificando k qubits em n qubits é representado usando a notação $[[n, k]]$. Este código C_Q está em um subespaço 2^k-dimensional de um espaço de Hilbert 2^n-dimensional que é caracterizado pelo conjunto S de produtos tensoriais de operadores de Pauli que deixa invariante cada estado do código. Mais precisamente, o código C_Q é um autoespaço do conjunto dos operadores em S. O grupo gerado pelo estabilizador S é um grupo abeliano que é gerado por $(n - k)$ elementos.

Alguns métodos eficientes para a construção de códigos estabilizadores têm sido desenvolvidos [10, 20, 22]. Entretanto, um problema que tais métodos apresentam é que a verificação da capacidade de correção de erros (verificação das condições de Knill-Laflamme para tipos particulares de erros [11]) frequentemente requer uma quantidade muito grande de operações.

Devido a dificuldade mencionada acima, Schlingemann e Werner [1] apresentaram uma nova maneira para construir códigos estabilizadores encontrando certos grafos (ou matrizes) com propriedades específicas. Eles verificaram que esse método pode ser usado para obter

muitos códigos quânticos saturando o limitante quântico de Singleton. Para essa construção dois ingredientes básicos são necessários: o primeiro é um grupo abeliano finito de ordem igual a dimensão do espaço de Hilbert do sistema quântico; o segundo ingrediente da construção é um grafo com duas classes de vértices, rotulando os sistemas de entrada e saída do código, respectivamente. Eles também estabeleceram as condições necessárias e suficientes para um grafo gerar um CCEQ, adaptadas das condições de Knill-Laflamme [11]. Um outro resultado interessante foi dado por Grassl *et al.* [77], os quais provaram que um CGQ sobre um corpo finito é um código estabilizador.

Uma das motivações consideradas para a construção de CGQ's é que as condições necessárias e suficientes para a correção de erro são diretamente "visíveis" da estrutura do grafo [1, 31]. Simetrias úteis para o código podem ser implementadas pela escolha de grafos com grupos de simetrias compatíveis com as capacidades de correção de erro. Essas simetrias não são necessariamente iguais às simetrias utilizadas para códigos estabilizadores [29].

Os códigos grafos quânticos possuem algumas características interessantes [1]:

- frequentemente as condições para a correção de erros podem ser provadas para muitos grupos simultaneamente, já que se obtêm famílias de códigos para sistemas de tamanhos variáveis;
- a intuição geométrica sobre grafos tem se apresentado como sendo bastante útil para se encontrar novas construções de códigos;
- têm a propriedade que todos os elementos da matriz do operador de codificação possuem módulo 1, como a matriz de Hadamard complexa que é uma matriz cujas entradas são números complexos de módulo 1 [78–80]. Tal características possibilita a obtenção de uma expressão compacta para o código;
- para alguns códigos é possível permutar alguns vértices de entrada com alguns vértices de saída mantendo a propriedade de correção de erros. Esta classe de simetria é muito difícil de se ver em construções de estabilizadores usuais, e podem ser úteis em problemas de codificação com entradas e saídas adicionais.

De acordo com Schlingemann [81], a *performance* dos CGQ's, ou seja, qual tipo e quantos erros podem ser corrigidos, podem ser diretamente obtidos da estrutura do grafo.

Nas seções a seguir aborda-se, respectivamente, os seguintes tópicos: uma descrição dos CGQ's, a equivalência entre os CGQ's e os códigos estabilizadores e, por fim, as condições necessárias e suficientes para detecção de erros em CGQ's.

3.2 Descrição Geral dos Códigos Grafos Quânticos

Um CCEQ geral, denotado por $C_Q = [[n, K, d]]_q$, é um subespaço K-dimensional do espaço de Hilbert $\mathcal{H}_q^{\otimes n} = (\mathbb{C}^q)^{\otimes n}$ de dimensão q^n, que é o produto tensorial de n espaços

de Hilbert complexos $\mathcal{H}_q = \mathbb{C}^q$ de dimensão q [50]. Restringe-se aqui $q = p$, em que p é um número primo. Um CCEQ com distância mínima d permite corrigir erros computacionais arbitrários que afetam no máximo $(d-1)/2$ dos n subsistemas. O código estabilizador (ou aditivo) correspondente é denotado por $C_Q = [[n, k, d]]_p$ e tem dimensão $K = p^k$.

Usa-se $\mathbb{F}_p$ para denotar um corpo finito $\mathbb{F}$ de ordem p. Para um conjunto finito V, o espaço vetorial $\mathbb{F}_p^{|V|}$ consiste de tuplas d^V, em que $|V|$ denota a cardinalidade de V. Vetores em $\mathbb{F}_p^{|V|}$ têm um índice superior que representa o grau de liberdade. Assim, usa-se $d^V \in \mathbb{F}_p^{|V|}$ para representar um vetor $d^V = (d^{v_j})_{v_j \in V}$ composto de $|V|$ elementos em $\mathbb{F}_p$, com $j = 0, \ldots, |V|-1$. Por exemplo, se for considerado que $d^V \in \mathbb{F}_p^3$ com $V = \{v_0, v_1, v_2\}$, então $d^V = (d^{v_0}, d^{v_1}, d^{v_2})$, em que $d^{v_0}, d^{v_1}, d^{v_2} \in \mathbb{F}_p$.

Para um subconjunto $L \subset V$ escreve-se $d^L = (d^{l_j})_{l_j \in L}$ para a sub-tupla em $\mathbb{F}_p^{|L|}$. Por exemplo, seja $d^V \in \mathbb{F}_p^3$ com $V = \{l_0, l_1, v_2\}$ e $d^L \in \mathbb{F}_p^2$ com $L = \{l_0, l_1\}$, então $L \subset V$ e $d^L = (d^{l_0}, d^{l_1})$. Pode-se proceder a adição dos vetores d^J e d^L com diferentes índices superiores. Isto é muito conveniente para escrever muitos sistemas de equações de uma forma compacta. O vetor $d^J + d^L$ está contido em $\mathbb{F}_p^{|JL|}$, em que $JL = J \cup L$ é uma notação abreviada para a união dos conjuntos.

Denota-se por $\mathbb{F}_p^{|JL|}$ o espaço vetorial de matrizes retangulares $\Gamma_{J,L} = (\Gamma_{j,l})_{j \in J}^{l \in L}$. Para subconjuntos $B \subset J$ e $F \subset L$ o correspondente sub-bloco em $\mathbb{F}_p^{|BF|}$ é denotado por $\Gamma_{B,F} = (\Gamma_{b,f})_{b \in B}^{f \in F}$. Uma matriz $\Gamma_{J,L}$ é um operador $\mathbb{F}_p$-linear que mapeia $\mathbb{F}_p^{|L|}$ em $\mathbb{F}_p^{|J|}$. Por exemplo, um vetor d^L é mapeado para um vetor d^J da seguinte forma:

$$\Gamma_{J,L} d^L := \sum_{l \in L} \Gamma_{J,l} d^l, \tag{3.1}$$

em que o somatório à direita é uma soma de vetores em $\mathbb{F}_p^{|J|}$.

Para descrever os elementos que determinam um CGQ, é dada a seguir a definição de bicaracter simétrico.[1]

Definição 3.1. *[77] Um bicaracter simétrico $\aleph$ sobre o grupo abeliano $\mathcal{G} \simeq \mathbb{F}_p^m$ pode ser escrito como*

$$\aleph(g, g') = e^{\left[(2\pi i/p) \cdot b(g,g')\right]}, \tag{3.2}$$

em que $g, g' \in \mathcal{G}$, m é um inteiro, $i = \sqrt{-1}$ e b é uma forma bilinear simétrica sobre $\mathbb{F}_p$, isto é,

$$b(g, g') = g^T M g', \tag{3.3}$$

sendo M uma matriz simétrica sobre $\mathbb{F}_p$ e g^T indica o vetor transposto ao vetor g.

Um bicaracter é não-degenerado se, para qualquer $g' \in \mathcal{G}$, satisfaz:

[1] Uma introdução sobre Caracter de Grupos é dada no Apêndice C.

$$\sum_{g\in\mathcal{G}} \aleph(g,g') = |\mathcal{G}|\delta(g') \equiv \begin{cases} |\mathcal{G}| & \text{para} \quad g'=0 \\ \\ 0 & \text{para} \quad g'\neq 0. \end{cases} \tag{3.4}$$

Exemplo 3.1. *Considere um grupo $\mathcal{G}$ cujos elementos pertencem a $\mathbb{F}_3^3$. Seja a matriz geradora de $\mathcal{G}$:*

$$\mathbb{G} = \left[\begin{array}{cc|c} 1 & 0 & 2 \\ 0 & 1 & 2 \end{array}\right], \tag{3.5}$$

ou seja, $\mathcal{G}$ é dado por

$$\mathcal{G} = \{000, 012, 021, 102, 111, 120, 201, 210, 222\}. \tag{3.6}$$

Sendo $g \in \mathcal{G}$, considerando g' como um dos elementos de $\mathcal{G}$ e levando em conta a matriz simétrica

$$M = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \tag{3.7}$$

então tem-se que $\aleph(g,g')$ é um bicaracter simétrico não-degenerado de acordo com (3.2) e (3.4). Para ver isso, considera-se:

(i) $g' = [000]$, para o qual obtém-se

$$\sum_{g\in\mathcal{G}} \aleph(g,[000]) = 1+1+1+1+1+1+1+1+1 = 9 = |\mathcal{G}|; \tag{3.8}$$

(ii) $g' = [012]$, para o qual obtém-se

$$\sum_{g\in\mathcal{G}} \aleph(g,[012]) = 1+\mathrm{e}^{2\pi i/3}+\mathrm{e}^{4\pi i/3}+\mathrm{e}^{4\pi i/3}+1+\mathrm{e}^{2\pi i/3}+\mathrm{e}^{2\pi i/3}+\mathrm{e}^{4\pi i/3}+1 = 0, \tag{3.9}$$

em que este resultado é similarmente obtido para qualquer $g' \in \mathcal{G}$ diferente de $[000]$.

A descrição de um grafo (ou matriz) para CGQ é dada como segue:

Definição 3.2 (Grafo para CGQ [1])**.** *Todo código baseado em grafo aqui construído é completamente determinado pelos seguintes elementos:*

- *Um grafo não-dirigido $G = (V(G), E(G))$, em que $V = V(G) = \mathcal{X} \cup \mathcal{Y}$ é o conjunto de vértices. Distingue-se o conjunto $\mathcal{X}$ de vértices de entrada (com k elementos) e o conjunto $\mathcal{Y}$ de vértices de saída (com n elementos, $n > k$). O conjunto de arestas é dado por $E = E(G) \subset V \times V$;*

- *As arestas do grafo são dadas pela matriz de adjacência do grafo, a qual será denotada por Γ. Cada aresta $\overline{z_j z_l} \in E$ (com $z_j, z_l \in \mathcal{X} \cup \mathcal{Y}$) é rotulada por $\Gamma_{j,l}$. O elemento $\Gamma_{j,l}$ é igual a 1 se, e somente se, os vértices $z_j, z_l \in (\mathcal{X} \cup \mathcal{Y})$ estão conectados, considerando $j, l = 1, \ldots, k+n$ com $j < l$, e 0 caso contrário. De maneira geral, tem-se grafos ponderados, nos quais as matrizes de adjacência têm entradas inteiras arbitrárias, sujeitas as restrições $\Gamma_{j,l} = \Gamma_{l,j}$ e $\Gamma_{j,j} = 0$;*

- *Um grupo finito abeliano $\mathcal{G}$ com um bicaracter simétrico não-degenerado.*

Tendo um grafo cuja descrição está de acordo com os elementos dados pela Definição 3.2 e que $\mathcal{G} \simeq \mathbb{F}_p^m$, o operador de codificação para CGQ é definido a seguir.

Definição 3.3 (Operador de Codificação para CGQ [31])**.** *Seja G um grafo que satisfaz a Definição 3.2. A codificação para um CGQ de tal grafo é dada pelo operador*

$$f(|v\rangle) = \frac{1}{\sqrt{p^{|\mathcal{Y}|}}} \sum_{d^{\mathcal{Y}} \in \mathbb{F}_p^{|\mathcal{Y}|}} \lambda(d^{\mathcal{Y}}) \left| d^{\mathcal{Y}} \right\rangle \in (\mathbb{C}^p)^{\otimes n}, \tag{3.10}$$

em que

$$|v\rangle = \sum_{d^{\mathcal{X}} \in \mathbb{F}_p^{|\mathcal{X}|}} c(d^{\mathcal{X}}) \left| d^{\mathcal{X}} \right\rangle \in (\mathbb{C}^p)^{\otimes k} \tag{3.11}$$

é um vetor diferente de zero com $c(d^{\mathcal{X}}) \in \mathbb{C}$, e sendo

$$\lambda(d^{\mathcal{Y}}) \;=\; \sum_{d^{\mathcal{X}} \in \mathbb{F}_p^{|\mathcal{X}|}} e^{(\frac{2\pi i}{p})\left\{ \frac{1}{2}\left[(d^{\mathcal{X}})^T, (d^{\mathcal{Y}})^T \right] \Gamma \begin{bmatrix} d^{\mathcal{X}} \\ d^{\mathcal{Y}} \end{bmatrix} \right\}} c(d^{\mathcal{X}}) \tag{3.12}$$

com $i = \sqrt{-1}$ e $\sum_k [c(d^{\mathcal{X}})]^2 = 1$.

As provas de que o operador dado em (3.10) gera uma palavra código para um CGQ encontram-se em [31, p. 2390].

Os expoentes $\Gamma_{j,l}$ são dados pela matriz de adjacência Γ de um grafo não dirigido ponderado com pesos $\Gamma_{j,l} \in \mathbb{Z}$. Note que Γ pode também ser visto como um "padrão de interação" ou como um operador simétrico. Desde que (3.10) é independente dos elementos da diagonal $\Gamma_{j,j}$, é possível assumir, sem perda de generalidade, que o grafo é simples.

Neste grafo, os vértices representam os qubits e as arestas representam as interações entre eles (ver Figura 3.1). Além disso, considera-se nessa construção que as interações (arestas) entre os qubits (vértices) são realizadas como no modelo de Ising [1], isto é, somente são consideradas interações entre os vizinhos (qubits) mais próximos. Um número associado a aresta (peso) diferente de zero pode ser visto como a força ou intensidade da interação. Isso pode ser pensado, por exemplo, como uma estrutura de um reticulado óptico bidimensional, em que cada qubit ocupa um ponto dentro de um reticulado cúbico bidimensional com interações entre os vizinhos mais próximos [1].

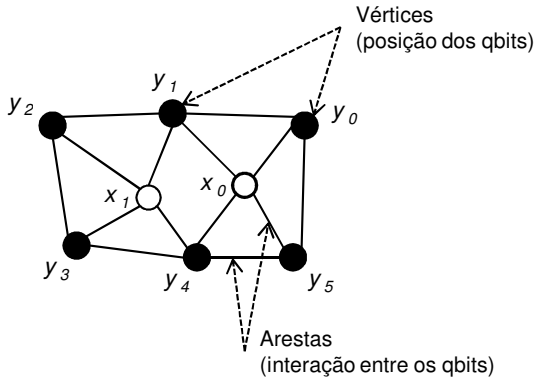

Figura 3.1 Representação de um grafo ilustrando o significado dos vértices e arestas para CGQ.

Após ser realizada a codificação fazendo uso da expressão (3.10), o estado $|\psi\rangle$ representa a palavra código $|\psi\rangle = f(|v\rangle)$, isto é,

$$
\begin{aligned}
|\psi\rangle \;=\; & \frac{1}{\sqrt{p^{|\mathcal{Y}|}}}\Bigg[\Bigg(e^{(\frac{2\pi i}{p})\left\{\frac{1}{2}\left[(d^{\mathcal{X}(0)})^T,(d^{\mathcal{Y}(0)})^T\right]\Gamma\left[\begin{smallmatrix} d^{\mathcal{X}(0)} \\ d^{\mathcal{Y}(0)} \end{smallmatrix}\right]\right\}}\left|d^{\mathcal{Y}(0)}\right\rangle + \ldots + \\
& + e^{(\frac{2\pi i}{p})\left\{\frac{1}{2}\left[(d^{\mathcal{X}(0)})^T,(d^{\mathcal{Y}(p^{|\mathcal{Y}|})})^T\right]\Gamma\left[\begin{smallmatrix} d^{\mathcal{X}(0)} \\ d^{\mathcal{Y}(p^{|\mathcal{Y}|})} \end{smallmatrix}\right]\right\}}\left|d^{\mathcal{Y}(p^{|\mathcal{Y}|})}\right\rangle\Bigg)c(d^{\mathcal{X}(0)}) + \ldots \\
& + \Bigg(e^{(\frac{2\pi i}{p})\left\{\frac{1}{2}\left[(d^{\mathcal{X}(p^{|\mathcal{X}|})})^T,(d^{\mathcal{Y}(0)})^T\right]\Gamma\left[\begin{smallmatrix} d^{\mathcal{X}(p^{|\mathcal{X}|})} \\ d^{\mathcal{Y}(0)} \end{smallmatrix}\right]\right\}}\left|d^{\mathcal{Y}(0)}\right\rangle + \ldots + \\
& + e^{(\frac{2\pi i}{p})\left\{\frac{1}{2}\left[(d^{\mathcal{X}(p^{|\mathcal{X}|})})^T,(d^{\mathcal{Y}(p^{|\mathcal{Y}|})})^T\right]\Gamma\left[\begin{smallmatrix} d^{\mathcal{X}(p^{|\mathcal{X}|})} \\ d^{\mathcal{Y}(p^{|\mathcal{Y}|})} \end{smallmatrix}\right]\right\}}\left|d^{\mathcal{Y}(p^{|\mathcal{Y}|})}\right\rangle\Bigg)c(d^{\mathcal{X}(p^{|\mathcal{X}|})})\Bigg]. \qquad (3.13)
\end{aligned}
$$

3.3 Códigos Grafos Quânticos e Códigos Estabilizadores

Um estado estabilizador de n qubits $|\psi\rangle$ é definido como um autovetor simultâneo com autovalor 1 de n elementos do grupo de Pauli independentes e que comutam M_j.[2] As n equações

[2]Isto significa que nenhum produto da forma $M_1^{x_1} \ldots M_n^{x_n}$, em que $x_j \in \{0, 1\}$, produz a identidade exceto quando todos os x_j são iguais a zero.

de autovalores $M_j |\psi\rangle = |\psi\rangle$ definem o estado $|\psi\rangle$ completamente (até uma fase arbitrária). O conjunto $S := \{M \in \mathcal{G}_n | M |\psi\rangle = |\psi\rangle\}$ é chamado *o estabilizador* do estado $|\psi\rangle$. Ele é um grupo de 2^n operadores de Pauli que comutam, todos os quais tem uma fase global real ± 1 e os n operadores M_j são chamados *geradores* de S, uma vez que cada $M \in S$ pode ser escrito como $M = M_1^{x_1} \ldots M_n^{x_n}$, para algum $x_j \in \{0, 1\}$ [82].

Schlingemann [29] estabeleceu a equivalência entre CGQ's e códigos estabilizadores. Grassl *et al.* [77] provaram que um CGQ sobre um corpo finito é um código estabilizador, como é declarado no teorema a seguir.

Teorema 3.1. *[77] Todo código estabilizador sobre o alfabeto $A = \mathbb{F}_p^m$ é equivalente a um CGQ. Da mesma forma, todo CGQ sobre A é um código estabilizador.*

Tem-se que um grafo convenientemente interpretado é uma outra maneira para representar um espaço vetorial, sendo uma forma de representação que tem a vantagem de tornar mais fácil a visualização do espaço vetorial. No escopo deste trabalho, grafos são utilizados para visualizar estados quânticos.

Para mostrar que um código estabilizador é equivalente a um código grafo, primeiro deve-se encontrar um conjunto de geradores no qual um estado quântico seja estabilizado.

Após encontrar todos os geradores do estabilizador para um determinado estado quântico, deve-se então transformar esses geradores em uma matriz binária, a qual será chamada de *estabilizador binário*, denotada por S_b, composta pelas submatrizes Z_b e X_b, caracterizada da seguinte forma [10]:

$$S_b = \left[\, Z_b \, \middle| \, X_b \, \right], \tag{3.14}$$

em que a submatriz Z_b indica onde estão localizados os operadores Z nos geradores do estabilizador. A submatriz X_b é construída de maneira análoga, mas levando em conta a localização dos operadores X. Considerando uma matriz geradora de um código estabilizador S, a construção de S_b deve ser realizada da seguinte forma:

- Se for encontrado um operador Z na posição s_{ij} de S: a submatriz Z_b recebe 1 na posição z_{ij}, enquanto que a posição x_{ij} de X_b recebe 0;
- Se for encontrado um operador X na posição s_{ij} de S: a submatriz X_b recebe 1 na posição x_{ij}, enquanto que a posição z_{ij} de Z_b recebe 0;
- Se for encontrado um operador Y na posição s_{ij} de S: as submatrizes Z_b e X_b recebem 1 nas posições z_{ij} e x_{ij}, respectivamente;
- Se for encontrado um operador I na posição s_{ij} de S: as submatrizes Z_b e X_b recebem 0 nas posições z_{ij} e x_{ij}, respectivamente.

Por exemplo, seja um código estabilizador gerado pela seguinte matriz:

$$S = \begin{bmatrix} X & I & I & Z & Z & Z \\ I & X & I & Y & Z & X \\ I & I & X & Y & X & Z \\ I & Z & I & X & Y & Z \\ I & Z & Z & I & X & X \\ Z & Z & I & Z & I & X \end{bmatrix},$$

então o correspondente estabilizador binário é

$$S_b = \left[\begin{array}{c|c} Z_b & X_b \end{array}\right] = \left[\begin{array}{cccccc|cccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Uma vez que todo código estabilizador é equivalente a um CGQ (vide Teorema 3.1), Nest *et al.* [82] desenvolveram um esquema sistemático para se obter a representação de um grafo a partir de um código estabilizador, bem como se obter um código estabilizador equivalente a partir da matriz de adjacência de um grafo. Assim, descreve-se a seguir um algoritmo, adaptado por [30], para transformar um código estabilizador em um grafo equivalente, o que permite a obtenção do correspondente CGQ.

1. Obter $\mathcal{T}$ que é a matriz transposta do estabilizador binário, ou seja, $\mathcal{T} = S_b^T = \left[\dfrac{Z_b^T}{X_b^T}\right]$. Tomando $A = Z_b^T$ e $B = X_b^T$, obtém-se $\mathcal{T} = \left[\dfrac{A}{B}\right]$ que, para o exemplo em questão, é dado como segue

$$\mathcal{T} = \left[\frac{A}{B}\right] = \left[\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right].$$

2. Uma vez obtidos A e B, a meta agora é transformar $\mathcal{T}$ em $\mathcal{T}'$, que é o estabilizador binário transposto de um grafo equivalente a este código estabilizador. Para isso, pode-se multiplicar à direita de $\mathcal{T}$ por uma matriz inversível, para desempenhar a mudança de base. Caso a matriz utilizada não seja inversível a mudança de base não é garantida. Sendo B inversível, tem-se:

$$\mathcal{T}' = \mathcal{T}\left[B^{-1}\right] = \left[\frac{AB^{-1}}{BB^{-1}}\right] = \left[\frac{AB^{-1}}{I}\right].$$

Considerando que no exemplo utilizado a matriz B é inversível, então

$$\mathcal{T}' = \mathcal{T}\left[B^{-1}\right] = \left[\frac{AB^{-1}}{I}\right] = \left[\begin{array}{cccccc} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]. \tag{3.15}$$

3. Tendo que a matriz de adjacência Γ corresponde ao estabilizador binário $S_b = \left[\, \Gamma^T \middle| I^T \,\right]$, em que I é a matriz identidade, então AB^{-1} é matriz de adjacência Γ do grafo que repre-

senta o referido código estabilizador. Tomando $A' = AB^{-1}$, segue que $\mathcal{T}' = \left[\, A'^{\,T} \middle| I^T \,\right]$. Caso A' tenha elemento(s) na diagonal que seja(m) diferente(s) de zero, simplesmente deve-se substituí-lo(s) por zero. Dessa forma, obtém-se a matriz de adjacência Γ almejada. Para o exemplo em foco, a matriz de adjacência Γ é dada em (3.16), e o grafo não dirigido equivalente é mostrado na Figura (3.2).

$$\Gamma = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{3.16}$$

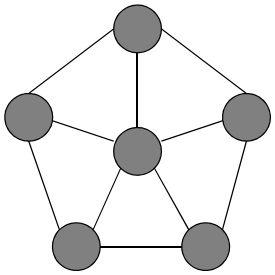

Figura 3.2 Grafo roda que é representado pela matriz de adjacência Γ.

De posse da matriz de adjacência do grafo, pode-se realizar a codificação e a decodificação para o respectivo CGQ.

Para identificar como os qubits estão posicionados no grafo da Figura 3.2, construído com base na matriz de adjacência (3.16), pode-se fazer o seguinte:

1. Constrói-se a nova matriz geradora S' obtida a partir do estabilizador binário $S_b = (\mathcal{T}')^T = \left[\, \Gamma \middle| I \,\right]$, ou seja,

$$S' = \begin{bmatrix} X & I & I & Z & Z & Z \\ I & X & Z & Z & I & Z \\ I & Z & X & Z & Z & I \\ Z & Z & Z & X & Z & Z \\ Z & I & Z & Z & X & I \\ Z & Z & I & Z & I & X \end{bmatrix}. \tag{3.17}$$

2. Para os geradores de S' em (3.17), rotula-se a posição de cada elemento (qubit). Como cada um dos geradores de S' possui seis elementos, estes serão rotulados da esquerda para a direita como 0, 1, 2, 3, 4 e 5.

3. Toma-se X significando o qubit e Z indicando se o referido qubit está conectado ou não. Assim, para a construção do grafo com os respectivos rótulos (posições do qubits) segue-se pela realização dos geradores, observando da esquerda para a direita, as posições dos operadores X e Z. É sugerido que se coloque o rótulo atribuído ao gerador que possui maior número de ligações (i.e., gerador com maior número de operadores Z) no vértice central do grafo da Figura 3.2.

Como resultado do procedimento mencionado acima, têm-se que os vértices do grafo obtido com base nos geradores da matriz (3.17) são rotulados como representado na Figura 3.3.

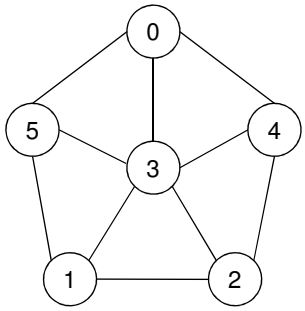

Figura 3.3 Grafo rotulando as posições dos qubits, obtido com base na matriz geradora S'.

Note que se houver uma mudança na configuração do grafo, a matriz geradora correspondente será outra. Essa percepção será fundamental para a compreensão das condições necessárias e suficientes dadas por Schlingemann e Werner [1] para que um grafo gere um CCEQ, as quais serão abordadas na próxima seção.

Também foi provado por Nest *et al.* [82] que $\mathcal{T}$ pode ser transformado em um código equivalente (i.e., com mesmos valores de enumeradores de peso e distância mínima) $\mathcal{T}' = \left[A'^{\,T} \middle| B'^{\,T}\right]$, desde que B' seja inversível.

3.4 Condições para a Correção de Erros em Códigos Grafos Quânticos

Como visto no Seção 2.4, uma caracterização geral de códigos de correção de erros quânticos foi primeiramente trabalhada por Knill e Laflamme [11]. Com base nessa caracterização, Schlingemann e Werner [1] estabeleceram as condições necessárias e suficientes para detecção de erros em CGQ's.

Na teoria estabelecida por Knill e Laflamme [11], um código quântico é uma isometria $f : \mathcal{H}^E \to \mathcal{H}^S$ de um espaço de Hilbert de entrada $\mathcal{H}^E$ para o espaço de Hilbert de saída $\mathcal{H}^S$. Portanto, um operador densidade ρ é transformado por codificação em $f\rho f^*$, o qual é um operador densidade em $\mathcal{H}^S$. A saída da codificação é então passada por meio de um canal ruidoso.

O ruído é descrito por uma certa classe de erros, os quais são representados por um subespaço linear $\mathfrak{E}$ de operadores em $\mathcal{H}^S$. O canal é, portanto, representado por um mapeamento linear completamente positivo da forma

$$\vartheta = \mathrm{T}(\rho) = \sum_{\alpha} \mathcal{E}_\alpha \rho \mathcal{E}_\alpha^*, \tag{3.18}$$

em que $\mathcal{E}_\alpha \in \mathfrak{E}$ e são escolhidos de tal maneira que a saída seja sempre normalizada. A isometria f é um código corretor de erro para $\mathfrak{E}$ se existe um "operador de recuperação" $\mathcal{R}$ completamente positivo tal que

$$\mathcal{R}(\vartheta) = \rho \tag{3.19}$$

para todos os operadores densidade em $\mathcal{H}^E$. Pela teoria de Knill e Laflamme [11] isso é equivalente a condição de fatoração

$$\langle f\psi_1 | \mathcal{E}_\alpha^* \mathcal{E}_\beta f\psi_2 \rangle = \omega(\mathcal{E}_\alpha^* \mathcal{E}_\beta) \langle \psi_1 | \psi_2 \rangle, \tag{3.20}$$

em que $\omega(\mathcal{E}_\alpha^*, \mathcal{E}_\beta)$ é um fator independente dos vetores arbitrários $|\psi_1\rangle, |\psi_2\rangle$ [1]. Será considerado aqui um tipo específico de erros, os chamados erros de ocorrência para somente um pequeno número de saídas do código. Portanto, a estrutura do produto tensorial $\mathcal{H}^{\otimes \mathcal{Y}} = L^2(G^{\mathcal{Y}})$ do espaço de saída vem a ser importante.

Definição 3.4. *[1] Seja $\mathfrak{A}(\mathcal{E})$ denotando o conjunto de todos os operadores em $L^2(G^{\mathcal{Y}})$, os quais são identificados por $\mathcal{E} \subset \mathcal{Y}$, i. e., que são o produto tensorial de um operador arbitrário em $\mathcal{H}^{\otimes \mathcal{E}}$ com a identidade em $\mathcal{H}^{\otimes \mathcal{Y} \setminus \mathcal{E}}$. Diz-se que um código corrige uma quantidade e de erros se $\mathcal{E}_\alpha, \mathcal{E}_\beta$ na equação (*3.20) podem ser escolhidos arbitrariamente no conjunto linearmente gerado (*linear span*) de $\cup_{|\mathcal{E}| \leq e} \mathfrak{A}(\mathcal{E})$.

Note que os operadores $\mathcal{E}_\alpha^* \mathcal{E}_\beta$ aparecendo no produto escalar em (3.20) podem então ser localizados em conjuntos arbitrários de $2e$ elementos e qualquer operador com tal localização pode ser escrito como uma combinação linear de $\mathcal{E}_\alpha^* \mathcal{E}_\beta$. É por isso que torna-se conveniente estabelecer a seguinte definição.

Definição 3.5. *[1] Diz-se que o código f detecta o erro de configuração $\mathcal{E} \subset \mathcal{Y}$ se, e somente se,*

$$\langle f\psi_1 | \mathcal{E} f\psi_2 \rangle = \omega(\mathcal{E}) \langle \psi_1 | \psi_2 \rangle, \tag{3.21}$$

para todo $\mathcal{E} \in \mathfrak{A}(\mathcal{E})$. Então um código corrige uma quantidade e de erros se, e somente se, ele detecta todas as configurações de erros $\mathcal{E} \subset \mathcal{Y}$ com $|\mathcal{E}| \leq 2e$.

Seguem então as condições necessárias e suficientes para detecção de erro quântico em códigos grafos.

Teorema 3.2. *[1] Dado um grupo abeliano finito $\mathcal{G}$ e um grafo ponderado Γ com construção determinada pelos elementos estabelecidos na Definição 3.3. Então uma configuração de erro $\mathcal{E} \subset \mathcal{Y}$ é detectado por um código quântico f_Γ se, e somente se, o sistema de equações*

$$\Gamma_{\mathcal{I},\mathcal{X}\cup\mathcal{E}} d^{\mathcal{X}\cup\mathcal{E}} = 0, \tag{3.22}$$

com $\mathcal{I} = \mathcal{Y} \setminus \mathcal{E}$, implica que

$$d^{\mathcal{X}} = 0 \text{ e } \Gamma_{\mathcal{X},\mathcal{E}} d^{\mathcal{E}} = 0. \tag{3.23}$$

Note que a condição para f_Γ ser uma isometria é equivalente à detecção de zero erro, o qual pode ser visto da equação (3.21) escolhendo-se $\mathcal{E} = I$ para o operador de erro. Isto significa, expresso em termos do grafo, que $\Gamma_{\mathcal{Y},\mathcal{X}} d^{\mathcal{X}} = 0$ implica $d^{\mathcal{X}} = 0$.

