



Universidade Federal de Campina Grande  
Centro de Ciências e Tecnologia  
Programa de Pós-Graduação em Física

Dissertação de Mestrado

**Utilização do Teleporte Quântico na  
Computação Quântica Tolerante a Falhas**

Antonildo Santos Pereira

Campina Grande – PB

Novembro - 2011

Universidade Federal de Campina Grande  
Centro de Ciências e Tecnologia  
Programa de Pós-Graduação em Física

## **Utilização do Teleporte Quântico na Computação Quântica Tolerante a Falhas**

Antonildo Santos Pereira

Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Física da Universidade Federal de Campina Grande como parte dos requisitos necessários para obtenção do grau de Mestre em Ciências no Domínio da Física.

Área de Concentração: Informação Quântica.

Aécio F. Lima  
Orientador

Campina Grande – PB, Paraíba, Brasil

©Antonildo Santos Pereira



FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCC

P436u Pereira, Antonildo Santos.  
Utilização do Teleporte Quântico na Computação Quântica Tolerante a Falhas / Antonildo Santos Pereira. - Campina Grande, 2011  
63 f.: il.

Dissertação (Mestrado em Física) – Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia.  
Orientador: Prof. Dr. Aécio F. Lima  
Referências.

1. Teoria da Informação – Computação Quântica. 2. Portas Quânticas.  
3. Teletransporte Quântico. 4. Qudits. I. Título.

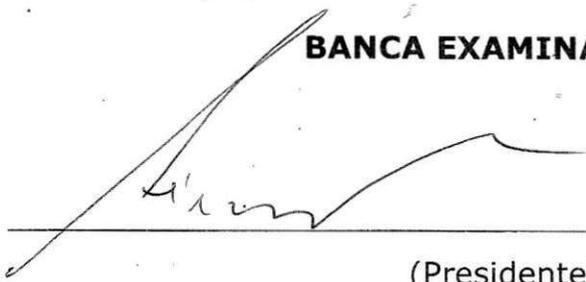
CDU 530.145 (043)

**ANTONILDO SANTOS PEREIRA**

**UTILIZAÇÃO DO TELEPORTE QUÂNTICO NA COMPUTAÇÃO QUÂNTICA  
TOLERANTE A FALHAS**

Dissertação aprovada em 25/11/2011

**BANCA EXAMINADORA**



(Presidente)

Prof. Dr. Aécio Ferreira de Lima  
Unidade Acadêmica de Física - UFCG



(Membro interno)

Prof. Dr. Rafael de Lima Rodrigues  
Unidade Acadêmica de Educação - UFCG



(Membro externo)

Prof. Dr. Eládio José de Goes Brennand  
Departamento de Física - UFPB

*A minha mãe Luzia Rodrigues dos Santos e a meus irmãos  
Antonio Pereira de Araújo Junior e Maria Luíza Santos  
Delfino com muito amor e carinho.*

---

---

# Agradecimentos

---

- Gostaria de agradecer primeiramente ao senhor supremo Deus que me conduziu e possibilitou o andamento deste trabalho.
- A minha mãe e aos meus avós que me criaram e contribuíram com exemplo e orientação para formação do meu caráter;
- Ao professor Aécio de Lima, pela orientação, sugestão, estímulo e competência com que conduziu esse trabalho.
- Aos professores: Francisco de Brito, Rômulo Rodrigues da Silva, Alex de Albuquerque da Silva pela colaboração que recebi durante a fase de preparação desta dissertação.
- A todos os professores da Unidade Acadêmica de Física da UFCG que contribuíram com a minha formação profissional.
- A Shimenny Ludmilla por ser minha companheira sempre que precisei.
- A Emilio Lucena, Aubery, Elialdo Andriola, Paulo Ribeiro Junior, Pablo Sampaio, Jardel Lucena, Neymar Nepomuceno, Camilla dos Santos, Jean Spinelly, José Fideles Filho, José Wagner por contribuírem com minha vida acadêmica e pessoal.
- Aos meus familiares pelo apoio, confiança e incentivo.
- Aos colegas da Pós-Graduação e funcionários da Unidade Acadêmica de Física pela grata convivência durante a minha permanência nesta Unidade.
- À CAPES/REUNE por suporte financeiro
- A todos que direta ou indiretamente possibilitaram a conclusão deste trabalho.

---

---

## Resumo

---

A Computação e a Criptografia Quântica têm sido campo de intenso estudo nas últimas décadas. Contribuíram para isso o surgimento de esquemas para correção de erros através de códigos quânticos e procedimentos para construção de portas quânticas tolerantes a falhas. Também a utilização de espaços de estados quânticos arbitrários maiores que dois (qubit), têm recentemente se mostrado relevante para diminuição do custo na implementação em sistemas físicos de portas quânticas universais [1]. O teleporte quântico é uma técnica usada para deslocar estados quânticos de um lugar para outro, sem a necessidade de transmitir o sistema quântico que armazena a informação. Pode-se mostrar que esse procedimento constitui um ingrediente básico na construção de esquemas para proteção de erros. Assim o teleporte quântico surge como um recurso fundamental na área da comunicação quântica segura, e sua aplicabilidade, têm destaque na Teoria da Informação Quântica, nas áreas da Criptografia, Comunicação e Computação. O objetivo principal desse trabalho foi apresentar um esquema utilizando o teleporte quântico de dois qudits na construção de uma lógica clássica capaz de proteger portas quânticas generalizadas ( $dG_{xor}$ ) contra falhas, ou seja, contra eventuais erros de operações. Para esse fim, utilizam-se estados quânticos arbitrários (qudits) pertencentes ao espaço de Hilbert  $d$ -dimensional. O estudo teórico do espaço  $d$ -dimensional ( $d > 2$ ) tem se mostrado útil na construção de esquemas de codificação quântica de correção de erros. O esquema proposto aqui é uma generalização daquele apresentado por [2], o qual utiliza o teleporte quântico de dois qubits para construir uma porta quântica (C-NOT) tolerante a falhas operacionais.

**Palavras-chave:** Teoria da Informação e Computação Quântica, Portas quânticas, Teleporte quântico, qudits.

---

---

## Abstract

---

Computing and quantum cryptography field have been of intense study in recent decades. Contributed to the emergence of schemes for error correction via quantum codes and procedures for building fault-tolerant quantum gates. Also the use of arbitrary quantum state space larger than two (qubit), have recently been shown to be relevant to the implementation of cost reduction in physical systems of universal quantum gates [1]. The quantum teleportation is a technique used to move quantum states from one place to another without the need for transmission system storing quantum information. It can be shown that this procedure is a basic ingredient in the construction of schemes for error protection. Thus quantum teleportation arises as a key resource in the field of secure quantum communication, and their applicability, are featured in Quantum Information Theory in the areas of Cryptography, Communication and Computing. The main objective of this paper is to present a quantum teleportation scheme using two qudits in the construction of a classical logic capable of protecting generalized quantum gates (dGxor) fail, or operations against possible errors. To this end use is arbitrary quantum states (qudits) belonging to the Hilbert space d-dimensional. The theoretical study of d-dimensional space ( $d > 2$ ) has proven useful in the construction of encoding schemes for quantum error correction. The scheme proposed here is a generalization of that presented by [2], which uses quantum teleportation two qubits to construct a quantum gate (C-NOT) fault-tolerant operations.

**Keywords:** Information Theory and Quantum Computing, Quantum Gates, Quantum Teleportation , Qudits.

---

---

# Sumário

---

<b>1</b>	<b>Introdução</b>	<b>1</b>
<b>2</b>	<b>Representação dos qubits e qudits, e das portas lógicas quânticas</b>	<b>4</b>
2.1	Introdução . . . . .	4
2.2	Qubits ou estados quânticos . . . . .	5
2.3	Qudits ou estados quânticos d-dimensional . . . . .	7
2.4	Portas quântica sobre qubits . . . . .	7
2.4.1	Porta de um qubit . . . . .	8
2.4.2	Porta de dois qubits . . . . .	9
2.4.3	Porta de três qubits . . . . .	12
2.5	Portas quântica sobre qudits . . . . .	13
2.5.1	A ação da porta ${}_dX$ . . . . .	14
2.5.2	A ação da porta ${}_dZ$ . . . . .	15
2.5.3	A ação da porta Hadamard generalizada - ${}_dF$ . . . . .	15
2.5.4	A ação da porta ${}_dG_{xor}$ . . . . .	16
2.6	Conclusões . . . . .	17
<b>3</b>	<b>Teleporte de estados quânticos</b>	<b>18</b>
3.1	Introdução . . . . .	18
3.2	Teleporte Quântico . . . . .	19
3.2.1	Descrição matemática do teleporte quântico de qubits . . . . .	19
3.2.2	Descrição matemática do teleporte quântico de qudits . . . . .	22
3.3	Exemplo . . . . .	24
3.4	Conclusões . . . . .	26
<b>4</b>	<b>Aplicação do Teleporte Quântico</b>	<b>27</b>
4.1	Introdução . . . . .	27
4.2	Aplicação do teleporte quântico para correções de erros das portas quânticas CNOT . . . . .	28
4.3	Exemplo . . . . .	31

---

4.4	Aplicação do teleporte quântico para correções de erros das portas quânticas generalizadas ( $dG_{xor}$ ) . . . . .	32
4.5	Exemplo . . . . .	36
4.6	Conclusões . . . . .	40
<b>5</b>	<b>Considerações Finais</b>	<b>41</b>
	<b>Referências Bibliográficas</b>	<b>42</b>
<b>A</b>	<b>Noções de aritmética modular</b>	<b>45</b>
A.1	Introdução . . . . .	45
A.2	Noções básicas . . . . .	45
A.3	Congruência modular . . . . .	46
A.4	Conclusão . . . . .	48
<b>B</b>	<b>Breve Introdução a Algebra e Notação da Mecânica Quântica</b>	<b>49</b>
B.1	Estados . . . . .	49
B.2	Espaço de Hilbert . . . . .	<del>49</del>
B.3	Sistemas Compostos . . . . .	<del>51</del>
B.4	Conclusão . . . . .	52

---

---

# Lista de Figuras

---

2.1	Representação de um q-bit na esfera de Bloch. . . . .	6
2.2	Simbolo gráfico das portas lógicas quântica NOT ou (X), Hadamard (H) e a troca de fase (Z) de um q-bit. . . . .	9
2.3	Simbolo gráfico da porta lógica quântica CNOT a dois qubit, em que o $ A\rangle$ representa o qubit de controle e $ B\rangle$ o alvo. . . . .	10
2.4	Simbolo gráfico da porta lógica quântica (S) de dois q-bit. . . . .	12
2.5	Simbolo gráfico da porta lógica quântica Toffoli de três qubits. . . . .	13
3.1	Circuito quântico que representa teleporte de um qubit. As duas linhas de cima representam o sistema de Alice, e a de baixo o sistema de Bob. . . . .	19
3.2	Circuito quântico é formado por uma porta Hadamard seguida por uma CNOT para criar estados de Bell. . . . .	20
3.3	Circuito quântico representando uma medição na base de Bell. A direita é mostrado um circuito quântico alternativo, representando uma medida na base de Bell . . . . .	20
3.4	Circuito quântico que representa teleporte de um qudit. As duas linhas de cima representam o sistema de Alice, e a de baixo o sistema de Bob. . . . .	22
3.5	Circuito quântico é formado por uma porta quântica de Fourier ( ${}_dF$ ) seguida por uma ( ${}_dG_{xor}$ ) para criar estados de Bell. . . . .	23
3.6	Circuito quântico para criar estados de Bell generalizados. . . . .	23
4.1	Essa figura ilustra um erro no primeiro qubit ocorrendo antes da aplicação da porta CNOT. . . . .	27
4.2	Essa figura ilustra a propagação do erro ocorrido na figura anterior para os dois qubits. . . . .	27
4.3	Circuito para teleportar os estados $\alpha_0  0\rangle + \alpha_1  1\rangle$ e $\gamma_0  0\rangle + \gamma_1  1\rangle$ . . . . .	28
4.4	A implementação de uma porta CNOT entre o par de estados teleportado, onde atua em uma parte como bit de controle e no outro como bit alvo. . . . .	29
4.5	A implementação de uma par de portas CNOT adicionados no circuito entre o par de estados teleportado. . . . .	29
4.6	O par de portas CNOT removido depois da modificação da lógica clássica controlando as aplicações das portas X e Z. . . . .	30

