LUIZ PEREIRA LINS NETTO

CÓDIGOS DE BLOCO QUÂNTICOS COM PROTEÇÃO DESIGUAL DE ERROS

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para obtenção do grau de **Mestre em Engenharia Elétrica**

ORIENTADOR: PROF. CECILIO JOSÉ LINS PIMENTEL

Recife, fevereiro de 2008.

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE TECNOLOGIA E GEOCIÊNCIAS

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Luiz Pereira Lins Netto

Códigos de Bloco Quânticos Com Proteção Desigual de Erros

'Esta Dissertação foi julgada adequada para obtenção do Título de Mestre em Engenharia Elétrica, Área de Concentração em Comunicações, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco'.

Prof. Eduardo Fontana
Coordenador do Programa de
Pós-graduação em Engenharia Elétrica

Banca Examinadora:

Prof. Hélio Magalhães de Oliveira
Universidade Federal de Pernambuco

Prof. Valdemar Cardoso da Rocha Júnior
Universidade Federal de Pernambuco

Prof. Francisco Marcos de Assis
Universidade Federal de Campina Grande

29 de fevereiro de 2008

Universidade Federal de Pernambuco

Pós-Graduação em Engenharia Elétrica

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE DISSERTAÇÃO DO MESTRADO ACADÊMICO DE

LUIZ PEREIRA LINS NETTO

TÍTULO

"CÓDIGOS DE BLOCO QUÂNTICOS COM PROTEÇÃO DESIGUAL DE ERROS"

A comissão examinadora composta pelos professores: VALDEMAR CARDOSO DA ROCHA JÚNIOR, DES/UFPE, HÉLIO MAGALHÃES DE OLIVEIRA, DES/UFPE, e FRANCISCO MARCOS DE ASSIS, DEE/UFCG sob a presidência do primeiro, consideram o candidato **LUIZ PEREIRA LINS NETTO** **APROVADO**.

Recife, 29 de fevereiro de 2008

EDUARDO FONTANA
Coordenador do PPGEE

HÉLIO MAGALHÃES DE OLIVEIRA
Membro Titular Interno

FRANCISCO MARCOS DE ASSIS
Membro Titular Externo

VALDEMAR CARDOSO DA ROCHA JÚNIOR
Membro Titular Interno

N472c **Netto, Luiz Pereira Lins**

Códigos de bloco quânticos com proteção desigual de erros / Luiz Pereira Lins Netto. – Recife: O Autor, 2008.

x, 75f.; il., figs., tabs.

Dissertação (Mestrado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2008.

Inclui Referências Bibliográficas.

1. Engenharia elétrica. 2. Código corretor de erro quântico. 3. Hardware quântico. I. Título.

621.3 CDD (22.ed.) **UFPE/BCTG/2009-148**

A Tio Sérgio pelo exemplo de vida deixado

DEDICO

AGRADECIMENTOS

Ao professor Dr. Cecilio José Lins Pimentel pela dedicação e orientação, mesmo quando distante e aos professores da banca examinadora pelas valiosas observações fornecidas. A meus pais pelo constante apoio e suporte ao longo de minha vida. A meus irmãos pela companhia. A Millene pelo apoio nesta reta final. A meus companheiros de graduação e mestrado, de importância singular para minha formação profissional e pessoal, a todos sem exceção meu muito obrigado.

LUIZ PEREIRA LINS NETTO

Universidade Federal de Pernambuco

29 de fevereiro de 2008

Resumo da Dissertação apresentada à UFPE como parte dos requisitos necessários para a obtenção do grau de Mestre em Engenharia Elétrica

CÓDIGOS DE BLOCO QUÂNTICOS COM PROTEÇÃO DESIGUAL DE ERROS

Luiz Pereira Lins Netto

fevereiro/2008

Orientador: Prof. Cecilio José Lins Pimentel
Área de Concentração: Comunicações
Palavras-chaves: canal de inversão de bit, canal de inversão de fase, proteção desigual de erros, códigos de bloco quânticos, vetor de separação
Número de páginas: 85

Os códigos corretores de erros quânticos estão sendo desenvolvidos com o intuito de aumentar a confiabilidade do hardware quântico. A maioria dos códigos quânticos conhecidos são códigos de bloco, tendo os primeiros códigos convolucionais quânticos surgido recentemente. Já bastante difundida na teoria da codificação clássica, a proteção desigual de erros (UEP - *do inglês* unequal error protection), ainda não foi estudada no contexto de códigos quânticos, sendo este o principal objetivo desta dissertação. Introduziremos o conceito do vetor de separação quântico e uma técnica de análise da característica UEP de códigos de bloco quânticos para canais de inversão de bit e canais de inversão de fase.

Abstract of Dissertation presented to UFPE as a partial fulfillment of the requirements for the degree of Master in Electrical Engineering

QUANTUM BLOCK CODES WITH UNEQUAL ERROR PROTECTION

Luiz Pereira Lins Netto

February/2008

Supervisor: Prof. Cecilio José Lins Pimentel
Area of Concentration: Communication
Keywords: bit flip channel, phase flip channel, unequal error protection, quantum block codes, separation vector
Number of pages: 85

Quantum error correction codes have been developed to enhance the reliability of the quantum hardware. The majority of the known quantum codes belong to the class of block codes, while quantum convolutional codes have been recently proposed. The class of unequal error protection (UEP) codes, well known in the theory of classical codes, has not been studied in the context of quantum codes. This study is the main objective of this dissertation. The concept of quantum separation vector is introduced as well as a technique to analyze the UEP property of quantum block codes for two classes of channels: bit flip and phase flip.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

CAPÍTULO 1

INTRODUÇÃO

No início do século XX surgiram inúmeros fenômenos experimentais inexplicáveis de acordo com a teoria da física clássica. Trabalhos de Einstein, Heisenberg, Planck, Bohr, entre outros, culminaram no surgimento da mecânica quântica [1] [2], que compreende um conjunto de regras matemáticas voltadas para a construção de teorias físicas. Desde sua criação a mecânica quântica se mostra como uma das teorias mais bem sucedidas na física, com aplicações que vão da física atômica e molecular à astrofísica.

Os sistemas quânticos representam um grande salto tecnológico em processamento de informação. Neles a *informação quântica* é armazenada em *bits quânticos*, denominados de q-bits, cujos estados são processados por um computador quântico. Algumas etapas da evolução teórica e experimental dos sistemas quânticos são mostrados na Tabela 1.1.

Os computadores quânticos estabelecem uma alternativa, dando um ganho significativo para resolver problemas que exigem uma grande quantidade de recursos computacionais para um computador clássico. Bons exemplos constituem o problema da fatoração de grandes números e o problema do logaritmo discreto que, ao se utilizar a transformada de Fourier quântica [7, cap 5], ocorre um ganho de velocidade exponencial, em relação aos melhores algoritmos clássicos, seja para fatoração de grandes números, seja no cálculo do logaritmo discreto. A utilização do logaritmo discreto irá propiciar, entre outras coisas, a quebra de sistemas critptográficos, como o RSA [3].

Outra vantagem de se utilizar os computadores quânticos, se refere às chamadas *buscas quânticas*, que utilizam técnicas baseadas no algoritmo de Grover [10] e apresentam ganho quadrático de tempo em relação aos melhores algoritmos clássicos. Com o algoritmo quântico de busca será possível, por exemplo, acelerar o processo para se encontrar o elemento mínimo em um conjunto de dados

Tabela 1.1: Evolução dos sistemas quânticos.

Ano	*Acontecimento*
1973	Charles Bennet, comprova a possibilidade da computação reversível [4].
1980	É proposto o computador quântico por Paulo Benioff, tendo o trabalho de Bennet como base [5].
1984	Bennet e Gilles Brassard descobrem o protocolo de criptografia quântica BB84 [6].
1985	David Deutsch cria o primeiro algoritmo quântico [7, cap 1].
1993	O teleporte quântico é proposto por Charles Bennett e colaboradores [8].
1994	Peter Shor cria o algoritmo de fatoração [9].
1994	Lov Grover cria o algoritmo de busca [10].
1996	A IBM demonstra o BB84 de Bennet experimentalmente, utilizando fótons e enviando por fibras comerciais de telecomunicações.
1997	Neil Gershenfeld e Isaac Chuang descobrem os estados pseudo-puros e dão início à comunicação quântica por ressonância magnética nuclear (RMN) [11].
1998	Demonstração através da computação quântica por RMN dos algoritmos de busca e teletransporte. Implementação de diversas portas lógicas quânticas usando esta teoria.
2001	Demonstra-se o algoritmo de Shor por RMN.
2003	Demonstração de emaranhamento entre os spins do núcleo e de um elétron na mesma molécula combinando-se as técnicas de RMN e ressonância paramagnética eletrônica (RPE).
2004	Um grupo do Instituto de Tecnologia da Georgia consegue transferir informação da matéria para a luz, dando início para o desenvolvimento de redes quânticas em grande escala.
2004	Pesquisadores do instituto Max Planck, na Alemanha, fazem o caminho inverso dos americanos da Georgia e transmitem informação da luz para a matéria.
2007	Cientistas da Universidade de Delaware, nos Estados Unidos, conseguem injetar elétrons com spins polarizados de um lado de um componente de silício, manipular e medir o mesmo spin do outro lado do componente [12].
2007	Cientistas de Harvard descobrem o “q-bit de diamante”, mudando o paradiga, da “fabricação” de um bit quântico, para meramente encontrá-lo na natureza[13].
2007	Cientistas das universidades de Copenhagen e Harvard, demonstram uma teoria para construir um transistor para um computador quântico [14].
2007	Descobre-se que a eficiência energética da fotossíntese depende do efeito de superposição quântico.

desordenados, ou aumentar a velocidade na busca por chaves criptográficas, como aquelas utilizadas no sistema DES [3].

Assim, como um computador clássico é construído a partir de circuitos elétricos, o computador quântico é construído a partir de circuitos quânticos, contendo portas lógicas quânticas, responsáveis pelo carregamento, processamento e manipulação da informação quântica [7]. O *hardware* quântico deve possuir a característica de isolamento entre os q-bits. Estes devem estar isolados do meio e isolados uns dos outros de maneira a minimizar os erros devidos a decoerência. Esta dificuldade é um dos maiores desafios da implementação do hardware quântico, visto que, qualquer alteração de campo magnético, choque de moléculas com o ar pode transformar os q-bits. Dependendo da especificidade desta transformação define-se algumas classes de canais quânticos, entre os quais podemos citar, canal de inversão de bit, canal de inversão de fase, canal de despolarização. Entende-se por ruído quântico todo e qualquer fenômeno de natureza exclusivamente quântica que interfira ou corrompa a informação quântica. A decoerência e as correlações formadas entre o sistema principal e o ambiente, são exemplos de ruído quântico.

Uma maneira comumente adotada para aumentar a confiabilidade de um sistema de informação quântica é a utilização de códigos corretores de erros quânticos. Diversas construções de tais códigos foram propostas, entre as quais destacamos, o código de Shor (proteção contra a inversão de bit e de fase simultaneamente), códigos estabilizadores (equivalentes quânticos dos códigos lineares), códigos convolucionais quânticos [15], códigos BCH quânticos [16], entre outros.

Para diversas aplicações clássicas é desejável que determinados bits da informação sejam mais protegidos que os demais. Isso acontece, por exemplo, em sistemas de conversão A/D, onde os bits mais significativos da transmissão devem ter uma proteção maior. Um outro exemplo consiste na transmissão via Internet, na qual os cabeçalhos das páginas precisam de um grau de proteção maior em relação aos outros dados. A característica de proteção desigual de erros (UEP, do inglês *unequal error protection*) dos códigos corretores de erros clássicos foram primeiramente observadas por Masnick e Wolf [17], em 1967, e desde então diversos pesquisadores apresentaram códigos de bloco [18] [19], convolucionais [20] [21], turbo [22], LDPC [23] com caracaterísticas UEP. Entretanto, a característica UEP de códigos quânticos ainda não foi estudada e constitui o objetivo principal deste trabalho.

1.1 Objetivo e Estrutura da Dissertação

O objetivo principal desta dissertação é demonstrar a existência de códigos de bloco quânticos com características UEP em canais de inversão de bit e canais de inversão de fase.

Este trabalho está organizado em cinco capítulos e dois apêndices.

No **Capítulo 2** será apresentado um material introdutório sobre computação e informação quântica.

No **Capítulo 3** serão mostrados diversos tipos de canais quânticos, os tipos de ruído associados a cada um deles, além das operações quânticas que modelam matematicamente a ação do ruído. Neste capítulo também abordaremos algumas classes de códigos corretores de erros quânticos, seus circuitos codificadores, esquema de decodificação por síndrome, além de um breve resumo sobre códigos estabilizadores.

No **Capítulo 4** se abordará a característica UEP de códigos corretores de erros quânticos. Fixada uma taxa arbitrária proporemos códigos de bloco com características UEP distintas que têm o potencial de servir a diversas aplicações.

No **Capítulo 5** serão apresentadas as conclusões e as perspectivas para trabalhos futuros.

O **Apêndice A** apresenta a demonstração do teorema da codificação quântica.

CAPÍTULO 2

INTRODUÇÃO À INFORMAÇÃO QUÂNTICA

"A teoria do tudo será quântica"
Nielsen

Este capítulo tem por objetivo apresentar um arcabouço matemático necessário para o entendimento da teoria da informação quântica e da teoria da correção de erros quânticos. O material coberto envolve os quatro postulados da mecânica quântica, matriz densidade, o conceito de bit quântico, emaranhamento, portas lógicas quânticas, paralelismo quântico, entre outros. Maiores detalhes sobre estes temas são encontrados em [7] e [24]

2.1 Álgebra Linear - Uma breve Revisão

Nesta subseção introduziremos alguns conceitos de Álgebra Linear, utilizando a notação de Dirac.

Na mecânica quântica o espaço vetorial de interesse é o C^n, composto por todas as n-uplas com componentes complexas. Os vetores deste espaço vetorial, também conhecidos por *ket* na notação de Dirac, são dados por:

$$|\psi\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, \tag{2.1}$$

onde as componentes v_i são números complexos. Definimos $\langle\psi|$ como sendo o *vetor dual* de $|\psi\rangle$, também conhecido por *bra*

$$\langle\psi| = \begin{pmatrix} v_1^* & v_2^* & ... & v_n^* \end{pmatrix}, \tag{2.2}$$

onde o superescrito * indica conjugado complexo. De posse de n vetores linearmente independentes de C^n, $|v_1\rangle, |v_2\rangle, ..., |v_n\rangle$, podemos definir um conjunto de bases, através das quais qualquer outro vetor do espaço vetorial pode ser representado da forma:

$$|v\rangle = \sum_{i=1}^{n} a_i |v_i\rangle, \tag{2.3}$$

onde a_i são números complexos. O *produto interno* entre $|\psi\rangle$ e $|\varphi\rangle$ é definido como a multiplicação do dual do primeiro vetor pelo segundo. A notação utilizada é $\langle\varphi|\psi\rangle$ ou $(|\psi\rangle, |\varphi\rangle)$.

A relação entre dois espaços vetoriais distintos V e W é definida através de um *operador linear* que também pode ser uma aplicação de um espaço vetorial nele mesmo. É matematicamente representado por uma matriz. Dado um operador linear A geralmente escreve-se $A|v\rangle$ para denotar a aplicação do operador A ao vetor $|v\rangle$ de V.

Sendo A uma matriz que representa um operador linear, definimos A^* como sendo o complexo conjugado desta matriz. Definimos também o conjugado hermitiano $A^\dagger$ como sendo o conjugado transposto da matriz A.

Dado um operador A: $V \rightarrow W$ e $|v\rangle$ e $|w\rangle$ vetores de V e W, respectivamente, tais que $|w\rangle = A|v\rangle$, então $\langle w| = \langle v|A^\dagger$. Denotamos o produto interno entre $|\varphi\rangle$ e A$|\psi\rangle$ por $\langle\varphi|A|\psi\rangle$.

Um operador linear pode também ser decomposto na multiplicação de um vetor $|\varphi\rangle$ pelo dual de um segundo vetor $|\psi\rangle$. Essa representação é conhecida como produto externo entre $|\varphi\rangle$ e $|\psi\rangle$:

$$A = |\varphi\rangle\langle\psi|. \tag{2.4}$$

Dado um operador linear representado por uma matriz A, denota-se o traço de A por Tr(A). Relacionando o traço com o produto interno temos

$$\text{Tr}(|\varphi\rangle\langle\psi|) = \langle\varphi|\psi\rangle. \tag{2.5}$$

Define-se *norma* de um vetor como sendo a raiz quadrada do produto interno dele com o seu dual:

$$\||\psi\rangle\| \equiv \sqrt{\langle\psi|\psi\rangle} = \sqrt{\text{Tr}(|\psi\rangle\langle\psi|)}. \tag{2.6}$$

Uma outra relação entre vetores é o *produto tensorial*. Dado dois vetores $|\varphi\rangle$ e $|\psi\rangle$, seu produto tensorial é representado por $|\varphi\rangle \otimes |\psi\rangle$ ou $|\varphi\rangle|\psi\rangle$.

Exemplo 1. *Dado os vetores:*

$$|\varphi\rangle = \begin{pmatrix} 1 \\ \imath \end{pmatrix} \quad |\psi\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{2.7}$$

o produto interno é:

$$\langle\varphi|\psi\rangle = \begin{pmatrix} 1 & -\imath \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1 - \imath, \tag{2.8}$$

O produto externo é:

$$|\varphi\rangle\langle\psi| = \begin{pmatrix} 1 & 1 \\ \imath & \imath \end{pmatrix}. \tag{2.9}$$

Por último, o produto tensorial é dado por:

$$|\varphi\rangle \otimes |\psi\rangle = \begin{pmatrix} 1 \\ 1 \\ \imath \\ \imath \end{pmatrix}. \tag{2.10}$$

Teorema 1 (Relação de Clausura)**.** *Sendo I a matriz identidade, $|v\rangle$ um vetor do espaço vetorial V de dimensão d, e $|0\rangle, |1\rangle ... |d-1\rangle$ uma base deste espaço vetorial, então $\sum_{i=0}^{d-1} |i\rangle\langle i| = I$.*

Prova: *Sendo v_i a componente do vetor $|v\rangle$ na direção $|i\rangle$, então $v_i = \langle i|v\rangle$ e portanto, o vetor $|v\rangle$ pode ser representado por:*

$$|v\rangle = \begin{pmatrix} \langle 0|v\rangle \\ \langle 1|v\rangle \\ \vdots \\ \langle d-1|v\rangle \end{pmatrix}. \tag{2.11}$$

Desta forma, como $\langle i|v\rangle$ é um escalar

$$|v\rangle = \sum_i v_i|i\rangle = \sum_i (\langle i|v\rangle)|i\rangle = \sum_i |i\rangle(\langle i|v\rangle) = \sum_i (|i\rangle\langle i|)|v\rangle, \tag{2.12}$$

o que implica

$$\sum_i |i\rangle\langle i| = I. \tag{2.13}$$

Pode-se decompor um operador linear através de sua representação em produto externo, utilizando a relação de clausura. Seja A uma operação de W em V, $\{w_j\}$ as bases de W e $\{v_i\}$ as bases de V, então

$$\begin{aligned} A &= IAI; && (2.14)\\ &= (\sum_j |w_j\rangle\langle w_j|)A(\sum_i |v_i\rangle\langle v_i|); && (2.15)\\ &= \sum_{ij} |w_j\rangle(\langle w_j|A|v_i\rangle)\langle v_i|; && (2.16)\\ &= \sum_{ij} (\langle w_j|A|v_i\rangle)|w_j\rangle\langle v_i|. && (2.17) \end{aligned}$$

Existem algumas classes especiais de operadores lineares. Um operador é dito ser um operador normal se satisfizer a relação $AA^\dagger = A^\dagger A$. Se além de normal o operador satisfizer $AA^\dagger = I$, dizemos que este é um operador unitário. Uma característica de operadores unitários para a mecânica quântica é o fato de que preservam o produto interno entre os vetores:

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|I|w\rangle = \langle v|w\rangle. \tag{2.18}$$

Um operador é dito ser positivo se para qualquer vetor $|v\rangle$ do espaço vetorial, $\langle v|A|v\rangle$ é um número real não negativo. Operadores positivos possuem autovalores positivos. Existe uma maneira alternativa para representar um operador normal, dada pelo *teorema da decomposição espectral*. Antes de enunciar o teorema, introduziremos alguns conceitos a seguir.