O código de cinco qubits foi o primeiro exemplo de código MDS quântico [16]. Entretanto, o código original não é fácil de verificar. Assim, ele será usado para ilustrar que a construção de códigos grafos quânticos pode ser verificada com poucas linhas.

Considere o grafo da Figura 3.4, em que o vértice central (rotulado como "0") é o vértice de entrada e os cinco restantes são os vértices de saída. As Figuras 3.4b e 3.4c representam as configurações relevantes de dois erros em relação aos vértices de saída, ou seja, nos vértices de saída os erros ocorrem em vértices adjacentes - Figura 3.4b - ou em vértices não adjacentes - Figura 3.4c.

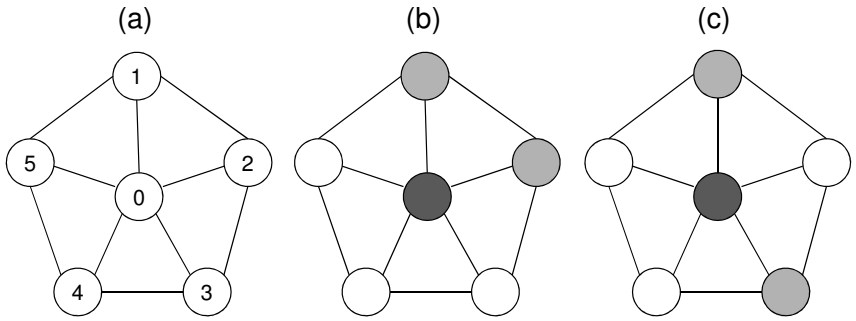

Figura 3.4 Grafo para um código de comprimento 5 e suas configurações relevantes de dois erros [1].

Para verificar as condições dadas pelo Teorema 3.2, mostra-se que para toda configuração de erro $\mathcal{E}$ de dois elementos, tem-se que

$$\Gamma_{\mathcal{I},\mathcal{X}\cup\mathcal{E}} d^{\mathcal{X}\cup\mathcal{E}} = 0 \;\; \Rightarrow \;\; d^{\mathcal{X}\cup\mathcal{E}} = 0. \tag{3.24}$$

Acontece que, em termos da condição de Knill-Laflamme, a Equação (3.24) corresponde à Equação (3.21), em que ω é substituído pelo traço normalizado e, portanto, um código satisfazendo a equação (3.24) é não-degenerado.

A *configuração de erro* é um subconjunto de dois elementos dos vértices de saída (rotulados como $1, 2, 3, 4$ e 5), e para o propósito do critério de verificação (3.24) o vértice de entrada "0" também atuará como um vértice de erro (ver Figura 3.4). Está claro por simetria que somente as duas configurações para $\mathcal{X} \cup \mathcal{E}$ identificadas pelos círculos escuros nas Figuras 3.4b e 3.4c precisam ser consideradas, pois só existem duas possibilidades de ocorrência de erros nos vértices de saída: (i) os erros ocorrem entre vértices adjacentes; ou (ii) os erros ocorrem entre vértices não adjacentes.[3]

Agora a condição $\Gamma_{\mathcal{I},\mathcal{X}\cup\mathcal{E}} d^{\mathcal{X}\cup\mathcal{E}} = 0$ é um conjunto de equações, uma para cada "vértice de integração" $y \in \mathcal{I}$ ($\mathcal{I} = \mathcal{Y} \setminus \mathcal{E}$): para cada vértice y tem-se que somar o d^x para todos os vértices de $x \in \mathcal{X} \cup \mathcal{E}$ conectados à y, igualando-os a zero (em um grafo ponderado, pode-se ter que somar com coeficientes dados pela matriz Γ). A Tabela 3.1 apresenta as equações que originam a primeira configuração de erro, $\mathcal{X} \cup \mathcal{E} = \{0, 1, 2\}$. Observa-se claramente que isso implica em $d^0 = d^1 = d^2 = 0$, em qualquer grupo abeliano. Similarmente, as equações para a segunda configuração de erro $\mathcal{X} \cup \mathcal{E} = \{0, 1, 3\}$ são dadas na Tabela 3.2, o que novamente implica em $d^0 = d^1 = d^3 = 0$. Isto conclui a verificação que o código associado com o grafo da Figura 3.4, e um grupo abeliano finito arbitrário $\mathcal{G}$, detecta quaisquer dois erros e, portanto, corrige um erro.

Tabela 3.1 Erros em vértices adjacentes

Vértice $y(\mathcal{I} = \mathcal{Y} \setminus \mathcal{E})$	Equação $(\mathcal{X} \cup \mathcal{E})$
3	$d^0 + d^2 = 0$
4	$d^0 = 0$
5	$d^0 + d^1 = 0$

Tabela 3.2 Erros em vértices não adjacentes

Vértice $y(\mathcal{I} = \mathcal{Y} \setminus \mathcal{E})$	Equação $(\mathcal{X} \cup \mathcal{E})$
2	$d^0 + d^1 + d^3 = 0$
4	$d^0 + d^3 = 0$
5	$d^0 + d^1 = 0$

[3]Na Teoria dos Grafos, diz-se que um vértice é adjacente a outro se existe uma aresta que os interliga.

3.5 Considerações Finais

Neste capítulo foram apresentados os elementos que permitem construir um CGQ, bem como a forma do operador de codificação para esses códigos. Foi apresentado também a equivalência entre os CGQ's e os códigos estabilizadores e, por fim, as condições necessárias e suficientes para detecção de erros em CGQ's.

No próximo capítulo apresenta-se a primeira contribuição desta tese que é um operador que permite calcular a síndrome de erro para os CGQ's, descreve-se como realizar a decodificação para os CGQ's não-degenerados.

CAPÍTULO 4

Decodificação para Códigos Grafos Quânticos

4.1 Introdução

A dicotomia entre o estado não observável de um qubit e as observações que se pode fazer está no cerne da Computação Quântica, incluindo os CCEQ's. Em correção de erro clássica, a saída do canal é observada, medida e usada diretamente no processo de decodificação. Tal observação no escopo da Mecânica Quântica não somente pode destruir o estado quântico e fazer com que a restauração seja impossível, como também não fornece nenhuma informação a respeito do estado original. O resultado da medição (ou observação) na base computacional é sempre um dos estados da base, $|0\rangle$ e $|1\rangle$ no caso de qubits, no qual a probabilidade de ocorrência é proporcional ao poder da projeção do estado original naquela base [14].

Por esta razão, a decodificação de um CCEQ consiste basicamente em três etapas: medição da síndrome na base computacional, identificação do padrão de erro baseado na síndrome, e aplicação de uma operação corretiva para reverter o erro.

O diagnóstico da síndrome e a reversão do erro são procedimentos bem estabelecidos na teoria de correção de erros quânticos e são realizados, normalmente, obedecendo-se os seguintes passos [8, 83, 84]:

1. Obtenção da síndrome, conseguida após a aplicação de uma operação unitária na palavra recebida.

2. Medição da síndrome.

3. Realização de consulta a uma tabela de síndromes para identificar o padrão de erro mais provável e a consequente identificação da operação de recuperação (correção) a ser aplicada.

A tabela de síndromes é constituída por todas as possibilidades de ocorrência dos erros computacionais, como também a síndrome e a operação de correção a ser aplicada para cada uma dessas possíveis ocorrências.

O procedimento para a construção da tabela de síndromes é relativamente simples, porém é um procedimento exaustivo. Por exemplo, a construção da tabela de síndromes para um código de 5 qubits envolve $2^5 = 32$ possibilidades de ocorrência de erros computacionais diferentes, o que implica em se ter então uma tabela com 32 síndromes. De maneira direta e similar, um código de n qudits terá p^n possibilidades e, portanto, irá conter p^n síndromes, em que p é um número primo.[1] Isso pode ser generalizado para potências de primo $q = p^l$, em que l é um número natural.

Schlingemann [33, 85] apresentou quais são as condições as quais um grafo deve satisfazer para corrigir uma quantidade e de erros com o uso de síndromes e também mostrou que a operação de decodificação para códigos grafos quânticos pode ser realizada para modelos de computadores quânticos *one-way*. Ele também provou que, para qualquer síndrome de erro calculada para um CGQ, existe uma operação de correção local apropriada. Entretanto, não foi encontrado na literatura nenhuma referência a um operador para calcular a síndrome de erro para os CGQ's.

Neste capítulo, apresenta-se uma das contribuições desta tese que é a construção explicita de um operador capaz de calcular a síndrome de erro para os CGQ's. Esta construção possibilita o desenvolvimento de uma operação de decodificação para os CGQ's não-degenerados, também descrita neste capítulo.

A definição de degenerescência depende do conjunto de erros para o qual o CCEQ foi construído para corrigir. Entretanto, quando dois erros tem o mesmo efeito no espaço do código e, portanto, não podem e não necessitam ser distinguidos, então pode-se chamar tal CCEQ de *degenerado*. Por outro lado, se cada erro no conjunto de erros conduz a uma síndrome de erro distinta, tal CCEQ é dito *não-degenerado* [33, 86].

Com o intuito de que o operador desenvolvido para calcular a síndrome de erro possa ser executado de maneira eficiente, fez-se o uso da transformada de Fourier quântica inversa (TFQI) como recurso para realizar a operação inversa da codificação. Isso porque a transformada de Fourier quântica (TFQ) pode ser realizada eficientemente em um computador quântico [8]. Note-se também que o melhor algoritmo de transformada de Fourier quântica conhecido requer somente $O(n \log n)$ portas, em que n é a quantidade de elementos do vetor de entrada, para alcançar uma aproximação eficiente [87]. Alguns exemplos envolvendo a realização da TFQ e TFQI são apresentados no Apêndice B.4.2.

Na seção a seguir apresenta-se uma caracterização dos erros para os CGQ's. Na seção subsequente descreve-se as condições para um grafo corrigir um número e de erros, bem como

[1] Além do termo qubit, usa-se aqui também o termo "qudit" para denotar uma unidade de informação quântica em um sistema quântico d-dimensional.

o operador para o cálculo da síndrome de erro e a descrição da operação de decodificação proposta.

4.2 Representação de Erros para CGQ

A modelagem dos erros computacionais para os CGQ's segue a notação e as recomendações propostas por Feng [31].

Um erro computacional quântico $\sigma_b\tau_s$ $(b, s \in \mathbb{F}_p)$ em um qudit é um operador linear unitário em $\mathbb{C}^p$, o qual age na base $\{|0\rangle, |1\rangle, \ldots, |p-1\rangle\} = \{|a\rangle : a \in \mathbb{F}_p\}$ de $\mathbb{C}^p$ como

$$\sigma_b\tau_s|a\rangle = e^{\frac{2\pi i}{p}(sa)}|a+b\rangle \quad (a \in \mathbb{F}_p). \tag{4.1}$$

O conjunto

$$\mathcal{E}_1 = \{e^{(\frac{2\pi i}{p})m}\sigma_b\tau_s|m, b, s \in \mathbb{F}_p\} \tag{4.2}$$

forma um grupo de erro (não abeliano) [31]. Um erro computacional quântico em n qudits é um operador linear unitário ξ em $(\mathbb{C}^p)^{\otimes n}$ com a seguinte forma:

$$\xi = e^{(\frac{2\pi i}{p})m}\omega_1 \otimes \omega_2 \otimes \ldots \otimes \omega_n, \tag{4.3}$$

em que $\omega_j = \sigma_{b_j}\tau_{s_j}$ and $m, b_j, s_j \in \mathbb{F}_p$. O operador ξ age na base $\{|a_1 \ldots a_n\rangle = |a_1\rangle \otimes |a_2\rangle \otimes \ldots \otimes |a_n\rangle : (a_1, \ldots, a_n) \in \mathbb{F}_p^n\}$ de $(\mathbb{C}^p)^{\otimes n}$. Este operador age no estado de entrada como segue:

$$\begin{aligned} \xi|a_1 \ldots a_n\rangle &= e^{(\frac{2\pi i}{p})m}(\omega_1|a_1\rangle) \otimes (\omega_2|a_2\rangle) \otimes \ldots \otimes (\omega_n|a_n\rangle) \\ &= e^{(\frac{2\pi i}{p})m}e^{(\frac{2\pi i}{p})[(s)^T(a)]}|a+b\rangle, \end{aligned} \tag{4.4}$$

em que $s = (s_1, s_2, \ldots, s_n) \in \mathbb{F}_p^n, b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_p^n$.

O conjunto de todos os erros que podem ser representados por ξ forma um grupo de erro, o qual será denotado por $\mathcal{E}_n$.

Para ξ da forma (4.3), pode-se encontrar $\mathcal{E} \subset \mathcal{Y}, \mathcal{I} = \mathcal{Y} \setminus \mathcal{E}$, tal que

$$\begin{aligned} \xi|d^{\mathcal{Y}}\rangle &= \xi|d^{\mathcal{E}}, d^{\mathcal{I}}\rangle = e^{(\frac{2\pi i}{p})m}\, e^{(\frac{2\pi i}{p})[(s^{\mathcal{E}})^T(d^{\mathcal{E}})]}\big|d^{\mathcal{E}} + b^{\mathcal{E}}, d^{\mathcal{I}}\big\rangle \\ &\quad (m, s^{\mathcal{E}}, b^{\mathcal{E}}, d^{\mathcal{E}} \in \mathbb{F}_p^{\mathcal{E}}). \end{aligned} \tag{4.5}$$

Considere que, quando passando através de um canal quântico, o estado $|\psi\rangle$, vide (3.13), sofra um erro especificado por (4.3). Então, o estado resultante $|\varphi\rangle$ pode ser descrito como segue:

$$\begin{aligned} |\varphi\rangle = \xi|\psi\rangle &= \sum_{d^{\mathcal{Y}} \in \mathbb{F}_p^{|\mathcal{Y}|}} \lambda(d^{\mathcal{Y}})\xi \big| d^{\mathcal{Y}} \big\rangle \\ &= \sum_{d^{\mathcal{Y}} \in \mathbb{F}_p^{|\mathcal{Y}|}} \lambda(d^{\mathcal{E}}, d^{\mathcal{I}})\ \xi\ \big| d^{\mathcal{E}}, d^{\mathcal{I}} \big\rangle \\ &= \sum_{d^{\mathcal{Y}} \in \mathbb{F}_p^{|\mathcal{Y}|}} \lambda(d^{\mathcal{E}}, d^{\mathcal{I}})\ e^{(\frac{2\pi i}{p})m}\ e^{(\frac{2\pi i}{p})[(s^{\mathcal{E}})^T (d^{\mathcal{E}})]} \big| d^{\mathcal{E}} + b^{\mathcal{E}}, d^{\mathcal{I}} \big\rangle. \end{aligned} \tag{4.6}$$

em que

$$\lambda(d^{\mathcal{E}}, d^{\mathcal{I}}) = \sum_{d^{\mathcal{X}} \in \mathbb{F}_p^{|\mathcal{X}|}} e^{(\frac{2\pi i}{p})[\eta]} c(d^{\mathcal{X}}) \tag{4.7}$$

e

$$\eta = \frac{1}{2}\Big[(d^{\mathcal{X}})^T, (d^{\mathcal{E}})^T, (d^{\mathcal{I}})^T\Big] \Gamma \begin{bmatrix} d^{\mathcal{X}} \\ d^{\mathcal{E}} \\ d^{\mathcal{I}} \end{bmatrix}. \tag{4.8}$$

A matriz Γ em (4.8) tem a seguinte forma:

$$\Gamma = \begin{bmatrix} \Gamma_{\mathcal{X},\mathcal{X}} & \Gamma_{\mathcal{X},\mathcal{E}} & \Gamma_{\mathcal{X},\mathcal{I}} \\ \Gamma_{\mathcal{E},\mathcal{X}} & \Gamma_{\mathcal{E},\mathcal{E}} & \Gamma_{\mathcal{E},\mathcal{I}} \\ \Gamma_{\mathcal{I},\mathcal{X}} & \Gamma_{\mathcal{I},\mathcal{E}} & \Gamma_{\mathcal{I},\mathcal{I}} \end{bmatrix}. \tag{4.9}$$

Ao substituir a matriz (4.9) em (4.8) e realizando algumas manipulações algébricas, tomando que as submatrizes $\Gamma_{\mathcal{X},\mathcal{X}} = 0$, $\Gamma_{\mathcal{X},\mathcal{E}} = (\Gamma_{\mathcal{E},\mathcal{X}})^T$, $\Gamma_{\mathcal{X},\mathcal{I}} = (\Gamma_{\mathcal{I},\mathcal{X}})^T$ e $\Gamma_{\mathcal{E},\mathcal{I}} = (\Gamma_{\mathcal{I},\mathcal{E}})^T$ (Definição 3.2), obtém-se

$$\begin{aligned} \eta &= (d^{\mathcal{X}})^T \Gamma_{\mathcal{X},\mathcal{E}}(d^{\mathcal{E}}) + (d^{\mathcal{X}})^T \Gamma_{\mathcal{X},\mathcal{I}}(d^{\mathcal{I}}) + (d^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}}) \\ &\quad + \frac{1}{2}(d^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}}) + \frac{1}{2}(b^{\mathcal{E}})^T \Gamma_{\mathcal{E},\mathcal{E}}(b^{\mathcal{E}}) + \frac{1}{2}(d^{\mathcal{I}})^T \Gamma_{\mathcal{I},\mathcal{I}}(d^{\mathcal{I}}). \end{aligned} \tag{4.10}$$

4.3 Cálculo da Síndrome de Erro e Decodificação para CGQ's Não-Degenerados

Nesta seção descreve-se um operador que faz uso da TFQI adaptada para os CGQ's a fim de calcular a síndrome de erro. Tal operador, chamado *operador de decodificação*, será adotado para construir uma operação de decodificação explicita para CGQ's não-degenerados.

A definição do operador de decodificação para um CGQ é baseada em uma extensão convenientemente ajustada do grafo de codificação pela adição de vértices síndrome L e arestas conectando esses vértices com os vértices de saída $\mathcal{Y}$ de um modo apropriado [33], considerando que $|L| = |\mathcal{Y}| - |\mathcal{X}|$. Os vértices síndrome são vértices de medição usados para estabelecer a síndrome. O conjunto de grafos corretores de uma quantidade e de erros com vértices de entrada $\mathcal{X}$, vértices de saída $\mathcal{Y}$ e vértices de síndrome L devem satisfazer as condições de admissibilidade estabelecidas por Schlingemann [33], as quais são dadas a seguir.

Definição 4.1 (Condições de Admissibilidade – [33] p. 4327)**.** *O conjunto de grafos para CGQ's corretores de uma quantidade e de erros $\mathcal{G}_e(\mathcal{X}, \mathcal{Y}, L)$ é definido como sendo constituído por todos os grafos na união dos vértices de entrada $\mathcal{X}$, de saída $\mathcal{Y}$ e de síndrome L para os quais a matriz de adjacência $\widehat{\Gamma} = \Gamma_{i,j}$, em que $i, j \in \mathcal{X} \cup \mathcal{Y} \cup L$, satisfaz as seguintes condições:*

(c1) *A matriz bloco $\widehat{\Gamma}_{\mathcal{X}\cup L,\mathcal{Y}}$ é inversível, sendo a sua inversa denotada por $\breve{\Gamma}_{\mathcal{Y},\mathcal{X}\cup L}$;*

(c2) *Não existem arestas que conectem vértices de entrada com vértices síndrome, isto é, $\Gamma_{\mathcal{X},L} = 0$ e $\Gamma_{L,\mathcal{X}} = 0$;*

(c3) *Para todos os conjuntos $\mathcal{E} \subset \mathcal{Y}$ que contém no máximo $2e$ elementos, o grafo deve satisfazer a condição*

$$\Gamma_{\mathcal{Y}\setminus\mathcal{E},\mathcal{X}\cup\mathcal{E}} d^{\mathcal{X}\cup\mathcal{E}} = 0 \text{ implica } d^{\mathcal{X}} = 0 \text{ e } \Gamma_{\mathcal{X},\mathcal{E}} d^{\mathcal{E}} = 0. \tag{4.11}$$

Os vértices síndrome L podem ser vistos como qudits que são medidos com o objetivo de fixar a *síndrome de erro*. A síndrome de erro é o resultado da medição e informa qual(ais) erro(s) ocorreu(am) e qual(ais) deve(m) ser a(s) correspondente(s) operação(ões) de correção a ser(em) aplicada(s), relembrando que a síndrome de erro é unicamente determinada para a ocorrência de erro se o código é não-degenerado [33, 86].

Admita que $|\varphi\rangle$ seja obtido após o estado $|\psi\rangle$ sofrer a ocorrência de erros computacionais, i.e., $|\varphi\rangle = \xi\,|\psi\rangle$. Tendo como base um grafo satisfazendo a Definição 4.1, foi desenvolvido neste trabalho um operador de decodificação para CGQ's não-degenerados via TFQI, o qual é dado pelo teorema a seguir.

Teorema 4.1 (Operador de decodificação)**.** *Seja $|\psi\rangle$ o estado codificado de acordo com a Definição 3.3. Suponha que este tenha sofrido erros computacionais ao passar através de um canal*

quântico, resultando em $|\varphi\rangle$*, como descrito em* (4.6). Seja também $\widehat{\Gamma} \in \mathcal{G}_e(\mathcal{X}, \mathcal{Y}, L)$ um grafo corretor de e erros (Definição 4.1). A decodificação para um CGQ não-degenerado é obtido pelo operador

$$\mathcal{T}(|\varphi\rangle) = \frac{1}{\sqrt{p^{|\mathcal{Y}|}}} \sum_{d^L \in \mathbb{F}_p^{|L|}} \sum_{d^{\widehat{\mathcal{X}}} \in \mathbb{F}_p^{|\mathcal{X}|}} e^{-(\frac{2\pi i}{p})[\mu]} \left| d^L d^{\widehat{\mathcal{X}}} \right\rangle, \tag{4.12}$$

em que

$$\mu = \frac{1}{2} \left[(d^{\widehat{\mathcal{X}}})^T, (d^{\mathcal{E}} + b^{\mathcal{E}})^T, (d^{\mathcal{I}})^T, (d^L)^T \right] \widehat{\Gamma} \begin{bmatrix} d^{\widehat{\mathcal{X}}} \\ d^{\mathcal{E}} + b^{\mathcal{E}} \\ d^{\mathcal{I}} \\ d^L \end{bmatrix}, \tag{4.13}$$

notando que $\mathcal{T}$ é uma TFQI "ponderada".

Demonstração: A estratégia da prova é mostrar que o operador $\mathcal{T}$ aplicado ao estado $|\varphi\rangle$ possibilita obter uma síndrome de erro que é unicamente determinada para um erro computacional descrito em (4.3). Sem perda de generalidade, os fatores de normalização serão omitidos.

Considere que o estado $|\psi\rangle$, codificado pela expressão (3.10), tenha sofrido a ocorrência de erros computacionais, i.e.,

$$|\varphi\rangle = \xi \, |\psi\rangle \quad = \quad \sum_{d^{\mathcal{Y}} \in \mathbb{F}_p^{|\mathcal{Y}|}} e^{(\frac{2\pi i}{p}) \left[m + (s^{\mathcal{E}})^T (d^{\mathcal{E}}) \right]} \, \lambda(d^{\mathcal{E}}, d^{\mathcal{I}}) \, \left| d^{\mathcal{E}} + b^{\mathcal{E}}, d^{\mathcal{I}} \right\rangle, \tag{4.14}$$

em que $|\mathcal{Y}| = |\mathcal{E}| + |\mathcal{I}|$.

Dado que o operador $\mathcal{T}$ em (4.12) é uma TFQI, então pela propriedade da linearidade tem-se que

$$\mathcal{T}(|\varphi\rangle) \quad = \quad \sum_{d^{\mathcal{Y}} \in \mathbb{F}_p^{|\mathcal{Y}|}} e^{(\frac{2\pi i}{p}) \left[m + (s^{\mathcal{E}})^T (d^{\mathcal{E}}) \right]} \, \lambda(d^{\mathcal{E}}, d^{\mathcal{I}}) \, \mathcal{T}\Big(\left| d^{\mathcal{E}} + b^{\mathcal{E}}, d^{\mathcal{I}} \right\rangle \Big). \tag{4.15}$$

Substituindo em (4.15) a expressão para $\lambda(d^{\mathcal{E}}, d^{\mathcal{I}})$ dada em (4.7), considerando (4.10), obtém-se

$$\begin{aligned}\mathcal{T}(|\varphi\rangle) \;=\; & \sum_{d^{\mathcal{X}}\in\mathbb{F}_p^{|\mathcal{X}|}} \Bigg\{ \sum_{d^{\mathcal{Y}}\in\mathbb{F}_p^{|\mathcal{Y}|}} e^{(\frac{2\pi i}{p})\left[m+(s^{\mathcal{E}})^T(d^{\mathcal{E}})\right]}\; e^{(\frac{2\pi i}{p})\Big[(d^{\mathcal{X}})^T\Gamma_{\mathcal{X},\mathcal{E}}(d^{\mathcal{E}}) \\ & +(d^{\mathcal{X}})^T\Gamma_{\mathcal{X},\mathcal{I}}(d^{\mathcal{I}})+(d^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}})+\tfrac{1}{2}(d^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}})+\tfrac{1}{2}(d^{\mathcal{I}})^T\Gamma_{\mathcal{I},\mathcal{I}}(d^{\mathcal{I}})\Big]} \\ & \mathcal{T}\Big(\big|d^{\mathcal{E}}+b^{\mathcal{E}},d^{\mathcal{I}}\big\rangle\Big)\Bigg\}\, c(d^{\mathcal{X}}). \end{aligned} \tag{4.16}$$

A matriz $\widehat{\Gamma}$ em (4.13) tem a forma

$$\widehat{\Gamma}=\begin{bmatrix} \Gamma_{\mathcal{X},\mathcal{X}} & \Gamma_{\mathcal{X},\mathcal{E}} & \Gamma_{\mathcal{X},\mathcal{I}} & \Gamma_{\mathcal{X},L} \\ \Gamma_{\mathcal{E},\mathcal{X}} & \Gamma_{\mathcal{E},\mathcal{E}} & \Gamma_{\mathcal{E},\mathcal{I}} & \Gamma_{\mathcal{E},L} \\ \Gamma_{\mathcal{I},\mathcal{X}} & \Gamma_{\mathcal{I},\mathcal{E}} & \Gamma_{\mathcal{I},\mathcal{I}} & \Gamma_{\mathcal{I},L} \\ \Gamma_{L,\mathcal{X}} & \Gamma_{L,\mathcal{E}} & \Gamma_{L,\mathcal{I}} & \Gamma_{L,L} \end{bmatrix}. \tag{4.17}$$

Resolvendo $\mathcal{T}\big(\big|d^{\mathcal{E}}+b^{\mathcal{E}},d^{\mathcal{I}}\big\rangle\big)$ em (4.16), considerando que as submatrizes $\Gamma_{\mathcal{X},\mathcal{X}}=0$ e $\Gamma_{L,L}=0$ (Definição 3.2), $\Gamma_{\mathcal{X},L}=0$ e $\Gamma_{L,\mathcal{X}}=0$ (condição c2, Definição 4.1), $\Gamma_{\mathcal{X},\mathcal{E}}=(\Gamma_{\mathcal{E},\mathcal{X}})^T$, $\Gamma_{\mathcal{X},\mathcal{I}}=(\Gamma_{\mathcal{I},\mathcal{X}})^T$, $\Gamma_{\mathcal{E},\mathcal{I}}=(\Gamma_{\mathcal{I},\mathcal{E}})^T$, $\Gamma_{\mathcal{E},L}=(\Gamma_{L,\mathcal{E}})^T$ e $\Gamma_{\mathcal{I},L}=(\Gamma_{L,\mathcal{I}})^T$, então depois de realizar algumas manipulações algébricas obtém-se

$$\begin{aligned}\mathcal{T}(|\varphi\rangle) \;=\; & \sum_{d^{\mathcal{X}}\in\mathbb{F}_p^{|\mathcal{X}|}} \Bigg\{ \sum_{d^{\mathcal{Y}}\in\mathbb{F}_p^{|\mathcal{Y}|}} e^{(\frac{2\pi i}{p})\left[m+(s^{\mathcal{E}})^T(d^{\mathcal{E}})\right]}\; e^{(\frac{2\pi i}{p})\Big[(d^{\mathcal{X}})^T\Gamma_{\mathcal{X},\mathcal{E}}(d^{\mathcal{E}}) \\ & +(d^{\mathcal{X}})^T\Gamma_{\mathcal{X},\mathcal{I}}(d^{\mathcal{I}})+(d^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}})+\tfrac{1}{2}(d^{\mathcal{E}})^T\Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}})\Big]} \\ & \Bigg[\sum_{d^L\in\mathbb{F}_p^{|L|}}\sum_{d^{\widehat{\mathcal{X}}}\in\mathbb{F}_p^{|\mathcal{X}|}} e^{-(\frac{2\pi i}{p})\Big[(d^{\widehat{\mathcal{X}}})^T\Gamma_{\mathcal{X}\mathcal{E}}(d^{\mathcal{E}}+b^{\mathcal{E}})+(d^{\widehat{\mathcal{X}}})^T\Gamma_{\mathcal{X},\mathcal{I}}(d^{\mathcal{I}}) \\ & +\tfrac{1}{2}(d^{\mathcal{E}}+b^{\mathcal{E}})\Gamma_{\mathcal{E},\mathcal{E}}(d^{\mathcal{E}}+b^{\mathcal{E}})+(d^{\mathcal{E}}+b^{\mathcal{E}})\Gamma_{\mathcal{E},\mathcal{I}}(d^{\mathcal{I}})+(d^{\mathcal{E}}+b^{\mathcal{E}})^T\Gamma_{\mathcal{E},L}(d^L) \\ & +(d^{\mathcal{I}})^T\Gamma_{\mathcal{I},L}(d^L)\Big]\big|d^Ld^{\widehat{\mathcal{X}}}\big\rangle\Bigg]\Bigg\}\, c(d^{\mathcal{X}}). \end{aligned} \tag{4.18}$$

É possível notar em (4.18) que a primeira exponencial representa o erro de troca de fase e que a segunda exponencial representa a fase gerada na etapa de codificação, respectivamente, enquanto que a expressão entre colchetes é a aplicação do operador $\mathcal{T}$ para cada estado da base.

Desde que o operador $\mathcal{T}$ é uma TFQI, então combinando os resultados de $\mathcal{T}$ com os resultados das duas primeiras exponenciais para os $p^{|\mathcal{Y}|}$ estados da base de $|\varphi\rangle$ em (4.18), irá resultar em somente um estado $|d^Ld^{\widehat{\mathcal{X}}}\rangle$ para cada $c(d^{\mathcal{X}})$, em que $|\mathcal{Y}|=|L|+|\mathcal{X}|$. Com a finalidade de recuperar o estado, o qual foi codificado pela expressão (3.10), considerando que se tem um $|d^{\widehat{\mathcal{X}}}\rangle$ diferente para cada $c(d^{\mathcal{X}})$, então deve-se separá-los de $\big|d^L\big\rangle$ (vértices síndromes). Para fazer isso é necessário que os $\big|d^L\big\rangle$ sejam iguais para todo $c(d^{\mathcal{X}})$. Tendo que d^L é o conjunto

dos qudits de medição e que é o mesmo para todo $c(d^{\mathcal{X}})$, então conclui-se que para cada erro descrito em (4.3) haverá uma síndrome de erro unicamente determinada.

□

O cálculo da síndrome de erro permite obter os qudits de medição d^L. Depois de medi-los na base computacional, deve-se fazer uso da tabela de síndromes. Esta tabela consiste de todos os possíveis resultados de medição dos qudits síndromes. Cada um desses resultados está associado com o tipo de erro que ocorreu e também a operação de correção local que deve ser aplicada para recuperar o estado codificado originalmente.

Levando em conta os aspectos mencionados anteriormente e também o Teorema 4.1, uma operação de decodificação apropriada para os CGQ's não-degenerados, o qual tem como entrada o estado $|\varphi\rangle$, consiste dos seguintes passos:

Passo 1. Aplicar o operador $\mathcal{T}$ para cada um dos estados da base $d^{\mathcal{Y}}$ do estado $|\varphi\rangle$ para calcular a síndrome de erro d^L.

Passo 2. Realizar um procedimento de medição em d^L para obter a síndrome de erro.

Passo 3. Checar na tabela de síndromes qual é a operação de correção local que está associada com a síndrome de erro.

Passo 4. Aplicar a operação de correção local obtida na tabela de síndromes para restaurar o estado originalmente codificado.

O operador $\mathcal{T}$ pode ser realizado eficientemente de acordo com [8, 87], e para qualquer síndrome de erro calculada existe uma operação de correção local apropriada [33]. Entretanto, a operação de decodificação apresentada acima pode ser considerada um problema NP-difícil devido ao crescimento exponencial da tabela de síndromes concernente ao comprimento do código.

