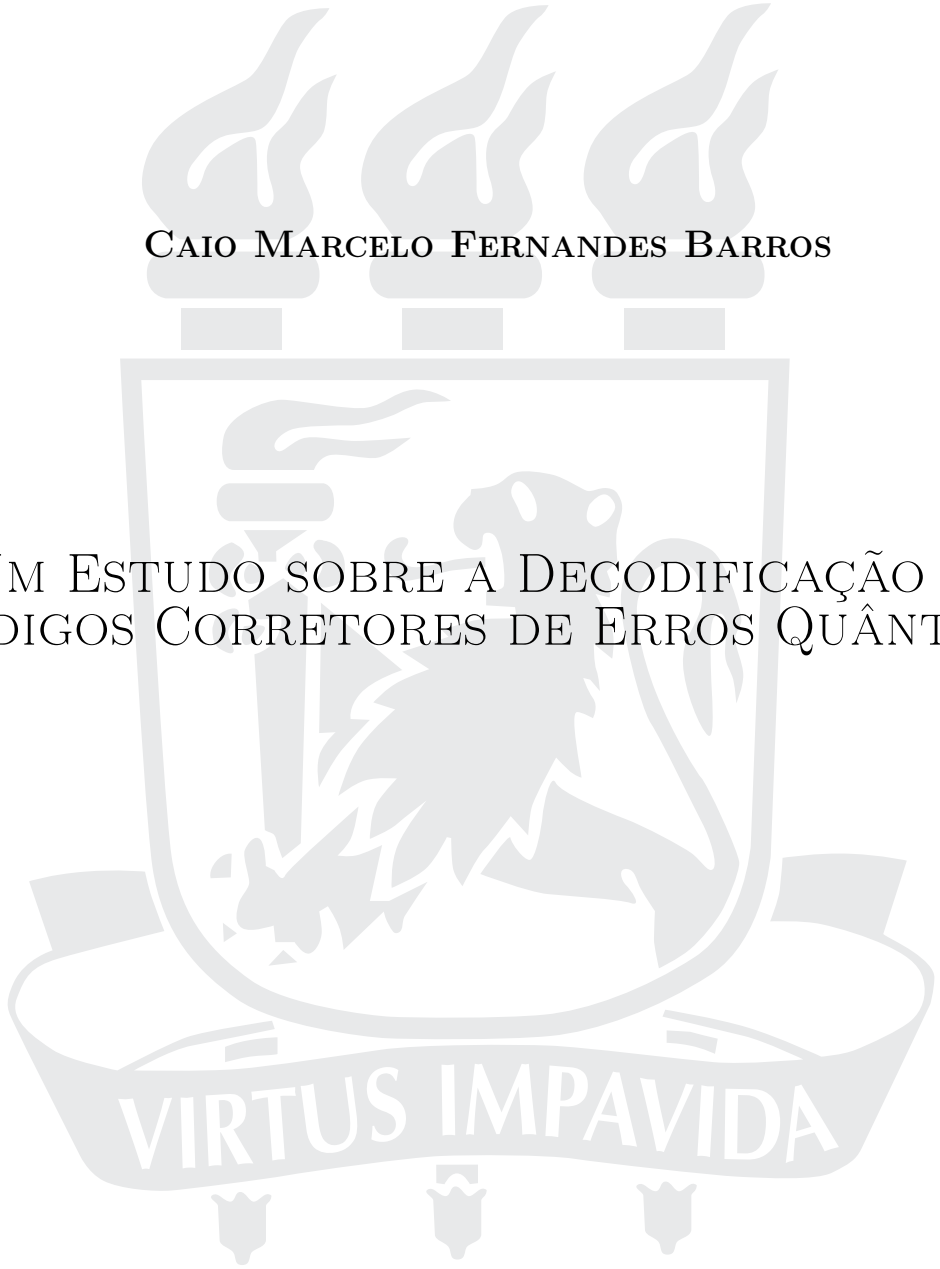
Universidade Federal de Pernambuco
Centro de Tecnologia e Geociências
Programa de Pós-Graduação em Engenharia Elétrica



Caio Marcelo Fernandes Barros

Um Estudo sobre a Decodificação de Códigos Corretores de Erros Quânticos

Orientador : Hélio Magalhães de Oliveira, Dr.

Recife, Julho de 2011.

Sumário

Lista de Figuras

Lista de Tabelas

capítulo 1

Introdução

A área das telecomunicações, tudo o que está relacionado à troca de informação entre pontos distantes no espaço, cresce a passos largos. As inovadoras tecnologias oriundas desta área têm impacto em diversas áreas da sociedade, modificando o mundo para o estado em que se encontra atualmente, de modo que seria muito difícil de concebê-lo sem os seus benefícios. O mais surpreendente é que a eletrônica, principal área contribuidora, tem seu nascimento bastante recente. A sua história se confunde com parte da história moderna das telecomunicações. As válvulas eletrônicas, antecessores dos transistores, têm sua origem relacionada aos tubos de raios catódicos usados nas experiências de J. J. Thompson na descoberta do elétron, em que recebeu o prêmio Nobel de física no ano de 1906. Através desse dispositivo foram inventados meios revolucionários de comunicação, os rádios em transmissão AM e FM, com contribuições relevantes de E. H. Armstrong [1], os televisores e os antigos computadores.

Os sinais analógicos eram, sem sombra de dúvida, os sinais conhecidos preferidos como formas de comunicação/ transmissão daquela época. No entanto, esse cenário estava por ser modificado quando surgiu o teorema da amostragem, atualmente atribuído a quatro autores, Whittaker, Nyquist, Shannon e Kotelnikov [34]. Este teorema permitia que sinais analógicos de banda limitada pudessem ser convertidos em sinais binários de modo que no processo de recuperação não ocorresse perda da informação contida no sinal original [2]. Outro avanço no âmbito das telecomunicações ocorreu na década de 40, quando C. E. Shannon tentou responder a duas questões: "Quais os recursos estritamente necessários para se enviar informação através de um canal de comunicação?" E "como seria possível proteger a informação enviada em um canal de comunicação contra os efeitos nocivos do ruído presente no meio?" Em uma primeira etapa foi necessário que Shannon definisse, matematicamente, o conceito de informação para então responder aos questionamentos, respectivamente, através dos teoremas da codificação em canais sem ruído e da codificação em canais ruidosos [3]. Esses teoremas são de vital importância para as telecomunicações, pois a teoria surgida através deles reflete bem os problemas de comunicação encontrados na realidade.

Shannon mostrou [3], com o segundo teorema, que se pode transmitir informação através de um canal ruidoso de maneira tal que esta informação, relevante ao destinatário, possa ser recuperada

com confiabilidade controlada. É necessário, no entanto, a construção de códigos para a proteção dessa informação. Este teorema também estabelece um limite superior para a proteção que pode ser alcançada por tais códigos. Infelizmente, esta prova não é construtiva, ou seja, sabe-se que existem códigos que atingem a cota superior de proteção (como exemplo pode-se citar os códigos turbos [35]). Desde então, diversos pesquisadores tentam encontrar maneiras de construir códigos que apresentem essa propriedade, criando assim uma área de pesquisa bastante versátil e sofisticada que proporcionou conquistas tecnológicas importantes. Como exemplo dessas conquistas temos os gravadores e reprodutores de CDs e DVDs, a comunicação por satélite, modems, entre outras.

Na mesma época ocorria outro avanço também importante para a concretização da era digital. Em 1948, J. Bardeen, W. Brattain e W. Shockley apresentaram ao mundo o primeiro transistor [36], transistor de junção bipolar, TBJ, considerado como uma das invenções mais relevantes para as áreas da computação e dos sistemas eletrônicos [4]. A partir de então houve a necessidade de se ter sistemas mais rápidos e eficientes, apresentando uma melhora em sua qualidade. Este fato caracterizou a corrida pela melhoria dos dispositivos e processos de fabricação, tornando-os cada vez menores e mais velozes. Por volta da metade dos anos 60, a constatação de que os processos de fabricação estavam concebendo dispositivos cada vez menores, proporcionando assim um fantástico crescimento das áreas ligadas a esses dispositivos, computação e telecomunicação, levou a criação de uma lei empírica bastante interessante. A lei empírica de Moore, proposta por Gordon Moore [37], diz que a um custo constante, a capacidade dos computadores dobra a cada dois anos. A veracidade desta lei vem sendo verificada desde a sua proposição. Ocorre que os meios convencionais de fabricação desses dispositivos estão encontrando dificuldades relacionadas aos tamanhos dos mesmos, tendo em vista que atingiu-se escalas nanométricas que são responsáveis pelo alto desempenho de certos aparelhos eletrônicos. Efeitos quânticos passam a ser observados e se tornam relevantes para estes dispositivos, o que provocaria uma estagnação da tecnologia caso esses problemas não pudessem ser contornados. Então uma nova teoria deve ser desenvolvida provendo assim uma continuidade aos avanços requeridos.

A outra ponta para o desenvolvimento desta nova teoria é a ferramenta conceitual que teve seus primeiros passos no início do século XX, a física quântica. O nascimento da física quântica, no final do Século XX, foi proporcionado pelas incoerências explicativas da teoria física vigente [5]. Podemos mencionar o problema da radiação de corpo negro, o problema da espiralização do elétron para o núcleo do átomo, entre outros. A solução encontrada foi incorporar hipóteses à antiga teoria para a explicação desses fenômenos, mas isso não ocorreu de forma a obter resultados satisfatórios pelas constantes contradições que se seguiram. Então, no ano de 1920, foi criada a mecânica quântica, que vem a ser um conjunto de regras, fundamentos matemáticos, para a explicação, entendimento, inicialmente, de fenômenos relacionados aos estudos dos átomos e partículas fundamentais, ou seja, atualmente, está relacionada à criação de teorias físicas. Podemos destacar grandes cientistas pioneiros na área, tais como: N. Bohr, P. Dirac, E. Schrödinger, W. Heisenberg, M. Planck.

Desta forma, uma aposta para a continuidade do desenvolvimento, evolução dos sistemas eletrônicos, computadores e os sistemas de telecomunicações em geral é a teoria da informação quântica. A teoria da informação quântica pode ser construída a partir dos fundamentos bem estabelecidos da teoria da informação e da mecânica quântica. Esses novos computadores estarão a utilizar novos componentes, conceitos, diretamente relacionados à mecânica quântica. A unidade fundamental de informação, para a tecnologia clássica, é conhecida como bit. No entanto para este novo paradigma

esta nova unidade básica de informação é conhecida como q-bit. As portas lógicas são também modificadas de modo a se adaptarem a essa nova unidade de informação. Todos esses novos conceitos, as idéias relacionadas ao fato de que os novos computadores poderiam operar no nível da mecânica quântica, ao invés da física convencional, seriam concebidos para que esse novo computador pudesse realizar tarefas de modo eficiente.

Este ganho de eficiência é medido quando se relacionam tarefas que para um computador convencional requereriam um esforço computacional considerável. É sobre este fato, por exemplo, que a segurança dos criptossistemas atuais está embasada [6], pois para a computação clássica existe uma dificuldade bastante relevante na fatoração, encontrar os fatores primos, de números de alta ordem de grandeza ou na resolução do problema do logaritmo discreto. No entanto, prevê-se que para um computador quântico esta tarefa não representaria grande esforço, a utilização da transformada de Fourier quântica daria um ganho de velocidade, comparando-se aos melhores algoritmos convencionais, quer para o problema da fatoração, quer para o problema do logaritmo discreto. Outro ganho dessa nova tecnologia estaria relacionado ao problema de buscas em conjuntos, por exemplo, encontrar o elemento mínimo em um conjunto desordenado ou então a busca de chaves criptográficas, referindo-se aos melhores algoritmos, o algoritmo de Grove [7] desempenha um ganho quadraticamente mais eficiente. Por sua vez, como já foi mencionado, os *hardwares* seriam também modificados para adaptar-se a essa nova concepção. Para que essa modificação fosse, em princípio, alcançada era necessário que se pudesse obter um controle mais substancial sobre os sistemas quânticos isolados. Isso foi possível a partir da década de 1970, pois antes disto, o controle sobre estes sistemas isolados não era tão sofistiado. Os métodos de aprisionamento de átomos e as armadilhas iônicas [39], estas nos últimos anos veem sendo consideradas como experimentos promissores, proporcionaram realizar-se experimentos com bastante precisão. Desta forma novos maquinários puderam ser elaborados, tais como o microscópio de tunelamento de varredura [38] que move átomos podendo criar novas configurações atômicas e dispositivos eletrônicos usados na transferência, individual, de elétrons.

A seguir, na tabela 1.1, um breve relato histórico sobre a evolução dos sistemas quânticos, no intuito de abordar a contextualização do processo evolutivo desta nova área do conhecimento no atual ambiente tecnológico e de evidênciar quais foram os caminhos tomados para o desenvolvimento pleno do seu estado da arte.

Tabela 1.1: Histórico Evolutivo dos Sistemas Quânticos.

Ano	Acontecimento
1973	Comprovação da possibilidade da computação reversível, C. Bennet [8].
1980	Proposição do computador quântico por P. Benioff, embasado por trabalhos de C. Bennet [9].
1984	Protocolo criptográfico BB84, por C. Bennet e G. Brassard. [10].
1985	Criação do primeiro algoritmo quântico, por *D. Deutsch* [7].
1993	Proposição do teletransporte quântico, por C. Bennet e colaboradores [11].
1994	Algoritmo de fatoração, por P. Shor [12].
1994	Algoritmo de busca, por *L. Grover* [13].
1996	Demonstração experimental, pela IBM, do protocolo BB84.
1997	Descoberta dos estados pseudo-puros, comunicação quântica por RMN[1], por *N. Gershenfeld* e *I. Chuang* [14].
1998	Demonstração dos algoritmos de busca e teletransporte através da computação quântica por RMN e concepção de portas lógicas quânticas.
2001	Demonstração do algoritmo de Shor por RMN[1].
2003	Emaranhamento de spins do núcleo e de um elétron na mesma molécula por combinação de RMN[1] e RPE[2].
2004	Transferência de informação de matéria à luz iniciando as redes quânticas em grande escala, por pesquisadores do Inst. Tecnológico da Georgia.
2004	Transferência de informação de luz à matéria, por pesquisadores do Inst. Max Planck.
2007	Descoberta do *q-bit* de diamante [16].
2007	Demonstração de uma teoria para a construção do transistor para um computador quântico por pesquisadores das Universidades de Copenhagen e Harvard [17].
2010	Armadilha iônica para transmissão em antenas [20]

capítulo 2

Princípios da Informação Quântica

"Quels que soient les progrès des connaissances humaines, il y aura toujours place pour l'ignorance et par suite pour le hasard et la probabilité."
Émile Borel

O conceito básico fundamental de informação , em que se refere a comunicações digitais, é o bit, termo derivado da abreviação dos nomes **bi**nary uni**t**. Este elemento básico pode assumir dois e somente dois possíveis valores, 0 ou 1. No entanto, para a teoria da informação quântica, a unidade fundamental de informação, para comunicações quântica, conhecida por **bit q**uântico, recebe a designação de *qbit*, pode assumir dois possíveis valores e quaisquer estados intermediários entre eles em um espaço tridimensional. Da mesma maneira que o bit pode ser representado fisicamente, por exemplo, por dois níveis diferentes de tensão para a indicação de dois possíveis valores diferentes, o q-bit também possui representação física. Os exemplos são diversos, tais como as duas polarizações do fóton, os estados de excitação de um átomo, os estados de alinhamentos de um spin nuclear. Nesta dissertação será considerada somente a representação matemática desse elemento.

Neste capítulo faz-se necessário a introdução de alguns conceitos matemáticos. Uma visita aos conceitos relacionados à álgebra linear e às manipulações matriciais é requerida para que o entendimento pleno desse nova ferramenta seja alcançado. Uma notação própria é introduzida para uma designação específica nesta área do conhecimento, entre outros conceitos.

2.1 Alguns Conceitos de Álgebra Linear

A notação de *Dirac* é usada, como padrão, para representação do q-bit [43]. Esta notação é conhecida como *braket*, em que $|.\rangle$ é nomeado de *ket* e $\langle .|$ é nomeado de *bra*. Essa notação vem para

representar as n-uplas com entradas complexas, o conjunto de vetores em $\mathbb{C}^n$, o conjunto de interesse da mecânica quântica. Assim, a Equação (2.1) representa um vetor arbitrário pertencente a $\mathbb{C}^n$. As representações se relacionam em que uma é a dual da outra, no contexto mencionado.

$$|\psi\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}; \langle\psi| = \begin{pmatrix} a_1^* & a_2^* & \cdots & a_n^* \end{pmatrix}; \tag{2.1}$$

O símbolo * sobrescrito indica o complexo conjugado. Outro fato importante reside sobre a representação do elemento nulo, o vetor zero, definido por 0. Este elemento do espaço vetorial é a exceção em relação ao uso da notação de *Dirac*, ele é representado sem a notação para que não haja confusão em relação ao elemento $|0\rangle$ que representa um estado quântico bem definido.

Após essas definições iniciais é possível conceber a idéia de um conjunto de elementos $|v_1\rangle$, $|v_2\rangle$, $\cdots$, $|v_n\rangle$, oriundos do mesmo espaço vetorial, de tal modo que qualquer vetor, que pertença ao mesmo espaço desse vetores, possa ser representado por uma soma ponderada, ou seja, uma combinação linear dos elementos desse conjunto, o qual definimos como conjunto gerador do espaço considerado. A equação (2.2) mostra a expressão de um vetor arbitrário como combinação linear dos vetores de um espaço arbitrário.

$$|w\rangle = a_1 |v_1\rangle + a_2 |v_2\rangle + \cdots + a_n |v_n\rangle . \tag{2.2}$$

Exemplo 2.1.1. *Como exemplo, podemos considerar o espaço vetorial $\mathbb{R}^2$, que por sua vez está contido no espaço vetorial $\mathbb{C}^{n\,2}$:*

$$|i\rangle \triangleq \vec{i} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; e \; |j\rangle \triangleq \vec{j} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Podemos representar qualquer vetor a partir dos vetores apresentados, $|i\rangle$ e $|j\rangle$.

□

Uma característica exigida para um conjunto gerador é a *independência linear*. Considere a expressão 2.3, caso haja $a_t \neq 0$, para algum valor de t, de modo que esta seja verificada, então o conjunto gerador tem a característica de ser linearmente dependente. Caso contrário, receberia a característica de independência linear.

$$0 = a_1 |v_1\rangle + a_2 |v_2\rangle + \cdots + a_j |v_j\rangle . \tag{2.3}$$

Exemplo 2.1.2. *Considere dois vetores, $|f_1\rangle$ e $|f_2\rangle$, mostrados abaixo.*

$$|f_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; e \; |f_2\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Através da Equação (2.3), podemos verificar que essa escolha de vetores para compor a base vetorial recebe a característica de ser linearmente independente. O mesmo pode ser dito da escolha de vetores do Exemplo (2.1.1)

□

Uma maneira de relacionar espaços vetoriais, diferentes ou não, é através de um *operador linear* A, mais convenientemente representado por matrizes. Matematicamente, um *operador linear* A é definido como uma aplicação de uma matriz, de dimensões m por n e entradas no corpo dos complexos, que relaciona um vetor, de um espaço vetorial de dimensão m e entradas no corpo dos complexos, e outro vetor, de um espaço vetorial de dimensão n e entradas no corpo dos complexos. Normalmente escreve-se $A|v\rangle = |w\rangle$ para indicar essa aplicação.

É de extrema importância saber que uma *transformação linear* também pode ser considerada como uma aplicação de um *operador linear*, e desta forma toda aplicação de um operador linear se torna bem especificada quando esta ocorre nos vetores da base. A partir da equação 2.2 podemos representar de maneira geral a aplicação de um *operador linear*.

$$A|v\rangle = A\left(a_1|v_1\rangle + a_2|v_2\rangle + \cdots\right) = a_1 A|v_1\rangle + a_2 A|v_2\rangle + \cdots \tag{2.4}$$

Fica claro que a representação de um vetor qualquer através dos vetores componentes da base pode facilitar o entendimento do comportamento de certos operadores lineares, dessa forma existe uma maneira de se encontrar os coeficientes da equação 2.2 que não seja por tentativa e erro, esta maneira fica a cargo de uma operação conhecida por *produto interno*, entre vetores.

O *produto interno* sobre um espaço V é definido como uma função que associa a um par de vetores um número complexo obedecendo algumas propriedades [18]. No contexto da notação de *Dirac* e da mecânica quântica podemos definir o *produto interno* entre $|v\rangle$ e $|w\rangle$ como o produto de $\langle v|$, dual de $|v\rangle$, por $|w\rangle$. A notação padrão para o produto interno entre $|v\rangle$ e $|w\rangle$ é $\langle v|w\rangle$, algumas vezes é utilizada também $(.;.)$.

É interessante observar que o *produto interno* é uma função que opera entre vetores do mesmo espaço vetorial. Diante do conceito de produto interno é possível definir características importantes relacionadas aos vetores tais como a norma de um vetor e a ortogonalidade. Um espaço vetorial munido da propriedade de produto interno é chamado "espaço de produto interno". Frequentemente, as discussões em mecânica quântica fazem referência a um espaço vetorial específico, o espaço de *Hilbert*. Para vias de entendimento basta considerar o espaço de *Hilbert* um espaço vetorial de produto interno.

Exemplo 2.1.3. *Seja um vetor* $|v\rangle = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$, *pertencente a* $\mathbb{R}^2$. *Seja também uma base linearmente independente e ortonormal, cujos vetores* $|v_1\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}/\sqrt{2}$ *e* $|v_2\rangle = \begin{pmatrix} -1 \\ 1 \end{pmatrix}/\sqrt{2}$, *são seus elementos. Aplicando o produto interno entre os vetores da base no vetor considerado, podemos calcular quais são os coeficientes, equação 2.2, para compor a combinação linear do vetor em questão.*

$$a_1 = \langle v_1|v\rangle = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 2 \\ 4 \end{pmatrix} = 3\sqrt{2}.$$

$$a_2 = \langle v_2|v\rangle = \begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 2 \\ 4 \end{pmatrix} = \sqrt{2}.$$

□

Embasados pelo conceito do produto interno podemos definir um operador linear A de V em W, $A|v\rangle = |w\rangle$ como sendo $A = |w\rangle\langle v|$, se $\langle v|v\rangle = 1$. Esta maneira de representar um operador linear é conhecida como representação através do produto externo entre vetores. A vantagem que se tem em se representar um operador linear dessa forma esta relacionada a um importante resultado conhecido como *relação de completitude*[7].

Teorema 2.1. *Sejam* $|0\rangle$, $|1\rangle$, $\cdots$, $|i-1\rangle$, *vetores que compõem uma base linearmente independente ortonormal de* V, *com dimensão* i. *Através do produto externo têm-se que:*

$$\sum_{k=0}^{i-1} |k\rangle\langle i| = I.$$ *Em que* I *representa a matriz identidade.*

Exemplo 2.1.4. *Considere um vetor* $|v\rangle = \begin{pmatrix} i/\sqrt{10} \\ 3/\sqrt{10} \end{pmatrix}$, *pertencente ao* C^2. *Considere também um operador linear* A, *cuja aplicação sobre o vetor* $|v\rangle$ *resulta no vetor* $|w\rangle = \begin{pmatrix} i \\ i \end{pmatrix}$. *Desta forma tem-se que a representação por produto externo do operador linear* A *é:*

$$A|v\rangle = A\begin{pmatrix} i/\sqrt{10} \\ 3/\sqrt{10} \end{pmatrix} = \begin{pmatrix} i \\ i \end{pmatrix}.$$

$$A = \begin{pmatrix} i \\ i \end{pmatrix}\begin{pmatrix} \frac{-i}{\sqrt{10}} & \frac{3}{\sqrt{10}} \end{pmatrix}.$$

$$A = \begin{pmatrix} \frac{1}{\sqrt{10}} & \frac{3i}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} & \frac{3i}{\sqrt{10}} \end{pmatrix}.$$

□

Existe um conjunto especial de vetores relacionado diretamente a um operador linear A. Esse conjunto é conhecido como conjunto de *autovetores* do operador linear A; estes, são tais que $A|v\rangle = \lambda|v\rangle$, para todo vetor pertencente a este conjunto. o número complexo λ é denominado autovalor do autovetor $|v\rangle$. Uma maneira de se encontrar todos os possíveis autovalores λ de um operador linear específico A é através das raízes do polinômio característico do operador, Equação (2.5).

$$c(\lambda) = det|A - \lambda I|. \tag{2.5}$$

O teorema fundamental da álgebra garante que dado um polinômio de grau estritamente positivo e coeficientes complexos, existe pelo menos uma raiz complexa [40]. Então, pela equação característica, equação 2.5, é garantido que para um dado operador linear existe, assim, um autovalor, correspondente a um autovetor associado ao operador linear A, ou seja, para qualquer operador linear é garantido existir pelo menos um autovalor e autovetor associados entre si e ao próprio operador.

Uma representação alternativa para um operador A em um espaço vetorial V é conhecida como representação diagonal. Esta representação é tal que é formada pelo produto externo de todos os vetores pertencentes ao autoespaço, ponderada pelos seus autovalores. $A = t_1|v_1\rangle\langle v_1| + t_2|v_2\rangle\langle v_2| +$

$\cdots$, em que t_i é o autovalor associado ao autovetor $|v_i\rangle$. Um operador é diagonalizável se ele aceitar uma representação diagonal [18].

Exemplo 2.1.5. *Sejam* $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *e* $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$*, dois vetores pertencentes ao* $\mathbb{C}^2$*. Considere também um operador linear* $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$*. O polinômio característico, Equação (2.5), do operador* Z *é* $c(\lambda) = (1-\lambda)(-1-\lambda)$*. Concluí-se então que os possíveis autovalores do operador são* 1*, associado ao vetor* $|0\rangle$*, e* -1*, associado ao vetor* $|1\rangle$*. Deste modo pode-se escrever o operador* Z *como se segue:*

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

□

Da mesma maneira que os vetores possuem um representante dual de si mesmo, os operadores também o têm, chamado de operador *adjunto* de A, ou também conjugado *hermitiano*. Por definição, dado qualquer operador linear A com aplicação em um espaço vetorial V, tem-se que: $(|v\rangle\,; A\,|w\rangle) = (A^\dagger\,|v\rangle\,; |w\rangle)$, em que $A^\dagger$ é o único operador linear no espaço vetorial V, para qualquer $|v\rangle$ e $|w\rangle$, em que a relação é possível. Ocorre que existem operadores que são seus próprios adjuntos, conhecidos assim como auto-adjuntos. Mencionar esta classe de operadores é interessante diante de dois resultados importantes, verificados mais adiante, os *projetores*, Teorema (2.2) e o *teorema espectral*, Teorema (2.3); as demonstrações e abordagen mais aprofundadas sobre esses assuntos encontram-se em [7].

Teorema 2.2. *Dada uma base ortonormal sobre um espaço vetorial* W*,* $|1\rangle$,$|2\rangle$,$\cdots$,$|d\rangle$*, de modo que o conjunto de vetores,* $|1\rangle$,$|2\rangle$,$\cdots$,$|k\rangle$*, tal que* $k < d$*, é também uma base para um espaço vetorial* V *contido em* W*, diz-se que*

$$P = (|1\rangle\langle 1| + |2\rangle\langle 2| + \cdots + |k\rangle\langle k|)\,,\ \textit{é um projetor sobre } V.$$

□

Caso $A^\dagger A = AA^\dagger$, este operador é denominado como **normal**. O *teorema espectral* garante que um operador é normal se e só se ele for diagonalizável.

Teorema 2.3. *Qualquer operador normal* M *em um espaço vetorial* V *é diagonal em relação a alguma base ortonormal de* V*. Reciprocamente, qualquer operador diagonalizável é normal.[18]*

Existe ainda uma operação importante, entre vetores, que vale ser mencionada, conhecido como *produto tensorial*. Define-se o *produto tensorial* através do símbolo $\otimes$, que relaciona um par de vetores de dimensões x e y, respectivamente, a um vetor de dimensão $x + y$. Esta operação pode relacionar, também, operadores lineares.

Exemplo 2.1.6. *Seja* $|x\rangle = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}$ *e* $|y\rangle = \begin{pmatrix} 1 \\ 5 \end{pmatrix}$*, dois vetores de dimensões* 3 *e* 2 *respectivamente.*

O vetor $|v\rangle$ é o resultado do produto tensorial desses dois vetores.

$$|v\rangle = |x\rangle \otimes |y\rangle = \begin{pmatrix} 1\begin{pmatrix} 1 \\ 5 \end{pmatrix} \\ 2\begin{pmatrix} 1 \\ 5 \end{pmatrix} \\ 4\begin{pmatrix} 1 \\ 5 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 2 \\ 10 \\ 4 \\ 20 \end{pmatrix}$$

□

No campo da mecânica quântica existe uma interessante relação entre operadores que é bastante útil; essa relação é chamada de comutatividade. Foram definidas para essa relação, duas operações específicas conhecidas como *comutador* e *anticomutador*, respectivamente mostradas a seguir:

$$[A;B] = AB - BA. \text{ e } \{A;B\} = AB + AB.$$

Caso dois operadores comutem $[A;B] = 0$ e caso anticomutem $\{A;B\} = 0$.

Detalhes de propriedades relacionadas aos produtos interno, externo, tensorial e tudo o mais que foi mencionado nesta seção não foram descritas, a despeito de serem de interesse para uma compreensão bem fundamentada para os postulados da mecânica quântica. É necessário, desta forma, tornar essa linguagem familiar para que se possa entender amplamente todo o desenvolvimento teórico vindouro [7][19][21].

capítulo 3

Postulados da Mecânica Quântica

"Les jeux de langage sont les formes de langage par lesquelles un enfant commence à utiliser les mots. L'étude des jeux de langage est l'étude de formes primitives du langage, ou de langages primitifs"
Ludwig Wittgenstein

Há um engano, por parte de alguns interessados na área da física, em pensar que a mecânica quântica é uma teoria física, e a cerca desse tema existe acalorado debate entre os físicos quanto a divergência dessa idéia. O que ocorre na realidade é que o papel fundamental da mecânica quântica é dar estrutura matemática, através dos seus postulados fundamentais, para que uma teoria científica possa ser formulada. Desta forma, não faz parte do seu tronco principal de proposições ser uma teoria científica, é o seu papel ainda mais sutil, ela foi desenvolvida para prover, fornecer, apoio conceitual e matemático para o desenvolvimento destas teorias. O desenvolvimento desses postulados através dos anos foi realizado por processos exaustivos e persistentes de tentativas e erros - os quais por vezes incluía escolhas infelizes e por vezes escolhas que aparentavam ser adivinhações.