Definição 1 (Operador Diagonalizável)**.** *Para um operador linear $A : V \mapsto W$, seja $|0\rangle, |1\rangle, ...|d-1\rangle$ um conjunto de autovetores deste operador cujos respectivos autovalores são $\lambda_0, \lambda_1, ..., \lambda_{d-1}$. Dizemos que este operador é* diagonalizável*, podendo ser escrito na* forma diagonal $A = \sum_{i=0}^{d} \lambda_i |i\rangle\langle i|$*, se os autovetores formarem uma base deste espaço vetorial.*

Para ilustrar um operador diagonalizável vamos decompor as matrizes identidade (I) e a matriz de Pauli (Z) em suas respectivas formas diagonais:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{2.19}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{2.20}$$

onde

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.21}$$

Bases ortonormais de um espaço vetorial V de dimensão d podem ser encontradas pelo *processo de Gram-Schmidt*, que constrói um conjunto de vetores de base $\{|v_i\rangle\}$ a partir de um conjunto de vetores qualquer $\{|w_i\rangle\}$, não necessariamente ortonormais. Define-se um vetor inicial da base ortonormal como sendo $|v_1\rangle = \frac{|w_1\rangle}{\||w_1\|}$. A partir de $|v_i\rangle$ realiza-se $d-1$ iterações através da fórmula:

$$|v_{k+1}\rangle \equiv \frac{|w_{k+1}\rangle - \sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle}{\||w_{k+1}\rangle - \sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle\|}. \tag{2.22}$$

Definição 2 (Projetores)**.** *Seja* V *um espaço vetorial de dimensão d, e W um subespaço vetorial de V com dimensão k. Através do processo de Gram-Schmidt é possível construir uma base ortonormal $|0\rangle, |1\rangle ... |d-1\rangle$ de V, em que $|0\rangle, |1\rangle ... |k-1\rangle$ é uma base ortonormal de W. Desta forma define-se:*

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i|, \tag{2.23}$$

como sendo o projetor de V sobre W.

O operador $Q = I - P$ é o complemento ortogonal de P. Temos como conseqüência imediata da definição de projetores, o Teorema 2.

Teorema 2. *Seja P um projetor do espaço vetorial V no subespaço W, então $P^n = P$.*

Prova: *Escreve-se P^n como*

$$P^n \equiv P \times P \times \ldots \times P; \tag{2.24}$$

$$= \sum_i |v_i\rangle\langle v_i| \sum_j |v_j\rangle\langle v_j| ... \sum_n |v_n\rangle\langle v_n|; \tag{2.25}$$

$$= \sum_{i,j,\ldots,n} |v_i\rangle\langle v_i|v_j\rangle\langle v_j| ... |v_n\rangle\langle v_n|. \tag{2.26}$$

Como $\langle v_i|v_j\rangle = \delta_{i,j}$, então todos os termos tais que $i \neq j$ em (2.26) são iguais a zero de forma que esta equação se reduz a

$$P^n = \sum_i |v_i\rangle(\langle v_i|v_i\rangle\langle v_{i+1}|v_{i+1}\rangle \ldots)\langle v_i|. \tag{2.27}$$

O termo entre parênteses é igual a 1, logo

$$P^n = \sum_i |i\rangle\langle i| = P. \tag{2.28}$$

Podemos agora enunciar o *teorema da decomposição espectral*, cuja prova pode ser encontrada em [7] .

Teorema 3 (Teorema da Decomposição Espectral)**.** *Todo e qualquer operador N de um espaço vetorial V é normal se e somente se for diagonal em relação a alguma base ortonormal de V.*

2.2 A Física e a Informação

É comum estudar a física, a teoria da informação e a teoria da computação sem perceber a correlação entre as mesmas. Rolf Landauer foi quem primeiro chamou a atenção do fato da informação ser algo codificado em um sistema físico, enquanto a computação é algo a ser executado sobre um objeto fisicamente realizável, ou seja, ambos estão diretamente relacionados a sistemas físicos, e conseqüentemente, estão diretamente relacionados aos diversos processos físicos fundamentais.

Diversas considerações a respeito da implementação em hardware devem ser levadas em consideração, mas vamos num primeiro momento nos ater ao ponto de vista mais abstrato da física e a três resultados recentes: o *Princípio de Landauer*, a *computação reversível* e o *demônio de Maxwell*.

Rolf Landauer, em 1961, se referiu ao apagamento da informação como um processo dissipativo e conseqüentemente irreversível. Um exemplo conhecido que explica o *Princípio de Landauer* [25] é o caso do gás espalhado numa caixa com uma partição. Suponha que o apagamento seja a

movimentação do gás para o lado esquerdo, independente que o estado inicial seja o lado direito ou o esquerdo. Num instante de tempo qualquer retiramos a partição e começamos a comprimir o gás com um pistão até que o mesmo esteja por completo do lado esquerdo. Pelo *Princípio de Landauer*, esta compressão reduzirá a entropia do gás de ΔS = $\kappa \ln 2$, onde κ é constante de Boltzman. Para um processo isotérmico a temperatura T o trabalho que devemos fornecer à caixa para realizar o apagamento é W = $\kappa T \ln 2$.

O *Princípio de Landauer* apenas estabelece uma cota inferior para a quantidade de energia que deve ser gasta para que se apague um bit de informação. Os *hardwares* clássicos implementados atualmente encontram-se relativamente próximos desta cota. Na geração atual, um apagamento de uma unidade lógica elementar requer cerca de $500\kappa T \ln 2$ de energia.

Um problema futuro de implementação a ser resolvido, caso os computadores continuem a diminuir de tamanho, é se aproximar cada vez mais do limite de Landauer, evitando assim que os componentes se fundam. Desta forma uma saída viável seria a *computação reversível*.

Realizando a computação de maneira reversível o *Princípio de Landauer* implicaria na inexistência de um limite inferior, visto que não haveria apagamento de informação, pois nenhum bit seria destruído, já que neste tipo de computação é possível saber quais as entradas do sistema a partir de suas saídas.

Para entender melhor o conceito de *reversibilidade* podemos tomar como exemplo as portas lógicas NAND (duas entradas) e NOT. No caso da primeira, se o bit de saída for "1" sabe-se apenas que uma das entradas estava no nível lógico "0", podendo a outra entrada está tanto no nível "1", quanto no "0". Portanto, o sinal de saída não especifica por completo a entrada do sistema, e conseqüentemente, se trata de uma porta lógica irreversível. O mesmo não ocorre para a porta NOT, cuja saída especifica por completo a entrada. No caso das portas irreversíveis fica claro que parte da informação de entrada foi perdida, ou seja, ocorreu o apagamento de pelo menos um bit de informação de entrada e conseqüentemente necessitamos de no mínimo W = $\kappa T \ln 2$ para operar estas portas.

Coube a Charles Bennett [4] mostrar que todo e qualquer tipo de computação pode ser realizado de forma reversível, não existindo apagamento, e por conseguinte dissipação. Citamos anteriormente a porta NAND como uma lógica irreversível, entretanto a mesma pode ser implementada utilizando-se a porta Toffoli, exemplificada abaixo:

$$(a, b, c) \longrightarrow (a, b, c \oplus a \wedge b), \tag{2.29}$$

onde a, b e c representam as entradas da porta, $\oplus$ representa a operação "ou-exclusivo" e o símbolo $\wedge$ representa a operação AND. Pode-se mostrar que as lógicas da porta NAND e da porta Toffoli são

idênticas.

O último dos três resultados desta seção é o paradoxo físico representado pelo *demônio de Maxwell*. O demônio representa um minúsculo ser inteligente capaz de observar o estado microscópico de um sistema físico e aproveitar a ocorrência de flutuações favoráveis para diminuir a entropia deste sistema. Para explicar melhor este paradoxo, utilizemos as palavras do próprio Maxwell:

"Mas se concebermos um ser cujas faculdades são tão aguçadas que ele consegue acompanhar cada molécula em seu curso, tal ser, cujos atributos são ainda essencialmente tão finitos quantos os nossos, seria capaz de fazer o que atualmente nos é impossível fazer. Pois vimos que as moléculas em um recipiente cheio de ar a uma temperatura uniforme movem-se com velocidades que não são de modo algum uniformes. Suponhamos agora que tal recipiente é separado em duas porções, A e B, por meio de uma divisória no qual há um pequeno orifício, e que um ser, que pode ver as moléculas individuais, abre e fecha este orifício, de forma a permitir que somente as moléculas mais rápidas passem de A para B, e somente as mais lentas passem de B para A. Ele irá portanto, sem gasto de trabalho, elevar a temperatura de B e abaixar a de A, em contradição à segunda lei da termodinâmica."

Inúmeros físicos se debateram tentando responder esta possibilidade. Leo Szilard sugeriu que a queda de entropia do gás seria compensada por um aumento de entropia na cabeça do demônio. Brillouin e Gabor argumentaram que a medição que o demônio faz da posição de uma molécula levaria a um aumento compensatório de entropia (a absorção de um fóton dissipa energia). Para Charles Bennett, tendo o demônio uma capacidade de memória finita em determinado momento seria necessário apagar uma determinada quantidade de informação para se armazenar novas informações, neste momento se pagaria pelo esfriamento obtido, ou seja, o apagamento que dissiparia a informação e não a observação. Esta tese defendida por Bennett é hegemônica na atualidade, apesar de ainda existirem defensores de Brilloin.

2.3 A Mecânica Quântica

Entende-se por mecânica quântica uma estrutura matemática para o desenvolvimento da teoria quântica. A física quântica utiliza a mecânica quântica para explicar a natureza (da mesma forma que a física clássica, utiliza o cálculo diferencial para explicar a natureza). Logo a mecânica quântica não fornece necessariamente um conjunto de leis que um determinado sistema físico deve seguir, mas fornece toda base matemática para o desenvolvimento de tais leis. Os efeitos da física quântica são

fortemente evidenciados para escala molecular, atômicas e subatômicas. Na escala macroscópica, aquela do nosso cotidiano, a física quântica reproduz os resultados e previsões da física clássica.

O "mundo quântico" é uma representação de um mundo onde não vigoram as leis do mundo macroscópico, leis as quais, todo ser humano está habituado e tão bem definido pela física newtoniana. De uma maneira geral podemos dizer que o mundo deixa de ser determinístico e passa a ser regido por um conjunto de probabilidades.

Considere, por exemplo, um sistema quântico representado por um átomo que pode ou não emitir um elétron. Pensando classicamente diríamos que existem dois estados possíveis: o estado |com emissão$\rangle$ e o estado |sem emissão$\rangle$. Experimentalmente é possível demonstrar que em um determinado intervalo de tempo teremos uma probabilidade de 0,5 de emissão de um elétron. Desta forma de acordo com a física quântica, neste instante de tempo específico, o sistema não estaria nem no estado |com emissão$\rangle$, nem no estado |sem emissão$\rangle$ e sim numa *superposição*. Denotando este estado superposto por $|\psi\rangle$, dizemos que o sistema encontra-se no estado $|\psi\rangle = \sqrt{0,5}|$com emissão$\rangle + \sqrt{0,5}|$sem emissão$\rangle$. Os estados |com emissão$\rangle$ e |sem emissão$\rangle$ formam uma base do sistema quântico representado por este átomo e seus elétrons emitidos.

Erwin Schrödinger utilizou este caso da emissão radioativa para criar um exemplo mundialmente conhecido como o *gato de Schrödinger*. Sua idéia inicial ao criar este exemplo foi tentar mostrar a falta de completude da teoria quântica. Schrödinger imaginou a situação em que o mesmo sistema de emissão radioativa estivesse presente no interior de uma caixa preta juntamente com um gato, um contador Geiger, um martelo e um frasco de vidro com gás venenoso, de maneira que o contador ao detectar a emissão acionaria o martelo que quebraria o frasco. Schrödinger ressalta o fato de que o aparelho deve estar protegido contra uma intervenção direta por parte do gato.

Este novo sistema classicamente apresentaria dois estados possíveis que chamaremos $|vivo\rangle$ e $|morto\rangle$ em alusão a morte certa do gato no momento em que o gás é liberado. No mundo macroscópico a morte do gato tem probabilidade igual a 50% de ocorrer, e podemos, mesmo sem abrir o interior da caixa, verificar se o gato encontra-se vivo ou morto. Para Schrödinger, isto mostrava que a mecânica quântica não podia ser uma teoria completa, já que não faz sentido supor que o gato está vivo e morto ao mesmo tempo.

Pensando quanticamente, nenhuma das duas possibilidades $|vivo\rangle$ ou $|morto\rangle$ tem probabilidade de concretização a menos que seja *observada* e portanto não podemos dizer se o gato morreu ou sobreviveu sem ao menos que se abra a caixa para descobrir o "estado" do gato. O gato estará numa espécie de "limbo", nem $|morto\rangle$, nem $|vivo\rangle$ até que se abra a caixa. Com o tempo pôde-

se responder melhor a dúvida de Schrödinger, pois o estado $|\psi\rangle = \sqrt{0,5}|vivo\rangle + \sqrt{0,5}|morto\rangle$ é possível, entretanto, trata-se de um estado extremamente instável e por isso raramente visto.

2.3.1 O Bit Quântico

No mundo da informação clássica, o bit é a unidade de informação básica e pode assumir os valores "0" e "1". Analogamente a unidade fundamental da informação quântica é o bit quântico ou q-bit. Matematicamente o q-bit é representado por um vetor complexo no espaço bidimensional com produto interno (espaço de Hilbert). Chamaremos os vetores que compõem a base deste estado de $|0\rangle$ e $|1\rangle$. O estado de um q-bit é portanto uma combinação linear destes estados:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.30}$$

onde $\alpha^2 + \beta^2 = 1$, com α e β pertencentes ao corpo dos números complexos. Equivalentemente, representa-se matricialmente o estado de um q-bit:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{2.31}$$

Uma base alternativa para representar um q-bit é a chamada base conjugada definida por:

$$|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \tag{2.32}$$

Qualquer estado da forma $\alpha|0\rangle + \beta|1\rangle$ pode ser representado em função da base $|\pm\rangle$, visto que:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle. \tag{2.33}$$

Observe que no caso clássico é possível determinar o estado de um bit. Computadores clássicos sempre fazem isso ao recarregarem uma memória, verificando se cada bit está no estado "0" ou no estado "1". No caso do bit quântico encontraremos o valor $|0\rangle$ com probabilidade α^2 e o valor $|1\rangle$ com probabilidade β^2. A mecânica quântica nos ensina que não é possível determinar os valores de α e β, visto que qualquer medida realizada neste intuito fará o sistema representado pelo q-bit "colapsar" para um outro estado. Entretanto é possível manipular e transformar os estados de um q-bit de modo a conduzir a resultados de medidas que dependam tão somente de diferentes estados. Em resumo, ao medir um q-bit poderemos obter apenas "0" ou "1" probabilisticamente.

Uma representação geométrica para o espaço de Hilbert representado por um q-bit é a *Esfera de Bloch*, mostrada na Figura 2.1. Na esfera de Bloch, os ângulos θ e φ definem um possível estado

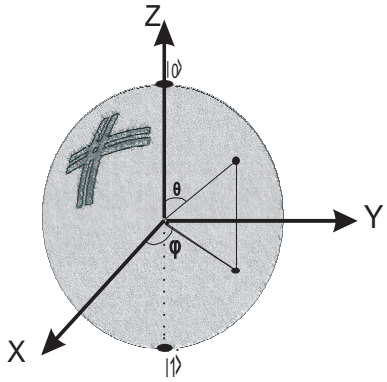

Figura 2.1: A Esfera de Bloch.

para o q-bit. Desta forma reescrevemos a equação (2.30) como:

$$|\psi\rangle = \exp(\imath\gamma)\left[\cos\frac{\theta}{2}|0\rangle + \exp(\imath\varphi)\sin\frac{\theta}{2}|1\rangle\right]. \tag{2.34}$$

Fisicamente o valor $\exp \imath\gamma$ não é observável e portanto torna-se irrelevante, fazendo (2.34) se reduzir a:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \exp(\imath\varphi)\sin\frac{\theta}{2}|1\rangle. \tag{2.35}$$

A *Esfera de Bloch* é uma ótima ferramenta para se visualizar um q-bit, entretanto não existem generalizações para múltiplos q-bits, tornando esta análise ainda mais abstrata para estes casos.

Entre várias implementações possíveis de um q-bit, podemos citar:

- ▷ O alinhamento de um spin de um elétron de um átomo qualquer em relação a um campo magnético externo.
- ▷ O alinhamento de um spin nuclear em relação ao campo magnético também nuclear.
- ▷ Duas diferentes polarizações de um fóton.
- ▷ Estados eletrodinâmicos de circuitos supercondutores.
- ▷ Polarização de fótons com interações via cavidade óptica.
- ▷ Estado do spin nuclear em polímeros [11].

2.3.2 Múltiplos q-bits

Suponha um sistema composto por dois q-bits. Uma base computacional possível para este espaço de Hilbert é $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$. Um par de q-bits pode existir como uma superposição destes

quatro estados, logo o vetor estado que o descreve pode ser escrito como:

$$|\psi\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle. \tag{2.36}$$

Matematicamente, representamos um estado de um sistema de múltiplos q-bits por um vetor em um espaço de 2^n dimensões, ou seja, o produto tensorial de n espaços. Um vetor geral para representar um estado de um sistema de n q-bits é:

$$|\psi\rangle = \sum_{x=0}^{2^n-1} a_x|x\rangle. \tag{2.37}$$

A Equação (2.37) mostra uma representação do princípio da superposição, onde o estado $|\psi\rangle$ é uma combinação linear das bases $|x\rangle$ do sistema quântico em questão. Os coeficientes a_x são números complexos tais que:

$$\sum_x |a_x|^2 = 1. \tag{2.38}$$

2.3.3 Os Postulados da Mecânica Quântica

A teoria quântica pode ser desenvolvida baseada em quatro postulados básicos. Tais postulados fornecem a base para a computação e informação quântica, descrevendo por completo qualquer sistema físico. O primeiro postulado define o tipo de espaço no qual se enquadra o sistema quântico.

Postulado 1 [Espaço de estados]. *Associado com qualquer sistema quântico, existe um espaço vetorial complexo com produto interno, com seqüência de Cauchy e que são covergentes (Espaço de Hilbert) chamado de espaço de estados. O estado do sistema quântico é um vetor unitário neste espaço de estados.*

O q-bit descrito anteriormente representa o sistema quântico mais simples. Sendo $|0\rangle$ e $|1\rangle$, bases deste espaço de Hilbert, o estado $|\psi\rangle = a|0\rangle + b|1\rangle$, satisfaz a condição $\langle\psi|\psi\rangle = 1$, uma vez que $|a|^2 + |b|^2 = 1$. O segundo postulado é responsável por descrever a lei de evolução temporal de um sistema quântico.

Postulado 2 - [A dinâmica do Sistema]. *A evolução de um sistema quântico isolado do meio é representada por uma transformação unitária, ou seja, se $|\psi\rangle$ é o estado do sistema em t_1, $|\varphi\rangle$ o estado do sistema em t_2 e U é um operador unitário que relaciona os dois estados, então*

$$|\varphi\rangle = U|\psi\rangle. \tag{2.39}$$

No Postulado 1, vimos que a mecânica quântica não diz qual o espaço de estados de um sistema. Para o Postulado 2 este raciocínio é análogo visto que ela também não diz quais operadores U descrevem sua dinâmica. No caso de um q-bit, qualquer operador unitário U pode ser implementado. Portas lógicas quânticas são exemplo de operadores unitários. Existem momentos em que torna-se necessário *observar* o sistema. A observação não é necessariamente descrita por uma transformação unitária.

Postulado 3 [Medições]. *Medições quânticas são descritas por uma coleção M_m de operadores de medição. Estes são operadores atuantes no espaço de estados do sistema que está sendo medido. O índice m refere-se aos resultados da medição que podem ocorrer no experimento. Se o estado do sistema quântico imediatamente antes da medição é $|\psi\rangle$, então a probabilidade do resultado m ocorrer é dada por:*

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{2.40}$$

O estado do sistema após a medida será:

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}, \tag{2.41}$$

Os operadores de medição satisfazem a relação de clausura $\sum_m M_m^\dagger M_m = I$, que expressa também o fato da soma das probabilidades ser igual a 1:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{2.42}$$

Observa-se que o ato de medir irá perturbar ou colapsar o sistema para um determinado estado. Esta pertubação está relacionada com a aleatoriedade quântica. A medida possui em si um elemento aleatório que não permite que determinemos o resultado do sistema a partir do resultado da medida. Ninguém sabe ao certo porque este colapso acontece ao se realizar a medida.