4.4 Considerações Finais

Neste capítulo descreveu-se uma construção explicita da operação de decodificação para CGQ's não-degenerados. Esta operação pode ser aplicada a qualquer código estabilizador não-degenerador sobre corpos finitos de ordem p, desde que tal código seja equivalente a um CGQ.

Uma das principais vantagens da decodificação proposta é que o operador de decodificação $\mathcal{T}$ pode ser implementado eficientemente em um computador quântico, de acordo com [8, 87].

Apesar do cálculo da síndrome de erro poder ser realizado eficientemente (atribuído a $\mathcal{T}$), encontrar uma operação de correção local apropriada por meio de uma tabela de síndrome

é um problema NP-difícil, uma vez que as linhas da tabela de síndromes crescem exponencialmente em função do comprimento do código. Isso também reforça as constatações apresentadas por Hsieh e Le Gall [86].

Um exemplo ilustrando a aplicação da Definição 3.3 e a operação de decodificação proposta será dado no Capítulo 6.

No próximo capítulo apresenta-se um esquema capaz de proteger a informação contra a ocorrência de múltiplos apagamentos quânticos, fazendo uso de estados GHZ.

CAPÍTULO 5

Um Esquema para a Proteção Contra Múltiplos Apagamentos Quânticos

5.1 Introdução

O uso de sistemas quânticos em várias aplicações de computação e processamento de informação está sujeito à mitigação de efeitos de um fenômeno conhecido como descoerência. Uma das implicações da descoerência é a ocorrência de perda de informação quântica. Por exemplo, fótons são usualmente perdidos em linha de transmissão (correspondendo a um apagamento em linguagem da Teoria da Informação), os quais representam um significante obstáculo para a sobrevivência da coerência quântica [41].

Códigos corretores de apagamentos são conhecidos em teoria de codificação clássica, e sua contrapartida quântica tem sido teoricamente desenvolvida. Uma classe especial de códigos corretores de apagamentos quânticos foi proposta por Grassl *et al.* [39], que consideraram a situação na qual a posição dos qubits errôneos (perdidos) é conhecida. Em concordância com a teoria de codificação clássica, eles chamaram esse modelo de QEC e apresentaram alguns cenários físicos nos quais a posição de um qubit errôneo é determinada, tal como emissão espontânea.

Grassl *et al.* [39] mostraram que somente um código corretor de quatro qubits é requerido para codificar um qubit e corrigir um apagamento. Eles também apresentaram que dois qubits de informação pode ser codificado e um apagamento pode ser corrigido estendendo tal código de quatro qubits, no sentido que somente um qubit adicional é requerido para codificar um qubit de "mensagem" em média. Sem dúvida, este código é um código bastante compacto para realizar a proteção de um ou dois qubits de informação quântica quando a posição do qubit "ruim" é conhecida. Entretanto, ao menos oito qubits são necessários para proteger três qubits de informação quântica contra um apagamento usando tal código (quatro qubits requeridos para a codificação de um qubit de informação quântica e mais outros quatro qubits requeridos para a codificação dos dois qubits restantes de informação quântica).

Tendo em vista a existência de poucos códigos que tratassem a recuperação da informação quando da ocorrência de apagamento quântico e também pela importância que tal alteração representa para vários cenários em computação e comunicação quânticas, Yang *et al.* [42] apresentaram um código que faz uso de três qubits auxiliares (i.e., um total de seis qubits) para proteger três qubits de informação contra a ocorrência de um apagamento. Para isso, eles idealizaram uma operação de codificação que atua da seguinte maneira:

(a) um estado contendo três qubits de informação $|\psi\rangle$ é preparado (espaço 2^3-dimensional);

(b) um bloco de três qubits auxiliares é preparado de forma que todos esses qubits fiquem inicialmente no estado $|0\rangle$;

(c) o produto tensorial dos estados da base de $|\psi\rangle$ com o bloco dos três qubits auxiliares é realizado, ou seja, tem-se agora um estado imerso num espaço 2^6-dimensional;

(d) ao produto tensorial composto por esses dois blocos ($|\psi\rangle$ e qubits auxiliares) é aplicado um operador linear unitário. Esse operador transforma cada um dos estados da base (originalmente na base computacional), em um produto de dois estados GHZ idênticos de três qubits cada, em que a quantidade de amplitudes não é alterada.

Na realização desse código se observa que, depois da operação de codificação, o bloco de qubits auxiliares torna-se um bloco de redundância em relação ao primeiro bloco dos qubits de $|\psi\rangle$. Dessa forma, havendo apagamento em um bloco, pode-se recuperar o qubit apagado via o outro bloco por meio de uma operação de recuperação.

No decorrer deste trabalho de pesquisa foi desenvolvido uma generalização do referido código, fazendo uso de um único bloco de redundância, para tratar qualquer quantidade $k \geq 3$ de qubits. Entretanto, foi percebido que simplesmente aumentando a quantidade de qubits só é possível proteger os k qubits de informação contra apenas a ocorrência de um apagamento, conforme relatado em [45].

Do ponto de vista de algumas aplicações, tais como em junções de Josephson [35], átomos neutros em reticulados ópticos [36], e, mais notoriamente, em fótons isolados que podem ser perdidos durante o processamento ou podem ter a perda atribuída ao uso de fontes e/ou detectores ineficientes [37, 38], pode ser notado que a ocorrência de apagamento dificilmente é restrita a somente um qubit.

Sendo assim, neste capítulo apresenta-se uma das contribuições deste trabalho de tese, que é a caracterização de um esquema capaz de proteger a informação contra a ocorrência de múltiplos apagamentos, conseguida via o aperfeiçoamento do código de Yang *et al.* [42]. Essa técnica permite proteger k-qubits ($k \geq 3$) de informação contra a ocorrência de $t = \lfloor k/2 \rfloor$ apagamentos. Neste esquema $(t+1)$ blocos redundantes são utilizados e restringe-se ao caso em que cada apagamento deve ocorrer em blocos distintos (enviado através de canais diferentes). A detecção da ocorrência de apagamentos em diferentes canais já é comumente usada em experimentos práticos [41, 48].

Este capítulo é organizado como segue. Na seção 5.2 apresenta-se a ideia do esquema proposto para a proteção da informação contra a ocorrência de múltiplos apagamentos quânticos usando estados GHZ. Na Seção 5.3 são mostradas as operações de codificação e restauração que possibilitam a proteção da informação contra a ocorrência de múltiplos apagamentos quânticos. Na Seção 5.4, são apresentadas as considerações finais.

5.2 Ideia Geral do Esquema Proposto

A ideia básica é aprimorar o código dado por Yang *et al.* [42] a fim de desenvolver um esquema que tenha a habilidade de proteger a informação contra a ocorrência de múltiplos apagamentos quânticos. Uma das possibilidades para se conseguir isso seria aumentar a quantidade de blocos de redundância. Mas aí surgem as seguintes questões:

- Aumentar essa quantidade de blocos para quanto?
- E qual seria o tamanho adequado de cada bloco?

Com o intuito de responder a essas indagações, realizou-se neste trabalho de pesquisa uma análise nos operadores de codificação, decodificação e recuperação a fim de verificar como poderia ser aumentada a quantidade de blocos de redundância, de modo a permitir a proteção contra a ocorrência de múltiplos apagamentos. Nessa análise, verificou-se que, para proteger k qubits de informação contra a ocorrência de $t = \lfloor k/2 \rfloor$ apagamentos, faz-se necessário o uso de $t + 1$ blocos redundantes (um bloco auxiliar de k qubits para cada um dos t apagamentos).

Apesar de estar lidando com um caso especial em que uma única parte não pode obter qualquer informação a respeito do estado como um todo, o propósito aqui é apresentar um esquema concreto para proteger k qubits de informação contra a ocorrência de t apagamentos.

Será feita a partir de agora uma breve descrição das quatro etapas que compõem o esquema proposto para proteger a informação contra a ocorrência de múltiplos apagamentos:

1. Prepara-se o estado $|\psi\rangle$ de $k \geq 3$ qubits a ser transmitido, bem como os t blocos de k qubits auxiliares cada (todos inicialmente no estado $|0^{\otimes k}\rangle$), em que $t = \lfloor k/2 \rfloor$.

2. Aplica-se o operador de codificação U_{enc} ao produto do estado $|\psi\rangle$ com os t blocos de qubits auxiliares, de tal maneira a transformar cada um dos 2^k estados da base de $|\psi\rangle$ em um produto de $(t + 1)$ blocos idênticos de estados GHZ de k qubits cada, chamados de *estados lógicos*.

3. Cada um dos $(t + 1)$ blocos do estado codificado é enviado através de $(t + 1)$ canais independentes, os quais podem sofrer até t apagamentos (enfatizando que cada um dos apagamentos deve ocorrer em blocos distintos).

4. O estado corrompido é recuperado por meio da operação de restauração. Esta operação faz uso de um outro bloco de k qubits auxiliares (todos inicialmente no estado $|0\rangle$) com índice $(t+1)$ e dos operadores de decodificação U_{dec} e recuperação U_{rec}. Caso num determinado bloco ocorra apagamento ele será tratado pelo operador U_{rec}, caso contrário será trabalhado pelo operador U_{dec}. Como resultado da aplicação desses operadores, obtém-se: (a) $|B|$ blocos de estados GHZ,[1] tal que cada um destes blocos tem forma idêntica para todos os estados lógicos; e (b) $(t+1-|B|)$ blocos de estados na forma $|0^{\otimes k}\rangle$. Com isso, pode-se então obter o estado $|\psi\rangle$ via o bloco de índice $(t+1)$, agora livre de apagamentos.

Uma vez que no esquema descrito acima cada estado lógico é um produto tensorial de $(t+1)$ blocos, sendo cada bloco um estado GHZ de k qubits, considera-se cada um destes blocos como um *subsistema* do sistema completo. Para recuperar o estado originalmente codificado livre de apagamentos, faz-se uso de um subsistema denominado *sistema de referência*, caracterizado por um bloco de índice $(t+1)$.

Considerando que se deseja que o esquema proposto tenha um sistema de referência estatisticamente independente de qualquer parte escolhida arbitrariamente dentre aquelas que irão interagir com o ambiente, como descrito por Cerf e Cleve [88], então pode-se considerar a situação em que cada subsistema seja enviado por um canal independente de modo que o sistema de referência venha a ser obtido via os blocos de qubits que permanecerem intactos ao passarem através do QEC (doravante denominados de *blocos intactos*).

Na próxima seção mostra-se a formulação das operações de codificação e restauração para a realização do esquema proposto.

5.3 Operações de Codificação e Restauração

Nesta seção mostra-se como é a forma das operações de codificação e restauração que possibilitam a proteção da informação contra a ocorrência de $t = \lfloor k/2 \rfloor$ apagamentos quânticos ($k \geq 3$).

São utilizadas as seguintes notações:

- $\overbrace{|0\rangle \otimes \ldots \otimes |0\rangle}^{k} = |\overbrace{0 \ldots 0}^{k}\rangle = |0^{\otimes k}\rangle$;
- $\bigotimes_{d=1}^{n} |0^{\otimes k}\rangle_{(d)}$ para representar a sequência de produtos tensoriais $|0^{\otimes k}\rangle_{(1)} \otimes \ldots \otimes |0^{\otimes k}\rangle_{(n)}$;
- $m(d)$ significando a posição m de um qubit no bloco de índice (d);
- $|V|$ denotando a cardinalidade de V.

[1] $B \subset D$, $D = \{0, \ldots, t\}$, é o conjunto de blocos nos quais apagamentos foram detectados.

Seja $|\psi\rangle$ um estado arbitrário de $k \geq 3$ qubits. Pode-se codificar o estado $|\psi\rangle$ em

$$|\psi\rangle_{GHZ} = \frac{1}{\sqrt{2^{t+1}}} \sum_{i=0}^{2^k-1} \lambda_i \bigotimes_{d=0}^{t} \left[\left| u_{1(d)}^{(i)} u_{2(d)}^{(i)} \dots u_{k(d)}^{(i)} \right\rangle + (-1)^i \left| \hat{u}_{1(d)}^{(i)} \hat{u}_{2(d)}^{(i)} \dots \hat{u}_{k(d)}^{(i)} \right\rangle \right], \qquad (5.1)$$

em que $\sum_{i=0}^{2^k-1} |\lambda_i|^2 = 1$ e (d) refere-se a blocos de $k \geq 3$ qubits da seguinte maneira: o bloco de índice (0) corresponde aos primeiros k qubits (da "mensagem"), enquanto que os blocos de índices (1) a (t) correspondem a blocos de k qubits auxiliares cada, respectivamente. Aqui, $|u_{m(d)}^{(i)}\rangle$ e $|\hat{u}_{m(d)}^{(i)}\rangle$ representam dois estados ortogonais do qubit na posição $m(d)$, sendo $\hat{u}_{m(d)}^{(i)} = 1 - u_{m(d)}^{(i)}$ e $u_{m(d)}^{(i)} \in \{0, 1\}$.

Desde que o estado $|\psi\rangle_{GHZ}$ é composto por um produto de $(t+1)$ blocos idênticos de estados GHZ de k-qubits cada, é direto mostrar que para o estado codificado (5.1), o operador densidade de cada qubit é dado por $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. Este resultado significa que a informação quântica de k-qubits, originalmente carregada pelos k qubits da mensagem, é distribuída sobre cada qubit após a codificação do estado $|\psi\rangle$ no estado $|\psi\rangle_{GHZ}$.

Com a realização da codificação, dada em (5.1), obtém-se $(t+1)$ blocos redundantes, todos na base GHZ. Como resultado da redundância, o estado quântico de $k \geq 3$ qubits originalmente codificado pode ser recuperado pela operação de restauração quando ele sofrer apagamentos.

A operação de codificação dada em (5.1) pode facilmente ser realizada com o uso de operações (portas) CNOT e da transformada de Hadamard, de acordo com as seguintes etapas:

1. Cada estado da base de $|\psi\rangle$ é identicamente preparado nos t blocos de qubits auxiliares via um operador unitário U_{red}, que faz uso de operações CNOT. Como resultado, o estado gerado é imerso num espaço $2^{k(t+1)}$-dimensional.

2. Ao k-ésimo qubit de cada bloco é aplicado a transformada de Hadamard, e como resultado disso tem-se que o k-ésimo qubit de cada bloco será agora uma soma ou uma subtração, dependendo se o k-ésimo qubit está no estado $|0\rangle$ ou no estado $|1\rangle$.

3. Por fim, utiliza-se um operador unitário U_{GHZ}, consistindo de operações CNOT, que age em cada bloco de tal modo a fazer com que os qubits do segundo termo da soma (subtração) sejam o complemento dos qubits do primeiro termo, similarmente a expressão (5.1).

Depois das três etapas descritas, obtém-se um estado composto por um produto de $(t+1)$ blocos idênticos na base GHZ de k qubits cada. É importante observar que, ao concluir a codificação, nenhuma amplitude tem sido alterada.

Admite-se ao longo deste trabalho que as operações lógicas são *perfeitas*, ou seja, que os códigos são projetados de forma a proteger a informação de erros de transmissão (ou de armazenamento) mas não de erros *operacionais*, intrínsecos às portas lógicas.

A realização da etapa 1 da codificação é descrita pelo lema a seguir. Para isso, mostra-se que tendo um estado arbitrário $|\psi\rangle$ de k qubits e fazendo o produto tensorial dele com t blocos de k qubits auxiliares cada (em que esses qubits estão todos inicialmente no estado $|0\rangle$), obtém-se um estado imerso no espaço $2^{k(t+1)}$-dimensional de forma que ele seja composto por $t+1$ blocos idênticos na base computacional.

Lema 5.1. *Sejam $|\psi\rangle$ um estado de k-qubits ($k \geq 3$) na base computacional e $t = \lfloor k/2 \rfloor$ blocos auxiliares de k qubits cada, todos inicialmente no estado $|0\rangle$. Então, o operador linear unitário U_{red} codifica o produto do estado $|\psi\rangle$ com os t blocos auxiliares de tal forma que o resultado é o produto de $t+1$ blocos idênticos aos dos estados da base de $|\psi\rangle$ (imersão em um espaço de dimensão $2^{k(t+1)}$), em que*

$$U_{red} \;=\; \prod_{d=1}^{t}\left(\prod_{i=1}^{k} C_{i(0),i(d)}\right) \tag{5.2}$$

e $C_{x,y}$ é uma operação CNOT agindo no qubit y (qubit alvo) controlado pelo estado do qubit x (qubit de controle).

Demonstração: Um estado arbitrário $|\psi\rangle$ de k qubits ($k \geq 3$) pode ser descrito, em decomposição binária, da seguinte forma:

$$|\psi\rangle = \lambda_0 |0_1 0_2 \cdots 0_k\rangle + \lambda_1 |0_1 0_2 \cdots 1_k\rangle + \cdots + \lambda_{2^k-1} |1_1 1_2 \cdots 1_k\rangle\,, \tag{5.3}$$

em que $\sum_{i=0}^{2^k-1} |\lambda_i|^2 = 1$.

O produto tensorial de $|\psi\rangle$ com $d = \{1, \ldots, t\}$ blocos de k qubits auxiliares, todos no estado $|0\rangle$, fica como segue

$$\begin{aligned} |\psi\rangle_{(0)} \bigotimes_{d=1}^{t} |0\rangle_{(d)}^{\otimes k} \;&=\; \Big(\lambda_0 |0_1 0_2 \cdots 0_k\rangle_{(0)} + \lambda_1 |0_1 0_2 \cdots 1_k\rangle_{(0)} + \cdots + \lambda_{2^k-1} |1_1 1_2 \cdots 1_k\rangle_{(0)}\Big) \\ &\quad \otimes \Big(|0_1 0_2 \cdots 0_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_k\rangle_{(t)}\Big) \end{aligned}$$

$$\begin{aligned} \;=\; &\lambda_0 \Big(|0_1 0_2 \cdots 0_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_k\rangle_{(t)}\Big) \\ &+\lambda_1 \Big(|0_1 0_2 \cdots 1_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_k\rangle_{(t)}\Big) + \\ &\vdots \\ &+\lambda_{2^k-1} \Big(|1_1 1_2 \cdots 1_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_k\rangle_{(t)}\Big). \end{aligned} \tag{5.4}$$

Tendo em vista que U_{red} é um operador linear, sua aplicação em (5.4), resulta:

$$\begin{aligned}
|\psi\rangle' &= U_{red}\Big(|\psi\rangle_{(0)} \bigotimes_{d=1}^{t} |0\rangle_{(d)}^{\otimes k} \Big) \\
&= U_{red}\Big[\lambda_0\big(|0_1 0_2 \cdots 0_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_k\rangle_{(t)} \big)\Big] \\
&\quad + U_{red}\Big[\lambda_1\big(|0_1 0_2 \cdots 1_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_k\rangle_{(t)} \big)\Big] \\
&\quad + \cdots + U_{red}\Big[\lambda_{2^k-1}\big(|1_1 1_2 \cdots 1_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_k\rangle_{(1)} \otimes \ldots \\
&\quad \otimes |0_1 0_2 \cdots 0_k\rangle_{(t)} \big)\Big]. \qquad (5.5)
\end{aligned}$$

Observe que

$$\begin{aligned}
U_{red} &= \prod_{d=1}^{t}\left(\prod_{i=1}^{k} C_{i(0),i(d)}\right) \\
&= \Big(C_{1(0),1(1)} C_{2(0),2(1)} \ldots C_{k(0),k(1)}\Big) \ldots \Big(C_{1(0),1(t)} C_{2(0),2(t)} \ldots C_{k(0),k(t)}\Big), \qquad (5.6)
\end{aligned}$$

em que essas composições dos operadores CNOT são realizadas da direita para a esquerda.

Como se pode perceber em (5.6), para cada aplicação de $C_{x,y}$ a posição do bit de controle, que é sempre observada no bloco de índice (0), é igual a posição do bit alvo a ser aplicado no bloco de índice (d), sendo $d \in \{1, \ldots, t\}$, para cada uma das k posições.

Realizando agora a aplicação de (5.6) em (5.5), obtém-se

$$\begin{aligned}
|\psi\rangle' &= \lambda_0\Big(|0_1 0_2 \cdots 0_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_k\rangle_{(t)} \Big) \\
&\quad + \lambda_1\Big(|0_1 0_2 \cdots 1_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 1_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 1_k\rangle_{(t)} \Big) \\
&\quad \vdots \\
&\quad + \lambda_{2^k-1}\Big(|1_1 1_2 \cdots 1_k\rangle_{(0)} \otimes |1_1 1_2 \cdots 1_k\rangle_{(1)} \otimes \ldots \otimes |1_1 1_2 \cdots 1_k\rangle_{(t)} \Big). \qquad (5.7)
\end{aligned}$$

Portanto, após a aplicação do operador U_{red} ao produto $\Big(|\psi\rangle_{(0)} \bigotimes_{d=1}^{t} |0\rangle_{(d)}^{\otimes k}\Big)$, obtém-se um estado composto por $t+1$ blocos idênticos aos estados da base de $|\psi\rangle$, em que $t = \lfloor k/2 \rfloor$.

□

Para a realização da etapa 2 da codificação (p. 59), aplica-se a transformada de Hadamard ao k-ésimo qubit de cada um dos $(t+1)$ blocos de (5.7), ou seja, $H_k |\psi\rangle'$. Com isso, obtém-se (os fatores de normalização serão omitidos):

$$
\begin{aligned}
|\psi\rangle'' = H_k\,|\psi\rangle' \;=\; & \lambda_0\Big[\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(0)} \\
& \otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(1)} \\
& \otimes\ldots\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(t)}\Big] \\
& +\lambda_1\Big[\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(0)} \\
& \otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(1)} \\
& \otimes\ldots\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(t)}\Big] + \\
& \vdots \\
& +\lambda_{2^k-1}\Big[\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(0)} \\
& \otimes\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(1)} \\
& \otimes\ldots\otimes\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(t)}\Big]. \qquad (5.8)
\end{aligned}
$$

O lema a seguir mostra que a etapa 3 da codificação (p. 59) pode ser realizada por meio de uma operação unitária em $|\psi\rangle''$ tal que, no segundo termo, cada soma/subtração em cada bloco de k qubits seja o complemento do primeiro termo.

Lema 5.2. *Seja $|\psi\rangle''$ um estado composto por $t+1$ blocos idênticos de k qubits cada, como descrito em* (5.8), em que $k \geq 3$ e $t = \lfloor k/2 \rfloor$. Então, o operador linear unitário

$$
U_{GHZ} \;=\; \prod_{d=0}^{t}\left(\prod_{i=1}^{k-1} C_{k(d),i(d)}\right) \qquad (5.9)
$$

codifica o estado $|\psi\rangle''$ tal que o segundo termo de cada soma/subtração, em cada bloco de k qubits, seja o complemento do primeiro termo.

Demonstração: Tendo o estado $|\psi\rangle''$ como descrito em (5.8) e sendo U_{GHZ} um operador linear unitário, então ao aplicar U_{GHZ} em (5.8), tem-se:

$$
\begin{aligned}
|\psi\rangle_{GHZ} \;&=\; U_{GHZ}\big(\,|\psi\rangle''\,\big) \\
&=\; \lambda_0\Big\{U_{GHZ}\Big[\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(0)} \\
&\quad \otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(1)} \\
&\quad \otimes\ldots\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(t)}\Big]\Big\}
\end{aligned}
$$

$$
\begin{aligned}
&+\lambda_1\Big\{U_{GHZ}\Big[\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(0)}\\
&\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(1)}\\
&\otimes\ldots\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(t)}\Big]\Big\}+\\
&\vdots\\
&+\lambda_{2^k-1}\Big\{U_{GHZ}\Big[\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(0)}\\
&\otimes\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(1)}\\
&\otimes\ldots\otimes\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(t)}\Big]\Big\}. \qquad (5.10)
\end{aligned}
$$

Observe que:

$$
\begin{aligned}
U_{GHZ} &= \prod_{d=0}^{t}\left(\prod_{i=1}^{k-1} C_{k(d),i(d)}\right)\\
&= \Big(C_{k(0),1(0)}C_{k(0),2(0)}\cdots C_{k(0),k-1(0)}\Big)\Big(C_{k(1),1(1)}C_{k(1),2(1)}\cdots C_{k(1),k-1(1)}\Big)\\
&\quad\cdots\Big(C_{k(t),1(t)}C_{k(t),2(t)}\cdots C_{k(t),k-1(t)}\Big). \qquad (5.11)
\end{aligned}
$$

A fim de fazer com que cada soma/subtração em cada bloco de k qubits no segundo termo seja o complemento do primeiro termo, o operador $C_{x,y}$ em (5.11) deve agir nos qubits que estão nas posições 1 até $k-1$, para cada um dos $t+1$ blocos, considerando o qubit da k-ésima posição (bit de controle), como segue: se ele está no estado $|1\rangle$, então os qubits b_i (em que $i = 1,\ldots,k-1$ indica a posição do qubit) serão alterados para $(b_i + 1 \mod 2)$; caso contrário não serão alterados.

Realizando agora a aplicação de (5.11) em (5.10), obtém-se

$$
\begin{aligned}
|\psi\rangle_{GHZ} &= U_{GHZ}\big(\,|\psi\rangle''\big)\\
&= \lambda_0\Big[\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(0)}\\
&\quad\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(1)}\\
&\quad\otimes\ldots\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(t)}\Big]\\
&\quad+\lambda_1\Big[\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(0)}\\
&\quad\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(1)}\\
&\quad\otimes\ldots\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(t)}\Big]+\\
&\quad\vdots
\end{aligned}
$$

$$
\begin{aligned}
&+\lambda_{2^k-1}\Big[\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(0)}\\
&\otimes\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(1)}\\
&\otimes\ldots\otimes\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(t)}\Big].
\end{aligned}
\tag{5.12}
$$

Portanto, após a aplicação do operador U_{GHZ} em $|\psi\rangle''$, obtém-se um estado $|\psi\rangle_{GHZ}$ tal que o segundo termo de cada soma/subtração, em cada bloco de k qubits, seja o complemento do primeiro termo.

□

O teorema a seguir mostra a operação que codifica cada um dos estados da base do estado $|\psi\rangle$, de $k \geq 3$ qubits, como um produto de $(t+1)$ blocos redundantes de estados GHZ, de k-qubits cada.

Teorema 5.1. *Sejam $|\psi\rangle$ um estado de k-qubits ($k \geq 3$) na base computacional e $t = \lfloor k/2 \rfloor$ blocos de k qubits auxiliares cada, todos inicialmente no estado $|0\rangle$. Então, a operação de codificação, denotada por $\mathfrak{E}_{GHZ}$, codifica cada um dos estados da base de $|\psi\rangle$ como um produto de $(t+1)$ blocos redundantes de estados GHZ de k-qubits cada. Essa operação de codificação $\mathfrak{E}_{GHZ}$ é dada por*

$$
\mathfrak{E}_{GHZ} = U_{enc}\left[|\psi\rangle_{(0)}\bigotimes_{d=1}^{t}\left(|0^{\otimes k}\rangle_{(d)}\right)\right],
\tag{5.13}
$$

em que

$$
U_{enc} \;=\; U_{GHZ}\cdot\left(\prod_{d=0}^{t} H_{k(d)}\right)\cdot U_{red},
\tag{5.14}
$$

sendo U_{red} como em (5.2) e U_{GHZ} como em (5.9).

Demonstração: Seja $|\psi\rangle$ um estado arbitrário de k qubits ($k \geq 3$) o qual é descrito, em decomposição binária, da seguinte forma

$$
|\psi\rangle = \lambda_0\,|0_1 0_2\cdots 0_{k-1}0_k\rangle + \lambda_1\,|0_1 0_2\cdots 0_{k-1}1_k\rangle + \cdots + \lambda_{2^k-1}\,|1_1 1_2\cdots 1_{k-1}1_k\rangle\,,
\tag{5.15}
$$

em que $\sum_{i=0}^{2^k-1}|\lambda_i|^2 = 1$.

Agora será aplicado o operador U_{enc}, dado em (5.14), a $\left[|\psi\rangle_{(0)}\bigotimes_{d=1}^{t}\left(|0^{\otimes k}\rangle_{(d)}\right)\right]$.

Pelo Lema 5.1, após a aplicação do operador U_{red} a $\left[|\psi\rangle_{(0)}\bigotimes_{d=1}^{t}\left(|0^{\otimes k}\rangle_{(d)}\right)\right]$, tem-se

$$
\begin{aligned}
|\psi\rangle' &= U_{red}\Big[|\psi\rangle_{(0)} \bigotimes_{d=1}^{t} \big(|0^{\otimes k}\rangle_{(d)}\big)\Big] \\
&= \lambda_0\big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_{k-1} 0_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_{k-1} 0_k\rangle_{(t)}\,\big) \\
&\quad +\lambda_1\big(\,|0_1 0_2 \cdots 0_{k-1} 1_k\rangle_{(0)} \otimes |0_1 0_2 \cdots 0_{k-1} 1_k\rangle_{(1)} \otimes \ldots \otimes |0_1 0_2 \cdots 0_{k-1} 1_k\rangle_{(t)}\,\big) + \\
&\quad \vdots \\
&\quad +\lambda_{2^k-1}\big(\,|1_1 1_2 \cdots 1_{k-1} 1_k\rangle_{(0)} \otimes |1_1 1_2 \cdots 1_{k-1} 1_k\rangle_{(1)} \otimes \ldots \otimes |1_1 1_2 \cdots 1_{k-1} 1_k\rangle_{(t)}\,\big).
\end{aligned}
\tag{5.16}
$$

Aplicando a transformada de Hadamard ao k-ésimo qubit de cada um dos $(t+1)$ blocos de $|\psi\rangle'$, obtém-se (os fatores de normalização são omitidos):

$$
\begin{aligned}
|\psi\rangle'' &= H_k\,|\psi\rangle' \\
&= \lambda_0\Big[\big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle + |0_1 0_2 \cdots 0_{k-1} 1_k\rangle\,\big)_{(0)} \\
&\quad \otimes\big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle + |0_1 0_2 \cdots 0_{k-1} 1_k\rangle\,\big)_{(1)} \\
&\quad \otimes \ldots \otimes \big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle + |0_1 0_2 \cdots 0_{k-1} 1_k\rangle\,\big)_{(t)}\Big] \\
&\quad +\lambda_1\Big[\big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle - |0_1 0_2 \cdots 0_{k-1} 1_k\rangle\,\big)_{(0)} \\
&\quad \otimes\big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle - |0_1 0_2 \cdots 0_{k-1} 1_k\rangle\,\big)_{(1)} \\
&\quad \otimes \ldots \otimes \big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle - |0_1 0_2 \cdots 0_{k-1} 1_k\rangle\,\big)_{(t)}\Big] + \\
&\quad \vdots \\
&\quad +\lambda_{2^k-1}\Big[\big(\,|1_1 1_2 \cdots 1_{k-1} 0_k\rangle - |1_1 1_2 \cdots 1_{k-1} 1_k\rangle\,\big)_{(0)} \\
&\quad \otimes\big(\,|1_1 1_2 \cdots 1_{k-1} 0_k\rangle - |1_1 1_2 \cdots 1_{k-1} 1_k\rangle\,\big)_{(1)} \\
&\quad \otimes \ldots \otimes \big(\,|1_1 1_2 \cdots 1_{k-1} 0_k\rangle - |1_1 1_2 \cdots 1_{k-1} 1_k\rangle\,\big)_{(t)}\Big].
\end{aligned}
\tag{5.17}
$$

Pelo Lema 5.2, após a aplicação do operador U_{GHZ} ao estado $|\psi\rangle''$, tem-se

$$
\begin{aligned}
|\psi\rangle_{GHZ} &= U_{GHZ}\,|\psi\rangle'' \\
&= \lambda_0\Big[\big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle + |1_1 1_2 \cdots 1_{k-1} 1_k\rangle\,\big)_{(0)} \\
&\quad \otimes\big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle + |1_1 1_2 \cdots 1_{k-1} 1_k\rangle\,\big)_{(1)} \\
&\quad \otimes \ldots \otimes \big(\,|0_1 0_2 \cdots 0_{k-1} 0_k\rangle + |1_1 1_2 \cdots 1_{k-1} 1_k\rangle\,\big)_{(t)}\Big]
\end{aligned}
$$

$$
\begin{aligned}
&+\lambda_1\Big[\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(0)}\\
&\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(1)}\\
&\otimes\ldots\otimes\big(\,|0_1 0_2\cdots 0_{k-1}0_k\rangle - |1_1 1_2\cdots 1_{k-1}1_k\rangle\,\big)_{(t)}\Big] +\\
&\vdots\\
&+\lambda_{2^k-1}\Big[\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(0)}\\
&\otimes\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(1)}\\
&\otimes\ldots\otimes\big(\,|1_1 1_2\cdots 1_{k-1}0_k\rangle - |0_1 0_2\cdots 0_{k-1}1_k\rangle\,\big)_{(t)}\Big].
\end{aligned}
\tag{5.18}
$$

O resultado apresentado em (5.18) conclui a aplicação da operação de codificação $\mathfrak{E}_{GHZ}$. Portanto, o produto tensorial do estado $|\psi\rangle$, de k-qubits ($k \geq 3$), com os $t = \lfloor k/2 \rfloor$ blocos auxiliares de k qubits cada (todos inicialmente no estado $|0\rangle$), é codificado por $\mathfrak{E}_{GHZ}$ de tal maneira a produzir um estado $|\psi\rangle_{GHZ}$, o qual possui $(t+1)$ blocos redundantes de k qubits cada $(k \geq 3)$ na base GHZ.