Postulado 3.1. *A qualquer sistema físico isolado existe associado um espaço vetorial complexo, munido com produto interno, conhecido como espaço de estados do sistema. O sistema é completamente descrito pelo seu vetor de estado, um vetor unitário no espaço de estados.*

É interessante notar que este postulado, podendo ser encontrando em [7], não especifica que tipo de estrutura vetorial deve ser usado. Cada situação requer que o pesquisador adapte o sistema de estudo a um espaço vetorial e também o elemento de estudo a um elemento do espaço vetorial. Diversos sistemas físicos veem sendo bem sucedidamente explicados por meio dessas adaptações, um exemplo disto é a Eletrodinâmica Quântica (EDQ). Esta teoria tem por objetivo apresentar as interações

existentes entre os átomos e a luz. Por questões de conveniência didática e ocasião de entendimento de todo o trabalho textual, este texto primará por expor o sistema quântico mais simples, o qbit. Podemos considerar o qbit como um ente matemático que, em um sistema físico genérico de estudo, apresenta duas dimensões, em seu caso binário, e os seus vetores da base são ortonormais, $|0\rangle$ e $|1\rangle$. Assim qualquer estado quântico arbitrário pode ser expresso como:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{3.1}$$

Em que os números complexos α e β são restritos de forma que o estado quântico, da Equação (3.1), seja representado pelo vetor de estados unitário. Isso quer dizer que o produto interno deste estado consigo mesmo deve ter valor 1, ou seja, $\langle\psi|\psi\rangle = 1$. Esta relação se estende aos números α e β produzindo a relação de normalização, $|\alpha|^2 + |\beta|^2 = 1$. Não é coincidência a semelhança entre os estados da base e os valores possíveis para os níveis lógicos do bit clássico, o que ocorre é que no caso do qbit não existe a necessidade do estado quântico estar exclusivamente em um dos estados da base, pode ocorrer de o estado quântico figurar em um arranjo intermediário entre os estado da base, o que se conhece como superposição de estados, fato que não acontece com o bit clássico. É pouco palpável a idéia de um elemento poder estar em um estado intermediário entre dois estados bem definidos, no sentido de que o mundo em volta não evidência casos como este frequentemente. Por exemplo, em um jogo de cara e coroa, em perfeitas condições, os possíveis resultados são cara ou coroa e somente estes casos. É difícil imaginar que em um jogo como este a moeda permaneceria em um estado intermediário entre as duas faces. No entanto é justamente isto que acontece com o *qbit*, ele permanece em um estado intermediário contínuo entre os estados da base, até que seja examinado.

No caso clássico é bastante comum examinarmos qual o nível lógico de um determinado bit que trafega em um canal de comunicação; isso não pode acontecer com o *qbit*. Por apresentar-se em um estado de superposição, qualquer tentativa de examinar a ponderação de um estado da base irá danificar a ponderação do outro estado da base, considerando a base computacional binária, pois examinar é sinônimo de medir [44]. Como será mostrado mais adiante, medir significa interagir com o vetor de estado, modificando-o. Pode-se pensar também, por exemplo, em um átomo que está a ser excitado; um átomo ao ser excitado, dependendo da excitação, pode emitir um elétron que está preso a ele. Então existem dois possíveis casos, ou o átomo emite o elétron, o que representa um estado quântico possível denominado $|$é emitido$\rangle$, ou o átomo não emite o elétron, o que representa o outro estado quântico possível denominado $|$é preso$\rangle$. É possível que se o fornecimento de energia para que o átomo emita esse elétron seja contínuo e crescente, este fato ocorrerá. No entanto, em qualquer instante de tempo desde o início do fornecimento de energia, haverá uma probabilidade de o elétron ser emitido e consequentemente a probabilidade complementar deste não ser emitido, este fato por si só configura um clássico estado de superposição, em que os estados $|$é emitido$\rangle$ e $|$é preso$\rangle$ são os estados ortonormais da base.

Outro exemplo clássico dos estados superpostos é a experiência do gato de Schrödinger [44]. Considere haver numa caixa um contador Geiger-Müller, uma massa radioativa ligada somente ao contador, um martelo e um vidro com gás venenoso. Um gato seria colocado no interior da caixa juntamente com todos os utensílios e em seguida a caixa seria hermeticamente fechada. Os objetos seriam dispostos de tal modo que o contador Geiger-Müller ao detectar uma emissão radioativa da massa acionaria o martelo que quebraria o frasco com o gás venenoso, matando assim o gato. A

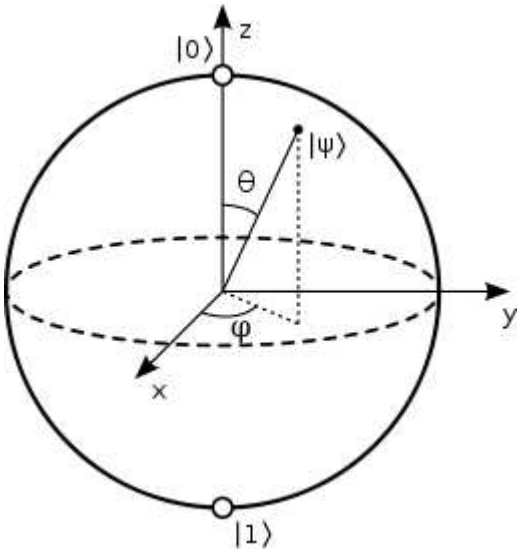


Figura 3.1: Representação de um qbit na Esfera de Bloch

situação descrita por Schrödinger é semelhante a excitação atômica, ressaltando o fato que a única maneira de o frasco com gás ser quebrado é através do martelo que só pode ser acionado pelo contador Geiser-Müller. Assim a partir do momento em que a caixa é lacrada, existe a possibilidade do gato esta vivo ou morto e só essa duas possibilidades.

Um espaço vetorial munido de produto interno pode ser associado à situação descrita, em que os estados da base desse sistema vetorial são as duas possibilidades, mutuamente excludentes, apresentadas, o gato está vivo, $|\text{vivo}\rangle$, ou o gato está morto, $|\text{morto}\rangle$. Desde o instante em que a caixa foi fechada e o contador posto a operar, havia uma probabilidade crescente com o tempo de o gato estar morto e complementarmente a probabilidade deste permanecer vivo, assim enquanto a caixa estiver lacrada, existiram essas probabilidades que representam, indiretamente, os números complexos α e β da Equação (3.1). É interessante notar que a dualidade/superposição dos estados quânticos é consequência direta do desconhecimento a priori.

O ato de se realizar uma medida nesse sistema quântico é abrir a caixa e neste instante o gato está ou vivo, $|\text{vivo}\rangle$, ou está morto, $|\text{morto}\rangle$, dissipando assim qualquer dúvida ou, em outras palavras destruindo a superposição. Antes disso, pode-se dizer que o gato está em um limbo, ou seja, ente a vida e a morte, entre os estado $|\text{vivo}\rangle$ e $|\text{morto}\rangle$.

Para facilitar o entendimento do conceito de estados quânticos representados por qbits, a Figura (3.1) mostra uma representação geométrica do mesmo através da esfera de Bloch [45]. Os ângulos θ e φ determinam um ponto sobre a superfície da esfera que tem raio unitário, já que o vetor de estado tem essa característica. É comum utilizar-se deste elemento geométrico para visualizar o funcionamento de um determinado operador sobre o vetor de estado. Esta representação, evidênciada pela Equação (3.2), também é limitada, pois existem casos muito complicados em que a mesma não consegue extrapolar ao ponto de representar fielmente os acontecimentos desejados.

$$|\psi\rangle = \mathrm{e}^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right). \tag{3.2}$$

Postulado 3.2. *A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Em outras palavras, o estado quântico* $|\psi_1\rangle$ *de um sistema em um tempo* t_1 *está relacionado ao estado quântico* $|\psi_2\rangle$ *do sistema em um tempo* t_2 *por um operador unitário* U *que depende unicamente de* t_1 *e* t_2*.*

Igualmente como no caso do postulado 3.1, e que também pode ser encontrado em [7], em que não é possível definir qual a melhor adaptação do sistema vetorial para o sistema quântico, este postulado não determina que tipo de transformação unitária deve ser usada para descrever a transformação temporal verificada em um estado quântico. Este postulado somente garante que uma transformação temporal em um sistema quântico fechado pode ser representada através de um operador unitário. Para o caso do qbit, qualquer operador unitário representa uma evolução temporal que pode ser verificada em um sistema quântico. Alguns exemplos bem conhecidos no âmbito da mecânica quântica de operadores unitários, conhecidos como matrizes de Pauli [7] estão relacionados nas equações 3.3, 3.4, 3.5,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{3.3}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3.4}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{3.5}$$

No meio clássico, dois dos principais elementos em que a informação trafega são fios/cabos e portas lógicas. Os fios somente transportam a informação sem modificá-la, mas as portas lógicas transmitem a informação convertendo-a em outra forma de informação. Então, podemos considerar que as portas lógicas no caso clássico seriam equivalentes aos operadores lineares no caso quântico, pois os papéis que estes desempenhem são semelhantes.

Alguns operadores têm um funcionamento interessante, por exemplo, o operador X. Semelhante ao funcionamento da porta lógica de negação, o operador X quando posto a interagir com o vetor de estado $|0\rangle$, o transforma no vetor de estado $|1\rangle$, e vice versa, por essa semelhança, essa matriz é conhecida como matriz de inversão de bit. A matriz Z quando posta a operar sobre o estado $|0\rangle$ não realiza mudança alguma. No entanto, quando opera sobre o estado $|1\rangle$, o modifica para $-|1\rangle$. Assim ela é conhecida como matriz de inversão de fase, e o fator -1 é chamado de fator de fase. Outro operador importante é chamado de porta Hadamard e denotado por H; quando esta porta lógica quântica opera sobre o estado $|0\rangle$ ocorre a mudança deste estado para um estado de superposição à meio caminho entre os estados da base. Algo semelhante ocorre quando esta porta opera sobre o estado $|1\rangle$; nas equações 3.6 e 3.7 e na figura 3.2 está a representação matricial da porta Hadamard e sua aplicação sobre os estados da base.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.6}$$

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \equiv |+\rangle\,.\,;\; H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \equiv |-\rangle\,. \tag{3.7}$$

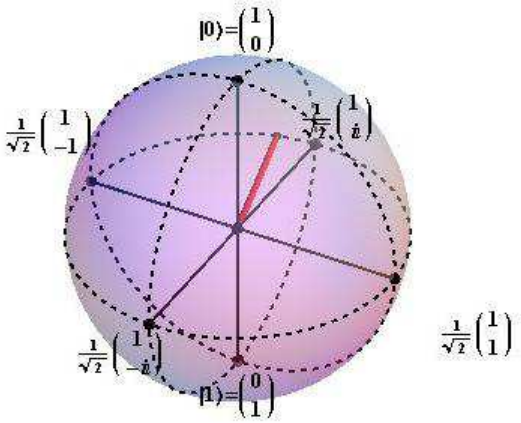


Figura 3.2: *Representação geométrica da aplicação da porta Hadamard e outras portas lógicas quânticas*

Os operadores lineares estão para a informação e computação quântica, assim como as portas lógicas e suas configurações estão para a informação e computação clássica. As restrições sobre as características desses operadores lineares podem ser extraídas do postulado 2. Um exemplo claro é a característica unitária do operador, isso é necessário para preservar a normalização do vetor de estado. Não importa qual a matriz que é considerada como responsável por promover a evolução temporal do estado quântico, basta que ele tenha a característica de ser unitária. Assim é de se esperar que o número de operadores lineares que possuem esse atributo seja bastante grande, mas é possível que as propriedades desse conjunto de operadores sejam também analisadas através de três matrizes de rotações, assim é possível construir qualquer operador evolutivo a partir desse conjunto de três matrizes de rotação, evidenciados pela equação (3.8) os quais simulam qualquer ação específica sobre um qbit arbitrário. Existem outras parametrizações, contudo a equação (3.8) é obtida a partir da matrizes de Pauli, pois essas quando exponenciadas dão origem as matrizes de rotação nos existe cartesianos canônicos.

$$U = \mathrm{e}^{i\alpha} \begin{bmatrix} \mathrm{e}^{-i\beta/2} & 0 \\ 0 & \mathrm{e}^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} \mathrm{e}^{-i\delta/2} & 0 \\ 0 & \mathrm{e}^{i\delta/2} \end{bmatrix}. \tag{3.8}$$

Postulado 3.3. *As medidas quânticas são descritas por determinados operadores lineares de medidas* $\{M_m\}$. *Esses operadores atuam sobre o espaço de estados do sistema. O índice m se refere aos possíveis resultados da medida. Se o estado de um sistema quântico for* $|\psi\rangle$, *imediatamente antes da medida, a probabilidade de um resultado m ocorrer é dada por :*

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle , \tag{3.9}$$

e o estado imediatamente seguinte a medida é

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}. \tag{3.10}$$

Os operadores de medida satisfazem à relação de completude

$$\sum_m M_m^\dagger M_m = I. \tag{3.11}$$

Como exemplo de uma aplicação do postulado da medida pode-se fazer a medida na base computacional, exemplo retirado de [7]. Considere o operador $M_0 = |0\rangle\langle 0|$ e $M_1 = |1\rangle\langle 1|$, esses operadores, respectivamente, são usados para medir um determinado estado que está na base computacional. Vale mencionar o fato que $M_0^2 = M_0$ e $M_1^2 = M_1$ (idempotentes), o que representa que esses operadores satisfazem a equação de completitude e que são hermitianos. O estado que será medido é um qbit genérico, assim a medida na base computacional tem uma probabilidade de apresentar resultado 0 na medida, expressa por:

$$p(0) = \left\langle \psi | M_0^\dagger M_0 | \psi \right\rangle = \langle \psi | M_m | \psi \rangle = |\alpha|^2 . \tag{3.12}$$

A probabilidade de se encontrar o resultado 1 na medida é $1 - p(0)$. Pelo postulado da medida, todo estado quântico, após ser medido é modificado e evolui temporalmente. No caso da base computacional, ao se medir o estado $|0\rangle$, o objeto alvo de medição evoluirá para $|0\rangle$ com um termo de ajuste de amplitude e vice-versa. Nas equações (3.13) e (3.14) estão representados os estados quântico após a medição dos estados $|0\rangle$ e $|1\rangle$.

$$\frac{M_0 |\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|} |0\rangle . \tag{3.13}$$

$$\frac{M_1 |\psi\rangle}{|\beta|} = \frac{\beta}{|\beta|} |1\rangle . \tag{3.14}$$

Alguns interessados mais atentos aos postulados poderiam levantar a hipótese do postulado da medida poder ser derivado do postulado 3.2, já que o sistema analisado e o instrumento de análise formam um sistema, maior, fechado e também isolado e que segundo o postulado 3.2 é possível representar a evolução temporal do sistema através de um operador unitário. Muitas discussões perduram atualmente sobre este assunto o que faz com que seja necessário desprezar essa idéia momentaneamente e isolar esses dois postulados. Existe um caso importante do postulado da medida que deve ser mencionado, este caso é conhecido como medidas projetivas ou de Von Neumann [7].

Postulado 3.4. *Uma medida projetiva é descrita por um observável M, um operador no espaço de estados do sistema sendo observado. O observável tem uma decomposição espectral*

$$M = \sum_m m P_m, \tag{3.15}$$

... em que P_m é o projetor sobre o auto-espaço de M com autovalor m. Os possíveis resultados da medida correspondem aos autovalores m do observável. Medindo-se o estado $|\psi\rangle$, a probabilidade de se obter o resultado m é dada por:

$$p(m) = \langle \psi | P_m | \psi \rangle . \tag{3.16}$$

Obtido o resultado m, o estado do sistema logo após a medida será:

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \tag{3.17}$$

Considere que os operadores de medida do postulado 3.3 satisfaçam, além da equação de completitude, a condição de ortonormalidade, desta forma garante-se que o postulado 3.3 se reduz ao caso especial anteriormente apresentado. É possível, portanto calcular o valor médio das medidas e o seu desvio padrão, dado pelas equações (3.18) e (3.19).

$$\begin{aligned} E(M) &= \sum_m m p(m) \\ &= \sum_m m \langle\psi|P_m|\psi\rangle \\ &= \langle\psi| \left(\sum_m m P_m \right) |\psi\rangle, \end{aligned}$$

$$E(M) = \langle\psi|M|\psi\rangle \equiv \langle M\rangle . \tag{3.18}$$

$$stdv(M) = \left\langle M^2 \right\rangle - \langle M\rangle^2 . \tag{3.19}$$

Interpretando esse caso especial do postulado da medida, pode-se constatar que o valor de uma medida realizada representa em qual vetor do autoespaço o estado medido foi projetado. De forma alguma o resultado da medida apresenta informação sobre qualquer coeficiente da combinação linear do vetor de estado considerado. Considere o caso em que deseja-se que uma medida seja realizada utilizando o operador linear Z, do conjunto das matrizes de Pauli, equação 3.4. O estado a ser medido é $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Para o operador Z, os possíveis autovalores são 1 e -1, com autovetores $|0\rangle$ e $|1\rangle$, respectivamente. A probabilidade de se realizar a medida e se encontrar o valor 1 é 1/2.

Para o caso de usar-se o operador X para realizar uma medida sobre o estado $|0\rangle$, dois possíveis resultados poderiam ocorrer, 1 e -1, já que esses são os autovalores associados aos estados $|+\rangle$ e $|-\rangle$ (autovetores), respectivamente. O valor 1 pode ocorrer $\langle 0|+\rangle\langle +|0\rangle = 1/2 = 50\%$ das vezes, o mesmo acontece para o valor -1 da medida; isso leva à conclusão que o valor esperado da medida é 0, com desvio padrão de 1.

Postulado 3.5. *O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas individuais. Se os sistemas forem numerados de* 1 *ate n, e o sistema i for preparado no estado* $|\psi_1\rangle$*, decorre que o estado do sistema composto será* $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Por motivos de simplicidade teórica é conveniente aceitar esse postulado como uma das pedras fundamentais para o desenvolvimento da mecânica quântica, já que muitos questionamentos poderiam ser levantados. Um desses estaria relacionado à operação de produto vetorial. Não fica claro, ou evidente por si, o motivo da escolha dessa operação como componente fundamental para compor sistemas mais complexos. No entanto, o que é evidente é que deve haver uma forma bem estabelecida para que se possam representar os sistemas mais complexos. Por vezes os pesquisadores poderiam se referir a sistemas simples por incógnitas, em que $|x\rangle$ e $|y\rangle$ seriam estados quânticos e o estado $\alpha|x\rangle+\beta|y\rangle$

é o estado quântico de superposição, em que $|a|^2 + |b|^2 = 1$. No entanto, a escolha da representação dos estados da base computacional foi feito justamente por semelhança ao caso clássico. Assim, como também na lógica binária clássica, o poder de representação biunívoca, pode ser aumentado por concatenação simples dos símbolos que representam conjuntos de ordens menores. Ou seja o conjunto $B = \{0, 1, 2, 3\}$ pode ser presentado pelo conjunto $B_b = \{00, 01, 10, 11\}$, em que o conjunto B_b foi construído a partir do conjunto de ordem mais simples $A_b = \{0, 1\}$ que, por sua vez, representa $A = \{0, 1\}$. Seguindo esse pensamento determinado é intuitivo aumentar um determinar conjunto de representação de elementos, unicamente, compondo-os com conjuntos mais básicos e tomando como ferramenta de junção o produto tensorial é possível realizar essa tarefa.

Como exemplo do postulado 3.5, pode-se considerar existirem dois *qbits*, cada um deles com dois estados possíveis, $|0\rangle$ e $|1\rangle$. Dessa forma, como na lógica clássica em que com dois bits é possível representar quatro níveis lógicos distintos: 00, 01, 10, 11, é factível para o caso quântico poder representar também 4 estados quânticos distintos: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Mas, foi visto que um estado quântico pode permanecer em um estado superpostos de estados da base, com um número complexo associado a cada estado da base; assim, um estado quântico, formado por dois qbits simples terá uma representação matemática da forma

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \tag{3.20}$$

Uma medida realizada na base computacional para o estado da equação 3.20 produzirá qualquer um dos resultado: 00, 01, 10, 11, com probabilidade $|a_i|^2$, associado a cada valor. Vale mencionar que esse vetor é unitário. Uma possibilidade interessante relacionada à medida é que nesse caso é possível medir, isoladamente, cada qbit. Por exemplo, caso se desejasse medir, na base computacional, o primeiro qbit, dois resultados seriam validos: 0 e 1, com probabilidades $|a_{00}|^2 + |a_{01}|^2$ e $|a_{10}|^2 + |a_{11}|^2$, respectivamente. O estado quântico após a medida seria

$$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

Os termos $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$ e $\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}$, são introduzidos pelo postulado da medida **??**, mas é bem verdade que a inclusão deste termo termina por verificar a condição de normalização dos estados quânticos.

Algo interessante, identificado por pesquisadores há algum tempo, reside no fato constatado de que nem todos os elementos que fazem parte de um sistema composto podem ser representados como junção de elementos mais simples. Parece algo estranho relatar que esse elemento exista e que é objeto de muitas aplicações bastante engenhosas, ele é conhecido como estado emaranhado.

Um exemplo de um estado emaranhado é o par EPR ou estado de Bell, equação 3.21. Esse elemento quântico é o responsável por diversas aplicações intrigantes na computação quântica, a codificação superdensa e o teletransporte, aplicações que serão vista no capítulo '"Aplicações dos Postulados".

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{3.21}$$

Esse estado apresenta uma propriedade interessante, em relação à medida. Suponha-se que se queira medir, na base computacional, o estado do primeiro qbit. Os resultados poderiam ser 0 ou

1, com mesma probabilidade para ambos, 1/2. No entanto, o estado quântico que se origina após a medida está diretamente ligado ao resultado das medidas, pois se o resultado da medida foi 0, o estado após a medição será $|00\rangle$ e caso contrário, o resultado da medida for 1, o estado quântico após a medida será $|11\rangle$. Essa correlação entre os resultados das medidas é bastante forte graças à estrutura do estado quântico, pois mesmo que se aplique sobre este operações lineares sobre qualquer dos *qbits* do estado e outros tipos de medidas sejam realizadas, a correlação apresentada permanecerá.

Este estado quântico recebe o nome de par EPR graças à três pesquisadores [22], Einstein, Podolsky, Rosen, que estudaram as diversas propriedades intrigantes, pela primeira vez, dos estados emaranhados que apresentam a mesma estrutura do estado aqui descrito. Em seguida, John Bell, desenvolveu exaustivamente os resultados apresentados pelos três pesquisadores e descobriu outro resultado notável, o qual havia passado despercebido pelos pesquisadores: *as correlações observadas em medidas feitas em pares de Bell são maiores do que quaisquer outras que poderiam existir em sistemas clássicos*. Essa foi a primeira indicação direta de que a mecânica quântica seria um meio viável de se conseguir processamentos de informação mais rápidos e mais profundos do que seria possível no meio clássico.

Os postulados da mecânica quântica foram apresentados e é a partir deles que se inicia todo o desenvolvimento da física quântica, se estendendo a informação e computação quântica. Desta forma podemos condensar em pequenas frases os pontos principais desses fundamentos.

- O postulado 3.1 define em que área deve ser desenvolvida toda a teoria quântica e quais os elementos de trabalho para a representação de elementos.
- O postulado 3.2 define como se pode estudar e representar as mudanças que o sistema quântico estudado experimenta.
- O postulado 3.3 define um meio de se extrair informação de um estado quântico lembrando que qualquer meio, maneira, forma de examinar um estado quântico, sem exceção alguma, acarretará uma mudança no mesmo. Além do caso especial deste portulado, postulado 3.4, que define uma maneia de decompor o observável.
- O postulado 3.5 define uma maneira de formar estados quânticos mais complexos através de estados quânticos mais simples.

capítulo 4

Aplicações dos Postulados da Mecânica Quântica

"L'imagination est la reine du vrai, et le possible est une des provinces du vrai. Elle est positivement apparentée avec l'infini."
Baudelaire

4.1 Portas de Múltiplos qbits

Após serem colocadas as pedras fundamentais para o entendimento da mecânica quântica é possível apresentar alguns resultados decorrentes das aplicações dos postulados. Possivelmente, alguns resultados são relativamente simples e intuitivos, bastando para isso a aplicação de dois ou mais postulados para que se entenda o processo como um todo. Entretanto, existem aplicações que fogem totalmente da compreensão natural convencional, tornando a informação quântica um campo bastante fértil a inovações e descobertas com resultados intrigantes.

Suponha que se deseje modelar a evolução temporal constatada em um sistema quântico com estados formados por dois *qbits*. Como muitos casos da computação quântica foram extraídos por semelhança em relação a casos clássicos, não seria errado tentar modelar um operador linear, unitário, que apresentasse relativa similaridade com uma porta lógica de dois bits. Existem diversas portas lógicas: E, OU, OU-EXCLUSIVO, NÃO-E, NÃO-OU; dentre essas podemos destacar as portas NÃO-E e NÃO-OU que são consideradas universais, já que a partir delas é possível construir quaisquer uma das outras portas mostradas [46]. Outra porta lógica interessante é a OU-EXCLUSIVO. Ela apresenta a propriedade de preservar a paridade entre os bits de entrada e saída. Então, uma porta lógica quântica foi construída em função da porta clássica OU-EXCLUSIVO, ela se chama Não-Controlado.

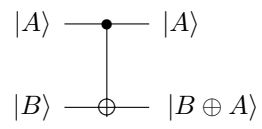


Figura 4.1: Circuito da porta Não-Controlado

$$\mathrm{U}_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{4.1}$$

Esta porta lógica quântica apresenta dois *qbits* de entrada e dois *qbits* de saída. Há uma diferença entre os *qbits* de entrada, um *qbit* irá governar a atuação da porta lógica e o outro *qbit* irá receber a ação da porta, esses *qbits* são nomeados de *qbit* de controle e *qbit* alvo, respectivamente. Na figura 4.1 está apresentado um esquema do circuito quântico que representa a porta "Não-Controlado". A linha superior da figura representa o *qbit* de controle e a linha inferior representa o *qbit* alvo. Esta porta funciona de maneira tal que se o qbit de controle for $|0\rangle$, nenhuma ação é presenciada no *qbit* alvo. No caso do *qbit* de controle ser $|1\rangle$, realiza-se uma soma módulo 2 entre o *qbit* de controle e o *qbit* alvo e o resultado é inserido no lugar do segundo *qbit*.

$$|00\rangle \rightarrow |00\rangle \; ; \; |01\rangle \rightarrow |01\rangle \; ; \; |10\rangle \rightarrow |11\rangle \; ; \; |11\rangle \rightarrow |10\rangle. \tag{4.2}$$

Pode-se dizer então que a porta Não-Controlado é uma generalização da porta OU-EXCLUSIVO, já que esta última realiza, justamente, a ação de somar módulo 2 os seus bits de entrada; então podemos representar o funcionamento da porta lógica quântica como $|A, B\rangle \rightarrow |A, A \oplus B\rangle$. Existe ainda a representação matricial desta porta lógica. É interessante notar que as colunas da matriz são também as representações matriciais dos elementos do conjunto de base do espaço vetorial considerado e suas posições não são postas ao acaso. A equação (4.2), revela quais devem ser as posições das representações dos estados de base.

Deve-se tomar bastante cautela com as possíveis analogias feitas entre o mundo clássico e o mundo quântico. A porta Não-Controlado pode ser vista como análoga à OU-EXCLUSIVO, mas não igual. Existe ainda a relação entre a porta Não-clássica e a Não-quântica que neste caso é igual tanto no caso clássico quanto no caso quântico. A condição para que um determinado operador linear possa ser interpretado como porta lógica é ser unitário, o que aparentemente seria uma condição simples e sem importância; mas o que está subjacente a essa condição é o conceito de reversibilidade. Em linhas gerais uma porta lógica pode ser considerada reversível se tomando a informação de saída, as entradas são completamente especificadas em todos os casos possíveis. Aplicando esse conceito as portas: E, OU, OU-EXCLUSIVO, NÃO-E, NÃO-OU, fica evidente que elas não apresentam essa propriedade.

Para que seja possível fazer uma "migração"do mundo clássico para o mundo quântico é necessário que no mundo clássico a porta seja reversível, esse fato equivale a assegurar que no mundo quântico a representação matricial terá a propriedade de ser unitária. Mais comentários relacionados a este assunto podem ser encontrados e descritos com detalhes em [47], em que é relatada outra relação

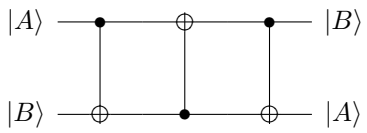


Figura 4.2: Circuito de Troca

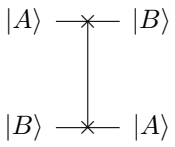


Figura 4.3: Representação do Circuito de Troca

interessante que a reversibilidade desempenha. É bem salutar intuir que existam outras portas lógicas de múltiplos *qbits* além da Não-Controlado, porém, esta porta desempenha um papel central no desenvolvimento de circuitos quânticos. Um resultado que não será demonstrado neste texto, assegura que a partir das portas de um qbit e da porta Não-Controlado é possível construir qualquer porta lógica de múltiplos qbits, esse resultado seria o análogo ao resultado da universalidade das portas NÃO-E e NÃO-OU.