---

4.7	Aplicação da porta CNOT entre os dois qubits em uma computação quântica, sem o risco de destruir o estado dos dois qubits se a porta C-NOT falhar. . . . .	30
4.8	Circuito para teleportar dois estados quânticos generalizados $ \psi\rangle$ e $ \varphi\rangle$ . . . . .	33
4.9	A implementação de uma porta ${}_dG_{xor}$ entre o par de qudits, onde atua em uma parte como bit de controle e no outro como bit alvo. . . . .	33
4.10	Um par de porta ${}_dG_{xor}$ adicionados no circuito que não causa nenhum efeito. . . . .	34
4.11	O par de portas ${}_dG_{xor}$ removido depois da modificação da lógica clássica controlando as aplicações das portas ${}_dX$ e ${}_dZ$ . . . . .	35
4.12	Aplicação da porta ${}_dG_{xor}$ entre os dois qudits em uma computação quântica, sem o risco de destruir o estado dos dois qudits se a porta quântica ${}_dG_{xor}$ falhar. . . . .	35

---

---

# Lista de Símbolos

---

$\mathbb{C}$  Conjunto dos números complexos

$\mathbb{Z}$  Conjunto dos números inteiros

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

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

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

$\perp$  Ortogonalidade entre vetores

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

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

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

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

$\mathcal{H}$  Espaço de Hilbert

$i$  Unidade imaginária,  $\sqrt{-1}$

$\oplus$  Soma módulo dois, e.g.,  $a \oplus b \equiv a + b \pmod{2}$

$\ominus$  Subtração módulo dois, e.g.,  $a \ominus b \equiv a - b \pmod{2}$

$\oplus$  Soma módulo dimensional, e.g.,  $a \oplus b \equiv a + b \pmod{d}$

$\ominus$  Subtração módulo dimensional, e.g.,  $a \ominus b \equiv a - b \pmod{d}$

$d$  Representa a dimensão.

## CAPÍTULO 1

---

# Introdução

---

A informação tem como definição a ação e o efeito de informar, que, na linguagem escolástica, é dar uma forma a uma matéria [3]. Emprega-se também na linguagem comum, para indicar o ato pelo qual se faz conhecer alguma coisa a alguém [4]. Este ato, estudado pelas tradicionais áreas da informação e computação, sofreu uma revolução na década de 80, quando físicos, em colaboração com cientistas destas áreas, propuseram a utilização da teoria quântica para o armazenamento, a transmissão e a codificação de informação. O resultado destes estudos foi o surgimento de duas novas áreas interdisciplinares, nomeadas informação e computação quânticas, que estão atualmente em expansão [5].

A diferença fundamental entre a tradicional teoria da informação e a informação quântica, que é uma intensa área de pesquisa na qual se combinam teoria da informação e mecânica quântica, no qual a idéia principal é aplicar as leis quânticas para manipular a informação de forma mais eficiente, é devido ao uso do princípio da superposição quântico, aplicado a um ou mais sistemas físicos, para a codificação da informação. Enquanto esta era anteriormente codificada em bits, que são entidades discretas e binárias, nos sistemas quânticos toda a informação é codificada no estado quântico do sistema conhecido como qubit, que geralmente pode ser escrito como uma superposição dos elementos de uma base do espaço vetorial que o contém, ou seja, num espaço de Hilbert de dimensão 2.

A partir do princípio de superposição aplicado a sistemas simples e compostos, protocolos de transmissão de informação criptografada [6], e algoritmos de computação paralela [7] foram propostos, assim como a realização de redes quânticas de comunicação [8]. Neste contexto, um dos mais importantes protocolos de informação desenvolvidos foi o teleporte quântico [9].

A importância do protocolo de teleporte se dá tanto no âmbito fundamental como no das aplicações. No âmbito fundamental, o protocolo demonstra que correlações quânticas acrescentadas de comunicação clássica constituem um recurso poderoso, pois ele permite a transmissão de informação quântica de um lugar a outro sem o transporte da matéria. No entanto, entender a natureza dessas correlações quânticas se tornou uma tarefa fundamental [10]. Por outro lado, o teleporte quântico tem sido aplicado nas redes de transmissão de informação criptografada,

que poderão ser entendidas a longas distâncias via repetidores quânticos [11], e na arquitetura e comunicação de computadores quânticos [12].

Nos últimos anos o protocolo de teleporte quântico foi verificado experimentalmente em sistemas fotônicos [13], em íons aprisionados [14], em sistemas de ressonância nuclear magnética [15]. O protocolo foi também realizado a longas distâncias, onde cientistas austríacos conseguiram teleportar informação quântica por cabos de fibra óptica de 800 metros de comprimento, cruzando transversalmente um canal do rio Danúbio e cobrindo uma distância de 600 metros em linha reta [16]. Transferir o estado quântico de uma partícula para outra, como revela a experiência dos investigadores austríacos, é o mesmo que transmitir dados (quânticos) entre dois pontos.

O domínio do teleporte quântico tem se tornado uma peça fundamental na teoria da computação quântica, que promete converter os computadores atuais em arcaicos, ou seja, substituir os microprocessadores atuais que operam por transmissão elétrica por computadores quânticos, que poderiam ser milhões de vezes mais rápidos. Estes computadores permitiriam analisar sistemas complexos e concluir de forma rápida os cálculos que hoje demoram dias. No âmbito das aplicações temos o conhecimento das moléculas de ADN, sistemas extremamente complexos. Os resultados poderiam ser utilizados, por exemplo, no campo da engenharia genética e medicina. Outra das aplicações seria a transmissão de dados cem por cento segura. Por exemplo, ao enviar o número do cartão de crédito pela Internet, os dados seriam teleportados diretamente para o destino, sem possibilidade de interceptação das informações. Outra aplicação notável e interessante do teleporte é em circuitos quânticos, pois na implementação de circuitos quânticos em geral temos acesso a um conjunto de portas lógicas quânticas, onde tal conjunto inclui sempre pelo menos portas que atuam sobre dois qubits, como por exemplo uma porta C-NOT, sendo que essas portas podem falhar na sua ação sobre os qubits, logo, o estados dos qubits em que ela estava agindo serão corrompidos, portanto, sem alguma forma de correção de erro, isso levaria a um resultado não confiável do cálculo. Uma maneira da aplicação da porta quântica sem a ocorrência de falhas é por meio da utilização do protocolo de teleporte onde podemos fazer uma aplicação não destrutiva das portas quânticas de qubits, logo, os estado quânticos não seriam corrompidos como foi proposto por [2], portanto, obteríamos informações confiáveis por meio da ação das portas quânticas utilizadas no circuito. Diante de tantos fatos, o teleporte se torna uma grande conquista tecnológica, que vem abrir novos caminhos e descobertas em várias áreas da computação quântica.

Sabemos que o processamento de informação quântica é frequentemente descrito como uma série de operações unitárias e de medidas em algum sistema físico. Imperfeições nestas operações e interações com o meio ambiente circundante são inevitáveis tanto no processamento de informação clássica quanto quântica. O acúmulo de erros será prejudicial em qualquer processamento de informação de larga escala.

Portanto, para que a computação quântica funcione na prática, tem-se um grande obstáculo a superar: proteger a informação quântica de erros. Sem esta proteção, por exemplo, o

computador quântico certamente irá falhar. Qualquer estratégia efetiva para impedir que erros ocorram em um computador quântico deve proteger contra pequenos erros unitários em um circuito quântico, bem como contra erros de descoerência (causado pela interação do sistema quântico com o ambiente).

Esse trabalho tem como objetivo principal propor uma aplicação do protocolo de teleporte de estados quânticos arbitrários generalizados, ou seja, qudits, no espaço de Hilbert  $\mathcal{H}$  de dimensão- $d$ , onde podemos fazer uso das portas quânticas generalizadas ( ${}_dG_{xor}$ ) sem correr o risco da informação ser corrompida devido a erros. A relevância desse trabalho, está no sentido de que se um dia o computador quântico vier se concretizar com a utilização de qubits, o mesmo poderar ser melhorado com a utilização de qudits, ou seja, poderiam acelerar algumas operações em um computador quântico de maneira segura.

Este trabalho está organizado em cinco capítulos e um apêndice. O capítulo 2 introduz alguns conceitos e definições dos qubits, qudits, das portas lógicas quânticas atuando sobre qubits e das portas quânticas generalizadas atuando sobre os qudits. No capítulo 3 faremos uma abordagem do teleporte quântico com as respectivas descrições matemáticas sobre qubits e qudits e em seguida exemplificando-os. No capítulo 4 apresentaremos o esquema proposto por [2] e em seguida o esquema da aplicação do teleporte quântico para assegurar a confiabilidade das portas quânticas generalizadas atuando sobre os qudits para termos credibilidade na informação sem a ocorrência de erros. E por fim, o capítulo 5 apresentaremos as devidas conclusões do trabalho.

## CAPÍTULO 2

---

# Representação dos qubits e qudits, e das portas lógicas quânticas

---

Nesse capítulo iremos revisar os conceitos de bit quântico ou qubit e a sua generalização (qudit), que é um estado quântico arbitrário num espaço de Hilbert  $d$ -dimensional. Iremos também revisar os conceitos das portas lógicas quânticas atuando sobre qubits e qudits com suas respectivas ações.

### 2.1 Introdução

Um bit quântico, ou qubit é uma unidade de informação quântica, ou seja, é um estado quântico em um espaço de Hilbert ( $\mathcal{H}$ ) de dimensão 2, sendo que, esta informação é descrita por um vetor de estado em um sistema quântico de dois níveis o qual é normalmente equivalente a um vetor de espaço bidimensional sobre os números complexos. Benjamin Schumacher descobriu uma maneira de interpretar estados quânticos como informação. Ele apresentou um forma de comprimir a informação em um estado, e armazenar esta em um número menor de estados. Isto é agora conhecido por compressão Schumacher. Nos agradecimentos de seu paper [17], Schumacher afirma que o termo qubit foi inventado como um gracejo, durante suas conversas com Bill Wootters. A computação quântica trabalha com estados quânticos em vez de estados clássicos utilizados na computação clássica. O bit e os transistores como são utilizados na computação clássica são substituídos pelos bit quântico ou qubit e os átomos, e os valores dos números binários 0 e 1 são substituídos pelos vetores  $|0\rangle$  e  $|1\rangle$ .

Uma generalização dos qubits é o qudit, em vez de trabalharmos agora com um estado quântico em um espaço de Hilbert de dimensão 2, trabalhamos com um estado quântico arbitrário em um espaço de Hilbert de dimensão- $d$ . Para a computação quântica a física de um qudit é mais rica<sup>1</sup> do que a de um único qubit, pois o qudit possibilita guardar simultaneamente até cinco informações em vez de duas, isso é possível porque ele possui mais graus de liberdade

---

<sup>1</sup>Porque o qudit é o equivalente quântico de uma chave de cinco posições, em vez de apenas ligado e desligado.

do que o qubit. Com o qudit é permitido explorar determinados aspectos da mecânica quântica que vão além do que pode ser observado pelos qubits.

Como os bits são usados como blocos fundamentais na construção de computadores, os qubits poderiam um dia ser usados como blocos de construção de um computador quântico, ou seja, um dispositivo que explora as leis da mecânica quântica para a realização de cálculos mais rápidos do que podem ser feitos com pedaços clássicos. Alguns pesquisadores acreditam que os qudits podem ser usados em computadores quânticos, o que poderia acelerar algumas operações em um computador quântico.

Da mesma forma que os bits representam os 0s e 1s dos computadores atuais, os qudits poderão um dia representar os 0s, 1s, 2s, 3s e 4s dos computadores quânticos. A maioria das pesquisas na computação quântica feitas até hoje têm-se focado nos sistemas de qubits, mas espera-se que os qudits possa ser mais uma ferramenta para o processamento da informação quântica.