□

Pode-se certamente imaginar situações em que se poderia, de fato, saber onde o erro ocorreu (usando métodos para determinar a posição de um erro, ver [39]). Devido aos estados $|0\rangle$ e $|1\rangle$ formarem uma base para um qubit, é preciso somente saber o que ocorre com esses dois estados. Em geral, o processo de descoerência deve ser

$$
\begin{aligned}
|e_0\rangle|0\rangle &\longrightarrow |\epsilon_0\rangle|0\rangle + |\epsilon_1\rangle|1\rangle,\\
|e_0\rangle|1\rangle &\longrightarrow |\epsilon_0^{'}\rangle|0\rangle + |\epsilon_1^{'}\rangle|1\rangle,
\end{aligned}
\tag{5.19}
$$

em que $|\epsilon_0\rangle$, $|\epsilon_1\rangle$, $|\epsilon_0^{'}\rangle$ e $|\epsilon_1^{'}\rangle$ são estados do ambiente apropriados, não necessariamente ortogonais ou normalizados, e $|e_0\rangle$ é o estado inicial do ambiente [42].

Como será mostrado posteriormente, durante a operação de restauração, não existe a necessidade de realizar quaisquer operações nos qubits "ruins". Para simplificar, pode-se reescrever (5.19) como

$$
\begin{aligned}
|e_0\rangle|0\rangle &\longrightarrow |\overline{0}\rangle\\
|e_0\rangle|1\rangle &\longrightarrow |\overline{1}\rangle,
\end{aligned}
\tag{5.20}
$$

em que os estados do ambiente $|\epsilon_0\rangle$, $|\epsilon_1\rangle$, $|\epsilon_0^{'}\rangle$ e $|\epsilon_1^{'}\rangle$ em (5.19) têm sido incluídos em $|\overline{0}\rangle$ e $|\overline{1}\rangle$. Supõe-se inicialmente que qualquer apagamento somente ocorre após o estado emaranhado ter sido gerado. Por referência, o estado $|\psi\rangle_{GHZ}$ depois de sofrer apagamento será representado por $|\overline{\psi}\rangle_{GHZ}$. Admite-se também que podem ocorrer no máximo $t = \lfloor k/3 \rfloor$ apagamentos e que estão em blocos distintos. Levando em conta estas considerações, para restaurar o estado originalmente protegido contra a ocorrência de t apagamentos, serão utilizados os seguintes tipos de operadores:

- *Operador de decodificação* que atua no(s) bloco(s) em que não foi detectado apagamento;
- *Operador de recuperação*, um para cada bloco em que foi detectado apagamento.

Para extrair o estado original livre de apagamentos, aplica-se primeiro uma transformação unitária nos blocos de qubits que ao passarem pelo QEC não tenha sido detectado apagamento, os quais são chamados de *blocos intactos*. Esta transformação é considerada como um operador de decodificação parcial (uma vez que os blocos que sofreram apagamento não são envolvidos no operador de decodificação). Para evitar que o Teorema da Não-Clonagem seja violado e também para facilitar o uso de um bloco de referência no operador de recuperação, essa transformação unitária faz uso de um novo bloco de k qubits auxiliares (todos inicialmente no estado $|0\rangle$).

Este operador de decodificação, denotado por U_{dec}, atua da seguinte maneira:

1. Realiza uma transformação da base GHZ para a base computacional no(s) bloco(s) intacto(s).
2. O(s) bloco(s) intacto(s) é(são) identicamente preparado(s) no bloco de índice $(t+1)$, consistindo k qubits auxiliares que estão inicialmente no estado $|0\rangle$.
3. Transforma cada um dos k qubits do(s) bloco(s) intacto(s) no estado $|0\rangle$.

A expressão deste operador U_{dec} é dada a seguir:

Lema 5.3. *Sejam $|\overline{\psi}\rangle_{GHZ}$, um estado composto de $t+1$ blocos idênticos na base GHZ de k-qubits cada ($k \geq 3$) os quais podem ter sofrido até $t = \lfloor k/2 \rfloor$ apagamentos ao passar pelo QEC, e $B \subset D$ ($D = \{0, \ldots, t\}$), o conjunto dos índices que identificam os blocos em que foram detectados apagamentos. Se for aplicado o operador linear unitário*

$$U_{dec} = \prod_{\substack{d=0 \\ (d \notin B)}}^{t} \left(\prod_{i=1}^{k} C_{i(t+1),i(d)} \right) \cdot \prod_{\substack{d=0 \\ (d \notin B)}}^{t} \left(\prod_{i=1}^{k} C_{i(d),i(t+1)} H_{k(d)} \prod_{i=1}^{k-1} C_{k(d),i(d)} \right), \tag{5.21}$$

ao produto tensorial

$$|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)},$$

então os seguintes passos são realizados: (i) *todos os blocos intactos de* $|\overline{\psi}\rangle_{GHZ}$ *são transformados da base GHZ para a base computacional;* (ii) *esses blocos intactos são identicamente preparados no bloco de índice* $(t+1)$*; e, finalmente,* (iii) *os qubits dos blocos intactos são transformados no estado* $|0\rangle$*.*

Demonstração: Seja $|\overline{\psi}\rangle_{GHZ}$ o estado obtido depois que o estado $|\psi\rangle_{GHZ}$, o qual tem $(t+1)$ blocos redundantes de k qubits cada $(k \geq 3)$ na base GHZ, passou pelo QEC e pode ter sofrido até $t = \lfloor k/2 \rfloor$ apagamentos (em que cada apagamento deve ocorrer em blocos distintos).

Tendo em vista que o operador de decodificação U_{dec} irá atuar apenas nos blocos intactos, é interessante verificar sua aplicação em dois casos:

1. Quando apenas um bloco está intacto (t apagamentos ocorreram);
2. Quando dois ou mais blocos estiverem intactos.

Para esses dois casos, será mostrados que o operador U_{dec} (5.21): (a) irá identicamente preparar, no bloco de índice $(t+1)$, todos os blocos intactos; e (b) irá transformar os k qubits dos blocos intactos no estado $|0\rangle$.

Caso 1: O estado $|\overline{\psi}\rangle_{GHZ}$ possui $t+1$ blocos e sofreu t apagamentos. Considera-se o caso em que apenas um destes blocos está intacto, i.e., que houve a ocorrência desses apagamentos em t blocos diferentes (um apagamento em cada bloco). Será estabelecido, sem perda de generalidade, que esses apagamentos ocorreram nos blocos de índices (0) a $(t-1)$, ficando intacto então o bloco de índice (t).

Note que para U_{dec}, a posição em que ocorreu o apagamento não é importante. Entretanto, para fins de representação, será admitido que o mesmo tenha ocorrido na posição a, em que $0 \leq a < k$. Assim, o estado $|\overline{\psi}\rangle_{GHZ}$ para este caso tem a seguinte forma:

$$|e_0\rangle \otimes |\psi\rangle_{GHZ} \rightarrow |\overline{\psi}\rangle_{GHZ} \;\; = \;\; \lambda_0|\overline{0}\rangle_L + \lambda_1|\overline{1}\rangle_L + \ldots + \lambda_{2^k-2}|\overline{2^k-2}\rangle_L + \lambda_{2^k-1}|\overline{2^k-1}\rangle_L, \tag{5.22}$$

em que os estados lógicos são dados como segue, considerando que o traço na parte superior representa a posição onde o apagamento ocorreu e também que são denotadas as possíveis mudanças de fase:

$$
\begin{aligned}
|\overline{0}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \\
&\quad \otimes\ldots\otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \otimes\Big(|\ldots 0_a\ldots 0_k\rangle + |\ldots 1_a\ldots 1_k\rangle\Big)_{(t)}\Big], \\
|\overline{1}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \mp |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \\
&\quad \otimes\ldots\otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \mp |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \otimes\Big(|\ldots 0_a\ldots 0_k\rangle - |\ldots 1_a\ldots 1_k\rangle\Big)_{(t)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle + |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(0)} \\
&\quad \otimes\ldots\otimes\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle + |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \otimes\Big(|\ldots 1_a\ldots 0_k\rangle + |\ldots 0_a\ldots 1_k\rangle\Big)_{(t)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle - |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(0)} \\
&\quad \otimes\ldots\otimes\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle - |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \otimes\Big(|\ldots 1_a\ldots 0_k\rangle - |\ldots 0_a\ldots 1_k\rangle\Big)_{(t)}\Big].
\end{aligned} \tag{5.23}
$$

Desde que U_{dec} é somente aplicado aos blocos intactos, isto significa que, para o caso em tela, ele será aplicado somente ao bloco de índice (t). Sendo assim, ele terá a forma:

$$
\begin{aligned}
U_{dec} &= \left(\prod_{i=1}^{k} C_{i(t+1),i(t)}\right)\left(\prod_{i=1}^{k} C_{i(t),i(t+1)}\right) H_{k(t)}\left(\prod_{i=1}^{k-1} C_{k(t),i(t)}\right) \\
&= \Big(C_{1(t+1),1(t)}\cdots C_{k(t+1),k(t)}\Big)\Big(C_{1(t),1(t+1)}\cdots C_{k(t),k(t+1)}\Big) \\
&\quad H_{k(t)}\Big(C_{k(t),1(t)}\cdots C_{k(t),[k-1](t)}\Big).
\end{aligned} \tag{5.24}
$$

Aplicando o operador (5.24) ao produto $\Big(|\overline{\psi}\rangle_{GHZ}\otimes|0^{\otimes k}\rangle_{(t+1)}\Big)$, obtém-se

$$
\begin{aligned}
|\overline{0}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \\
&\quad \otimes\ldots\otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \otimes\Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{1}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \mp |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \\
&\quad \otimes\ldots\otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \mp |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \otimes \Big(|\ldots 0_a\ldots 1_k\rangle\Big)_{(t+1)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle + |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(0)} \\
&\quad \otimes\ldots\otimes\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle + |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \otimes \Big(|\ldots 1_a\ldots 0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle - |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(0)} \\
&\quad \otimes\ldots\otimes\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle - |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \otimes \Big(|\ldots 1_a\ldots 1_k\rangle\Big)_{(t+1)}\Big]. \qquad (5.25)
\end{aligned}
$$

Note em (5.25) que, pela aplicação do operador (5.24), o bloco de índice (t) passou da base GHZ para a base computacional. Depois disso, este bloco intacto foi identicamente preparado no bloco de índice $(t+1)$ e então teve seus k qubits transformados para o estado $|0\rangle$. Enfatiza-se também que os blocos de índices (0) a $(t-1)$ não sofreram nenhuma alteração depois da aplicação de U_{dec}, dado em (5.24).

Caso 2: Considera-se que em $|\overline{\psi}\rangle_{GHZ}$ existem $t+1$ blocos intactos, significando que nenhum apagamento foi detectado.

Desde que U_{dec} é somente aplicado aos blocos intactos, pode-se explicitamente denotá-lo como segue:

$$
U_{dec} = \prod_{d=0}^{t}\left(\prod_{i=1}^{k} C_{i(t+1),i(d)}\right)\cdot\prod_{d=0}^{t}\left(\prod_{i=1}^{k} C_{i(d),i(t+1)} H_{k(d)} \prod_{i=1}^{k-1} C_{k(d),i(d)}\right)
$$

$$
\begin{aligned}
= \quad & \Big[\Big(C_{1(t+1),1(0)}\cdots C_{k(t+1),k(0)}\Big)\cdots\Big(C_{1(t+1),1(t)}\cdots C_{k(t+1),k(t)}\Big)\Big] \\
& \Big[\Big(C_{1(0),1(t+1)}\cdots C_{k(0),k(t+1)}\Big)H_{k(0)}\Big(C_{k(0),1(0)}\cdots C_{k(0),[k-1](0)}\Big)\cdots \\
& \Big(C_{1(t),1(t+1)}\cdots C_{k(t),k(t+1)}\Big)H_{k(t)}\Big(C_{k(t),1(t)}\cdots C_{k(t),[k-1](t)}\Big)\Big]. \qquad (5.26)
\end{aligned}
$$

Agora, aplicando o operador (5.26) ao produto $\Big(|\overline{\psi}\rangle_{GHZ}\otimes|0^{\otimes k}\rangle_{(t+1)}\Big)$, obtém-se

$$
\begin{aligned}
|\overline{0}\rangle_L &= \Big[\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(0)}\otimes\ldots\otimes\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{1}\rangle_L &= \Big[\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(0)}\otimes\ldots\otimes\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|0_1\ldots0_{k-1}1_k\rangle\Big)_{(t+1)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(0)}\otimes\ldots\otimes\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|1_1\ldots1_{k-1}0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(0)}\otimes\ldots\otimes\Big(|0_1\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|1_1\ldots1_{k-1}1_k\rangle\Big)_{(t+1)}\Big]. \qquad (5.27)
\end{aligned}
$$

Nota-se em (5.27) que, após a aplicação do operador (5.26), todos os blocos de índices (0) a (t) passaram da base GHZ para a base computacional. Em seguida esses blocos foram identicamente preparados no bloco de índice $(t+1)$ e depois tiveram os seus k qubits transformados para o estado $|0\rangle$.

Conclui-se com isso a demonstração do Lema 5.3.

□

Depois de aplicar o operador U_{dec} (Lema 5.3) a $\Big(|\overline{\psi}\rangle_{GHZ}\otimes|0^{\otimes k}\rangle_{(t+1)}\Big)$, torna-se necessário aplicar o(s) operador(es) de recuperação, um operador para cada bloco em que foi detectado apagamento, a fim de se obter o estado $|\psi\rangle$ livre de apagamentos.

Seja $B \subset D$ ($D = \{0,\ldots,t\}$) o conjunto dos índices que identificam os blocos em que ocorreram apagamentos. Na aplicação do operador de recuperação, deve-se considerar dois casos para o qubit que sofreu apagamento no bloco de índice $(b) \in B$:

1. Quanto a posição é diferente de k.

2. Quando a posição é igual a k.

O lema a seguir apresentará como deve ser a forma do operador de recuperação para o Caso **1**.

Lema 5.4. *Seja $B \subset D(D = \{0, \ldots, t\})$ o conjunto dos índices que identificam os blocos em que ocorreram apagamentos e considere também que tenha sido aplicado o operador U_{dec} a $\left(|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)}\right)$. Se a posição do qubit é diferente de k, para o qubit na posição a onde ocorreu apagamento no bloco de índice $(b) \in B$, então o operador de recuperação $U_{rec}^{a,b}$, que irá transformar o bloco de índice (b) de tal maneira que ele fique da mesma forma para todos os estado lógicos, é dado por*

$$\begin{aligned} U_{rec}^{a,b} &= T_{[k-r](t+1),k(t+1),r(b)} Z_{k(t+1),r(b)}\, T_{[k-r](t+1),k(t+1),r(b)} \\ &\prod_{i=1(i\neq a)}^{k-1} C_{i(t+1),i(b)} \prod_{i=1(i\neq a)}^{k} C_{[k-r](t+1),i(b)}, \end{aligned} \tag{5.28}$$

em que $r = \max_{r\neq k}(\mathcal{W})$ e $\mathcal{W} = \{1, \ldots, k\} \setminus \{a\}$, com T representando uma operação de porta Toffoli [2] *e Z representando uma operação σ_Z de Pauli controlada* [3].

Demonstração: Mostra-se que considerando $|\overline{\psi}\rangle_{GHZ}$, um estado que tem $(t+1)$ blocos de k-qubits cada ($k \geq 3$) na base GHZ, que tenha sofrido $t = \lfloor k/2 \rfloor$ apagamentos em blocos diferentes depois de passar através do QEC, então a operação de restauração, dada por (5.28), irá transformar o bloco de índice (b) que sofreu apagamento em uma posição diferente de k de tal maneira que ele fique da mesma forma para todos os estado lógicos.

O estado $|\overline{\psi}\rangle_{GHZ}$ contém $(t+1)$ blocos e tem t apagamentos em diferentes blocos. Desde que existam $(t+1)$ blocos, os apagamentos podem ter ocorrido em qualquer um dos blocos de índices (0) a (t). Entretanto, sem perda de generalidade, considera-se que os apagamentos ocorreram em qualquer posição a ($a \neq k$) dos blocos de índices (0) até $(t-1)$, i.e., $B = \{0, \ldots, t-1\}$. Assim, considerando que já tenha sido aplicado U_{dec} a $\left(|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)}\right)$, o estado $|\overline{\psi}\rangle_{GHZ}$ é reescrito como segue:

$$|e_0\rangle \otimes |\psi\rangle_{GHZ} \rightarrow |\overline{\psi}\rangle_{GHZ} = \lambda_0|\overline{0}\rangle_L + \lambda_1|\overline{1}\rangle_L + \ldots + \lambda_{2^k-2}|\overline{2^k-2}\rangle_L + \lambda_{2^k-1}|\overline{2^k-1}\rangle_L, \tag{5.29}$$

em que

[2] Para mais detalhes sobre a porta Toffoli ver Apêndice B.3.5.

[3] A operação σ_Z de Pauli controlada $Z_{x,y}$ tem o bit de controle x e o bit alvo y, o qual envia o estado do bit alvo $|0\rangle \rightarrow |0\rangle$ e $|1\rangle \rightarrow -|1\rangle$ quando o bit de controle está no estado $|1\rangle$; caso contrário, quando o bit de controle está em $|0\rangle$, o estado do bit alvo não mudará.

$$
\begin{aligned}
|\overline{0}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{1}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \mp |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \mp |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 0_a\ldots 1_k\rangle\Big)_{(t+1)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle + |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle + |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 1_a\ldots 0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle - |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(\pm|\ldots\overline{1}_a\ldots 0_k\rangle - |\ldots\overline{0}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 1_a\ldots 1_k\rangle\Big)_{(t+1)}\Big]. \qquad (5.30)
\end{aligned}
$$

Considerando que o apagamento ocorreu no qubit de posição a $(1 \leq a \leq k-1)$ dos blocos de índices (0) a $(t-1)$, então $\mathcal{W} = \{1,\ldots,k\} \setminus \{a\}$ e $r = max_{r\neq k}(\mathcal{W})$. Os operadores de recuperação, um operador para cada bloco de índice (0) até $(t-1)$, são explicitamente dados como segue:

$$
\begin{aligned}
U_{rec}^{a,0} &= T_{[k-r](t+1),k(t+1),r(0)} Z_{k(t+1),r(0)}\, T_{[k-r](t+1),k(t+1),r(0)} \\
&\quad \prod_{i=1(i\neq a)}^{k-1} C_{i(t+1),i(0)} \prod_{i=1(i\neq a)}^{k} C_{[k-r](t+1),i(0)}, \\
&\vdots \\
U_{rec}^{a,t-1} &= T_{[k-r](t+1),k(t+1),r(t-1)} Z_{k(t+1),r(t-1)}\, T_{[k-r](t+1),k(t+1),r(t-1)} \\
&\quad \prod_{i=1(i\neq a)}^{k-1} C_{i(t+1),i(t-1)} \prod_{i=1(i\neq a)}^{k} C_{[k-r](t+1),i(t-1)}. \qquad (5.31)
\end{aligned}
$$

Tendo que U_{dec} tenha sido aplicado a $\Big(|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)}\Big)$, então aplicando os operadores de recuperação, dados por (5.31) em (5.29), obtém-se

$$\begin{aligned}
|\overline{0}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{1}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 0_a\ldots 1_k\rangle\Big)_{(t+1)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 1_a\ldots 0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots\overline{0}_a\ldots 0_k\rangle \pm |\ldots\overline{1}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 1_a\ldots 1_k\rangle\Big)_{(t+1)}\Big]. \qquad (5.32)
\end{aligned}$$

Observe agora em (5.32) que os blocos de índices (0) até $(t-1)$ estão da mesma maneira para todos os estados lógicos. Com isso, o sistema e o ambiente estarão no estado

$$\begin{aligned}
&\Big(|\ldots\overline{x}_a\ldots 0_k\rangle \pm |\ldots\overline{x}_a\ldots 1_k\rangle\Big)_{(0)} \otimes \Big(|\ldots\overline{x}_a\ldots 0_k\rangle \pm |\ldots\overline{x}_a\ldots 1_k\rangle\Big)_{(1)} \\
&\otimes\ldots\otimes\Big(|\ldots\overline{x}_a\ldots 0_k\rangle \pm |\ldots\overline{x}_a\ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a\ldots 0_k\rangle\Big)_{(t)} \\
&\otimes\Big(|\psi\rangle\Big)_{(t+1)}, \qquad (5.33)
\end{aligned}$$

em que $\overline{x}_a \in \{0,1\}$.

Portanto, o estado original da mensagem $|\psi\rangle$ pode ser recuperado por intermédio do bloco de índice $(t+1)$ mesmo depois de passar pelo QEC e ter sofrido apagamento no qubit de posição $\{a\}$ $(a \neq k)$ dos blocos de índices (0) até $(t-1)$.

□

Depois da prova do Lema 5.4 para o Caso 1, agora será considerado o Caso 2 o qual é tratado pelo lema a seguir.

Lema 5.5. *Considere $B \subset D$ $(D = \{0, \ldots, t\})$ o conjunto dos índices que identificam os blocos em que ocorreram apagamentos e também que tenha sido aplicado o operador U_{dec} a $\Big(|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)}\Big)$. Se a posição for igual a k, para o qubit que sofreu apagamento no bloco de índice $(b) \in B$, então o operador $U_{rec}^{k,b}$ que irá transformar o bloco de índice (b) de tal maneira que ele fique da mesma forma para todos os estado lógicos é dado por*

$$U_{rec}^{k,b} = Z_{k(t+1),k-1(b)} \prod_{i=1}^{k-1} C_{i(t+1),i(b)}, \tag{5.34}$$

em que Z representa a operação σ_Z de Pauli controlada.

Demonstração: Tome as considerações para $|\overline{\psi}\rangle_{GHZ}$, t, k e para o número de blocos como sendo as mesmas do Lemma 5.4, exceto que a posição do apagamento é igual a k. Assim, o estado $|\overline{\psi}\rangle_{GHZ}$ para esta situação, considerando que U_{dec} tenha sido aplicada a $\Big(|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)}\Big)$, tem a seguinte forma:

$$|e_0\rangle \otimes |\psi\rangle_{GHZ} \rightarrow |\overline{\psi}\rangle_{GHZ} \;\; = \;\; \lambda_0|\overline{0}\rangle_L + \lambda_1|\overline{1}\rangle_L + \ldots + \lambda_{2^k-2}|\overline{2^k-2}\rangle_L + \lambda_{2^k-1}|\overline{2^k-1}\rangle_L, \tag{5.35}$$

em que

$$\begin{aligned} |\overline{0}\rangle_L \;\; = \;\; & \Big[\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\ & \otimes\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\ & \otimes\Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t+1)}\Big], \end{aligned}$$

$$
\begin{aligned}
|\overline{1}\rangle_L &= \Big[\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \mp |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\otimes\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \mp |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\otimes\Big(|0\ldots0_{k-1}1_k\rangle\Big)_{(t+1)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(\pm|1\ldots1_{k-1}\overline{0}_k\rangle + |0\ldots0_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\otimes\Big(\pm|1\ldots1_{k-1}\overline{0}_k\rangle + |0\ldots0_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\otimes\Big(|1\ldots1_{k-1}0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(\pm|1\ldots1_{k-1}\overline{0}_k\rangle - |0\ldots0_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\otimes\Big(\pm|1\ldots1_{k-1}\overline{0}_k\rangle - |0\ldots0_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\otimes\Big(|1\ldots1_{k-1}1_k\rangle\Big)_{(t+1)}\Big]. \qquad (5.36)
\end{aligned}
$$

Considerando que o apagamento ocorreu no qubit de posição k dos blocos de índices (0) até $(t-1)$, então $\mathcal{W} = \{1,\ldots,k\} \setminus \{k\} = \{1,\ldots,k-1\}$ e $r = max_{r\neq k}(\mathcal{W}) = k-1$. Os operadores de recuperação, um operador para cada bloco de índice (0) até $(t-1)$, são explicitamente dados como segue:

$$
\begin{aligned}
U_{rec}^{k,0} &= Z_{k(t+1),k-1(0)} \prod_{i=1}^{k-1} C_{i(t+1),i(0)}, \\
&\vdots \\
U_{rec}^{k,t-1} &= Z_{k(t+1),k-1(t-1)} \prod_{i=1}^{k-1} C_{i(t+1),i(t-1)}. \qquad (5.37)
\end{aligned}
$$

Aplicando os operadores de recuperação dados por (5.37) em (5.35), obtém-se

$$
\begin{aligned}
|\overline{0}\rangle_L &= \Big[\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\otimes\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\otimes\Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t+1)}\Big],
\end{aligned}
$$

$$
\begin{aligned}
|\overline{1}\rangle_L &= \Big[\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|0\ldots0_{k-1}1_k\rangle\Big)_{(t+1)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|1\ldots1_{k-1}0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|1\ldots1_{k-1}1_k\rangle\Big)_{(t+1)}\Big]. \qquad (5.38)
\end{aligned}
$$

Note agora em (5.38) que os blocos de índices (0) até $(t-1)$ estão da mesma maneira para todos os estados lógicos. Deste modo, o sistema e o ambiente estarão no estado

$$
\begin{aligned}
&\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(0)} \otimes \Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(1)} \\
&\otimes\ldots\otimes\Big(|0\ldots0_{k-1}\overline{0}_k\rangle \pm |1\ldots1_{k-1}\overline{1}_k\rangle\Big)_{(t-1)} \otimes \Big(|0\ldots0_{k-1}0_k\rangle\Big)_{(t)} \\
&\otimes\Big(|\psi\rangle\Big)_{(t+1)}. \qquad (5.39)
\end{aligned}
$$

Portanto, o estado original da mensagem $|\psi\rangle$ pode ser recuperado via o bloco de índice $(t+1)$, mesmo depois de passar pelo QEC e ter sofrido apagamento no qubit de posição k nos blocos de índices (0) até $(t-1)$.

□

Considere que o estado $|\psi\rangle_{GHZ}$ ao passar pelo QEC tenha sofrido $t = \lfloor k/2 \rfloor$ apagamentos (em blocos distintos), resultando em $|\overline{\psi}\rangle_{GHZ}$. O teorema a seguir mostra como deve ser a operação de restauração capaz de obter o estado que foi codificado livre de apagamento.

Teorema 5.2. *Sejam $|\overline{\psi}\rangle_{GHZ}$, um estado que possui $t+1$ blocos redundantes de k-qubits cada ($k \geq 3$) na base GHZ tendo sofrido $t = \lfloor k/2 \rfloor$ apagamentos ao passar pelo QEC, e $B \subset D$ ($D = \{0,\ldots,t\}$) o conjunto dos índices que identificam os blocos em que foram detectados*

apagamentos, então a operação de restauração $\mathcal{R}$, capaz de obter o estado que foi codificado livre de apagamentos, é dada por

$$\mathcal{R} \;=\; \prod_{b}\left\{U_{rec}^{a,b}\circ\left[U_{dec}\Big(|\overline{\psi}\rangle_{GHZ}\otimes|0^{\otimes k}\rangle_{(t+1)}\Big)\right]\right\}, \tag{5.40}$$

em que $a \in \{1,\ldots,k\}$ é a posição do qubit que sofreu apagamento e $b \in B$, sendo U_{dec} como em (5.21) e $U_{rec}^{a,b}$ como em (5.28) ou como em (5.34), exceto para $U_{rec}^{0} = I$ quando $|B| = 0$ (em que I é a matriz identidade de ordem k).

Demonstração: Mostra-se que a partir de $|\overline{\psi}\rangle_{GHZ}$, um estado que possui $t+1$ blocos redundantes de k-qubits cada ($k \geq 3$) na base GHZ, que sofreu $t = \lfloor k/2 \rfloor$ apagamentos ao passar pelo QEC, então a operação de restauração, dada pela expressão (5.40), é capaz de recuperar o estado que foi codificado livre de apagamentos.

A demonstração deve considerar tanto os casos que envolvem o operador de decodificação (ver Lema 5.3), quanto os casos para o operador de recuperação (ver Lemas 5.4 e 5.5), ou seja:

- todos os blocos permanecem intactos (nenhum apagamento ocorreu);
- apenas um bloco permanece intacto (t apagamentos ocorreram);
- a posição é diferente da última (k-ésima posição) para o qubit que sofreu apagamento;
- a posição é igual a k para o qubit que sofreu apagamento.

Para o primeiro caso listado, a prova é dada no Lema 5.3. Para provar o outros três casos a seguinte situação irá ser apresentada.

Considere que o estado $|\overline{\psi}\rangle_{GHZ}$ contenha $(t+1)$ blocos e tenha sofrido $t = \lfloor k/2 \rfloor$ apagamentos, todos em blocos diferentes, depois de passar através do QEC. Desde que existem $(t+1)$ blocos, então haverá um bloco em que não foi detectado apagamento. Esse bloco pode ser qualquer um dos $(t+1)$ blocos, incluindo os blocos de índices (0) e (t). Entretanto, sem perda de generalidade, será estabelecido que o bloco intacto seja o bloco de índice (t). Devido a isso, os apagamentos irão ocorrer numa posição qualquer $\{a\}$ dos blocos de índices (0) a $(t-1)$.

Visando envolver os casos de aplicação do operador de recuperação, dados pelos Lemas 5.4 e 5.5, considera-se que a posição do qubit que sofreu apagamento seja a k-ésima no bloco de índice (0) e diferente da k-ésima nos blocos de índices (1) a $(t-1)$. O estado $|\overline{\psi}\rangle_{GHZ}$ para esta situação tem a seguinte forma:

$$|e_0\rangle \otimes |\psi\rangle_{GHZ} \rightarrow |\overline{\psi}\rangle_{GHZ} = \lambda_0|\overline{0}\rangle_L + \lambda_1|\overline{1}\rangle_L + \ldots + \lambda_{2^k-2}|\overline{2^k-2}\rangle_L + \lambda_{2^k-1}|\overline{2^k-1}\rangle_L, \tag{5.41}$$

em que

$$\begin{aligned}
|\overline{0}\rangle_L &= \Big[\Big(|\ldots 0_a \ldots \overline{0}_k\rangle \pm |\ldots 1_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots \overline{0}_a \ldots 0_k\rangle \pm |\ldots \overline{1}_a \ldots 1_k\rangle\Big)_{(t-1)} \otimes \\
&\quad \otimes\Big(|\ldots 0_a \ldots 0_k\rangle + |\ldots 1_a \ldots 1_k\rangle\Big)_{(t)}\Big], \\
|\overline{1}\rangle_L &= \Big[\Big(|\ldots 0_a \ldots \overline{0}_k\rangle \mp |\ldots 1_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots \overline{0}_a \ldots 0_k\rangle \mp |\ldots \overline{1}_a \ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \otimes\Big(|\ldots 0_a \ldots 0_k\rangle - |\ldots 1_a \ldots 1_k\rangle\Big)_{(t)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(|\ldots 1_a \ldots \overline{0}_k\rangle \pm |\ldots 0_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(\pm|\ldots \overline{1}_a \ldots 0_k\rangle + |\ldots \overline{0}_a \ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \otimes\Big(|\ldots 1_a \ldots 0_k\rangle + |\ldots 0_a \ldots 1_k\rangle\Big)_{(t)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(|\ldots 1_a \ldots \overline{0}_k\rangle \mp |\ldots 0_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(\pm|\ldots \overline{1}_a \ldots 0_k\rangle - |\ldots \overline{0}_a \ldots 1_k\rangle\Big)_{(t-1)} \\
&\quad \otimes\Big(|\ldots 1_a \ldots 0_k\rangle - |\ldots 0_a \ldots 1_k\rangle\Big)_{(t)}\Big].
\end{aligned} \tag{5.42}$$

A operação de restauração é, portanto, dada com segue:

$$\begin{aligned}
\mathcal{R} &= \left\{U_{rec}^{k,0} \circ U_{dec}\Big(|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)}\Big)\right\} \\
&\quad \left\{\prod_{b=1}^{t-1}\left[U_{rec}^{a,b} \circ U_{dec}\Big(|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)}\Big)\right]\right\}.
\end{aligned} \tag{5.43}$$

O primeiro passo na operação dada em (5.43) é a aplicação de U_{dec}, a qual somente agirá no bloco de índice (t).