Os exemplos apresentados até agora fazem parte de um conjunto de circuitos quânticos simples, mas como foi mencionada, é a partir desse simples conjunto de portas lógicas, considerados exemplos simples de circuitos quânticos, que circuitos quânticos mais complexos são formados. Suponha que se queira trocar os estados quânticos em um estado de dois *qbits*, de tal maneira que um estado inicial $|A, B\rangle$ seja transformado em $|B, A\rangle$. Para que essa tarefa seja realizada é necessário o uso da porta lógica Não-Controlado, pois a sua operação pode ser expressa, matematicamente, pela matriz 4.1. A idéia de se usar essa função surge do conhecimento da propriedade de reversibilidade, aplicando a função a sua própria saída retorna-se aos estados quânticos iniciais,esta função é involutiva. O procedimento usado para que ocorra a troca de estados quânticos é descrita a seguir , juntamente com o circuito quântico correspondente. É interessante notar que o circuito é formado por três portas quânticas Não-Controlado.

$$\begin{aligned} |a, b\rangle &\rightarrow |a, a \oplus b\rangle \\ &\rightarrow |a \oplus (a \oplus b), a \oplus b\rangle \\ &\rightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle. \end{aligned} \tag{4.3}$$

Outro exemplo bastante comum em circuitos quânticos são as portas quânticas controladas, para múltiplos *qbits*. A idéia dos circuitos quânticos controlados é bem simples. Considere que uma porta lógica quântica, representada por um operador linear P, receba um estado quântico com um ou mais qbits, denominado estado alvo. Além disso, suponha que haja um estado quântico auxiliar, denominado estado de controle, que em caso de estar em um estado da base definido pelo projetista, acionará o funcionamento da porta lógica sobre o estado alvo, realizando o funcionamento da porta

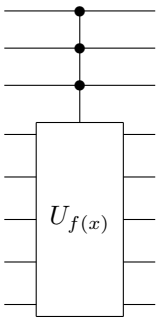


Figura 4.4: Circuito Controlado por mqbits

Figura 4.5: Circuito de Medição

lógica em diversos estados, resultando em diversas configurações de saída,(uma para cada estado de controle). Na figura 4.4 é possível visualizar o esquema representativo do circuito dessas portas lógicas.

Quando se menciona o assunto de circuitos, deve-se ter em mente que algumas ações que são permitidas em circuitos clássicos, não são permitidas em circuitos quânticos [7] . Por exemplo, retroalimentações são configurações bastante comuns em circuitos clássicos e os resultados decorrentes dessa configuração são fundamentais nas áreas da engenharia eletrônica e automação: circuitos osciladores, estudo de estabilidade de servomecanismos, entre outros. No entanto, essa configuração não é permitida em circuitos quânticos. Os circuitos quânticos são geralmente conhecidos como acíclicos. Contudo, a controlabilidade dos circuitos quânticos pode ser realizado através de alguns *qbits* auxiliares, figura 4.4. Outra impossibilidade que os circuitos quânticos experimentam, e que é comum em circuitos clássicos, é a união de dois fios, uma operação conhecida como *Fan-In*, em que o fio resultante carrega um bit de saída que é o resultado de uma porta OU clássica das informações dos fios de entrada. O motivo de tal operação ser proibida é que a operação OU é irreversível. Através de fundamentos físicos relacionados à termodinâmica, em [47], é possível mostrar que toda operação irreversível é proibida em computação quântica. A última impossibilidade enfrentada pelos circuitos quânticos é a bipartição de fios, ou seja, ligar a um fio qualquer, dois outros fios de modo que seja realizada uma cópia da informação portada pelo fio primário, esta operação é conhecida como *Fan-Out* que é proibida, pois é impossível realizar a cópia de estados quânticos em superposição.

Como já foi mencionado anteriormente, é possível considerar a realização de uma medida como uma transformação linear e consequentemente, com um circuito quântico. O símbolo de uma medição é um "mostrador", algo parecido com um voltímetro ou amperímetro analógico. A operação de medição modifica um qbit genérico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ em um bit clássico aleatório, que é o resultado da medição, com essa aleatoriedade definida pelos números complexos α e β e cujo valor são 0 e 1, se medidos na base computacional. O circuito de medição, com o seu símbolo, pode ser visualizado na figura 4.5.

O campo da informação quântica apresenta, por diversas vezes, resultados que são no mínimo

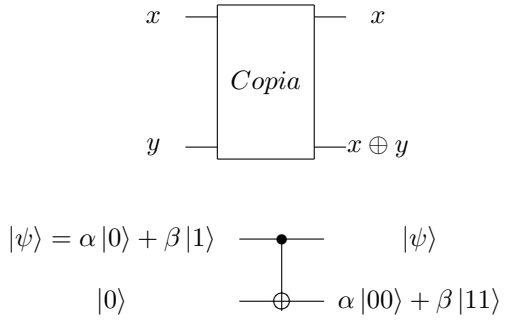


Figura 4.6: Circuitos Clássico e Quântico de Cópia

estranhos se comparado aos casos clássicos. Como em qualquer circuito clássico, principalmente nos casos em que se deseja verificar se uma determinada informação está ou não correta, faz-se uma cópia do estado a ser testado e realizam-se experimentos sobre ele, no intuito de se saber se ocorreu algum erro. Se ocorreu o erro procura-se identificar que tipo de erro foi esse para tentar corrigi-lo. Um esquema de um circuito clássico para cópia é apresentado na figura 4.6. Alguns podem desconfiar que isso também deva ser o processo a ser feito no âmbito da informação quântica, já que ao se realizar uma medida, o dano ao estado quântico é tão severo que não se pode mais retroceder ao elemento de informação anterior. No entanto, isso não é possível, copiar um bit é perfeitamente possível e viável na computação quântica, mas copiar um *qbit* não é possível em alguns casos [47].

Um pensamento engenhoso poderia ser norteado para a aplicação de troca de *qbits* em um estado quântico, a porta lógica Não-Controlado seria uma boa escolha de ferramenta para a duplicação de um *qbit*. Considere, então, um *qbit* genérico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ que deve ser copiado, sabe-se que a porta Não-Controlado tem seu funcionamento tal que: $|A, B\rangle = |A, A \oplus B\rangle$, então uma solução seria acoplar ao qbit genérico um estado quântico simples que pudesse receber a cópia do primeiro qbit, assim acoplasse o estado quântico $|0\rangle$ e em seguida aplicasse a porta lógica. O estado de saída do processo é descrito como $|\psi_1\rangle = \alpha|00\rangle + \beta|11\rangle$. O estado $|\psi_1\rangle$ apresenta certa semelhança com o estado $|\psi\rangle|\psi\rangle$, equação (4.4) , o que seria o estado que deveríamos alcançar na saída do processo de clonagem com dois estados quântico idênticos acoplados, mas esses estados são diferentes. A comparação das expressões matemáticas de ambos os estados, equações (4.4) e (4.5), pode esclarecer onde se encontra o problema da clonagem [7].

$$|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle. \tag{4.4}$$

$$|\psi_1\rangle = \alpha|00\rangle + \beta|11\rangle. \tag{4.5}$$

4.2 Medidas em bases diferentes da base computacional

Em todo o desenvolvimento do texto até o momento presente não foi mencionado se seria possível trabalhar de forma eficiente em uma base diferente da base computacional, sobretudo realizar medidas utilizando outra base. Foi mencionado que para um *qbit* no estado padrão de superposição $\alpha|0\rangle + \beta|1\rangle$,

em que α e β são números complexos, ao realizar-se uma medida através da base computacional seria possível obter dois possíveis valores: 0 ou 1, com probabilidades $|a|^2$ e $|b|^2$, respectivamente.É bem verdade que os estados da base $|0\rangle$ e $|1\rangle$ são dois entre muitas presumíveis escolhas de estados para compor a base de vetores.

Outras dessas presumíveis escolhas são os estados $|+\rangle$ e $|-\rangle$, eles se relacionam com os estados da base computacional através da porta de Hadamard, $|+\rangle = [|0\rangle + |1\rangle]/\sqrt{2} = H|0\rangle$ e $|-\rangle = [|0\rangle - |1\rangle]/\sqrt{2} = H|1\rangle$. Logo qualquer estado quântico em estado de superposição pode ser representado em função desses novos elementos que compõem a nova base ortonormal, essa nova base chamasse base de Hadamard. Às modificações de base, que seguem o exemplo da mudança da base computacional para a base de Hadamard, são "gerenciadas"por uma matriz de mudança de base. Essa mudança de base deve conservar a propriedade de normalização dos coeficientes α e β para a interpretação probabilística dos mesmos.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle. \tag{4.6}$$

Medindo-se um estado quântico genérico para a base de Hadamard, os possíveis valores das medições seriam + e −, como seria de se esperar, com probabilidades $|\alpha+\beta|^2/2$ para o valor + e $|\alpha-\beta|^2/2$ para o valor −. Em linhas gerais, qualquer que seja a base de estado especificada $|i\rangle$ e $|j\rangle$, para representar um estado quântico genérico $\alpha|i\rangle + \beta|j\rangle$, é sempre possível realizar uma medida na base considerada com dois possíveis valores a ser obtidos, i e j, com probabilidades $|a|^2$ e $|b|^2$, respectivamente.

4.3 Estados de Bell

Existem alguns estados quânticos que apesar de apresentarem uma expressão matemática simples, desempenham um papel surpreendente na computação e informação quântica. No decorrer do texto estes estados já foram mencionados, são conhecidos como estados de Bell, será mostrado aqui um circuito que possa criar esses estados e mostrar que eles podem ser considerados como uma base alternativa para a expressão de um estado quântico genérico.

Considere um estado quântico simples de dois *qbits* sem estar em superposição, por exemplo, $|00\rangle$. Sobre o primeiro *qbit* aplica-se a porta Hadamard, para criar neste *qbit* um estado de superposição equilibrada em probabilidades, o que resulta no estado $|00\rangle + |10\rangle/\sqrt{2}$. Em seguida, aplica-se a porta lógica Não-Controlado sobre o estado de saída da porta Hadamard, que tem por resultado o estado: $|00\rangle + |11\rangle/\sqrt{2}$. O processo descrito aqui é geral para qualquer entrada de modo que é possível criar quatro estados de Bell possíveis, já que existem quatro possíveis estados quânticos de dois qbits. Na figura 4.7 está exposto o circuito de transformação de um estado genérico para um par de Bell e na tabela 4.1 está explicitada as relações de entrada e saída para o circuito. Note que se um estado quântico genérico de dois qbits for usado como entrada do circuito da figura 4.7, ocorre uma mudança de base, da base computacional para a base de Bell.

A notação convencional para esses estados é dada por $|\beta_{00}\rangle$, $|\beta_{01}\rangle$, $|\beta_{10}\rangle$, $|\beta_{11}\rangle$, para condensar as informações presentes na equação genérica de estados de Bell, equação (4.7),

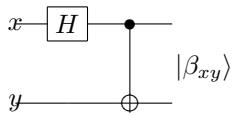


Figura 4.7: Circuito Quântico para Criação da Base de Bell

Tabela 4.1: Tabela de Mudança da Base Computacional para a Base de Bell

Entrada	Saída
$\|00\rangle$	$[\|00\rangle + \|11\rangle] / \sqrt{2} = \|\beta_{00}\rangle$
$\|01\rangle$	$[\|01\rangle + \|10\rangle] / \sqrt{2} = \|\beta_{01}\rangle$
$\|10\rangle$	$[\|00\rangle - \|11\rangle] / \sqrt{2} = \|\beta_{10}\rangle$
$\|11\rangle$	$[\|01\rangle - \|11\rangle] / \sqrt{2} = \|\beta_{11}\rangle$

$$|\beta_{xy}\rangle \equiv \frac{|0, y\rangle + (-1)^x |1, \overline{y}\rangle}{\sqrt{2}}. \tag{4.7}$$

Com o intuito de contextualizar e demonstrar o potencial aplicativo desta nova teoria, as seções seguintes tem o papel de ilustrar interessantes aplicações relacionadas aos postulados e conceitos enunciados anteriormente. A seção **Teleporte Quântico** tem o objetivo de enunciar uma aplicação surpreendente, utilizando os estados de Bell. Desta forma, é evidenciado o papel fundamental desses estados no âmbito da teoria da informação e computação quântica. A seção **Paralelismo Quântico** está inserida para mostrar o potencial de ganho da capacidade de processamento, no que concerne a necessidade de avaliação de funções. A seção **Codificação Superdensa** demonstra como é possível transmitir informação clássica sem que haja algum meio de comunicação estabelecido entre o receptor e o destinatário. A seção **Consumo de Energia e sua Relação com a Informação Quântica** apresenta o conceito de computação reversível e qual a sua importância na construção de portas lógicas quânticas.

4.4 Teleporte Quântico

Ao estar familiarizado com todos os resultados até aqui apresentados é possível progredir e expor um grande feito na área da comunicação quântica, chamado de teleporte quântico. Como o próprio nome relata, o teleporte quântico é uma maneira de se deslocar, transportar, um estado quântico genérico de um lugar do espaço para outro, sem que haja um meio de físico que sirva de meio de comunicação convencional ligando os pontos de Transmissão e de Recepção.

Suponha que Trajano e Ritha sejam amigos e vivam por um longo tempo juntos. Algum tempo depois, Trajano decide ir fazer Doutorado na França, desta forma ele é deslocado do seu local de vivência para outra localidade. Antes do seu deslocamento, Trajano prepara um estado de Bell e compartilha com Ritha um dos dois *qbits* desse estado. Tempos mais tarde, Ritha soube que Trajano estava com problemas, ele havia esquecido um estado quântico, de extrema importância para sua Tese de Doutorado na França, no laboratório em que trabalhava anteriormente. Assim, Ritha decide ajudá-lo, já que ele também não tinha dinheiro para as passagens de ida e volta. A maneira que foi

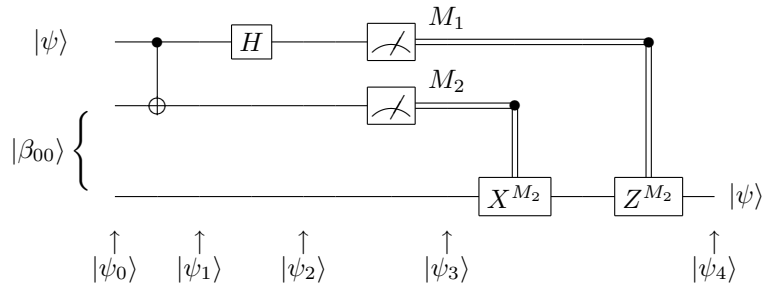


Figura 4.8: Circuito Quântico de Teleporte

encontrada para ajudar Trajano foi por meio do teleporte quântico, usando os *qbits* partilhados do estado de Bell.

Ritha, então, acopla o estado quântico que Trajano havia esquecido no laboratório aqui em Recife a seu *qbit* pertencente ao estado de Bell e após algumas transformações simples, Ritha realiza uma medição nos dois *qbits* que com ela estão. Então, envia a informação das medições para Trajano e dependendo do resultado das medições, Trajano realiza operações que irão preparar o *qbit* que com ele está, oriundo do compartilhamento com Ritha de *qbits* do estado de Bell, para que após essas transformações o estado quântico que ele possui seja modificado para o estado quântico que aqui ele havia esquecido.

Algumas pessoas poderiam pensar que o teleporte seria um esforço desmedido para se enviar uma informação, no entanto, vale salientar que não há outra maneira de por meios clássicos enviar esse tipo de mensagem. Não é possível medir e conhecer uma amplitude com certeza e esse processo destruiria o outro coeficiente, a quantidade de informação contida somente neste *qbit* simples é enorme, um contínuo de informação está contido neste elemento, assim, por esses motivos, o envio de informação clássico para que Trajano pudesse de alguma forma, preparar um estado quântico para ser idêntico ao que ele havia esquecido, é impossível.

O circuito da figura 4.8 mostra todo o processo de teleporte quântico em detalhes. Seja $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ o estado quântico que deve ser enviado a Trajano, em que α e β são os coeficientes complexos desconhecidos. Seja $|\beta_{00}\rangle$ o estado de Bell compartilhado por Trajano e Ritha e $|\psi_0\rangle$ o estado resultando do acoplamento entre $|\beta_{00}\rangle$ e $|\psi\rangle$,

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle|\beta_{00}\rangle \\ &= \frac{[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]}{\sqrt{2}}. \end{aligned}$$

...deve-se notar que o primeiro qbit é o qbit a ser teleportado, em posse de Ritha, o segundo qbit é o qbit de Ritha e o terceiro qbit está com Trajano, em estados de Bell ambos últimos. Ritha aplica então uma porta Não-Controlado aos dois qbits que estão em sua posse, resultando em $|\psi_1\rangle$.

$$|\psi_1\rangle = \frac{[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|01\rangle + |01\rangle)]}{\sqrt{2}}.$$

Tabela 4.2: Descrição das Ações para o Teleporte

Resultado da Medida	$\|\psi_3\rangle$	Porta a ser Aplicada	$\|\psi_4\rangle$
00	$\alpha\|0\rangle + \beta\|1\rangle$	I	$\alpha\|0\rangle + \beta\|1\rangle$
01	$\alpha\|1\rangle + \beta\|0\rangle$	X	$\alpha\|0\rangle + \beta\|1\rangle$
10	$\alpha\|0\rangle - \beta\|1\rangle$	Z	$\alpha\|0\rangle + \beta\|1\rangle$
11	$\alpha\|1\rangle - \beta\|0\rangle$	iY	$\alpha\|0\rangle + \beta\|1\rangle$

Após a aplicação da porta Não-Controlado, Ritha aplica uma porta de Hadamard, unicamente, ao primeiro qbit, resultando em $|\psi_2\rangle$.

$$|\psi_2\rangle = \frac{[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]}{2}.$$

Manipulações matemáticas podem ser realizadas agrupando termos semelhantes de modo a expressar o estado $|\psi_2\rangle$ como:

$$|\psi_2\rangle = \frac{[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]}{2}. \tag{4.8}$$

Essa expressão é interessante e pode dar uma noção dos procedimentos finais, já que se têm a soma de quatro termos distintos acoplados a estados de dois *qbits* cada, também distintos. Como os primeiros dois *qbits* estão em posse de Ritha, ela pode realizar medidas, na base computacional, e como medir é transformar irreversivelmente um estado quântico, os resultados das medidas irão informar qual o estado resultando que está de posse de Trajano sem que ele necessite medir. O propósito de Trajano é recuperar $|\psi\rangle$, assim caso os resultados das medidas de Ritha sejam 00, nada deve ser feito com o estado que com Trajano se encontra. Caso os resultados das medidas sejam 01, para recuperar o estado $|\psi\rangle$, deve se aplicar ao estado de Trajano um circuito de porta X (Não quântico). Se os resultados forem 10, basta que se aplique ao estado um circuito de Porta Z. E por fim, se os resultados das medidas forem 11, aplica-se sobre o estado primeiro a porta X e em seguida a porta Z.

Alguns comentários sobre o teleporte quântico são levantados, como a possibilidade de envio de informação mais rápido que a luz. As consequências desse fato seriam intrigantes, já que a teoria da relatividade garante que caso isso ocorra é o mesmo que enviar informação ao passado. A resposta para essa questão é que para que o estado quântico seja teleportado, o procedimento completo deve ter o envio de informação clássica, pois Ritha deve informar a Trajano quais são os resultados das medidas, e assim, como não existe informação clássica com a possibilidade de viajar mais rápido que a luz, o processo como um todo deve ser atrasado pelo menos até que essa informação clássica seja repassada, em outras palavras o teleporte só é possível graças à comunicação clássica, sem a comunicação clássica o teleporte não é possível.

Outro ponto intrigante é que, aparentemente o teleporte dá a impressão de que uma cópia de um estado quântico foi realizada, contradizendo o principio da não-clonagem [7]. Ocorre que os procedimentos realizados por Ritha preparam o estado de Trajano em função do estado que está com ela e que não é parte do par EPR, pois no final do processo só o qbit de Trajano se encontrará no

estado $|\psi\rangle$, e os qbits de Ritha se encontrarão nos estados $|0\rangle$ ou $|1\rangle$, cada. Para que se configurasse um processo de cópia deveria haver dois estados com o mesmo padrão de coeficientes, o que não ocorre.

Assim, o teleporte quântico é uma clara demonstração da força da computação e informação quântica, a diversidade de recursos para que se possa enviar informação, indicando que existem elementos simples que tem a capacidade de transmitir informação com alto grau de complexidade, algo sem precedentes na informação clássica, pois um par de Bell, compartilhado, juntamente com uma informação binária equivale a um qbit. O teleporte quântico foi descoberto por Bennet, Brasssard, Créupeau, Jozsa, Peres, Wootters [23] e experimentalmente testado de diversas maneiras por técnicas ópticas [24], por polarização de fótons [25], por estados comprimidos de luz [26], por RMN [27]. A diversidade de recursos, proporcionando que o tráfego de informação seja estabelecido, é o ponto chave dessa aplicação.

4.5 Paralelismo Quântico

Ao se aprofundar no estudo da realização da computação quântica, algumas questões são às vezes suscitadas quando relacionadas a sua capacidade de processamento e suas vantagens em relação ao campo clássico. Desta forma, é necessário exemplificar, para responder a essas questões, quais as possíveis ações que um computador quântico tem a capacidade de fazer, a sua comparação com o campo clássico, tanto no âmbito da viabilidade, tanto no âmbito da rapidez de processamento desta tarefa.

Qualquer nova teoria (seja ela física ou não), que se proponha a suplantar outra teoria deve ser apresentada de tal forma a explicar com mais clareza e solidez questões já abarcadas pela antiga teoria e dar suporte teórico a questões ainda sem esclarecimento e fazer previsões sobre outras questões ainda não elucidadas. Assim, a computação quântica preenche todos os requisitos mencionados para essa nova teoria. É de se esperar, com isso, que a computação quântica tenha a capacidade de realizar qualquer tarefa já praticada por um computador clássico e se proponha a realizar outras tarefas que sejam inviáveis de serem efetuadas pela computação convencional [7].

Um exemplo interessante deste tipo de tarefa é o paralelismo quântico. Este procedimento tem por finalidade calcular o valor de uma função estabelecida para tantos pontos quantos sejam necessários, simultaneamente. Considere uma função $f(x) : \{0,1\} \rightarrow \{0,1\}$, domínio e imagem. Considere um circuito quântico que opere com estados de dois *qbits*, capaz de realizar a seguinte tarefa: $|x,y\rangle \rightarrow |x, f(x) \oplus y\rangle$, em que $\oplus$ representa a soma módulo dois. O primeiro *qbit* será referenciado como registro de dados e o segundo *qbit* será referenciado como registro alvo e pelo postulado 3.2, sem perda de generalidade, pode-se referenciar o circuito quântico por $U_{f(x)}$. Tomando para o registro de dados um *qbit* que esteja na base de Hadamard, $|+\rangle = |0\rangle + |1\rangle/\sqrt{2}$, e no registro alvo um *qbit* preparado no estado padrão $|0\rangle$, ao se fazer aplicar sobre esses estados o circuito quântico, o estado de saída é:

$$|\psi\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}. \tag{4.9}$$

...ao se analisar o estado de saída, verifica-se que o circuito foi capaz de implementar, no estado superposto, ambos os valores possíveis da função $f(x)$. O resultado desses valores estão, todos, no que se chamou de registro alvo originado dos valores reservados no registro de dados do estado

quântico original. Cada parcela da soma contém todos os possíveis valores de x e consequentemente, todos os possíveis valores de $f(x)$, esse é o efeito do paralelismo quântico. A maneira pela qual essa "simultaneidade"de inferência quanto a todos os possíveis valores da função $f(x)$v pode ser realizado está novamente ligado aos estados de superposição, pois foi necessário, unicamente, um circuito que compute a função para diferentes valores do seu domínio e a preparação desses estados superpostos para se realizar o paralelismo. Isto difere do modelo clássico, no qual é necessário que vários circuitos sejam postos em paralelo para que se calculem os valores da função. Em outras palavras, a diferença do paralelismo está em se retirar o problema físico de vários circuitos que trabalham concomitantemente para se concentrar na simultaneidade de vários dados, os estados superpostos.

Esse procedimento pode ser generalizado, no intuito de se expandir o domínio da função a ser calculada, através da transformação de Hadamard-Walsh, em que várias portas Hadamard são aplicadas simultaneamente em vários *qbits* diferentes. Por questões didáticas, frequentemente, o símbolo $H^{\otimes n}$ refere-se à aplicação simultânea da porta Hadamard, em vários *qbits*. Ou seja, significa a aplicação simultânea desta porta em n *qbits* diferentes. O resultado, por exemplo, da aplicação de uma das portas $H^{\otimes 2}$ sobre o estado padrão $|00\rangle$ é:

$$|+\rangle|+\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}.$$

Através da aplicação sucessiva de portas Hadamard, sem perda de generalidade, sobre n *qbits*, oriundos do estado padrão $|0\cdots 0\rangle$ resulta em

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle, \forall x \ \in A; A = \{00\cdots 00, 00\cdots 01, \cdots, 11\cdots 01, 11\cdots 11\}$$

em que, cada parcela da soma, faz referência a um valor específico do domínio da função $f(x)$. O procedimento é o mesmo descrito, cada porta Hadamard cria um estado de superposição equilibrada, com todas as amplitudes iguais, para cada *qbit* padrão do estado de n *qbits*. Como todos os *qbits* estão ligados pelo produto tensorial, o resultado é a formação de uma soma de todos os possíveis valores, na base binária, compreendidos entre 0 e $n-1$.

Assim, o cálculo de uma função de n bits é feita da seguinte maneira: Inicialmente prepara-se um estado padrão de n *qbits*, $|0...0\rangle$, que será indicado como registro de dados. Em seguida, aplica-se a transformação de Hadamard-Walsh no estado preparado, modificado para a base de Hadamard. Na verdade isto corresponde a prepará-lo para um estado de superposição perfeitamente equilibrado em cada *qbit* que o compõe. O próximo passo é acoplar um *qbit*, no estado padrão, $|0\rangle$, ao estado de saída da transformação de Hadamard-Walsh, que será denominado registro alvo. Por fim, aplica-se sobre esse estado de $n+1$ *qbits* a porta quântica referente à função $f(x)$, denotada por $U_{f(x)}$. O estado quântico de saída do circuito, terá em cada parcela, um representante do domínio da função $f(x)$ e o cálculo da função para esse elemento do domínio, expressão (4.10),

$$\frac{1}{\sqrt{2^n}}\sum_x |x, f(x)\rangle\,. \tag{4.10}$$

Apesar do potencial aplicativo do paralelismo ser verdadeiramente fantástico, alguns comentários devem ser tecidos. O paralelismo quântico permite que para uma dada função, sejam avaliados todos os possíveis valores dos elementos do seu domínio, ou seja, avaliando-os de forma simultânea. O

problema seria como acessar, também, de forma simultânea, vários valores calculados dessa função, tendo em vista que os valores avaliados estão, todos, nos *qbits* acoplados. Pelo postulado da medida, existe o problema da aleatoriedade associado à base em que se realiza a medida e o problema de interferência no estado de teste, já que o estado quântico que resulta após a realização de medida se encontrará estritamente relacionado ao resultado da medida. Por exemplo, no caso de uma função binária, equação (4.9), caso uma medida seja realiza, na base computacional, sobre o primeiro qbit, haverão dois possível resultados 0 ou 1, com probabilidades iguais para ambos, o que significa que o estado resultante daria informação somente para um único valor do domínio da função. Mesmo para o caso mais genérico isso ocorrerá. Realizando-se uma medida na base computacional, sobre os n primeiros *qbits*, quaisquer resultados têm as mesmas chances de serem sorteados durante o processo de medida, o que resultará em um estado que só pode conter informação sobre um elemento avaliado na função. Para que o paralelismo se torne um processo útil é necessário que este problema seja transposto. Caso contrário, a tarefa realizada por ele é a mesma de um computador clássico.

4.6 Codificação Superdensa

Por fim, como uma última aplicação dos postulados da mecânica quântica, podendo ser encontrado em [7], é interessante apresentar a codificação superdensa, pois ela faz uso, de forma não trivial, de vários conceitos mencionados até agora, tornando-se um exemplo bem colocado de tarefa que só seria realizada pela mecânica quântica.

Suponha que três amigos, Alcides, Bezerra e Celice, morem em uma mesma localidade e, por motivos sem importância, Alcides e Bezerra necessitaram viajar. Antes que partissem, eles compartilharam com Celice um *qbit* que faz parte de um estado de Bell, o estado

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

... assim Alcides e Bezerra ficaram com um qbit em sua posse e entregaram a Celice o outro. Eles combinaram também que avisariam com antecedência em qual dos quatro aeroportos da cidade (AE0, AE1, AE2, AE3) eles iriam pousar na viagem de volta, e para isso eles iriam usar o *qbit* que estava em sua posse.

O procedimento que Alcides e Bezerra necessitariam realizar é bem simples. Caso o aeroporto que eles iriam pousar fosse AE0, nenhuma modificação seria aplicada ao estado quântico compartilhado por eles, e esse *qbit*, que está em posse de ambos, seria enviado para Celice, de modo que por medidas na base de Bell ela saberia qual dentre os possíveis estados da base é esse estado que ela detém. Caso o aeroporto de pouso fosse AE1, Alcides e Bezerra aplicariam a porta inversora de fase Z ao seu *qbit* compartilhado, e em seguida o enviariam para Celice que por medidas na base adequada identificaria qual o aeroporto indicado. Se o aeroporto de pouso fosse AE2, a modificação impressa sobre o estado quântico seria o efeito de uma porta de inversão de bit X, o *qbit* é enviado à Celice e identificado o aeroporto de pouso e por fim, se o aeroporto fosse AE3, a modificação desejada seria aquela que é realizada pela porta iY e o *qbit* seria enviado à Celice que o identificaria sabendo, então, o aeroporto de pouso.