O capítulo está organizado da seguinte forma: Nas Seções (2.2) e (2.3) representaremos os qubits e qudits matematicamente e na seção (2.4) falaremos da ação das portas lógicas quânticas sobre os qubits e na seção (2.5) a ação das portas quânticas sobre os qudits. Por fim a seção (2.6) as respectivas conclusões.

## 2.2 Qubits ou estados quânticos

Os bits clássicos também chamados de números binários podem ser substituídos pelos vetores  $|0\rangle$  e  $|1\rangle$ , que são os qubits, e podem ser representados pelas seguintes matrizes

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad e \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (2.1)$$

onde essa notação na mecânica quântica é conhecida como notação de Dirac.

A diferença entre um bit e um qubit é que um qubit genérico  $|\psi\rangle$  pode ser uma combinação linear dos vetores  $|0\rangle$  e  $|1\rangle$ , ou seja,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.2)$$

onde  $\alpha$  e  $\beta$  são números complexos. Observe que os vetores  $|0\rangle$  e  $|1\rangle$  formam uma base ortogonal  $B = \{|0\rangle, |1\rangle\}$  do espaço vetorial  $\mathbb{C}^2$ . Essa base é chamada de base computacional e o vetor  $|\psi\rangle$  é chamado de superposição dos vetores  $|0\rangle$  e  $|1\rangle$ , com amplitudes  $\alpha$  e  $\beta$ . Na mecânica quântica, o vetor é também chamado de estado, logo usaremos os dois termos com o mesmo significado. A interpretação física do qubit, na expressão (2.2), é que ele está simultaneamente nos estados  $|0\rangle$  e  $|1\rangle$ . Isso faz com que a quantidade de informação que pode ser armazenada no estado  $|\psi\rangle$  seja infinita. Entretanto, essa informação está no nível quântico. Para torná-la

acessível, no nível clássico, precisamos fazer uma medida. A mecânica quântica diz que o processo de medida altera o estado de um qubit, fazendo-o assumir o estado  $|0\rangle$ , com probabilidade  $|\alpha|^2$ , ou o estado  $|1\rangle$ , com probabilidade  $|\beta|^2$  (isso significa que os valores  $\alpha$  e  $\beta$  não podem ser conhecidos através de uma medida). Com apenas duas possibilidades,  $|0\rangle$  ou  $|1\rangle$ , temos, então,

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2.3)$$

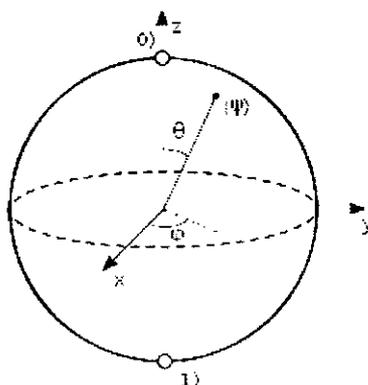
onde a medida da probabilidade deve ser sempre igual a 1.

Um qubit pode ser parametrizado podendo ser analisado como um ponto sobre a superfície de uma esfera conhecida como esfera de Bloch, usando para tanto os ângulos obtendo-se a partir de (2.2)

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \quad (2.4)$$

sendo  $\alpha = \cos\frac{\theta}{2}$  e  $\beta = e^{i\varphi}\sin\frac{\theta}{2}$ , estando assim o qubit já normalizado.

Os números  $\theta$  e  $\varphi$  definem um ponto sobre a superfície de uma esfera de raio unitário como mostrado na figura (2.1). A esfera de Bloch é bastante útil para a representação geométrica do estado de um qubit e de fundamental importância para a computação e informação quântica. Como é visto notoriamente na esfera de Bloch,  $\vec{r}$  é a representação de  $|\psi\rangle$ , logo, a projeção de  $\vec{r}$  sobre o plano  $xy$  forma um ângulo  $\varphi$  com o eixo  $x$  e o  $\theta$  é o ângulo de  $\vec{r}$  com o eixo  $z$ .



**Figura 2.1** Representação de um q-bit na esfera de Bloch.

Apesar da estranheza, qubits são decididamente reais, sua existência e comportamento foram extensivamente validados por experimentos, e muitos sistemas físicos podem ser usados para se concretizar os qubits. Segundo [18] é possível realizar qubits através de duas diferentes polarizações de um fóton; do alinhamento de spin nuclear num campo magnético uniforme; ou até de dois estados de um elétron orbitando um átomo de hidrogênio.

## 2.3 Qudits ou estados quânticos d-dimensional

A base<sup>2</sup> do estado quântico arbitrário ou do qudit em um espaço de Hilbert de dimensão  $d$  é definida da seguinte maneira

$${}_d B = \{|0\rangle, |1\rangle, \dots, |d-1\rangle\} \quad (2.5)$$

Dessa maneira, um estado quântico arbitrário em um espaço de Hilbert  $d$ -dimensional é representado por

$$|{}_d \psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle \quad (2.6)$$

Sendo  $|\alpha_0|^2 + |\alpha_1|^2 + \dots + |\alpha_{d-1}|^2 = 1$ , sendo a condição de normalização do estado  $|{}_d \psi\rangle$ .

A codificação em maior espaço de Hilbert (cuja lógica dos estados básicos são chamados de qudits em analogia com qubits bidimensional) apresenta várias vantagens tanto para as aplicações de Informação Quântica, onde sua utilização mostra uma maior segurança no campo do protocolo de distribuições de chaves criptografadas que é de bastante interesse na sociedade atual, baseada em uma rede de comunicação generalizada, quanto para estudos sobre Fundamentos da Mecânica Quântica, nomeadamente em relação aos estudos sobre o realismo local [19]. Experimentos utilizando qudits já foram concretizadas por meio de um circuito supercondutor, funcionando em temperaturas criogênicas como mostrado em [20], no campo da óptica quântica como pode ser visto em [19] e na eficiência de portas toffoli reduzindo o número de portas para a sua construção [1].

## 2.4 Portas quântica sobre qubits

Em 1995, Barenco et.al., [21], demonstraram que, analogamente ao que ocorre em um computador clássico, no modelo de computador quântico qualquer, a ação computacional pode ser implementada a partir de portas elementares. Um conjunto de portas pode ser usado para realizar a computação de uma função arbitrária. Esse conjunto é chamado de conjunto universal ou simplesmente portas universais. A universalidade na computação quântica significa que uma operação unitária qualquer pode ser aproximada com precisão, a partir de um conjunto infinito de portas, envolvendo as portas universais. As portas (CNOT, Hadamard, Fase,  $\pi/8$ ) formam um conjunto universal para a computação quântica, outro conjunto universal é (Hadamard, fase, CNOT, Toffoli). Por outro lado, existem diferenças entre as portas clássicas e quânticas, sendo a principal delas o fato de que certas operações clássicas, como por exemplo a AND ou a OR, são

<sup>2</sup>Na notação utilizada o sobrescrito a esquerda representa a dimensão de um estado ou porta quântica.

irreversíveis, ao passo que as operações quânticas são sempre reversíveis, pois estão associadas a transformações unitárias.

### 2.4.1 Porta de um qubit

Começaremos pela porta lógica mais simples, que é a porta NOT simbolizada por  $X$ , onde essa porta lógica quântica atua sobre um único qubit trocando seu estado, ou seja:

$$X |0\rangle = |1\rangle \quad X |1\rangle = |0\rangle \quad (2.7)$$

A partir dessa definição obtem-se a matriz de  $X$ , na base computacional  $\{|0\rangle, |1\rangle\}$ , ou seja:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2.8)$$

Onde observamos que a matriz  $X$  é a componente  $x$  das matrizes de Pauli.

Outra operação sobre o estado de 1 qubit é a troca de fase representada por  $Z$ , sendo  $Z$  a componente  $z$  das matrizes de Pauli, ou seja:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (2.9)$$

Sendo que a porta  $Z$  troca a fase do estado  $|1\rangle$  de 180 graus ( $e^{i\pi} = -1$ ):  $Z |1\rangle = -|1\rangle$ , ao passo que sua atuação sobre  $|0\rangle$  o deixa neutro.

A porta Hadamard, representada por  $H$ , cria superposições de estados quânticos. Sua atuação sobre os auto-estados da base computacional, e sua matriz representativa, são:

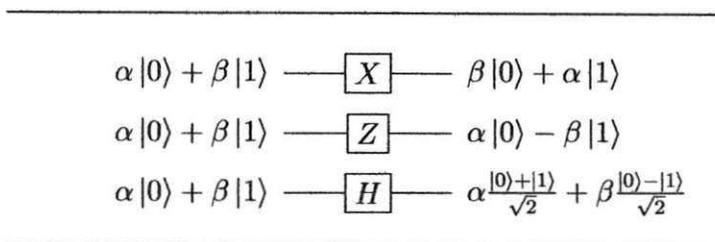
$$H |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad e \quad H |1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (2.10)$$

Na forma matricial, temos:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2.11)$$

Esta porta é algumas vezes denominada de raiz quadrada da porta NOT, sendo que é fácil mostrar que  $H^2$  não é uma porta NOT, e sim, que  $H^2 = I$ , portanto, aplicando  $H$  duas vezes não altera o estado. Essa porta tem um significado chave na lógica dos circuitos quântico. Os estados  $|0\rangle$  e  $|1\rangle$  que são perfeitamente distinguíveis (pois são ortogonais no espaço de Hilbert) são levados em superposições  $|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$  e  $|1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ .

A representação dos circuitos das porta lógicas quânticas de um qubit estão mostrados na figura (2.2).



**Figura 2.2** Símbolo gráfico das portas lógicas quântica NOT ou (X), Hadamard (H) e a troca de fase (Z) de um q-bit.

A porta  $T$  ou porta  $(\pi/8)$  atua também em um único qubit e a sua matriz unitária é representada da seguinte maneira:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix} \tag{2.12}$$

que poderia ser representada também da seguinte forma:

$$T = \exp(-i\pi/8) \begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix} \tag{2.13}$$

Aplicando-se  $T$  em um estado genérico,

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{2.14}$$

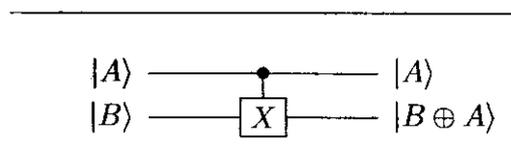
Obtem-se,

$$T |\psi\rangle = \alpha |0\rangle + \exp(i\pi/8)\beta |1\rangle \tag{2.15}$$

Também, nesse caso, se for feita uma medida do estado  $T |\psi\rangle$ , as probabilidades de se obter os estados  $|0\rangle$  ou  $|1\rangle$  serão as mesmas, comparadas com uma medida realizada sobre o estado  $|\psi\rangle$ .

### 2.4.2 Porta de dois qubits

A porta XOR também conhecida como CNOT (ou NOT controlada) que atua sobre dois qubits é representada na figura (2.3). Esta porta modifica o estado de um dos qubits, o chamado de qubit alvo, de forma condicionada ao estado do outro, chamado de qubit de controle. Se o estado do qubit de controle for 0, o qubit alvo é mantido; caso contrário, o estado do qubit alvo é trocado.



**Figura 2.3** Símbolo gráfico da porta lógica quântica CNOT a dois qubit, em que o  $|A\rangle$  representa o qubit de controle e  $|B\rangle$  o alvo.

Antes, porém, de definirmos a matriz XOR ou CNOT, é necessário definirmos a base computacional formada pelos auto-estados para dois q-bits.<sup>3</sup> O espaço de Hilbert de dois qubits é expandido pelos vetores formados pelo produto tensorial:

$$\{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\} \tag{2.16}$$

A representação matricial de cada um desses vetores da base computacional de dois qubits é

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}; |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}; |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}; |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \tag{2.17}$$

A aplicação da  $XOR_A$  (XOR com qubit de controle em A) sobre os estados da base computacional produz:

$$XOR_A |00\rangle = |00\rangle \tag{2.18}$$

$$XOR_A |01\rangle = |01\rangle \tag{2.19}$$

$$XOR_A |10\rangle = |11\rangle \tag{2.20}$$

$$XOR_A |11\rangle = |10\rangle \tag{2.21}$$

Sendo assim, a matriz  $XOR_A$  representada por:

$$XOR_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.22}$$

<sup>3</sup>vamos definir aqui a notação  $|0\rangle \otimes |0\rangle = |00\rangle$ .