Para um sistema de um q-bit definimos os operadores de medida:

$$M_0 = |0\rangle\langle 0| \quad M_1 = |1\rangle\langle 1|. \tag{2.43}$$

Suponha que o estado a ser medido é $|\psi\rangle = a|0\rangle + b|1\rangle$. Para o caso de um q-bit, a probabilidade de se obter 0 na primeira medida é:

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2. \tag{2.44}$$

Seguindo o mesmo raciocínio obtemos p(1) = $|b|^2$. Portanto, de acordo com (2.41) o estado final do q-bit em cada caso será:

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle, \tag{2.45}$$

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle. \tag{2.46}$$

Os termos $\frac{a}{|a|}$ e $\frac{b}{|b|}$ são chamados de fatores de fase globais, possuem módulo 1 e não interferem na estatística, portanto podem ser ignorados.

Um resultado interessante diz respeito a medida de dois q-bits. Suponha um par de q-bits no estado descrito por (2.36). Medindo o primeiro q-bit, por exemplo, obteremos 0 com probabilidade $a_0^2 + a_1^2$. Ocorre então uma renormalização do estado do sistema, sendo o estado após esta primeira medição igual a:

$$|\psi\rangle = \frac{a_0|00\rangle + a_1|01\rangle}{\sqrt{a_0^2 + a_1^2}}. \tag{2.47}$$

Realizando uma segunda medição no segundo q-bit, obteremos 0 com probabilidade $\frac{a_0^2}{a_0^2+a_1^2}$ e o próximo estado será

$$|\psi\rangle = \frac{\frac{a_0^2}{a_0^2+a_1^2}}{|\frac{a_0^2}{a_0^2+a_1^2}|}|00\rangle. \tag{2.48}$$

Ignorando o fator de fase global obteremos $|\psi\rangle = |00\rangle$.

Teorema 4 (Distinguibilidade entre Estados Quânticos)**.** *Apenas estados quânticos ortogonais podem ser perfeitamente distinguidos entre si.*

Prova: *Suponha que um transmissor e um receptor possuem um conjunto de n estados $\{|\psi_k\rangle\}$ de conhecimento de ambos. O transmissor após escolher um $|\psi_k\rangle$ tal que $(1 \leq k \leq n)$ e o envia pelo canal. Utilizando o Postulado 3, caso o conjunto de estados $\{|\psi_k\rangle\}$ seja ortonormal é possível distinguir os estados entre si utilizando operadores de medida M_k na forma:*

$$M_k \equiv |\psi_k\rangle\langle\psi_k|. \tag{2.49}$$

Para garantir a relação de clausura definimos também um operador M_0 como:

$$M_0 = \sqrt{I - \sum_{k \neq 0} |\psi_k\rangle\langle\psi_k|}. \tag{2.50}$$

Utilizando tais operadores, ao se preparar um estado $|\psi_k\rangle$ teremos para $j \neq k$:

$$p(j) = \langle\psi_k|M_j|\psi_k\rangle = 0, \tag{2.51}$$

$$p(k) = \langle\psi_k|M_k|\psi_k\rangle = 1, \tag{2.52}$$

o que nos dá a certeza que o índice k ocorreu. Por outro lado, caso o conjunto de estados $\{|\psi_k\rangle\}$ não sejam ortonormais o conjunto de probabilidades descritos em (2.51) e (2.52) retornará mais de um valor de $p(i) \geq 0$, para $(1 \leq i \leq n)$, pois o estado $|\psi_k\rangle$ terá componentes não nulas decompostas em diversas componentes não ortogonais.

O quarto postulado trata da relação entre dois ou mais sistemas simples que podem se unir para formar um sistema maior. O espaço de estado do sistema composto será formado pelo espaço de estados dos sistemas individuais.

Postulado 4 [Sistemas Compostos]. *O espaço de estados de um sistema quântico composto é o produto tensorial dos espaços de estados dos sistemas físicos componentes. Desta forma, se os sistemas são numerados de 1 a n e o sistema número i está preparado no estado $|\psi_i\rangle$, então o estado total do sistema é dado por $|\psi_1\rangle| \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.*

Para o exemplo de espaço de Hilbert formado por dois q-bits, temos: $|00\rangle = |0\rangle \otimes |0\rangle, |01\rangle = |0\rangle \otimes |1\rangle, |10\rangle = |1\rangle \otimes |0\rangle, |11\rangle = |1\rangle \otimes |1\rangle$.

Aplicar um operador unitário U ao primeiro q-bit, equivale a aplicar $U \otimes I$ ao sistema composto. No caso de múltiplos q-bits podem ocorrer estados que não podem ser escritos como produto tensorial de estados de um q-bit. O Postulado 4 e o princípio da superposição de estados quânticos permitem a consideração de estados de sistemas compostos da forma:

$$|\psi_1\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.53}$$

Estados desse tipo possuem propriedades notáveis e constituem um tipo de recurso computacional inteiramente novo e de natureza exclusivamente quântica, são conhecidos como *estados emaranhados* e serão melhor definidos mais adiante.

2.3.4 Medições Projetivas

Um importante caso especial do Postulado 3 são as medições projetivas, pois são de grande interesse para a decodificação quântica. Por definição, a medida projetiva é descrita por um observável M, que opera no espaço de estados do sistema a ser observado. A decomposição espectral de M é

$$M = \sum_m m P_m, \tag{2.54}$$

onde m são os possíveis resultados da medida e correspondem aos autovalores m do observável, assim como, P_m é o projetor sobre o auto-espaço de M de autovalor m.

Utilizando o Postulado 3 e Teorema 2, temos que a probabilidade de se obter o resultado m é dada por

$$p(m) = \langle\psi|P_m|\psi\rangle. \tag{2.55}$$

Ao se obter o resultado m, logo após a medida o novo estado $|\psi'\rangle$ do sistema será

$$|\psi'\rangle = \frac{P_m|\psi\rangle}{\sqrt{p(m)}}. \tag{2.56}$$

Vale ressaltar o fato dos projetores P_m, serem projetores ortonormais. Esta característica, juntamente com a distinguibilidade de estados quânticos (Teorema 4) é que tornará possível a decodificação da informação recebida em sistemas de comunicação quântica.

2.3.5 Representação em Matriz Densidade

O não-determinismo da mecânica quântica freqüentemente conduz a situações em que um vetor de estado do sistema não é conhecido, o que nos leva a trabalhar com uma coleção de estados possíveis $\{|\psi_i\rangle\}$ e suas probabilidades de ocorrência $\{p_i\}$. Estes estados, em conjunto com estas probabilidades, formam um *ensemble* estatístico que nos leva naturalmente a definição de *matriz densidade*:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.57}$$

em que $p_i \geq 0$ e $\sum_i p_i = 1$. Dentre as características da matriz densidade, podemos citar:

▷ É um operador positivo:

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i \langle\varphi|\psi_i\rangle\langle\varphi|\psi_i\rangle = \sum_i p_i (\langle\varphi|\psi_i\rangle)^2 \geq 0. \tag{2.58}$$

▷ Seu traço é igual a 1:

$$\text{Tr}(\rho) = \sum_i p_i \text{Tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i \langle\psi_i|\psi_i\rangle = \sum_i p_i = 1. \tag{2.59}$$

Através do traço de ρ^2, podemos saber se um estado é puro ou não. Define-se ρ^2 por:

$$\rho^2 = \sum_i \sum_j p_i p_j |\psi_i\rangle\langle\psi_i||\psi_j\rangle\langle\psi_j| = \sum_i \sum_j p_i p_j \delta_{i,j} |\psi_i\rangle\langle\psi_j| = \sum_i p_i^2 |\psi_i\rangle\langle\psi_i|. \tag{2.60}$$

Logo

$$\text{Tr}(\rho^2) = \sum_i p_i^2 \text{Tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i^2 \leq 1. \tag{2.61}$$

A igualdade será satisfeita se e somente se $p_i = 0$, exceto para um índice i_0 tal que $p_{i_0} = 1$, o que caracteriza um estado puro. Portanto, o estado será puro se $\text{Tr}(\rho^2) = 1$.

Em contrapartida chamaremos de *estado misto* todo estado tal que $\text{Tr}(\rho^2) < 1$. Sendo a evolução de um sistema fechado descrita por um operador linear U, $|\psi_i\rangle$ o estado inicial do sistema e $U|\psi_i\rangle$ o estado após a evolução, a evolução do operador densidade será dada por:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \rightarrow \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = U\rho U^\dagger. \tag{2.62}$$

Para o estado inicial $|\psi_i\rangle$ a probabilidade de se obter m como resultado de uma medida é:

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \text{Tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|). \tag{2.63}$$

Desta forma

$$p(m) = \sum_i p(m|i)p_i = \sum_i p_i \text{Tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|) = \text{Tr}(M_m^\dagger M_m \rho). \tag{2.64}$$

Ocorrendo uma medida com resultado m, então após esta medida, o sistema se encontrará no estado:

$$|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}}, \tag{2.65}$$

e o novo operador densidade será:

$$\rho_m = \sum_i p(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}. \tag{2.66}$$

Como

$$p(i|m) = \frac{p(m,i)}{p(m)} = \frac{p(m|i)p_i}{p(m)}, \tag{2.67}$$

substituindo (2.63) e (2.64) em (2.67) obtemos:

$$p(i|m) = \frac{\text{Tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|)p_i}{\text{Tr}(M_m^\dagger M_m \rho)}. \tag{2.68}$$

Então, substituindo (2.68) em (2.66) resulta em:

$$\rho_m = \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\text{Tr}(M_m^\dagger M_m \rho)} = \frac{M_m \rho M_m^\dagger}{\text{Tr}(M_m^\dagger M_m \rho)}. \tag{2.69}$$

2.3.6 Operador Densidade Reduzido e Traço Parcial

A aplicação mais importante do operador densidade diz respeito a descrição de subsistemas de sistemas quânticos compostos. Para esta análise utilizamos o operador densidade reduzido cuja definição vem atrelada ao conceito de traço parcial. Dado dois sistemas físicos puros A e B, a operação traço parcial sobre B é dada por:

$$\text{Tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2|\text{Tr}_B(|b_1\rangle\langle b_2|), \tag{2.70}$$

onde $|a_1\rangle$ e $|a_2\rangle$ são estados de A e $|b_1\rangle$ e $|b_2\rangle$ de B.

Logo, sendo $\rho^{AB} = \rho^A \otimes \rho^B$ o operador densidade do sistema composto, definimos o operador reduzido para o sistema A por:

$$\rho^A \equiv \text{Tr}_B(\rho^{AB}). \tag{2.71}$$

2.3.7 Entropia de Von Neumann

Na teoria da informação clássica, um importante parâmetro é a entropia de Shannon. Na teoria da informação quântica, temos uma descrição semelhante, onde os operadores densidade substituem as distribuições de probabilidade utilizadas na definição de Shannon. Von Neumann definiu a entropia de uma matriz ρ por:

$$S(\rho) = -\text{Tr}(\rho \log_2(\rho)) = -\sum_i \lambda_i \log_2 \lambda_i, \tag{2.72}$$

onde λ_i são os autovalores de ρ.

2.3.8 O Emaranhamento

O emaranhamento é responsável por diversas aplicações impossíveis de serem realizadas no mundo clássico, bem como pela grande capacidade de processamento dos computadores quânticos.

Dado o estado emaranhado em (2.53) é impossível definir tal estado na forma $|\psi\rangle = |A\rangle \otimes |B\rangle$, onde $|A\rangle$ e $|B\rangle$ são q-bits da forma $|A\rangle = \alpha|0\rangle + \beta|1\rangle$ e $|B\rangle = \delta|0\rangle + \gamma|1\rangle$, pois

$$|\psi\rangle = \alpha\delta|00\rangle + \alpha\gamma|01\rangle + \beta\delta|10\rangle + \beta\gamma|11\rangle. \tag{2.73}$$

Não existe, portanto, um conjunto de valores para α, β, δ e γ, que faça (2.73) se resumir à $(|00\rangle + |11\rangle)/\sqrt{2}$. Calculando a matriz densidade deste estado emaranhado obtemos:

$$\rho = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right); \tag{2.74}$$

$$= \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2}. \tag{2.75}$$

O operador matriz densidade do segundo q-bit (q-bit B) é:

$$\rho^B = \mathrm{Tr}_B(\rho); \tag{2.76}$$

$$= \frac{\mathrm{Tr}_B(|00\rangle\langle 00|) + \mathrm{Tr}_B(|11\rangle\langle 00|) + \mathrm{Tr}_B(|00\rangle\langle 11|) + \mathrm{Tr}_B(|11\rangle\langle 11|)}{2}; \tag{2.77}$$

$$= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2}. \tag{2.78}$$

Desta forma tem-se:

$$\rho^A = \rho^B = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2}. \tag{2.79}$$

Realizando o traço parcial em relação ao primeiro q-bit obteremos o mesmo resultado, que são matrizes que apresentam mistura estatística máxima para cada q-bit ($p_a = \frac{1}{2}$ e $p_b = \frac{1}{2}$). Perceba que individualmente cada q-bit apresenta entropia máxima ($S(\rho^A) = S(\rho^B) = 1$). Aparentemente temos um resultado contraditório visto que se aplicarmos a fórmula da entropia de Von Neumann à (2.75) encontraremos $S = 0$, ou seja, o emaranhamento é caracterizado por duas componentes individuais de entropia máxima que quando formam um sistema composto apresentam entropia zero. Além do estado (2.53) existem ainda outros três estados emaranhados para dois q-bits:

$$|\psi_2\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}; \tag{2.80}$$

$$|\psi_3\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}; \tag{2.81}$$

$$|\psi_4\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.82}$$

Note que $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle$ e $|\psi_4\rangle$ formam uma base no espaço de Hilbert para dois q-bits. Esta base é chamada *base de Bell* ou *pares* EPR, em homenagem aos pioneiros no estudo das propriedades do emaranhamento, Einstein, Podolsky e Rosen. Para maiores informações a respeito do resultado EPR consultar [26] e [27].

Uma outra característica importante do emaranhamento diz respeito ao terceiro postulado. Suponha que se faça uma medida no q-bit $|A\rangle$ de um estado emaranhado, representada por $M_0^A = |0\rangle\langle 0|$ e $M_1^A = |1\rangle\langle 1|$. Supondo que o resultado seja "0", o sistema então colapsa para o estado:

$$|\psi_{M_0}\rangle = \frac{M_0^A|\psi_1\rangle}{\sqrt{\frac{1}{2}}} = |00\rangle. \tag{2.83}$$

O resultado acima é bastante interessante, pois encontrando o resultado do primeiro q-bit, o segundo fica automaticamente determinado. Isto ocorre apenas em estados emaranhados, pois para estados não-correlacionados a medida de um q-bit não interfere no outro q-bit. Esta interferência entre q-bits localizados remotamente é conhecida por *não localidade*. Entre as inúmeras aplicações de estados emaranhados podemos citar o teleporte [7], a codificação superdensa [7] e aplicações à criptografia quântica [28].

2.4 A Informação Quântica

De posse de um arcabouço da mecânica quântica, podemos focar agora no estudo da informação quântica. O termo *informação quântica* engloba todos os meios de processamento da informação através da mecânica quântica.

Inicialmente vamos nos ater a alguns tópicos que evidenciam as diferenças entre a informação quântica e clássica: o *Teorema da Não Clonagem* e a *Desigualdade de Bell*, que trata das correlações não-locais.

Como vimos no Postulado 3, a aleatoriedade quântica implica na destruição do estado quântico. Isto se relaciona com o fato da informação quântica não poder ser copiada com perfeita fidelidade. Este resultado datado de 1982 foi obtido por Wooters, Zurek [29] e Diecks [30] e é conhecido como *Teorema da Não Clonagem*.

Teorema 5 (Teorema da Não Clonagem)**.** *O estado quântico não pode ser copiado.*

Prova: *Suponha que dois q-bits A e B estão nos estados puros $|\psi\rangle$ e $|\sigma\rangle$, respectivamente. O sistema encontra-se, portanto, inicialmente no estado $|\psi\rangle \otimes |\sigma\rangle$. Suponha uma transformação unitária U capaz de realizar a clonagem de um estado, ou seja:*

$$U(|\psi\rangle \otimes |\sigma\rangle) = |\psi\rangle \otimes |\psi\rangle. \tag{2.84}$$

Da mesma forma, se A encontra-se no estado $|\varphi\rangle$:

$$U(|\varphi\rangle \otimes |\sigma\rangle) = |\varphi\rangle \otimes |\varphi\rangle. \tag{2.85}$$

Para

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \quad |\sigma\rangle = \begin{pmatrix} c \\ d \end{pmatrix}, \quad |\varphi\rangle = \begin{pmatrix} e \\ f \end{pmatrix}, \tag{2.86}$$

teremos os produtos tensoriais:

$$|\psi\rangle \otimes |\sigma\rangle = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}, \quad |\varphi\rangle \otimes |\sigma\rangle = \begin{pmatrix} ec \\ ed \\ fc \\ fd \end{pmatrix}, \quad |\psi\rangle \otimes |\psi\rangle = \begin{pmatrix} a^2 \\ ab \\ ab \\ b^2 \end{pmatrix}, \quad |\varphi\rangle \otimes |\varphi\rangle = \begin{pmatrix} e^2 \\ ef \\ ef \\ f^2 \end{pmatrix}.$$

Tomando o produto interno de (2.84) e (2.85), obtemos:

$$\begin{aligned} UU^{\dagger}(aec^2 + aed^2 + bfc^2 + bfd^2) &= a^2e^2 + abef + abef + b^2f^2; && (2.87)\\ (ae)(c^2 + d^2) + (bf)(c^2 + d^2) &= (ae + bf)^2; && (2.88)\\ (ae + bf) &= (ae + bf)^2; && (2.89)\\ \langle\psi|\varphi\rangle &= \langle\psi|\varphi\rangle^2. && (2.90) \end{aligned}$$

Como as soluções de $x = x^2$ são obrigatoriamente $x = 0$ e $x = 1$ então (2.90) também terá como soluções $\langle\psi|\varphi\rangle = 0$ ou $\langle\psi|\varphi\rangle = 1$, ou seja, só é possível copiar estados ortogonais entre si, sendo impossível uma eventual máquina para clonagem geral.

Sabemos que a informação clássica pode ser copiada, já no caso quântico, se fosse possível a cópia perfeita do estado quântico, poderíamos então medir o observável da cópia sem perturbar o estado original violando o Postulado 3 (destruição do estado observado).

A maior diferença entre a informação clássica e quântica reside no conceito de *codificação em correlações não locais.*

A influencia do resultado de uma medida em um q-bit sobre o estado de outro q-bit, como descrito em (2.83), ainda que localizado remotamente em relação ao primeiro é um exemplo da não-localidade.

Coube a John Bell [27], em 1964, descobrir um resultado notável, capaz de decidir em um teste experimental se a não-localidade de fato existe em sistemas quânticos emaranhados. A este resultado chamou-se *Desigualdade de Bell*, que estabeleceu um limite superior para a correlação entre medidas feitas em observáveis de q-bits separados.

Mostrou que todos os prognósticos da mecânica não podem ser reproduzidas por nenhuma teoria de variável escondida local, ou seja, toda informação é codificada em *correlações não locais* entre as diferentes partes de um sistema físico, não havendo qualquer contra-partida clássica para tais correlações.