O que se pode constatar é que através de um estado quântico contendo dois qbit, na base adequada,

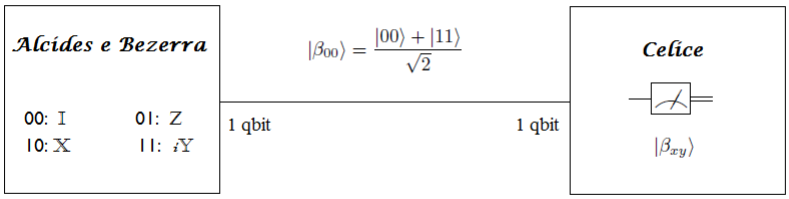


Figura 4.9: Esquema da Codificação Superdensa

é possível transmitir dois bits de informação. No mundo clássico essa tarefa não seria permitida de ser realizada. Em outras palavras, Alcides e Bezerra conseguiram enviar dois bits de informação para Celice, sem que nenhum meio físico fosse estabelecido, usando somente as propriedades de correlação dos estados de Bell e dos estados emaranhados. É importante notar que não existe possibilidade de se haver ruído na transmissão de informação, tendo em vista que não houve meio físico para a transmissão da informação binária clássica, e nem mesmo algum intruso no meio de comunicação, pois para se conhecer a informação transmitida é necessária a posse dos dois qbits que estão em lugares distantes.

$$\text{Informação: 00} \quad \text{Porta aplicada: } I \quad \text{Base de Bell: } \beta_{00} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$\text{Informação: 01} \quad \text{Porta aplicada: } Z \quad \text{Base de Bell: } \beta_{10} = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$\text{Informação: 10} \quad \text{Porta aplicada: } X \quad \text{Base de Bell: } \beta_{01} = \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$
$$\text{Informação: 11} \quad \text{Porta aplicada: } iY \quad \text{Base de Bell: } \beta_{11} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

4.7 Consumo de Energia e sua Relação com a Informação Quântica

Um fator bastante relevante, quando se refere a tecnologias, é o conceito de eficiência energética [47]. É desejável que as novas gerações de computadores permaneçam em sua curva ascendente de desempenho da capacidade de processamento. A lei empírica de *Moore* enuncia que a cada dois anos, mantidos os fatores de custos, a capacidade processual dos computadores dobra. No entanto, como seria o comportamento do fator energético, a eficiência, ao passo que se cresce o poder de processamento dos computadores?

O "consumo"energético passou a ser proeminente recentemente, no que pode ser conhecido como a era dos portáteis. Os celulares, os *notebooks*, iPad's são exemplos em que a eficiência energética é de extrema importância para o bom funcionamento dos processadores embutidos neles. Para estes aparelhos é interessante que os processadores gastem o mínimo de energia possível para realizar as funções necessárias para uma tarefa qualquer. Alternativamente, deseja-se que o fornecimento de energia para os processadores seja longo o suficiente para a realização das tarefas requeridas a eles. De maneira geral, a oferta energética não deve ser uma barreira diante da demanda dos processadores.

Então, para a resolução deste problema, foram criadas duas áreas de pesquisa, pautadas nos fatores mencionados. Uma destas é a área relacionada às baterias, sua eficiência no que concerne a vida útil, degradação, tecnologia do material utilizado, entre outros fatores. A outra área é aquela que estuda a economia de gasto energético por parte dos processadores. É nesta última área que se concentra nosso interesse.

Para entendermos adequadamente a solução apresentada para o problema descrito faz-se necessário conhecer o conceito de *reversibilidade*. Considere a função quadrática $f(x) = x^2$, conhecendo-se o valor da função para um determinado x_1, não conhecido, não é possível com plena certeza determiná-lo, sem alguma *informação adicional*. Por exemplo, sabendo que $f(x_1) = 9$, x_1 pode assumir dois possíveis valores, $x_1 = 3$ ou $x_1 = -3$. Qualquer uma destas possíveis escolhas de x_1, na função, tem o mesmo valor. Pode-se encontrar casos mais frequentes nas funções booleanas, um exemplo é a porta, ou função, **ou**, $f(a, b) = a + b$. Sabendo-se que o resultado, ou saída, da função é $f(a, b) = 1$, existem 3 possíveis casos em que este resultado é obtido, $(0, 1);(1, 1);(1, 0)$, de forma que é indecidível, sem *informações adicionais*, escolher com plena certeza entre as entradas apresentadas.

No entanto, a porta **não**, ou função de negação, é *reversível*, pois se conhecendo a saída, a entrada é completamente especificada. Assim o conceito de reversibilidade se torna bem definido, uma porta lógica é reversível quando, conhecendo-se a saída, a entrada é completamente especificada. No caso em que, após a aplicação, ou funcionamento da porta lógica, o resultado desta não permite completamente especificar as entradas, diz-se que a informação necessária para que se pudessem retroceder as entradas é perdida, ou *apagada*.

Pode-se interpretar o funcionamento dessas portas irreversíveis como destruição da informação adicional, como apagamento da informação adicional. E para as portas reversíveis nenhuma informação é apagada ou destruída. Enfim, o que faz conexão entre a eficiência energética dos processadores das gerações futuras e o apagamento de informação em portas lógicas irreversíveis é o princípio de Landauer[28] [29], [30].

Princípio 4.1. *Suponha que um computador apague um bit de informação. A quantidade de energia perdida, ou dissipada, para realizar tal tarefa é calculada ser de, pelo menos, $k_B T log 2$, em que k_B é a constante de Boltzmann e T é a temperatura.*

É possível apresentar o princípio de Landauer em função da entropia.

Princípio 4.2. *Suponha que um computador apague um bit de informação. A entropia do sistema aumenta em pelo menos $k_B log 2$, em que k_B é a constante de Boltzmann*

A partir desse princípio é possível extrair informações interessantes, como por exemplo, a quantidade mínima de energia necessária para o apagamento de uma informação. A evolução de qualquer geração de computadores pode ser mensurada em função da proximidade da quantidade de energia dissipada nos componentes, para apagar uma informação, por estes componentes em relação ao limite definido pelo princípio de Landauer. Esta energia é calculada em torno de $500 k_B T log 2$, em termos absolutos, o que não representa grande quantidade de energia. No entanto, em relação à cota, esta quantidade de energia está bem distante e se torna importante saber o quanto essa distância pode ser diminuída[28], [7].

A aplicação do princípio de Landauer ao comportamento das portas lógicas é bem pertinente quanto à interpretação da reversibilidade, pois o limite imposto pelo princípio é estabelecido se e

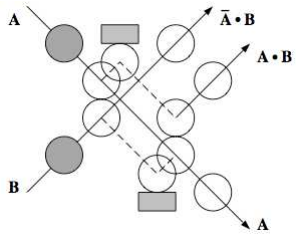


Figura 4.10: Esquema do Computador de Bolas de Bilhar

só se não houver a possibilidade de recuperação da informação. O caso mais interessante ocorre no momento em que a reversibilidade é permitida, pois o princípio é, então, não obedecido e desta forma não há apagamento de informação possibilitando a existência de computação reversível que é sinônimo de computação sem custo energético. Vale salientar que quando se menciona o fato de não haver custo energético refere-se ao funcionamento normal de uma porta lógica qualquer. Isso não garante que não haverá custo energético para a proteção da porta lógica considerada, quanto à influência de ruídos.

Então a busca pela eficiência energética reside em se encontrar uma maneira de se realizar a computação reversível. Os responsáveis pela realizabilidade dos computadores poderiam ter problemas quanto ao custo energético, mas os físicos garantem que este não é o caso, pois as leis físicas são completamente reversíveis. Eles garantem que dado um estado final de um sistema físico fechado, é sempre possível, pelas leis físicas e princípios físicos, retroceder e encontrar o estado inicial do sistema considerado. A questão então se encontra sobre como as portas lógicas que possuem a característica de serem irreversíveis, como por exemplo **E**, **OU**, podem ser modificadas para apresentar reversibilidade e se é possível essa modificação.

Os estudos realizados sobre este assunto focam este problema em duas vias de solução, dois circuitos que são capazes de realizar a computação reversível. O primeiro circuito, construído a partir de bolas de bilhar e barreiras refletoras, é um exemplo de computação reversível cujo funcionamento é regido em função das leis da mecânica clássica [7]. O segundo circuito é uma realização um pouco mais abstrata em relação ao primeiro, baseada em uma porta lógica reversível chamada *Toffoli*, ferramenta bastante usada quando se refere à computação quântica [7].

Na figura 4.10, está representado o circuito simulador do computador de bolas de bilhar. De modo diferente que nas portas lógicas convencionais, em que as entradas são níveis lógicos representados por diferença de potencial, ou tensão, neste caso, as entradas são bolas de bilhar que são inseridas da esquerda para a direita.

Postas a colidir entre si e em barreiras refletoras de modo que ao final do percurso a configuração da saída é justamente o efeito, o comportamento, a aplicação da porta lógica simulada diante de um arranjo de bolas de bilhar postas na entrada, notando que todo o processo é regido pela mecânica clássica e desta forma, conhecendo-se a configuração de saída é possível com plena certeza saber qual a configuração de entrada. Os níveis lógicos 0 e 1 são representados com a ausência ou presença, respectivamente, de bolas de bilhar na entrada do circuito. Outra característica interessante desse circuito de bolas de bilhar é sua universalidade, pois este pode simular, nos padrões apresentados, qualquer circuito lógico na sua forma-padrão de computação.

Espera-se, entretanto, que um circuito construído como da maneira que está apresentada seja de

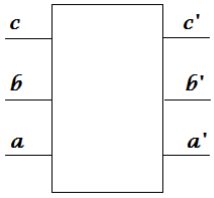


Figura 4.11: Porta Fredkin Genérica

certa forma suscetível a efeitos indesejados de ruídos, estes das mais diversas origens: trepidações, inclinações, pequenas perturbações em geral seriam suficientes para que o funcionamento perfeito do circuito fosse prejudicado, já que o ambiente em que este circuito opera é uma superfície sem atrito e com choques perfeitamente elásticos, entre as bolas e as barreiras refletoras. Assim um circuito como este requer que a sua operação seja realizada em circunstâncias perfeitas de ausência de perturbações externas, as quais são as origens dos ruídos para esta aplicação. A energia despendida para a realização dessas circunstâncias seria impraticável, caso fosse necessário fazer um computador como este. No entanto, para a finalidade que este texto se dispôs a comentar, não oferece dano algum ignorar os efeitos de quaisquer ruídos e focar unicamente no funcionamento do circuito e no entendimento das informações essenciais à computação reversível.

O computador de bolas de bilhar é um dispositivo engenhoso, unicamente regido pelas leis da mecânica, feito para simular o comportamento da *porta fredkin*, porta esta criada para a implementação de portas lógicas universais, diante de diferentes configurações de entrada [7]. Esta porta apresenta três bits de entrada e três bits de saída, denominados a, b, c e a', b', c', respectivamente. O bit c é conhecido como bit de controle, pois durante a operação da porta lógica o seu valor não é modificado e as saídas dos bits a e b são modificadas por diferentes valores do mesmo. Na tabela 4.3, está exposta a tabela verdade da *porta fredkin*; vê-se claramente que quando o bit c tem nível 0, nenhuma modificação é constatada em relação às entradas a e b, no caso em que o bit c tem nível lógico 1, os níveis lógicos postos nas entradas a e b, são constatados trocados na saída. Também se vê, pela tabela verdade, que a *porta fredkin* é reversível. Basta conhecer a saída para completamente especificar a entrada. Outra maneira de se encontrar a entrada de posse de uma saída específica é aplicar a *porta fredkin* tendo como entrada, as saídas especificadas, ou seja, a *porta fredkin* é involutiva. Uma curiosidade sobre a *porta fredkin* é que ela também é conhecida por apresentar a característica de conservação, no sentido de que a quantidade de níveis lógicos 1's é igual tanto na entrada como na saída. É por este motivo que a *porta fredkin* pôde ser simulada através de um computador de bolas de bilhar, pois a quantidade de bolas que entram no circuito deve ser igual a quantidade de bolas que saem.

Um modelo genérico da porta *fredkin* está exposto na figura 4.11. Através desta tabela verdade, é possível encontrar uma fórmula booleana para a representação do funcionamento da mesma. É fato conhecido dos estudiosos de tecnologias digitais que existe uma maneira de se expressar qualquer porta lógica através da porta Nand. Com esse conceito em mente, a figura 4.12 representa como implementar a porta Nand clássica utilizando a porta *fredkin* genérica, já que a porta *fredkin* apresenta a característica de ser reversível.

As equações booleanas das saídas da *porta fredkin*, equações (4.11) e (4.12), podem ser usadas

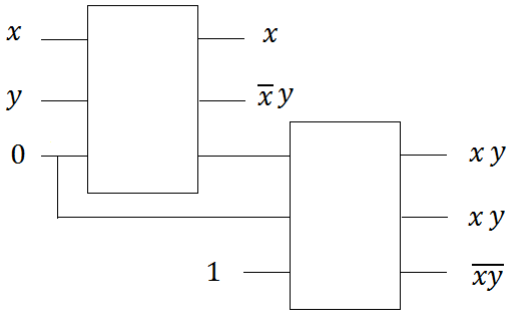


Figura 4.12: Implementação da Porta Nand

Tabela 4.3: Tabela Verdade da *Porta Fredkin*

Entrada			**Saída**		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1

para simular portas lógicas clássicas com operação reversível e que sejam também universais, obtendo assim quaisquer portas lógicas com propriedade de reversibilidade.

$$a' = \overline{b}\overline{c} + \overline{a}\overline{b} + \overline{a}\overline{c}, \tag{4.11}$$

$$b' = \overline{a}\overline{c} + \overline{a}\overline{b} + \overline{b}c. \tag{4.12}$$

Para simular a operação de uma porta **E**, através da *porta fredkin*, figura 4.12, é necessária a preparação de bits auxiliares na entrada, níveis lógicos 0 e 1, e utilização de bits auxiliares na saída. Estes podem ser considerados desnecessário para a operação clássica da porta considerada, pois são usados excepcionalmente para a preservação da característica de reversibilidade.

De forma geral, ampliando o conceito de simulação de portas clássicas, qualquer circuito que opere conforme uma função $f(x)$ arbitrária, pode ser simu-lado, de modo reversível, utilizando somente *portas fredkin*, tendo em vista a universalidade das portas **NOR** e **NAND**. Com auxílio de alguns bits de entrada "p", pré-definidos em um estado padrão, obtendo-se como resultado o valor esperado da função $f(x)$ para a entrada desejada x. Esse tipo de operação comumente apresenta uma saída que é também derivada da entrada x, o qual chamaremos de $g(x)$ que pode ser considerado desprezível, contudo é conhecido como resíduo da operação. Desat forma, a representação matemática para a simulação é dado por $(x, p) \rightarrow (f(x), g(x))$. O seguinte caso a ser estudado é como lidar com os bits auxiliares das saídas, o 'resíduo', já que eles são gerados para garantir a economia de energia, assim, seria possível que estes sejam eliminados por alguma configuração de portas lógicas?

Considere um arranjo inicial de estados de entrada dado por $(x, 0, 0, y)$ que deve ser aplicado a um circuito lógico quântico reversível simulador de uma função lógica clássica $f(x)$, produzindo a saída $(x, f(x), g(x), y)$, em que x é o estado cujo valor da função deseja-se conhecer, y é um estado-padrão auxiliar e $g(x)$ representa o 'resíduo' da simulação.

Suponha a aplicação de uma porta **NÃO-CONTROLADA** sobre os registros 2 e 4 do arranjo de saída considerado, de forma que se obteria o resultado $(x, f(x), g(x), y \oplus f(x))$, em que $\oplus$ representa a adição módulo 2 entre y e $f(x)$. E por fim, como em todo o processo descrito foram usados meios reversíveis, é possível aplicar novamente o circuito simulador da função $f(x)$ no arranjo final e obter, por conseguinte, o arranjo $(x, 0, 0, y \oplus f(x))$. Eliminando-se os passos intermediários e com isso os bits auxiliares usados no decorrer do processo, podemos expressar a ação conjunta desses elementos pela equação (4.13). Esta forma de expressão é bastante interessante por ser geral e involutiva. Após essa primeira discussão uma questão seria pertinente, qual seria o custo da computação reversível, de maneira como aqui foi apresentada?

Nesta análise deve ser levado em conta o número de bits auxiliares necessário à reversibilidade e a quantidade de portas no modelo clássico, pois esta quantidade deve igual à quantidade de portas no modelo reversível, a menos de um fator constante que representa a quantidade de *portas fredkin* usadas para simular cada elemento do circuito irreversível, com um fator de 2 por motivos da computação reversa.

$$(x, y) \rightarrow (x, y \oplus f(x)) \tag{4.13}$$

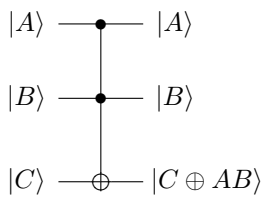


Figura 4.13: Esquema do circuito da Porta Toffoli

Tabela 4.4: Tabela Verdade da *Porta Toffoli*

Entrada			**Saída**		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Outra maneira de se programar a computação reversível é através da *porta toffoli*. Diferente da *porta fredkin*, em que havia a possibilidade de construção de um computador gerido somente pelas leis da mecânica, a *porta toffoli* não apresenta a fundamental característica de conservação, a qual seria necessária para a construção de um computador de bolas de bilhar. Mesmo utilizando outros meios de realização, a *porta toffoli* não tem uma construção física trivial.

A *porta toffoli* em sua operação faz uso de três bits de entrada, a, b, c, desses os bits a e b são bits de controle, pois durante o funcionamento da porta os seus valores não são modificados, e o bit c é o bit conhecido como bit-alvo. No caso em que os bits de controle têm, simultaneamente, níveis lógicos altos, o valor do bit-alvo é modificado, no caso contrário, o valor do bit-alvo não é modificado. na tabela 4.4, está exposta a tabela-verdade para a operação normal da porta toffoli, e na figura 4.13, a representação gráfica usual da porta.

É possível pela *porta toffoli*, realizar a computação clássica universal. Considere que se deseje simular a operação de uma porta **NÃO-E**, através da *porta toffoli*. Pela tabela-verdade e com auxílio do mapa-k, aplicada ao bit-alvo c, é possível extrair a equação booleana deste: $c' = c \oplus ab$; sabe-se que a equação de uma porta ou-exclusivo é da forma $\overline{a}b + a\overline{b}$, aplicando isto à equação do bit-alvo c' é possível obter a porta universal **NÃO-E**. Da mesma maneira como foi descrito no processo de simulação da porta universal **NÃO-E** para a *porta fredkin*, na existência de bits de resíduos, ocorre também na simulação da *porta toffoli*. A técnica descrita anteriormente para a eliminação dos bits residuais, na computação reversa, feitas na *porta fredkin*, pode também ser aplicada na *porta toffoli*.

Em termos gerais, o grande interesse da computação reversível jaz sobre a interpretação bem construída do principio de Landauer, princípio 4.2, sobre o apagamento de bits no funcionamento de

uma porta lógica. Apesar do modelo computacional do circuito de bolas de bilhar, o qual simula, de forma bastante elegante, a operação da *porta fredkin*, ser reversível e desta forma não necessitar de energia durante a sua operação, este é muito suscetível a efeitos danosos de ruídos, oriundos de diversas fontes, tornando-se impraticável a sua realização. A *porta toffoli*, por sua vez, tem uma construção mais complicada que a *porta fredkin* e que, no entanto, tem a característica de não implicar no gasto energético. Isso não quer dizer que não haverá nenhum gasto energético suplementar durante a operação de um computador construído a partir de lógicas reversíveis, pois ainda há a necessidade de proteger os circuitos contra efeitos de ruídos. Desta forma o circuito de proteção deve realizar medidas sobre as operações das portas para verificar se o desempenho desta está em conformidade com o que se espera. No entanto, como os circuitos de proteção têm, indubitavelmente, uma memória finita, em algum momento será necessário apagar-se uma informação armazenada na memória para que seja dado espaço para as informações oriundas de outra medidas e isso acarretará o gasto energético previsto pelo princípio de Landauer.

capítulo 5

Codificação Quântica

"La loi suprême de l'invention humaine est que l'on n'invente qu'en travaillant."
Gallimard

Na década de 40, um texto científico possibilitou um grande esclarecimento a todos os engenheiros de telecomunicação, sobre como e em que circunstâncias uma informação qualquer poderia trafegar em um canal de comunicação [3]. C. E. Shannon, através de dois teoremas, conseguiu a difícil façanha de responder as questões que há muito eram barreiras ao desenvolvimento tecnológico. Em que circunstâncias, relacionadas aos recursos tecnológicos, uma informação poderia ser transmitida em um canal de comunicação? Como essa informação poderia ser enviada nesse canal de modo que o efeito de um agente nocivo à integridade da informação pudesse ser percebido e dessa forma corrigido? Essas duas questões deram início a um campo de estudo cuja importância é sem sombra de dúvida indiscutível.

O teorema da codificação de canal sem ruído foi à forma que Shannon encontrou para responder ao primeiro questionamento. Este teorema quantifica quais os recursos físicos necessários para que uma determinada informação pudesse trafegar e ser armazenada. *O teorema da codificação de canal com ruído* quantifica a informação que pode ser transmitida com confiabilidade controlada em um canal que apresenta ruído. A partir de segundo teorema foi possível construir uma estrutura matemática que é capaz de identificar o padrão de erro e corrigi-lo, essa estrutura são os códigos corretores de erros.

Apesar do grande desenvolvimento proporcionado por esses dois teoremas, *o teorema da codificação de canal com ruído* não fornece uma maneira construtiva de se conceber um código adequado para uma determinada aplicação. Desta forma uma área de estudo e pesquisa foi criada no intuito de encontrar um código que seja ideal para qualquer aplicação. Destacam-se, entre os diversos tipos de códigos, os códigos de bloco usados em aplicações em que erros ocorrem aleatoriamente. Existem também outros tipos de códigos, por exemplo, códigos algébricos **??**, códigos de treliça **??**, códigos LDPC **??**,

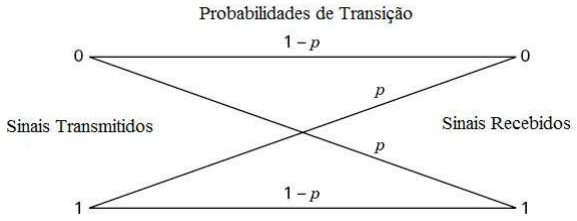


Figura 5.1: Esquema do canal BSC

códigos Turbo **??**. As aplicações dessas técnicas de correção estão por toda a parte; reprodutores de mídias como DVDs e CDs, modens, são exemplos de sistemas que necessitam de uma boa capacidade de correção de erros para poderem operar de forma aceitável.

O desenvolvimento da área de códigos corretores de erros quânticos seguiu como um desdobramento da área de códigos corretores de erros clássicos, adaptando as técnicas já existentes e por vezes criando novas técnicas. O conceito de ruído, por exemplo, é particular para o caso quântico, exigindo que algumas adaptações fossem realizadas.

Como já deve ser possível perceber, para o caso da área de codificação de erros quânticos, surgem alguns problemas que não haviam no caso clássico.O problema relacionado ao teorema da não-clonagem e o problema da medida, ambos proporcionam dificuldades maiores no processo de correção. O problema da não-clonagem, ou seja, a impossibilidade de se realizar uma cópia de um estado quântico em superposição apresentaria um entrave às necessidades das técnicas de correção quântica se estas fossem somente arranjos das técnicas de correção clássica. Ligado ao tópico apresentado está o problema da medida - por questões de que a medida destrói a informação quântica.

Um exemplo clássico e de fácil explicação é o código de repetição. Suponha que uma determinada mensagem deva ser enviada através de um canal de comunicação ao seu destinatário. Antes é realizado um estudo prévio sobre o comportamento do canal. Assim as características do canal são modeladas pelo conhecido *Canal Simétrico Binário* (BSC), Figura 5.1. Este modelo diz que existe uma probabilidade de que um dado bit seja invertido e que existe a probabilidade complementar de que o bit não seja alterado.

Desta forma, uma possível solução encontrada foi repetir um número "n" impar de vezes cada bit de informação da mensagem; este código é nomeado código de repetição $C(n, 1)$. Por exemplo, a mensagem 101, modificada pelo código de repetição $C(3, 1)$, resulta em 111000111. A escolha da implantação de um número impar de cópias de cada bit de mensagem vem do modelo probabilístico do canal, pois é mais provável que $\lfloor (n-1)/2 \rfloor$ bits, ou menos, tenham sido invertidos que $\lfloor (n-1)/2+1 \rfloor$, ou mais. Caso fosse implantado um número par de cópias do bit poderia, em pelo menos uma circunstância, haver ambiguidade quanto à decidibilidade da possível mensagem enviada.

Então, ao se receber a mensagem 110001110, analisando por blocos, a probabilidade de que num bloco tenha ocorrido um erro é maior que a de ter ocorrido mais que um erro. Assim, a decodificação é realizada por votação majoritária, resultando em 111000111. No entanto, no caso quântico é necessário definir o que é a mensagem a ser enviada. Para o caso quântico, os coeficientes α_i da combinação linear da equação (3.1) representa a informação a ser enviada, pois é isso que, de maneira suficiente, define o estado de superposição.

Desta forma, fica claro que no caso quântico não é possível fazer, da mesma maneira que no caso clássico, cópias das informações na tentativa de realizar um código quântico de repetição nos mesmos moldes do código clássico. Outro ponto a ser mencionado é a infinidade de erros possíveis que podem recair sobre o estado quântico em trânsito no canal de comunicação, já que o modelo mais bem aceito de um estado quântico em superposição é a esfera de Bloch.

5.1 Código de Inversão de Bit

Para que seja possível simular um código quântico que se assemelha ao código de repetição clássico é importante modelar o canal quântico em que a informação irá trafegar. Suponha que o canal quântico altere o estado quântico aplicando uma inversão de bit, Porta quântica X, com probabilidade p e que não altere o estado quântico com probabilidade $1-p$, este tipo de canal é chamado canal quântico de inversão de bit.

Suponha que um estado quântico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ contenha a mensagem a ser enviada através do canal de comunicação que pode ser considerado como o canal quântico de inversão de bit. Pelo modelo deste canal existe uma probabilidade p de o estado quântico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ser transformado no estado quântico $|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$ e uma probabilidade $1-p$ do estado permanecer inalterado. Visando esta situação, é possível, através da porta quântica Não-Controlado, conseguir, de modo semelhante ao código de repetição clássico, identificar o erro ocorrido no estado quântico em trânsito no canal e corrigi-lo.

Acoplando ao estado quântico original dois estados quânticos cada um em nível puro, isso significa que se é preparado dois estados $|0\rangle$ e que são acoplados à $|\psi\rangle$, resulta no estado $|\psi 00\rangle$. Essa modificação não afetará a informação contida no estado quântico. Em seguida, aplica-se a porta Não-Controlado sobre os *qbits* acoplados, tendo como *qbit* de controle os estados originais. Assim, o estado $|000\rangle$ não é alterado e pode ser nomeado como $|0_C\rangle$ e o estado quântico $|100\rangle$ é alterado para $|111\rangle$ que pode ser nomeado como $|1_C\rangle$, modificando o estado original $|\psi\rangle$ para $|\psi_C\rangle$, em que o sub-escrito C indica *codificado*

$$|\psi_C\rangle = \alpha|0_C\rangle + \beta|1_C\rangle = |\alpha|000\rangle + \beta|111\rangle.$$

A probabilidade que haja um erro, ou não haja erro nenhum é $(1-p)^3 + 3p(1-p)^2$, a qual é maior que a probabilidade de haver dois ou mais erros. O envio do estado quântico codificado é feito através de três linhas que tem a capacidade de transportar cada estado quântico. O circuito que implementa a codificação do estado quântico de informação $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ é mostrado na figura 5.2, em que $C_1 = (X_2X_3)^{x_1}$.

A notação $C_n = [f(X_i]^{g(x_1)}$ é uma maneira descritiva de representar uma porta quântica controlada. A função $g(x_i)$ tem como imagem o conjunto $I_{g(x_i)} = 0, 1$ e cujo domínio são todas as possíveis combinações dos *qbits* acoplados. A função $f(X_i)$ representa a atuação de qualquer porta quântica básica, ou mais precisamente as matrizes de Pauli, sobre alguns *qbits* específicos. Considere $C = (X_2X_3)^{x_1}$, essa porta quântica testa o primeiro *qbit* de um total de três *qbits* acoplados. Em caso positivo, as matrizes de Pauli atuam sobre na inversão dos *qbits* 2 e 3, representado pelos índices.

Suponha que um erro ocorra, não importando em que *qbit* tenha essa inversão de bit ocorrido. Aparentemente, mesmo com a capacidade de identificar o erro pelo voto majoritário, para que se

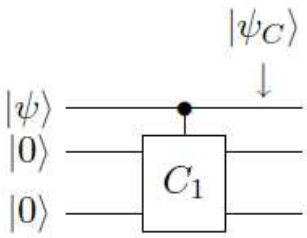


Figura 5.2: Esquema de circuito de codificação para o código quântico de repetição

pudesse usar este recurso deve-se realizar uma medição. Existe no entanto, um conjunto de transformações lineares que podem realizar uma medida e que podem detectar um possível erro nos estados codificados.

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|. \tag{5.1}$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|. \tag{5.2}$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|. \tag{5.3}$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|. \tag{5.4}$$

Sem perda de generalidade é correto supor que um erro $E = X_2$ possa ter ocorrido e afetado o estado quântico em trânsito, em que o índice identificará em que estado acoplado o erro atuou. Desta forma, o estado após ser afetado pelo erro é $|\psi_1\rangle = \alpha|010\rangle + \beta|101\rangle$. Pelo postulado da medida, (Postulado 3.3), uma medida realizada por qualquer observável M, terá como possíveis resultados os autovalores associados à este observável. Considerando P_3 como observável de medida, os possíveis valores são 1 e 0, que neste caso ocorrerá sempre, para este estado quântico afetado, o valor de medida 1.

É importante assegurar que o processo de identificação de erro não deva afetar o estado quântico de modo irreversível. Por exemplo, se for tomado para realização de uma medida o observável P_2 ou P_3, não é possível inferir que tipo de erro ocorreu no estado quântico de informação, $|\psi_1\rangle$. Além disso, este estado será afetado de modo que não seria possível extrair qualquer informação dele. Para a realização da síndrome de erro é possível, eficientemente, utilizar-se dos projetores, equações 5.1, 5.2, 5.3, 5.4. Cada um desses projetores pode informar qual o tipo de erro que ocorreu no estado quântico. Se o valor da síndrome for 1 para uma medida utilizando P_3 significa que um erro do tipo X_3 afetou o estado quântico. Como só estão sendo considerados, para esse canal em particular, erros que afetem um *qbit* por vez, as outras medidas serão 0 para os outros projetores.