De forma analoga, podemos definir os efeitos da porta  $XOR_B$  sobre os estados da base computacional, ou seja:

$$XOR_B |00\rangle = |00\rangle \quad (2.23)$$

$$XOR_B |01\rangle = |11\rangle \quad (2.24)$$

$$XOR_B |10\rangle = |10\rangle \quad (2.25)$$

$$XOR_B |11\rangle = |01\rangle \quad (2.26)$$

Logo, a matriz  $XOR_B$  será representada por:

$$XOR_B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad (2.27)$$

A operação ou transformação de Hadamard, no caso de dois qubits, é representada por:

$$H = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (2.28)$$

$H$  cria superposições uniformes de autoestados. Aplicada ao estado  $|00\rangle$ , por exemplo, obtemos:

$$H = \frac{1}{2} [|00\rangle + |01\rangle + |10\rangle + |11\rangle] \quad (2.29)$$

Generalizando para estados com  $n$  qubits, obtemos:

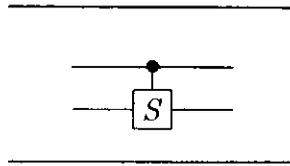
$$H^{\otimes n} |0\dots 0\rangle = (H |0\rangle)^{\otimes n} \quad (2.30)$$

$$H^{\otimes n} |0\dots 0\rangle = \left[ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right]^{\otimes n} \quad (2.31)$$

$$H^{\otimes n} |0\dots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \quad (2.32)$$

Uma seqüência de operações aplicadas sobre estados quânticos é chamada de circuito quântico.

A porta de Fase controlada ou porta ( $S$ ) é também uma porta de dois qubits e é representada simbolicamente pela figura (2.4) a seguir:



**Figura 2.4** Símbolo gráfico da porta lógica quântica ( $S$ ) de dois q-bit.

A matriz unitária associada à porta  $S$  é representada por:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad (2.33)$$

onde  $i$  é a unidade imaginária ( $i^2 = -1$ ). Podemos representar a porta  $S$  da seguinte maneira:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/2) \end{bmatrix} \quad (2.34)$$

Sabemos que  $\exp(i\pi/2) = \cos(\pi/2) + i\sin(\pi/2) = i$ . Logo, aplicando a porta ( $S$ ) em um estado genérico, temos:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.35)$$

Obteremos:

$$S|\psi\rangle = \alpha|0\rangle + i\beta|1\rangle \quad (2.36)$$

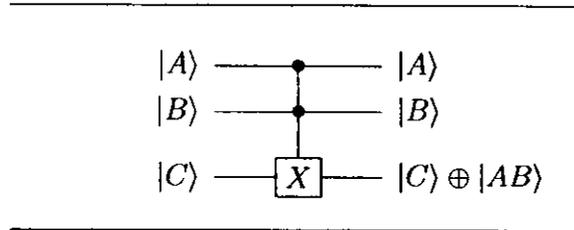
Note que, se for feita uma medida do estado  $S|\psi\rangle$ , as probabilidades de se obter os estados  $|0\rangle$  ou  $|1\rangle$  serão as mesmas, comparadas com uma medida realizada sobre o estado  $|\psi\rangle$ . Isso não acontece, por exemplo, usando a porta  $H$ .

### 2.4.3 Porta de três qubits

A porta quântica Toffoli tem três qubits de entrada e três de saída assim como na porta toffoli clássica<sup>4</sup> como mostra a figura (2.5)

Os dois primeiros qubits  $|A\rangle$  e  $|B\rangle$  são chamados de qubits de controle e não são afetados pela ação da porta, e o qubit  $|C\rangle$  é chamado de qubit alvo e seu estado é mudado somente se os dois qubits de controle forem  $|1\rangle$ . É notório que se aplicarmos a porta Toffoli duas vezes em um dado conjunto de qubits observaremos que ela é uma porta reversível.

<sup>4</sup>É uma porta que simula as portas clássicas NOT e AND, contendo dois bits de entrada (controle) e um bit de saída (alvo), onde o bit alvo só muda seu estado se os bits de entrada forem iguais a 1.



**Figura 2.5** Símbolo gráfico da porta lógica quântica Toffoli de três qubits.

Por definição, a implementação da porta quântica Toffoli permuta os estados da base computacional da mesma forma que no caso clássico. Por exemplo, a porta Toffoli atuando no estado  $|110\rangle$  retorna o estado  $|111\rangle$ .

A representação matricial da porta Toffoli para qubits em um espaço espaço de Hilbert de dimensão 2 é um pouco laborioso de se obter (mas não difícil), logo podemos representar da seguinte maneira:

$$U_{tof} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (2.37)$$

Uma propriedade interessante da porta Toffoli quântica é que ela pode ser usada para simular portas lógicas clássicas irreversíveis, da mesma forma da porta Toffoli clássica, e isso garante que os computadores quânticos são capazes de relizar qualquer operação que possa ser feita por um computador clássico (determinístico) [5].

## 2.5 Portas quântica sobre qudits

É natural a intenção de generalizar as portas quânticas conhecidas para qubits à espaços de Hilbert de dimensão  $d > 2$ . De fato, muitos dos sistemas físicos que suportam a representação dos qubits, como átomos ou íons de multi-níveis, interferômetros com vários “braços”, também permitem a consideração de qudits [22, 23].

Como já vimos a representação dos qudits, nosso objetivo agora é descrever a ação das portas quânticas sobre eles, no entanto, serão estudadas as portas integrantes na aplicação do teleporte quântico utilizando qudits, são elas:

- ${}_dX, {}_dZ$ : São portas conhecidas, que juntamente com  ${}_dY$  e  ${}_dI$  formam o grupo de Pauli.
- ${}_dF$ : A porta que representa a transformada de Fourier quântica e desempenha para o caso geral o papel que a Hadamard desempenha no caso bidimensional.
- ${}_dG_{XOR}$ : A porta que generaliza para o caso d-dimensional o papel da CNOT no caso bidimensional.

Pode-se encontrar outras maneiras de chegar a resultados da generalização das portas quânticas, como pode ser visto em [24], mas iremos utilizar a abordagem apresentada em [25, 26].

### 2.5.1 A ação da porta ${}_dX$

A porta  ${}_dX$  quando atuando sobre qubits ( $d = 2$ ) pode ser descrita como uma operação de soma módulo 2, onde é conhecida por inverter o bit de entrada, sendo também chamada de bit-flip. Portanto, para o caso mais geral, ou seja, o caso d-dimensional essa propriedade não se mantém. A expressão para o caso generalizado é dado por

$${}_dX |i\rangle = |(i + 1) \bmod d\rangle \quad (2.38)$$

Observamos que a ação, na base computacional para o caso mais geral, é levar o estado de entrada ao estado da base a sua direita ou retornar ao início, se o estado de entrada for o último da base. Tal comportamento mostra que o bit-flip observado na dimensão 2 é um caso específico de um comportamento mais geral chamado right shift bit. Para compreendermos melhor a ação da porta  ${}_dX$ , observemos uma aplicação para a dimensão 3, logo a ação de  ${}_3X$  nos estados da base computacional vai ser:

$${}_3X |0\rangle = |1\rangle, \quad {}_3X |1\rangle = |2\rangle, \quad {}_3X |2\rangle = |0\rangle \quad (2.39)$$

A representação matricial da porta  ${}_dX$  é dada pela seguinte expressão

$$a_{mn} = \begin{cases} 1, & \text{se } m = (n + 1) \bmod d \\ 0, & \text{caso contrário} \end{cases} \quad (2.40)$$

Usando esse procedimento para as dimensões 2, 3 e 4 dá origem as seguintes matrizes

$${}_2X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad {}_3X = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad {}_4X = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

### 2.5.2 A ação da porta ${}_dZ$

Para o caso bidimensional a porta  ${}_dZ$ , também conhecida por “troca de fase”, tem como ação inverter a fase do qubit de entrada. A expressão que representa a ação da porta  ${}_dZ$  em um estado da base canônica é

$${}_dZ |j\rangle = (e^{(2\pi i/d)})^j |j\rangle. \quad (2.41)$$

Onde daqui por diante chamaremos  $\omega = e^{(2\pi i/d)}$ .

Para o caso de  $d = 3$ , temos:

$${}_3Z |0\rangle = \omega^0 |0\rangle = |0\rangle, \quad (2.42)$$

$${}_3Z |1\rangle = \omega^1 |1\rangle = \omega |1\rangle, \quad (2.43)$$

$${}_3Z |2\rangle = \omega^2 |2\rangle = \omega^{-1} |2\rangle. \quad (2.44)$$

A representação matricial da porta  ${}_dZ$  é dada pela expressão

$$a_{mn} = \begin{cases} \omega^{m-1} & \text{se } m = n \\ 0 & \text{se } m \neq n \end{cases} \quad (2.45)$$

Usando esse procedimento para as dimensões 2, 3 e 4 dá origem as seguintes matrizes

$${}_2Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad {}_3Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & (\sqrt{3}i - 1)/2 & 0 \\ 0 & 0 & -(\sqrt{3}i + 1)/2 \end{bmatrix}, \quad {}_4Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{bmatrix}.$$

### 2.5.3 A ação da porta Hadamard generalizada - ${}_dF$

A porta Hadamard é um caso particular da transformada de Fourier discreta sobre um qubit em  $d = 2$ . Para dimensões arbitrárias, ou seja com dimensões maiores que 2, temos que utilizar a seguinte versão denotada por  ${}_dF$ . A ação da porta  ${}_dF$  na base computacional canônica é dada por

$${}_dF |j\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{jl} |l\rangle. \quad (2.46)$$

Outra maneira de escrever a equação 2.46 utilizando a expressão 2.41 é dada por

$${}_dF |j\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} ({}_dZ)^l |l\rangle. \quad (2.47)$$

Para o caso de  $d = 3$ , temos:

$${}_3F |0\rangle = [|0\rangle + |1\rangle + |2\rangle]/\sqrt{3}, \quad (2.48)$$

$${}_3F|1\rangle = [|0\rangle + \omega|1\rangle + \omega^2|2\rangle]/\sqrt{3}, \quad (2.49)$$

$${}_3F|2\rangle = [|0\rangle + \omega^2|1\rangle + \omega|2\rangle]/\sqrt{3}. \quad (2.50)$$

A representação matricial da porta  ${}_dF$  dada pela seguinte expressão

$$a_{mn} = \omega^{mn}/\sqrt{d} \quad (2.51)$$

Aplicando esse procedimento para as dimensões 2, 3 e 4, obtemos as seguintes matrizes

$${}_2F = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad {}_3F = \begin{bmatrix} 1 & 1 & 1 \\ 1 & (\sqrt{3}i-1)/2 & -(\sqrt{3}i+1)/2 \\ 1 & -(\sqrt{3}i+1)/2 & (\sqrt{3}i-1)/2 \end{bmatrix}, \quad {}_4F = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}.$$

### 2.5.4 A ação da porta ${}_dG_{xor}$

A generalização da porta CNOT (conhecida também por XOR) que atua em dois qubits, pode ser usada para emaranhamento e para teleporte de estados quânticos. Para qubits, a ação da porta quântica CNOT com seus estados da base computacional  $\{|i\rangle\}$  onde  $i \in \{0, 1\}$ , no espaço de Hilbert de dimensão 2 é dado por

$$CNOT|i, j\rangle = |i, i \oplus j\rangle. \quad (2.52)$$

Sendo que o primeiro (segundo) índice denota o estado de controle (alvo) do qubit e  $\oplus$  denota adição de módulo 2. Logo, a generalização da porta quântica C-NOT ( ${}_dG_{xor}$ ) deve agir em dois sistemas quânticos no espaço de Hilbert de dimensão-d, cuja definição proposta por [27] é dada por

$${}_dG_{xor}|i, j\rangle = |i, i \ominus j\rangle. \quad (2.53)$$

Algumas propriedades dessa definição pode ser vista com mais detalhes em [27], onde  $\ominus$  denota nesse caso a subtração módulo d.