2.5 Portas Lógicas Quânticas

O processamento da informação quântica é realizado pelos circuitos quânticos através do uso de *portas lógicas quânticas.*

No computador clássico, o exemplo mais simples de uma porta lógica é o inversor. Para um computador quântico, a operação análoga ao inversor é conhecida por *inversão de bit.* A porta lógica quântica irá operar não apenas nos estados $|0\rangle$ e $|1\rangle$ como também nas superposições destes estados. Um modo conveniente de representar o equivalente quântico do inversor lógico é definindo a matriz X como:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.91}$$

Para um estado $|\psi\rangle$ = $\alpha|0\rangle$ + $\beta|1\rangle$, temos o seguinte mapeamento:

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}. \tag{2.92}$$

Portas quânticas de um q-bit são representadas por matrizes 2x2, existindo desta forma uma infinidade de portas deste tipo. Três portas importantes, que podem ser visualizadas na Figura 2.2 são a Y, a Z e a H (operação Hadamard). Nenhuma possui equivalentes clássicos. A porta Z atua invertendo

a fase do sinal e a Hadamard transforma um estado puro em um estado emaranhado. São definidas por:

$$Y = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.93}$$

Um protótipo de porta lógica quântica de vários q-bits é a porta C-NOT ou *NÃO controlada*, que consiste de dois q-bits de entrada denominados por *q-bit de controle* e *q-bit alvo*. O *q-bit de controle* não tem seu estado afetado pela porta, entretanto define a transformação que ocorrerá no *q-bit alvo*. Caso o controle seja $|0\rangle$ nada acontece com o alvo. Se o controle for $|1\rangle$ o alvo é invertido. O mapeamento realizado por uma porta C-NOT é:

$$|00\rangle \mapsto |00\rangle, \quad |01\rangle \mapsto |01\rangle, \quad |10\rangle \mapsto |11\rangle, \quad |11\rangle \mapsto |10\rangle. \tag{2.94}$$

Como existem dois q-bits de entrada, uma possível base para este Espaço de Hilbert é $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$. Utilizando (2.94) chega-se à representação matricial para uma porta C-NOT, visto que $|00\rangle$ e $|01\rangle$ são mapeados neles mesmos, enquanto $|10\rangle$ e $|11\rangle$ são mapeados um no outro, o que nos dá a transformação unitária U_{CN} para a porta C-NOT:

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.95}$$

Para um q-bit de controle $|A\rangle = \alpha|0\rangle + \beta|1\rangle$ e um q-bit alvo $|B\rangle = \delta|0\rangle + \varphi|1\rangle$, temos uma entrada equivalente a $|AB\rangle = \alpha\delta|00\rangle + \alpha\varphi|01\rangle + \beta\delta|10\rangle + \beta\varphi|11\rangle$. Portanto

$$\begin{pmatrix} \alpha\delta \\ \alpha\varphi \\ \beta\varphi \\ \beta\delta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha\delta \\ \alpha\varphi \\ \beta\delta \\ \beta\varphi \end{pmatrix}. \tag{2.96}$$

Através de portas C-NOT, Figura 2.3, e portas de um q-bit de entrada é possível construir qualquer outra porta lógica quântica, ou seja, estas são portas universais.

2.6 Paralelismo Quântico

O fato de avaliar uma função genérica $f(x)$ para diversos pontos x simultaneamente é uma característica de computadores quânticos chamada de *paralelismo quântico*. O paralelismo foi citado

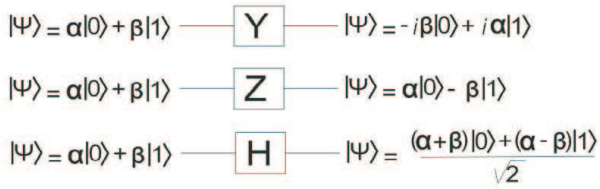

Figura 2.2: Portas lógicas quânticas Y, Z e H.

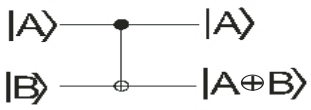

Figura 2.3: Portas lógicas C-NOT.

por David Deutsch [31] como o fenômeno que melhor enfatiza o poder de processamento dos computadores quânticos.

Analisemos a seguir o exemplo de Deutsch. Imagine uma função $f(x)$: {0,1} $\mapsto$ {0,1} de um único bit. Note que $f(0)$ e $f(1)$ podem assumir dois valores cada. Suponha que esta função seja computada por uma caixa preta e que desconhecemos quais das quatro funções possíveis esta sendo executada. Suponha também que o processamento dure cerca de uma hora.

Classicamente precisaríamos de uma hora para calcular o valor de $f(0)$ e mais uma hora para calcular o valor de $f(1)$, ou seja, 2 horas para definir qual das funções possíveis está a ser processada pela caixa. Suponha que tivéssemos uma versão quântica desta caixa preta. Como vimos nos postulados, a ação deste computador quântico deve ser unitária e inversível, ou seja, precisamos de uma função U_f que mapeia dois q-bits em dois q-bits.

Uma maneira possível de implementar a função em um computador quântico seria considerar uma máquina iniciada no estado $|x, y\rangle$ transformando-a mediante portas lógicas em $|x, y \oplus f(x)\rangle$, em que $\oplus$ indica a adição módulo 2, portanto definindo-se a transformação:

$$|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle. \tag{2.97}$$

Este mapeamento irá trocar o segundo q-bit se o primeiro for igual a “1” e preservá-lo caso o primeiro seja igual a “0”. Por se tratar de uma computação quântica, podemos utilizar o princípio da superposição e definir o q-bit alvo como sendo uma superposição de $|0\rangle$ e $|1\rangle$. Suponha então que

seja preparado o estado $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ como alvo e que $|x\rangle$ seja o q-bit de controle. Desta forma

$$U_f : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \mapsto |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |f(x) \oplus 1\rangle = |x\rangle(-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \quad (2.98)$$

Suponha agora que $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. A Equação (2.98) fica da forma:

$$U_f : \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \mapsto \frac{1}{\sqrt{2}}[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle] \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (2.99)$$

Se $f(0) = f(1)$, chamaremos esta função de *função constante*. Para $f(0) \neq f(1)$ a chamamos de *função balanceada*. Realizando uma medição projetiva sobre a base conjugada apenas para o primeiro q-bit $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ obteremos $|+\rangle$ se a função for balanceada ou $|-\rangle$ se for uma função constante, ou seja, com uma única medida é possível extrair uma característica da função que no mundo clássico exigiria duas medidas. Isso só foi possível graças a *superposição* da base $|0\rangle$ e $|1\rangle$, de modo que podemos extrair informação global analisando apenas uma parte do sistema e o grau de dependência desta parte com as informações $f(0)$ e $f(1)$.

O poder do paralelismo quântico é devido ao fato de na mecânica quântica a informação é codificada em correlações não locais. A capacidade de extrair a informação contida neste paralelismo é talvez a grande função do engenheiro para tais sistemas. Como exemplo podemos citar os algoritmos de Deutsch e Deutsch-Jozsa (ver Capítulo 1 de [7]).

CAPÍTULO 3

CÓDIGOS CORRETORES DE ERROS QUÂNTICOS

"Quando ouvi falar sobre o gato de Schrödinger, procurei pela minha arma"
Stephen Hawking

O sucesso da implementação de um computador quântico está associado à minimização dos efeitos do ruído quântico. Este computador deverá ser capaz de corrigir a informação quântica corrompida através do emprego de códigos corretores de erros quânticos (CCEQ). Neste capítulo, apresentaremos as operações quânticas que modelam matematicamente a atuação do ruído quântico. Em seguida, trataremos de conceitos fundamentais relacionados aos CCEQ e das condições necessárias e suficientes para a construção de um CCEQ [32]. Abordaremos a principal classe destes códigos: os códigos estabilizadores, além de exemplos de códigos para alguns tipos de canais quânticos, tais como o código de inversão de bit, código de inversão de fase e o código de Shor [33].

Convém destacar que erros operacionais, intrínsecos a portas lógicas quânticas, não serão abordados neste capítulo. Para o estudo destes, foi desenvolvida a *teoria quântica de tolerância a falhas* [7]. Já os erros de decoerência são protegidos pelos CCEQ, que são mapeamentos de k q-bits em n q-bits, onde $n > k$. Os $n - k$ q-bits adicionais são referentes à redundância adicionada a mensagem aumentando a proteção da mensagem frente a alterações indesejadas por parte do ruído quântico.

3.1 Operações Quânticas

3.1.1 Do Ruído Clássico ao Caso Quântico

Em um canal de comunicação clássico, a probabilidade do bit recebido estar no estado y é dada pela lei da probabilidade total:

$$p(Y = y) = \sum_x p(Y = y|X = x)p(X = x). \tag{3.1}$$

Sejam p_0 e p_1 as probabilidades a priori do bit clássico estar no estado 0 ou 1, respectivamente, e q_0 e q_1 as probabilidades correspondentes após a transmissão. Podemos escrever o sistema com base em (3.1) da forma:

$$\begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}, \tag{3.2}$$

onde p é a probabilidade de erro.

Para sistemas quânticos o raciocínio é análogo, pois estados quânticos são representados pelo operador densidade ρ e a atuação do ruído quântico no estado ρ, quando este é transmitido ao longo de um canal quântico, é representada por um mapeamento $\mathcal{E}$ que relaciona ρ com o estado final ρ' da forma:

$$\rho' = \mathcal{E}(\rho). \tag{3.3}$$

Este mapeamento reflete as mudanças devido à dinâmica do sistema, decorrente de algum processo físico. Tal mapeamento é chamado de *operação quântica*.

Existem diferentes abordagens de compreensão de operações quânticas: sistemas acoplados com a vizinhança, representação de operador-soma, axiomas fisicamente motivados. O primeiro método é baseado na idéia do estudo do sistema com sua vizinhança, traçando um forte paralelo com o mundo clássico e será descrito a seguir.

3.1.2 Sistema Acoplado com a Vizinhança

De acordo com os postulados da mecânica quântica, sabemos que a dinâmica de sistemas quânticos fechados é representada por transformações unitárias. Uma transformação U atuando sobre o estado inicial ρ, faz o sistema evoluir para um estado $U\rho U^\dagger$, como mostrado na Figura 3.1.

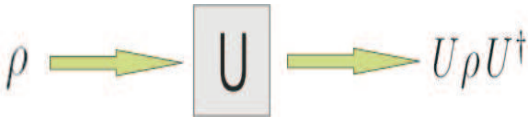

Figura 3.1: Evolução de um sistema quântico fechado.

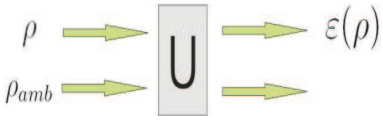

Figura 3.2: Evolução de um sistema quântico aberto.

Descreveremos sistemas quânticos abertos, como a interação do sistema principal com um segundo sistema que chamaremos de *ambiente*, inicialmente no estado ρ_{amb}, de maneira que a união do sistema principal com o ambiente forma um sistema quântico fechado, como ilustrado na Figura 3.2.

Neste modelo, supomos a entrada do novo sistema como sendo $\rho \otimes \rho_{amb}$. Em geral, isto não ocorre devido às constantes interações características de sistemas quânticos, o que leva à formação de correlações devido, entre outras coisas, às trocas de calor entre o sistema principal e o ambiente.

Vimos na Seção 2.3.6 que a operação traço parcial permite obter o operador densidade reduzido. Desta forma, de acordo com a Figura 3.2, o sistema não interage mais com o ambiente após a transformação unitária U e podemos então realizar o traço parcial sobre o ambiente que nos dá o operador densidade reduzido:

$$\mathcal{E}(\rho) = \mathrm{Tr}_{amb}[U(\rho \otimes \rho_{amb})U^{\dagger}]. \tag{3.4}$$

A Equação (3.4) é a definição de operações quânticas para o sistema acoplado com a vizinhança. No caso da transformação U não envolver qualquer interação com o ambiente o mapeamento será da forma:

$$\mathcal{E}(\rho) = \tilde{U}\rho\tilde{U}^{\dagger}, \tag{3.5}$$

onde definimos $\tilde{U}$ como sendo a parte de U que atua somente no sistema principal.

De um modo geral, se uma determinada operação quântica possui k elementos de operação, então:

$$\mathcal{E}(\rho) = \sum_{k} E_k \rho E_k^{\dagger}. \tag{3.6}$$

3.2 Ruído Quântico

O ruído clássico é um sinal aleatório que corrompe o sinal transmitido. Suas causas são as mais diversas possíveis, podendo ser causado por estática, temperatura, campos eletromagnéticos, dependendo do tipo de sistema a que se refere.

Entendemos por ruído quântico todo e qualquer fenômeno de natureza exclusivamente quântica que interfira ou corrompa a informação quântica. A decoerência e as correlações formadas entre o sistema principal e o ambiente, são exemplos de ruído quântico. Apresentaremos a seguir um breve resumo dos canais quânticos mais conhecidos, bem como os elementos de operação que compõem a operação quântica que modela o canal. Neste capítulo, usaremos os operadores X, Y, Z, H que descrevem as portas lógicas descritas na Seção 2.5.

Canal de Inversão de Bit

O canal *canal de inversão de bit* inverte o estado de um q-bit de $|0\rangle$ para $|1\rangle$ e vice-versa com probabilidade $1-p$. Os elementos desta operação são:

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \tag{3.7}$$

$$E_1 = \sqrt{1-p}X = \sqrt{1-p}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{3.8}$$

Desta forma, o estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ é mapeado no estado $|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$. Este canal é o equivalente quântico do canal clássico BSC.

Canal de Inversão de Fase

O canal de inversão de fase é representado pela operação quântica que mapeia q-bit no estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ no estado $|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$ com probabilidade $1-p$. Seus elementos de operação são:

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \tag{3.9}$$

$$E_1 = \sqrt{1-p}Z = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.10}$$

Canal de Despolarização

O canal de despolarização consiste do ruído quântico no qual existe uma probabilidade *p* do q-bit ser despolarizado, ou seja, ser substituído pelo estado $\frac{1}{2}I$. A operação quântica que representa este sistema é:

$$\mathcal{E}(\rho) = \frac{pI}{2} + (1-p)\rho. \tag{3.11}$$

Usando o fato que:

$$\frac{I}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4}, \tag{3.12}$$

e substituindo (3.12) em (3.11) temos:

$$\mathcal{E}(\rho) = (1 - \frac{3p}{4})\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z). \tag{3.13}$$

Portanto, os elementos de operação do canal de despolarização, são $\sqrt{1-3p/4}I$, $\sqrt{p}X/2$, $\sqrt{p}Y/2$ e $\sqrt{p}Z/2$.

3.3 Fidelidade

O conceito de *fidelidade* trata-se de uma medida de distância entre dois estados quânticos e não possui um conceito análogo na teoria da informação clássica.

Definição 3. *A fidelidade entre o estado puro $|\psi\rangle$ e o estado arbitrário ρ, denotado por $F(|\psi\rangle, \rho)$, é definida por:*

$$F(|\psi\rangle, \rho) \equiv \sqrt{\langle\psi|\rho|\psi\rangle}. \tag{3.14}$$

Se nos referimos a uma operação quântica $\mathcal{E}(\rho)$, a fidelidade entre ρ e $\mathcal{E}(\rho)$ medirá o quanto a saída do canal é fiel à entrada. Conseqüentemente, quanto maior o valor da fidelidade menor a distância entre os estados.

3.4 Códigos Corretores de Erros Quânticos

O projeto de um CCEQ leva em consideração as características que envolvem a informação quântica descrita na Seção 2.4. Dentre estas características específicas da informação quântica podemos citar:

1. O canal de inversão de fase não possui equivalente clássico. Logo erros deste tipo, e consequentemente, um código para corrigi-lo também não possuem análogos clássicos.

2. Erros quânticos são contínuos e portanto há, a priori, uma infinidade de erros possíveis.
3. De acordo com o teorema da não clonagem (Seção 2.4, Capítulo 2) não é possível clonar a informação quântica e mesmo se assim fosse possível, o postulado 3 (Seção 2.3.3) não permite medir e comparar estados quânticos. A observação de um estado quântico destrói a informação, o que torna impossível a recuperação do estado inicial.

Para entender o funcionamento de um CCEQ vamos estudar inicialmente os códigos mais simples, como o código de inversão de bit e o de inversão de fase, além do código de Shor, que protege um q-bit contra erros de inversão de bit e de fase, simultaneamente.

3.4.1 Código de Inversão de Bit

Suponha um canal de inversão de bit como visto na Seção 3.2. A seguir, descreveremos as operações de codificação e decodificação de um código específico com capacidade de correção de 1 q-bit neste canal.

Codificação

Para codificarmos um q-bit utilizaremos um procedimento análogo ao código de repetição clássico. Cada estado-base de um q-bit é mapeado em um estado de 3 q-bits, como descrito a seguir:

$$|0\rangle \mapsto |000\rangle, \quad |1\rangle \mapsto |111\rangle, \tag{3.15}$$

em que $|000\rangle$ e $|111\rangle$ são chamados de *estados-base lógicos*. O circuito codificador pode ser visto na Figura 3.3, onde o estado $|\psi\rangle$ representa a informação quântica a ser transmitida.

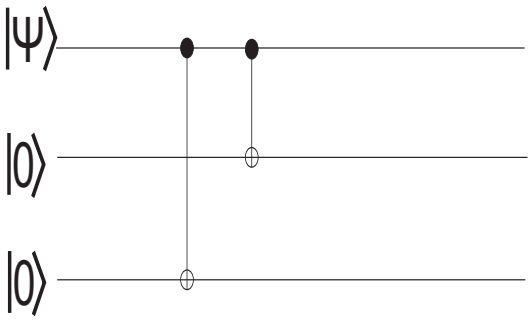

Figura 3.3: Circuito codificador para um código de inversão de bit de 3 q-bits.

Ao inserir redundância por meio de um código quântico mapeia-se o espaço de palavras código em um espaço maior de forma que um eventual erro (corrigível por este código) mapeará o estado

inicial em um estado ortogonal. Vamos supor que o estado $|\psi\rangle = a|0\rangle + b|1\rangle$ foi perfeitamente codificado no estado $|\psi\rangle' = a|000\rangle + b|111\rangle$.

Detecção e Correção de erro

Em princípio temos um problema para detectar um erro, devido à impossibilidade de se medir um q-bit, pois medi-lo significa colapsar o estado para um estado base. Ao se medir $|1\rangle$ teremos preparado o estado $|111\rangle$ e perdido a informação codificada nos coeficientes a e b. A solução para identificar o erro ocorrido é medir o estado quântico dos três q-bits e não de um q-bit individualmente. No caso do canal de inversão de bit existem quatro síndromes, equivalentes a quatro operadores de projeção diferentes (Seção 2, Capítulo 2), as síndromes são os resultados de medições correspondentes ao operador de projeção. Para o nosso exemplo temos:

$$P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|; \tag{3.16}$$

$$P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|; \tag{3.17}$$

$$P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|; \tag{3.18}$$

$$P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|. \tag{3.19}$$

O operador P_0 está associado a uma transmissão sem erros, enquanto P_1, P_2 e P_3 estão associados a inversões no primeiro q-bit, segundo q-bit e terceiro q-bits, respectivamente. Suponha que o estado recebido seja $|\psi\rangle = a|100\rangle + b|011\rangle$, então

$$\langle\psi|P_1|\psi\rangle = (a^*\langle 100| + b^*\langle 011|)(|100\rangle\langle 100| + |011\rangle\langle 011|)(a|100\rangle + b|011\rangle); \tag{3.20}$$

$$\langle\psi|P_1|\psi\rangle = |a|^2\langle 100|100\rangle\langle 100|100\rangle + |b|^2\langle 011|011\rangle\langle 011|011\rangle; \tag{3.21}$$

$$\langle\psi|P_1|\psi\rangle = |a|^2 + |b|^2; \tag{3.22}$$

$$\langle\psi|P_1|\psi\rangle = 1. \tag{3.23}$$

Da mesma maneira $\langle\psi|P_0|\psi\rangle$, $\langle\psi|P_2|\psi\rangle$ e $\langle\psi|P_3|\psi\rangle$ são medições iguais a zero. Então, a medição igual a 1 indica que a síndrome de erro é P_1. A síndrome, entretanto, não altera o estado recebido, este continua a ser $|\psi'\rangle = a|100\rangle + b|011\rangle$. Note também que a síndrome não fornece qualquer informação a respeito de a e b, apenas indica qual erro ocorreu.

Através da síndrome do erro é possível definir o procedimento para recuperar o estado original. No exemplo em que o estado corrompido é $|\psi\rangle = a|100\rangle + b|011\rangle$ a síndrome indica que a recupe-

ração do estado corresponde a inverter o primeiro q-bit. Equivalentemente, a síndrome P_2 equivale a inverter o segundo q-bit e assim sucessivamente. Devemos portanto, aplicar o operador X sobre o q-bit a ser invertido. Usamos a nomenclatura X_i para indicar a atuação do operador X em um q-bit específico, neste caso i assume os valores 1, 2 ou 3. Este procedimento falhará para este caso se ocorrer mais de um erro.

Uma outra possibilidade de detectar o erro no estado recebido é realizar medidas com os observáveis Z_1Z_2 (abreviação para $Z \otimes Z \otimes I$) e Z_2Z_3 ($I \otimes Z \otimes Z$), que possuem como autovalores ± 1. Neste caso, cada medida fornecerá um bit de informação (autovalor) para cada dois q-bits de informação.