Aplicando U_{dec} ao produto $\Big(|\overline{\psi}\rangle_{GHZ} \otimes |0^{\otimes k}\rangle_{(t+1)}\Big)$, obtém-se

$$
\begin{aligned}
|\overline{0}\rangle_L &= \Big[\Big(|\ldots 0_a \ldots \overline{0}_k\rangle \pm |\ldots 1_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots \overline{0}_a \ldots 0_k\rangle \pm |\ldots \overline{1}_a \ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 0_a \ldots 0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{1}\rangle_L &= \Big[\Big(|\ldots 0_a \ldots \overline{0}_k\rangle \mp |\ldots 1_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(|\ldots \overline{0}_a \ldots 0_k\rangle \mp |\ldots \overline{1}_a \ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 0_a \ldots 1_k\rangle\Big)_{(t+1)}\Big], \\
&\vdots \\
|\overline{2^k-2}\rangle_L &= \Big[\Big(|\ldots 1_a \ldots \overline{0}_k\rangle \pm |\ldots 0_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(\pm|\ldots \overline{1}_a \ldots 0_k\rangle + |\ldots \overline{0}_a \ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 1_a \ldots 0_k\rangle\Big)_{(t+1)}\Big], \\
|\overline{2^k-1}\rangle_L &= \Big[\Big(|\ldots 1_a \ldots \overline{0}_k\rangle \mp |\ldots 0_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
&\quad \otimes\Big(\pm|\ldots \overline{1}_a \ldots 0_k\rangle - |\ldots \overline{0}_a \ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle\Big)_{(t)} \\
&\quad \otimes\Big(|\ldots 1_a \ldots 1_k\rangle\Big)_{(t+1)}\Big]. \qquad (5.44)
\end{aligned}
$$

Note que depois da aplicação de U_{dec}: (a) o bloco de índice (t) foi transformado da base GHZ para a base computacional; (b) ele foi identicamente preparado no bloco de índice $(t+1)$; e (c) ele teve todos os seus qubits transformados no estado $|0\rangle$. Observe também que não houve nenhuma mudança nos blocos de índices (0) até $(t-1)$.

O próximo passo na operação dada em (5.43) é a aplicação dos operadores de recuperação, um para cada bloco no qual os apagamentos foram detectados.

Para o bloco de índice (0), em que o qubit de posição k sofreu apagamento, o operador de recuperação é dado pelo Lema 5.5. Considerando que neste caso $\mathcal{W} = \{1, \ldots, k\} \setminus \{k\}$ e, portanto, $r = k-1$, então o operador de recuperação tem a seguinte forma:

$$\begin{aligned} U_{rec}^{k,0} &= Z_{k(t+1),[k-1](0)} \prod_{i=1}^{k-1} C_{i(t+1),i(0)}; \\ &= Z_{k(t+1),[k-1](0)} \Big(C_{1(t+1),1(0)} \cdots C_{[k-1](t+1),[k-1](0)} \Big). \end{aligned} \tag{5.45}$$

Para o caso em que o apagamento ocorreu em um qubit de posição a ($1 \leq a \leq k-1$) dos blocos de índices (1) até $(t-1)$, o operador de recuperação é dado pelo Lema 5.4. Para este caso, $\mathcal{W} = \{1, \ldots, k\} \setminus \{a\}$ e $r = \max_{r \neq k}(\mathcal{W})$. Os operadores de recuperação, um operador para cada bloco de índices (1) até $(t-1)$, são explicitamente dados como segue:

$$\begin{aligned} U_{rec}^{a,1} &= T_{[k-r](t+1),k(t+1),r(1)} Z_{k(t+1),r(1)} \, T_{[k-r](t+1),k(t+1),r(1)} \\ &\quad \prod_{i=1(i\neq a)}^{k-1} C_{i(t+1),i(1)} \prod_{i=1(i\neq a)}^{k} C_{[k-r](t+1),i(1)}, \\ &\vdots \\ U_{rec}^{a,t-1} &= T_{[k-r](t+1),k(t+1),r(t-1)} Z_{k(t+1),r(t-1)} \, T_{[k-r](t+1),k(t+1),r(t-1)} \\ &\quad \prod_{i=1(i\neq a)}^{k-1} C_{i(t+1),i(t-1)} \prod_{i=1(i\neq a)}^{k} C_{[k-r](t+1),i(t-1)}. \end{aligned} \tag{5.46}$$

Aplicando os operadores de recuperação, dados por (5.45) e (5.46) em (5.44), obtém-se

$$\begin{aligned} |\overline{0}\rangle_L &= \Big[\Big(|\ldots 0_a \ldots \overline{0}_k\rangle \pm |\ldots 1_a \ldots \overline{1}_k\rangle \Big)_{(0)} \otimes \ldots \\ &\quad \otimes \Big(|\ldots \overline{0}_a \ldots 0_k\rangle \pm |\ldots \overline{1}_a \ldots 1_k\rangle \Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle \Big)_{(t)} \\ &\quad \otimes \Big(|\ldots 0_a \ldots 0_k\rangle \Big)_{(t+1)} \Big], \\ |\overline{1}\rangle_L &= \Big[\Big(|\ldots 0_a \ldots \overline{0}_k\rangle \pm |\ldots 1_a \ldots \overline{1}_k\rangle \Big)_{(0)} \otimes \ldots \\ &\quad \otimes \Big(|\ldots \overline{0}_a \ldots 0_k\rangle \pm |\ldots \overline{1}_a \ldots 1_k\rangle \Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle \Big)_{(t)} \\ &\quad \otimes \Big(|\ldots 0_a \ldots 1_k\rangle \Big)_{(t+1)} \Big], \\ &\vdots \\ |\overline{2^k - 2}\rangle_L &= \Big[\Big(|\ldots 0_a \ldots \overline{0}_k\rangle \pm |\ldots 1_a \ldots \overline{1}_k\rangle \Big)_{(0)} \otimes \ldots \\ &\quad \otimes \Big(|\ldots \overline{0}_a \ldots 0_k\rangle \pm |\ldots \overline{1}_a \ldots 1_k\rangle \Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle \Big)_{(t)} \\ &\quad \otimes \Big(|\ldots 1_a \ldots 0_k\rangle \Big)_{(t+1)} \Big], \end{aligned}$$

$$
\begin{aligned}
|\overline{2^k-1}\rangle_L \;=\; & \Big[\Big(|\ldots 0_a \ldots \overline{0}_k\rangle \pm |\ldots 1_a \ldots \overline{1}_k\rangle\Big)_{(0)} \otimes \ldots \\
& \otimes\Big(|\ldots \overline{0}_a \ldots 0_k\rangle \pm |\ldots \overline{1}_a \ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle\Big)_{(t)} \\
& \otimes\Big(|\ldots 1_a \ldots 1_k\rangle\Big)_{(t+1)}\Big]. \qquad (5.47)
\end{aligned}
$$

Note agora em (5.47) que os blocos de índices (0) até $(t-1)$ estão da mesma maneira para todos os estados lógicos. Deste modo, o sistema e o ambiente estarão no estado

$$
\begin{aligned}
& \Big(|\ldots 0_a \ldots \overline{x}_k\rangle + |\ldots 1_a \ldots \overline{x}_k\rangle\Big)_{(0)} \otimes \Big(|\ldots \overline{x}_a \ldots 0_k\rangle + |\ldots \overline{x}_a \ldots 1_k\rangle\Big)_{(1)} \\
& \otimes \ldots \otimes \Big(|\ldots \overline{x}_a \ldots 0_k\rangle + |\ldots \overline{x}_a \ldots 1_k\rangle\Big)_{(t-1)} \otimes \Big(|\ldots 0_a \ldots 0_k\rangle\Big)_{(t)} \\
& \otimes\Big(|\psi\rangle\Big)_{(t+1)}, \qquad (5.48)
\end{aligned}
$$

em que $\overline{x}_a \in \{0,1\}$.

Portanto, o estado original da mensagem $|\psi\rangle$ pode ser recuperado via o bloco de índice $(t+1)$, mesmo depois de ter passado pelo QEC e ter sofrido a ocorrência de apagamento nos blocos de índices (0) até $(t-1)$.

Conclui-se, portanto, a prova do Teorema 5.2.

□

5.4 Considerações Finais

Neste capítulo foi apresentado um esquema para a proteção de k qubits de informação ($k \geq 3$) contra a ocorrência de $t = \lfloor k/2 \rfloor$ apagamento, desde que tais apagamentos ocorram em blocos codificados distintos de k qubits cada. Este esquema aperfeiçoa o código proposto por Yang *et al.* [42] e faz uso de $(t+1)$ blocos redundantes na base GHZ.

Uma característica especial do esquema apresentado é que nenhum procedimento de medição é requerido, uma vez que a informação sobre os apagamentos é fornecida naturalmente pelo sistema, por exemplo, através de emissão espontânea. Esta informação pode ser capturada por detectores de apagamento e posteriormente tratada via operadores unitários que não causem distúrbio no sistema. Uma outra característica que pode ser notada é que a informação pode somente ser restaurada se existir uma colaboração de todos os blocos que compõem o estado recebido.

A implementação do esquema proposto é perfeitamente plausível, desde que tal esquema é alcançável via operadores unitários os quais consistem de uma composição apropriada de portas quânticas bem conhecidas na literatura (CNOT, Hadamard, Toffoli e σ_z de Pauli controlada).

É importante notar que os operadores que caracterizam a operação de codificação (Teorema 5.1) e operação de restauração (Teorema 5.2) para este esquema podem ser ajustados para construir diferentes CCAQ. Deve-se enfatizar que os códigos construídos via o esquema proposto podem corrigir somente apagamentos quânticos (i.e., alterações nas quais a posição é de alguma forma conhecida). Apesar disso, esses códigos podem ser concatenados com outros códigos como os CCEQ para proteger contra a ocorrência de erros computacionais [12].

Embora a taxa t/N decresça com k,[4] acredita-se que o presente esquema possa ser útil em muitas aplicações como, por exemplo, em armazenamento de informação quântica para computação quântica de pequena escala, processamento da informação e comunicação quânticas. Isto é particularmente enfatizado devido as propostas promissoras de sistemas físicos para computadores quânticos serem baseadas nas pequenas capacidades das tecnologias atuais, tais como: junções de Josephson [35, 89]; pontos quânticos acoplados [90, 91]; átomos neutros em reticulados ópticos [36, 92]; e fósforos dopados em cristais de silício [3, 93].

Um exemplo para ilustrar o esquema proposto aqui será dado no capítulo a seguir.

No próximo capítulo, apresenta-se um esquema de concatenação capaz de proteger a informação contra a ocorrência de erros computacionais e apagamentos quânticos.

[4] Aqui, $t = \lfloor k/2 \rfloor$ é o número de apagamentos, $N = k(\lfloor k/2 \rfloor + 1)$ é o número total de qubits requeridos e $k \geq 3$ é o comprimento da palavra código.

CAPÍTULO 6

Concatenação para Erros Computacionais e Apagamentos Quânticos

Nenhum sistema quântico está totalmente livre de descoerência, devido a inevitável interação entre este sistema e o ambiente no qual ele está inserido. Mas, pequenas quantidades de descoerência podem ser tratadas por meio da aplicação de várias técnicas reunidas sob o nome de *correção de erros quânticos*. Além disso, erros em computadores quânticos podem ser corrigidos utilizando-se recursos tolerantes a falhas para probabilidades de erro inferiores a um limiar crítico que depende do hardware do computador, das fontes de erro e dos protocolos usados para a correção de erros quânticos [3].

Erros computacionais e apagamentos são tipos de alterações que naturalmente podem ocorrer devido a interação entre os sistemas quânticos e seu ambiente. Diante da impossibilidade de ignorar a existência de tais alterações, há trabalhos na literatura que destacam a importância prática do desenvolvimento de códigos que sejam capazes de realizar a proteção contra estes dois tipos de alterações [13, 49].

De uma maneira geral, é possível manipular códigos existentes para construir um novo código adequado para um modelo de erro mais geral. Um dos artifícios que pode ser utilizado para isso é a *concatenação*, a qual possibilita produzir um novo código fazendo uso de outros existentes. A concatenação de códigos é considerado um método básico para a construção de bons códigos corretores de erros. Além disso, muitos dos códigos binários assintoticamente bons são construídos por meio da concatenação [94, 95].

O conceito de códigos concatenados foi inicialmente introduzido em esquemas de correção de erros clássicos por Forney [96]. A concatenação, em particular, pode ser entendida como um método de combinação de dois códigos (um código interno e um código externo) para formar um novo código [97]. No que concerne correção de erros clássicos, Forney realizou extensos estudos sobre códigos concatenados abordando, por exemplo, como escolher os códigos interno e externo e também que valores limites de probabilidade de erro podem ser alcançados.

As primeiras aplicações de códigos concatenados em correção de erros quânticos aparecem em [10, 52]. No cenário quântico, códigos concatenados desempenham um papel chave em computação quântica tolerante a falhas (CQTF) [52–54] e na construção de bons CCEQ's degenerados [50, 51, 97]. Por exemplo, Gottesman [10], ao fazer uso da concatenação em sua tese de doutorado, construiu um novo código pela concatenação do código de cinco qubits com ele próprio. Já o código degenerado de Shor pode ser construído concatenando-se o código de troca de bit com o código de troca de fase, ambos de três qubits [97].

Duan e outros [13] fizeram uso da concatenação combinando múltiplos códigos corretores de erros de amortecimento de amplitude, resultando em um código que simula o canal de apagamento quântico. Eles se basearam numa observação de que, com relação a uma codificação simples, duas utilizações do canal de amortecimento de amplitude (do inglês *amplitude damping channel*) simulam o canal de apagamento quântico.

Embora a concatenação já tenha sido aplicada a vários cenários de codificação quântica, não foi encontrada nenhuma referência na literatura que tenha concatenado um CCEQ com um CCAQ para produzir um código capaz de realizar proteção contra erros computacionais e apagamentos quânticos.

Com o objetivo de superar estas limitações, uma contribuição apresentada neste capítulo é a de mostrar que a concatenação de um CCEQ com um CCAQ, demanda que o código externo seja um CCEQ, enquanto que o código interno deve ser um CCAQ que não realiza medição. Se esta construção for respeitada, o código concatenado resultante protege tanto contra erros computacionais como também contra apagamentos quânticos.

Na seção a seguir é estabelecida a contribuição dada neste capítulo, mostrando o código concatenado apto a proteger a informação contra a ocorrência erros computacionais e apagamentos quânticos. Depois disso, é apresentado um exemplo que ilustra a implementação da concatenação proposta e as considerações finais do capítulo.

6.1 Concatenação de códigos quânticos

A *concatenação serial* (ou simplesmente *concatenação*) consiste de dois códigos, um *código externo* $[[M, k]]$ que codifica k qubits em M qubits (taxa $R_c^{ext} = k/M$), denotado por C^{ext}, e realização dada por $C^{ext} = (E^{ext}, D^{ext})$; e um *código interno* $[[N, M]]$ que codifica M qubits em N qubits (taxa $R_c^{int} = M/N$), denotado por C^{int}, e realização dada por $C^{int} = (E^{int}, D^{int})$, em que E e D representam as operações de codificação e decodificação, respectivamente [98]. Rahn *et al.* [2] mostraram que o mapa de uma concatenação de códigos é dada pela composição dos mapas dos códigos constituintes. A descrição dada por eles será usada para mostrar como dois códigos podem ser concatenados para formar um outro.

Um estado de k qubits lógicos ρ_i é primeiramente codificado usando o código externo C^{ext}, produzindo um estado de M qubits $E^{ext}[\rho_i]$. Cada um desses qubits é então codificado pelo código interno, isto é, usando o mapa $E^{int} \otimes E^{int} \otimes \ldots \otimes E^{int} = (E^{int})^{\otimes M}$ que age

em $E^{ext}[\rho_i]$. Estas sequências de codificações compõem o mapa da codificação do código concatenado:

$$\overline{E} = (E^{int})^{\otimes M} \circ E^{ext}. \tag{6.1}$$

As M seções em $E^{ext}[\rho_i]$ são chamadas de *blocos*, contendo N qubits cada. Depois de enviar através de um canal quântico, um processo ruidoso $\overline{\mathcal{N}}$ age nos MN qubits previamente codificados.

Um esquema de correção de erro simples corrige coerentemente cada um dos blocos do código baseado no código interno, e então corrige o registrador de entrada com base no código externo. Levando isto em conta, o mapa da decodificação para o código concatenado é dado por

$$\overline{D} = D^{ext} \circ (D^{int})^{\otimes M}. \tag{6.2}$$

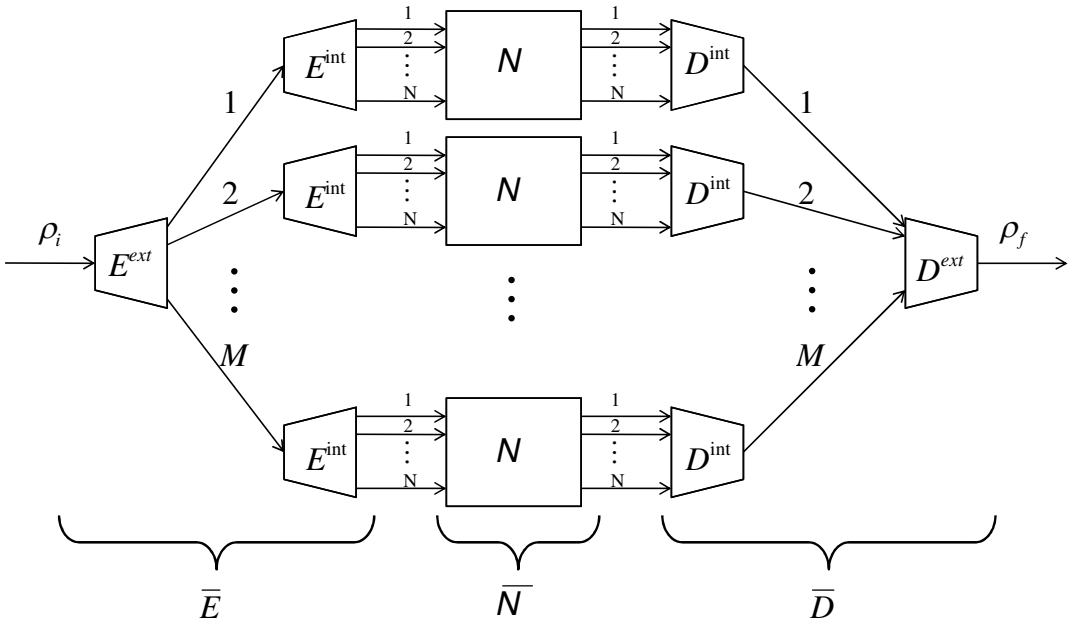

Figura 6.1 Representação do esquema de correção para um código concatenado, adaptado de [2].

Denota-se o código concatenado com este esquema de correção por Q_c, em que

$$Q_c = C^{ext}(C^{int}) = (\overline{E}, \overline{D}). \tag{6.3}$$

Note que $C^{ext}(C^{int})$ é um código de MN-qubits. Este esquema de correção é ilustrado na Figura 6.1.

Para que o mapa de decodificação (6.2) seja realizado no processamento quântico sem que haja o colapso do estado codificado em (6.1) antes da aplicação de D^{ext}, é necessário que no processo de decodificação $(D^{int})^{\otimes M}$ não haja medição.

Considerando que a ocorrência de um apagamento é, por definição (ver Seção 2.3), uma ação que é sinalizada e localizável de alguma forma, então é natural pensar em primeiro corrigir esse tipo de alteração. Depois disso, verifica-se se ocorreram alterações que não são sinalizadas. No contexto proposto neste trabalho, significa que se deve primeiro realizar a decodificação do CCAQ, para depois efetuar a decodificação do CCEQ.

Levando em conta as considerações mencionadas, o teorema a seguir sintetiza a ideia geral do esquema de concatenação proposto (ver Figura 6.2).

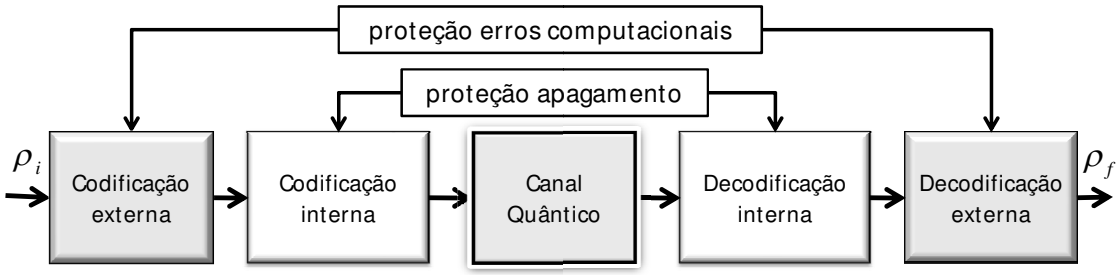

Figura 6.2 Representação do esquema de concatenação para erros computacionais e apagamentos.

Teorema 6.1. *Seja Q_c um esquema como em* (6.3) com C^{int} como um CCAQ (usando múltiplos blocos redundantes e sem realizar medição) capaz de proteger a informação contra até t apagamentos quânticos; e com C^{ext} como um CCEQ capaz de proteger a informação contra até e erros computacionais. Então Q_c é capaz de proteger a informação contra a ocorrência de até e erros computacionais e até t apagamentos quânticos.

Demonstração: Desde que Q_c é como em (6.3), o processo de codificação é dado em (6.1). Considere C^{ext} como sendo um CCEQ. Assumindo que se deseje proteger um estado arbitrário ρ_i, então o resultado do primeiro passo da codificação é dado por $\rho' = E^{ext}[\rho_i]$. Como assumiu-se que C^{int} é um CCAQ, então para completar a codificação aplica-se E^{int} em ρ'. Isso irá resultar em

$$\rho'' = E^{int}[\rho'], \tag{6.4}$$

em que ρ'' possui múltiplos blocos redundantes.

Tendo completado a codificação do Q_c, o estado obtido em (6.4) é enviado através do canal quântico, estando susceptível a ação de um processo ruidoso. Admitindo que ocorreu até t apagamentos quânticos e até e erros computacionais, todos eles em blocos distintos, tem-se como resultado o estado $\hat{\rho}$.

Procedendo agora com a decodificação do Q_c, se for considerado que a decodificação do CCAQ é composta de uma operação unitária com qubits auxiliares e que não realiza medições,

então a decodificação do CCAQ está apta a modificar o estado recebido de tal forma que ele fique livre de apagamentos, como estabelecido por [99]. Com isso, depois da aplicação de D^{int} obtém-se $\rho_d = D^{int}[\hat{\rho}]$, um estado livre de apagamentos o qual preserva o emaranhamento existente.

Agora ρ_d irá ser tratado por D^{ext}, a decodificação do CCEQ. Disso segue que se deve desempenhar um procedimento de detecção, fazendo uso de medição, para verificar se qualquer erro computacional ocorreu e em qual posição [8, 83]. Isto possibilita saber qual deve ser a operação local a ser aplicada para se obter o estado original desejado. Assim, depois da aplicação de D^{ext}, obtém-se

$$\rho_f = D^{ext}[\rho_d]. \tag{6.5}$$

Portanto, se Q_c é um código concatenado no qual C^{int} é um CCAQ (usando qubits auxiliares e que não realiza medição) e C^{ext} é um CCEQ, então Q_c está apto a proteger a informação contra a ocorrência de erros computacionais bem como apagamentos quânticos. Isto conclui a prova deste teorema.

□

Corolário 6.1. *Sendo Q_c é um código concatenado tendo como C^{ext} um CGQ e como C^{int} um CCAQ obtido via esquema apresentado no Capítulo 5, então Q_c é capaz de proteger a informação contra a ocorrência de erros computacionais e apagamentos quânticos, com a restrição que erros e apagamentos ocorram em blocos distintos.*

6.2 Exemplo

Para ilustrar como a informação é protegida pelo esquema de concatenação proposto no Teorema 6.1, apresenta-se um exemplo no qual C^{ext} é o código quântico $[[5, 1, 3]]$ (obtido via um grafo 3-regular) e C^{int} é um CCAQ (proposto no Capítulo 5). Tal código concatenado irá proteger um qubit de informação contra a ocorrência de dois apagamentos quânticos e um erro computacional.

Observando o código $[[5, 1, 3]]$, tem-se que $n = 5$ e $k = 1$. De acordo com [1], as cardinalidades para os conjunto $\mathcal{X}$ e $\mathcal{Y}$ são dadas por $|\mathcal{X}| = 1$ e $|\mathcal{Y}| = 5$, respectivamente. Um grafo representando este código é mostrado na Figura 6.3.

A matriz de adjacência correspondente ao grafo da Figura 6.3 é:

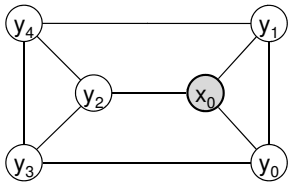

Figura 6.3 Grafo 3-regular para o código $[[5, 1, 3]]$.

$$\Gamma = \left(\begin{array}{c|c} \Gamma_{\mathcal{X},\mathcal{X}} & \Gamma_{\mathcal{X},\mathcal{Y}} \\ \hline \Gamma_{\mathcal{Y},\mathcal{X}} & \Gamma_{\mathcal{Y},\mathcal{Y}} \end{array}\right) = \begin{array}{c} \\ x_0 \\ y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{array} \begin{array}{c} \begin{array}{cccccc} x_0 & y_0 & y_1 & y_2 & y_3 & y_4 \end{array} \\ \left(\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right) \end{array}. \tag{6.6}$$

Considera-se, neste exemplo, o corpo $\mathbb{F}_2 = \{0, 1\}$ e que x_0 rotula o vértice de entrada e y_0, y_1, y_2, y_3, y_4 rotulam os vértices de saída. Com isso, $d^{\mathcal{X}} = (d^{x_0}) \in \mathbb{F}_2$ e $d^{\mathcal{Y}} = (d^{y_0}, d^{y_1}, d^{y_2}, d^{y_3}, d^{y_4}) \in \mathbb{F}_2^5$.

Seguindo a Definição 3.3, o operador de codificação para este grafo é dado como segue (fatores de normalização são omitidos):

$$f(|v\rangle) \;=\; \sum_{d^{x_0}=0}^{1} \left(\sum_{d^{y_0}=0}^{1} \sum_{d^{y_1}=0}^{1} \sum_{d^{y_2}=0}^{1} \sum_{d^{y_3}=0}^{1} \sum_{d^{y_4}=0}^{1} e^{(\pi i)[\gamma]} \left| d^{y_0} d^{y_1} d^{y_2} d^{y_3} d^{y_4} \right\rangle \right) c(d^{x_0}), \tag{6.7}$$

em que $|v\rangle = \sum_{d^{x_0}=0}^{1} c(d^{x_0})|d^{x_0}\rangle = c(0)|0\rangle + c(1)|1\rangle$ e

$$\gamma = \left\{ \frac{1}{2} \left[d^{x_0}, d^{y_0}, d^{y_1}, d^{y_2}, d^{y_3}, d^{y_4} \right]^T \Gamma \begin{bmatrix} d^{x_0} \\ d^{y_1} \\ d^{y_2} \\ d^{y_3} \\ d^{y_4} \end{bmatrix} \right\}. \tag{6.8}$$

Assim, depois da codificação, obtém-se

$$
\begin{aligned}
f(|v\rangle) \rightarrow |\psi\rangle \;=\; & \Big(|00000\rangle + |00001\rangle + |00010\rangle - |00011\rangle \ldots - |11100\rangle - |11101\rangle \\
& -|11110\rangle + |11111\rangle\Big)c(0) \\
& +\Big(|00000\rangle + |00001\rangle + |00010 - |00011\rangle \ldots + |11100\rangle + |11101\rangle \\
& +|11110\rangle - |11111\rangle\Big)c(1). \qquad (6.9)
\end{aligned}
$$

A codificação acima está representando E^{ext} do Q_c e irá proteger um qubit de informação contra a ocorrência de um erro computacional. O próximo passo é a codificação interna E^{int} do Q_c.

Como o estado resultante da codificação E^{ext} é um estado de cinco qubits, então o estado de entrada de E^{int} tem $k = 5$ qubits. Dessa forma, C^{int} irá fazer uso de $t = \lfloor 5/2 \rfloor = 2$ blocos de 5 qubits auxiliares cada, todos inicialmente no estado $|0\rangle$ (Teorema 5.1). A operação de codificação resultante para E^{int} é dada como segue:

$$
|\psi\rangle_{GHZ} = U_{enc}\big(|\psi\rangle_{(0)} \otimes |00000\rangle_{(1)} \otimes |00000\rangle_{(2)}\big), \qquad (6.10)
$$

em que

$$
\begin{aligned}
U_{enc} \;=\; & \prod_{d=0}^{2}\left(\prod_{i=1}^{4} C_{5(d),i(d)}\right)\prod_{d=0}^{2}\left(H_{5(d)}\right)\prod_{d=1}^{2}\left(\prod_{i=1}^{5} C_{i(0),i(d)}\right) \\
= \; & \Big(C_{5(0),1(0)}C_{5(0),2(0)}C_{5(0),3(0)}C_{5(0),4(0)}\Big) \\
& \Big(C_{5(1),1(1)}C_{5(1),2(1)}C_{5(1),3(1)}C_{5(1),4(1)}\Big) \\
& \Big(C_{5(2),1(2)}C_{5(2),2(2)}C_{5(2),3(2)}C_{5(2),4(2)}\Big) \\
& \Big(H_{5(0)}H_{5(1)}H_{5(2)}\Big) \\
& \Big(C_{1(0),1(1)}C_{2(0),2(1)}C_{3(0),3(1)}C_{4(0),4(1)}C_{5(0),5(1)}\Big) \\
& \Big(C_{1(0),1(2)}C_{2(0),2(2)}C_{3(0),3(2)}C_{4(0),4(2)}C_{5(0),5(2)}\Big). \qquad (6.11)
\end{aligned}
$$

com $C_{x,y}$ representando a operação CNOT e H representando a transformada de Hadamard, respectivamente.

Rearranjando o resultado de (6.10), obtém-se (fatores de normalização são omitidos)

$$
\begin{aligned}
|\psi\rangle_{GHZ} \;=\; & \gamma_0|0\rangle_L + \gamma_1|1\rangle_L + \gamma_2|2\rangle_L + \lambda_3|3\rangle_L + \cdots \\
& +\gamma_{28}|28\rangle_L + \gamma_{29}|29\rangle_L + \gamma_{30}|30\rangle_L + \gamma_{31}|31\rangle_L, \qquad (6.12)
\end{aligned}
$$

em que $\gamma_0 = c(0) + c(1)$, $\gamma_1 = c(0) + c(1)$, $\gamma_2 = c(0) + c(1)$, $\gamma_3 = -c(0) - c(1), \ldots,$ $\gamma_{28} = -c(0) + c(1)$, $\gamma_{29} = -c(0) + c(1)$, $\gamma_{30} = -c(0) + c(1)$, $\gamma_{31} = c(0) - c(1)$, e

$$\begin{aligned}
|0\rangle_L &= (|00000\rangle + |11111\rangle)_{(0)} \otimes (|00000\rangle + |11111\rangle)_{(1)} \otimes (|00000\rangle + |11111\rangle)_{(2)}, \\
|1\rangle_L &= (|00000\rangle - |11111\rangle)_{(0)} \otimes (|00000\rangle - |11111\rangle)_{(1)} \otimes (|00000\rangle - |11111\rangle)_{(2)}, \\
|2\rangle_L &= (|00010\rangle + |11101\rangle)_{(0)} \otimes (|00010\rangle + |11101\rangle)_{(1)} \otimes (|00010\rangle + |11101\rangle)_{(2)}, \\
|3\rangle_L &= (|00010\rangle - |11101\rangle)_{(0)} \otimes (|00010\rangle - |11101\rangle)_{(1)} \otimes (|00010\rangle - |11101\rangle)_{(2)}, \\
&\vdots \\
|28\rangle_L &= (|11100\rangle + |00011\rangle)_{(0)} \otimes (|11100\rangle + |00011\rangle)_{(1)} \otimes (|11100\rangle + |00011\rangle)_{(2)}, \\
|29\rangle_L &= (|11100\rangle - |00011\rangle)_{(0)} \otimes (|11100\rangle - |00011\rangle)_{(1)} \otimes (|11100\rangle - |00011\rangle)_{(2)}, \\
|30\rangle_L &= (|11110\rangle + |00001\rangle)_{(0)} \otimes (|11110\rangle + |00001\rangle)_{(1)} \otimes (|11110\rangle + |00001\rangle)_{(2)}, \\
|31\rangle_L &= (|11110\rangle - |00001\rangle)_{(0)} \otimes (|11110\rangle - |00001\rangle)_{(1)} \otimes (|11110\rangle - |00001\rangle)_{(2)}.
\end{aligned} \tag{6.13}$$

Isto completa a codificação $\overline{E}$ do Q_c, dada em (6.1).