Um fato interessante sobre o estado quântico $|\psi\rangle$ é que existem, pelo menos, dois operadores que não afetam a sua estrutura. Estes operadores podem ser usados para detectar que tipo de erro possa ter ocorrido sem que o estado seja afetado e a informação perdida. Z_1Z_2 e Z_2Z_3 são operadores que quando aplicados sobre o estado $|\psi\rangle$, não realizam qualquer efeito sobre este.

Tabela 5.1: Tabela de síndrome para os observáveis Z_1Z_2 e Z_2Z_3

Síndrome		**Erro**
1	1	I
-1	1	X_1
-1	-1	X_2
1	-1	X_3

.

$$Z_1Z_2 = ZZI = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{5.5}$$

$$Z_2Z_3 = IZZ = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{5.6}$$

$$Z_1Z_2|\psi_C\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta \end{pmatrix}. \tag{5.7}$$

$$Z_2Z_3|\psi_C\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta \end{pmatrix}. \tag{5.8}$$

Esses observáveis possuem ambos, autovalores ± 1 que indicam que serão estes, os possíveis resultados das medidas. É possível, com medidas em cascata, obter quatro possíveis resultados de síndrome como é requerido para identificar os erros considerados neste tipo de canal. Caso os resultados das medidas sejam 1 e 1, para Z_1Z_2 e Z_2Z_3, respectivamente, é assegurado que o erro que afetou o estado foi I, ou seja nenhum erro. Na tabela 5.1 estão expostos os erros e suas possíveis síndromes.

Outro operador que também apresenta a propriedade de não afetar o estado quântico é Z_1Z_3. O que ocorre é que é possível formar um conjunto, $A = \{Z_1Z_2; Z_2Z_3; Z_1Z_3\}$, com esses três operadores que englobam todos os operadores que apresentam essa característica. É possível realizar medidas de síndrome para os erros considerados, de modo eficiente, tomando-se dois operadores quaisquer do conjunto considerado, sem qualquer exigência.

A decodificação é realizada identificando o possível erro que afetou o estado quântico. Em seguida, aplica-se o operador adjunto associado ao erro identificado, eliminando o efeito do erro sobre o estado

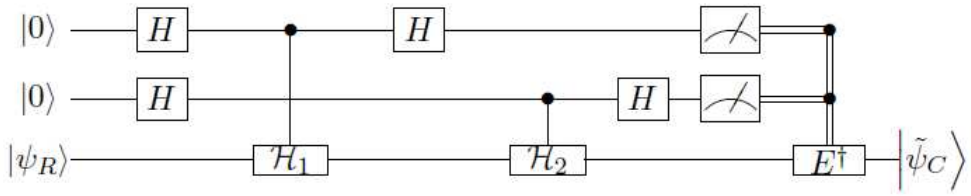


Figura 5.3: Esquema de circuito de decodificação para o código quântico de repetição

e recuperando de forma clara a informação. Na figura 5.3, está exposto o circuito de decodificação para o código de inversão de bit, em que os $i = \{1, 2\}$ em H_i, representam observáveis próprios para ser obtida a síndrome do erro.

As possibilidades de erros que afetam um estado quântico podem não apresentar um efeito dicotômico como o que pode ser visto no caso clássico. Um mesmo operador pode modificar drasticamente um estado quântico e não afetar em nada outro estado. Por exemplo, o operador X quando aplicado sobre $|0\rangle$ modifica o estado para $|1\rangle$. Porém, quando aplicado sobre o estado $(|0\rangle + |1\rangle)/2$, não apresenta nenhum efeito. Uma maneira de se quantificar quão distantes estão dois estados quânticos, em que $|\psi\rangle$ é uma estado puro e ρ é um estado arbitrário, é utilizando uma medida chamada de *fidelidade*,

$$F(|\psi\rangle, \rho) \equiv \sqrt{\langle\psi|\rho|\psi\rangle}; \tag{5.9}$$

define-se um estado quântico puro como aquele em que $tr(\rho^2) = 1$ e um estado quântico misto como aquele em que $tr(\rho^2) < 1$.

O Traço de uma matriz $A_{m\mathrm{X}m}$ define-se como:

$$tr(A) \equiv \sum_{i=1}^{m} A_{ii}.$$

Analisando a correção quântica de erros através da fidelidade é seguro afirmar que o objetivo desta métrica entre estados quânticos é atingir um valor máximo, o mais próximo da unidade possível. Considerando o caso em que nenhum processo de correção de erro é aplicado, o estado após o envio através do canal é

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

A Fidelidade é calculada como

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

...na equação anterior, os termos que contém $\langle\psi|X|\psi\rangle$ são nulos quando o estado a ser enviado é $|\psi\rangle = 0$ e assim a fidelidade mínima é $F = \sqrt{1 - p}$. Considere, agora, que seja implantado um processo de correção de erro e que o estado a ser enviado é $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ e o estado quântico possível na saída do canal é dado por:

$$\rho = \left[(1-p)^3 + 3p(1-p)^2\right] |\psi\rangle\langle\psi| + \cdots$$

Todos os termos não exposto na equação não modificam o fato de que a fidelidade calculada é limitada inferiormente em relação a fidelidade real. A fidelidade é então: $F = \sqrt{\langle\psi|\rho|\psi\rangle} \geq \sqrt{1-p)^3 + 3p(1-p)^2}$. Vê-se claramente que a fidelidade aumenta para o caso de aplicação de algum processo de correção quando a probabilidade de erro é menor que 1/2.

O conceito de fidelidade é requerido quando se deseja medir a distância entre dois estados quânticos arbitrários. Este conceito é semelhante ao conceito clássico de distância de Hamming, empregado ordinariamente quando se refere aos códigos clássicos. Por vezes, o conceito de fidelidade é empregado para se estudar a relação entre os estados quânticos, corrompidos e não corrompidos por um erro arbitrário, quando estes elementos passam por um meio de comunicação próprio a sua condução. A informação adquirida com o estudo da fidelidade dos estados quânticos pode ser alcançada seguindo os critérios próprios da correção quântica de erro. Desta forma, no estudo realizado sobre os estados quânticos, a métrica da fidelidade não é frequentemente empregada.

5.2 Código de Inversão de Fase

O exemplo de codificação apresentado anteriormente utilizou de proteção contra erros de inversão de bit que são representados pela matriz de Pauli X. Existe, igualmente ao caso de inversão de bit, um canal que pode afetar um estado quântico através de outra matriz de Pauli, a matriz de inversão de fase Z. Para este canal, existe uma probabilidade p de que o estado quântico de informação seja afetado pela matriz Z e uma probabilidade $1-p$ de que o estado não seja afetado.

A codificação é inicializada realizando-se uma modificação na base utilizada para uma base mais apropriada. No caso do canal de inversão de bit era conveniente usar a base computacional, $|0\rangle$ e $|1\rangle$. No caso do canal de inversão de fase a base mais conveniente é a base de Hadamard, $|+\rangle$ e $|-\rangle$. A conveniência decorre do fato que um estado quântico que deve trafegar através de um canal quântico que apresenta a característica de inversão de fase pode ser modificado pra que todo o arcabouço desenvolvido para a correção de erro quântico de inversão de bit seja utilizado para a inversão de fase.

Considere um estado quântico que deva ser inserido em um canal que apresenta inversão de fase, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. O erro que pode afetar o estado é representado pela matriz Z, o qual quando posto a interagir com o estado $|\psi\rangle$ resultará em um novo estado $|\psi_1\rangle = \alpha|0\rangle - \beta|1\rangle$. Utilizando a base de Hadamard para representar o estado $|\psi\rangle$, a representação do estado de informação é modificada para $|\psi\rangle = \alpha|+\rangle + \beta|-\rangle$. Quando este estado de informação modificado é posto a interagir com o erro próprio do canal, o resultado é o estado $|\psi_1\rangle = \alpha|-\rangle + \beta|+\rangle$. As expressões (5.10) e (5.11) mostram o efeito do erro sobre os estados da base.

$$Z|+\rangle = Z\left(\frac{|0\rangle + |1\rangle}{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 \\ -1/2 \end{pmatrix} = |-\rangle. \tag{5.10}$$

$$Z|-\rangle = Z\left(\frac{|0\rangle + |1\rangle}{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1/2 \\ -1/2 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} = |+\rangle. \tag{5.11}$$

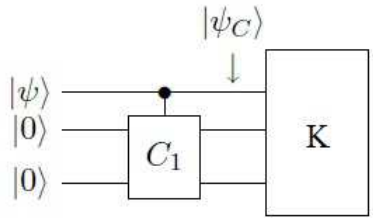


Figura 5.4: Esquema de circuito de codificação para o código quântico de inversão de fase

Fica claro que a aplicação do erro característico ao canal de inversão de bit sobre os estados da base computacional é semelhante à aplicação do erro característico do canal de inversão de fase na base de Hadamard. É este fato interessante que proporciona uma economia no que se refere à construção dos circuitos de codificação e decodificação.

A codificação para o estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ faz o mapeamento deste estado no estado $|\psi\rangle = \alpha|0_C\rangle + \beta|1_C\rangle$, em que os estados $|0_C\rangle$ e $|1_C\rangle$ têm suas expressões expostas nas equações (5.12) e (5.13),

$$|0_C\rangle = |+++\rangle = \frac{1}{8}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}; \tag{5.12}$$

$$|1_C\rangle = |---\rangle = \frac{1}{8}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \\ -1 \\ 1 \\ 1 \\ -1 \end{pmatrix}. \tag{5.13}$$

Esta codificação é conseguida utilizando-se o mesmo circuito de codificação para a codificação do canal de inversão de bit, figura 5.4, em que o bloco K representa a matriz de mudança de base, $K = H_1H_2H_3$.

O processo de decodificação também obedece ao princípio da semelhança. É possível utilizar, para o processo de decodificação, quatro projetores sobre o espaço de estados codificados, equações (5.14), (5.15), (5.16), (5.17).

$$P_0 = |+++\rangle\langle+++| + |---\rangle\langle---|. \tag{5.14}$$

$$P_1 = |-++\rangle\langle-++| + |+--\rangle\langle+--|. \tag{5.15}$$

$$P_2 = |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-|. \tag{5.16}$$

$$P_3 = |++-\rangle\langle++-| + |--+\rangle\langle--+|. \tag{5.17}$$

Medidas realizadas por estes projetores podem identificar que tipo de erro afetou o estado de informação. Por exemplo, caso tenha ocorrido um erro do tipo Z_1, as medidas utilizando os projetores P_1, P_3 e P_4 serão todas iguais a zero e a medida com o projetor P_2 terá como resultado um.

Da mesma forma que existem operadores que não apresentam efeito algum sobre o estado codificado para o canal de inversão de bit, existem também operadores que não afetam o estado codificado para o canal de inversão de fase. Estes operadores formam um conjunto que apresenta essa característica, $A = \{X_1X_2, X_1X_3, X_2X_3\}$.

O fato interessante é que esse conjunto de operadores pode ser obtido a partir do conjunto de operadores para a codificação de inversão de bit,

$$HXH = Z \leftrightarrow \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{5.18}$$

O circuito de decodificação também é o mesmo com a modificação de retorno a base computacional.

5.3 Código de Shor

Os códigos apresentados até aqui protegem a informação quanto a dois tipos de erros, erros de inversão de bit e inversão de fase, representados pelas matrizes de Pauli X e Z, respectivamente. No entanto, essas estruturas não têm a capacidade de proteger a informação que trafega no canal simultaneamente aos dois tipos de erros. Uma saída a este problema foi construída pelo matemático americano Peter Shor [12].

A construção do código de Shor tem plena semelhança com a estrutura de funções compostas. Este código é concebido utilizando as estruturas dos códigos de repetição para erros de inversão de fase e inversão de bit em que o elemento quântico de saída do primeiro codificador é utilizado como elemento quântico de entrada do segundo codificador.

Considere o estado quântico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$; a codificação inicia-se aplicando o código relativo à proteção da inversão de fase ao estado de informação e em seguida o código relativo à proteção da inversão de bit. Os estados da base são modificados e codificados inicialmente da representação computacional convencional para a representação de Hadamard: $|0\rangle \rightarrow |++\rangle$ e $|1\rangle \rightarrow |--\rangle$. A partir desse estado quântico de três *qbits* aplica-se a cada qbit a repetição na base computacional: $|+\rangle = (|0\rangle + |1\rangle)/2 \rightarrow |\widetilde{+}\rangle = (|000\rangle + |111\rangle)/2\sqrt{2}$. O processo total de codificação tem como resultado final os estados codificados:

$$|0_C\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}};$$

$$|1_C\rangle \equiv \frac{(|000\rangle - |111\rangle)\,(|000\rangle - |111\rangle)\,(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

Através do circuito de codificação para o código de Shor é possível visualizar que a primeira parte do circuito é construída com a mesma topologia do circuito de codificação de inversão de fase e a segunda parte é idêntica à estrutura do código de inversão de bit. Essa maneira de construir o circuito do código de Shor é semelhante a estrutura matemática de funções compostas e pode, desta forma ser representado como tal.

O código de Shor é interessante não apenas por introduzir uma maneira de proteger a informação contida no estado quântico contra os tipos de erros apresentados, mas também por apresentar uma maneira eficiente, denominada concatenação, de se construir novos códigos quânticos a partir de códigos quânticos já estabelecidos.

Suponha que um estado quântico de informação, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ seja codificado para trafegar em um canal quântico que apresente erros do tipo de inversão de bit e de inversão de fase. Um erro do tipo X_1 interage com o estado quântico codificado durante a passagem deste pelo canal. É possível identificar esse erro através do processo de medição pelo observável Z_1Z_2, o qual terá como resultado -1. No entanto, isso não é suficiente para identificar o erro. Outra medição é requerida através do operador Z_2Z_3: dois possíveis resultados podem ocorrer, 1 ou -1. No caso da medição obter como resultado 1, pode se supor que o provável erro que afetou o estado quântico de informação é X_1, caso a medida tenha como resultado -1, o erro que afetou o estado é X_2.

Suponha agora que outro tipo de erro afetou o estado, um erro do tipo Z_1. O efeito deste operador faz com que o primeiro bloco de três *qbits* tenha seu sinal modificado: $|000\rangle + |111\rangle$ para $|000\rangle - |111\rangle$. O que mais interessa sobre esse tipo de codificação é que alguns tipos de erros têm o mesmo efeito sobre o estado codificado. Os operadores Z_1, Z_2 ou Z_3 proporcionariam, se postos a interagir com o estado codificado, o mesmo efeito. Desta forma, seria possível fazê-los participantes de um grupo em que esta relação fosse a regra de admissão dos elementos. Isto é interessante pois neste sentido, alguns tipos de erros são agrupados de forma que é necessária unicamente a aplicação de um operador de correção para desfazer o efeito de qualquer elemento deste agrupamento; essa propriedade de agrupamento de erros torna o código conhecido como código degenerado. O processo necessário para uma escolha do provável erro que se incidiu é a comparação por bloco dos seus sinais. Comparando os sinais do primeiro e do segundo bloco, obtém-se que eles apresentam sinais diferentes; em seguida observa-se a comparação dos sinais do segundo e do terceiro bloco e obtém - que estes apresentam o mesmo sinal. Por votação majoritária, toma-se a decisão de que um erro cujo efeito seria modificar o sinal do primeiro bloco deve ter ocorrido. A recuperação é alcançada invertendo a fase do primeiro bloco.

É possível também corrigir erros simultâneos através desse tipo de codificação. Suponha que tenha ocorrido um erro de inversão de fase e inversão de bit, todos ocorridos no primeiro *qbit*. Através do procedimento descrito previamente, é possível reaplicá-lo e diante dos resultados esses erros serão detectados e corrigidos, confirmando assim a idéia de que o código de Shor corrige erros simultâneos sobre o mesmo *qbit*.

Uma análise mais profunda pode ser realizada de modo que uma explicação mais bem detalhada possa ser alcançada. Suponha que um estado quântico de informação seja codificado, $|\psi_C\rangle = \alpha|0_C\rangle + \beta|1_C\rangle$ e que durante o seu tráfego pelo canal de comunicação quântico, um ruído interagiu com o mesmo. Como os possíveis erros que podem afetar esse estado são os descritos pelas matrizes de Pauli

de inversão de bit e inversão de fase, é possível expressar o ruído como uma combinação linear dessas matrizes na forma de

$$E_i = e_{i0}I + e_{i1}X_1 + e_{i2}Z_1 + e_{i3}X_1Z_1. \tag{5.19}$$

Vale salientar que está sendo considerado o efeito de erros simultâneos sobre o mesmo qbit e mais precisamente sobre o primeiro qbit. Quando este ruído interage com o estado codificado, ocorre uma superposição não normalizada de estados quânticos $|\psi\rangle$, $X|\psi\rangle$, $Z|\psi\rangle$, $XZ|\psi\rangle$. Ocorre em seguida que o processo de medição irá destruir essa superposição não normalizada, proporcionada pelo ruído, para algum dentre os estados da combinação linear de modo que só reste o estado quântico que pode ser corrigido pelo processo de decodificação.

Esta mesma análise pode ser realizada para qualquer erro que atue sobre um qbit específico do estado quântico codificado. Isso é bastante interessante, o fato de que a correção de um agrupamento de erros possíveis: erros de fase, erros de bit e erros simultâneos dessas inversões, poder corrigir um *continuum* de erros que podem ser representados sobre a esfera de Bloch. Isto é, no entanto, uma classe de acontecimentos muito mais abrangente, já que esta última classe pertence ao *continuum* e a classe que é mais comumente referenciada é a classe de erros discretos.

5.4 Teoria da Correção Quântica de Erro

Após a apresentação desses exemplos de códigos quânticos, é natural que sejam feitas questões relacionadas à possibilidade de haver uma teoria geral para a correção de erros quânticos. Pois o estudo relacionados as condições para correção de erros, no sentido de apresentar algumas equações que devam ser satisfeitas para que essa tarefa possa ser realizada de maneira eficiente, pode facilitar a análise por parte do projetista do código. Essa estrutura matemática tem o objetivo de testar se o código projetado é capaz de detectar e corrigir os efeitos "corruptivos"à informação quântica. Sendo possível a estruturação matemática dessas condições , isso não é condição suficiente para garantir a existência de bons códigos quânticos.

Tomando por base o exemplo do código de Shor apresentado na seção anterior, é possível, mesmo intuitivamente iniciar através de idéias básicas, uma construção dessa estrutura. Recapitulando os procedimentos efetuados durante todo o trajeto, desde o envio do estado quântico de informação, por parte do remetente, até a recepção do estado quântico mais provável de haver sido enviado, por parte do destinatário, é possível apresentar essas idéias.

Inicialmente o estado quântico de informação é codificado por meio de operações unitárias em um código corretor de erros quânticos. Esse código é construído de modo a ser um subconjunto do espaço em que os estado quânticos são representados, ou seja, o espaço de Hilbert [21]. O segundo momento experimentado pelo estado quântico é a atuação do ruído, seguido da síndrome do mesmo para a sua identificação e por fim a aplicação do operador correspondente ao efeito inverso proporcionado pelo ruído.

No processo de identificação do erro alguns cuidados devem ser tomados. O erro tem a capacidade de transportar o estado quântico codificado para um subespaço diferente do qual este foi inicialmente projetado. Identificar o erro é identificar o subespaço de destino do estado quântico afetado pelo erro. Assim é importante garantir que todos os espaço vetoriais de destino sejam ortogonais para que

não haja problema de decidibilidade no momento da síndrome. Outra característica importante dos espaços vetoriais de destino é que estes sejam versões não deformadas do espaços vetorial original de codificação, pois os diferentes processos de erros que por sua vez transportam os estados quânticos originais para outras espaços vetoriais devem fazê-lo de modo que seja possível aplicar processos corretivos.

É interessante, no momento de construção dessa estrutura geral de correção de erros quânticos, fazer a menor quantidade de suposições possível, tanto no que concerne à natureza do ruído, quanto no que concernem aos procedimentos necessários para a correção dos efeitos do mesmo, pois desse modo, essa teoria se torna a mais abrangente possível. Por exemplo, duas considerações podem ser realizadas de modo a garantir a generalidade dessa teoria. O processo de ação do ruído pode ser descrito como uma operação quântica E e o processo de recuperação é descrito por outra operação quântica R. Não é necessário supor que o processo de recuperação deva ser realizado em sucessivas etapas, como identificação do erro e aplicação da operação inversa, pois essa operação quântica de recuperação agrupa o efeito de todas as etapas necessárias para que o estado quântico de saída seja o mais próximo possível do original. É necessário, por fim, que todas as operações quânticas descritas preservem o traço.

Assim, para que o processo de correção seja bem sucedido é importante que qualquer estado quântico descrito por $|\psi\rangle$ que pode ser, sem perda de generalidade, descrito por $\rho = |\psi\rangle\langle\psi|$, verifique a seguinte equação:

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

O simbolo $\propto$, significa que o estado quântico resultante do processo de recuperação do código deve ser igual em traço ao estado quântico original e o operador $\circ$ denota a composição de funções.

A partir dessa simples suposição é possível construir condições, nos moldes de equações, que garantam que um determinado código irá corrigir os efeitos nocivos de um determinado erro sobre o estado quântico de informação e também possam ser utilizados na construção de códigos corretores de erros.

Teorema 5.1. *(**Condições para correção quântica de erro**) Seja C um código quântico, e P um projetor sobre C. Seja E uma operação quântica com elementos de operação $\{E_i\}$. Uma condição necessária e suficiente para a existência de uma operação de correção de erro, R, corrigindo E sobre C é que*

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

para alguma matriz hermitiana α de números complexos.

□

Os elementos de operação $\{E_i\}$ do ruído E são chamados de erros, e se existir tal operação R, diz-se que $\{E_i\}$ constitui um conjunto de erros corrigíveis.

A demonstração desse teorema encontra-se em [7].

5.5 Limite Quântico de Hamming

É interessante notar que os códigos quânticos têm certa semelhança com os códigos clássicos. Desta forma, seria possível estabelecer um limitante que pudesse informar da possibilidade de existência de um código. A partir dessa necessidade é construído o limitante quântico de Hamming.

Considere que se possa realizar a codificação de um estado quântico de informação que contêm k *qbits*, para n *qbits*, de tal maneira que essa codificação seja capaz de corrigir erros que afetem quaisquer combinações de t *qbits* ou menos. Considere também que erros que afetem j *qbits* ocorram, em que $j \leq t$. Há um total de $C_{(n,j)}$ possíveis escolhas em que o erro pode interagir (a notação $C_{n,j}$ é usada para identificar as n possíveis combinações j à j). Para cada escolha, existem ainda três tipos de erros diferentes, definidos como as matrizes de Pauli X, Y, Z, que podem afetar cada *qbit*. Isso resulta em um total de 3^j possíveis erros diferentes. Por fim, a quantidade total de possíveis erros que podem ocorrer em t *qbits* ou menos é

$$\sum_{j=0}^{t} C_{(n,j)} 3^j.$$

É interessante realizar uma correspondência direta entre cada erro possível e um padrão de síndrome para que seja possível fazer uma correção eficaz, evitando uma codificação degenerada. Assim, cada erro deve corresponder a um subespaço ortogonal com 2^k dimensões, de modo que cada um desses subespaços ortogonais deve estar contido em um espaço geral de dimensão 2^n dos n qbits, resultando em uma desigualdade

$$\sum_{j=0}^{t} C_{(n,j)} 3^j 2^k \leq 2^n;$$

$$\sum_{j=0}^{t} C_{(n,j)} 3^j \leq 2^{n-k}. \tag{5.20}$$

Esta equação é conhecida como limite quântico de Hamming. A título de verificação, suponha que se realize uma codificação de um estado genérico de um *qbit* para n *qbits* e que qualquer erro, dentre as matrizes de Pauli, seja admitido sobre um *qbit*. Assim o limite de Hamming se verifica pela equação

$$2(1 + 3n) \leq 2^n.$$

Por esta equação é possível constatar que não existe código que realize a transformação de um estado quântico de informação de um *qbit* para n qbits e que seja capaz de aceitar qualquer dos três tipos de erros sobre um qbit, para $n < 4$. A desigualdade só é verificada para valores iguais ou maiores que 5 *qbits*. Porém, um código quântico de 5 *qbits* existe [7]. Vale ressaltar que o limitante quântico de Hamming não garante a existência de um código com as propriedades já descritas, mas garante a inexistência para o caso da não verificação da desigualdade.

Considerando os códigos clássicos, o código de Hamming clássico é um exemplo de código perfeito, no sentido de que este atinge a cota de Hamming clássica em sua igualdade, da mesma forma que o código de cinco *qbits* para a cota de Hamming quântica. Existe um outro importante código

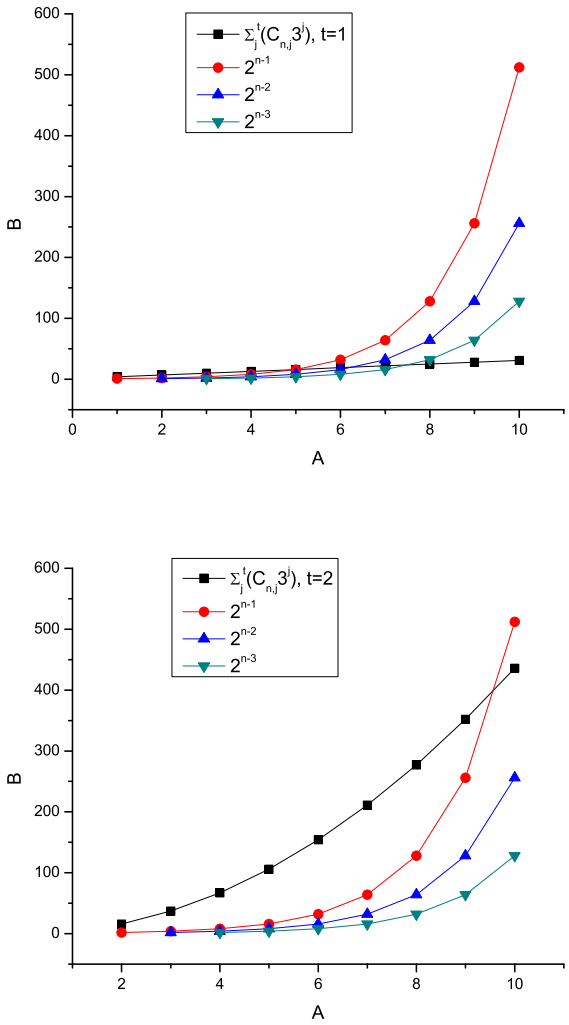


Figura 5.5: Conjunto 1 de gráficos para o limite quântico de Hamming

clássico conhecido como código de Golay [31] que também apresenta a capacidade de atingir a cota de Hamming em sua igualdade, sendo assim tomado como código perfeito. Tendo em mente estes dois códigos clássicos, poderiam ser levantados questionamentos sobre a possibilidade de haver outro código que apresenta a característica de atingir a cota de Hamming quântica em sua igualdade, semelhante ao código de Golay. Alguns gráficos foram construídos no sentido de investigar se o limite quântico de Hamming poderia expressar os parâmetros de algum código quântico que pudesse atingi-lo em sua igualdade.

A seguir, nas figuras 5.5 à 5.8,estão expressos os gráficos de ambos os lados da inequação (5.20). As investigações levam a conjecturar a inexistência de outro código quântico que verificando a inequação (5.20) em sua igualdade seja considerado perfeito. Pela semelhança das estruturas que constroem as cotas de Hamming clássica e quântica e tendo em vista que códigos clássicos perfeitos são raros era de se esperar a apresentação dessa conjectura.