A ação da porta  ${}_dG_{xor}$  na base computacional para o caso  $d = 3$  é dada por<sup>5</sup>:

$${}_3G_{xor}|00\rangle = |00\rangle, \quad {}_3G_{xor}|01\rangle = |02\rangle, \quad {}_3G_{xor}|02\rangle = |01\rangle, \quad (2.54)$$

$${}_3G_{xor}|10\rangle = |11\rangle, \quad {}_3G_{xor}|11\rangle = |10\rangle, \quad {}_3G_{xor}|12\rangle = |12\rangle, \quad (2.55)$$

$${}_3G_{xor}|20\rangle = |22\rangle, \quad {}_3G_{xor}|21\rangle = |21\rangle, \quad {}_3G_{xor}|22\rangle = |20\rangle. \quad (2.56)$$

<sup>5</sup>Nota-se que para o caso d-dimensional perde-se a noção intuitiva de que uma porta controlada pelo qudit zero não altera o qudit alvo.

A representação matricial da porta quântica  ${}_dG_{xor}$  é obtida por meio da seguinte equação

$$a_{mn} = \begin{cases} 1, & \text{se } m = [dx + (x - y) \bmod d] + 1 \forall n \in [1, d^2] \\ 0, & \text{caso contrário} \end{cases} \quad (2.57)$$

onde

$$x = (n - 1) \operatorname{div} d; \quad y = (n - 1) \bmod d. \quad (2.58)$$

Para  $d = 3$  este procedimento dá origem à seguinte matriz

$${}_3G_{xor} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

## 2.6 Conclusões

Neste capítulo foi realizada uma revisão a respeito dos qubits e qudits, e da ação das portas quânticas sobre eles. Foi apresentados também alguns exemplos das ações das portas lógicas quânticas ( ${}_dX, {}_dY, {}_dZ, {}_dF$  e  ${}_dG_{XOR}$ ) sobre os qudits e suas respectivas representações matriciais.

## CAPÍTULO 3

---

# Teleporte de estados quânticos

---

Neste capítulo são apresentados os conceitos básicos envolvidos na realização do teleporte de estados quânticos, e também uma aplicação matemática desse protocolo com a utilização de qubits e qudits.

### 3.1 Introdução

Desde que o protocolo de comunicação quântica conhecido como teleporte foi proposto por [9], o mesmo tem sido alvo de várias pesquisas, talvez por ser uma das mais intrigantes correlações não clássicas apontadas por Albert Einstein em seu artigo [28], no qual contesta a completude da Mecânica Quântica no papel de descrever a realidade física da natureza.

De maneira geral, o teleporte quântico é uma técnica usada para deslocar estados quânticos de um lugar para outro, mesmo quando não existe um canal quântico de comunicação conectando o transmissor do estado ao seu receptor. Vários trabalhos experimentais implementando o teleporte quântico já foram apresentados à comunidade científica, incluindo uso de fótons [29], ressonância magnética [15] e entre outros. Por mais interessante que uma descoberta científica tecnológica pareça ser, reside essencialmente no seu potencial de aplicabilidade, por essa razão o teleporte quântico é de fundamental importância na teoria da informação quântica, sendo aplicado nas áreas da criptografia quântica, comunicação e computação e na construção de portas quânticas.

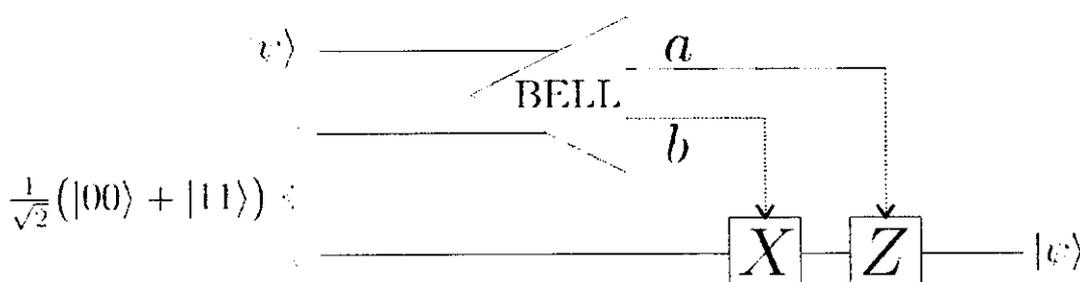
O restante do capítulo será organizado da seguinte maneira: são apresentados o circuito quântico para o teleporte e uma descrição analítica de sua execução. Aplicação do teleporte de estados arbitrários (qubit), teleporte quântico com a utilização de portas generalizadas e um exemplo do teleporte utilizando estados de qutrite. Por fim, apresentaremos as conclusões.

## 3.2 Teleporte Quântico

Podemos explicar o teleporte quântico através da literatura tradicionalmente adotada em vários livros, onde uma atividade deve ser realizada entre duas partes cooperantes, normalmente chamadas de Alice e Bob. O ponto central está na possibilidade de Alice enviar um estado quântico arbitrário, desconhecido mesmo para ela, à Bob sem que no entanto haja um portador físico entre eles. O estado quântico recebido por Bob deve ser absolutamente idêntico ao enviado por Alice. Sabendo que um estado quântico arbitrário de um sistema físico de dois níveis pode ser representado por  $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ , em que  $\alpha_0$  e  $\alpha_1$  são as amplitudes de probabilidade do estado, alguém pode pensar na possibilidade de transmissão clássica dos valores de  $\alpha_0$  e  $\alpha_1$ . Logo essa tentativa será abandonada por dois motivos, primeiro a teleportação requer uma transferência perfeita, segundo os parâmetros  $\alpha_0$  e  $\alpha_1$  são números complexos que variam em um contínuo, apenas obedecendo a relação  $|\alpha_0|^2 + |\alpha_1|^2 = 1$ . Desta maneira, transmitir os valores de  $\alpha_0$  e  $\alpha_1$  pode vir a requerer que uma quantidade infinita de informação seja enviada [5]. Para complicar ainda mais o cenário, quando não é Alice que gera  $|\psi\rangle$  as leis da mecânica quântica impedem que ela consiga conhecer com exatidão os valores de  $\alpha_0$  e  $\alpha_1$  uma vez que ela não pode copiar o estado  $|\psi\rangle$  (Teorema da não-clonagem quântica). Como pré-requisito fundamental para a realização da teleportação Alice e Bob devem compartilhar um estado de Bell e dispor de um canal clássico para troca de informação, pois, como será visto adiante, Alice necessitará enviar a Bob dois bits de informação.

### 3.2.1 Descrição matemática do teleporte quântico de qubits

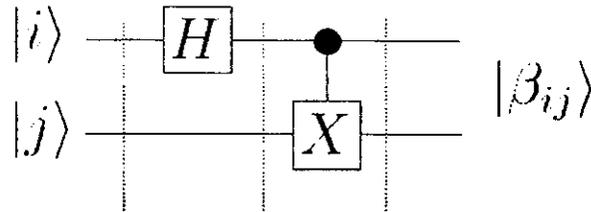
O esquema proposto por [2] mostra o circuito quântico responsável por implementar o protocolo de teleporte de qubits conforme a figura (3.2.1).



**Figura 3.1** Circuito quântico que representa teleporte de um qubit. As duas linhas de cima representam o sistema de Alice, e a de baixo o sistema de Bob.

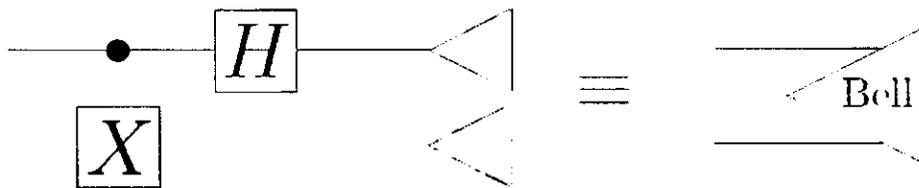
Para que o teleporte quântico funcione, Alice vai interagir o qubit  $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$  com sua parte do estado de Bell que ela compartilha com Bob, e mede seus dois qubits obtendo um dos quatro estados possíveis (00, 01, 10, 11), logo, Alice envia os dois bits de informação

para Bob, então, dependendo deles, Bob aplica a operação adequada para obter o estado teleportado por Alice. Podemos descrever matematicamente como mostra a figura (3.2.1), um circuito que implementa uma mudança de base computacional para a base de Bell da seguinte maneira



**Figura 3.2** Circuito quântico é formado por uma porta Hadamard seguida por uma CNOT para criar estados de Bell.

O circuito equivalente ao mostrado na figura (3.2.1) para construção da base de Bell é ilustrado na figura 3.2.1



**Figura 3.3** Circuito quântico representando uma medição na base de Bell. A direita é mostrado um circuito quântico alternativo, representando uma medida na base de Bell

Podemos mostrar como exemplo considerando os estados de entrada como  $|00\rangle$ , onde a porta Hadamard transforma esse estado inicial em  $(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$ , e a porta CNOT produz o estado de saída  $(|00\rangle + |11\rangle)/\sqrt{2}$ . Observe como funciona o procedimento: primeiro a transformação Hadamard coloca o qubit de cima em uma superposição; este então atua como o qubit de controle do CNOT, e o qubit alvo é invertido para o caso em que o de controle é 1. Os possíveis estados de saída

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (3.1)$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (3.2)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (3.3)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (3.4)$$

são conhecidos como estados de Bell, ou algumas vezes chamados de estados EPR (homenagem

a Einstein, Poldolsky e Rosen). Podemos escrever a notação mnemônica de  $|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle$  sintetizada na expressão

$$|\beta_{ij}\rangle = \frac{1}{\sqrt{2}} [ |0, j\rangle + (-1)^i |1, \bar{j}\rangle ] \quad (3.5)$$

em que  $\bar{j}$  é a negação de  $j$ .

Descrevendo agora o protocolo de teleporte, temos que o estado inicial do circuito mostrado na figura (3.2.1) é composto pelo estado quântico a ser teleportado  $|\psi\rangle$  e o estado de Bell

$$|\psi\rangle |\beta_{00}\rangle \quad (3.6)$$

Note que, reagrupando os qubits (mas mantendo-os na mesma ordem), este estado pode ser escrito como

$$|\psi\rangle |\beta_{00}\rangle = \frac{1}{2} |\beta_{00}\rangle |\psi\rangle + \frac{1}{2} |\beta_{01}\rangle (X |\psi\rangle) + \frac{1}{2} |\beta_{10}\rangle (Z |\psi\rangle) + \frac{1}{2} |\beta_{11}\rangle (XZ |\psi\rangle) \quad (3.7)$$

Alice faz uma medição dos dois primeiros qubits na base Bell. O estado em comum de Alice-Bob após esta medida é uma das

$$|\beta_{00}\rangle |\psi\rangle \quad (3.8)$$

$$|\beta_{01}\rangle (X |\psi\rangle) \quad (3.9)$$

$$|\beta_{10}\rangle (Z |\psi\rangle) \quad (3.10)$$

$$|\beta_{11}\rangle (XZ |\psi\rangle) \quad (3.11)$$

cada um com probabilidade de  $1/4$ . Os bits clássicos  $a$  e  $b$  resultantes da medição de Alice indica qual dos quatro estados é obtida. Alice envia esses dois bits para Bob, logo ele observa se o seu qubit é deixado no estado  $|\psi\rangle, X |\psi\rangle, Z |\psi\rangle, \text{ ou } XZ |\psi\rangle$ . Dependendo dos valores clássicos que Alice envia para Bob,  $a$  e  $b$ , Bob realiza uma das seguintes operações para transformar seu estado em  $|\psi\rangle$ .