A lógica deste processo consiste no fato da medida Z_1Z_2 ser uma forma de comparar os dois primeiros q-bits, tendo +1 como resultado da medida se os q-bits foram iguais e -1 se os q-bits forem diferentes. Da mesma forma Z_2Z_3 compara o segundo e o terceiro q-bit. Esta medida é melhor visualizada através de sua decomposição espectral dos observáveis, onde

$$Z_1Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I; \tag{3.24}$$

$$Z_2Z_3 = I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) - I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|). \tag{3.25}$$

Combinando o resultado de ambas as medidas podemos detectar a síndrome associada ao erro, e consequentemente, o erro ocorrido. Se tanto a medida de Z_1Z_2 quanto a de Z_2Z_3 forem +1 então, a menos que todos os bits quânticos tenham sido invertidos, não ocorreram erros na transmissão. Para uma medida de Z_1Z_2 igual a +1 e Z_2Z_3 igual a -1 então com grande probabilidade ocorreu um erro de inversão de bit no terceiro q-bit. Pode-se também utilizar outros dois conjuntos de observáveis, tais como, $\{Z_1Z_3, Z_2Z_3\}$ e $\{Z_1Z_2, Z_1Z_3\}$.

Uma análise mais precisa envolve uso da fidelidade quântica definida em (3.14). Como os estados quânticos estão em um espaço contínuo, é possível que alguns erros corrompam um estado por uma quantidade muito pequena, enquanto outros erros destruam completamente o estado. Um bom exemplo para visualizar este fato é verificar que o erro de inversão de bit X não afeta o estado $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, enquanto destrói completamente os estados $|0\rangle$ e $|1\rangle$, trocando um pelo outro.

No sistema não codificado, o estado do q-bit após ser enviado por um canal onde a probabilidade de inversão de um q-bit seja p será:

$$\rho = (1-p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X. \tag{3.26}$$

Já a fidelidade será:

$$F = \sqrt{\langle\psi|\rho|\psi\rangle} = \sqrt{(1-p) + p\langle\psi|X|\psi\rangle\langle\psi|X|\psi\rangle}. \tag{3.27}$$

Ambos os termos sob a raiz são não negativos. O segundo termo será igual a zero se $|\psi\rangle = |0\rangle$ e portanto a fidelidade mínima é $F = \sqrt{1-p}$. Aplicando um código de repetição de três q-bits para proteger um estado $|\psi\rangle = a|0\rangle + b|1\rangle$, o estado quântico corrompido após a correção será:

$$\rho = [(1-p)^3 + 3p(1-p)^2]|\psi\rangle\langle\psi| + ... \tag{3.28}$$

Os termos omitidos correspondem a contribuições de inversões de bit em mais de um q-bit. Todos os termos omitidos são operadores positivos e como vimos na Seção 2.1, se A é um operador positivo, então $\langle\psi|A|\psi\rangle$ é não negativo. Logo (3.28) será um limitante inferior da fidelidade, ou seja,

$$F = \sqrt{\langle\psi|\rho|\psi\rangle} \geq \sqrt{(1-p)^3 + 3p(1-p)^2}. \tag{3.29}$$

A fidelidade, portanto, será aumentada quando $p < \frac{1}{2}$.

3.4.2 Código de Inversão de Fase

Seguindo o exemplo anterior para códigos de 3 q-bits, vamos analisar um código de inversão de fase. Neste canal, há uma probabilidade p do q-bit permanecer com seu estado inalterado, e uma probabilidade $1-p$ de ocorrer uma inversão na fase, ou seja, aplicação do operador de inversão de fase Z definido em (2.20) ao q-bit em questão.

Codificação

Aplicando-se o operador Z a um q-bit no estado $a|0\rangle + b|1\rangle$ obtém-se o estado $a|0\rangle - b|1\rangle$. Aplicando o mesmo operador a um sistema na base $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, mapeia-se $|+\rangle$ em $|-\rangle$ e vice-versa, ou seja, atua-se como um canal de inversão de bit. Define-se os estados lógicos como:

$$|0_L\rangle \equiv |+++\rangle, \tag{3.30}$$

e

$$|1_L\rangle \equiv |---\rangle. \tag{3.31}$$

O circuito codificador para o código de inversão de fase pode ser visto na Figura 3.4.

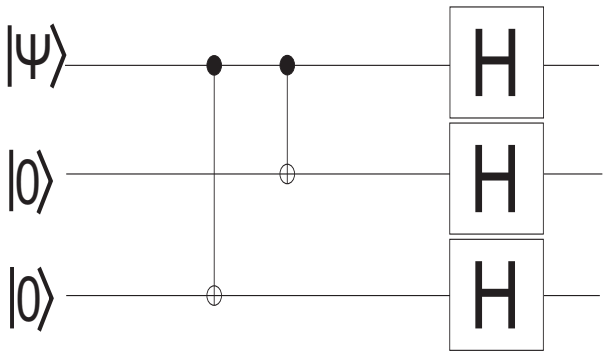

Figura 3.4: Circuito codificador para um código de inversão de fase de 3 q-bits.

Detecção e Correção de Erro

A detecção através de determinação das síndromes ocorre da mesma maneira que para o canal de inversão de bit, mudando-se apenas a base para $|+\rangle$ e $|-\rangle$. Utilizamos as mesmas medições projetivas utilizadas para o código de inversão de bit, só que conjugadas por portas Hadamard:

$$P_j \mapsto H^{\otimes 3} P_j H^{\otimes 3}, \tag{3.32}$$

onde $H^{\otimes 3}$ equivale a $H \otimes H \otimes H$. De maneira análoga ao canal de inversão de bit também pode-se medir as síndromes utilizando os observáveis $H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2$ e $H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3$. Neste caso, por exemplo, a medida de $X_1 X_2$ retorna +1 para os estados $|+\rangle|+\rangle \otimes |x\rangle$ e $|-\rangle|-\rangle \otimes |x\rangle$.

Suponha que ocorra um erro no i-ésimo q-bit, de $|+\rangle$ para $|-\rangle$. Para realizar a recuperação basta aplicar $HX_iH = Z_i$, no q-bit em questão e o erro de fase será corrigido. Devido às características similares entre os canais de inversão de fase e canais de inversão de bit, a fidelidade mínima será exatamente a mesma.

3.4.3 Código de Shor

O código de Shor de 3 q-bits protege o q-bit contra erros de inversão de bit e inversão de fase. Seguindo com os exemplos de códigos de três q-bits, para implementar um código de Shor basta combinar os códigos de inversão de bit e inversão de fase vistos anteriormente. O código de Shor segue a idéia do código de repetição e é eficiente para correção de no máximo 1 q-bit.

Codificação

O circuito codificador de um código de Shor mostrado na Figura 3.5 é a combinação dos circuitos das Figuras 3.3 e 3.4. Primeiramente o q-bit é codificado pelo código de inversão de fase, onde $|\psi\rangle =$

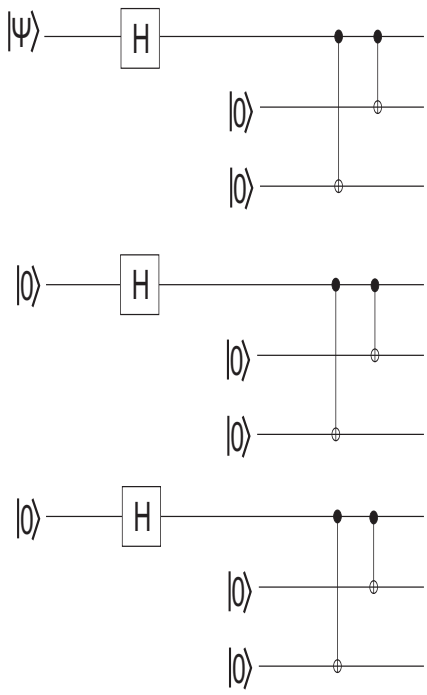

Figura 3.5: Circuito codificador para um código de inversão de bit de 3 q-bits.

$a|0\rangle+b|1\rangle$ é mapeado em $|\psi_1\rangle = a|+++\rangle+b|---\rangle$. Cada um destes q-bits é então codificado pelo código de inversão de bit, em que $|+\rangle \mapsto (|000\rangle + |111\rangle)/2$ e $|-\rangle \mapsto (|000\rangle - |111\rangle)/2$, resultando num código de nove q-bits em que:

$$|0\rangle \mapsto |0_L\rangle \quad = \quad \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}; \tag{3.33}$$

$$|1\rangle \mapsto |1_L\rangle \quad = \quad \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \tag{3.34}$$

O estado após a codificação é:

$$|\psi_2\rangle \quad = \quad a|0_L\rangle + b|1_L\rangle. \tag{3.35}$$

Detecção e Correção de Erros - Inversão de Bit

A detecção e eventual correção de um erro arbitrário neste código ocorre devido ao fato deste ser capaz de corrigir tantos erros provenientes do operador X quanto Z. Suponha, por exemplo, um erro no primeiro q-bit. Como vimos este erro pode ser identificado pelo código através da medida dos observáveis Z_1Z_2 e Z_2Z_3. O resultado das medidas serão, respectivamente, -1 e +1, indicando um erro no primeiro q-bit. A correção, como vimos, consiste na aplicação do operador X no q-bit

detectado.

Esta técnica pode ser usada em qualquer um dos nove q-bits do código. Perceba que caso não se saiba em que bloco ocorreu o erro de inversão de bit, será necessário medir seis observáveis: Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8 e Z_8Z_9.

Detecção e Correção de Erros - Inversão de Fase

Para um erro de inversão de fase, compara-se os sinais dos *blocos* de três q-bits para o primeiro e segundo q-bits em um código de inversão de fase. Supondo, portanto, um erro deste tipo no primeiro q-bit ocorre uma troca no sinal do primeiro bloco passando $|0_L\rangle$ de $|000\rangle + |111\rangle$ para $|000\rangle - |111\rangle$ e $|1_L\rangle$ de $|000\rangle - |111\rangle$ para $|000\rangle + |111\rangle$. Esta inversão é decorrente na inversão em qualquer um dos três primeiros q-bits, servindo este procedimento para qualquer um dos três q-bits em questão.

Os observáveis utilizados para a detecção e inversão de fase para o código de Shor são $X_1X_2X_3$-$X_4X_5X_6$ e $X_4X_5X_6X_7X_8X_9$. Para recuperar o estado original deve-se aplicar o operador $Z_1Z_2Z_3$. Uma característica do Código de Shor é o fato que este é um código *degenerado*, pois os erros de inversão de fase não são distinguíveis, visto que erros no mesmo bloco, independente se ocorre no primeiro, segundo ou terceiro q-bit, terão efeitos idênticos. Saberemos, portanto, em qual bloco ocorreu o erro, mas nunca em qual q-bit do bloco este erro ocorreu. Mesmo não sendo distinguíveis, os erros são corrigíveis, o que caracteriza a degenerecência do código.

Detecção e Correção de Erros - Inversão de Bit e de Fase Simultaneamente

Um erro de inversão de fase e inversão de bit no primeiro q-bit, correponde a aplicar o operador X_1Z_1 a este q-bit. Como estes dois tipos de erros são independentes, podemos aplicar os procedimentos para identificar os erros X e Z independentemente. Aplicando os dois procedimentos vistos para o canal de inversão de bit, corrigiremos o erro X_1. Entretanto, com o erro de inversão de fase no primeiro q-bit, este só será corrigido quando aplicarmos o procedimento de detecção e correção para o canal de inversão de fase. O código de Shor é capaz de corrigir um erro arbitrário em um q-bit qualquer, desde que apenas um q-bit seja afetado.

Como vimos no início deste capítulo, o ruído pode ser representado por uma operação quântica que preserva o traço. Utilizando a representação de sistema acoplado com a vizinhança, supondo um estado inicial $|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$, após a atuação do ruído, tem-se:

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i|\psi\rangle\langle\psi|E_i^\dagger. \tag{3.36}$$

Cada termo E_i do somatório, equivale a um tipo de erro diferente do *continuum* de erros existentes na comunicação quântica. O fato em destaque é que cada elemento E_i pode ser discretizado de forma que um erro arbitrário E_i, que atue no primeiro q-bit pode ser decomposto como:

$$E_i = c_{iI}I + c_{iX}X_1 + c_{iY}Y_1 + c_{iZ}Z_1. \tag{3.37}$$

Como $Y = \imath XZ$, podemos reescrever (3.37) como:

$$E_i = c'_{iI}I + c'_{iX}X_1 + c'_{iZ}Z_1 + c'_{iXZ}X_1Z_1. \tag{3.38}$$

A medida de uma síndrome irá colapsar o estado para termos corrigíveis pelo código de Shor: $|\psi\rangle$, $X_1|\psi\rangle$, $Z_1|\psi\rangle$ e $X_1Z_1|\psi\rangle$, de forma que em qualquer medida a correção resultará no estado original $|\psi\rangle$, utilizando-se a correção apropriada para cada caso.

3.5 Teoria da Correção de Erros Quânticos

O intuito desta seção é mostrar a possibilidade de construir uma teoria geral para a correção de erros quânticos, fazendo o menor número possível de considerações em relação ao ruído e ao procedimento de correção em questão.

Para um código quântico genérico de k q-bits de informação, tem-se 2^k palavras código-base. O espaço de Hilbert $\mathcal{C}$ de palavras código é um espaço de 2^k dimensões e também um subespaço de um espaço de Hilbert $\mathcal{N}$ de 2^n dimensões. O comprimento da palavra código é n-q-bits e a taxa do código é $R = k/n$.

A codificação é realizada através de uma operação unitária. Para um código com $k = 1$ e $n = 3$ temos um projetor de $\mathcal{N}$ em $\mathcal{C}$ definido por:

$$P = |000\rangle\langle 000| + |111\rangle\langle 111|. \tag{3.39}$$

Após a codificação tem-se a atuação do ruído. O código de Shor é um bom exemplo da teoria da correção de erros quânticos, em especial para o caso da atuação de um ruído quântico. Vimos na Seção 3.4.3 que se dois tipos de erros distintos, representados pelos operadores A e B, são corrigíveis por um determinado código quântico, implica que um erro da forma $aA+bB$ é igualmente corrigível por este código. Desta forma, o fato fundamental é que o código precisa corrigir uma base de erros.

Ao se realizar uma medida qualquer, não podemos obter informação sobre a palavra-código, pois isto acarretaria na destruição da superposição de estados impedindo uma posterior correção. Deve-se lembrar, entretanto que erros distintos A e B devem ser distinguíveis para todas as palavras-código-base de um código, ou seja, se $|i_0\rangle$, $|i_1\rangle$, ..., $|i_{k-1}\rangle$, compõem o conjunto de palavras-código-base

$A|i_j\rangle$ e $B|i_L\rangle$ devem ser ortogonais para todos valores de i e j menores que k, ou seja, o processo de erro deve levar um estado ortogonal em outro estado ortogonal, mantendo a distingüibilidade entre os estados. Para formular uma teoria quântica geral apenas assumiremos duas suposições:

- ▷ O ruído é descrito por uma operação quântica $\mathcal{E}$ que não necessariamente preserva o traço.
- ▷ A recuperação do estado original (detecção e correção do erro) é realizada por uma operação quântica $\mathcal{R}$.

Uma correção bem sucedida implica em:

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto (\rho). \tag{3.40}$$

Devido ao fato que $\mathcal{E}$ não necessariamente preservar o traço explica o fato do sinal de $\propto$ não ser a igualdade. A condição de funcionamento de um CCEQ foi provada por Knill e Laflame [34] e por Bennet [35] e encontra-se demonstrada no apêndice A.

3.6 Códigos Estabilizadores

Os códigos estabilizadores, ou códigos quânticos aditivos, são os equivalentes quânticos dos códigos clássicos lineares e possuem construção análoga a estes [36]. O método algébrico para o entendimento de tais códigos é o *formalismo estabilizador*. Este é utilizado não só na correção de erros quânticos, como também em outras teorias, como por exemplo, a teoria quântica de tolerância a falhas.

Definição 4 (Formalismo Estabilizador)**.** *Dado um estado $|\psi\rangle$ e um operador linear A, dizemos que A estabiliza $|\psi\rangle$ se $|\psi\rangle = A|\psi\rangle$.*

Exemplo 2. *Considere o operador $Z_1 Z_2$, atuando num espaço de Hilbet $\mathcal{H}$. Utilizando a notação matricial, obtemos:*

$$
\begin{aligned}
Z_1 Z_2 &= Z \otimes Z \otimes I; && (3.41)\\
&= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; && (3.42)\\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; && (3.43)\\
&= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. && (3.44)
\end{aligned}
$$

Como

$$
|000\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad (3.45)
$$

então

$$
|000\rangle = Z_1 Z_2 |000\rangle. \qquad (3.46)
$$

De maneira análoga, conclui-se que $|001\rangle$, $|110\rangle$ *e* $|111\rangle$, *também são estabilizados por* $Z_1 Z_2$.

Uma análise mais refinada indicará que cada estado quântico $|\psi\rangle$ possui um grupo de operadores para os quais $|\psi\rangle$ é o *único* estado estabilizado por este grupo. Este fato indica a possibilidade de

representar tais estados pelos operadores que os estabilizam. Esta é a idéia básica do formalismo estabilizador. Tal formalismo descreve classes de CCEQ, tais como o código de Shor e o código CSS [37] [38] de forma mais compacta. Não só os operadores lineares, como também os erros, medidas e portas lógicas quânticas podem ser representados pelo formalismo estabilizador. O poder deste formalismo vem da sua aplicação à teoria de grupos, onde se destacam os chamados *grupos de Pauli*.

Definição 5 (Grupos de Pauli)**.** *Seja $\mathcal{H}$ um espaço de Hilbert de dimensão 2^n (n q-bits), Chamamos de* Grupo de Pauli $\mathcal{G}_n$ *atuando sobre $\mathcal{H}$, o grupo formado pelos produtos tensoriais de ordem n de todas matrizes de Pauli, incluindo-se os autovalores ± 1 e $\pm\imath$. Para um único q-bit, temos:*

$$G_1 \equiv \{\pm I, \pm\imath I, \pm X, \pm\imath X, \pm Y, \pm\imath Y, \pm Z, \pm\imath Z\}, \tag{3.47}$$

pois $Y = XZ$. De uma maneira geral, $\mathcal{G}_n$ é gerado por $X^{(k)}$ e $Z^{(k)}$ ($k = 1, ..., n$).

Partindo do Exemplo 2 podemos concluir que Z_1Z_2 estabiliza $|000\rangle$, $|001\rangle$, $|110\rangle$ e $|111\rangle$, ou seja, Z_1Z_2 define um subespaço gerado por estes estados. Da mesma maneira, o subespaço definido por Z_2Z_3 é gerado por $|000\rangle$, $|100\rangle$, $|011\rangle$ e $|111\rangle$. Seguindo esta análise para I e Z_1Z_3 percebe-se que $|000\rangle$ e $|111\rangle$ são comuns em todos subespaços gerados até então. Note que I, Z_1Z_2, Z_1Z_3 e Z_2Z_3 formam um subgrupo S de $\mathcal{G}_3$ e, como visto, todos elementos deste subgrupo estabilizam $|000\rangle$ e $|111\rangle$. Portanto podemos dizer que S representa o subespaço gerado por $|000\rangle$ e $|111\rangle$. Neste caso,

$$Z_1Z_3 = (Z_1Z_2)(Z_2Z_3); \tag{3.48}$$

$$I = (Z_1Z_2)^2. \tag{3.49}$$

Dizemos, portanto, que S tem dois geradores e podemos denotá-lo por $S = \langle Z_1Z_2, Z_2Z_3\rangle$. Qualquer estado estabilizado pelos geradores é também estabilizado pelos demais elementos do grupo. De posse destes resultados, podemos agora definir o conceito de *código estabilizador*.

Definição 6 (Código Estabilizador)**.** *Dado k q-bits, codificados num espaço de Hilbert de 2^n dimensões, chamamos de* código estabilizador *[n, k] ou $C(S)$, o espaço vetorial estabilizado por um subgrupo S de $\mathcal{G}_n$ dotado de $n-k$ geradores comutativos independentes para o qual $-I \notin S$.*

Seja $S = \langle g_1, g_2, ..., g_{n-k}\rangle$. Pode-se escolher 2^k vetores ortonormais em $C(S)$ para serem as bases computacionais. Quaisquer dois elementos de $\mathcal{G}_n$ ou comutam ou anticomutam. Sendo S um subgrupo com $n-k$ geradores Hermitianos, implica que todos os geradores comutam entre si, além de definirem 2^{n-k} autoespaços simultâneos.