Considera-se agora a situação na qual o estado codificado $|\psi\rangle_{GHZ}$ sofre a ação do ambiente que causa, por exemplo, apagamento no qubit 1 (troca de fase) do bloco de índice (0) e no qubit 5 (troca de bit) do bloco de índice (1), bem como um erro computacional no qubit 1 (troca de bit) do bloco de índice (2). Assim, depois dessas alterações o estado resultante será $|e_0\rangle \otimes |\psi\rangle_{GHZ} \rightarrow |\overline{\psi}\rangle_{GHZ}$ (em que $|e_0\rangle$ e o estado inicial do ambiente) como segue:

$$\begin{aligned}
|\overline{\psi}\rangle_{GHZ} &= \lambda_0|\overline{0}\rangle_L + \lambda_1|\overline{1}\rangle_L + \lambda_2|\overline{2}\rangle_L + \lambda_3|\overline{3}\rangle_L + \cdots \\
&\quad + \lambda_{28}|\overline{28}\rangle_L + \lambda_{29}|\overline{29}\rangle_L + \lambda_{30}|\overline{30}\rangle_L + \lambda_{31}|\overline{31}\rangle_L,
\end{aligned} \tag{6.14}$$

em que

$$\begin{aligned}
|\overline{0}\rangle_L &= (|\overline{0}0000\rangle - |\overline{1}1111\rangle)_{(0)} \otimes (|0000\overline{1}\rangle + |1111\overline{0}\rangle)_{(1)} \otimes (|\underline{1}0000\rangle + |\underline{0}1111\rangle)_{(2)}, \\
|\overline{1}\rangle_L &= (|\overline{0}0000\rangle + |\overline{1}1111\rangle)_{(0)} \otimes (|0000\overline{1}\rangle - |1111\overline{0}\rangle)_{(1)} \otimes (|\underline{1}0000\rangle - |\underline{0}1111\rangle)_{(2)}, \\
|\overline{2}\rangle_L &= (|\overline{0}0010\rangle - |\overline{1}1101\rangle)_{(0)} \otimes (|0001\overline{1}\rangle + |1110\overline{0}\rangle)_{(1)} \otimes (|\underline{1}0010\rangle + |\underline{0}1101\rangle)_{(2)},
\end{aligned}$$

$$
\begin{aligned}
|\overline{3}\rangle_L &= (|\overline{0}0010\rangle + |\overline{1}1101\rangle)_{(0)} \otimes (|0001\overline{1}\rangle - |1110\overline{0}\rangle)_{(1)} \otimes (|\underline{1}0010\rangle - |\underline{0}1101\rangle)_{(2)}, \\
&\vdots \\
|\overline{28}\rangle_L &= (-|\overline{1}1100\rangle + |\overline{0}0011\rangle)_{(0)} \otimes (|1110\overline{1}\rangle + |0001\overline{0}\rangle)_{(1)} \otimes (|\underline{0}1100\rangle + |\underline{1}0011\rangle)_{(2)}, \\
|\overline{29}\rangle_L &= (-|\overline{1}1100\rangle - |\overline{0}0011\rangle)_{(0)} \otimes (|1110\overline{1}\rangle - |0001\overline{0}\rangle)_{(1)} \otimes (|\underline{0}1100\rangle - |\underline{1}0011\rangle)_{(2)}, \\
|\overline{30}\rangle_L &= (-|\overline{1}1110\rangle + |\overline{0}0001\rangle)_{(0)} \otimes (|1111\overline{1}\rangle + |0000\overline{0}\rangle)_{(1)} \otimes (|\underline{0}1110\rangle + |\underline{1}0001\rangle)_{(2)}, \\
|\overline{31}\rangle_L &= (-|\overline{1}1110\rangle - |\overline{0}0001\rangle)_{(0)} \otimes (|1111\overline{1}\rangle - |0000\overline{0}\rangle)_{(1)} \otimes (|\underline{0}1110\rangle - |\underline{1}0001\rangle)_{(2)}.
\end{aligned}
\tag{6.15}
$$

Comparando os estado lógicos de (6.15) com aqueles de (6.13), pode-se notar que cada qubit em que ocorreu apagamento (com um traço na parte superior) dos estados lógicos de (6.15), o bloco de índice (2) não foi afetado por apagamento. Este bloco, entretanto, tem um tipo diferente de alteração (erro computacional), i.e., uma troca de bit causada pelo ambiente (indicado por um traço na parte inferior).

De acordo com o Teorema 6.1, deve-se iniciar com a decodificação do código interno D^{int}, para depois realizar a decodificação do código externo D^{ext}.

A decodificação D^{int} do CCAQ é dado por meio da operação de restauração $\mathcal{R}$ (Teorema 5.2), a qual para a presente situação é como segue:

$$
\mathcal{R} = \left[U_{rec}^{5,1} \circ U_{dec}\Big(|\overline{\psi}\rangle_{GHZ} \otimes |00000\rangle_{(3)}\Big)\right]\left[U_{rec}^{1,0} \circ U_{dec}\Big(|\overline{\psi}\rangle_{GHZ} \otimes |00000\rangle_{(3)}\Big)\right]. \tag{6.16}
$$

Primeiramente, desempenha-se o operador U_{dec} em $\big(|\overline{\psi}\rangle_{GHZ} \otimes |00000\rangle_{(3)}\big)$. Relembrando que este operador atua somente em blocos intactos. Depois, aplica-se os operadores de recuperação $U_{rec}^{a,b}$.

Para este caso, o operador U_{dec} é dado como segue:

$$
\begin{aligned}
U_{dec} &= \prod_{d=0(d\notin\{0,1\})}^{2}\left(\prod_{i=1}^{5} C_{i(3),i(d)}\right)\prod_{d=0(d\notin\{0,1\})}^{2}\left(\prod_{i=1}^{5} C_{i(d),i(3)} H_{5(d)} \prod_{i=1}^{4} C_{5(d),i(d)}\right) \\
&= C_{1(3),1(2)}C_{2(3),2(2)}C_{3(3),3(2)}C_{4(3),4(2)}C_{5(3),5(2)}C_{1(2),1(3)}C_{2(2),2(3)}C_{3(2),3(3)}C_{4(2),4(3)} \\
&\quad C_{5(2),5(3)}H_{5(2)}C_{5(2),1(2)}C_{5(2),2(2)}C_{5(2),3(2)}C_{5(2),4(2)}.
\end{aligned}
\tag{6.17}
$$

Desde que os apagamentos ocorreram no qubit de posição 1 do bloco de índice (0) e no qubit de posição 5 do bloco de índice (1), então os operadores de recuperação para esta situação são dados como segue:

$$\begin{aligned} U_{rec}^{1,0} &= T_{1(3),5(3),4(0)} Z_{5(3),4(0)} T_{1(3),5(3),4(0)} \prod_{i=1(i\neq 1)}^{4} C_{i(3),i(0)} \prod_{i=1(i\neq 1)}^{5} C_{1(3),i(0)} \\ &= T_{1(3),5(3),4(0)} Z_{5(3),4(0)} T_{1(3),5(3),4(0)} \\ &\quad C_{2(3),2(0)} C_{3(3),3(0)} C_{4(3),4(0)} C_{1(3),2(0)} C_{1(3),3(0)} C_{1(3),4(0)} C_{1(3),5(0)}, \end{aligned} \tag{6.18}$$

em que T representa uma operação de porta Toffoli, Z representa a operação σ_Z-Pauli controlada e, para este caso, $\mathcal{W}_{(0)} = \{1,2,3,4,5\} \setminus \{1\} = \{2,3,4,5\}$ com $r = max_{r\neq 5}\{\mathcal{W}_{(0)}\} = 4$; e também:

$$\begin{aligned} U_{rec}^{5,1} &= Z_{5(3),4(1)} \prod_{i=1}^{4} C_{i(3),i(1)} \\ &= Z_{5(3),4(1)} C_{1(3),1(1)} C_{2(3),2(1)} C_{3(3),3(1)} C_{4(3),4(1)}, \end{aligned} \tag{6.19}$$

em que $\mathcal{W}_{(1)} = \{1,2,3,4,5\} \setminus \{5\} = \{1,2,3,4\}$ e $r = max_{r\neq 5}\{\mathcal{W}_{(1)}\} = 4$.

Depois de aplicar o operador (6.17) e os operadores (6.18) e (6.19) em (6.15), obtém-se

$$\begin{aligned} |\overline{0}\rangle_L &= (|\overline{0}1111\rangle - |\overline{1}0000\rangle)_{(0)} \otimes (|10000\overline{0}\rangle + |0111\overline{1}\rangle)_{(1)} \otimes |00000\rangle_{(2)} \otimes |\underline{1}0000\rangle_{(3)}, \\ |\overline{1}\rangle_L &= (|\overline{0}1111\rangle - |\overline{1}0000\rangle)_{(0)} \otimes (|10000\overline{0}\rangle + |0111\overline{1}\rangle)_{(1)} \otimes |00000\rangle_{(2)} \otimes |\underline{1}0001\rangle_{(3)}, \\ |\overline{2}\rangle_L &= (|\overline{0}1111\rangle - |\overline{1}0000\rangle)_{(0)} \otimes (|10000\overline{0}\rangle + |0111\overline{1}\rangle)_{(1)} \otimes |00000\rangle_{(2)} \otimes |\underline{1}0010\rangle_{(3)}, \\ |\overline{3}\rangle_L &= (|\overline{0}1111\rangle - |\overline{1}0000\rangle)_{(0)} \otimes (|10000\overline{0}\rangle + |0111\overline{1}\rangle)_{(1)} \otimes |00000\rangle_{(2)} \otimes |\underline{1}0011\rangle_{(3)}, \\ &\vdots \\ |\overline{28}\rangle_L &= (|\overline{0}1111\rangle - |\overline{1}0000\rangle)_{(0)} \otimes (|10000\overline{0}\rangle + |0111\overline{1}\rangle)_{(1)} \otimes |00000\rangle_{(2)} \otimes |\underline{0}1100\rangle_{(3)}, \\ |\overline{29}\rangle_L &= (|\overline{0}1111\rangle - |\overline{1}0000\rangle)_{(0)} \otimes (|10000\overline{0}\rangle + |0111\overline{1}\rangle)_{(1)} \otimes |00000\rangle_{(2)} \otimes |\underline{0}1101\rangle_{(3)}, \\ |\overline{30}\rangle_L &= (|\overline{0}1111\rangle - |\overline{1}0000\rangle)_{(0)} \otimes (|10000\overline{0}\rangle + |0111\overline{1}\rangle)_{(1)} \otimes |00000\rangle_{(2)} \otimes |\underline{0}1110\rangle_{(3)}, \\ |\overline{31}\rangle_L &= (|\overline{0}1111\rangle - |\overline{1}0000\rangle)_{(0)} \otimes (|10000\overline{0}\rangle + |0111\overline{1}\rangle)_{(1)} \otimes |00000\rangle_{(2)} \otimes |\underline{0}1111\rangle_{(3)}. \end{aligned} \tag{6.20}$$

Note que em (6.20), o bloco de índice (0) bem como o bloco de índice (1) agora têm a mesma forma para todos os estados lógicos. O sistema e o ambiente irão estar, portanto, no estado:

$$\Big(|\overline{0}1111\rangle - |\overline{1}0000\rangle\Big)_{(0)} \otimes \Big(|10000\overline{0}\rangle + |0111\overline{1}\rangle\Big)_{(1)} \otimes \Big(\,|00000\rangle\,\Big)_{(2)} \otimes \Big(|\overline{\psi}\rangle\Big)_{(3)}. \tag{6.21}$$

O estado recebido agora está livre de apagamentos. O próximo passo é a decodificação externa D^{ext} a qual será usada para verificar e corrigir a ocorrência de um erro computacional.

Com a finalidade de facilitar a compreensão da próxima etapa será mudada a maneira de representação do estado $|\overline{\psi}\rangle$. Assim, ele será reescrito como segue

$$\begin{aligned} |\overline{\psi}\rangle \;=\; & \Big(|\underline{1}0000\rangle + |\underline{1}0001\rangle + |\underline{1}0010\rangle - |\underline{1}0011\rangle + \cdots - |\underline{0}1100\rangle - |\underline{0}1101\rangle - |\underline{0}1110\rangle \\ & + |\underline{0}1111\rangle\Big)c(0) + \Big(|\underline{1}0000\rangle + |\underline{1}0001\rangle + |\underline{1}0010\rangle - |\underline{1}0011\rangle + \cdots + |\underline{0}1100\rangle \\ & + |\underline{0}1101\rangle + |\underline{0}1110\rangle - |\underline{0}1111\rangle\Big)c(1). \end{aligned} \tag{6.22}$$

O primeiro passo na operação de decodificação para o CGQ, D^{ext}, é o cálculo da síndrome de erro. Para isso, aplica-se o operador de decodificação $\mathcal{T}$ ao estado $|\overline{\psi}\rangle$ (Teorema 4.1). Desde que $\mathcal{T}$ é linear, ele é aplicado a todos os estados da base de $|\overline{\psi}\rangle$, resultando em:

$$\begin{aligned} \mathcal{T}(|\overline{\psi}\rangle) \;=\; & \Big[\mathcal{T}(|\underline{1}0000\rangle) + \mathcal{T}(|\underline{1}0001\rangle) + \mathcal{T}(|\underline{1}0010\rangle) - \mathcal{T}(|\underline{1}0011\rangle) + \ldots \\ & - \mathcal{T}(|\underline{0}1100\rangle) - \mathcal{T}(|\underline{0}1101\rangle) - \mathcal{T}(|\underline{0}1110\rangle) + \mathcal{T}(|\underline{0}1111\rangle)\Big]c(0) \\ & + \Big[\mathcal{T}(|\underline{1}0000\rangle) + \mathcal{T}(|\underline{1}0001\rangle) + \mathcal{T}(|\underline{1}0010\rangle) - \mathcal{T}(|\underline{1}0011\rangle) + \ldots \\ & + \mathcal{T}(|\underline{0}1100\rangle) + \mathcal{T}(|\underline{0}1101\rangle) + \mathcal{T}(|\underline{0}1110\rangle) - \mathcal{T}(|\underline{0}1111\rangle)\Big]c(1). \end{aligned} \tag{6.23}$$

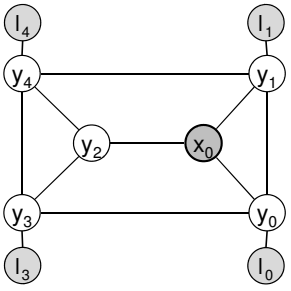

Figura 6.4 O grafo 3-regular para o código [[5,1,3]] com vértices síndromes.

A representação do grafo para a decodificação de $|\overline{\psi}\rangle$ é mostrado na Figura 6.4. Levando em conta este grafo, o operador de decodificação $\mathcal{T}$ a ser aplicado a cada estado da base é como segue (fatores de normalização são omitidos):

$$\mathcal{T}\left(\left|d^{y_0}d^{y_1}d^{y_2}d^{y_3}d^{y_4}\right\rangle\right) = \sum_{d^{l_0}=0}^{1}\sum_{d^{l_1}=0}^{1}\sum_{d^{l_3}=0}^{1}\sum_{d^{l_4}=0}^{1}\sum_{d^{\widehat{x}_0}=0}^{1} e^{-(\pi i)(\theta)}\left|d^{l_0}d^{l_1}d^{l_3}d^{l_4}d^{\widehat{x}_0}\right\rangle, \quad (6.24)$$

em que $\theta = d^{\widehat{x}_0}d^{y_0} + d^{\widehat{x}_0}d^{y_1} + d^{\widehat{x}_0}d^{y_2} + d^{y_0}d^{y_1} + d^{y_0}d^{y_3} + d^{y_1}d^{y_4} + d^{y_2}d^{y_3} + d^{y_2}d^{y_4} + d^{y_3}d^{y_4} + d^{y_0}d^{l_0} + d^{y_1}d^{l_1} + d^{y_3}d^{l_3} + d^{y_4}d^{l_4}$.

O cálculo da expressão (6.24) para cada um dos estados da base de $|\overline{\psi}\rangle$ (6.22), resulta em:

$$\begin{aligned}
\mathcal{T}(|\underline{1}0000\rangle) &= |00000\rangle - |00001\rangle + |00010\rangle - |00011\rangle + |00100\rangle - |00101\rangle \\
&\quad + |00110\rangle - |00111\rangle + |01000\rangle - |01001\rangle + |01010\rangle - |01011\rangle \\
&\quad + |01100\rangle - |01101\rangle + |01110\rangle - |01111\rangle - |10000\rangle + |10001\rangle \\
&\quad - |10010\rangle + |10011\rangle - |10100\rangle + |10101\rangle - |10110\rangle + |10111\rangle \\
&\quad - |11000\rangle + |11001\rangle - |11010\rangle + |11011\rangle - |11100\rangle + |11101\rangle \\
&\quad - |11110\rangle + |11111\rangle\,; \\
\mathcal{T}(|\underline{1}0001\rangle) &= |00000\rangle - |00001\rangle - |00010\rangle + |00011\rangle + |00100\rangle - |00101\rangle \\
&\quad - |00110\rangle + |00111\rangle + |01000\rangle - |01001\rangle - |01010\rangle + |01011\rangle \\
&\quad + |01100\rangle - |01101\rangle - |01110\rangle + |01111\rangle - |10000\rangle + |10001\rangle \\
&\quad + |10010\rangle - |10011\rangle - |10100\rangle + |10101\rangle + |10110\rangle - |10111\rangle \\
&\quad - |11000\rangle + |11001\rangle + |11010\rangle - |11011\rangle - |11100\rangle + |11101\rangle \\
&\quad + |11110\rangle - |11111\rangle\,; \\
\mathcal{T}(|\underline{1}0010\rangle) &= -|00000\rangle + |00001\rangle - |00010\rangle + |00011\rangle + |00100\rangle - |00101\rangle \\
&\quad + |00110\rangle - |00111\rangle - |01000\rangle + |01001\rangle - |01010\rangle + |01011\rangle \\
&\quad + |01100\rangle - |01101\rangle + |01110\rangle - |01111\rangle + |10000\rangle - |10001\rangle \\
&\quad + |10010\rangle - |10011\rangle - |10100\rangle + |10101\rangle - |10110\rangle + |10111\rangle \\
&\quad + |11000\rangle - |11001\rangle + |11010\rangle - |11011\rangle - |11100\rangle + |11101\rangle \\
&\quad - |11110\rangle + |11111\rangle\,;
\end{aligned}$$

$$
\begin{aligned}
\mathcal{T}(|\underline{1}0011\rangle) &= |00000\rangle - |00001\rangle - |00010\rangle + |00011\rangle - |00100\rangle + |00101\rangle \\
&\quad + |00110\rangle - |00111\rangle + |01000\rangle - |01001\rangle - |01010\rangle + |01011\rangle \\
&\quad - |01100\rangle + |01101\rangle + |01110\rangle - |01111\rangle - |10000\rangle + |10001\rangle \\
&\quad + |10010\rangle - |10011\rangle + |10100\rangle - |10101\rangle - |10110\rangle + |10111\rangle \\
&\quad - |11000\rangle + |11001\rangle + |11010\rangle - |11011\rangle + |11100\rangle - |11101\rangle \\
&\quad - |11110\rangle + |11111\rangle ; \\
&\vdots \\
\mathcal{T}(|\underline{0}1100\rangle) &= |00000\rangle + |00001\rangle + |00010\rangle + |00011\rangle + |00100\rangle + |00101\rangle \\
&\quad + |00110\rangle + |00111\rangle - |01000\rangle - |01001\rangle - |01010\rangle - |01011\rangle \\
&\quad - |01100\rangle - |01101\rangle - |01110\rangle - |01111\rangle + |10000\rangle + |10001\rangle \\
&\quad + |10010\rangle + |10011\rangle + |10100\rangle + |10101\rangle + |10110\rangle + |10111\rangle \\
&\quad - |11000\rangle - |11001\rangle - |11010\rangle - |11011\rangle - |11100\rangle - |11101\rangle \\
&\quad - |11110\rangle - |11111\rangle ; \\
\mathcal{T}(|\underline{0}1101\rangle) &= |00000\rangle + |00001\rangle - |00010\rangle + |00011\rangle + |00100\rangle + |00101\rangle \\
&\quad - |00110\rangle - |00111\rangle - |01000\rangle - |01001\rangle + |01010\rangle + |01011\rangle \\
&\quad - |01100\rangle - |01101\rangle + |01110\rangle + |01111\rangle + |10000\rangle + |10001\rangle \\
&\quad - |10010\rangle - |10011\rangle + |10100\rangle + |10101\rangle - |10110\rangle - |10111\rangle \\
&\quad - |11000\rangle - |11001\rangle + |11010\rangle + |11011\rangle - |11100\rangle - |11101\rangle \\
&\quad + |11110\rangle + |11111\rangle ; \\
\mathcal{T}(|\underline{0}1110\rangle) &= - |00000\rangle - |00001\rangle - |00010\rangle - |00011\rangle + |00100\rangle + |00101\rangle \\
&\quad + |00110\rangle + |00111\rangle + |01000\rangle + |01001\rangle + |01010\rangle + |01011\rangle \\
&\quad - |01100\rangle - |01101\rangle - |01110\rangle - |01111\rangle - |10000\rangle - |10001\rangle \\
&\quad - |10010\rangle - |10011\rangle + |10100\rangle + |10101\rangle + |10110\rangle + |10111\rangle \\
&\quad + |11000\rangle + |11001\rangle + |11010\rangle + |11011\rangle - |11100\rangle - |11101\rangle \\
&\quad - |11110\rangle - |11111\rangle ; \\
\mathcal{T}(|\underline{0}1111\rangle) &= |00000\rangle + |00001\rangle - |00010\rangle - |00011\rangle - |00100\rangle - |00101\rangle \\
&\quad + |00110\rangle + |00111\rangle - |01000\rangle - |01001\rangle + |01010\rangle + |01011\rangle \\
&\quad + |01100\rangle + |01101\rangle - |01110\rangle - |01111\rangle + |10000\rangle + |10001\rangle \\
&\quad - |10010\rangle - |10011\rangle - |10100\rangle - |10101\rangle + |10110\rangle + |10111\rangle \\
&\quad - |11000\rangle - |11001\rangle + |11010\rangle + |11011\rangle + |11100\rangle + |11101\rangle \\
&\quad - |11110\rangle - |11111\rangle . \qquad (6.25)
\end{aligned}
$$

A fim de se obter a síndrome de erro, deve-se substituir os resultados de (6.25) na expressão (6.23). Depois disso, tem-se

$$\begin{aligned}\mathcal{T}(|\varphi\rangle) &= |01100\rangle c(0) - |01101\rangle c(1) \\ &= |0110\rangle\,|0\rangle\, c(0) - |0110\rangle\,|1\rangle\, c(1) \\ &= |0\rangle|1\rangle|1\rangle|0\rangle\Big(c(0)|0\rangle - c(1)|1\rangle\Big). \end{aligned} \tag{6.26}$$

De acordo com (6.24), os qubits síndrome para este exemplo correspondem aos quatro primeiros em (6.26). Medindo-os na base computacional, obtém-se a *síndrome de erro*, que neste caso é igual a $\mathbf{0110}$.

O próximo passo é verificar na Tabela de Síndromes (Tabela 6.1) o tipo de erro computacional que a síndrome obtida corresponde e qual deve ser a ação a ser desempenhada no quinto qubit. A síndrome de erro está localizada na Coluna 1 da Tabela. Neste exemplo, pode-se ver que esta síndrome indica que um erro de troca de bit ocorreu no qubit 1; que a forma geral do estado a ser recuperado é $c(0)\,|0\rangle - c(1)\,|1\rangle$ (Coluna 3); e que a correspondente operação de correção local é uma troca de fase no quinto qubit (Coluna 4).

Como último passo, deve-se aplicar a operação de correção local obtida via a Tabela de Síndromes para restaurar o estado originalmente codificado.

Tabela 6.1 Síndromes de erro para um código de 5 qubits via grafo 3-regular

qubits síndromes $q_1q_2q_3q_4$	Erro (*)	Estado do qubit q_5	Operação de correção (*)
0000	Nenhum	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
0001	S_5	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
0010	S_4	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
0011	B_3	$c(0)\|0\rangle - c(1)\|1\rangle$	S_5
0100	S_2	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
0101	B_4	$c(0)\|1\rangle + c(1)\|0\rangle$	B_5
0110	$\mathbf{B_1}$	$\mathbf{c(0)\|0\rangle - c(1)\|1\rangle}$	$\mathbf{S_5}$
0111	BS_4	$-c(0)\|1\rangle - c(1)\|0\rangle$	SBS_5
1000	S_1	$c(0)\|0\rangle + c(1)\|1\rangle$	Nenhuma
1001	B_2	$c(0)\|0\rangle - c(1)\|1\rangle$	S_5
1010	B_5	$c(0)\|1\rangle + c(1)\|0\rangle$	B_5
1011	BS_5	$-c(0)\|1\rangle - c(1)\|0\rangle$	SBS_5
1100	S_3	$c(0)\|1\rangle + c(1)\|0\rangle$	B_5
1101	BS_2	$-c(0)\|0\rangle + c(1)\|1\rangle$	BSB_5
1110	BS_1	$-c(0)\|0\rangle + c(1)\|1\rangle$	BSB_5
1111	BS_3	$-c(0)\|1\rangle + c(1)\|0\rangle$	BS_5

(*) B e S denotam as operações de troca de bit e troca de fase, respectivamente;

O índice subescrito n denota o qubit ao qual a operação se refere.

Este exemplo ilustra as operações de codificação e decodificação do esquema de concatanação proposto no Teorema 6.1. Ele também mostra explicitamente a proteção da informação contra erros de apagamento simultâneos e um erro computacional.

É importante enfatizar, numa visão mais geral, que o código concatenado deste exemplo está apto a proteger a informação contra um erro computacional ou dois apagamentos quânticos que ocorram em qualquer um dos três blocos, ou contra a ocorrência simultânea de dois apagamentos e um erro computacional, desde que o erro computacional ocorra em um bloco intacto, como ilustrado aqui. Pode-se também observar que a implementação deste código é plausível uma vez que ele faz uso de portas quânticas bem conhecidas com CNOT, Hadamard, σ_Z-Pauli, entre outras.

6.3 Considerações Finais

Neste Capítulo foi apresentada a ideia da construção um código concatenado capaz de realizar a proteção da informação contra a ocorrência de erros computacionais e apagamentos quânticos por meio da concatenação de um CCEQ e de um CCAQ (sem operação de medida).

A abordagem apresentada aqui concatena dois códigos para realizar a proteção contra os erros para os quais eles foram originalmente concebidos. Uma vantagem disso é que ela se beneficia dos CCEQ's e CCAQ's que já existem, descrevendo como combiná-los.

O esquema de concatenação proposto foi ilustrado por meio de um exemplo em que, fazendo uso de um código obtido via um grafo 3-regular e um CCAQ obtido como descrito no Capítulo 5, conseguiu-se proteger um qubit de informação contra a ocorrência de dois apagamentos e de um erro computacional.

No próximo capítulo são apresentadas as conclusões deste trabalho.

CAPÍTULO 7

Conclusões e Perspectivas

Neste capítulo são sintetizados os principais resultados obtidos e as sugestões para investigações futuras.

7.1 Principais Conclusões

Considerando-se as condições que um grafo deve satisfazer para que um CGQ possa corrigir um número e de erros, dadas por Schlingemann [33, 85], e a realização de uma adaptação da TFQI, uma das contribuições dadas neste trabalho foi a construção de um operador que possibilita calcular a síndrome de erro para os CGQ's.

Fazendo uso do operador construído para calcular a síndrome de erro, foi apresentado a descrição de uma operação de decodificação para os CGQ's não-degenerados.

Aprimorando o código dado por Yang *et al.* [42], uma outra contribuição apresentada neste trabalho de tese foi o desenvolvimento de um esquema capaz de proteger a informação contra a ocorrência de múltiplos apagamentos quânticos utilizando-se estados GHZ. Este esquema permite proteger k qubits ($k \geq 3$) de informação contra a ocorrência de $t = \lfloor k/2 \rfloor$ apagamentos quânticos, com a restrição de que cada apagamento deve ocorrer em blocos distintos.

Cumprindo o objetivo posto para este trabalho de tese, foi apresentado um esquema de concatenação, o qual possui como código externo um CCEQ e como código interno um CCAQ que não realiza medição, capaz de proteger a informação contra a ocorrência de erros computacionais e, ao mesmo tempo, de apagamentos quânticos.

O esquema de concatenação proposto pode ser especialmente interessante do ponto de vista das aplicações que consideram um modelo de ruído que trate tanto a ocorrência de ruído de despolarização (erro computacional) quanto a ocorrência de perda de fótons (apagamento). Uma vantagem deste esquema é que ele pode ser perfeitamente implementável. Isso porque envolve recursos já conhecidos em Computação e Comunicação Quânticas. Além disso, as variá-

veis usadas neste esquema podem ser modificadas e melhoradas no processo de implementação do mesmo.

Por fim, os resultados obtidos foram ilustrados por meio de um exemplo em que a palavra-código resultante da codificação de um qubit de informação é protegida contra a ocorrência de dois apagamentos e um erro computacional.

Embora tenha sido mostrado aqui que se pode concatenar um CCEQ com um CCAQ para proteger a informação contra a ocorrência de erros computacionais e de apagamentos quânticos, é importante ressaltar que o problema de decodificação quântica geral é NP-difícil, conforme [86].

7.2 Perspectivas para Futuras Pesquisas

O trabalho realizado dá abertura para novas investigações. Lista-se a seguir algumas perspectivas para futuros trabalhos:

- Investigar o uso da transformada de Fourier quântica como recurso para realizar decodificação de outros códigos quânticos, além dos CGQ's;
- Analisar a possibilidade de realizar uma analogia de esquemas de decodificação usados em códigos clássicos para a decodificação de códigos quânticos;
- Verificar a aplicação do esquema proposto para a proteção contra múltiplos apagamentos quânticos em outros cenários do processamento da informação e comunicação quânticas, tais como em compartilhamento de segredo quântico [60, 100] e criptografia quântica [101, 102];
- Realizar a concatenação de outros CCEQ's e CCAQ's existentes na literatura objetivando encontrar uma combinação tal que o código concatenado resultante tenha uma taxa melhor que a combinação ilustrada no exemplo deste trabalho.

Referências Bibliográficas

[1] D. M. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phy. Rev. A*, 65:012308, 2001.

[2] B. Rahn, A. C. Doherty, and H. Mabuchi. Exact performance of concatenated quantum codes. *Phys. Rev. A*, 66:032304, 2002.

[3] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O' Brien. Quantum computers. *Nature*, 464:45–53, 2010.

[4] E. Knill. Quantum computing. *Nature*, 463:441–443, 2010.

[5] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, 1995.

[6] F. Buscemi, G. Chiribella, and G. M. D'Ariano. Quantum erasure of decoherence. *Open Sys. and Information Dyn.*, 14:53–61, 2007.

[7] D. Bouwmeester, A. K. Ekert, and A. Zeilinger. *The Physics of Quantum Information*. Springer-Verlag, 2000.

[8] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[9] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997.

[10] D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.

[11] E. K. Knill and R. Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55:900–911, 1997.

[12] T. M. Stace, S. D. Barrett, and A. C. Doherty. Thresholds for topological codes in the presence of loss. *Phys. Rev. Lett.*, 102:200501, 2009.

[13] R. Duan, M. Grassl, Z. Ji, and B. Zeng. Multi-error-correcting amplitude damping codes. In *Proc. IEEE Inter. Symp. on Inf. Theory (ISIT 2010)*, pages 2672–2676, Austin, Texas, U.S.A., 2010.

[14] F. Gaitan. *Quantum Error Correction and Fault Tolerant Quantum Computing*. CRC Press., 2008.

[15] C. H. Bennett, D. DiVicenzo, J. A. Smolin, and W. K. Wooters. Mixed state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, 1996.

[16] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek. Perfect quantum error correction code. *Phys. Rev. Lett.*, 77:198–201, 1996.

[17] A. R. Calderbank, M. Eric, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. on Inf. Theory*, 44:1369–1387, 1998.

[18] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793–797, 1996.

[19] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.

[20] M. Grassl, Th. Beth, and T. Pellizari. Quantum BCH codes. In *Proc. X Int. Symp. Theoretical Electrical Engineering*, Magdeburg, 1999.

[21] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. on Inf. Theory*, 53:1183–1188, 2007.

[22] M. Grassl, W. Geiselmanni, and T. Beth. Quantum Reed-Solomon codes. In *Proc. of the 13th Int. Symp. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, AAECC-13, pages 231–244, London, UK, 1999. Springer-Verlag.

[23] A. C. A. Almeida and R. Palazzo-Jr. A concatenated [[4,1,3]] quantum convolutional code. In *Proc. IEEE Inf. Theory Workshop*, Santo Antonio, 2004.

[24] G. D. Forney, M. Grassl, and S. Guha. Convolutional and tailbiting quantum error-correcting codes. *IEEE Trans. on Inf. Theory*, 53:865–880, 2007.

[25] M. S. Postol. A proposed quantum low density parity check code. quant-ph/0108131:12, 2001.