Podemos resumir a performance de Bob da seguinte maneira

BITS: $a, b$	PORTAS	PERFORMANCE DE BOB
0, 0	$I$ :	$\alpha_0  0\rangle + \alpha_1  1\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle =  \psi\rangle$
0, 1	$X$ :	$\alpha_0  1\rangle + \alpha_1  0\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle =  \psi\rangle$
1, 0	$Z$ :	$\alpha_0  0\rangle - \alpha_1  1\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle =  \psi\rangle$
1, 1	$ZX$ :	$\alpha_0  1\rangle - \alpha_1  0\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle =  \psi\rangle$

Então, condicionalmente Bob aplica  $Z$  e  $X$  para o seu qubit, condicionado sobre os valores clássicos  $a$  e  $b$ , respectivamente. Depois desta transformação, Bob recupera o estado  $|\psi\rangle$  que Alice lhe enviou com sucesso.

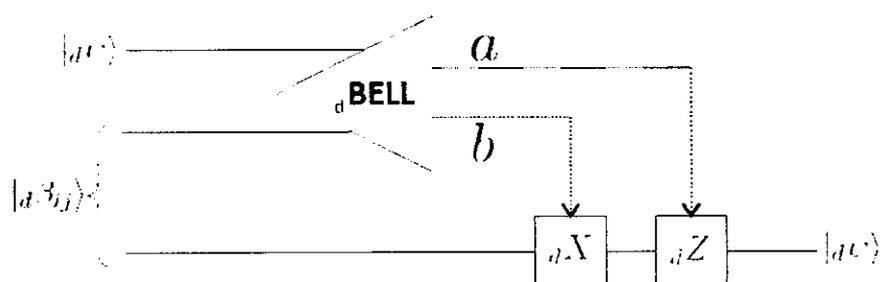
Vamos fazer uma descrição do que ainda é necessário ser feito para completar o processo. Caso Alice resolvesse não enviar os bits clássicos oriundos da medição por ela realizada seria impossível completar a teleportação com sucesso uma vez que independentemente do estado a ser teleportado, a medição na base de Bell sempre apresentará resultados equiprováveis, portanto, mesmo que Alice dispusesse de várias cópias de  $|\psi\rangle$  para repetir o processo Bob nunca conseguiria inferi-lo com certeza para o caso geral.

Essa característica garante que a teleportação não represente um paradoxo no que diz respeito à transmissão de informação acima da velocidade da luz. Como é requerida a transmissão de informação clássica, a velocidade com a qual a teleportação se realiza fica limitada à velocidade com a qual é transmitida a informação clássica participante do processo. Também se deve observar que o estado  $|\psi\rangle$  originalmente utilizado por Alice é destruído pelo processo de medição para posteriormente ser reconstruído por Bob usando sua partícula de um estado de Bell, isso assegura que a teleportação não viole o teorema da não clonagem [5].

Seguindo então o protocolo, Alice envia para Bob os dois bits clássicos obtidos com a medição dos dois primeiros qubits (a forma como essa informação é representada e enviada é completamente irrelevante para o processo). Bob, de posse de tal informação, deve agora executar uma dentre quatro possíveis operações de correção, alcançando assim em todas as hipóteses a reconstrução do estado originalmente teleportado.

### 3.2.2 Descrição matemática do teleporte quântico de qudits

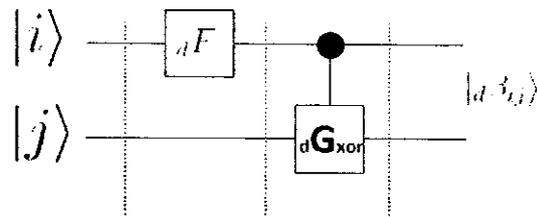
Agora iremos fazer uma generalização do teleporte quântico, onde a figura (3.2.2) mostra um esquema de circuito quântico responsável pelo teleporte de qudits.



**Figura 3.4** Circuito quântico que representa teleporte de um qudit. As duas linhas de cima representam o sistema de Alice, e a de baixo o sistema de Bob.

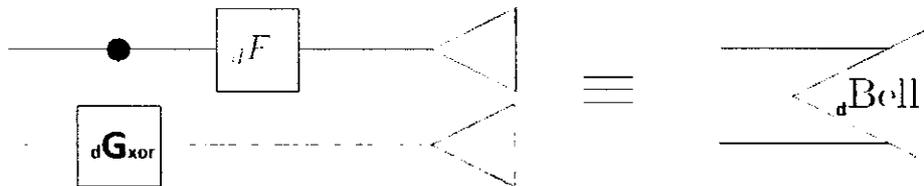
Alice agora vai interagir o seu qudit  $|a^\psi\rangle$  com sua parte do estado de Bell  $|a^{\beta_{ij}}\rangle$  generalizado que compartilha com Bob, e mede seus qudits obtendo  $n$ -estados possíveis, logo, Alice envia a informação para Bob, e, dependendo da mensagem clássica dela, ele irá realizar as várias operações na sua metade do estado de Bell generalizado, recuperando assim o estado  $|a^\psi\rangle$ .

A generalização do estado de Bell utilizando qudits pode ser obtido a partir do seguinte esquema mostrado na figura (3.2.2).



**Figura 3.5** Circuito quântico é formado por uma porta quântica de Fourier ( ${}_dF$ ) seguida por uma ( ${}_dG_{xor}$ ) para criar estados de Bell.

O circuito equivalente ao mostrado na figura (3.2.2) para construção da base de Bell generalizados é ilustrado na figura (3.2.2).



**Figura 3.6** Circuito quântico para criar estados de Bell generalizados.

Descrevendo o protocolo de teleporte para estados quânticos generalizados, temos que o estado inicial do circuito mostrado na figura (3.2.2) é composto pelo estado quântico a ser teleportado  $|{}_d\psi\rangle$  e o estado de Bell generalizado

$$|{}_d\psi\rangle |{}_d\beta_{ij}\rangle \quad (3.12)$$

Logo, podemos escrever o estado geral na base de Bell generalizada da seguinte maneira

$$|{}_d\psi\rangle |{}_d\beta_{ij}\rangle = \frac{1}{d} \sum_{a,b=0}^{d-1} |{}_d\beta_{ab}\rangle ({}_dX_a^b Z^a |{}_d\psi\rangle) \quad (3.13)$$

sendo assim, dependendo dos estados clássicos  $a$  e  $b$  enviados por Alice a Bob, ele poderá recuperar o estado  $|{}_d\psi\rangle$ .

### 3.3 Exemplo

Nesta seção iremos ilustrar matematicamente como podemos fazer o teleporte de um estado quântico (qutrite), proposto pela primeira vez por [30]. Vamos supor que Alice e Bob compartilhem o seguinte estado de Bell para um qutrite

$$|_{3}\beta_{00}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle) \quad (3.14)$$

e Alice queira enviar o seguinte estado para Bob

$$|_{3}\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle \quad (3.15)$$

O estado inicial do circuito é composto pelo estado quântico a ser teleportado e o par estado de Bell, ou seja

$$\begin{aligned} |_{3}\psi\rangle |_{3}\beta_{00}\rangle &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle) \otimes \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle) \\ &= \frac{1}{\sqrt{3}}(\alpha_0 |000\rangle + \alpha_0 |011\rangle + \alpha_0 |022\rangle + \alpha_1 |100\rangle + \alpha_1 |111\rangle + \alpha_1 |122\rangle + \\ &\quad \alpha_2 |200\rangle + \alpha_2 |211\rangle + \alpha_2 |222\rangle) \end{aligned} \quad (3.16)$$

Podemos reescrever a expressão (3.16) da seguinte maneira

$$\begin{aligned} |_{3}\psi\rangle |_{3}\beta_{00}\rangle &= \frac{1}{\sqrt{3}}(|00\rangle \otimes \alpha_0 |0\rangle + |01\rangle \otimes \alpha_0 |1\rangle + |02\rangle \otimes \alpha_0 |2\rangle + \\ &\quad |10\rangle \otimes \alpha_1 |0\rangle + |11\rangle \otimes \alpha_1 |1\rangle + |12\rangle \otimes \alpha_1 |2\rangle + |20\rangle \otimes \alpha_2 |0\rangle + \\ &\quad |21\rangle \otimes \alpha_2 |1\rangle + |22\rangle \otimes \alpha_2 |2\rangle) \end{aligned} \quad (3.17)$$

Escrevendo a expressão 3.17 na forma da base de Bell, temos

$$\begin{aligned} |_{3}\psi\rangle |_{3}\beta_{00}\rangle &= \frac{1}{3}[(|_{3}\beta_{00}\rangle + |_{3}\beta_{10}\rangle + |_{3}\beta_{20}\rangle) \otimes \alpha_0 |0\rangle + \\ &\quad (|_{3}\beta_{02}\rangle + |_{3}\beta_{12}\rangle + |_{3}\beta_{22}\rangle) \otimes \alpha_0 |1\rangle + \\ &\quad (|_{3}\beta_{01}\rangle + |_{3}\beta_{11}\rangle + |_{3}\beta_{21}\rangle) \otimes \alpha_0 |2\rangle + \\ &\quad (|_{3}\beta_{01}\rangle + \omega^2 |_{3}\beta_{11}\rangle + \omega |_{3}\beta_{21}\rangle) \otimes \alpha_1 |0\rangle + \\ &\quad (|_{3}\beta_{00}\rangle + \omega^2 |_{3}\beta_{10}\rangle + \omega |_{3}\beta_{20}\rangle) \otimes \alpha_1 |1\rangle + \\ &\quad (|_{3}\beta_{02}\rangle + \omega^2 |_{3}\beta_{12}\rangle + \omega |_{3}\beta_{22}\rangle) \otimes \alpha_1 |2\rangle + \end{aligned}$$

$$\begin{aligned}
& (|_3\beta_{02}\rangle + \omega |_3\beta_{12}\rangle + \omega^{-1} |_3\beta_{22}\rangle) \otimes \alpha_2 |0\rangle + \\
& (|_3\beta_{01}\rangle + \omega |_3\beta_{11}\rangle + \omega^{-1} |_3\beta_{21}\rangle) \otimes \alpha_2 |1\rangle + \\
& |_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle + \omega^{-1} |_3\beta_{20}\rangle) \otimes \alpha_2 |2\rangle]
\end{aligned} \tag{3.18}$$

Onde

$$|00\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + |_3\beta_{20}\rangle) \tag{3.19}$$

$$|01\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{02}\rangle + |_3\beta_{12}\rangle + |_3\beta_{22}\rangle) \tag{3.20}$$

$$|02\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{01}\rangle + |_3\beta_{11}\rangle + |_3\beta_{21}\rangle) \tag{3.21}$$

$$|10\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{01}\rangle + \omega^2 |_3\beta_{11}\rangle + \omega |_3\beta_{21}\rangle) \tag{3.22}$$

$$|11\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle + \omega |_3\beta_{20}\rangle) \tag{3.23}$$

$$|12\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{02}\rangle + \omega^2 |_3\beta_{12}\rangle + \omega |_3\beta_{22}\rangle) \tag{3.24}$$

$$|20\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{02}\rangle + \omega |_3\beta_{12}\rangle + \omega^{-1} |_3\beta_{22}\rangle) \tag{3.25}$$

$$|21\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{01}\rangle + \omega |_3\beta_{11}\rangle + \omega^{-1} |_3\beta_{21}\rangle) \tag{3.26}$$

$$|22\rangle = \frac{\sqrt{3}}{3} (|_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle + \omega^{-1} |_3\beta_{20}\rangle) \tag{3.27}$$

A expressão (3.18) pode ser reescrito da seguinte forma, após reagruparmos os termos

$$\begin{aligned}
|_3\psi\rangle |_3\beta_{00}\rangle &= \frac{1}{3} [ |_3\beta_{00}\rangle \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle) + \\
& |_3\beta_{01}\rangle \otimes (\alpha_0 |2\rangle + \alpha_1 |0\rangle + \alpha_2 |1\rangle) + \\
& |_3\beta_{02}\rangle \otimes (\alpha_0 |1\rangle + \alpha_1 |2\rangle + \alpha_2 |0\rangle) + \\
& |_3\beta_{10}\rangle \otimes (\alpha_0 |0\rangle + \omega^2 \alpha_1 |1\rangle + \omega \alpha_2 |2\rangle) + \\
& |_3\beta_{11}\rangle \otimes (\alpha_0 |2\rangle + \omega^2 \alpha_1 |0\rangle + \omega \alpha_2 |1\rangle) + \\
& |_3\beta_{12}\rangle \otimes (\alpha_0 |1\rangle + \omega^2 \alpha_1 |2\rangle + \omega \alpha_2 |0\rangle) + \\
& |_3\beta_{20}\rangle \otimes (\alpha_0 |0\rangle + \omega \alpha_1 |1\rangle + \omega^{-1} \alpha_2 |2\rangle) + \\
& |_3\beta_{21}\rangle \otimes (\alpha_0 |2\rangle + \omega \alpha_1 |0\rangle + \omega^{-1} \alpha_2 |1\rangle) + \\
& |_3\beta_{22}\rangle \otimes (\alpha_0 |1\rangle + \omega \alpha_1 |2\rangle + \omega^{-1} \alpha_2 |0\rangle) ]
\end{aligned} \tag{3.28}$$