Definição 7 (Normalizador)**.** *Chamamos de* normalizador *de $\mathcal{G}_n$, denotado por $N(\mathcal{G}_n)$, o conjunto de operadores U, tais que $U\mathcal{G}_nU^\dagger = \mathcal{G}_n$.*

Definição 8 (Centralizador)**.** *O centralizador de um grupo S é um grupo composto por todas as operações que comutam com todo $M \in S$.*

3.6.1 Revisitando os Códigos Quânticos de Acordo com o Formalismo Estabilizador

Código de Inversão de Bit

Para o código de inversão de bit de 3 q-bits gerado por $|000\rangle$ e $|111\rangle$, os geradores do estabilizador são os operadores Z_1Z_2 e Z_2Z_3 ($S = \langle Z_1Z_2, Z_2Z_3\rangle$). Para o gerador Z_1Z_2 temos que:

$$Z_1Z_2|000\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |000\rangle. \tag{3.50}$$

O estado $|000\rangle = |0_L\rangle$ é portanto um autovetor de autovalor +1. O mesmo vale para $|111\rangle = |1_L\rangle$ em relação a Z_1Z_2. O gerador Z_2Z_3 igualmente possui os estados $|0_L\rangle$ e $|1_L\rangle$ como autovetores com autovalor +1, ou seja, sendo $u = 0, 1$, $i = 0, 1$ e G um elemento do estabilizador, então

$$G_i|u_L\rangle = |u_L\rangle. \tag{3.51}$$

Inspecionando-se o conjunto de erros I, X_1, X_2, X_3, bem como os produtos possíveis: X_1X_2, X_1X_3 e X_2X_3, percebe-se que eles anticomutam com pelo menos um dos geradores do estabilizador, excetuando-se I, que encontra-se em S. Conclui-se, portanto, pelo critério de correção para códigos estabilizadores, que o conjunto de erros $E = \{I, X_1, X_2, X_3\}$ forma um conjunto de erros corrigíveis para o código de inversão de bit de 3 q-bits.

A medição dos autovalores dos geradores é realizada para detectar os erros para este código. Os geradores de um código quântico estabilizador possuem uma função semelhante à matriz de verificação de paridade. O erro X_1, por exemplo, mapeia os geradores $< Z_1Z_2, Z_2Z_3 >$ em $< -Z_1Z_2, Z_2Z_3 >$. Cada erro possui um conjunto de síndromes específico, como pode ser visto na Tabela 3.1.

Tabela 3.1: Erros e síndromes para o código de inversão de bit de 3 q-bits.

Tipo de Erro	Medidas da Síndrome	Ação
X_1	-1, +1	Inverter o q-bit 1
X_2	-1, -1	Inverter o q-bit 2
X_3	+1, -1	Inverter o q-bit 3

Código de Inversão de Fase

Para o código de inversão de fase, o procedimento é estritamente análogo ao de inversão de bit. Neste caso, os geradores do estabilizador são os operadores X_1X_2 e X_2X_3 ($S = \langle X_1X_2, X_2X_3\rangle$). Para o código de inversão de fase gerado por (3.33), temos para o caso do gerador X_1X_2 e para o estado lógico $|0_L\rangle$:

$$X_1X_2|0_L\rangle = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = |0_L\rangle. \qquad (3.52)$$

O estado $|0_L\rangle$ é portanto um autovetor correspondendo ao autovalor +1. Seguindo o mesmo procedimento para $|1_L\rangle$ conclui-se que $G_i|u_L\rangle = |u_L\rangle$, que também é válida para o gerador X_2X_3.

Código de Shor

O código de Shor para 9 q-bits possui 8 geradores, como mostrado na Tabela 3.2. Seguindo o mesmo procedimento utilizado para os códigos de inversão de bit e inversão de fase sob a ótica do formalismo estabilizador, verifica-se que para o caso do código de Shor, as palavras código $|0_L\rangle$ e $|1_L\rangle$ mostradas em (3.33) são autovetores de todos os oito geradores do código de Shor, com autovalores iguais a +1. A medida das síndromes que comparam os q-bits, ou o sinal dos blocos, correspondem à medida dos autovalores dos geradores. Pode-se verificar que o código de Shor pode corrigir todos os erros de um q-bit, pois todos operadores de Pauli com peso menor ou igual a dois ou estão em S ou anticomutam com algum elemento de S.

Tabela 3.2: Geradores do estabilizador do código de Shor de 9 q-bits.

$G_{X,1}$	$ZZIIIIIII$
$G_{X,2}$	$IZZIIIIII$
$G_{X,3}$	$IIIZZIIII$
$G_{X,4}$	$IIIIZZIII$
$G_{X,5}$	$IIIIIIZZI$
$G_{X,6}$	$IIIZZIIZZ$
$G_{Z,1}$	$XXXXXXIII$
$G_{Z,2}$	$IIIXXXXXX$

CAPÍTULO 4

CÓDIGOS DE BLOCO QUÂNTICOS COM PROTEÇÃO DESIGUAL DE ERROS

Neste capítulo proporemos códigos de bloco quânticos com característica UEP. Consideraremos inicialmente erros referentes a uma transmissão em um canal de inversão de bit. A seguir faremos uma extensão para considerar canais de inversão de fase.

4.1 Vetor de Separação Quântico

O estudo da característica UEP para códigos clássicos depende de pôr uma análise isolada do grau de proteção associado a cada bit de informação. Os primeiros a apresentar códigos UEP foram Masnick e Wolf [17], que forneceram exemplos de códigos UEP lineares, definiram cotas e descreveram algumas propriedades. Em [17] definiu-se para cada bit de informação um índice de proteção f_i, para o qual, caso f erros ocorram na recepção de uma palavra código, todos bits com proteção $f_i > f$ seriam decodificados corretamente, mesmo que a palavra código não fosse decodificada de maneira correta.

O conceito de vetor de separação foi introduzido por Dunning e Robbins [39] com o intuito de quantificar a característica UEP do código. A seguir este conceito será estendido para o caso de um canal quântico.

Definição 9. *Para um código quântico de um canal de inversão de bit de k q-bits de informação, definido no espaço de Hilbert de 2^n dimensões, define-se o* vetor de separação quântico *(VSQ), de-*

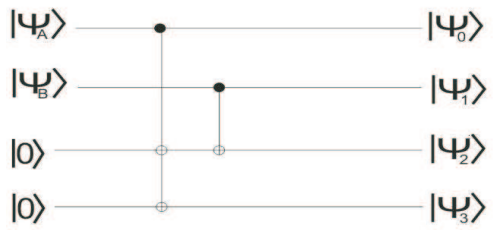

Figura 4.1: Circuito codificador para um código de inversão de bit de 4 q-bits, sendo dois q-bits de informação.

notado por $S(G) = (S(G)_1, ..., S(G)_k)$*, como um vetor cuja i-ésima componente corresponde à quantidade de erros de inversão de bit que podem ocorrer na palavra código para que o i-ésimo q-bit possa ser decodificado corretamente, mesmo que haja um erro de decodificação na palavra como um todo.*

Um VSQ de componentes iguais em todas as direções indica que o código não possui característica UEP. Algumas construções de códigos de bloco quânticos com característica UEP serão propostas para o canal de inversão de bit na próxima subseção.

4.2 Códigos Quânticos UEP

Para ilustrar a característica UEP de um código quântico, analisaremos o código descrito pelo circuito codificador da Figura 4.1. A operação de codificação de $|\psi_i\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |0\rangle| \otimes |0\rangle$ em $|\psi_C\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle| \otimes |\psi_3\rangle$ é regida pelo operador:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.1}$$

Dado os bits quânticos de informação A e B nos respectivamente nos estados

$$|\psi_A\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad |\psi_B\rangle = \begin{pmatrix} \gamma \\ \sigma \end{pmatrix}, \tag{4.2}$$

teremos

$$|\psi_i\rangle = \begin{pmatrix} \alpha\gamma \\ 0 \\ 0 \\ 0 \\ \alpha\sigma \\ 0 \\ 0 \\ 0 \\ \beta\gamma \\ 0 \\ 0 \\ 0 \\ \beta\sigma \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{4.3}$$

Podemos também reescrever o operador G na forma

$$\begin{aligned} G \quad &= |0000\rangle\langle 0000| + |0001\rangle\langle 0001| + |0010\rangle\langle 0010| + |0011\rangle\langle 0011| \\ &+|0110\rangle\langle 0100| + |0101\rangle\langle 0101| + |0110\rangle\langle 0110| + |0111\rangle\langle 0111| \\ &+|1011\rangle\langle 1000| + |1001\rangle\langle 1001| + |1010\rangle\langle 1010| + |1011\rangle\langle 1011| \\ &+|1101\rangle\langle 1100||1101\rangle\langle 1101| + |1110\rangle\langle 1110| + |1111\rangle\langle 1111|, \end{aligned} \tag{4.4}$$

além do operador $G^\dagger$ como

$$\begin{aligned} G^\dagger \quad &= |0000\rangle\langle 0000| + |0001\rangle\langle 0001| + |0010\rangle\langle 0010| + |0011\rangle\langle 0011| \\ &+|0100\rangle\langle 0110| + |0101\rangle\langle 0101| + |0110\rangle\langle 0110| + |0111\rangle\langle 0111| \\ &+|1000\rangle\langle 1011| + |1001\rangle\langle 1001| + |1010\rangle\langle 1010| + |1011\rangle\langle 1011| \\ &+|1100\rangle\langle 1101||1101\rangle\langle 1101| + |1110\rangle\langle 1110| + |1111\rangle\langle 1111|. \end{aligned} \tag{4.5}$$

A representação de G e $G^\dagger$ como descrita em (4.4) e (4.5) se tornam impraticáveis para matrizes de grandes dimensões. Desta forma podemos decompor o circuito conforme a Figura 4.2. Esta decomposição permite representar G como

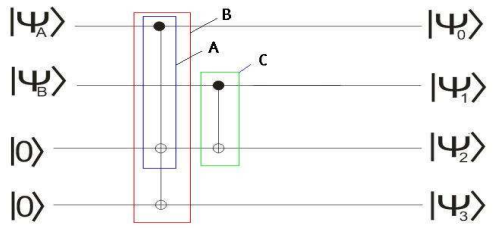

Figura 4.2: Circuito codificador decomposto em três portas.

$$G = ABC, \tag{4.6}$$

onde

$$A = P_0 \otimes I \otimes I \otimes I + P_1 \otimes I \otimes X \otimes I); \tag{4.7}$$

$$B = (P_0 \otimes I \otimes I \otimes I + P_1 \otimes I \otimes I \otimes X); \tag{4.8}$$

$$C = (I \otimes P_0 \otimes I \otimes I + I \otimes P_1 \otimes X \otimes I); \tag{4.9}$$

com $P_0 = |0\rangle\langle 0|$ e $P_1 = |1\rangle\langle 1|$. As síndromes $P'i$, onde i corresponde a uma inversão no i-ésimo q-bit, com $i = 0$ indicando nenhuma inversão, e $i = 5$ indicando a projeção no subespaço restante que satisfaz a relação de clausura, são:

$$P_0 = |0000\rangle\langle 0000| + |0110\rangle\langle 0110| + |1011\rangle\langle 1011| + |1101\rangle\langle 1101|; \tag{4.10}$$

$$P_1 = |1000\rangle\langle 1000| + |1110\rangle\langle 1110| + |0011\rangle\langle 0011| + |0101\rangle\langle 0101|; \tag{4.11}$$

$$P_2 = |0100\rangle\langle 0100| + |0010\rangle\langle 0010| + |1111\rangle\langle 1111| + |1001\rangle\langle 1001|; \tag{4.12}$$

$$P_3 = |0010\rangle\langle 0010| + |0100\rangle\langle 0100| + |1001\rangle\langle 1001| + |1111\rangle\langle 1111|; \tag{4.13}$$

$$P_4 = |0001\rangle\langle 0001| + |0111\rangle\langle 0111| + |1010\rangle\langle 1010| + |1100\rangle\langle 1100|; \tag{4.14}$$

$$P_5 = I - \sum_{i=0}^{4} P_i. \tag{4.15}$$

Inicialmente, observa-se que $P_2 = P_3$. Dado um estado recebido $|\psi_R\rangle$ teremos $\langle\psi_R|P_2|\psi_R\rangle = \langle\psi_R|P_3|\psi_R\rangle$, pois a inversão do segundo ou terceiro q-bit do código em questão projeta o sistema no mesmo subespaço. Podemos substituir ambos operadores de projeção por uma única medida $P_{23} = P_2 = P_3$, que indica a inversão no segundo q-bit ou no terceiro q-bit. Assumiremos que o estado $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ é codificado no estado $|\psi_C\rangle = a|0000\rangle + b|0110\rangle + c|1011\rangle + d|1101\rangle$ através do circuito codificador da Figura 4.1 e enviado pelo canal de inversão de

bit, onde $a^2 + b^2 + c^2 + d^2 = 1$. Calcularemos o VSQ $s(G) = (s(G)_1, s(G)_2)$ associado a este código, começando pela análise de inversão de até um q-bit.

Caso 1 - Informação transmitida sem erros

Estado recebido: $|\psi_R\rangle = \alpha\gamma|0000\rangle + \alpha\sigma|0110\rangle + \beta\gamma|1011\rangle + \beta\sigma|1101\rangle$.

Detecção de erro:

$\langle\psi_R|P_0|\psi_R\rangle = a^2 + b^2 + c^2 + d^2 = 1$.

$\langle\psi_R|P_1|\psi_R\rangle = 0$.

$\langle\psi_R|P_{23}|\psi_R\rangle = 0$.

$\langle\psi_R|P_4|\psi_R\rangle = 0$.

$\langle\psi_R|P_5|\psi_R\rangle = 0$.

Recuperação: O resultado da medida de síndrome é zero e portanto nada se deve fazer ao estado recebido, pois o mesmo foi recebido sem erros. Vemos claramente que

$$G^\dagger|\psi_R\rangle = |\psi_i\rangle. \tag{4.16}$$

Conclusão: O estado foi recebido corretamente e não fornece qualquer informação a respeito do vetor de separação quântico.

Caso 2 - Inversão no primeiro q-bit

Estado recebido: $|\psi_R\rangle = \alpha\gamma|1000\rangle + \alpha\sigma|1110\rangle + \beta\gamma|0011\rangle + \beta\sigma|0101\rangle$.

Detecção de erro:

$\langle\psi_R|P_0|\psi_R\rangle = 0$.

$\langle\psi_R|P_1|\psi_R\rangle = a^2 + b^2 + c^2 + d^2 = 1$.

$\langle\psi_R|P_{23}|\psi_R\rangle = 0$.

$\langle\psi_R|P_4|\psi_R\rangle = 0$.

$\langle\psi_R|P_5|\psi_R\rangle = 0$.

Recuperação: Inverter o primeiro q-bit de $|\psi_R\rangle$ para obter o estado $\psi_{R1}\rangle$. Desta forma tem-se

$$|\psi_{R1}\rangle = \alpha\gamma|0000\rangle + \alpha\sigma|0110\rangle + \beta\gamma|1011\rangle + \beta\sigma|1101\rangle \tag{4.17}$$

$$G^\dagger|\psi_{R1} = |\psi_i\rangle. \tag{4.18}$$

Conclusão: O estado será decodificado corretamente. Ainda não temos elementos para concluir sobre o VSQ.

Caso 3 - Inversão no segundo q-bit

Estado recebido: $|\psi_R\rangle = \alpha\gamma|0100\rangle + \alpha\sigma|0010\rangle + \beta\gamma|1111\rangle + \beta\sigma|1001\rangle$.

Detecção de erro:

$\langle\psi_R|P_0|\psi_R\rangle = 0.$

$\langle\psi_R|P_1|\psi_R\rangle = 0.$

$\langle\psi_R|P_{23}|\psi_R\rangle = a^2 + b^2 + c^2 + d^2 = 1.$

$\langle\psi_R|P_4|\psi_R\rangle = 0.$

$\langle\psi_R|P_5|\psi_R\rangle = 0.$

Recuperação: A medida de síndrome indica para inverter o segundo q-bit ou o terceiro q-bit. Se invertermos o segundo bit quântico teremos:

$$|\psi_{R2}\rangle = \alpha\gamma|0000\rangle + \alpha\sigma|0110\rangle + \beta\gamma|1011\rangle + \beta\sigma|1101\rangle, \tag{4.19}$$

que ao operar com $G^\dagger$ tem-se

$$G^\dagger|\psi_{R2}\rangle = |\psi_i\rangle. \tag{4.20}$$

Por outro lado, optando-se por inverter o terceiro q-bit, tem-se

$$|\psi_{R3}\rangle = \alpha\gamma|0110\rangle + \alpha\sigma|0000\rangle + \beta\gamma|1101\rangle + \beta\sigma|1011\rangle. \tag{4.21}$$

Aplicando $G^\dagger$ a $|\psi_{R3}\rangle$ temos:

$$G^\dagger|\psi_{R3}\rangle = \alpha\sigma|0000\rangle + \alpha\gamma|0100\rangle + \beta\sigma|1000\rangle + \beta\gamma|1100\rangle \tag{4.22}$$

$$= \left[\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \otimes \begin{pmatrix}\sigma\\ \gamma\end{pmatrix} \otimes \begin{pmatrix}1\\ 0\end{pmatrix} \otimes \begin{pmatrix}1\\ 0\end{pmatrix}\right] |\psi_i\rangle. \tag{4.23}$$

Conclusão: Se optarmos pela inversão do segundo q-bit, o estado será decodificado corretamente. Entretanto, se optarmos pela inversão do terceiro bit quântico, note de 4.22 que o primeiro bit quântico é recuperado corretamente, com os coeficientes α e β nas posições corretas, mesmo o segundo bit quântico não sendo recuperado de maneira correta, visto que o mesmo sofrerá uma inversão de bit. Em resumo, para um único erro na palavra código já não temos certeza na decodificação do segundo q-bit, o que equivale à segunda componente nula do VSQ.

Caso 4 - Inversão no terceiro q-bit

Estado recebido: $|\psi_R\rangle = \alpha\gamma|0010\rangle + \alpha\sigma|0100\rangle + \beta\gamma|1001\rangle + \beta\sigma|1111\rangle$.

Detecção de erro:

$\langle\psi_R|P_0|\psi_R\rangle = 0.$

$\langle\psi_R|P_1|\psi_R\rangle = 0.$

$\langle\psi_R|P_{23}|\psi_R\rangle = 1.$

$\langle\psi_R|P_4|\psi_R\rangle = 0.$

$\langle\psi_R|P_5|\psi_R\rangle = 0.$

Recuperação: A medida de síndrome indica para inverter o segundo q-bit ou o terceiro q-bit. Este caso é análogo ao caso 3 e seguindo os mesmos passos chegaremos aos mesmos resultados.

Conclusão: Confirma os dados do caso 3.

Caso 5 - Inversão no quarto q-bit

Estado recebido: $|\psi_R\rangle = \alpha\gamma|0001\rangle + \alpha\sigma|0111\rangle + \beta\gamma|1010\rangle + \beta\sigma|1100\rangle.$

Detecção de erro:

$\langle\psi_R|P_0|\psi_R\rangle = 0.$

$\langle\psi_R|P_1|\psi_R\rangle = 0.$

$\langle\psi_R|P_{23}|\psi_R\rangle = 0.$

$\langle\psi_R|P_4|\psi_R\rangle = 1.$

$\langle\psi_R|P_5|\psi_R\rangle = 0.$

Recuperação: A medida de síndrome indica para inverter o quarto q-bit, obtendo-se $|\psi_{R4}\rangle$, de tal forma que $G^\dagger|\psi_{R4}\rangle = |\psi_i\rangle$.

Conclusão: Ocorre o mesmo que no caso 1, o estado é decodificado corretamente e nada podemos concluir a respeito do VSQ.

O resultado dos cinco primeiros casos fornece um VSQ igual a $s(G) = (s(G)_1, 0)$ e $s(G)_1 \geq 1$. A determinação da componente $s(G)_1$ necessita de novas análises, visto que, para até um erro de inversão de bit, o primeiro bit quântico é sempre decodificado de maneira correta.