[26] H. Lou and J. Garcia-Frias. On the application of error-correcting codes with low-density generator matrix over different quantum channels. In *Proc. Int. Symp. Turbo Codes*, 2006.

[27] P. Tan and J. Li. Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions. *IEEE Trans. on Inf. Theory*, 56:476–491, 2010.

[28] S. A. Aly and A. Klappenecker. Subsystem code constructions. In *Proc. 2008 IEEE Int. Symp. on Inf. Theory*, Toronto, 2008.

[29] D. M. Schlingemann. Stabilizer codes can be realized as graph codes. *Quant. Inf. Comp.*, 2 (4):307–323, 2002.

[30] L. E. Danielsen. On self-dual quantum codes, graphs, and boolean functions. Master's thesis, University of Bergen, Norway, 2005.

[31] Q. Feng. Quantum codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ $(p \geq 3)$ exist. *IEEE Trans. on Inf. Theory*, 48:2384–2391, 2002.

[32] S. Beigi, I. Chuang, M. Grassl, P. Shor, and B. Zeng. Graph concatenation for quantum codes. *J. Math. Phys.*, 52:022201, 2011. (Preprint arXiv:0910.4129 [quant-ph]).

[33] D. M. Schlingemann. Error syndrome calculation for graph codes on a one-way quantum computer: Towards a quantum memory. *Journal of Math. Phys.*, 45:4322–4333, 2004.

[34] C.-Y. Lu, W.-B. Gao, J. Zhang, X.-Q. Zhou, T. Yang, and J.-W. Pan. Experimental quantum coding against qubit loss error. *PNAS*, 105:11050–11054, 2008.

[35] R. Fazio, G. M. Palma, and J. Siewert. Fidelity and leakage of Josephson qubits. *Phys. Rev. Lett.*, 83:5385–5388, 1999.

[36] J. Vala, K. B. Whaley, and D. S. Weiss. Quantum error correction of a qubit loss in an addressable atomic system. *Phys. Rev. A*, 72:052318, 2005.

[37] E. Knill, R. Laflamme, and G. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52, 2001.

[38] W. Wasilewski and K. Banaszek. Protecting an optical qubit against photon loss. *Phys. Rev. A*, 75:042316, 2007.

[39] M. Grassl, Th. Beth, and T. Pellizari. Codes for the quantum erasure channel. *Phys. Rev. A*, 56:33–38, 1997.

[40] F. Caruso and V. Oguri. *Física Moderna: Origens Clássicas e Fundamentos Quânticos*. Elsevier, Rio de Janeiro, 2006. Portuguese.

[41] M. Lassen, M. Sabuncu, A. Huck, J. Niset, G. Leuchs, N. J. Cerf, and U. L. Andersen. Quantum optical coherence can survive photon losses: a continuous-variable quantum erasure correcting code. *Nature Photonics*, 4:700–705, 2010.

[42] C. Yang, S. Chu, and S. Han. A small error-correction code for protecting three-qubit quantum information. *JETP Letters*, 79:236–240, 2004.

[43] D. Greenberger, M. Horne, and A. Zeilinger. Bell's theorem, quantum theory, and conceptions of the universe. pages 69–72. Kluwer Academics, 1989.

[44] G. O. dos Santos, F. M. de Assis, and A. F. de Lima. Um código concatenado para a correção de erro e apagamento quântico. In *27º Simpósio Brasileiro de Telecomunicações (SBrT2009)*, Blumenau-SC, 2009.

[45] G. O. dos Santos, F. M. de Assis, and A. F. de Lima. A scheme of concatenated quantum code to protect against both computational errors and one erasure. Online, 2010. arXiv:cs.IT/1005.3968v2.

[46] A. Broadbent, P.-R. Chouha, and A. Tapp. The GHZ state in secret sharing and entanglement simulation. In *Proc. IEEE Int. Conf. on Quantum, Nano and Micro Technologies*, pages 59–62, 2009.

[47] J. Eisert. Discrete quantum states versus continuous variables. In D. Bruß and G. Leuchs, editors, *Lectures on Quantum Information*, pages 39–52. Wiley-VCH, Weinheim, 2007.

[48] J. Niset, U. L. Andersen, and N. J. Cerf. Experimentally feasible quantum erasure-correcting code for continuous variables. *Phys. Rev. Lett.*, 101:130503, 2008.

[49] C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen. Noise thresholds for optical cluster-state quantum computation. *Phys. Rev. A*, 73:052306, 2006.

[50] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng. Generalized concatenated quantum codes. *Phys. Rev. A*, 79:050306, 2009.

[51] H. Fujita. Several classes of concatenated quantum codes: Constructions and bounds, 2006. quant-ph/0608063v1.

[52] E. Knill and R. Laflamme. Concatenated quantum codes. *Phys. Rev. Lett.*, 102:200501, 1966.

[53] E. Knill, R. Laflamme, and W. Zurek. Threshold accuracy for quantum computation. arXiv:quant-ph/9610011:20, 1996.

[54] C. Zalka. Threshold estimate for fault tolerant quantum computation, 1996. (Preprint arXiv:quant-ph/9612028).

[55] A. L. Vignatti, F. Summa Netto, and L. F. Bittencourt. Uma introdução à computação quântica. 2004. www.dainf.ct.utfpr.edu.br/ vignatti/downloads/tg.pdf.

[56] N. D. Mermin. *Quantum Computer Science: An Introduction*. Cambridge University Press, Cambridge, UK, 2007.

[57] M. W. Coffey and R. Dwiotte. Greenberger-Horne-Zeilinger state for fully connected qubit networks. *Phys. Rev. A*, 80:062302, 2009.

[58] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger. Observation of three-photon Greenberger-Horne-Zeilinger entanglement. *Phys. Rev. Lett.*, 82:1345, 1999.

[59] A. Peres and D. Termo. Quantum information and relativity theory. *Rev. Mod. Phys.*, 76:93–123, 2004.

[60] M. Hillery, V. Buzek, and A. Berthiaume. Quantum secret sharing. *Rev. Mod. Phys.*, 76:93–123, 1999.

[61] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. Briegel, and J.-W. Pan. Experimental demonstration of open-destination quantum teleportation. *Nature*, 430:54–58, 2004.

[62] P. Shor. Fault-tolerant quantum computation. In *Proc. of the 37th Ann. Symp. on Found. of Comp. Sc. (FOCS)*, Los Alamitos, CA, 1996.

[63] E. Knill. Fault-tolerant quantum computation. *Nature*, 434:39–44, 2005.

[64] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle, and D. J. Wineland. Creation of a six-atom 'Schrödinger cat' state. *Nature*, 438:639–642, 2005.

[65] J. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[66] A. Ekert and A. Kay. Requirements for a quantum computer. In D. Bruß and G. Leuchs, editors, *Lectures on Quantum Information*, pages 315–348. Wiley-VCH, Weinheim, 2007.

[67] F. Verstraete, B. Dehaene, and B. De Moor. Normal forms and entanglement measures for multipartite quantum states. *Phys. Rev. A*, 68:012103, 2003.

[68] R. Horodecki, P. Horodecki, P. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, 2009.

[69] W. Dur, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phy. Rev. A*, 62:062314, 2000.

[70] B. Piechocinsha. Information erasure. *Phys. Rev. A*, 61:062314, 2000.

[71] R. Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.*, 5:183, 1961.

[72] H. Mabuchi and P. Zoller. Inversion of quantum jumps in quantum optical systems under continuous observation. *Phys. Rev. Lett.*, 56, 1996.

[73] A. C. A. Almeida. *Códigos Convolucionais Quânticos Concatenados*. PhD thesis, Faculdade de Engenharia Elétrica e Computação, Universidade Estadual de Campinas, Campinas, 2004.

[74] A. Ashikhmin and S. Listsyn. Upper bounds on the size of quantum codes. *IEEE Trans. on Inf. Theory*, 45:1206–1215, 1999.

[75] D. Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation. In *Proceedings of Symposia in Applied Mathematics*, volume 68, pages 13–58, Providence, Rhode Island, 2010. Amer. Math. Soc. arXiv: 0904.2557 [quant-ph].

[76] W. K. Wooters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[77] M. Grassl, A. Klappenecker, and M. Rotteler. Graphs, quadratic forms, and quantum codes. In *Proc. of the 2002 IEEE Int. Symp. on Inf. Theory (ISIT 2002)*, 2002.

[78] W. Tadej and K. Zyczkowski. A concise guide to complex hadamard matrices. *Open Systems & Infor. Dyn.*, 13:133–177, 2006.

[79] J. Seberry and M. Mitrouli. Some remarks on Hadamard matrices. *Cryptogr. Commun.*, 2:293–306, 2010.

[80] P. J. Cameron. Hadamard matrices. On-line, 2006. http://designtheory.org/library/encyc/topics/hab.pdf.

[81] D. M. Schlingemann. *Quantum Information Processing with Graph States*. PhD thesis, Technischen Universität Carolo-Wilhelmina, Braunschweig, 2005.

[82] M. Van den Nest, J. Dehaene, and B. De Moor. Graphical description of the action of local Clifford transformations on graph states. *Phys. Rev. A*, 69:022316, 2004.

[83] Th. Beth and M. Grassl. The Quantum Hamming and Hexacodes. *Fortschr. Phys.*, 46:459–491, 1998.

[84] A. Barg and S. Zhou. A quantum decoding algorithm for the simplex code. In *Proc. of the 36th Annual Allerton Conference on Communication, Control and Computing*, pages 359–365, Monticello, September 1998.

[85] D. M. Schlingemann. Cluster states, algorithms and graphs. *Quant. Inf. Comp.*, 4:287–324, 2004.

[86] M-H. Hsieh and F. Le Gall. NP-hardness of decoding quantum error-correction codes. *Phy. Rev. A*, 83:052331, 2011.

[87] L. Hales and S. Hallgren. An improved quantum Fourier transform algorithm and applications. In *41st Annual Symposium on Foundations of Computer Science*, 2000.

[88] N. J. Cerf and R. Cleve. Information-theoretic interpretation of quantum error-correcting codes. *Phys. Rev. A*, 56:1721–1732, 1997.

[89] X. Zhou and A. Mizel. Quantum manipulation and simulation using josephson junction arrays. *Physica C*, 432:59–64, 2005.

[90] D. Loss and D. P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A*, 57:120–126, 1998.

[91] H. E. Caicedo-Ortiz and S. T. Perez-Merchancano. Exchange energy in coupled quantum dots. *Brazilian J. Phys.*, 36:874–877, 2006.

[92] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch. Quantum logic gates in optical lattices. *Phy. Rev. Lett.*, 82:1060–1063, 1999.

[93] B. E. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393:133–137, 1998.

[94] I. I. Dumer, V. S. Pless, and W. C. Huffman. Concatenated codes and their multilevel generalizations. In *Handbook of Coding Theory*. Elsevier Science, Nova York, 1998.

[95] Z. Li, L. Xing, and X. Wang. A family of asymptotically good quantum codes based on code concatenation. *IEEE Trans. on Inf. Theory*, 55:3821–3824, 2009.

[96] G. D. Forney. *Concatenated Codes*. M.I.T. Press, Cambridge,MA, 1966.

[97] C. Cafaro and S. Mancini. Concatenation of error avoiding with error correcting quantum codes for correlated noise models. *Int. J. Quant. Inf.*, 9:309–330, 2011.

[98] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara. Serial concatenation of interleaved codes: performance analysis, design, and iterative decoding. Technical report, Politecnico di Torino, 1996.

[99] Q.-Y. Cai. Information erasure and recovery in quantum memory. *Chin. Phys. Lett.*, 21:1189–1190, 2004.

[100] Y. Li, K. Zhang, and K. Peng. Multiparty secret sharing of quantum information based on entanglement swapping. *Phys. Lett. A*, 324:420–424, 2004.

[101] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE Int. Conf. Comput., Syst. Signal*, pages 175–179, Bangalore, India, Dec. 1984.

[102] F. Gao, S.-J. Qin, Q.-Y.Wen, and F.-C. Zhu. Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. *Opt. Commun.*, 283(1):192–195, Jan. 2010.

[103] K. Kraus. States, effects, and operations: Fundamental notions of quantum theory. In *Lecture Notes in Physics*, volume 190. Springer, Berlin, 1983.

[104] B. Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54:2614–2628, 1996.

[105] R. Portugal, C. C. Lavor, L. M. Carvalho, and N. Maculan. *Uma Introdução à Computação Quântica*, volume 8 of *Notas em Matemática Aplicada*. SBMAC, São Carlos, SP, 2004.

[106] M. R. Spiegel. Análise de Fourier. In *Coleção Schaum*. McGraw-Hill do Brasil, 1976.

[107] A. V. Oppenheim and A. S. Willsky. *Signals and Systems*. Prentice-Hall, 2nd edition, 1996.

[108] F. L. Marquezino. A transformada de fourier quântica aproximada e sua simulação. Master's thesis, Lab. Nac. de Comp. Científica, Petrópolis-RJ, Março 2006.

[109] C. Lomont. Quantum convolution and quantum correlation algorithms are physically impossible, 2003. (Preprint arXiv:quant-ph/0309070).

[110] I. M. Isaacs. *Character Theory of Finite Groups*. Academic Press, Dover, 1994.

[111] G. James and M. Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 2nd edition, 2001.

[112] T. Gannon. *Moonshine beyond the Monster: The Bridge Connecting Algebra, Modular Forms and Physics*. Cambridge Monographs on Mathematical Physics, 2006.

[113] T. M. Apostol. Introduction to Analytic Number Theory. In *Undergraduate Texts in Mathematics*. Springer-Verlag, 1976.

[114] K.-U. Schmidt. Sequence families with low correlation derived from multiplicative and additive characters, 2010. http://www.sfu.ca/˜ksa39/pub/char_seq.pdf.

[115] J.-P. Serre. *Linear Representations of Finite Groups*. Springer-Verlag, 1977.

[116] R. Lidl, H. Niederreiter, and P. M. Cohn. Finite fields. In G.-C. Rota, editor, *Encyclopedia of Mathematics and its applications*, volume 20. Cambridge University Press, 1997.

[117] E. M. Zmud. Symplectic geometries over finite abelian groups. *Math. USSR Sbornik*, 15(1):7–29, 1971.

APÊNDICE A

Lista de Artigos Produzidos

Segue abaixo a lista de artigos produzidos ao longo deste trabalho de tese.

[1] G. O. dos Santos e F. M. de Assis, "A scheme for protecting multiple quantum erasures", Submetido para a revista *Quantum Information and Computation (Rinton Press)*. Disponível em: arxiv.org/abs/1111.1555.

[2] G. O. dos Santos, F. M. de Assis e A. F. de Lima, "Explicit error syndrome calculation for quantum graph codes," Submetido para a revista *Quantum Information Processing (Springer)*.

[3] G. O. dos Santos e F. M. de Assis, "Protect Information Against Both Computational Errors and Quantum Erasures via Concatenation", Submetido para o *IEEE International Symposium on Information Theory (ISIT'2012)*, Boston-MA, USA.

[4] G. O. dos Santos, F. M. de Assis e A. F. de Lima, "Decodificação para Códigos Grafos Quânticos," in *XXIX Simpósio Brasileiro de Telecomunicações (SBrT2011)*, Curitiba-PR, 2011.

[5] G. O. dos Santos, F. M. de Assis e A. F. de Lima, "A Code for Correcting Quantum Erasures," in *IEEE/SBrT International Telecommunications Symposium (ITS 2010)*, Manaus-AM, Brasil, 2010.

[6] G. O. dos Santos, F. M. de Assis e A. F. de Lima, "Um código concatenado para a correção de erro e apagamento quântico," in *XXVII Simpósio Brasileiro de Telecomunicações (SBrT2009)*, Blumenau-SC, 2009.

APÊNDICE B

Tópicos em Processamento da Informação Quântica

B.1 Notação de Dirac

Notação Bra-ket é uma notação padrão para descrever estados quânticos na teoria da mecânica quântica, principalmente devido à sua praticidade em representar as transformações e estados quânticos, como será visto adiante. O símbolo $\langle\cdot|$ é chamado de *bra* e o símbolo $|\cdot\rangle$ é chamado de *ket*. A notação $\langle\cdot|\cdot\rangle$ é então chamada de *bracket*. A notação foi criada por Paul Dirac, e por isso é também conhecida como notação de Dirac.

Além disso, a notação de Dirac para espaços vetoriais adquire um significado adicional. Um *ket* como $|x\rangle$ denota vetores em coluna e são geralmente usados para descrever estados quânticos. O *bra* $\langle x|$ denota a conjugada[1] transposta de $|x\rangle$, e é denotado por um vetor em linha.

De acordo com a notação de Dirac para espaços vetoriais, $\langle\phi|\psi\rangle$ agora denota o *produto interno* de dois vetores. Por exemplo, sejam $|0\rangle$ e $|1\rangle$ duas bases ortonormais.[2] Como $|0\rangle$ é um vetor unitário, então $\langle 0|0\rangle = 1$ e como $|0\rangle$ e $|1\rangle$ são ortonormais, então $\langle 0|1\rangle = 0$. A notação $|\phi\rangle\langle\psi|$ significa o *produto vetorial* (produto externo) dos dois vetores. Pode-se também expressar $|\phi\rangle\langle\psi|$ em forma de matrizes. Por exemplo, $|0\rangle\langle 1|$ poderia ser escrito em sua forma matricial, onde $|0\rangle = [1,0]^T$, $\langle 0| = [1,0]$, $|1\rangle = [0,1]^T$, $\langle 1| = [0,1]$, então:

$$|0\rangle\langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \tag{B.1}$$

Como visto acima, um ket $|x\rangle$ é uma maneira útil e concisa para descrever as bases (e estados como um todo) de um espaço vetorial.

[1] O complexo conjugado de um número complexo $z = a + bi$ é definido como $z^\dagger = a - bi$. A matriz conjugada da matriz A é a matriz obtida substituindo cada elemento $a_{j,k} \in A$ pelo seu complexo conjugado $a^\dagger_{j,k}$.

[2] Base ortonormal é uma base ortogonal onde os vetores da base são unitários.

B.2 Ruídos e Canais Quânticos

A teoria de informação clássica, a qual lida com o uso ótimo de canais clássicos para transmitir informação clássica, tem sido recentemente estendida para incluir o estudo de canais quânticos e seu uso ótimo, sozinho ou em conjunto com canais clássicos, para comunicação não somente de informação clássica mas também de estados quânticos intactos, e para compartilhar emaranhamento entre observadores separados. Um canal clássico (discreto e sem memória) é geralmente descrito por um conjunto de probabilidades condicionais $P(j \mid i)$, a probabilidade da saída j do canal dada a entrada i do canal. Um canal quântico pode ser descrito [103, 104] por um mapeamento linear completamente positivo e preservando o traço (superoperador) das matrizes densidades do estado de entrada para as matrizes densidades do estado de saída.

Para canais quânticos, confiabilidade é medida pela *fidelidade*, a probabilidade que a saída do canal poderá passar em um teste e ser qualificada como sendo a mesma da entrada, conduzida por alguém ou algo que conheça o que foi a entrada [8, 104]. Quando um estado puro $\rho = |\psi\rangle \langle\psi|$ é enviado em um canal χ, surgindo, em geral, como um estado misturado $\rho' = \chi(\rho)$, a fidelidade da saída relativa à entrada é

$$F = \langle\psi| \rho' |\psi\rangle . \tag{B.2}$$

O objetivo dos códigos quânticos é proteger os sistemas quânticos dos efeitos de interações indesejadas com o ambiente externo. Para descrever essas interações, é necessário um formalismo que lide com sistemas abertos [8]. Um dos modelos utilizados para descrever esse tipo de interação consiste em admitir que um sistema quântico ρ e o ambiente ρ_{amb} partem inicialmente de um estado produto $\rho \otimes \rho_{amb}$ que sofre uma transformação unitária U. O estado do sistema quântico após a interação unitária é obtido por meio do traço parcial sobre o ambiente, ou seja:

$$\rho_f = \mathcal{E}(\rho) = Tr_{amb}[U(\rho \otimes \rho_{amb})U^\dagger]. \tag{B.3}$$

Uma representação mais adequada para manipulação matemática - conhecida como representação de operador-soma - pode ser obtida considerando-se o ambiente representado por $\rho_{amb} = \sum_l \lambda_l |\phi_l\rangle \langle\phi_l|$ e uma base ortonormal $\{|e_m\rangle\}$ para o espaço de Hilbert do ambiente $\mathcal{H}_E$. Dessa forma, pode-se reescrever (B.3) como

$$\rho_f = \mathcal{E}(\rho) = \sum_{l,m} \lambda_l \langle e_m| U\big(\rho \otimes |\phi_l\rangle \langle\phi_l|\big)U^\dagger |e_m\rangle = \sum_{l,m} \mathcal{E}_{l,m}\rho\mathcal{E}_{l,m}^\dagger. \tag{B.4}$$

onde $\mathcal{E}_{l,m} = \sqrt{\lambda_l} \langle e_m| U |\phi_l\rangle$. Os operadores $\mathcal{E}_{lm}$ são operadores lineares no espaço de Hilbert do sistema quântico ρ e especificam o efeito do ambiente na dinâmica do sistema. Os operadores

$\mathcal{E}_{l,m}$ são também conhecidos como operadores de erro e são frequentemente referenciados por um único índice k no lugar de lm.

A representação de operador-soma permite fazer uma analogia com os canais clássicos, resultando em um modelo para canais quânticos ruidosos. Para um conjunto de operadores de erro $\{\mathcal{E}_k\}$, o estado do sistema é transformado como segue

$$\rho \longrightarrow \frac{\mathcal{E}_k \rho \mathcal{E}_k^\dagger}{Tr(\mathcal{E}_k \rho \mathcal{E}_k^\dagger)} \tag{B.5}$$

com probabilidade $Tr(\mathcal{E}_k \rho \mathcal{E}_k^\dagger)$.

A representação de operador-soma não é única, de modo que bases de erro diferentes podem resultar em operadores de erro diferentes. Assim como para os canais clássicos, há diversos modelos de canais quânticos. Dentre os canais quânticos, são descritos a seguir alguns canais de Pauli (canal de inversão de bit, canal de inversão de fase, canal de inversão de bit e fase e o canal de despolarização).

B.2.1 Canal de Inversão de Bit

O canal de inversão de bit inverte o estado de um qbit de $|0\rangle$ para $|1\rangle$ (e vice-versa) com probabilidade $1-p$ e mantém o estado inalterado com probabilidade p. O modelo de operador-soma para esse canal é dado por dois elementos:

$$\mathcal{E}_0 = \sqrt{p} I; \;\; \mathcal{E}_1 = \sqrt{1-p} X. \tag{B.6}$$

Canal de Inversão de Fase

O canal de inversão de fase inverte a fase de um qbit com probabilidade $1-p$ e mantém o estado inalterado com probabilidade p. O modelo de operador-soma para esse canal é dado por dois elementos:

$$\mathcal{E}_0 = \sqrt{p} I; \;\; \mathcal{E}_1 = \sqrt{1-p} Z. \tag{B.7}$$

B.2.2 Canal de Inversão de Bit e Fase

O canal de inversão de bit e fase inverte a fase e o estado de um qbit com probabilidade $1-p$ e mantém o estado inalterado com probabilidade p. O modelo de operador-soma para esse canal é dado por dois elementos:

$$\mathcal{E}_0 = \sqrt{p} I; \;\; \mathcal{E}_1 = \sqrt{1-p} Y. \tag{B.8}$$

B.2.3 Canal de Despolarização

O canal de despolarização transforma o estado ρ em um estado completamente misturado $I/2$ com probabilidade p e mantém o estado polarizado (inalterado) com probabilidade $1-p$. A operação quântica que descreve esse processo de ruído é dada por:

$$\mathcal{E}(\rho) = \frac{pI}{2} + (1-p)\rho. \tag{B.9}$$

A representação em operador-soma para o canal de despolarização é obtida a partir da identidade:

$$\frac{I}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4}. \tag{B.10}$$

Considerando agora o canal de despolarização com uma parametrização dada por:

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}\big(X\rho X + Y\rho Y + Z\rho Z\big) \tag{B.11}$$

Substituindo (B.10) em (B.11), tem-se os seguintes operadores para o canal de despolarização:

$$\mathcal{E}_0 = \sqrt{1 - \frac{3p}{4}}I;\ \ \mathcal{E}_1 = \sqrt{p}\frac{X}{2};\ \ \mathcal{E}_2 = \sqrt{p}\frac{Y}{2};\ \ \mathcal{E}_3 = \sqrt{p}\frac{Z}{2}. \tag{B.12}$$

B.3 Portas Quânticas Elementares

Inicialmente serão mostradas algumas portas bem simples, a saber: NOT, Inversão de fase e Hadamard-Walsh. Algumas são utilizadas com frequência, outras não são muito utilizadas mas ilustram bem o funcionamento das portas quânticas. Para construir circuitos quânticos não triviais é necessário a inclusão de operações que manipulam mais de um qbit. Assim, serão mostradas algumas portas quânticas de múltiplos qbits, a saber: NOT-Controlado e Toffoli (estas são fundamentais no desenvolvimento de parte do trabalho apresentado neste documento). Note que todas as portas a serem descritas são matrizes unitárias (que realizam transformações unitárias).

B.3.1 NOT

A porta clássica mais simples é a porta NOT, que é uma porta de um bit que nega o estado do bit de entrada: 0 vira 1 e vice-versa. A porta quântica correspondente é implementada via uma operação unitária que faz com que os estados-base mudem seus estados de acordo com a tabela-verdade do NOT clássico. O U_{not} é a operação quântica unitária que corresponde ao NOT clássico. Essa operação, aplicada a um estado, pode ser descrita como

$$
\begin{aligned}
U_{not}(|0\rangle) &= |1\rangle\,, \\
U_{not}(|1\rangle) &= |0\rangle\,.
\end{aligned}
$$

A matriz de transformação dessa operação é dada por

$$
U_{not} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{B.13}
$$

Supondo que $|0\rangle$ e $|1\rangle$ sejam definidos como os vetores $[1,0]^T$ e $[0,1]^T$, respectivamente, então a operação de NOT funciona da seguinte maneira:

$$
U_{not}(|0\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle.
$$

Analogamente, pode-se aplicar U_{not} para $|1\rangle$.

Com a porta NOT quântica, temos situações sem contrapartida no caso clássico, pois, se a entrada $|\psi\rangle$ for uma superposição dos estados $|0\rangle$ e $|1\rangle$

$$
|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{B.14}
$$

a saída será

$$
U_{not} = \beta\,|0\rangle + \alpha\,|1\rangle\,. \tag{B.15}
$$

A porta U_{not} é apenas uma das portas de 1-qbit, já que há infinitas matrizes unitárias 2×2 [105].

B.3.2 Inversão de fase ou S

A matriz de transformação dessa operação é dada por

$$
U_{if} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \tag{B.16}
$$

em que i é a unidade imaginária ($i^2 = -1$). A porta de inversão de fase pode também ser representada por [105]

$$U_{if} = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/2) \end{bmatrix}, \tag{B.17}$$

já que $\exp(i\pi/2) = \cos(\pi/2) + i\,\mathrm{sen}(\pi/2) = i$.

Aplicando U_{if} em um estado genérico

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{B.18}$$

obtém-se

$$U_{if}\,|\psi\rangle = \alpha\,|0\rangle + i\beta\,|1\rangle\,. \tag{B.19}$$

B.3.3 Hadamard-Walsh

Uma das mais importantes portas da computação quântica, a porta Hadamard não tem uma função análoga na computação clássica. Sua matriz é dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{B.20}$$

Sua função é a seguinte

$$\begin{aligned} H\big(\,|0\rangle\,\big) &= \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big), \\ H\big(\,|1\rangle\,\big) &= \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big). \end{aligned}$$

Quando a porta H é aplicada a mais de um qbit, chama-se essa transformação de Walsh, ou Hadamard-Walsh. Ela pode ser definida recursivamente como

$$\begin{cases} W_1 &= H, \\ W_{n+1} &= H \otimes W_n. \end{cases}$$

A porta H é aplicada em todos os qbits de um estado. Essa transformação é de grande utilidade: seja $|\psi\rangle$ um estado inicialmente configurado com todos os seus qbits em $|0\rangle$. Aplicando-se a porta H em cada qbit separadamente, então o resultado fica

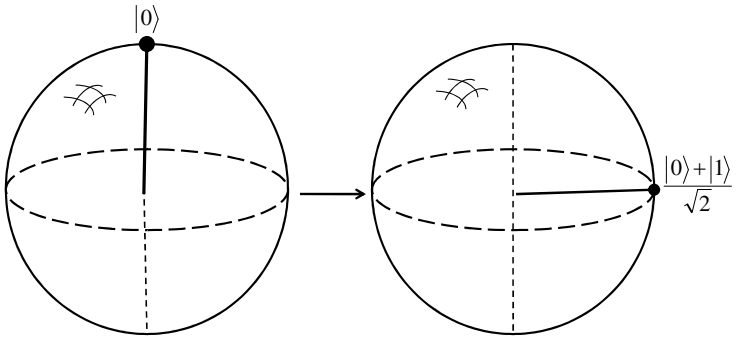

Figura B.1 Representação geométrica da porta Hadamard aplicada ao estado $|0\rangle$.

$$
\begin{aligned}
|\psi\rangle &= H \otimes H \otimes \cdots \otimes H \, |00\cdots0\rangle \\
&= \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \\
&= \left(\frac{1}{\sqrt{2}}\right)^{n} \Big(\,|00\cdots0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle\,\Big) \\
&= \left(\frac{1}{\sqrt{2}}\right)^{n} \sum_{i=0}^{2^n-1} |i\rangle\,. \qquad \text{(B.21)}
\end{aligned}
$$

Em outras palavras, ao aplicar a transformação Hadamard-Walsh num estado inicialmente configurado em $|00\cdots0\rangle$, consegue-se uma sobreposição de todos os valores possíveis de ser armazenados nesse estado. Além disso, com um número linear de operações (i.e, para um estado de n qbits, aplica-se a porta Hadamard n vezes), gera-se um estado que contém um número exponencial (2^n) de termos distintos, i.e., o estado contém todos os valores numéricos de tamanho n possíveis em sobreposição e com a mesma amplitude. Em contraste com o caso clássico, num estado de n bits, pode-se armazenar somente um único valor numérico em cada estado.

B.3.4 NOT-Controlado

A porta NOT-Controlado (abreviada como CNOT) tem seu funcionamento descrito pelo diagrama da Figura B.2, em que $\oplus$ denota a operação de ou-exclusivo (XOR).

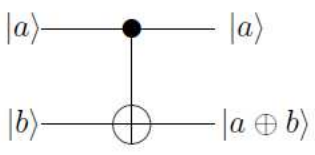

Figura B.2 Notação para a porta NOT-Controlado (CNOT).

Assim, entra o estado $|a\rangle$ e sai o estado $|a\rangle$. Por outro lado, entra o estado $|b\rangle$, e sai o estado $|a \oplus b\rangle$.

Mas, uma maneira diferente de interpretar esse diagrama é dizer que o qbit $|a\rangle$ é um sinal de controle para especificar se deve-se ou não negar o qbit $|b\rangle$. Em outras palavras, se o qbit $|a\rangle$ estiver "ligado", o qbit $|b\rangle$ é negado. Se $|a\rangle$ estiver "desligado", $|b\rangle$ não é modificado. Essa transformação é dada pela matriz[3]

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

A porta CNOT é uma porta muito importante para a composição de operações mais complexas. Como exemplo, pode ser construído um circuito composto de CNOT's que troca um par de qbits que estão na base computacional, descrito no diagrama da Figura B.3.

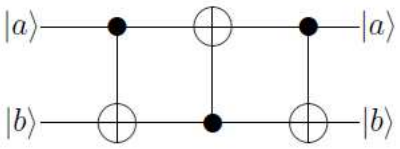

Figura B.3 Circuito que simula um SWAP.

A ação do circuito é

$$\begin{aligned} |a,b\rangle \overset{U_{CNOT}}{\longrightarrow} |a, a\oplus b\rangle \overset{U_{CNOT}}{\longrightarrow} |(a\oplus b)\oplus a, a\oplus b\rangle &= |b, a\oplus b\rangle \overset{U_{CNOT}}{\longrightarrow} \\ |b, b\oplus(a\oplus b)\rangle &= |b,a\rangle. \end{aligned} \tag{B.22}$$

B.3.5 Toffoli

A próxima porta a ser considerada é a correspondente quântica da porta Toffoli. Também é uma porta controlada, só que nesse caso, com dois qbits de controle (Figura B.4). Similarmente à porta CNOT, a porta Toffoli nega o terceiro qbit se, e somente se, os dois primeiros qbits são 1. Como é descrito logo a seguir.