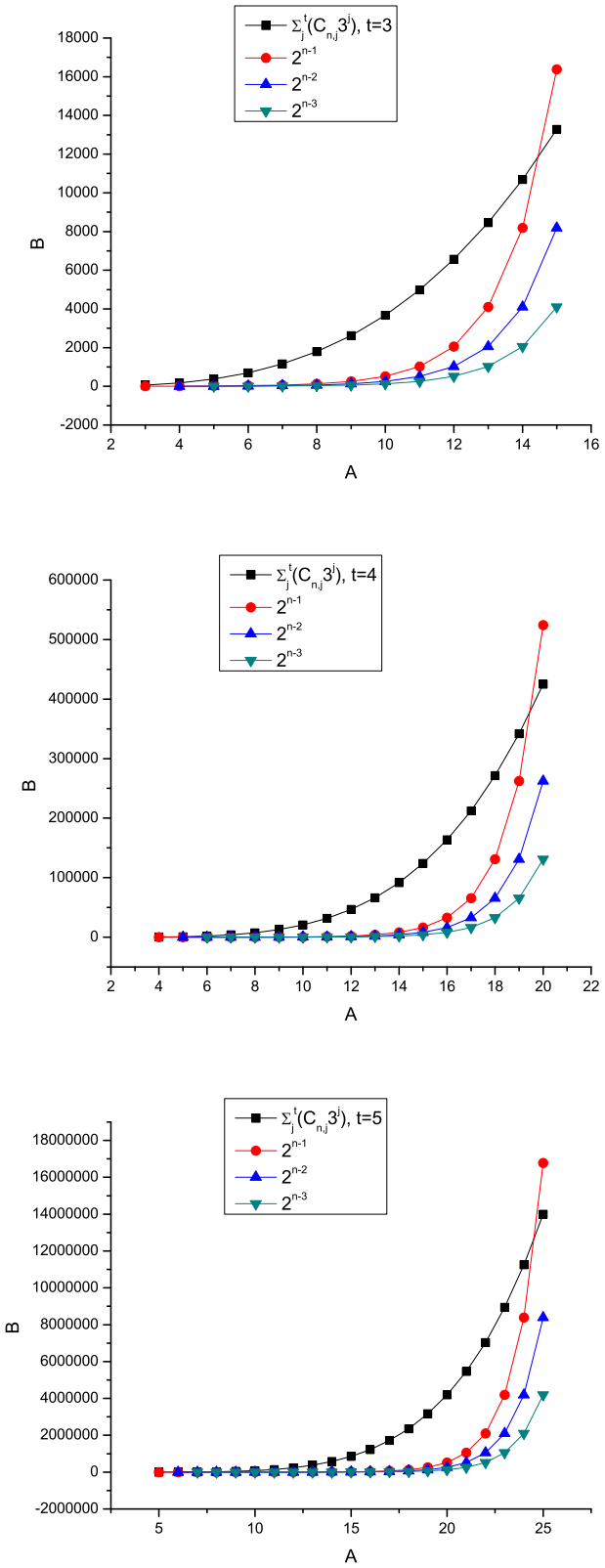


Figura 5.6: Conjunto 2 de gráficos para o limite quântico de Hamming

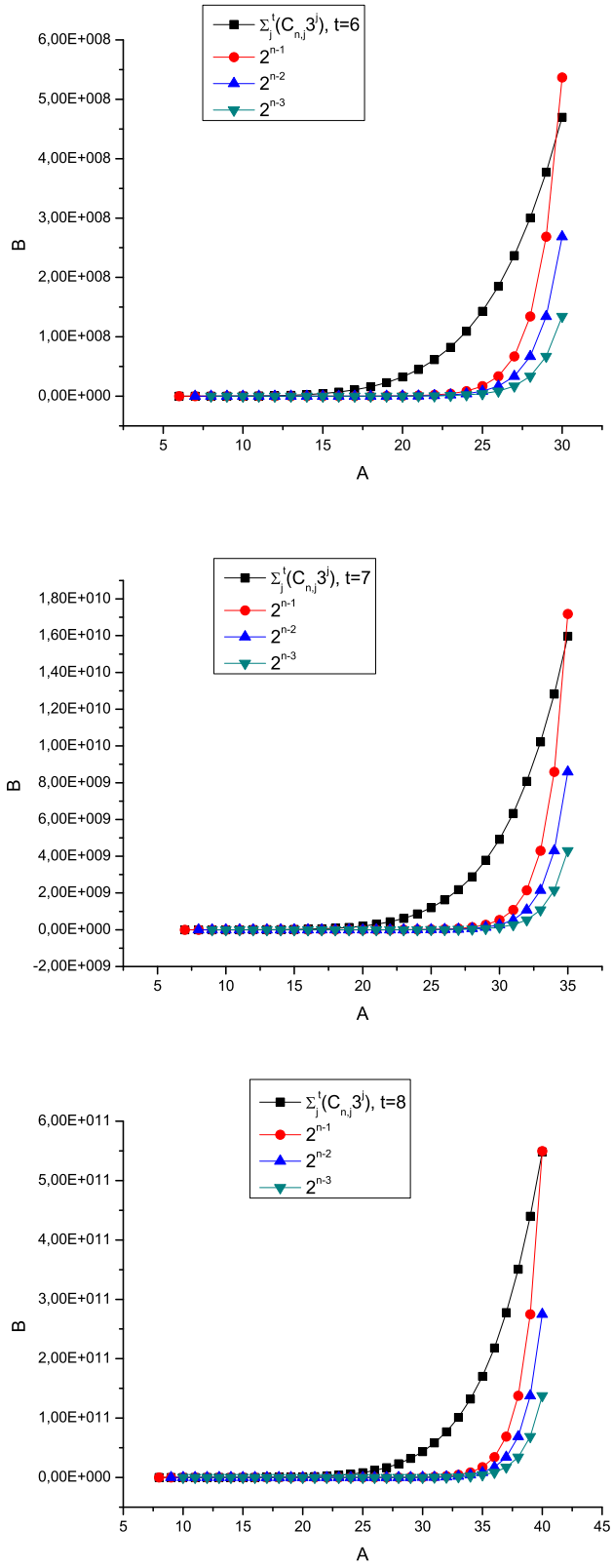


Figura 5.7: Conjunto 3 de gráficos para o limite quântico de Hamming

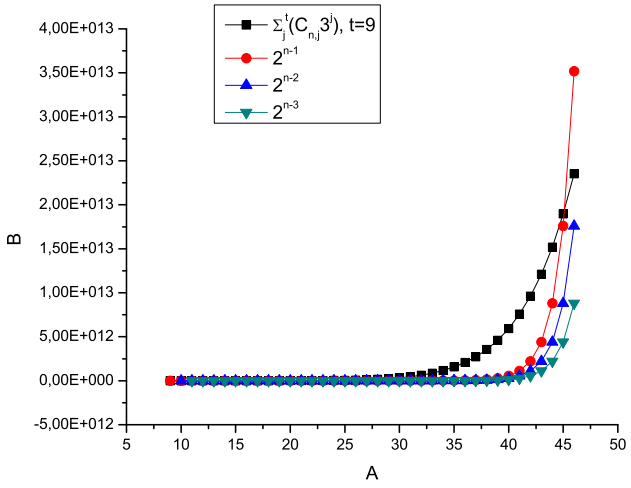


Figura 5.8: Conjunto 4 de gráficos para o limite quântico de Hamming

Nos gráficos apresentados nas figuras 5.5 à 5.8, os pontos de cor preta representam o lado esquerdo da inequação (5.20), para diversos valores de n. Os demais pontos dos gráficos representam o lado direito da inequação, para diversos valores de n. Para que a inequação seja obedecida, a curva com pontos pretos deve estar abaixo das demais curvas.

5.6 Códigos Lineares Clássicos

Apesar de até aqui já ser possível verificar a possibilidade de correção dada uma estrutura de codificação e também verificar a possibilidade de existência de um código não-degenerado, não existem, no entanto, numerosos exemplos de códigos corretores de erros quânticos que possam *ajudar* no perfeito entendimento dessa ferramenta.

Na tentativa de superar essa dificuldade, uma alternativa seria tomar como base os códigos clássicos, no intuito de que algumas características destes pudessem, após adaptações, serem reproduzidas na construção de códigos quânticos.

Um código clássico é um estrutura matemática linear que faz uma relação unívoca entre uma matriz linha de dimensão k, conhecida como informação ou mensagem, e uma outra matriz linha de dimensão n, conhecida como palavra-código, esta relação é conhecida como codificação. A função ou matriz que faz esta ligação entre a informação e a palavra-código é conhecida como matriz geradora do código, representada por G.

Assim, uma mensagem "u"com k bits de informação é mapeada na palavra-código "v"com n bits, tal que $v = uG$. Neste processo de codificação existe a inserção de $n - k$ bits de paridade que têm a função de verificar a autenticidade dos bits que fazem parte da mensagem. Todos os elementos desse conjunto de operações atuam sobre o corpo Z_2, tanto os elementos que compõem a mensagem, quanto os elementos que compõem a palavra-código (em que $Z_2 = \{0, 1; +_2\}$ com $+_2$ representa a adição módulo 2). Uma estrutura matemática que apresenta essas característica é conhecida como código

clássico e denotada por $C(n, k)$.

Um exemplo simples que já foi mencionado anteriormente foi o código de repetição. Este código faz a correspondência de uma mensagem, ou vetor de informação, que contém apenas um único bit de para uma palavra-código de n bits, para simplicidade de exemplificação serão inseridos 4 bits de paridade idênticos ao bit de mensagem, isso corresponde a uma matriz geradora da forma:

$$G = [11111].$$

Desta forma, uma mensagem do tipo $u = [0]$ será univocamente mapeada para apresentar-se como $v = [00000]$, identicamente, uma mensagem do tipo $u = [1]$ é univocamente mapeada para apresentar-se como $v = [11111]$; denota-se este código por $C(5, 1)$. Existe uma medida de informação que proporciona saber o quanto cada mensagem, quando recebida, informa ao seu destinatário, em outras palavras, quanto cada palavra-código carrega de informação. Essa medida é conhecida como taxa do código:

$$R = k/n.$$

Aplicando-se esse último conceito ao código de repetição, mencionado anteriormente, pode-se constatar que o poder informativo de cada palavra-código é pequeno, $R = 1/5$. Isso ocorre porque a quantidade de bits inseridos à mensagem, ou vetor de informação, é quatro vezes maior que a quantidade de bits do vetor de informação (ou no caso genérico para o código de repetição, $n - 1$ vezes maior). Além de que, quando a proporção entre os bits da palavra-código e os bits do vetor de informação é grande, pode-se constatar que a codificação foi projetada a apresentar relevante robustez na detecção/correção de erros. Esse código de repetição é um código interessante para aplicações em que se tenha a necessidade de grande proteção à mensagem, em contra partida deve-se aceitar uma pequena "taxa de informação"por palavra-código. Exemplos desse tipo de aplicação são movimentações financeiras, trocas de informações relativas as senhas de cartões, etc.

No outro extremo, ainda se referindo a taxa do código, pode-se mencionar o código conhecido como *single parity check* ou código de um único digito de paridade. A tarefa de codificação dessa estrutura é fazer uma adição binária entre todos os bits de informação da mensagem e incluir o resultado como o último bit, formando assim a palavra-código. Desta forma, uma mensagem do tipo $u = [1101]$ é mapeada em uma palavra-código $v = [11011]$, igualmente, uma mensagem do tipo $u = [1111]$ é mapeada na palavra-código $v = [11110]$; esse código é denotado por $C(k+1, k)$ e sua taxa é calculada como $R = k/(k+1)$. Vê-se que o poder informativo de cada palavra-código para esse tipo de codificação é grande, bem diferente do caso anteriormente apresentado para o código de repetição, aproximando-se no limite para 1 à medida que se cresce a quantidade de bits do vetor de informação. Contudo, a alta taxa do código carrega a em si a noção de que a codificação não apresenta grande robustez quanto a proteção da informação, neste caso sendo necessário unicamente a inversão de de bits em um número par de posições da palavra-código para que não seja possível detectar a ocorrência de qualquer erro.

A matriz geradora do código de um único dígito de paridade é

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

O processo de mapeamento através da multiplicação da mensagem pela matriz geradora torna a conexão entre as duas partes da codificação bastante transparente. Deseja-se também que essa transparência seja notada no processo de decodificação. Igualmente ao processo de codificação - em que foi utilizada uma matriz para realizar o mapeamento da mensagem para a palavra-código - o processo de decodificação irá utilizar uma matriz conhecida como matriz de paridade, denotada por $H_{n-k\ x\ n}$. Essa matriz de paridade, $H_{n-k\ x\ n}$, apresenta a característica de que a sua multiplicação por toda e qualquer palavra-código v_i, em que $0 \leq i \leq k$, deve ter como resultado o vetor nulo:

$$v_i H^T = [000\cdots 0]_{1x n-k};\ \forall\ i\ \in\ \{0, 1, 2, \cdots, k-1\}.$$

Tomando-se todas as palavras-código para um código genérico $C(n, k)$, ou seja, um código que transforma vetores de informação u_{1k} em vetores $v_{1_x n}$, é possível achar um conjunto específico de vetores que formam todas as palavras-código do código. Esse conjunto de vetores é chamado de conjunto gerador do código. Esse conjunto pode ser tomando como os vetores-linha da matriz geradora do código, quando na sua forma padrão. Outra maneira de definir o código $C(n, k$ é através da matriz de paridade. Já foi mostrado anteriormente que qualquer palavra-código v_i obedece a relação $v_i H^T = [0]$. Por conseguinte, tomamos o código como o *kernel* de H.

A equação a seguir evidência o enunciado precedente, para o caso do código de repetição com $k = 1$:

$$GH^T = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}_{k_x(n-k)}$$

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}_{1_x n} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}_{(n)_x(n-1)} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}_{1_x(n-1)}.$$

A estrutura dos códigos clássicos apresenta robustez quanto a sua estrutura matemática, de modo que é possível encontrar uma das matrizes mencionadas, G ou H, dada a outra matriz. Isso significa que, é possível encontrar a matriz H dada a matriz G ou é possível encontrar a matriz G dada a matriz H. No entanto, para que isso possa ser realizado facilmente é necessário expressar as matrizes de uma maneira específica, conhecidas como forma padrão:

$$G = [I_k | P]; \tag{5.21}$$

$$H = \left[-P^T | I_{n-k}\right]. \tag{5.22}$$

Seguem as matrizes de verificação de paridade do código de repetição de um dígito e do código de único dígito de paridade, respectivamente (as matrizes geradoras desses códigos já foram mostradas anteriormente):

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

$$H = [1111 \cdots 1].$$

O procedimento de decodificação se utiliza de uma propriedade já mencionada. O fato de que o código pode ser visto como o kernel da matriz de paridade transposta é usado para esse fim. A equação (5.23) representa essa particularidade, conhecida como equação de síndrome do código. A sua interpretação mais direta é que toda palavra-código deve ter como resultado da equação de síndrome, valor nulo. Em contra partida, caso a síndrome não tenha valor nulo, o vetor v não é uma palavra-código. É dessa forma que é feito o processo de detecção de erro. Aplicando ao vetor recebido a equação (5.23), testa-se o valor resultante. Caso seja nulo, decide-se que não houve erro no processo de transporte da palavra-código, caso contrário, o valor resultante sendo diferente de zero, decide-se que houve erro.

$$vH^T = S; \text{ em que } S \text{ é a síndrome e } v \text{ é o vetor recebido.} \tag{5.23}$$

Pode-se separar em dois grupos os efeitos da interação de um erro genérico sobre a palavra-código. Um efeito é a modificação da palavra-código para um vetor cuja síndrome não tem valor nulo. Esse efeito pode ser detectado pelo processo de decodificação. O outro efeito é a modificação da palavra-código para um outro vetor cuja síndrome tem valor nulo. Esse último efeito ocorre sempre que o erro é também uma palavra-código, não sendo possível detectar o erro.

Através de um estudo detalhado do padrão de erros que ocorrem em um canal específico, constrói-se o código de modo a minimizar os efeitos do segundo grupo. Esse estudo detalhado do canal de comunicação também pode proporcionar a estruturação de uma tabela de padrões de síndromes diretamente ligados aos erros que o originam.

Para evitar a ocorrência, com alta probabilidade, de erros que sejam palavras-código, deve-se construir o código de modo que exista o máximo possível de espalhamento entre os seus constituintes. A distância entre os elementos do código, ou seja, entre as palavras-código é calculada por uma métrica conhecida como a distância de Hamming. A distância de Hamming mínima é definida como a menor distância entre duas palavras-código, a menos do vetor nulo; a expressão da distância de Hamming está exposta em (5.24), em que C é o código.

$$d_C \equiv min_{x,y \in\ C, x \neq y}\ d(x, y). \tag{5.24}$$

O cálculo dessa medida seria algo bastante trabalhoso a depender da dimensão do código, no entanto, pode se tomar como apoio uma importante característica dessa estrutura e adaptar a equação (5.24) para que por meio dessa propriedade possa ser calculada de forma menos árdua. É conhecido

que os códigos corretores de erros a que se refere neste texto apresentam, pela definição, a propriedade da linearidade e do fechamento. A operação de adição módulo 2 realizada entre duas palavras-código deve resultar em uma outra palavra-código, pela propriedade do fechamento. Isso significa que a distância de Hamming entre duas palavras-código quaisquer pode ser vista como o peso de Hamming, equação (5.25), da palavra-código resultante como adição módulo 2 das duas palavras-código em questão. Isso é interessante, pois, para se conhecer a distância de um código é necessário somente calcular o peso de Hamming da palavra que possui o menor peso de Hamming.

$$d_C = min_{x \in C, x \neq 0} wt(x). \tag{5.25}$$

Assim aquele código que apresenta a máxima distância mínima e alta taxa pode ser considerado um bom código. De posse desses novos parâmetros que servem como critério de avaliação entre os códigos, pode-se definir uma nomenclatura convencional para rápida avaliação do código. Denota-se um código corretor de erro genérico como $C(n, k, d)$, em que n é a quantidade total de bits da palavra-código, k é a quantidade de bits de informação oriundos da mensagem e d é a distância mínima de Hamming. É possível expressar a capacidade de correção de erros do código através da distância mínima:

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor ; \text{em que } t \text{ representa a capacidade de correção de erro do código.}$$

Tendo em vista que a distância mínima de Hamming tem a competência de informar a capacidade de correção e detecção de erros do código, seria um interessante alvo de exploração qual a sua limitação em função da dos parâmetros do código.Como já foi mencionado anteriormente, uma definição alternativa para o código é que este é o kernel da matriz de paridade. Sem perda de generalidade, o código é também um espaço vetorial fechado, em relação a operação de adição módulo 2. Existe uma operação bem comum em álgebra linear conhecida como posto de uma matriz. Existem dois tipos de posto: o posto-linha e o posto-coluna. O posto-linha de uma matriz identificará a quantidade de linhas linearmente independentes do conjunto total de linhas da matriz e o posto-coluna identificará as colunas linearmente independentes. É possível calcular a distância de Hamming através do posto-coluna da matriz H do código. É possível extrair um importante limitante da matriz H em relação ao seu posto-linha e o posto-coluna: este limitante é conhecido como cota de Singleton [32],

$$d \leq n - k + 1.$$

Um bom exemplo, não trivial, de códigos corretores de erros é o código de Hamming. Os códigos de Hamming são códigos interessantes, pois tem a capacidade de correção de erros que atuem na inversão de 1 bit e detecção de erros que atuem na inversão de 2 bits.conseguem corrigir 1 erro por bit ou detectar 2 erros em bits diferentes. O código de Hamming mais simples é o $C(7, 4, 3)$, em que suas matrizes geradora e de paridade estão expostas nas expressões (5.26) e (5.27),

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \tag{5.26}$$

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{5.27}$$

O código de Hamming pode ser estendido para vários comprimento de modo que a sua expressão geral é dada por $C(n = 2^r - 1, k = n - r, 3)$, em que r é um número inteiro qualquer maior que dois.

Por fim é importante mencionar o que vem a ser código dual. Suponha que a partir de um dado código $C(n, k)$, seja possível construir outro código utilizando para matriz geradora do segundo a matriz de paridade do primeiro. Qualquer código construído dessa forma é conhecido como dual do código $C(n, k)$ e pode ser denotado por $C(n, n - k)$ ou $C(n, k)^{\perp}$.

É importante verificar que o espaço gerado pelas palavras-código do código dual é ortogonal ao código original. Existem ainda alguns códigos que apresentam a interessante característica de serem autoduais, ou seja, o espaço vetorial das palavras-código é ortogonal em relação a si mesmo. É essa importante estrutura que irá dar embasamento matemático a uma outra classe de códigos quânticos, os códigos conhecidos como CSS [7].

A título de exemplo, expõem-se o código dual do código de Hamming $C(7, 4, 3)$ através das matrizes G e H, conhecido como código simplex [31],

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \tag{5.28}$$

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{5.29}$$

Para uma abordagem mais completa sobre os códigos clássicos existem livros textos de autores consagrados nesta área do conhecimento [32] [31].

5.7 Códigos de Calderbank-Shor-Steane

Após uma breve incursão na teoria dos códigos clássicos já é possível iniciar algumas análises aprofundadas com o objetivo analítico da construção de alguns códigos quânticos. Realizando uma comparação entre o código quântico de repetição para proteção de inversão de bit e o código de repetição clássico, é possível identificar que as palavras-código do caso clássico são os rótulos para o código quântico em questão. Nomeia-se rótulo de um estado quântico a representação binária contida na simbologia de Dirac, $|\ \rangle$.

Assim, o mapeamento realizado pelo código de repetição quântico faz com que os rótulos da base binária, utilizada na representação do estado genérico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, sejam modificados para uma nova representação, em que essa nova representação é idêntica as palavras-código do código de repetição clássico; esse procedimento esta esquematizado pelas equações a seguir,

$$|u = 0\rangle \rightarrow |v = 000\rangle,$$

$$|u = 1\rangle \rightarrow |v = 111\rangle.$$

Esse fato é interessante, pois o erro de inversão de bit, para o caso quântico, pode ser encarado como um simples erro de inversão de bit, para o caso clássico, que ocorre num canal de comunicação comum. No que se refere aos rótulos dos estados quânticos, as equações a seguir podem esclarecer a abordagem descrita.

$$e = [010] + v = [111] \rightarrow r = [101] \rightleftharpoons X_2|111\rangle = |101\rangle, \tag{5.30}$$

$$e = [100] + v = [000] \rightarrow r = [100] \rightleftharpoons X_1|000\rangle = |100\rangle. \tag{5.31}$$

Em (5.30) e (5.31) evidência-se que os erros clássicos $e = [010]$ e $e = [100]$ tem equivalência com os erros quânticos de inversão de bit X_2 e X_1, respectivamente, pela comparação do vetor resultado com os rótulos dos estados quânticos resultantes.

Desta forma pode-se encarar os operadores lineares de inversão de bit, em sua forma extensa, como possuindo uma representação binária, na forma de vetor-linha, em que, nas posições em que se encontra a matriz de identidade, coloca-se no vetor-linha o bit zero e nas posições em que se encontra a matriz de inversão de bit, coloca-se o bit um. Isso pode ser inferido, pois a ação de inversão de bit no caso clássico é realizada quando à palavra-código é somada um vetor-linha. As equações a seguir abordam a explicação apresentada acima,

$$e = [010] \rightleftharpoons E = IXI,$$

$$e = [100] \rightleftharpoons E = XII.$$

Então é possível que qualquer código clássico possa ser transportado para apresentar uma aplicação quanto aos códigos quânticos, no que se refere a erros de inversão de bit, já que não existe paralelo clássico para erros de inversão de fase. Isso se torna interessante, pois a capacidade de correção do código clássico é transportada também para o código quântico, no que se refere a erros de inversão de bit.

Este idéia foi inicialmente proposta por Calderbank, Shor e Steane e conhecido atualmente como códigos CSS [7]. Esses pesquisadores formularam essa idéia embasadados nas explicações apresentadas até o momento, adicionada a idéia de ortogonalidade entre espaços vetoriais que contém as palavras-código.

Sejam C_1 e C_2 códigos clássicos lineares $C_1(n_1, k_1)$ e $C_2(n_2, k_2)$, tais que $C_2 \subset C_1$ e C_1 e $C_2^{\perp}$,em que ambos corrigem t erros. Constroi-se um código quântico CSS(C_1,C_2),$[n, k_1 - k_2]$ (Denota-se código CSS de C_1 sobre C_2) , capaz de corrigir erros em t *qbits*, através das seguintes definições. Considere v uma palavra-código de C_1, e defina-se o estado quântico $|v + C_2\rangle$ como:

$$|v + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |v \oplus y\rangle, \tag{5.32}$$

em que " $\oplus$ " indica a adição módulo 2.

Toda a teoria de códigos CSS é baseada em classes laterais [32]. Suponha que exista um elemento v_1 pertencente à C_1, tal que $v - v_1$ pertence à C_2. O estado quântico $|v_1 + C_2$ é o mesmo que o estado $|v + C_2$ (equação 5.33),

$$|v + C_2\rangle = |v + v - v_1 + C_2\rangle = |v_1 + C_2\rangle. \tag{5.33}$$

Isso evidência o fato que o estado padrão de codificação depende unicamente da classe lateral de C_1/C_2 em que v pertence, formando assim um conjunto fechado. Assim o código quântico CSS(C_1,C_2) é definido como o espaço vetorial formado pelos estados codificados $|v + C_2\rangle$, em que v pertence a C_1. É interessante que a quantidade de estados que podem ser codificados dessa maneira é relacionado diretamente à quantidade de classes laterais de C_2 em C_1; como a dimensão de C_1 é k_1 e a dimensão de C_2 é k_2, então a quantidade de estado codificados é $2^{k_1-k_2}$.

É interessante notar que esse tipo de construção, além de proteger o estado quântico de informação contra erros de inversão de bit, também é capaz de proteger o mesmo quanto a erros de inversão de fase. Para este código é garantido que a sua capacidade de correção seja t, para erros de inversão de bit ou erros de inversão de fase.

Considere que um operador linear, que em sua forma extensa, apresente e_1 matrizes de Pauli do tipo X distribuídas em n posições. Para este operador de inversão de bit é interessante representá-lo na forma de vetor-linha com zero nas posições em que se encontram as identidades e um nas posições em que se encontram as matrizes de Pauli. Considere também que outro operador linear, responsável pelo erro de inversão de fase, seja posto a interagir com o estado quântico codificado, da mesma forma que o operador de inversão de bit, e que e_2 matrizes de Pauli do tipo Z sejam distribuídas em n posições. Para este operador de inversão de fase é interessante também expressá-lo na forma de vetor-linha igualmente ao operador anterior. Suponha que o estado quântico codificado alvo desses erros seja $|v + C_2\rangle$ que após a ação dos operadores resulta em

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

É comum em certas situações de correção quântica de erros introduzir sistemas de teste para que seja possível projetar sobre este sistema informações que, para sua obtenção, seria necessário realizar medições resultando em dano à informação portada pelo estado quântico. Assim, introduz-se no estado corrompido um sistema quântico com uma quantidade de *qbits* suficientes para que sobre este sistema introduzido seja armazenado a síndrome de erro para o código C_1.

Para a introdução desse sistema quântico faz-se uso da computação reversível para que possa ser possível aplicar a matriz de paridade ao rótulo do estado codificado corrompido. Vale ressaltar que todos os estados são inicializados pelo estado padrão da base computacional $|0$; esse procedimento transforma o estado $|v + w + e_1\rangle|0\rangle$ para $|v + w + e_1\rangle|0\rangle|(v + w + e_1)H_1^T\rangle = |v + w + e_1\rangle|e_1 H_1^T\rangle$. Assim o resultado dessa operação é

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(v+y)\cdot e_2} |v + y + e_1\rangle|e_1 H_1^T\rangle.$$

O erro de inversão de bit pode ser detectado realizando uma medida sobre o sistema quântico introduzido, já que neste sistema está contido o padrão de síndrome do erro que afetou o estado codi-

ficado. Ao se realizar uma medição sobre o sistema quântico auxiliar não existe efeito de modificação do estado quântico principal o que permanece intacto

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

Para que se possa corrigir o erro introduzido pelo operador de inversão de bit o procedimento é utilizar portas NÃO nas posições em que o erro interagir, já que pelo padrão de síndrome se infere o possível erro. Essa operação resulta no estado

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(v+y)\cdot e_2} |v + y\rangle.$$

Até este instante foram corrigidos os erros de inversão de bit. Para a correção de erros de inversão de fase é requerido uma mudança de base computacional para a base de Hadamard. Aplica-se a cada *qbit* do estado codificado corrompido uma porta de Hadamard para que essa mudança de base seja efetuada, e o estado quântico resultante é

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z} \sum_{y \in C_2} (-1)^{(v+y)\cdot(e_2+z)} |z\rangle.$$

O somatório introduzido é realizado sobre todos os valores de z, em que z representa uma $n-upla$ binária. O próximo passo na resolução do problema é uma mudança de variável, em que $z^{'} = z + e_2$. Assim, o estado quântico pode ser reescrito como:

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

Considerando que z' pertence ao espaço vetorial ortogonal à C_2 é possível ver que $\sum_{w \in C_2} (-1)^{w.z'} = |C_2|$, caso contrário se essa suposição não pode ser realizada então $\sum_{w \in C_2} (-1)^{w.z'} = 0$. Assim, o estado quântico pode novamente, ser reescrito como

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

O interessante de se realizar a mudança de base para uma base mais apropriada é que os erros de inversão de fase transformam-se em erros de inversão de bit para essa base. Novamente introduz-se um sistema quântico auxiliar para que esse possa receber o padrão de síndrome para o erro de inversão de fase, encarado aqui como erro de inversão de bit. Vale ressaltar que a matriz de verificação de paridade nos dois momentos de detecção de erros são diferentes: para a detecção de erros de fase é usada a matriz H_2.

No entanto, a recuperação do estado original é realizada da mesma maneira. A partir do momento em que se conhece o padrão de síndrome correspondente ao erro e_2, aplica-se portas NÃO para inverter os *qbits* danificados de forma que o estado quântico resultante do processo de desinversão é

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

Como última etapa do processo de correção de erro, aplicam-se portas Hadamard em todos os *qbits* para que se retorne ao estado quântico original

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |v + y\rangle.$$

Em suma, alguns comentários podem ser tecidos quanto ao que foi apresentado neste texto sobre os códigos CSS. Os códigos CSS são códigos quânticos construídos a partir de códigos clássicos C_1 e C_2, os quais devem apresentar certas características a saber, $C_2 \subset C_1$ e tanto C_1 quanto $C_2^{\perp}$ devem corrigir t erros. Com essas propriedades sendo obedecidas é garantido que o código quântico CSS(C_1,C_2)$[n, k_1 - k_2]$ também corrija t erros arbitrários.

É salutar neste momento introduzir alguns exemplos de código CSS que utilizem-se de códigos clássicos bastante conhecidos na literatura apropriada. Um exemplo interessante é conhecido como código quântico de Steane; esse código é construído tomando-se como base o código de Hamming $C(7, 4, 3)$, cuja matriz de verificação está exposta na expressão (5.27):

Para saber se é possível utilizar o código de Hamming $C(7, 4, 3)$ para a construção de um código CSS é necessário saber se este código clássico apresenta as características necessárias para isso. Assim, considere que esse código clássico seja nomeado por C_1 e o seu código dual, o código simplex seja nomeado por C_2. Em primeira instância, deseja-se ter conhecimento se o código simplex é um subconjunto do código de Hamming. Essa informação pode ser alcançada por uma análise das matrizes de paridade e geradora dos códigos. É interessante notar que como esses códigos são duais entre si, ou seja, a matriz de paridade de um é justamente a matriz geradora do outro e vice-versa.

Analisando essas matrizes fica claro que o espaço vetorial gerado pelas linhas, conhecido como espaço-linha, de H de C_2 contém estritamente o espaço-linha a partir de H de C_1, e sabendo que os códigos podem, como definição alternativa, serem considerados os *kernel's* do mapeamento $S = vH^T$ para H de C_2 e de H de C_1,é garantido afirmar que $C_2 \subset C_1$. A segunda propriedade esta relacionada à capacidade dos códigos; deseja-se que C_1 e $C_2^{\perp}$ corrijam ambos t erros. O que ocorre é que $C_2^{\perp} = (C_1^{\perp})^{\perp} = C_1$; essa propriedade está também garantida.

Assim, esse código quântico CSS, gerado a partir do código clássico de Hamming, tem capacidade de corrigir um erro arbitrário, pois carrega consigo a capacidade do código clássico. E que pode codificar até dois estados da base para o estado quântico de informação, já que o código C_1 é descrito por apresentar dimensão quatro e o código dual tem dimensão três, fatos que resultam em que o código quântico tem dimensão um e comprimento sete. Para que se faça a codificação é necessária a lista de todas as palavras-código que pertencem a C_2, o que é realizado a partir da matriz 5.27. Uma possível codificação é mostrada

$$\begin{aligned} |0_C\rangle &= \frac{1}{\sqrt{8}} [|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &\quad + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle], \end{aligned} \tag{5.34}$$

$$\begin{aligned} |1_C\rangle &= \frac{1}{\sqrt{8}} [|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &\quad + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle]. \end{aligned} \tag{5.35}$$

O estado codificado (5.35) indica um aspecto importante dessa codificação, para que esta seja considerada eficiente é necessário encontrar uma palavra-código de C_1 que não esteja em C_2, caso contrário a codificação representará o mesmo elemento quântico.