Sendo assim, os possíveis resultados para o qubit de Bob, condicionados aos resultados da medida de Alice são

$$\begin{aligned}
|_3\psi\rangle |_3\beta_{00}\rangle &= \frac{1}{3} |_3\beta_{00}\rangle |_3\psi\rangle + \frac{1}{3} |_3\beta_{01}\rangle ({}_3X |_3\psi\rangle) + \\
&\frac{1}{3} |_3\beta_{02}\rangle ({}_3X^2 |_3\psi\rangle) + \frac{1}{3} |_3\beta_{10}\rangle ({}_3Z |_3\psi\rangle) + \frac{1}{3} |_3\beta_{11}\rangle ({}_3X{}_3Z |_3\psi\rangle) + \\
&\frac{1}{3} |_3\beta_{12}\rangle ({}_3X{}_3^2Z |_3\psi\rangle) + \frac{1}{3} |_3\beta_{20}\rangle ({}_3Z^2 |_3\psi\rangle) + \frac{1}{3} |_3\beta_{21}\rangle ({}_3X{}_3Z^2 |_3\psi\rangle) + \\
&\frac{1}{3} |_3\beta_{22}\rangle ({}_3X{}_3^2Z^2 |_3\psi\rangle)
\end{aligned} \tag{3.29}$$

conforme a equação (3.13).

Podemos resumir a performance de Bob da seguinte maneira

BITS: $a,b$	PORTAS	PERFORMANCE DE BOB
0,0	$I$ :	$\alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$
0,1	${}_3X$ :	$\alpha_0  2\rangle + \alpha_1  0\rangle + \alpha_2  1\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$
0,2	${}_3X^2$ :	$\alpha_0  1\rangle + \alpha_1  2\rangle + \alpha_2  0\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$
1,0	${}_3Z$ :	$\alpha_0  0\rangle + \omega^2 \alpha_1  1\rangle + \omega \alpha_2  2\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$
1,1	${}_3X{}_3Z$ :	$\alpha_0  2\rangle + \omega^2 \alpha_1  0\rangle + \omega \alpha_2  1\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$
1,2	${}_3X{}_3^2Z$ :	$\alpha_0  1\rangle + \omega^2 \alpha_1  2\rangle + \omega \alpha_2  0\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$
2,0	${}_3Z^2$ :	$\alpha_0  0\rangle + \omega \alpha_1  1\rangle + \omega^{-1} \alpha_2  2\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$
2,1	${}_3X{}_3Z^2$ :	$\alpha_0  2\rangle + \omega \alpha_1  0\rangle + \omega^{-1} \alpha_2  1\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$
2,2	${}_3X{}_3^2Z^2$ :	$\alpha_0  1\rangle + \omega \alpha_1  2\rangle + \omega^{-1} \alpha_2  0\rangle \mapsto \alpha_0  0\rangle + \alpha_1  1\rangle + \alpha_2  2\rangle =  _3\psi\rangle$

Sendo que Bob aplica  ${}_3Z$  e  ${}_3X$  para o seu qudit, condicionado sobre os valores clássicos  $a$  e  $b$ , respectivamente enviados por Alice. Depois desta transformação, Bob recupera o estado  $|_3\psi\rangle$  que Alice lhe enviou com sucesso.

### 3.4 Conclusões

Neste capítulo foi realizada uma revisão do protocolo de teletransporte de estados arbitrários proposto por [2]. Na sequência foi apresentado um esquema para construção de estados de Bell generalizados e um protocolo de telepte de estados generalizados (qudits). E por último para validar o teleporte de estados generalizados, foi feito um exemplo com o estado generalizado qutrite.

## CAPÍTULO 4

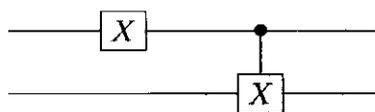
# Aplicação do Teleporte Quântico

Neste capítulo serão apresentados dois esquemas para aplicação do teleporte quântico de qubits e qudits para eventuais correções de erros devido a falhas em portas quânticas universais.

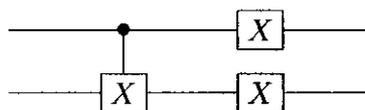
### 4.1 Introdução

O teleporte quântico tem uma aplicação bastante interessante quando se refere ao modelo de computação baseado em circuitos quânticos. Para a implementação de circuitos quânticos precisamos ter acesso a um conjunto de portas lógicas quânticas universal, onde tal conjunto inclui sempre pelo menos uma porta que atua sobre dois qubits (exemplos, uma porta CNOT ou  $dG_{xor}$ ). Muitas vezes fica bastante laborioso ou mesmo desafiador implementar tecnicamente portas quânticas que atuam em mais de um qubit e que dependem de sistemas quânticos acoplados. É possível que numa aplicação particular, por exemplo, a porta CNOT ou  $dG_{xor}$  não atue com perfeição. Se essa porta CNOT ou  $dG_{xor}$  falhar no meio de algum cálculo, os estados dos qubits e qudits que ela estava agindo serão corrompidos imediatamente, pois, sem alguma forma para correção desse erro, os cálculos não serão confiáveis.

Como um exemplo simples de erro na atuação da porta CNOT, considere a situação apresentada no circuito



**Figura 4.1** Essa figura ilustra um erro no primeiro qubit ocorrendo antes da aplicação da porta CNOT.



**Figura 4.2** Essa figura ilustra a propagação do erro ocorrido na figura anterior para os dois qubits.

Uma falha no primeiro qubit antes da aplicação da porta unitária ( $U=CNOT$ ), se propaga para os dois qubits. Tudo se passa como se a porta unitária ( $U$ ) fosse aplicada corretamente seguida de um erro nos dois qubits, ou seja,  $UX_1 = UX_1U^\dagger U = X_1X_2U$ .

Outra forma de ilustrar a porta unitária ruidosa seria considerar a porta correta ( $U$ ) e uma porta com erro  $\mathcal{E} = (\mathcal{E} \circ U^{-1}) \circ U$ . Note que o efeito de  $\mathcal{E}$  será de uma porta correta ( $U$ ), seguida de uma porta com erro  $\mathcal{E} \circ U^{-1}$ . Observe que o grau de desvio da porta correta é representado pela operação:  $\mathcal{E} \circ U^{-1} = (\mathbf{I} + \bar{\mathcal{E}})$

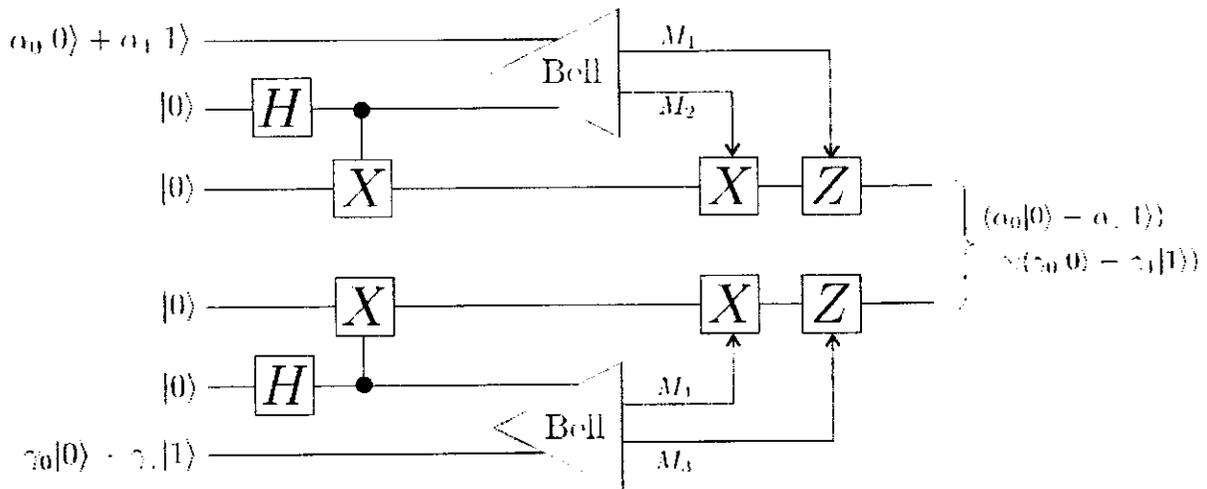
Uma solução pensada para contornar esse problema poderia ser a de se criar uma cópia do estado que se gostaria de aplicar a porta CNOT ou  $dG_{xor}$ , e manter essa cópia guardada em algum lugar seguro, e tentar novamente aplicar o CNOT ou  $dG_{xor}$ , mas infelizmente, isso é impossível, devido ao teorema da Não-Clonagem quântica, que afirma que é impossível implementar um circuito quântico que realiza uma cópia quântica de um estado arbitrário.

O que almejávamos é uma forma da aplicação tolerante a falhas de uma porta quântica CNOT ou de uma porta quântica  $dG_{xor}$ , onde se elas falhassem, os estados quânticos de qubits e qudits não fossem corrompidos, e simplesmente poderíamos novamente tentar as portas CNOT ou  $dG_{xor}$ . Uma maneira de se fazer isso é com a aplicação do teleporte quântico, desde que tenhamos a capacidade de preparar um estado de Bell, e medir os estados de Bell diretamente.

Faremos portanto a aplicação do teleporte quântico para correções de erros utilizando portas CNOT na seção 4.2 e na seção 4.3 utilizando portas quânticas  $dG_{xor}$ . E por fim, na seção 4.4 as devidas conclusões.

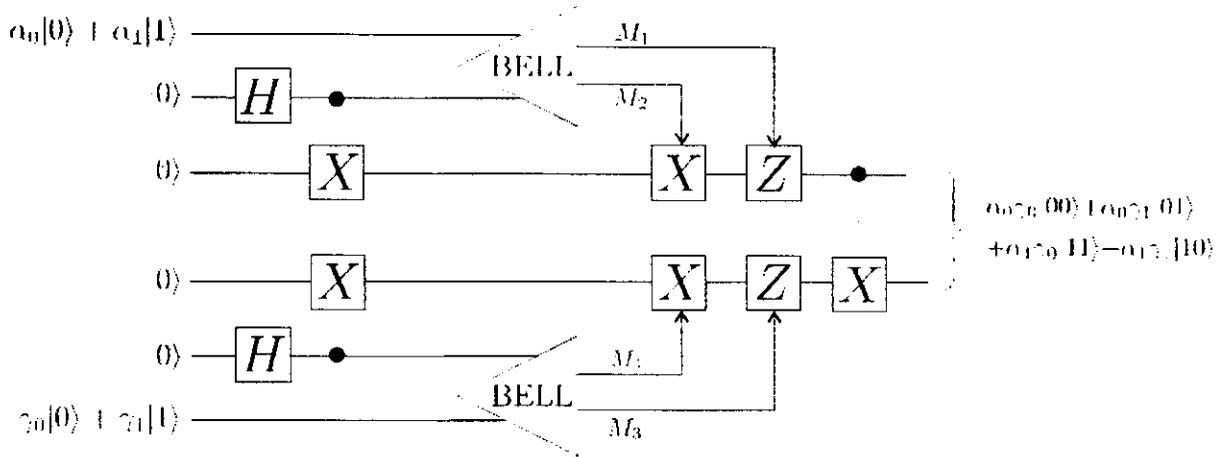
## 4.2 Aplicação do teleporte quântico para correções de erros das portas quânticas CNOT

O circuito apresentado na figura (4.3) ilustra um esquema de teleporte quântico de dois qubits



**Figura 4.3** Circuito para teleportar os estados  $\alpha_0 |0\rangle + \alpha_1 |1\rangle$  e  $\gamma_0 |0\rangle + \gamma_1 |1\rangle$ .