Uma operação Toffoli $T_{i,j,r}$ tem dois qbits de controle correspondendo aos dois primeiros subescritos (i,j), e o bit alvo r. Sua ação na base computacional associada pode ser representada por

$$|i,j,k\rangle \rightarrow |i,j,k\oplus ij\rangle\,, \tag{B.23}$$

[3]Assumindo que $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$ estão associados a $[1,0,0,0]^T$, $[0,1,0,0]^T$, $[0,0,1,0]^T$ e $[0,0,0,1]^T$, respectivamente.

em que $i, j, k \in \{0, 1\}$ e $\oplus$ é a adição módulo 2 [105]. Observe que, nesse caso, a base computacional possui 8 elementos.

Por exemplo, quando os dois bits de controle estão no estado $|11\rangle$, o estado do bit alvo irá mudar, seguindo $|0\rangle \rightarrow |1\rangle$ ou $|1\rangle \rightarrow |0\rangle$, enquanto que quando os dois bits de controle estão nos estados $|00\rangle$, $|01\rangle$ ou $|10\rangle$, o estado do bit alvo será invariante.

A representação gráfica da porta Toffoli é apresentada na Figura B.4.

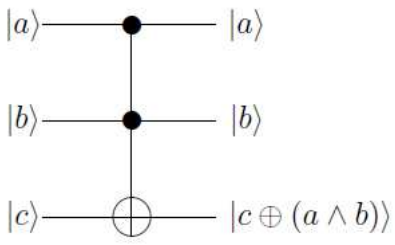

Figura B.4 Circuito representando a porta Toffoli.

A porta Toffoli também pode ser utilizada para computar uma operação de AND. Se for inicializado $|c\rangle$ com 0, o estado final do terceiro qbit é $|a \wedge b\rangle$. Essa porta também é chamada de NOT-Controlado-Controlado, devido a isso alguns trabalhos fazem uso da abreviação, C^2-NOT.

B.4 Transformada de Fourier Quântica e sua Inversa

Similar a transformada de Fourier clássica e sua inversa [106, 107], pode-se definir análogos quânticos, operando nas sequências dos números complexos armazenados como coeficientes de estados quânticos.

Todos os algoritmos quânticos conhecidos até hoje que são exponencialmente mais rápidos que seus correspondentes clássicos utilizam a Transformada de Fourier Quântica (TFQ) em alguma parte. Por exemplo, o algoritmo de Shor utiliza uma versão quântica do algoritmo para TFQ que é eficiente quando os fatores primos do número a ser fatorado não são grandes [108].

Uma razão para que um algoritmo quântico seja superior a um clássico é que a tranformada de Fourier quântica tem complexidade $O(n^2)$, que é exponencialmente mais rápido que a versão clássica que tem complexidade $O(n\ 2^n)$ [8, 56].

Nesta seção são apresentados as definições da TFQ e TFQI. Depois disso, ilustra-se o uso de tais definições por meio de exemplos.

B.4.1 Definições

A seguir é apresentado a definição de TFQ.

Definição B.1. *[109] A Transformada de Fourier Quântica (TFQ) é o mapeamento unitário definido nos estados bases $|j\rangle$ como*

$$|j\rangle \xrightarrow{TFQ} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \tag{B.24}$$

e estendido por linearidade.

Tem-se que na equação (B.24) acima N=2^n, sendo n algum inteiro e a base $|0\rangle, \ldots, |2^n - 1\rangle$ é a base computacional para um computador quântico de n qbits.

A transformada inversa é definida a seguir.

Definição B.2. *[8, 109] A Transformada de Fourier Quântica Inversa (TFQI) é o mapeamento unitário definido nos estados bases $|k\rangle$ como*

$$|k\rangle \xrightarrow{TFQI} \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi ijk/N} |j\rangle \tag{B.25}$$

e estendido por linearidade.

B.4.2 Exemplos

Para ilustrar a aplicação das Definições B.1 e B.2 são dados alguns exemplos.

Exemplo B.1. *Para $N = 2$ (1 qbit) a transformada de fourier para $|0\rangle$ fica,*

$$|0\rangle \xrightarrow{TFQ} \frac{1}{\sqrt{2}} \sum_{k=0}^{1} e^{2\pi i 0k/2} |k\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right). \tag{B.26}$$

Para obter a inversa deve-se calcular $f^{-1}\left[\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right]$. Mas, devido a propriedade de linearidade da Fourier quântica tem-se que

$$f^{-1}\left[\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right] = \frac{1}{\sqrt{2}} f^{-1}(|0\rangle) + \frac{1}{\sqrt{2}} f^{-1}(|1\rangle). \tag{B.27}$$

Assim,

$$|0\rangle \xrightarrow{TFQI} \frac{1}{\sqrt{2}} \sum_{j=0}^{1} e^{-2\pi.i.0.j/2} |j\rangle = \frac{1}{\sqrt{2}} \left(e^{-2\pi i 0.0/2}|0\rangle + e^{-2\pi i 0.1/2}|1\rangle\right) = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right). \tag{B.28}$$

$$|1\rangle \xrightarrow{TFQI} \frac{1}{\sqrt{2}} \sum_{j=0}^{1} e^{-2\pi i.1.j/2} |j\rangle = \frac{1}{\sqrt{2}} \left(e^{-2\pi i 1.0/2}|0\rangle + e^{-2\pi i 1.1/2}|1\rangle\right) = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right). \tag{B.29}$$

Substituindo esses resultados na equação (B.27), obtém-se

$$\begin{aligned} f^{-1}\left[\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right] &= \frac{1}{\sqrt{2}}f^{-1}(|0\rangle)+\frac{1}{\sqrt{2}}f^{-1}(|1\rangle) \\ &= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right]+\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\right] \\ &= |0\rangle. \end{aligned} \tag{B.30}$$

Para se obter a transformada do qbit $|1\rangle$ e sua inversa aplica-se o mesmo processo ilustrado acima.

Para a obtenção do estado quântico $|v\rangle = \sum a_j|j\rangle$ a transformada de Fourier é dada como [109]:

$$\begin{aligned} \sum_{j=0}^{N-1} a_j|j\rangle &\overset{TFQ}{\longrightarrow} \sum_{j=0}^{N-1} a_j\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle \\ &= \sum_{k=0}^{N-1}\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} a_j e^{2\pi ijk/N}\right)|k\rangle. \end{aligned} \tag{B.31}$$

A transformada inversa para a equação (B.31) é como descrita na Definição B.2.

A fim de ilustrar a aplicação da transformada de Fourier envolvendo a equação (B.31) apresenta-se alguns exemplos.

Deve-se notar que as aplicações das TFQ e TFQI tomam sempre como entrada um estado da base computacional. Como será visto, após a aplicação da TFQI se obtém que associado a cada amplitude haverá apenas um estado da base, uma vez que os demais estados da base associados a uma amplitude em particular irão desaparecer no decorrer do processamento.

Exemplo B.2. *Considerando N=2, tem-se*

$$\begin{aligned} \sum_{j=0}^{1} a_j|j\rangle = a_0|0\rangle + a_1|1\rangle &\overset{TFQ}{\longrightarrow} \sum_{k=0}^{1}\left(\frac{1}{\sqrt{2}}\sum_{j=0}^{1} a_j e^{\pi ijk}\right)|k\rangle \\ &= \frac{1}{\sqrt{2}}\left[(a_0+a_1)|0\rangle+(a_0-a_1)|1\rangle\right] \\ &= \frac{1}{\sqrt{2}}(a_0|0\rangle+a_0|1\rangle+a_1|0\rangle-a_1|1\rangle). \end{aligned} \tag{B.32}$$

Para obter a inversa deve-se calcular $f^{-1}\left[\frac{1}{\sqrt{2}}(a_0|0\rangle + a_0|1\rangle + a_1|0\rangle - a_1|1\rangle)\right]$. *Mas, devido a propriedade de linearidade da Fourier quântica tem-se que*

$$\begin{aligned} f^{-1}\Big[\frac{1}{\sqrt{2}}(a_0|0\rangle + a_0|1\rangle + a_1|0\rangle - a_1|1\rangle)\Big] &= \frac{1}{\sqrt{2}}\Big[a_0 f^{-1}(|0\rangle) + a_0 f^{-1}(|1\rangle) \\ &\quad + a_1 f^{-1}(|0\rangle) - a_1 f^{-1}(|1\rangle)\Big]. \end{aligned} \tag{B.33}$$

Substituindo os resultados obtidos nas equações (B.28) e (B.29) na equação (B.33), tem-se que

$$\begin{aligned} f^{-1}\left[\frac{1}{\sqrt{2}}(a_0|0\rangle + a_0|1\rangle + a_1|0\rangle - a_1|1\rangle)\right] &= \frac{1}{\sqrt{2}}\Big\{a_0\Big[\frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)\Big] \\ &\quad + a_0\Big[\frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)\Big] \\ &\quad + a_1\Big[\frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)\Big] \\ &\quad - a_1\Big[\frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)\Big]\Big\} \\ &= \frac{1}{\sqrt{2}}\Big\{\frac{1}{\sqrt{2}}\Big(a_0|0\rangle + a_0|1\rangle\Big) \\ &\quad + \frac{1}{\sqrt{2}}\Big(a_0|0\rangle - a_0|1\rangle\Big) \\ &\quad + \frac{1}{\sqrt{2}}\Big(a_1|0\rangle + a_1|1\rangle\Big) \\ &\quad - \frac{1}{\sqrt{2}}\Big(a_1|0\rangle - a_1|1\rangle\Big)\Big\} \\ &= a_0|0\rangle + a_1|1\rangle, \end{aligned} \tag{B.34}$$

Note em (B.34) que, dos dois estado que estavam associados a cada amplitude, apenas um permaneceu no final do processo.

Exemplo B.3. *Considerando N=4, tem-se*

$$|v\rangle = \sum_{j=0}^{3} a_j|j\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle \tag{B.35}$$

e, portanto,

$$
\begin{aligned}
|v\rangle \stackrel{TFQ}{\longrightarrow} |\psi\rangle &= \sum_{k=0}^{3}\left(\frac{1}{\sqrt{4}}\sum_{j=0}^{3} a_j e^{2\pi i j k/4}\right)|k\rangle \qquad \text{(B.36)}\\
&= \frac{1}{2}\Big[\big(a_0+a_1+a_2+a_3\big)|0\rangle+\big(a_0+ia_1-a_2-ia_3\big)|1\rangle\\
&\quad +\big(a_0-a_1+a_2-a_3\big)|2\rangle+\big(a_0-ia_1-a_2+ia_3\big)|3\rangle\Big].
\end{aligned}
$$

Para obter a inversa deve-se calcular

$$
\begin{aligned}
f^{-1}(|\psi\rangle) &= f^{-1}\Big\{\frac{1}{2}\Big[\big(a_0+a_1+a_2+a_3\big)|0\rangle+\big(a_0+ia_1-a_2-ia_3\big)|1\rangle\\
&\quad +\big(a_0-a_1+a_2-a_3\big)|2\rangle+\big(a_0-ia_1-a_2+ia_3\big)|3\rangle\Big]\Big\}. \qquad \text{(B.37)}
\end{aligned}
$$

Mas, devido a propriedade de linearidade tem-se que

$$
\begin{aligned}
f^{-1}(|\psi\rangle) &= \frac{1}{2}\Big[(a_0+a_1+a_2+a_3)f^{-1}\big(|0\rangle\big)+(a_0+ia_1-a_2-ia_3)f^{-1}\big(|1\rangle\big)\\
&\quad +(a_0-a_1+a_2-a_3)f^{-1}\big(|2\rangle\big)+(a_0-ia_1-a_2+ia_3)f^{-1}\big(|3\rangle\big)\Big]. \qquad \text{(B.38)}
\end{aligned}
$$

Sabendo que

$$
|k\rangle \stackrel{TFQI}{\longrightarrow} f^{-1}(|k\rangle) = \sum_{j=0}^{3}\frac{1}{\sqrt{4}}e^{-2\pi.i.j.k/4}|j\rangle, \qquad \text{(B.39)}
$$

obtém-se

$$
\begin{aligned}
f^{-1}(|0\rangle) &= \frac{1}{2}\Big(|0\rangle+|1\rangle+|2\rangle+|3\rangle\Big); \qquad \text{(B.40)}\\
f^{-1}(|1\rangle) &= \frac{1}{2}\Big(|0\rangle-i|1\rangle-|2\rangle+i|3\rangle\Big); \qquad \text{(B.41)}\\
f^{-1}(|2\rangle) &= \frac{1}{2}\Big(|0\rangle-|1\rangle+|2\rangle-|3\rangle\Big); \qquad \text{(B.42)}\\
f^{-1}(|3\rangle) &= \frac{1}{2}\Big(|0\rangle+i|1\rangle-|2\rangle-i|3\rangle\Big). \qquad \text{(B.43)}
\end{aligned}
$$

Substituindo os resultados obtidos nas equações (B.40) a (B.43) em (B.39), obtém-se

$$
\begin{aligned}
f^{-1}\left(|\psi\rangle\right) &= \frac{1}{2}\Big\{(a_0+a_1+a_2+a_3)\Big[\frac{1}{2}\big(|0\rangle+|1\rangle+|2\rangle+|3\rangle\big)\Big] \\
&\quad +(a_0+ia_1-a_2-ia_3)\Big[\frac{1}{2}\big(|0\rangle-i|1\rangle-|2\rangle+i|3\rangle\big)\Big] \\
&\quad +(a_0-a_1+a_2-a_3)\Big[\frac{1}{2}\big(|0\rangle-|1\rangle+|2\rangle-|3\rangle\big)\Big] \\
&\quad +(a_0-ia_1-a_2+ia_3)\Big[\frac{1}{2}\big(|0\rangle+i|1\rangle-|2\rangle-i|3\rangle\big)\Big]\Big\} \\
&= a_0|0\rangle+a_1|1\rangle+a_2|2\rangle+a_3|3\rangle, \qquad \text{(B.44)}
\end{aligned}
$$

Pode-se notar em (B.44) que no final do processo apenas um estado da base ficou associado a cada amplitude a_i ($i=0\ldots3$).

É útil também escrever a transformada de Fourier para o estado quântico $|\psi\rangle=\sum a_j|j\rangle$ usando a representação binária. Assim, a transformada de Fourier para dimensão n fica da seguinte forma [8]

$$
\begin{aligned}
\sum_{j_1=0}^{1}\cdots\sum_{j_n=0}^{1}a_{j_1\ldots j_n}|j_1\ldots j_n\rangle \overset{TFQ}{\longrightarrow} \sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\Bigg(\frac{1}{\sqrt{2^n}}\sum_{j_1=0}^{1}\cdots\sum_{j_n=0}^{1}a_{j_1\ldots j_n}e^{2\pi i\left(j_1 2^{n-1}+j_2 2^{n-2}\right.} \\
\left.{}+\ldots+j_n 2^0\right)\left(\sum_{l=1}^{n}k_l/2^l\right)\Bigg)|k_1\ldots k_n\rangle \qquad \text{(B.45)}
\end{aligned}
$$

e a inversa é dada como a seguir

$$
|k_1\ldots k_n\rangle \overset{TFQI}{\longrightarrow} \frac{1}{\sqrt{2^n}}\sum_{j_1=0}^{1}\cdots\sum_{j_n=0}^{1}e^{-2\pi i(j_1 2^{n-1}+j_2 2^{n-2}+\ldots+j_n 2^0)(\sum_{l=1}^{n}k_l/2^l)}|j_1\ldots j_n\rangle \qquad \text{(B.46)}
$$

Para ilustrar a aplicação das equações (B.45) e (B.46) é apresenta-se o exemplo que vem a seguir.

Exemplo B.4. *Considerando $n=2$ ($N=2^2=4$) tem-se*

$$
|v\rangle=\sum_{j_1=0}^{1}\sum_{j_2=0}^{1}a_{j_1j_2}|j_1j_2\rangle=a_{00}|00\rangle+a_{01}|01\rangle+a_{10}|10\rangle+a_{11}|11\rangle \qquad \text{(B.47)}
$$

e

$$
\begin{aligned}
|v\rangle \stackrel{TFQ}{\longrightarrow} |\psi\rangle &= \sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\left(\frac{1}{\sqrt{2^2}}\sum_{j_1=0}^{1}\sum_{j_2=0}^{1} a_{j_1 j_2} e^{2\pi(2j_1+j_2)(\sum_{l=1}^{2} k_l/2^l)}\right)|k_1 k_2\rangle \qquad \text{(B.48)}\\
&= \frac{1}{2}\left[(a_{00}+a_{01}+a_{10}+a_{11})|00\rangle + (a_{00}+ia_{01}-a_{10}-ia_{11})|01\rangle\right.\\
&\quad \left.+(a_{00}-a_{01}+a_{10}-a_{11})|10\rangle + (a_{00}-ia_{01}-a_{10}+ia_{11})|11\rangle\right].
\end{aligned}
$$

Para obter a inversa, deve-se calcular

$$
\begin{aligned}
f^{-1}(|\psi\rangle) &= f^{-1}\{\frac{1}{2}\left[(a_{00}+a_{01}+a_{10}+a_{11})|00\rangle + (a_{00}+ia_{01}-a_{10}-ia_{11})|01\rangle\right.\\
&\quad \left.+(a_{00}-a_{01}+a_{10}-a_{11})|10\rangle + (a_{00}-ia_{01}-a_{10}+ia_{11})|11\rangle\right]\}. \qquad \text{(B.49)}
\end{aligned}
$$

Mas, devido a propriedade de linearidade tem-se que

$$
\begin{aligned}
f^{-1}(|\psi\rangle) &= \frac{1}{2}\left[(a_{00}+a_{01}+a_{10}+a_{11})f^{-1}(|00\rangle) + (a_{00}+ia_{01}-a_{10}-ia_{11})f^{-1}(|01\rangle)\right.\\
&\quad +(a_{00}-a_{01}+a_{10}-a_{11})f^{-1}(|10\rangle)\\
&\quad \left.+(a_{00}-ia_{01}-a_{10}+ia_{11})f^{-1}(|11\rangle)\right]. \qquad \text{(B.50)}
\end{aligned}
$$

Com isso, basta calcular as inversas de $f^{-1}(|00\rangle), f^{-1}(|01\rangle), f^{-1}(|10\rangle), f^{-1}(|11\rangle)$. Assim, calculando

$$
|k_1 k_2\rangle \stackrel{TFQI}{\longrightarrow} \frac{1}{2}\sum_{j_1=0}^{1}\sum_{j_2=0}^{1} e^{-2\pi i(j_1 2+j_2)(\sum_{l=1}^{2} k_l/2^l)}|j_1 j_2\rangle \qquad \text{(B.51)}
$$

obtém-se

$$
\begin{aligned}
f^{-1}(|00\rangle) &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle); \qquad \text{(B.52)}\\
f^{-1}(|01\rangle) &= \frac{1}{2}(|00\rangle - i|01\rangle - |10\rangle + i|11\rangle); \qquad \text{(B.53)}\\
f^{-1}(|10\rangle) &= \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right); \qquad \text{(B.54)}\\
f^{-1}(|11\rangle) &= \frac{1}{2}\left(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle\right). \qquad \text{(B.55)}
\end{aligned}
$$

Substituindo os resultados obtidos nas equações (B.52) a (B.55) em (B.50), obtém-se

$$
\begin{aligned}
f^{-1}\left(|\psi\rangle\right) &= \frac{1}{2}\Big\{(a_{00}+a_{01}+a_{10}+a_{11})\Big[\frac{1}{2}\big(|00\rangle+|01\rangle+|10\rangle+|11\rangle\big)\Big]+ \\
&\quad +(a_{00}+ia_{01}-a_{10}-ia_{11})\Big[\frac{1}{2}\big(|00\rangle-i|01\rangle-|10\rangle+i|11\rangle\big)\Big] \\
&\quad +(a_{00}-a_{01}+a_{10}-a_{11})\Big[\frac{1}{2}\big(|00\rangle-|01\rangle+|10\rangle-|11\rangle\big)\Big] \\
&\quad +(a_{00}-ia_{01}-a_{10}+ia_{11})\Big[\frac{1}{2}\big(|00\rangle+i|01\rangle-|10\rangle-i|11\rangle\big)\Big]\Big\} \\
&= a_{00}|00\rangle+a_{01}|01\rangle+a_{10}|10\rangle+a_{11}|11\rangle. \qquad \text{(B.56)}
\end{aligned}
$$

Observe que, do mesmo modo que nos casos anteriores, apenas um estado da base permaneceu associado a cada amplitude.

Estas observações são importantes no contexto deste trabalho porque ajudam no entendimento da demonstração do Teorema 4.1.

APÊNDICE C

Caracter de Grupos

C.1 Introdução

Em matemática, um *caracter* é uma classe especial de funções de um grupo para um corpo (tal como os números complexos).

O caracter de uma representação φ de um grupo $\mathcal{G}$ em um espaço vetorial de dimensão finita V sobre um corpo $\mathbb{F}$ é o traço da representação φ. Em geral, o traço não é um homomorfismo de grupo, ou o conjunto de traços não forma um grupo. Os caracteres da representação unidimensional são idênticos à representações unidimensionais, assim a noção de caracter multiplicativo pode ser vista como um caso especial de caracteres multidimensionais. O estudo de representações usando caracteres é chamado de Teoria de Caracter e caracteres unidimensionais são também chamados de "caracteres lineares" dentro desse contexto.

Georg Frobenius inicialmente desenvolveu a teoria de representação de grupos finitos inteiramente baseada em caracteres, e sem qualquer realização matricial explícita de representações próprias [110]. Isso é possível porque uma representação complexa de um grupo finito é determinada (a menos de isomorfismo) por seu caracter. A situação com representações sobre um corpo de característica positiva, chamado "representações modulares", é mais delicada. Mas, Richard Brauer desenvolveu uma teoria poderosa de caracteres também para este caso [111, 112]. Muitos teoremas sobre a estrutura dos grupos finitos usam caracteres de representações modulares.

Um *caracter de grupo* é o grupo de representações de um grupo por funções de valores complexos. Essas funções podem ser pensadas como representações de matrizes unidimensionais e por isso são casos especiais de caracteres de grupo que surgem no contexto relacionado da Teoria de Caracter [110, 113].

Sempre que um grupo é representado por matrizes, a função definida pelo traço da matriz é chamada de um *caracter*. No entanto, esses traços não constituem de uma forma geral um grupo. Algumas propriedades importantes desses caracteres unidimensionais se aplicam à caracteres em geral:

- Caracteres são invariantes em classes conjugadas;
- Os caracteres de representações irredutíveis são ortogonais.

A importância primordial do caracter de grupo para grupos abelianos finitos está na Teoria dos Números, em que é usado para construir caracteres de Dirichlet. O Caracter de grupo do grupo cíclico também aparece na teoria da transformada de Fourier discreta. Para grupos abelianos localmente compactos, o caracter de grupo (com o pressuposto de continuidade) é central para a Análise de Fourier [113].

C.2 Definições

Seja $\mathcal{G}$ um grupo abeliano finito. Um *caracter* é um homomorfismo de grupo de $\mathcal{G}$ para os números complexos [114]. Tome p como sendo um primo e seja $\mathbb{F}_p$ um corpo finito contendo p elementos, e escreve-se $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Sempre que conveniente, trata-se inteiros depois da redução módulo p como elementos em $\mathbb{F}_p$. Está-se interessado em caracteres definidos no grupo aditivo $(\mathbb{F}_p, +)$ e no grupo multiplicativo $(\mathbb{F}_p, \cdot)$.

Para um inteiro positivo n se escreve

$$\zeta_n(x) := e^{\left(i2\pi x/n\right)}, \tag{C.1}$$

em que $i = \sqrt{-1}$.

Definição C.1. *[114] Dado $b \in \mathbb{F}_p$, o mapeamento $\Delta_b : \mathbb{F}_p \to \mathbb{C}$, definido por*

$$\Delta_b(x) = \zeta_p(bx), \tag{C.2}$$

é chamado um caracter aditivo de $\mathbb{F}_p$.

Para $b = 0$, o caracter Δ_b é chamado *trivial*, caso contrário ele é chamado *não trivial* [114]. É facilmente verificado que um caracter aditivo Δ de $\mathbb{F}_p$ é de fato um homomorfismo:

$$\Delta(x + y) = \Delta(x)\Delta(y), \text{ para todo } x, y \in \mathbb{F}_p. \tag{C.3}$$

Definição C.2. *[114] Seja g um gerador para o grupo cíclico $(\mathbb{F}_p, \cdot)$. Então, para um inteiro a, o mapeamento $\chi_a : \mathbb{F}_p^* \to \mathbb{C}$, dado por*

$$\chi_a(g^i) = \zeta_{p-1}(ai), \tag{C.4}$$

é chamado um caracter multiplicativo de $\mathbb{F}_p$.

Exemplo C.1. *[115] Considere o grupo* $(ax + b)$*, em que*

$$\mathcal{G} = \left\{ \left[\begin{array}{cc} a & b \\ 0 & 1 \end{array} \right] \middle| \, a > 0, \; b \in \mathbb{R} \right\}. \tag{C.5}$$

Funções $f_u : \mathcal{G} \to \mathbb{C}$ *tais que*

$$f_u\left(\left[\begin{array}{cc} a & b \\ 0 & 1 \end{array} \right] \right) = a^u, \tag{C.6}$$

em que u *varia sobre os números complexos* $\mathbb{C}$*, são caracteres multiplicativos.*

Exemplo C.2. *[115] Considere o grupo multiplicativo dos números reais positivos* $(\mathbb{R}^+, \cdot)$*. Então funções* $f_u : (\mathbb{R}^+, \cdot) \to \mathbb{C}$ *tais que* $f_u(a) = a^u$*, em que* a *é um elemento de* $(\mathbb{R}^+, \cdot)$ *e* u *varia sobre o números complexos* $\mathbb{C}$*, são caracteres multiplicativos.*

Este grupo de caracter de $\mathcal{G}$ será denotado por $\hat{\mathcal{G}}$. Para $a \equiv 0 \; (mod \; p-1)$, o caracter χ_a é chamdo *trivial*, caso contrário ele é chamado *não trivial*. É conveniente estender um caracter multiplicativo χ para um mapeamento agindo em $\mathbb{F}_p$ colocando $\chi(0) = 0$. Esta extensão preserva a propriedade de homomorfismo, já que para cada caracter multiplicativo χ de $\mathbb{F}_p$ se tem

$$\chi(xy) = \chi(x)\chi(y), \text{ para todo } x, y \in \mathbb{F}_p. \tag{C.7}$$

A ordem de um caracter multiplicativo χ_a é definido como sendo o menor inteiro positivo d tal que $da \equiv 0 \; (mod \; p-1)$. Equivalentemente, $d = (p-1)/\text{mdc}(a, p-1)$.

Dado uma quantidade finita de caracteres $\chi_1, \ldots, \chi_n$ de $\mathcal{G}$, pode-se formar o produto de caracteres $\chi_1 \cdots \chi_n$ como sendo $(\chi_1 \cdots \chi_n)(g) = \chi_1(g) \cdots \chi_n(g)$, para todo $g \in \mathcal{G}$. Se $\chi_1 = \ldots = \chi_n = \chi$, escreve-se χ^n para $\chi_1 \cdots \chi_n$. É obvio que o conjunto $\hat{\mathcal{G}}$ de caracteres de $\mathcal{G}$ forma um grupo abeliano sob sua multiplicação de caracteres. Desde que os valores dos caracteres de $\mathcal{G}$ somente podem ser $|\mathcal{G}|$-ésimas raízes da unidade, $\hat{\mathcal{G}}$ é finito [116].

Exemplo C.3. *Seja* $\mathcal{G}$ *um grupo cíclico finito de ordem* n*, e seja* g *um gerador de* $\mathcal{G}$*. Por outro lado, se* χ *é caracter qualquer de* $\mathcal{G}$*, então* $\chi(g)$ *deve ser uma* n*-ésima raiz da unidade, diz-se que* $\chi(g) = e^{2\pi ij/n}$ *para algum* j*,* $0 \leq j \leq n-1$ *e segue que* $\chi = \chi_j$*. Portanto,* $\hat{\mathcal{G}}$ *consiste exatamente dos caracteres* $\chi_0, \chi_1, \ldots \; \chi_{n-1}$*, em que* χ_0 *é o caracter trivial definido como* $\chi_0(g) = 1$ *para todo* $g \in \mathcal{G}$*.*

Sejam $\mathcal{G}$ e $\mathcal{B}$ grupos abelianos e que Λ é um corpo, sendo Λ^* seu grupo multiplicativo.

Definição C.3. *[117] Um mapeamento* $\Theta : \mathcal{G} \times \mathcal{B} \to \Lambda^*$ *é um* Λ*-bicaracter do acoplamento* $\{\mathcal{G}, \mathcal{B}\}$ *se* $\Theta(x, y)$ $(x \in \mathcal{G}, y \in \mathcal{B})$ *é um* Λ*-caracter multiplicativo* ϕ_x *de* $\mathcal{B}$*, para um* x *fixado, e um* Λ*-caracter multiplicativo* ψ_y *de* $\mathcal{G}$*, para um* y *fixado. No caso de* $\mathcal{G} = \mathcal{B}$*, diz-se que é um bicaracter do grupo* $\mathcal{G}$*.*

Exemplo C.4. *Para $\mathcal{G} = \mathbb{Z}_p$, o grupo cíclico de ordem p, o bicaracter padrão é dado por*

$$\Theta(g,h) = e^{\left[(2\pi i/p)g\cdot h\right]}, \tag{C.8}$$

em que g, h são inteiros representando sua classe módulo p. Desde de que todo grupo abeliano finito é um produto direto de grupos cíclicos, isto também mostra a existência de bicaracteres para qualquer um desses grupos.

O Λ-caracter de um acoplamento $\{\mathcal{G},\mathcal{B}\}$ de grupos abelianos forma um grupo abeliano $B(\mathcal{G},\mathcal{B}|\Lambda)$ com a multiplicação naturalmente definida. Em particular $B(\mathcal{G},\mathcal{G}|\Lambda) = B(\mathcal{G}|\Lambda)$.

Os mapeamentos $x \to \phi_x$ e $y \to \psi_y$ são homomorfismos, respectivamente, dos grupos $\mathcal{G}$ e $\mathcal{B}$ dentro dos grupos $\mathcal{G}^*$ e $\mathcal{B}^*$ de Λ-caracteres de $\mathcal{G}$ e $\mathcal{B}$.

Definição C.4. *[117] Os núcleos dos homomorfismos $x \to \phi_x(x \in \mathcal{G})$ e $y \to \psi_y(y \in \mathcal{B})$ são chamados, respectivamente, os núcleos à esquerda e os núcleos à direita do Λ-bicaracter $\Theta \in B(\mathcal{G},\mathcal{B}|\Lambda)$ e são denotados por $Ker_l(\Theta)$ e $Ker_r(\Theta)$.*

Definição C.5. *[117] O bicaracter $\Theta \in B(\mathcal{G},\mathcal{B}|\Lambda)$ é dito ser não-degenerado se ambos os seus núcleos são triviais.*

A seguir, o corpo Λ é suposto ser algebricamente fechado e os grupos sendo de ordem finita não divisíveis pela característica de Λ. Uma vez que o corpo será mantido fixo, será suprimido sua menção e se escreve $B(\mathcal{G},\mathcal{B})$ ao invés de $B(\mathcal{G},\mathcal{B}|\Lambda)$, $B(\mathcal{G})$ ao invés de $B(\mathcal{G}|\Lambda)$ e se chamará um Λ-bicaracter simplesmente de *bicaracter*.

Será considerado daqui em diante $\mathcal{B} = \mathcal{G}$. Um bicaracter Θ do grupo $\mathcal{G}$ define uma relação de ortogonalidade: o elemento $x \in \mathcal{G}$ é ortogonal a um elemento $y \in \mathcal{G}$ (notação $x \perp y$) se $\Theta(x,y) = 1$. Se $J, K \subset \mathcal{G}$, então $J \perp L$ significa $(\forall x \in J)\ (\forall y \in K)\ x \perp y$.

Definição C.6. *[117] O grupo abeliano $\mathcal{G}$ é chamado métrica se ele é fornecido com um bicaracter Θ que define uma relação simétrica de ortogonalidade, isto é, $x \perp y$ implica $y \perp x$. O bicaracter Θ é dito ser associado ao grupo métrica $\mathcal{G}$.*

Não é difícil mostrar que o bicaracter Θ do grupo abeliano $\mathcal{G}$ define um relação simétrica de ortogonalidade se, e somente se, $(\forall x, y \in \mathcal{G})\ \Theta(x,y) = \Theta(y,x)^\lambda$, em que λ é uma raiz da congruência $\lambda^2 \equiv 1 \pmod{\exp \mathcal{G}}$. Tem-se que para bicaracteres simétricos $\Theta(x,y) = \Theta(y,x)$ e que para bicaracteres antisimétricos $\Theta(x,x) = 1$. Pode ser facilmente visto que para bicaracteres antisimétricos tem-se que $\Theta(x,y)\Theta(y,x) = 1$ para todo $x, y \in \mathcal{G}$.

Um bicaracter simétrico corresponde à geometria ortogonal enquanto que um bicaracter antisimétrico corresponde à geometria simplética em um grupo abeliano [117].