Uma possibilidade de codificação quântica pode ser pensada nos mesmo moldes do código de inversão de bit. Suponha que se tenha um estado quântico cuja dimensão é três, uma codificação possível seria tomar cada estado quântico da base e transformá-lo conforme o código simplex,

$$\begin{aligned} |\psi_C\rangle &= \alpha_0|0000000\rangle + \alpha_1|1101001\rangle + \alpha_2|1011010\rangle + \alpha_3|0110011\rangle \\ &\quad +\alpha_4|0111100\rangle + \alpha_5|1010101\rangle + \alpha_6|1100110\rangle + \alpha_7|0001111\rangle. \end{aligned} \tag{5.36}$$

Esse tipo de codificação é interessante para uma aplicação em que o canal de comunicação só apresenta erros de inversão de bit e não erros de inversão de fase, pois para esse caso o código construído dessa maneira não é capaz de corrigir.

Analisando este código pelos parâmetros dos códigos CSS é possível verificar porque esse tipo de construção não possibilita a correção de erros de fase. Suponha que o código simplex, dual do código de Hamming $C(7,4,3)$, seja utilizado como o código C_1. Para que seja possível resultar nessa construção, através dos códigos CSS, é necessário escolher o código C_2 de maneira tal que a dimensão do código quântico seja idêntica à do código simplex clássico. Isso parece um pouco estranho já que, pela teoria de classes laterais [32], a dimensão do código quântico é calculada como a diferença entre as dimensões dos códigos C_1 e C_2.

Assim, para que o código quântico apresente a mesma dimensão do código C_1 é necessário que o código C_2 tenha dimensão nula. Uma das propriedades dos códigos CSS é que o código C_2 deve estar contido no código C_1. Então todos esses fatos só podem ocorrer se o espaço vetorial formado pelas palavras-código do código C_2, que deve estar contido em C_1, tiver em si somente a palavra-código nula.

Mas existe outra propriedade fundamental dos códigos CSS que possibilita resolver o problema da correção de erros de fase. É necessário também que a capacidade dos códigos C_1 e $C_2^{\perp}$ seja, para ambos, t, ou seja ambos os códigos devem corrigir t erros clássicos. Isso é de extrema importância, pois no processo de decodificação descrito anteriormente foi necessário a utilização das matrizes verificadoras de paridade para ambos os códigos C_1 e $C_2^{\perp}$. A matriz de verificação de paridade para o código C_1 foi utilizada para a correção dos erros de inversão de bit. A matriz verificadora de paridade do código $C_2^{\perp}$ foi utilizada para calcular a síndrome dos erros de fase que, após a mudança de base, foram transformados em erros de inversão de bit.

A capacidade de correção do código simplex, com parâmetro de comprimento sete e dimensão três, pode ser calculada através da distância de Hamming, que para esse código é quatro, resultando numa correção de um erro de inversão clássica. No entanto, para o código $C_2^{\perp}$ encontra-se um problema, pois como C_2 tem dimensão nula, a capacidade de correção pra $C_2^{\perp}$ é nula; o processo de decodificação por síndrome não é capaz de corrigir nenhum erro de inversão clássica.

Desta forma, um código construído como foi descrito, apresenta uma capacidade de correção de erros de inversão de bit equivalente ao seu "primo"clássico, no entanto não é capaz de corrigir nenhum erro de inversão de fase tendo em vista que a dimensão nula acarreta na capacidade de correção nula pra $C_2^{\perp}$.

Uma maneira de tentar reparar o fato de que os erros de fase, para esse tipo de codificação, não são corrigidos, é realizar outro tipo de codificação. Esse tipo de codificação direta levará sempre à correção de erros de inversão de bit, mas também à não correção dos erros de inversão de fase.

Uma possível codificação a ser realizada é utilizar as palavras-código do código simplex. Elas seriam usadas como rótulos dos estados da base do estado quântico codificado, no entanto, não realizando essa codificação de maneira direta. A idéia é utilizar o código simplex como o código C_1. Um estudo dos possíveis erros de fase que ocorrem no canal de comunicação conduziria a uma escolha apropriada para o espaço vetorial que contém as palavras-código para C_2.

Suponha que um estudo do canal de comunicação quântico, o qual deverá transportar o estado quântico de informação, indicou que os possíveis erros de fase que poderiam afetar qualquer estado quântico em trânsito no mesmo são descritos pelo conjunto

$$EF_i = \{Z_2, Z_3, Z_4, Z_5\}.$$

Desta maneira, é possível escolher um código C_2, de modo que o código dual de C_2 tenha a capacidade de corrigir erros de inversão de bits normais nas posições. E que tenha a mesma capacidade de correção do código simplex, que por ocasião do texto será considerado o código simplex $C(7, 3, 4)$, apresentando $d_{mn} = 4$ com consequente capacidade de correção de 1 erro e detecção de 3 erros. Assim, uma escolha para o código C_2,no intuito de conseguir detectar esses erros de fase é

$$C_2 = \{(0000000); (0111100)\}.$$

A partir de então é possível realizar uma codificação eficiente de modo que todos os erros de inversão de bit sejam corrigidos e os erros de inversão de fase, contidos em EF_i obtidos pelo estudo do canal, também sejam corrigidos. A seguir têm-se o estado quântico codificado

$$\begin{aligned} |\psi_C\rangle &= \alpha_0(|0000000\rangle + |0111100\rangle) + \alpha_1(|0110011\rangle + |0001111\rangle) \\ &\quad +\alpha_2(|1010101\rangle + |1101001\rangle) + \alpha_3(|1011010\rangle + |1100110\rangle). \end{aligned} \tag{5.37}$$

É interessante notar o fato de que a medida que mais erros são constatados e por conseguinte o código deve ser modificado para que tenha a capacidade de corrigir esses erros, a quantidade de informação quântica diminui. No caso do código de Steane, a informação quântica é a mínima possível, tendo em vista que esta é os números complexos que ponderam a combinação linear dos estados da base e que deve ser protegida indiretamente pela codificação usada, já que a dimensão do código de Steane é um.

No caso da codificação direta apresentada em seguida ao código de Steane, a quantidade de informação quântica que deve ser transportada até o destinatário é máxima, já que a dimensão do código quântico é idêntica à dimensão do código clássico. Porém, a capacidade de correção de erros é severamente restringida. Para esse tipo de codificação são somente encarados como possíveis erros os erros de inversão de bit.

Em resumo, o caso da escolha da codificação quântica, como no caso clássico, recai sobre o ajuste fino entre a taxa do código e a capacidade de correção do mesmo. O aumento da redundância

pode conduzir a uma redução da taxa de transmissão de informação a cada vez que uma palavra de informação é codificada.

No caso apresentado, tanto para os códigos CSS, quanto para os outros tipos de codificação, a redundância dos estados quânticos é a dimensão da classe lateral que pode ser calculada como a diferença entre as dimensões dos códigos C_1 e C_2.

É possível ainda realizar uma extensão dos conceitos apresentados até aqui. É certo o fato de que todos os códigos mostrados como exemplos estão todos embasados sobre um corpo finito $GF(2)$, para mais detalhes sobre a estrutura de corpos finitos vide [31]. Mas também é certo o fato de que se for possível transpor os conceitos de códigos clássicos para os códigos quânticos para o caso binário, também deve ser possível realizar essa passagem de informação para códigos clássicos p-ários.

Inicialmente é necessário entender como seria o ruído que possivelmente poderia interagir com os estados quânticos de informação em trânsito pelo canal de comunicação. Anteriormente, uma abordagem foi realizada em relação aos operadores lineares; esses operadores lineares poderiam apresentar uma representação equivalente no espaço vetorial dos vetores-linha. Como foi apresentada, a equi-valência seria feita, através da representação extensa do operador (inversão de 2nd *qbit* X_2 $\rightleftharpoons$IXI), $modificandooselementosqueocompunham$.

Nas posições em que houvesse a matriz de Pauli de inversão de bit, foi colocado um bit com valor um. Nas posições em que houvesse a matriz de identidade, foram colocados bits com valor zero, formando assim um vetor-linha. O que ocorre é que para a extensão dessa aplicação para código com p primo maior que 2, essa abordagem não é mais suficiente.

Uma solução para esse impasse é utilizar-se da representação de vetores-linha, e a partir delas construir operadores lineares equivalentes, no sentido de que esse operadores agiriam, sobre os rótulos dos estados da base do estado codificado, como agiriam os vetores-linha sobre as palavras-código.

Analisando de forma rápida a adição de um vetor-linha arbitrário sobre outro vetor-linha também arbitrário, considerando aritmética modular com $p = 3$, é possível entender qual a abordagem necessária

$$[000120] + [100120] = [100210],$$

$$[112000] + [100120] = [212120].$$

O vetor-linha padrão, [100120], quando afetado pelo vetor-linha de teste, [000120], tem seus bits modificados conforme o valor do bit equivalente do segundo vetor-linha. O primeiro bit do vetor-linha padrão não tem seu valor modificado, pois o primeiro bit do vetor-linha de teste tem nesta posição um bit de valor zero, o que acarreta uma não modificação do valor do bit do vetor-linha padrão. Já o quinto bit do vetor-linha padrão tem seu valor acrescido de duas unidades, já que na mesma posição, o vetor-linha de teste tem um bit com esse mesmo valor.

O que se vê, e que já é conhecido de muitos estudiosos, é que bit-a-bit é realizada uma adição módulo o primo p que define o corpo finito de operação do código. Dessa forma, uma possível abordagem seria transformar cada bit em uma matriz do tipo que realizasse uma adição módulo o p primo sobre os rótulos dos estados quânticos da base.

Suponha que o vetor-linha de teste [112000] seja tomado para realizar essa transformação. A idéia seria criar um operador linear na forma extensa, ou seja, uma representação descrita pela concatenação de matrizes quânticas, com base em vetores-linha que apresentam a adição módulo p primo. O operador linear seria descrito pela sua aplicação sobre um estado quântico genérico:

$$S_{a,p} \rightleftharpoons S_{a,p}|x\rangle = |(x+a)\ mod\ p\rangle, \tag{5.38}$$

em que a seria o valor do bit oriundo do vetor-linha e p seria o primo em $GF(p)$, onde as operações de adição são realizadas.

Assim o vetor-linha [112000] seria transformado no operador linear $A = S_{1,3}S_{1,3}S_{2,3}S_{0,3}S_{0,3}S_{0,3}$. É interessante notar que a matriz de inversão de bit, X, é um caso particular dessa extensão descrita, quando se realiza a adição sobre o corpo finito $GF(2)$. Essa matriz de Pauli, X, representa a adição de uma unidade módulo 2 e a identidade não representa adição de qualquer quantidade.

A abordagem usada até o momento foi bastante pertinente para que se pudesse formular um operador linear para os erros de inversão de bit, já que é esse tipo de erro é próprio aos códigos clássicos. Essa abordagem é insuficiente para que se possa estender o raciocínio de modo que seja possível extrapolar e encontrar uma representação da matriz de inversão de fase para o caso $p - rio$.

O que se pode realizar é uma abordagem superficial sobre o assunto, de modo que não é objetivo desse texto apresentar profundidade conceitual sobre qual o caminho adotado para a extrapolação necessária. Considere que da mesma maneira que a matriz de inversão de bit extrapolada tem em sua expressão fatores que dependem tanto do p, adição sobre $GF(p)$, em que opera o vetor-linha, quanto do valor do bit em que ela deve ser retirada. É característica da matriz de inversão de fase acrescentar um fator multiplicativo ao estado alvo, sem que modifique o valor do rótulo do mesmo. Assim, podemos encarar uma expressão inicial para a extrapolação da matriz de inversão de fase como:

$$Z_{a,p} \rightleftharpoons Z_{a,p}|x\rangle = \lambda(p)^{ax}|x\rangle. \tag{5.39}$$

Vê-se que essa escolha inicial de expressão para a matriz extrapolada não é ruim, já que é possível sem maiores problemas retroceder ao caso em que já se conhece sobre operações binárias. Aplicando essa expressão para o caso binário tem-se:

$$Z_{1,2}|0\rangle = \lambda(2)^{1.0}|0\rangle = |0\rangle.$$

$$Z_{1,2}|1\rangle = \lambda(2)^{1.1}|1\rangle = -|1\rangle.$$

A partir das equações precedentes é possível, com um relativo esforço imaginativo, extrair o valor de $\lambda(p)$:

$$\lambda(p) = e^{\frac{2i\pi}{p}}.$$

Assim, a expressão extrapolada da matriz de inversão de fase é:

$$Z_{a,p} \rightleftharpoons Z_{a,p}|x\rangle = e^{\frac{2ixa\pi}{p}}|x\rangle.$$

Tendo por base as matrizes de erro já extrapoladas, é possível realizar a conversão das idéias dos códigos clássicos para os códigos quânticos, como no caso dos códigos CSS, tomando agora um corpo de extensão, mais abrangente do que já foi apresentado.

5.8 Códigos Estabilizadores e os Diagramas de Venn

Os códigos estabilizadores são uma classe importante de códigos quânticos. Eles têm uma construção análoga aos códigos clássicos de bloco lineares, são chamados também de códigos aditivos. No entanto, para que não exista dificuldade na abordagem e entendimento dos códigos estabilizadores é salutar introduzir inicialmente o formalismo estabilizador. O formalismo estabilizador é uma ferramenta de descrição para as operações da mecânica quântica. Em seguida, é possível exemplificar como as portas lógicas quânticas e as medidas podem ser descritas através desse formalismo e realizar a apresentação de um teorema muito importante que põe limitações nas operações descritas pelo formalismo.

Considere o estado quântico descrito por

$$\psi\rangle = \frac{|00\rangle + |11\rangle}{2}.$$

É fácil identificá-lo como um estado quântico EPR de dois *qbits*. Sobre este estado algumas características são bastante importantes, este estado verifica as equações $X_1X_2|\psi\rangle = |\psi\rangle$ e $Z_1Z_2|\psi\rangle = |\psi\rangle$. Através dessas equações é possível identificar o estado como o estado que é imutável em relação à interação dos operadores lineares X_1X_2 e Z_1Z_2, ou também referenciá-lo como o estado que é estabilizado pelos operadores descritos. Mais interessante, e por isso menos evidente, é o fato de que esse estado quântico é o único estado que é estabilizado por esses operadores. Assim, como certos estados quânticos são únicos em relação à estabilização de alguns operadores é possível descrevê-los somente através dos operadores que os estabiliza, essa é a idéia fundamental do formalismo estabilizador. O formalismo estabilizador tem por principal idéia identificar os estados quânticos através dos operadores que apresentam a característica de estabilizá-los.

Algumas dúvidas poderiam surgir em relação a operações de erros que interagem com os estados quânticos, modificando-os e destruindo a característica de estabilidade, no entanto, o formalismo prevê estes casos e os engloba.

A idéia por detrás da conceito do formalismo estabilizador está diretamente relacionado com a teoria de grupos [48]. Para as aplicações relacionadas aos códigos quânticos o grupo fundamental é o grupo das matrizes de Pauli, G_n relacionadas para estados de n qbits. Este conjunto de matrizes forma um grupo em relação à operação de multiplicação matricial [48]. O grupo das matrizes de Pauli para um *qbit* é definido como se segue,

$$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Z, \pm iZ, \pm Y, \pm iY\}.$$

Define-se o grupo G_n em função do seus elementos constituintes,

$$A_{G_n} \in G_n \text{ se e só se, } A = \pm\alpha P_1 \cdots P_n, \text{ em que } P_i \in \{X, Z, Y, I\} \text{ e } \alpha = 1 \text{ ou } \alpha = i.$$

Considere S um subgrupo de G_n. Considere V_S, o conjunto de estados quânticos que apresentam a característica de serem estáveis em relação a todos os operadores do subgrupo de Pauli S. V_S é o

espaço vetorial estabilizado por S e analogamente S estabiliza V_S, na medida em que cada elemento de V_S não é modificado quando sobre ele age um elemento de S.

Para melhor exemplificar e entender o caso apresentado é salutar introduzir alguns exemplos. Considere um conjunto $S = \{I, Z_1Z_2, Z_1Z_3, Z_2Z_3\}$ que tem sua operação definida sobres estados quânticos de três qbits. Os estados que são estáveis em relação a Z_1Z_2 (equação 5.7) são $|000\rangle, |001\rangle, |110\rangle$, e $|111\rangle$. Já para o operador Z_2Z_3 (equação 5.8), os estados são $|000\rangle, |100\rangle, |011\rangle$ e $|111\rangle$. É interessante notar que os únicos estados quânticos que fazem parte dos dois conjuntos de estados estabilizados são $|000\rangle$ e $|111\rangle$. Assim é possível concluir que o conjunto vetorial que é estabilizado pelos operadores Z_1Z_2 e Z_2Z_3 é formado pelos estados quânticos $|000\rangle$ e $|111\rangle$. Vê-se claramente que o espaço vetorial de estados estáveis foi completamente determinado através de dois operadores, isso é uma característica muito importante, pois o conjunto de vetores pode ser determinado através dos operadores geradores.

Seja um conjunto de elementos, $g_1, g_2, ..., g_f$, de um grupo G. Diz-se que estes elementos são geradores do Grupo G, se todo e qualquer elemento do grupo puder ser representado como um produto destes elementos , $g_1, g_2, ..., g_f$. Assim, uma notação especial é usada para identificar o conjunto de geradores, $G = \langle g_1, g_2, ..., g_f\rangle$. No exemplo apresentado acima, o conjunto de geradores é $G_S = \langle Z_1Z_2, Z_2Z_3\rangle$, pois, $Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$ e $I = (Z_1Z_2)^2$ (a ordem de G, também denotado por $|G|$, é quatro, tendo em vista que existem quatro elementos em S). Esse grupo pode ser chamado como grupo estabilizador dos estados quânticos $|000\rangle$ e $|111\rangle$, ou seja, os operados que são elementos do conjunto S não afetam os estados $|000\rangle$ e $|111\rangle$ quando postos a interagir. O uso de geradores para a descrição dos processos ocorridos no grupo de operadores representa uma vantagem clara, tendo em vista que existe nomenclatura sucinta, clareza de descrição e também representa uma economia de operações, pois caso se queira saber se um determinado estado quântico é estabilizado por um grupo específico de operadores lineares, é suficiente testá-lo quanto aos geradores.

Um fato que vale a pena ser mencionado é que existem restrições quanto à utilização de subgrupos de Pauli que podem ser usados como estabilizadores para um espaço vetorial não-trivial. É necessário realizar um teste quanto a duas condições.

1. Os elementos de S devem comutar entre si.

2. O elemento $-I$ não pode pertencer ao conjunto de matrizes estabilizadoras.

É interessante entender o motivo pelo qual essas condições são necessárias. Considere que um espaço vetorial não específico seja não-trivial e contenha um elemento não nulo $|\psi\rangle$. Considere também que dois operadores J e K sejam operadores que pertençam ao grupo estabilizador de operadores. Uma característica importante que concerne às matrizes de Pauli é que elas, entre si, comutam ou anticomutam, havendo unicamente essas duas possibilidades [7]. Assim, o mesmo pode ser dito em relação às duas matrizes J e K. Sem perda de generalidade, pode-se supor que essas matrizes podem apresentar a característica de anticomutatividade, ou seja, $JK = -KJ$. Esse fato pode ser estendido para o estado quântico, pois $|\psi\rangle = JK|\psi\rangle = -KJ|\psi\rangle = -|\psi\rangle$. Isso significa que o único estado quântico que satisfaz essa característica é o estado quântico nulo, o que representa uma contradição (já que o espaço vetorial é não-trivial). A segunda condição, quando aplicado aos estados quânticos resultará na mesma contradição.

Após essa breve introdução é interessante aplicar o que já foi mencionado em alguns casos de códigos quânticos já estabelecidos. O código de Steane é um bom exemplo de aplicação de códigos

Tabela 5.2: Operadores geradores estabilizadores para o Código de Steane [7,1].

Referência	**Operador**
g_1	$IIIXXXX$
g_2	$IXXIIXX$
g_3	$XIXIXIX$
g_4	$IIIZZZZ$
g_5	$IZZIIZZ$
g_6	$ZIZIZIZ$

.

estabilizadores. Na Tabela 5.2 estão destacados os geradores do grupo estabilizador de operadores para o código de Steane de sete qbits [7].

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \tag{5.40}$$

É significativo notar que a descrição do código através dos estabilizadores, principalmente para esse caso, é mais clara e sucinta que a descrição do código através dos estados quânticos. Há ainda vantagens em relação ao processo de identificação e correção de erro. Mais ainda, a incrível semelhança da disposição da forma extensa dos operadores com as matrizes de paridade usadas no processo de decodificação do código. Tomando as linhas da matriz de paridade 5.40 (Código de Hamming $C(7,4,3)$), não na forma padrão, que pode ser encontrada em [31] e realizando uma comparação entre os três primeiros operadores do grupo estabilizador para o código de Steane: g_1, g_2, g_3, nota-se que nas posições em que se acham as matrizes de inversão de bit, nas linhas da matriz de paridade encontram-se os números um, e onde se acham as matrizes de identidade, nas linhas da matriz de paridade acham os números zeros. A mesma orientação de pensamento pode ser aplicada aos três últimos estabilizadores: g_4, g_5, g_6, no entanto o que diferencia é que a matriz de paridade que é referenciada é a matriz de paridade do código $C_2^{\perp}$, contudo pela escolha do código de Steane $C_2^{\perp} \equiv (C^{\perp})^{\perp} \equiv C$, ou seja a matriz de paridade para os operadores g_4, g_5, g_6 é a matriz 5.40. Assim, nas posições em que se acham as matrizes de Pauli de inversão de bit, na matriz de paridade estão os números um. O grupo estabilizador referente ao código e Steane apresenta ordem 2^6.

Dado um conjunto de geradores estabilizadores com cardinalidade n, a ordem do grupo estabilizador é 2^n.

É relevante notar que a descrição quanto ao formalismo estabilizador pode ser estendida aos postulados da mecânica 3.1, 3.2, 3.3, 3.5, para um aprofundamento dessa relação vide [7].

O formalismo estabilizador pode ser estendido para descrever as operações em portas lógicas quânticas também. O processo de dinâmica desses espaços vetoriais diante das interações de outros operadores é útil na descrição dos efeitos dos ruídos sobre o espaço de estados ao qual pertence o código corretor de erros. Considere que um operador linear U seja posto a interagir com um estado quântico que é estabilizado por um grupo S. Considerando que $|\psi\rangle$ seja um elemento qualquer do espaço vetorial estabilizado, tem-se que

Tabela 5.3: Conjugação matricial para várias portas lógicas quânticas - $UO_IU^\dagger = O_S$.

Operador de Conjugação - U	**Operador de entrada - O_I**	**Operador de Saída - O_S**
Não $-$ *Controlado*	X_1	X_1X_2
Não $-$ *Controlado*	X_2	X_2
Não $-$ *Controlado*	Z_1	Z_1
Não $-$ *Controlado*	Z_2	Z_1Z_2
H	X	Z
H	Z	X
S	X	Y
S	Z	Z
X	X	X
X	Z	$-Z$
Y	X	$-X$
Y	Z	$-Z$
Z	X	$-X$
Z	Z	Z

.

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle. \tag{5.41}$$

Pela equação 5.41 é possível concluir que o estado $U|\psi\rangle$ é estabilizado por $UgU^\dagger$. Isso pode se estendido para todo o espaço vetorial, já que não se realizou nenhuma observação que pudesse afetar a generalidade das hipóteses, resultando em garantir que o espaço UV_S é estabilizado por $USU^\dagger \equiv UgU^\dagger | g \in S$. Essa extensão pode ser alcançada mesmo aos geradores, já que o conjunto $g_1, ..., g_{n-k}$ gera o grupo S, então $Ug_1U^\dagger, ..., Ug_{n-k}U^\dagger$ gera o grupo $USU^\dagger$. A interpretação é clara quanto aos fatos, qualquer modificação ocorrida nos estados quânticos causado por ruído ou operação de portas lógicas pode ser reaplicado aos geradores do grupo estabilizador para que a característica de invariância seja mantida.

Na Tabela 5.3 estão referenciadas algumas operações de transformação úteis na interpretação dos códigos corretores.

Para exemplificar o processo de conjugação quando uma porta lógica é posta a interagir com um estado quântico estabilizado pode-se calcular explicitamente o caso para as portas de Hadamard e a Não-controlada para o caso de X_1,

$$UX_1U^\dagger = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = X_1X_2,$$

$$HXH^\dagger = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z,$$

$$HZH^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X.$$

Assim é possível enunciar um importante teorema [7].

Teorema 5.2. *Considere U um operador unitário sobre n qbits, com a propriedade de que, se* $g \in G_n$*, então* $UgU^\dagger \in G_n$*. Tem-se que, a menos de uma fase global, U pode ser construído a partir de* $O(n^2)$ *portas Hadamard, de fase e Não-controlado.*

Quanto às medidas, o formalismo pode englobá-lo. Suponha que se realize uma medida de g e que este elemento, g, pertence à G_n, ao grupo de Pauli para n qbits. Isso pode ser feito, já que g é um operador linear e pode ser visto como um observável. Como o caso em que se estuda é relacionado às matrizes de Pauli, não há problema algum em supor que este elemento é formado por uma multiplicação de matrizes de Pauli, sem inserir qualquer fator multiplicativo. Considere ainda que o sistema quântico esteja no estado $|\psi\rangle$ que apresenta como grupo estabilizador $S = \langle g_1, ..., g_n\rangle$; é possível descrever as transformações as quais o grupo estabilizador é submetido após a realização da medida iniciando pela análise de dois possíveis casos:

1. g comuta com todos os geradores do estabilizador.

2. g anticomuta com um ou mais estabilizadores.

Analisando o primeiro caso, pode-se garantir que g faz parte do conjunto de geradores, pois $g_i g|\psi\rangle = gg_i|\psi\rangle = g|\psi\rangle$. Isso implica que o estado $g|\psi\rangle$ faz parte do espaço vetorial formado por estados quânticos que são estabilizados por S. Assim, o estado $g|\psi\rangle$ é um múltiplo de $|\psi\rangle$, mas como $g \in G_n$ tem-se que $g^2 = I$. Então, $g|\psi\rangle = \pm|\psi\rangle$, implicando no fato de que g ou $-g$ é um estabilizador do estado $|\psi\rangle$. Se $g|\psi\rangle = |\psi\rangle$, então uma medida com g resultará, sempre, no valor 1 com probabilidade 1. Caso $g|\psi\rangle = -|\psi\rangle$, uma medida com g resultará, sempre, no valor -1 com probabilidade 1.

No segundo caso, o operador g anticomuta com g_1 e comuta com todos os outros geradores. Como $g \in G_n$, os seus possíveis autovalores são ± 1, os seus projetores para as medidas são $(I \pm g)/2$. Assim, as medidas podem ter os resultados com as probabilidades

$$p(+1) = tr\left(\frac{I+g}{2}|\psi\rangle\langle\psi|\right),$$

$$p(-1) = tr\left(\frac{I-g}{2}|\psi\rangle\langle\psi|\right).$$

Sabendo-se que $g_1|\psi\rangle = |\psi\rangle$ e $gg_1 = -g_1 g$, é possível expressar a probabilidade de resultado 1 como:

$$p(+1) = tr\left(\frac{I+g}{2}g_1|\psi\rangle\langle\psi|\right),$$

$$p(+1) = tr\left(g_1\frac{I-g}{2}|\psi\rangle\langle\psi|\right).$$

Através de manipulação matemática e usando para isso propriedades específicas relacionadas ao traço matricial, tem-se que

$$p(+1) = tr\left(\frac{I-g}{2}|\psi\rangle\langle\psi|\right) = p(-1).$$

Assim, como $p(+1) + p(-1) = 1$ e $p(+1) = p(-1)$, então $p(+1) = p(-1) = 1/2$. No caso do resultado da medida ser de valor 1 o estado quântico é modificado com a medida e o conjunto estabilizador é modificado de modo acrescentar novo estado quântico.

Após essa breve introdução sobre o formalismo estabilizador é possível avançar de modo a conseguir construir os códigos corretores de erros quânticos baseados no formalismo estabilizador. Considere um código quântico estabilizador $[n, k]$ que é definido como o espaço vetorial V_S estabilizado por um grupo $S \in G_n$, esse código é referenciado por $C(S)$. Suponha que um erro E atue sobre o sistema e que esse erro $E \in G_n$. Dois possíveis fatos podem ocorrer. O erro pode comutar com o operadores de S ou anticomutar. Para um compelto entendimento do processo de decodificação é necessário a introdução de duas definições que serão necessárias.

Definição: Chama-se de normalizador de G_n, referenciado por $N(G_n)$, o conjunto de operadores U, tal que $UG_nU^\dagger = G_n$.

Definição: O centralizador $Z(S)$ de S em G_n é um conjunto de operadores E_i tal que $E_i \in G_n$ e $E_ig = gE_i$, em que $g \in S$.

Para que seja mais didático apresentar o poder de descrição do formalismo estabilizador aplicado aos códigos corretores de erros, considere que um estado quântico seja codificado conforme o código $C(S)$ estabilizador $[n, k]$, o qual tem como estabilizador $\langle g_1, ..., g_{n-k}\rangle$. Um erro E, $E \in G_n$, afeta o estado quântico codificado danificando os dados do estado. Como o erro faz parte do conjunto das matrizes de Pauli de n qbits, dois possíveis casos podem ocorrer: ou o erro comuta com todos os geradores ou comuta com pelo menos um dos geradores. No caso em que E anticomuta com todos os geradores, o espaço de estados do código é transportado para um espaço vetorial ortogonal que acarreta numa possibilidade de identificação do erro por medidas projetivas. Outro possível caso ocorre quando o erro comuta com todos os elementos do estabilizador. Pode acontecer de o erro fazer parte do próprio conjunto de estabilizadores e isso não é danoso ao estado codificado. Pode acontecer que o erro comute com os estabilizadores, mas não é parte desse conjunto. Isso ocorre porque o erro pode fazer parte do centralizador do código, $Z(S)$. Para os casos de estudo desse texto é possível considerar que o conjunto centralizador é idêntico ao conjunto normalizador.