Caso 6 - Inversão no primeiro e segundo q-bit

Estado recebido: $|\psi_R\rangle = \alpha\gamma|1100\rangle + \alpha\sigma|1010\rangle + \beta\gamma|0111\rangle + \beta\sigma|0001\rangle.$

Detecção de erro:

$\langle\psi_R|P_4|\psi_R\rangle = 1.$

Recuperação: Ao inverter o quarto q-bit temos

$$|\psi_{R4}\rangle = \alpha\gamma|1101\rangle + \alpha\sigma|1011\rangle + \beta\gamma|0110\rangle + \beta\sigma|0000\rangle. \tag{4.24}$$

o que nos dá

$$G^{\dagger}|\psi_{R4}\rangle = \beta\sigma|0000\rangle + \beta\gamma|0100\rangle + \alpha\sigma|0100\rangle + \alpha\gamma|1100\rangle \quad (4.25)$$

$$= \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \otimes \begin{pmatrix} \sigma \\ \gamma \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \quad (4.26)$$

O que nos leva a concluir que ambos os q-bits foram invertidos e portanto o VSQ é (1,0).

4.3 Códigos Quânticos com Mesma Taxa e VSQ Distintos

Códigos quânticos de mesma taxa podem apresentar VSQ distintos. Apresentaremos a seguir códigos com dois q-bits de informação e taxas 2/6, 2/7, 2/8, 2/9. Estes evidenciam a modificação na matriz geradora e no circuito codificador a fim de aumentar a proteção do primeiro q-bit.

4.3.1 Código(6,2)

Os circuitos codificadores são mostrados nas Figuras 4.3 (VSQ = (1,1)) e 4.4 (VSQ = (2,0)).

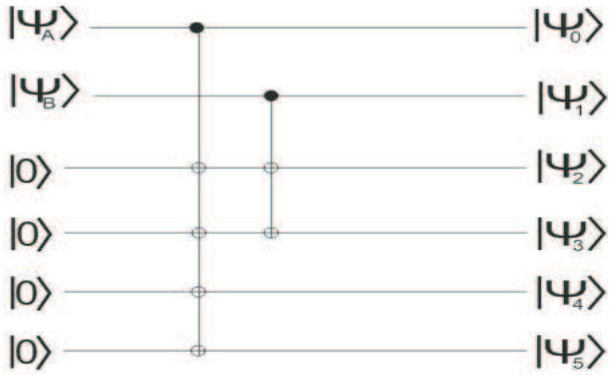

Figura 4.3: Circuito codificador para um código de inversão de bit de taxa 2/6 e QSP igual a (1,1).

4.3.2 Código(7,2)

Os circuitos codificadores são mostrados nas Figuras 4.5 (VSQ = (1,1)) e 4.6 (VSQ = (2,0)).

4.3.3 Código(8,2)

Os circuitos codificadores são mostrados nas Figuras 4.7 (VSQ = (1,1)) e 4.8 (VSQ = (2,0)).

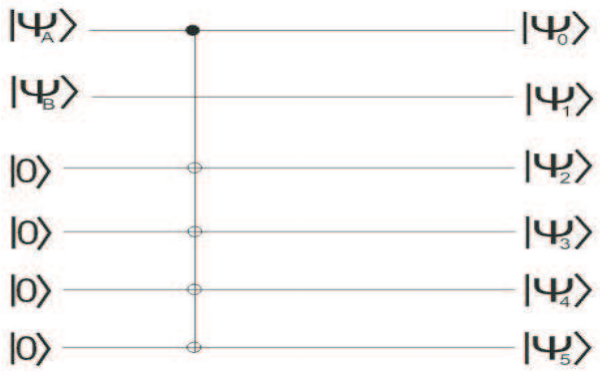

Figura 4.4: Circuito codificador para um código de inversão de bit de taxa 2/6 e VSQ igual a (2,0).

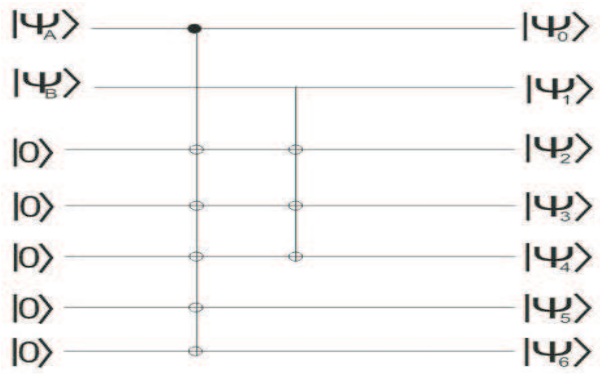

Figura 4.5: Circuito codificador para um código de inversão de bit de taxa 2/7 e VSQ igual a (1,1).

4.3.4 Código(9,2)

Os circuitos codificadores são mostrados nas Figuras 4.9 (VSQ = (2,2)), 4.10 (VSQ = (3,1)) e 4.11 (VSQ = (4,0)).

4.4 Códigos UEP Quânticos para Canais de Inversão de Fase

Todos os códigos quânticos com proteção desigual de erros apresentados neste capítulo possuem equivalentes para canais de inversão de fase com o mesmo VSQ. Utilizando as bases $|+\rangle$ e $|-\rangle$ ao invés de $|0\rangle$ e $|1\rangle$ transformamos o canal de inversão de fase em um canal de inversão de bit, sujeito aos mesmos desenvolvimentos do VSQ das seções anteriores. Para

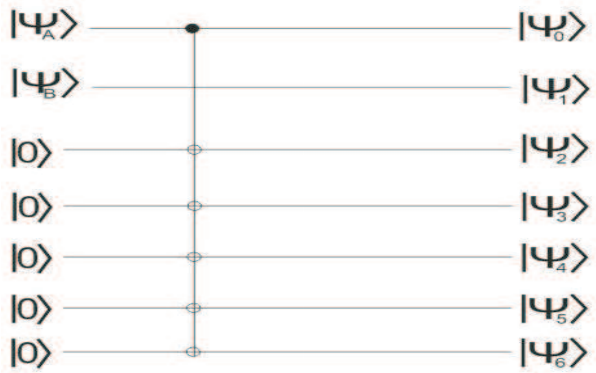

Figura 4.6: Circuito codificador para um código de inversão de bit de taxa 2/7 e VSQ igual a (2,0).

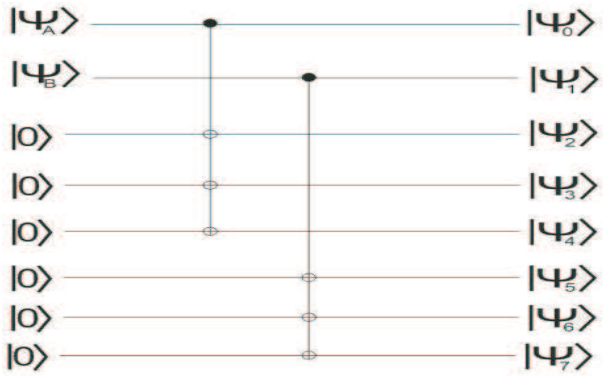

Figura 4.7: Circuito codificador para um código de inversão de bit de taxa 2/8 e VSQ igual a (1,1).

$$
\begin{aligned}
|\psi\rangle &= a|0\rangle + b|1\rangle; && (4.27)\\
&= a(\frac{|+\rangle + |-\rangle}{\sqrt{2}}) + b(\frac{|+\rangle - |-\rangle}{\sqrt{2}}); && (4.28)\\
&= \frac{1}{\sqrt{2}}((a+b)|+\rangle + (a-b)|-\rangle). && (4.29)
\end{aligned}
$$

Aplicando o operador Z em (4.29) obtemos

$$
\begin{aligned}
|\psi'\rangle &= Z|\psi\rangle; && (4.30)\\
&= \frac{1}{\sqrt{2}}((a-b)|+\rangle + (a+b)|-\rangle); && (4.31)\\
&= a|0\rangle - b|1\rangle. && (4.32)
\end{aligned}
$$

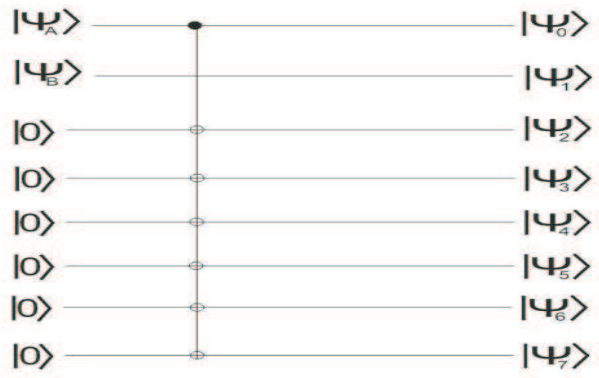

Figura 4.8: Circuito codificador para um código de inversão de bit de taxa 2/8 e VSQ igual a (2,0).

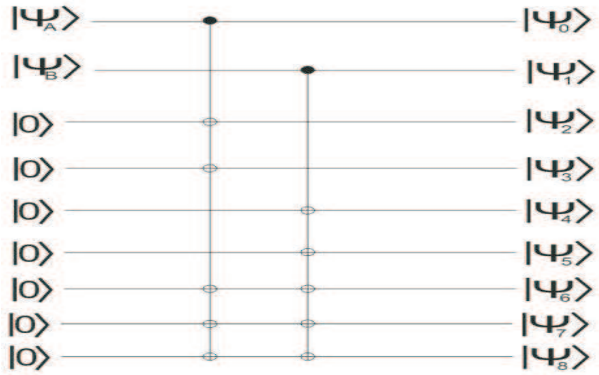

Figura 4.9: Circuito codificador para um código de inversão de bit de taxa 2/9 e VSQ igual a (2,2).

Para o circuito codificador da Figura 4.12 com taxa 2/4 temos as seguintes síndromes:

$$
\begin{aligned}
P_0 &= |++++\rangle\langle++++|+|+--+\rangle\langle+--+|+|-+--\rangle\langle-+--|+|--+-\rangle\langle--+-|; \\
P_1 &= |-+++\rangle\langle-+++|+|---+\rangle\langle---+|+|++--\rangle\langle++--|+|+-+-\rangle\langle+-+-|; \\
P_2 &= |+-++\rangle\langle+-++|+|++-+\rangle\langle++-+||+|-++-\rangle\langle-++-|+|----\rangle\langle----|; \\
P_3 &= |++-+\rangle\langle++-+|+|+-++\rangle\langle+-++|+|-+++\rangle\langle-+++|+|----\rangle\langle----|; \\
P_4 &= |+++-\rangle\langle+++-|+|+---\rangle\langle+---|+|-+-+\rangle\langle-+-+|+|--++\rangle\langle--++|; \\
P_5 &= I - \sum_{i=0}^{4} P_i.
\end{aligned}
$$

Este código, bem como suas síndromes, são análogas ao mostrado na Seção 4.2, e seguindo os mesmos passos encontraremos um VSQ igual a $(1, 0)$.

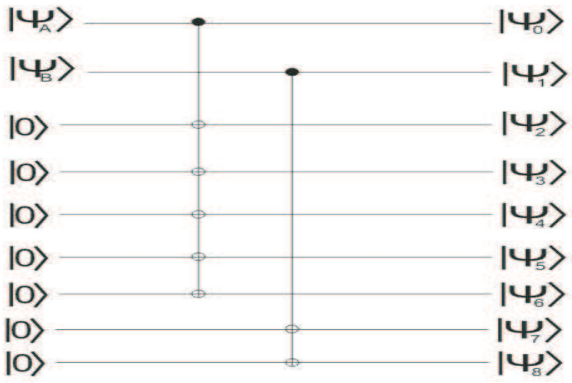

Figura 4.10: Circuito codificador para um código de inversão de bit de taxa 2/9 e VSQ igual a (3,1).

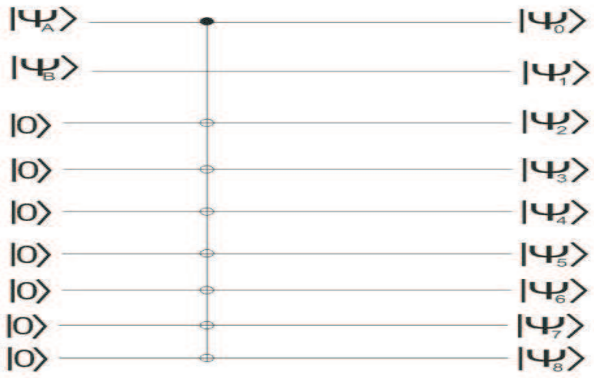

Figura 4.11: Circuito codificador para um código de inversão de bit de taxa 2/9 e VSQ igual a (4,0).

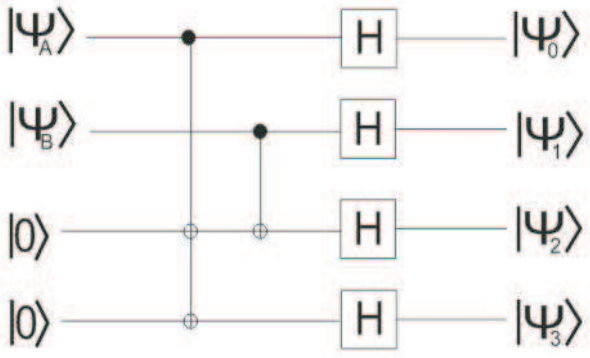

Figura 4.12: Circuito codificador para um código de inversão de fase com taxa 2/4.

CAPÍTULO 5

CONCLUSÕES E PERSPECTIVAS PARA A PESQUISA COM CÓDIGOS QUÂNTICOS UEP

Esta dissertação introduziu códigos quânticos para canais de inversão de bit com proteção desigual de erros. Estendemos este conceito para canais de inversão de fase através da técnica de mudança de base. A característica UEP, bastante abordada na teoria de codificação clássica, foi analisada na construção de códigos quânticos, verificando-se o grau de proteção individual de cada q-bit de informação.

O grau de proteção de cada q-bit de informação está diretamente relacionado com a quantidade de q-bits de paridade controlados por este q-bit de informação. Quanto maior o número de portas C-NOT no circuito codificador com o q-bit de informação como q-bit de controle, maior será a proteção deste q-bit.

A principal contribuição deste trabalho está no Capítulo 4, onde fizemos uma análise a respeito de códigos quânticos UEP, apresentando códigos com diversas taxas e graus de proteção distintos, desde o código sem proteção desigual de erros até a diferença máxima entre as coordenadas do VSQ.

Julgamos que os códigos quânticos utilizados nos exemplos exibidos neste texto, em especial os códigos usados na análise UEP, não serão objeto de implementação futura com o advento do computador quântico, dada sua simplicidade, porém o julgamos ideais para o entendimento didático da proteção desigual de erros. Por se tratar de uma área recente, acreditamos que ainda existe um vasto campo a ser explorado, havendo uma grande possibilidade de várias classes de códigos quânticos apresentarem proteção desigual de erros.

O futuro desenvolvimento do hardware quântico poderá difundir códigos com tais características, assim como aconteceu na teoria clássica, quando a internet e sistemas de transmissão sem fio passaram a exigir o desenvolvimento de códigos clássicos UEP.

Outro objetivo desta dissertação foi despertar o interesse para esta nova área de pesquisa, trazendo novas perguntas a serem respondidas por novos pesquisadores que se interessem por esta promissora e inexplorada área de pesquisa.

Dentre as possíveis linhas de pesquisa com códigos quânticos UEP, sugerimos:

- Implementação de um algoritmo em um computador clássico para análise da característica UEP para canais de inversão de bit em códigos de taxas elevadas.
- Busca de códigos de Shor com característica UEP. A existência de códigos para canais de inversão de bit e inversão de fase são uma forte evidência para a existência de códigos de Shor com tais características.
- Códigos convolucionais quânticos UEP.
- Análise UEP em sistemas concatenados.

APÊNDICE A - TEOREMA DA CODIFICAÇÃO QUÂNTICA

Este apêndice tem por objetivo descrever o teorema da condição para correção quântica de erros. Antes de enunciá-lo, vamos provar o teorema da decomposição polar e o da liberdade unitária do operador soma.

Teorema 6 (Decomposição Polar)**.** *Seja A um operador linear definido num espaço vetorial V, existem operadores positivos $J = \sqrt{A^\dagger A}$ e $K = \sqrt{AA^\dagger}$ e uma transformação unitária U tais que:*

$$A = UJ = KU. \tag{5.1}$$

Prova: *Se J consiste em um operador positivo, este pode ser reescrito pela sua decomposição espectral:*

$$J = \sum_j \lambda_j |j\rangle\langle j|. \tag{5.2}$$

Definindo $|\psi_j\rangle = A|j\rangle$ temos $\langle\psi_j|\psi_j\rangle = \lambda_j^2$. Definimos também um conjunto de vetores de base normalizados e ortogonais

$$e_k \equiv \frac{|\psi_i\rangle}{\lambda_i}. \tag{5.3}$$

O processo de Gram-Schmidit fornece um conjunto de base ortonormal a partir de $|e_k\rangle$. De posse deste conjunto de bases define-se:

$$U = \sum_i |e_i\rangle\langle i|. \tag{5.4}$$

Então

$$UJ|i\rangle = \lambda_i|e_i\rangle = |\psi_i\rangle = A|i\rangle, \tag{5.5}$$

para $\lambda_i > 0$. Já para $\lambda_i = 0$ temos

$$UJ|i\rangle = 0 = |\psi_i\rangle, \tag{5.6}$$

o que implica nas mesmas ações do operador A e, portanto, $A = UJ$. A decomposição polar à direita $(J = KU)$ é análoga.

Teorema 7. *Sejam $\{|\psi\rangle\}$ e $\{|\varphi\rangle\}$ bases de um mesmo espaço de Hilbert. Estas terão a mesma matriz densidade se e somente se $|\psi\rangle = \sum_j c_{ij}|\varphi_j\rangle$, onde c_{ij} são elementos de uma matriz unitária complexa. No caso dos conjuntos não possuírem o mesmo número de elementos, o menor deve ser completado com vetores nulos adicionais.*

Prova: *Provando a implicação direta, seja $|\psi_i\rangle = \sum_j c_{ij}|\varphi_j\rangle$ e $\langle\psi_i| = \sum_j c^*_{ij}|\varphi_j\rangle$ tem-se:*

$$\sum_i |\psi_i\rangle\langle\psi_i| = \sum_{ijk}(c^*_{ki}c_{ij})|\varphi_j\rangle\langle\varphi_k| \tag{5.7}$$

$$= \sum_{jk}(\sum_i c^*_{ki}c_{ij})|\varphi_j\rangle\langle\varphi_k|. \tag{5.8}$$

Como os coeficientes u são elementos de uma matriz unitária U, então $\sum_i c^\dagger_{ki}c_{ij} = 1$. Desta forma

$$\sum_i |\psi_i\rangle\langle\psi_i| = \sum_j |\varphi_j\rangle\langle\varphi_j|, \tag{5.9}$$

o que demonstra a implicação direta.

Para provar a reciprocidade da aplicação, usando a decomposição espectral em (5.9), tem-se:

$$\sum_k \lambda_k|k\rangle\langle k| = \sum_i |\psi_i\rangle\langle\psi_i| = \sum_j |\varphi_j\rangle\langle\varphi_j|, \tag{5.10}$$

com autovalores estritamente positivos. Seja, $|\omega\rangle$ ortonormal a $\lambda_k|k\rangle$ tem-se:

$$\sqrt{\lambda_k}\langle\omega|k\rangle = 0; \tag{5.11}$$

$$\lambda_k\langle\omega|k\rangle\langle\omega|k\rangle = 0; \tag{5.12}$$

$$\lambda_k\langle\omega|k\rangle\langle k|\omega\rangle = 0; \tag{5.13}$$

$$\sum_k \lambda_k\langle\omega|k\rangle\langle k|\omega\rangle = 0; \tag{5.14}$$

$$\sum_i \langle\omega|\psi_i\rangle\langle\psi_i|\omega\rangle = 0; \tag{5.15}$$

$$\sum_i |\langle\omega|\psi_i\rangle|^2 = 0; \tag{5.16}$$

$$\langle\omega|\psi_i\rangle = 0, \tag{5.17}$$

para todo i e todo $|\omega\rangle$ ortonormal a $\lambda_k|k\rangle$. Desta forma podemos representar cada $|\psi_i\rangle$ por

$$|\psi_i\rangle = \sum_k c_{ik}\sqrt{\lambda_k}|k\rangle. \tag{5.18}$$

Como $\sum_k \lambda_k|k\rangle\langle k| = \sum_i |\psi_i\rangle\langle\psi_i|$, então

$$\sum_k \lambda_k|k\rangle\langle k| = \sum_{kl}\sqrt{\lambda_k}\sqrt{\lambda_l}(\sum_i (c_{ik}c_{il}^*)\lambda_k|k\rangle\langle l|. \tag{5.19}$$

Como os operadores $|k\rangle\langle l|$ são linearmente independentes temos

$$\sum_i c_{ik}c_{il}^* = \delta_{kl}. \tag{5.20}$$

Este resultado garante que pode-se adicionar colunas à matriz dos elementos c para obter uma matriz unitária v tal que $|\psi_i\rangle = \sum_k v_{ik}\lambda_k|k\rangle$. Da mesma forma também se encontra uma matriz w tal que $|\varphi_j\rangle = \sum_k w_{jk}\lambda_k|k\rangle$, o que implica em

$$|\psi\rangle = \sum_j u_{ij}|\varphi_j\rangle, \tag{5.21}$$

e consequentemente $u = vw^\dagger$.