Teorema 5.3. ***(Condições para correção de erros para códigos estabilizadores)****: Considere S o conjunto estabilizador de um código estabilizador $C(S)$. Considere também E_j um conjunto de operadores em G_n tais que $E_j^\dagger E_k \notin N(S) - S$ para todo j e k. Esse conjunto de erros que apresenta essa característica pode ser considerado como o conjunto de erros corrigíveis para o código $C(S)$.*

A demonstração desse teorema pode ser vista em [7].

$N(S) - S$ é o conjunto de matrizes que fazem parte do centralizador, $N(S)$, porém não fazem parte de S.

Apesar da beleza matemática deste enunciado, seria mais interessante propor uma maneira sistemática de detecção e correção de erros. Para isso é possível utilizar a interpretação dos diagramas de Venn aplicados aos resultados das medidas.

Suponha que um grupo estabilizador $S = \langle g_1, ..., g_{n-k}\rangle$ seja o conjunto de operadores que estabilizam os estados quânticos referentes aos código $C(S)$ $[n, k]$ e que E_j seja um conjunto de erros

que podem ser corrigidos pelo código em questão. Para que haja detecção do erro, caso este tenha interagido com o estado codificado, é necessário realizar medidas em cascata tendo como observáveis os geradores. Associa-se a cada observável g_j, um valor de medição b_j, formando assim um padrão de síndrome para cada erro possível, pois $E_j g_l E_j^\dagger = b_l g_l$. Através dos padrões de síndrome identifica-se o erro E_j resultando que para corrigir o efeito desse erro é suficiente aplicar $E_j^\dagger$. Pode ocorrer de dois erros distintos apresentarem o mesmo padrão de síndrome E_j e $E_{j'}$. Neste caso ocorre que $E_j P E_j^\dagger = E_{j'} P E_{j'}^\dagger$, em que P é o projetor sobre o espaço do código. Como $E_j^\dagger E_{j'} P E_{j'}^\dagger E_j = P$ tem-se que $E_j^\dagger E_{j'} \in S$, assim basta que seja aplicado o operador $E_j^\dagger$ mesmo após a ocorrência de $E_{j'}$, para que o efeito deste operador sobre o estado codificado seja corrigido.

Assim, em síntese, após a identificação do operador linear de erro pelo padrão de síndrome, aplica-se o conjugado hermitiano do mesmo para que o efeito deste sobre o estado quântico seja corrigido. Para que os códigos estabilizadores sejam considerados verdadeiros códigos análogos aos códigos de bloco clássico, seria interessante apresentar algum conceito análogo ao conceito de distância de Hamming do código. Para os códigos estabilizadores define-se o conceito de peso de Hamming como sendo a quantidade de matrizes diferentes da identidade na forma extensa deste operador. Por exemplo, um erro do tipo $E = X_1 X_4$, para 7 *qbits* tem peso igual a 2. Assim para um código estabilizador $C(S)[n, k]$, define-se a distância deste código de forma congênere ao caso clássico. No caso clássico, o cálculo da distância mínima de um código pode ser adaptada para ser calculada como o peso da palavra-código de menor peso, no caso quântico temos o menor peso de um elemento de $N(S) - S$. Também semelhante ao caso clássico, um código quântico com uma distância mínima $2t+1$ pode corrigir erros arbitrários em até t *qbits*.

Uma possível interpretação para o processo de decodificação é a utilização dos diagramas de Venn, tendo em mente a idéia apresentada por McEliece para códigos clássicos [33]. No caso da decodificação é possível apresentar uma configuração padrão baseada nos diagramas de Venn para cada erro corrigível possível e através desse padrão identificá-lo e corrigi-lo. Seria interessante no decorrer das apresentações de códigos quânticos estabelecidos apresentar os diagramas de Venn correspondentes aos padrões de decodificação.

5.8.1 O código quântico [3,1] para inversão de bit

Para o código de inversão de bit é conhecido que o estado padrão de informação $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ é transformado em $|\psi_C\rangle = \alpha|000\rangle + \beta|111\rangle$. Para este estado codificado, os operadores $Z_1 Z_2$ e $Z_2 Z_3$ são os estabilizadores considerados. Os possíveis erros que podem interagir com o estado codificado são I, X_1,X_2,X_3, $X_1 X_2$, $X_1 X_3$, $X_2 X_3$. É fácil verificar que todos os erros apresentados, a menos da identidade, anticomutam com os geradores estabilizadores. Isso significa que o conjunto $\{I, X_1, X_2, X_3\}$ é um conjunto de erros corrigíveis para o código de inversão de bit. As equações a seguir mostram a relação de comutatividade entre X_2 e os operadores geradores $Z_1 Z_2$ e $Z_2 Z_3$.

$$X_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, Z_1Z_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$X_2 \cdot Z_1Z_2 = \begin{pmatrix} 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix},$$

$$Z_1Z_2 \cdot X_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

$$(X_2 \cdot Z_1Z_2) = -(Z_1Z_2 \cdot X_2),$$

$$Z_2Z_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

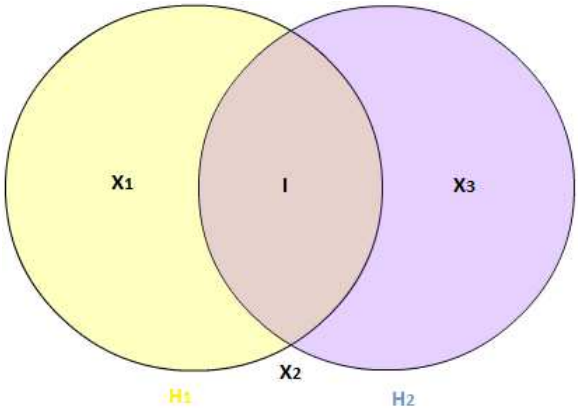


Figura 5.9: *Diagrama de Venn para o padrão de síndrome dos erros para o código de inversão de bit.*

$$X_2 \cdot Z_2Z_3 = \begin{pmatrix} 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix},$$

$$Z_2Z_3 \cdot X_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

$$(X_2 \cdot Z_2Z_2) = -(Z_2Z_3 \cdot X_2)$$

Para a detecção do erro é possível formar o padrão de síndrome através das medidas utilizando como observável os geradores dos estabilizadores. Considere que um erro do tipo X_2 ocorreu e que os observáveis utilizados são os operadores Z_1Z_2 e Z_2Z_3. Assim, o estabilizador será modificado para $\langle -Z_1Z_2, -Z_2Z_3 \rangle$. O diagrama de Venn para os possíveis casos de erros é apresentado na figura 5.9, em que os símbolos H_i fazem referencia aos operadores geradores do código, $H_1 = Z_2Z_3$ e $H_1 = Z_1Z_2$.

O processo de codificação e decodificação é bastante interessante quando abordado pelo formalismo estabilizador, pois este formalismo possibilita compacta e de fácil entendimento do mesmo. Assim, um método de codificação e decodificação pode ser elaborado tendo em mente todos os pontos abordados. Os circuitos de codificação e decodificação são apresentados nas figuras 5.2 e 5.3. Pode ser visto na

Tabela 5.4: Operadores geradores estabilizadores para o Código de Shor [9,1].

Referência	**Operador**
g_1	$ZZIIIIIII$
g_2	$IZZIIIIII$
g_3	$IIIZZIIII$
g_4	$IIIIZZIII$
g_5	$IIIIIIZZI$
g_6	$IIIIIIIZZ$
g_7	$XXXXXXIII$
g_8	$IIIXXXXXX$

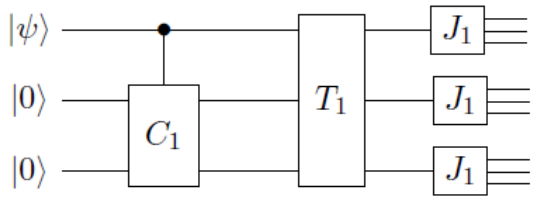


Figura 5.10: Circuito de codificação para o código de Shor

figura 5.2 a utilização de um bloco C_1. Esse bloco representa uma matriz que se diz controlada por um *qbit* específico. O valor deste qbit irá perminitir ou não a interação da matriz sobre o estado quântico. A sua expressão é $C_1 = (X_2X_3)^{x_1}$.

5.8.2 Código de Shor [9,1]

Para o código de Shor, existem oito geradores para o conjunto de operadores estabilizadores. Na tabela 5.4 é possível visualizá-los. Por motivos óbvios de quantidades de geradores estabilizadores, a confecção do diagrama de Venn de todos os padrões de síndromes de erros possíveis se torna imprat-icável. Considere como exemplo de decodificação a ocorrência de um erro do tipo X_1 e outro erro do tipo Y_4, todos para um *qbit*. O erro de inversão de bit X_1 anticomuta com o primeiro gerador e somente este, apresentando assim um padrão de síndrome bem específico; o erro de inversão de bit e fase Y_4 anticomuta com o terceiro, sétimo e oitavo geradores, também formando um padrão de síndrome bem específico. Consequentemente é possível estabelecer que qualquer erro de um *qbit* pode ser corrigido pelo código, já que todos os operadores de Pauli com peso menor ou igual a dois ou estão em S ou anticomutam com algum elemento de S.

Os circuitos de codificação, podem ser elaborados a partir de métodos sistemáticos já utilizados nos códigos de inversão de bit. No circuito de codificação de Shor, as caixas J_1, são os circuitos de codificação para o código de repetição, e no circuito de decodificação as caixas H_i representam os geradores estabilizadores para o código em questão.

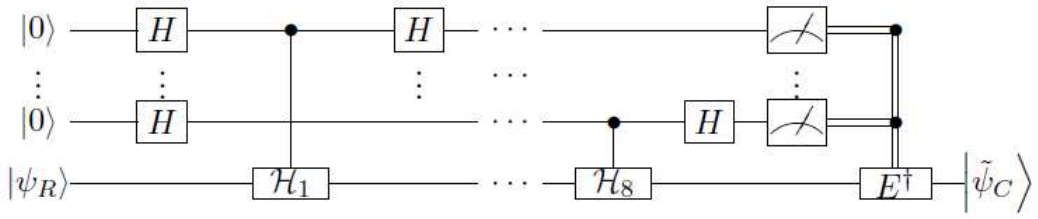


Figura 5.11: Circuito de decodificação para o código de Shor

Tabela 5.5: Operadores geradores estabilizadores para o Código de 5 qbits.

Referência	**Operador**
g_1	$XZZXI$
g_2	$IXZZX$
g_3	$XIXZZ$
g_4	$ZXIXZ$

.

5.8.3 O código de cinco qbits [5,1]

Um estudo mais cuidadoso sobre o limite quântico de Hamming pode suscitar alguns questionamentos quanto à possibilidade de existir algum código que consegue verificar o limite quântico de Hamming em sua igualdade. E desta forma, qual a quantidade de *qbits* mínima que essa codificação pode ser realizada de modo que qualquer erro de um *qbit* possa ser detectado e corrigido?

Na Tabela 5.5 estão expostos os operadores geradores estabilizadores para o código de cinco *qbits* que apresenta a propriedade de conseguir detectar e corrigir qualquer erro que atue sobre um *qbit* do estado de informação.

Considere o esquema de codificação apresentado pelo circuito exposto na figura 5.12, em que as matrizes C_1 e T_1, representam uma matriz controlada de preparação do estado pré-codificado com expressão $C_1 = (X_4X_3X_2X_1)^{x_5}$ e uma matriz de transformação do estado pré-codificado para o estado codificado com expressão $T_1 = \frac{1}{\sqrt{8}} \prod_{i=1}^{4} \left\{ \sum_{j=0}^{1} H_i^j \right\}$, respectivamente.

Todo o processo de codificação e decodificação pode ser expresso através de um método sistemático, um algoritmo que, para o caso do código de cinco *qbits*, é descrito a seguir:

Informação	$\|\psi\rangle = \alpha_0 \|0\rangle + \alpha_1 \|1\rangle$
Acoplamento de 4 *qbits*	$\|\psi_0\rangle = \|\psi\rangle \otimes \|0000\rangle = \alpha_0 \|00000\rangle + \alpha_1 \|10000\rangle$
Preparação da Matriz Controlada C_1	$C_1 = (X_4X_3X_2X_1)^{x_5}$
Aplicação da Matriz Controlada C_1	$\|\psi_1\rangle = C_1 \|\psi_0\rangle = \alpha_0 \|00000\rangle + \alpha_1 \|11111\rangle$
Preparação da Matriz de Transformação T_1	$T_1 = \frac{1}{\sqrt{8}} \prod_{i=1}^{4} \left\{ \sum_{j=0}^{1} H_i^j \right\}$
Aplicação da Matriz de Transformação	$T_1 \|\psi_1\rangle = \|\psi_C\rangle$
Estado Codificado	$\|\psi_C\rangle = \alpha_0 \|0_L\rangle + \alpha_1 \|1_L\rangle$

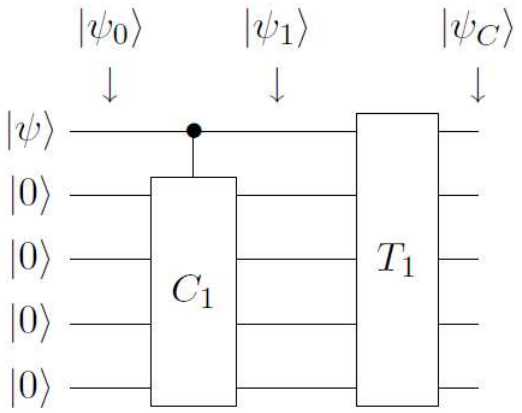


Figura 5.12: Circuito de codificação para o código de 5 qbits

Na figura 5.13, estão referenciados todos os padrões de síndrome para todos os erros possíveis que o código de cinco qbits é capaz de corrigir. Para se obter o padrão de síndrome que possibilita a identificação dos erros é necessário a medição em cascata utilizando os geradores. A seguir um método sistemático de decodificação.

Estado Recebido	$\|\psi_R\rangle = E\,\|\psi_C\rangle$
Cálculo da Síndrome	$S_i = \langle\psi_R\|\,H_i\,\|\psi_R\rangle$
Identificação do Erro	$(S_1S_2S_3S_4) \longleftrightarrow E$
Correção do Erro	$E^\dagger \longrightarrow E^\dagger\,\|\psi_R\rangle = \|\psi_C\rangle$, pois $E^\dagger E = I$
Preparação da Matriz de Recuperação P	$P = \sqrt{8}\{\|00000\rangle\langle 00000\| + \|11111\rangle\langle 11111\|\}$
Aplicação da Matriz de Recuperação P	$P\,\|\psi_C\rangle = \|\psi_1\rangle$
Acoplamento de 1 *qbit*	$\|\psi_1\rangle \otimes \|0\rangle$
Preparação da Matriz Controlada C_2	$C_2 = (X_1)^{x_6x_5x_4x_3x_2}$
Aplicação da Matriz Controlada C_2	$C_2\,\|\psi_1 0\rangle$
Colapso do 5 primeiros *qbits*	$\|\psi\rangle = \alpha_0\,\|0\rangle + \alpha_1\,\|1\rangle$

5.8.4 Os códigos CSS e o código de sete qbits

Tomando todos os códigos quânticos apresentados neste texto, o código que pode expressar de forma elegante a simplicidade de descrição do formalismo estabilizador, tornando a compreensão e exposição dos elementos concernentes a ele clara, é a classe de códigos conhecida como códigos CSS.

Por apresentar uma confecção totalmente embasada pelos códigos clássicos, a montagem dos operadores geradores estabilizadores se torna relativamente fácil. Considere C_1 e C_2 códigos clássicos lineares com parâmetros $[n, k_1]$ e $[n, k_2]$, respectivamente. Esses códigos são tais que C_2 está contido em C_1 e ainda C_1 e $C_2^\dagger$ apresentam a característica de corrigirem ambos t erros. Para se conhecer os operadores geradores estabilizadores é necessário tomar cada linha das matrizes de verificação de paridade dos códigos C_1 e $C_2^\dagger$ e realizar a transformação previamente descrita. Como exemplo da abordagem via grupos estabilizadores para a classe de código CSS temos o código de Steane ou código

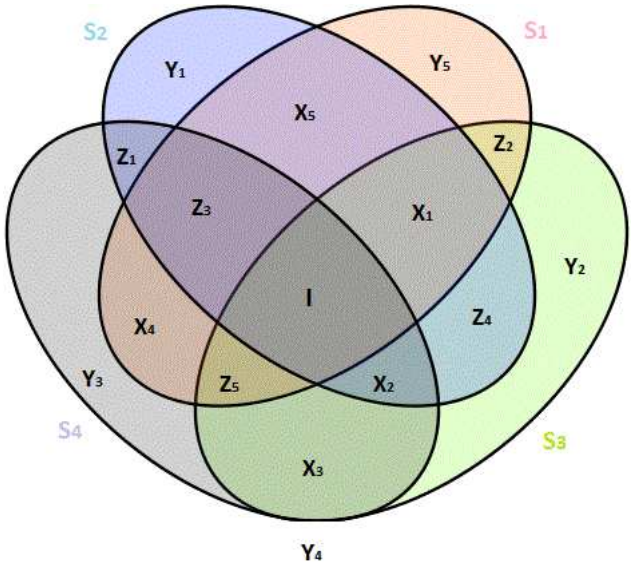


Figura 5.13: Diagrama de Venn com os padrões de síndrome para o código de 5 qbits

de sete *qbits*. Esse código foi formado pelo código de Hamming $C(7,4,3)$ como o código C_1 e o código simplex, dual do código de Hamming, com parâmetros $C(7,3,4)$ como código C_2. Para a identificação dos operadores, que são elementos do grupo estabilizador, são necessárias as matrizes de paridade de C_1 e de $C_2^{\perp}$. Já foi mostrado que as matrizes procuradas são as mesmas, que não estando da forma padrão, está expressa em 5.40 e os estabilizadores na Tabela 5.2. Não foi colocado diagrama de Venn para esse tipo de código diante de possível do elevado número de conjuntos o que poderia resultar em confusão de entendimento.

capítulo 6

Conclusões

O maior desafio para lidar com os códigos quânticos é a dificuldade envolvida, desde conceitos quânticos fundamentais até a notação empregada. Mesmo aqueles que conhecem relativamente bem à codificação clássica de canal, enfrentam dificuldades em compreender os princípios e o mecanismo de funcionamento dos códigos quânticos. Particularmente, ao ler artigos publicados no assunto, há um sentimento pouco óbvio de como os circuitos de codificação e decodificação operam.

Assim o objetivo desta dissertação foi tentar dar uma contribuição na abordagem da teoria de detecção e correção quântica de erros, cujo escopo teórico apresenta quase que em sua totalidade uma abordagem mais próxima dos pesquisadores das ciências físicas, uma visão própria de engenheiros seria salutar diante das contribuições à esta área dos pesquisadores do segundo grupo. A predominância de pesquisadores da área de ciências físicas trás, como consequência, um ferramental mais familiarizado a esta área, isso torna o entendimento da teoria básica algo difícil e relativamente confuso, já que no processo de formação de dos engenheiros essas ferramentas não são apresentadas com o mesmo objetivo.

Uma forma bastante interessante de alcançar este objetivo foi usar-se de algo mais apropriado aos engenheiros, como os processo relacionados à algoritmos, processos sistemáticos de codificação e decodificação clássica e a interpretação de diagramas de Venn introduzida por McEliece.

6.1 Contribuições

Apresenta-se aqui a codificação e decodificação quântica com uma visão intuitiva e compreensível para os engenheiros que lidam com a codificação clássica. A idéia do decodificador é aclarada com base no arranjo padrão, não abordada nesse trabalho contudo podendo ser vista em [31] [32], e no cálculo de síndromes, reinterpretando o uso de estabilizadores como modelos isométricos aos de equações clássicas de verificação de paridade. O cálculo das componentes da síndrome é resultado de uma medição quântica. A despeito de o exemplo apresentado ser ingênuo, os resultados podem ser extrapolados para o caso geral. O objetivo, como mencionado, é tornar o mecanismo mais compreensível, com uma descrição em linguagem mais próxima da teoria clássica de códigos, tentando não se perder em

meandros da Física quântica.

6.2 Perspectivas de Investigações

- Para trabalhos futuros um possível caminho seria abordar os diagramas de Venn para encontrar um conjunto de operadores estabilizadores dado os padrões de síndrome.
- Possíveis aplicações da interpretação dos diagramas de Venn à códigos quânticos de treliça, entre outros.
- Possíveis adaptações dos anti-códigos clássicos, para maiores detalhes vide [49], para a teoria da computação e informação quântica, na tentativa de construção de anti-códigos quânticos e sua semelhança com os códigos CSS.

Referências Bibliográficas

[1] Redford, J.; A biography of Armstrong, Disponível em <http://world.std.com/ jlr/doom/armstrng.htm>. Acesso em: 16/05/2011.

[2] Oppenheim, A.; Schafer, R.; *Discrete-Time Signal Processing.*2ª Edição. New Jersey. Prentice Hall. 1999. 870p.

[3] Shannon, C.E., *A Mathematical Theory of Communication*, Bell, Syst. Tech. J. 27, pp.379-423(Part I),623-656(Part II), Julho 1948

[4] Brinkman, W.F.; Haggan, D.E.; Troutman, W.W.; A history of the invention of the transistor and where it will lead us. *Solid-State Circuits, IEEE Journal of* , vol.32, no.12, pp.1858-1865, Dezembro 1997,doi: 10.1109/4.643644 .

[5] Pais, A.; *Inward bound: of matter and forces in the physical world.* Oxford University Press, Oxford, 1991.

[6] Schneier,B.; *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* 2ª Edição. New York, NY, USA: John Wiley Sons, Inc. 1995.

[7] Nielsen, M.A.; Chuang, I.L.; *Computação Quântica e Informação Quântica.*Trad. Sob a direção de Ivan S. Oliveira. Porto Alegre: Bookman, 2005. 733p.

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

[9] Benniof, P.; *The computer as a physics systems: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines.* J. Stat. Phys., 22(5), pp. 5563-591, 1980.

[10] Bennet, C.H.; Brassard, G.; *Quatum cryptography: Public Key distribution and coin tossing.*In proceedings of IEEE international Conference on Computers, Systems and Signals Processing, pp. 175-179, New York, 1984. IEEE. Bangalore, India, Dezembro 1984.

[11] Bennet, C.H.; Brassard, G.; Crépeau, C.; Jozsa, R.; Peres, A.; Wooltters, W. K.; Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.*Phys. Rev. Lett.70*, pp. 18951899, Março 1993, doi: 10.1103/PhysRevLett.70.1895 .

[12] Shor, P.W.; Algorithms for quantum computation: discrete logarithms and factoring, *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on* , pp.124-134, 20-22 Novembro 1994, doi: 10.1109/SFCS.1994.365700 .

[13] Grover, L.K.; A fast quantum mechanical algorithm for database search. *In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*,New York, NY, USA (STOC '96). ACM, pp. 212-219, 1996. doi: 10.1145/237814.237866 .

[14] Gershenfeld,N.A.; Chuang, I.L.; Bulk Spin-Resonance Quantum Computation. *Science*, 275, pp. 350-356,Janeiro 1997. doi:10.1126/science.275.5298.350

[15] Appelbaum, I.; Huang, B.; Monsma, D.J.; Electronic measurement and control of spin transport in silicon. *Nature*, vol. 447, pp. 295-298, Maio 2007. doi:10.1038/nature05803

[16] Dutt, M.V.G.; Childress,L.; Jiang, L.; Togan, E.; Maze, J.; Jelezko, F.; Zibrov, A. S.; Hemmer, P. R.; Lukin, M. D.; Quantum Register Based on Individual Electronic and Nuclear Spin Qubits in Diamond, *Science 1*,vol. 316, no., pp. 1312-1316., Junho 2007, doi:10.1126/science.1139831.

[17] Chang,D.E.; Sørensen, A.S.; Demler, E.A.; Lukin, M.D.; A single-photon transistor using nanoscale surface plasmons. *Nature Physics*, vol. 3, pp. 807 - 812, Agosto 2007, doi:10.1038/nphys708.

[18] Boldrini, J.L.; Costa, S.R.; Figueiredo, V.L.; Wetzler, H.G. *Álgebra Linear*. 3ª Edição. São Paulo. Harper Row do Brasil. 1980.

[19] Desurvire, E.*Classical and Quantum Information*. 1ª Edição. Cambridge. Cambridge University Press. 2009.

[20] Harlander, M.; Lechner, R.; Brownnutt, M.; Blatt, R.; Hänsel, W.; Trapped-ion antennae for the transmission of quantum information. *Nature*, vol. 471, pp. 200-203, Março 2011. doi:10.1038/nature09800

[21] Hoffman, K. M.; Kunze, R. *Linea Algebra*. 1ª Edição. New York. Prentice Hall. 1985.

[22] Einstein, A.; Podolsky, B.; Rosen, N.; Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, *Phys. Rev.*, 47:777-780, 1935.

[23] Bennet, C.H.; Brassard, G.; Crépeau, C.; Jozsa, R.; Peres, A.; Wooters, W.; Teleporting an Unknown Quantum State Via Dual Classical and EPR Channels, *Phys. Rev. Lett.*, 70:1895-1899, 1993.

[24] Boschi, D.; Branca, S.; De Martini, F.; Hardy, L.; Popescu, S.; Experimental Realization of Teleporting an Unkown Pure Quantum State Via Dual Classical And Einstein-Podolsky-Rosen Channels, *Phys. Rev. Lett.*, 80:1121-1125, 1998. arXiv:quant-ph/9710013.

[25] Bouwmeerst, D.; Pan, J.W.; Mattle, K.; Eibl, M.; Weinfurter, H.; Zeilinger, A.; Experimental Quantum Teleportation. *Nature*,390(6660):575-579, 1997.

[26] Furusawa, A.; Sorensen, J.L.; Braunstein, S.L.; Fuchs, C.A.; Kimble, H.J.; Polzik, E.S.; Unconditional Quantum Teleportation, *Science*, 282:706-709, 1998.

[27] Nielsen, M.A.; Knill, E.; Laflamme, R.; Complete Quantum Teleportation Using Nuclear Magnetic Resonance. *Nature*, 398:786-788, 1999.

[28] Landauer, R.; Irreversibility and Heat Generation in The Computing Process. *IBM J. Res Dev.*, 5:183, 1961.

[29] Szilard, L.; Uber Die Entropieverminderung in einem thermodynamischen system bei eingriffen intelligenter wesen. *Zeitscrift fur Physik*, 53:840-856, 1929.

[30] von Neumann, J.; Fourth University of Illinois Lecture. In A W. Burks, editor, *Theory of Self-Reproducing Automata*, pg 66, Urbana, 1966. University of Illinois Press.

[31] MacWillians, F.J.; Sloane, N.J.A; *The theory os error-correcting codes*. North-Holland. Amsterdam, 1977.

[32] Lin, S.; Costello, D.J.; *Error control coding*.Prentice-Hall. New Jersey. 1983.

[33] Han V.A.J; Remarks about the Hamming Code: a Tribute to Bob McEliece, *Benelux-Japan Workshop on Coding and Information*.

[34] Donoho, D.L.; Tanner, J.; Precise Undersampling Theorems, *Proceedings of the IEEE* , vol.98, no.6, pp.913-924, Junho 2010, doi: 10.1109/JPROC.2010.2045630.

[35] Glavieux, A; *Channel Coding in Communications Networs*. London: ISTE. 2007.

[36] Shockley, W.; The path to the conception of the junction transistor, *Electron Devices, IEEE Transactions on* , vol.23, no.7, pp. 597- 620, Julho 1976,doi: 10.1109/T-ED.1976.18463.

[37] Schaller, R.R.; Moore's law: past, present and future, *Spectrum*, IEEE , vol.34, no.6, pp.52-59, Junho 1997 doi: 10.1109/6.591665.

[38] Valadares, E.C.; Introdução aos Microscópios Eletrônicos de Varredura e Tunelamento, *Revista Brasileira de ensino de Física*, vol.14, no.2, pp.63-71.

[39] Leibfried, D.; Blatt, R.; Monroe, C.; Wineland, D.; Quantum dynamics of single trapped ions, *Rev. Mod. Phys*, vol.75, no.1, pp.281-324, Março 2003, doi: 10.1103/RevModPhys.75.281.

[40] Milies, C.P.; Breve História da Álgebra Abstrata, *II Bienal da Sociedade Brasileira de Matemática*, 58pp, 2004.

[41] Halliday, D.; Resnick, R.; Walker, J.; *Fundamentos da Física*. 8ª Edição. Rio de Janeiro: Editora LTC. 2009. 310 pp.

[42] Blahut, R.E.; *Algebric Codes on Lines, Planes and Curves*, New York: Cambridge University Press, 2008, 543 pp.

[43] Dirac, P.;*The Principles of Quantum Mechanics*, Cambridge: Oxford University Press, 1958, 314 pp.

[44] Griffiths,D.J.;*Introduction to Quantum Mechanics*, USA: Pearson Prentice Hall, 2005, 470 pp.

[45] Chrúscinski, D.; Geometric Aspects of Quantum Mechanics and Quantum Entanglement, *Journal of Physics: Conference Series*, Vol. 30, no.1, pp. 9-16, Jun 2006, doi: 10.1088/1742-6596/30/1/002

[46] Floyd, T.; *Sistemas Digitais: Fundamentos e Aplicações*, Porto Alegre : Bookman, 2007, 888 pp.

[47] Benenti, G.; Casati, G.; Strini, G.; *Principles of Quantum Computation and Information*, London : World Scientific Publishing Co., 2007, 256 pp.

[48] Conway, J.H.; Slone,N.J.A.;*Sphere Packings,Lattices and Groups*, Princeton: Springer-Verlag New York, 1999, 703 pp.

[49] Farrell, P.G., "Linear binary anticodes,"*Electronics Letters* , vol.6, no.13, pp.419,421, June 25 1970 doi:10.1049/el:19700293