Teorema 8 (Liberdade Unitária do Operador Soma)**.** *Seja $\{E_1, ...E_m\}$ elementos de operação de uma operação quântica $\mathcal{E}$ e $\{F_1, ...F_n\}$ elementos de uma outra operação quântica $\mathcal{F}$, tal que $m > n$. Adicionando-se operadores nulos para assegurar $m = n$, teremos $\mathcal{E}$ igual a $\mathcal{F}$ se e somente se existirem coeficientes complexos c_{ij}, elementos de uma matriz complexa de dimensão m por m tal que $E_i = \sum_j c_{ij}F_j$.*

Prova: *Sejam os conjuntos $\{E_i\}$ e $\{F_j\}$ elementos de operação de uma mesma operação quântica, temos*

$$\sum_i E_i\rho E_i^\dagger = \sum_j F_j\rho F_j^\dagger. \tag{5.22}$$

Partindo do Teorema 7, temos que $|\psi\rangle$ e $|\varphi\rangle$ possuem o mesmo operador densidade se e somente se

$$|\psi_i\rangle = \sum_j c_{ij}|\varphi_j\rangle. \tag{5.23}$$

Vamos utilizar uma outra característica interessante de sistemas quânticos envolvendo o emaranhamento e sistemas acoplados. Para saber como uma determinada operação quântica atua em um

sistema B, basta saber como ela atua em um estado de emaranhamento máximo num sistema composto AB, tendo o sistema A, a mesma dimensão do sistema B. Sejam $|i_A\rangle$ e $|i_B\rangle$ bases ortonormais de A e B respectivamente, e seja $|\alpha\rangle$ um estado de máximo emaranhamento, excluindo-se o fator de normalização, do sistema AB, então:

$$|\alpha\rangle \equiv \sum_i |i_A\rangle|i_B\rangle. \tag{5.24}$$

Definindo um novo operador W e um estado $|\beta\rangle$ tais que:

$$W \equiv (I_A \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|); \tag{5.25}$$

$$|\beta\rangle\langle\beta| = W(|\alpha\rangle\langle\alpha|). \tag{5.26}$$

Para recuperar $\mathcal{E}$ de W é preciso ainda definir dois estados quaisquer, um em A e outro em B, de forma que:

$$|\psi_A\rangle \equiv \sum_j \psi_{A_j}|j_A\rangle; \tag{5.27}$$

$$|\psi_B\rangle \equiv \sum_j \psi_{B_j}|j_B\rangle. \tag{5.28}$$

De posse de W e de $|\psi_A\rangle$ faz-se:

$$\langle\psi_A|W|\psi_A\rangle = \langle\psi_A|(I \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|)|\psi_A\rangle; \tag{5.29}$$

$$= (\sum_j \psi_{A_j}|j_A\rangle)^\dagger(\sum_{ij} |i_A\rangle\langle j_A| \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|)(\sum_j \psi_{A_j}|j_A\rangle); \tag{5.30}$$

$$= (\sum_{ij} \psi^*_{A_j}\psi_{A_j}\langle j_A|i_A\rangle\langle j_A|i_A\rangle \otimes \mathcal{E}(|\psi_B\rangle\langle\psi_B|); \tag{5.31}$$

$$= (\sum_{ij} \psi^*_{A_j}\psi_{A_j}\langle j_A|i_A\rangle\langle j_A|i_A\rangle \otimes \mathcal{E}(|\psi_B\rangle\langle\psi_B|); \tag{5.32}$$

$$= \mathcal{E}(|\psi_B\rangle\langle\psi_B|). \tag{5.33}$$

De posse de (5.33), da definição de W para $\sum_i |e_i\rangle\langle e_i| = \sum_j |f_j\rangle\langle f_j|$, e definindo

$$|e_i\rangle \equiv \sum_k |k_A\rangle(E_i|k_B\rangle); \tag{5.34}$$

$$|f_j\rangle \equiv \sum_k |k_A\rangle(F_j|k_B\rangle), \tag{5.35}$$

temos pelo teorema 7 que

$$|e_i\rangle = c_{ij}|f_j\rangle. \tag{5.36}$$

Desta forma, definindo um mapa:

$$E_i|\psi_B\rangle = \langle\psi_A|e_i\rangle; \tag{5.37}$$

$$F_j|\psi_B\rangle = \langle\psi_A|f_i\rangle, \tag{5.38}$$

tem-se:

$$E_i|\psi_B\rangle = \sum_j c_{ij}\langle\psi_A|f_j\rangle; \tag{5.39}$$

$$= \sum_j c_{ij}F_j|\psi_B\rangle. \tag{5.40}$$

Isto prova a implicação direta. Reciprocamente, temos:

$$\mathcal{E}(|\psi_B\rangle\langle\psi_B|) = \sum_i E_i|\psi_B\rangle\langle\psi_B|E_i^\dagger; \tag{5.41}$$

$$= \sum_i \langle\psi_A|e_i\rangle\langle e_i|\psi_A\rangle, \tag{5.42}$$

como $\sum_i |e_i\rangle\langle e_i| = \sum_j |f_j\rangle\langle f_j|$*, então*

$$\mathcal{E}(|\psi_B\rangle\langle\psi_B|) = \sum_j \langle\psi_A|f_j\rangle\langle f_j|\psi_A\rangle; \tag{5.43}$$

$$= \sum_j F_j|\psi_B\rangle\langle\psi_B|F_j^\dagger; \tag{5.44}$$

$$= F(|\psi_B\rangle\langle\psi_B|). \tag{5.45}$$

Teorema 9 (Condição para Correção Quântica de Erro)**.** *Para um código* $\mathcal{C}$*,* P *um projetor sobre* $\mathcal{C}$ *e* $\mathcal{E}$ *uma operação quântica (ruído quântico) com elementos de operação* E_i *(erros). Seja* $\mathcal{R}$ *uma operação quântica (detecção e correção) que preserva o traço, corrigindo os efeitos de* $\mathcal{E}$ *sobre* $\mathcal{C}$*. A condição necessária e suficiente para a existência de* $\mathcal{R}$ *é*

$$PE_i^\dagger E_j P = \alpha_{ij}P, \tag{5.46}$$

onde α_{ij} são elementos de alguma matriz α hermitiana de números complexos. A existência de $\mathcal{R}$ faz de E_i o conjunto dos erros corrigíveis.

Prova: *Vamos provar a suficiência de (5.46) como condição de existência de um CCEQ. A verificação direta por exigir muitas manipulações algébricas não será abordada neste trabalho.*

Seja E_i um conjunto de elementos de operação que satisfazem as condições de correção de erro (5.46). A matriz α, por hipótese, é hermitiana e portanto pode ser diagonalizada na forma

$$d = u^\dagger \alpha u, \tag{5.47}$$

onde u é uma matriz unitária e d uma matriz diagonal. Definimos um novo conjunto de operadores F_k como

$$F_k \equiv \sum_i u_{ik} E_i. \tag{5.48}$$

Pelo Teorema 8 temos que os operadores F_k também formam um conjunto de elementos de operação de $\mathcal{E}$. Como $F_k^\dagger = \sum_i u_{ki} E_i^\dagger$ então

$$P F_k^\dagger F_l P = \sum_{ij} u_{ki}^\dagger u_{jl} P E_i^\dagger E_j P. \tag{5.49}$$

Substituindo (5.46) em (5.49) tem-se:

$$P F_k^\dagger F_l P = \sum_{ij} u_{ki}^\dagger u_{jl} \alpha_{ij} P. \tag{5.50}$$

Como $d = u^\dagger \alpha u$ então

$$P F_k^\dagger F_l P = d_{kl} P. \tag{5.51}$$

Da decomposição polar, temos

$$F_k P = U_k \sqrt{P F_k^\dagger F_k P} = \sqrt{d_{kk}} U_k P, \tag{5.52}$$

sendo U_k um operador unitário. Multiplicando ambos os lados de (5.52) por $U_k^\dagger$ temos

$$F_k P U_k^\dagger = \sqrt{d_{kk}} U_K P U_K^\dagger \quad (5.53)$$

$$U_K P U_K^\dagger = \frac{F_k P U_k^\dagger}{\sqrt{d_{kk}}}. \quad (5.54)$$

Definindo o projetor P_k como

$$P_k \equiv U_k P U_k^\dagger = \frac{F_k P U_k^\dagger}{\sqrt{d_{kk}}}. \quad (5.55)$$

Utilizando (5.51) podemos provar que a família de subespaços P_k são ortogonais. Para $k \neq l$ temos:

$$P_l P_k = P_l^\dagger P_k = \frac{U_l P F_l^\dagger F_k P U_k^\dagger}{\sqrt{d_{ll} d_{kk}}} = 0. \quad (5.56)$$

Portanto a medida de síndrome é uma medida formada pelos operadores P_k acrescido, se necessário, de um outro projetor satisfazendo assim a relação de clausura $\sum_k P_k = I$. Para um certo estado ρ do código, sendo $\mathcal{R}$ a operação quântica de recuperação, podemos provar que U_k são os elementos de operação de $\mathcal{R}$. Desta forma, sendo $\mathcal{E}$ o ruído quântico em questão, temos:

$$\mathcal{E}(\rho) = \sum_l F_l \rho F_l^\dagger \quad (5.57)$$

$$\mathcal{R}(\mathcal{E}(\rho)) = \sum_l U_k^\dagger P_k F_l \rho F_l^\dagger P_k U_k. \quad (5.58)$$

Por outro lado, tem-se que:

$$U_k^\dagger P_k F_l \sqrt{\rho} = U_k^\dagger P_k^\dagger F_l \sqrt{\rho}; \quad (5.59)$$

$$= U_k^\dagger (\frac{U_k P F_k^\dagger}{\sqrt{d_{kk}}}) F_l \sqrt{\rho}; \quad (5.60)$$

$$= \frac{\delta_{kl} \sqrt{\rho}}{\sqrt{d_{kk}}}; \quad (5.61)$$

$$= \frac{\delta_{kl}}{\sqrt{d_{kk}}} \sqrt{\rho}, \quad (5.62)$$

pois, P é um projetor sobre $\mathcal{C}$ e ρ um estado de $\mathcal{C}$. Substituindo (5.62) em (5.58) temos

$$\mathcal{R}(\mathcal{E}(\rho)) = \frac{\delta_{kl}}{d_{kk}} \sqrt{\rho}; \quad (5.63)$$

$$\propto \rho. \quad (5.64)$$

De posse destes resultados podemos provar a condição de necessidade (5.46). Suponha um conjunto de erros corrigíveis E_i e elementos de operação R_j de $\mathcal{R}$. Seja ρ um estado qualquer e $P\rho P$ um estado pertencente ao código, temos de acordo com (5.64):

$$\mathcal{R}(\mathcal{E}(\rho)) \propto P\rho P. \tag{5.65}$$

De (5.58) e (5.65) tem-se:

$$\sum_{kl} R_k E_l P\rho P E_l^\dagger R_k^\dagger \propto P\rho P. \tag{5.66}$$

O Teorema 8 implica na existência de

$$R_k E_l P = c_{kl} P, \tag{5.67}$$

e

$$P E_l^\dagger R_k^\dagger = c_{kl}^* P, \tag{5.68}$$

onde c_{kl} é um número complexo. Desta forma:

$$P E_l^\dagger R_k^\dagger R_k E_j P = c_{kl}^* P c_{kj} P = c_{kl}^* c_{kj} P. \tag{5.69}$$

Como $\mathcal{R}$ é uma operação quântica que preserva o traço, ou seja, $\sum_k R_k^\dagger R_k = I$ e definindo $\alpha_{lj} \equiv \sum_k c_{kl}^* c_{kj}$ como elementos de uma matriz hermitiana de números complexos temos,

$$P E_l^\dagger E_j P = \alpha_{lj} P. \tag{5.70}$$

BIBLIOGRAFIA

[1] C.C. Tannoudji, B. Diu and F. Laloë. *Quantum Mechanics - Volume One*. John Wiely and Sons, New York, 1977.

[2] C.C. Tannoudji, B. Diu and F. Laloë. *Quantum Mechanics - Volume Two*. John Wiely and Sons, New York, 1977.

[3] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[4] C. H. Bennet. *Logical Reversibility of Computation.* IBM J. Res. 1973.

[5] P. Benniof. *The computer as a physical systems: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines.* J. Stat. Phys., 22(5), pp. 563-591, 1980.

[6] C. H. Bennett and G. Brassard. *Quantum cryptography: Public Key distribution and coin tossing.* In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179, New York, 1984. IEEE. Bangalore, India, December 1984.

[7] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information* Cambridge University Press, UK, 2000.

[8] C. H. Bennet, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. Wooters. *Teleporting an unknown quantum state via dual classical and EPR channels.* Phys. Rev. Lett. 70, pp. 1895-1899, 1993.

[9] P. Shor. *Alghoritms for quantum camputation: Discrete logarithms and factoring.* In Proc. 35^{th} Annual Symposium on Foundations of Computer Science, pp. 124, Los Alamitos, CA, 1994. IEEE Computer Society Press.

[10] L. K. Grover. *A fast quantum mechanical algorithm for database search*. In $28th$ ACM Symposium on Theory of Computation, pp. 212, New York, 1996. Association for Computing Machinery.

[11] N. Gershenfeld and I. Chuang. *Bulk spin resonance quantum computation.* Science, 275, pp. 350, 1997.

[12] I. Appelbaum, B. Huang, D. Monsma. *Electronic measurement and control of spin transport in silicon*. Nature May 17 2007 Vol. 447, pp. 295-298 DOI: 10.1038/nature05803.

[13] M. V. G. Dutt, L. I. Childress, L. Jiang, E. Togan, J. Maze, F. Jelezko, A. S. Zibrov, P. R. Hemmer, M. D. Lukin. *Quantum Register Based on Individual Electronic and Nuclear Spin Qubits in Diamond* Science 1 June 2007 Vol. 316, pp. 1312-1316 DOI: 10.1126/science.1139831.

[14] D. E. Chang, A. S. Sarensen, E. A. Demler, M. D. Lukin. *A single-photon transistor using nanoscale surface plasmons*. Nature Physics 26 Aug 2007 Vol.: Advance online publication.

[15] A. C. A. de Almeida. *Códigos Convolucionais Quânticos Concatenados*. Tese de Doutorado UNICAMP 2004.

[16] M. Grassl, T. Beth. *Quantum BCH Codes*. Proceedings X. International Symposium on Theoretical Electrical Engineering, Magdeburg, 1999, pp. 207-212.

[17] B. Masnick, and J.K. Wolf, *On Linear unequal error protection codes*, IEEE Trans. Inform. Theory, vol.IT-13, pp. 600-607, Oct. 1967.

[18] W. J. van Gils. *Linear unequal error protection codes from shorter codes*. IEEE Trans. Inform. Theory, vol 30, no. 3, pp. 544-546, May 1984.

[19] W. J. van Gils, *Two topics on linear unequal error protection codes: bounds on their length and cyclic codes classes*, IEEE Trans. Inform. Theory, vol.IT-29, pp. 866-876, Nov. 1983.

[20] R. Palazzo Jr. *Linear unequal error protection convolutional codes*. Proc. IEEE Int. Symp. Inform. Theory, Brighton, U.K., Jun. 1985, pp. 88-89.

[21] V.Pavlushkov, R. Johannesson, V. V. Zyablov, *Unequal error protection for convolutional codes*. IEEE Trans. Inform. Theory, vol. 52, no. 2, pp. 700-708, Feb. 2006.

[22] G. Caire, E. Biglieri, *Parallel concatenated codes with unequal error protection*. IEEE Trans. Commun., vol 46, no.5, pp. 565-567, May 1998.

[23] N. Rahnavard, H. Pishro-Nik, F. Fekri. *Unequal error protection using partially regular LDPC codes*. IEEE Trans. Commum., vol. 55, no.3, pp.387-391, Mar. 2007.

[24] J. Preskill. *Lectures Notes for Physics 229: Quantum Information and Computation.* California Institute 1998. Disponível em www.theory.caltech.edu/people/preskill/ph229.

[25] R. Landauer. *Irreversibility and heat generation in the computing process*. IBM J. Res. Dev., 5, pp. 183, 1961.

[26] A. Einstein; B. Podolsky and N. Rosen. *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev., 47(10), pp. 777-780, 1935.

[27] J.S.Bell. *On the Einstein-Podolsky-Rosen paradox.* Physics, 1, pp. 195-200, 1964.

[28] A. K. Ekert. *Quantum cryptography based on Bell's theorem* Phys. Rev. Lett., 67(6), pp. 661-663, 1991.

[29] W.K. Wooters and W.H. Zurek. *A single quantum cannot be cloned.* Nature, pp. 802-803, 1982.

[30] D. Diecks *Communication by EPR devices.* Physics Letter A, 92(6), pp. 271-272, 1982.

[31] D. Deutsch. *Quantum theory, the Church-Turing Principle and the universal quantum computer*. Proc. R. Soc. Lond. A, 400, pp. 97, 1985.

[32] D. Gottesman. *Stabilizer codes and quantum error correction.*PhD Thesis - California Institute of Technology, Pasadena, CA, 1997.

[33] P. W. Shor. *Scheme for reducing decoherence in quantum computer memory.* Phys. Rev. A, 52 (4), pp. 2493-2496, 1995.

[34] E. Knill and R. Laflamme. *A theory of quantum error-correcting condes.* Prys. Rev. A, 55(2), pp. 900-911, 1997.

[35] C. H. Bennet; D. P. DiVicenzo; J. A. Smolin and W. K. Wooters. *Mixed state entanglement and quantum error correction.* Phys. Rev. A, 54(5), pp. 3824-3851, 1996.

[36] R. Cleve. *Quantum stabilizer codes and classical linear codes.* Phys. Rev. A, 55(6), pp. 4054-4059, 1997

[37] A. R. Calderbanck and P. W. Shor. *Good quantum error-correcting codes exist.* Phys. Rev. A, 54(2), pp. 1098-1105, 1996.

[38] A. M. Steane. *Error correcting codes in quantum theory.* Phys. Rev. Lett., 77(5), pp. 793-797, 1996.

[39] L.A. Dunning and W. E. Robbins, *Optimal encodings of linear block codes for unequal error protection*,Inform. Contr., vol. 37, pp. 150-177, 1978.

[40] A. R. Caderbank and P. W. Shor. *Good quantum error-correcting codes exist*. Phys. Rev. A, 54(2), pp. 1098-1105, 1996.

[41] R. Palazzo, Jr., and K. V. O. Fonseca, *Unequal error protection of superlinear time-varying trellis coded modulation*, Proceedings of the 4-th Joint Sweden-USSR Intl Workshop on Inform. Theory, Visby, Sweden, 1989.

[42] C. C. Kilgus, W. C. Gore, *A class of cyclic unequal error protection codes*, IEEE Trans. Inform. Theory, vol.IT-18, pp. 687-690, Sept. 1972.

[43] D. Mandelbaum, *Unequal error protection codes derived from difference sets*, IEEE Trans. Inform. Theory, vol.IT-18, pp. 686-687, Sept. 1972.

[44] I. M. Boyarinov, and G. L. Katsman, *Linear unequal error protection codes*, IEEE Trans. Inform. Theory, vol.IT-27, pp. 168-175, Mar. 1981.

[45] D. G. Mills, D. J. Costello Jr., R. Palazzo Jr., *Achieving unequal error protection with convolutional codes*, submetido para publicação.