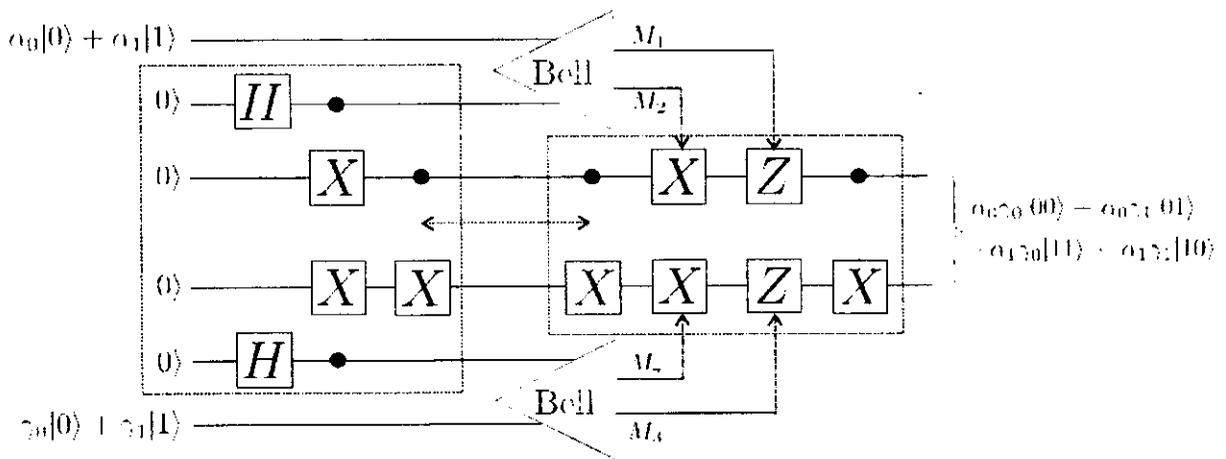
Utilizando-se do circuito para o teleporte de dois qubits podemos introduzir o esquema capaz de teleportar a porta CNOT. Segundo a sequência sugerida por [2], devemos introduzir a porta CNOT entre os qubits teleportados conforme a figura (4.4).



**Figura 4.4** A implementação de uma porta CNOT entre o par de estados teleportado, onde atua em uma pate como bit de controle e no outro como bit alvo.

A figura 4.5 mostra também o reagrupamento das portas CNOT dentro das caixas tracejadas, onde o efeito da caixa tracejada a esquerda cria o estado emaranhado de quatro qubits, ou seja

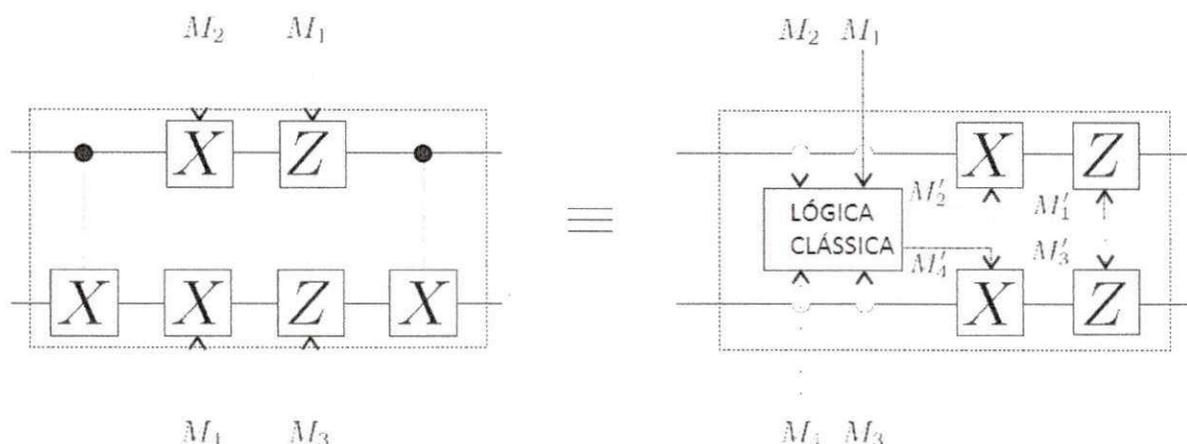
$$|E\rangle = \frac{1}{2} [ |0000\rangle + |0011\rangle + |1110\rangle + |1101\rangle ] \quad (4.1)$$



**Figura 4.5** A implementação de uma parde portas CNOT adicionados no circuito entre o par de estados teleportado.

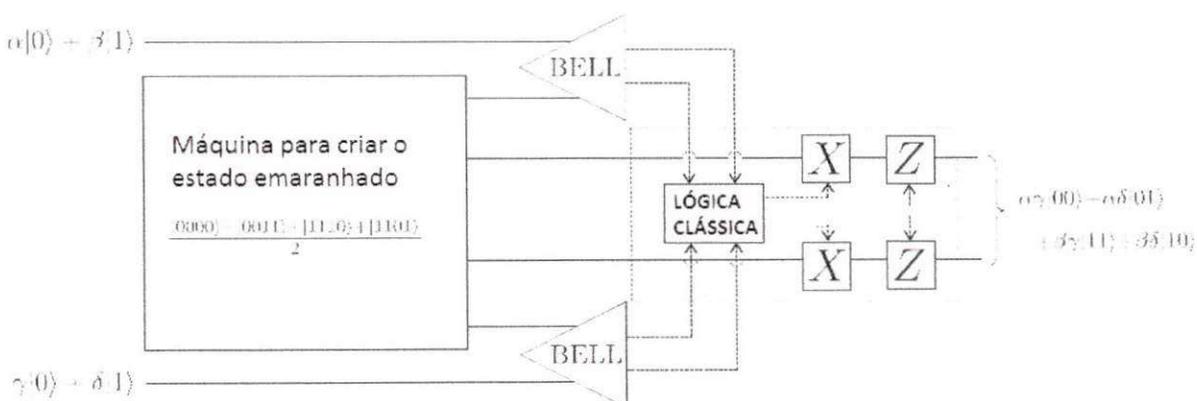
Na caixa tracejada a direita como mostra a figura (4.5), a porta CNOT altera as condições em que as portas X e Z são aplicadas separadamente para os dois qubits. Então, para qualquer combinação das medidas  $M_1, M_2, M_3$  e  $M_4$ , o efeito desejado pode ser alcançado através de

uma aplicação de uma combinação apropriada das portas X e Z individualmente para os dois qubits na caixa tracejada. Logo, podemos remover a porta CNOT da caixa tracejada se modificarmos a lógica clássica controlando as portas X e Z, como mostra a figura (4.6). Observe que estamos fazendo apenas a medida na base de Bell que nos fornece os resultados clássicos, e sabemos que essa medida na base de Bell não necessita de implementações de portas CNOT.



**Figura 4.6** O par de portas CNOT removido depois da modificação da lógica clássica controlando as aplicações das portas X e Z.

Logo, um circuito que contém a aplicação de uma porta CNOT entre dois qubits na computação quântica, sem que haja o risco de destruição do estado dos dois qubits se a porta CNOT falhar é mostrado na figura (4.7).



**Figura 4.7** Aplicação da porta CNOT entre os dois qubits em uma computação quântica, sem o risco de destruir o estado dos dois qubits se a porta C-NOT falhar.

Observamos que na primeira caixa tracejada a esquerda da figura (4.7) serviu para criar os estados emaranhados, então, basta ter alguma máquina que gere estes estados e algum meio para verificar que ela conseguiu, e se ela não conseguir criar esses estados, o nosso processo de verificação nos dirá isso, e logo poderemos preparar a máquina novamente com quatro estados

de qubits. Sendo assim, poderemos substituir a primeira caixa por uma máquina genérica para a criação dos estados, e que assumiremos também que essa máquina possui um procedimento de verificação que o estado foi criado com sucesso.

### 4.3 Exemplo

Considere o esquema que está ilustrado na figura (4.7) com os dois qubits a serem teleportados com a aplicação da porta CNOT, onde o estado de referência na saída é dada por

$$CNOT[(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)] = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle \quad (4.2)$$

A máquina cria o seguinte estado emaranhado

$$|E\rangle = \frac{1}{2} [|0000\rangle + |0011\rangle + |1110\rangle + |1101\rangle] \quad (4.3)$$

Fazendo o teleporte dos qubits, temos que

$$(\alpha|0\rangle + \beta|1\rangle) |E\rangle (\gamma|0\rangle + \delta|1\rangle) = \frac{1}{2} (\alpha|0\rangle + \beta|1\rangle) (|0000\rangle + |0011\rangle + |1110\rangle + |1101\rangle) (\gamma|0\rangle + \delta|1\rangle) \quad (4.4)$$

Resolvendo o produto tensorial, encontramos

$$\begin{aligned} (\alpha|0\rangle + \beta|1\rangle) |E\rangle (\gamma|0\rangle + \delta|1\rangle) = \frac{1}{2} [ & \alpha\gamma|000000\rangle + \alpha\delta|000001\rangle + \\ & \beta\gamma|100000\rangle + \beta\delta|100001\rangle + \alpha\gamma|000110\rangle + \alpha\delta|000111\rangle + \beta\gamma|100110\rangle + \\ & \beta\delta|100111\rangle + \alpha\gamma|011100\rangle + \alpha\delta|011101\rangle + \beta\gamma|111100\rangle + \beta\delta|111101\rangle + \\ & \alpha\gamma|011010\rangle + \alpha\delta|011011\rangle + \beta\gamma|111010\rangle + \beta\delta|111011\rangle ] \quad (4.5) \end{aligned}$$

Colocando os dois primeiros e os dois últimos termos da expressão (4.5) na base de Bell, obtemos

$$\begin{aligned} (\alpha|0\rangle + \beta|1\rangle) |E\rangle (\gamma|0\rangle + \delta|1\rangle) = \frac{1}{4} [ & \alpha\gamma(|\beta_{00}\rangle + |\beta_{10}\rangle) |00\rangle \\ & (|\beta_{00}\rangle + |\beta_{10}\rangle) + \alpha\delta(|\beta_{00}\rangle + |\beta_{10}\rangle) |00\rangle (|\beta_{01}\rangle + |\beta_{11}\rangle) + \\ & \beta\gamma(|\beta_{01}\rangle - |\beta_{11}\rangle) |00\rangle (|\beta_{00}\rangle + |\beta_{10}\rangle) + \beta\delta(|\beta_{01}\rangle - |\beta_{11}\rangle) |00\rangle \\ & (|\beta_{01}\rangle + |\beta_{11}\rangle) + \alpha\gamma(|\beta_{00}\rangle + |\beta_{10}\rangle) |01\rangle (|\beta_{01}\rangle - |\beta_{11}\rangle) + \\ & \alpha\delta(|\beta_{00}\rangle + |\beta_{10}\rangle) |01\rangle (|\beta_{00}\rangle - |\beta_{10}\rangle) + \beta\gamma(|\beta_{01}\rangle - |\beta_{11}\rangle) |01\rangle \\ & (|\beta_{01}\rangle - |\beta_{11}\rangle) + \beta\delta(|\beta_{01}\rangle - |\beta_{11}\rangle) |01\rangle (|\beta_{00}\rangle - |\beta_{10}\rangle) + \\ & \alpha\gamma(|\beta_{01}\rangle + |\beta_{11}\rangle) |11\rangle (|\beta_{00}\rangle + |\beta_{10}\rangle) + \alpha\delta(|\beta_{01}\rangle + |\beta_{11}\rangle) |11\rangle \end{aligned}$$

$$\begin{aligned}
& (|\beta_{01}\rangle + |\beta_{11}\rangle) + \beta\gamma(|\beta_{00}\rangle - |\beta_{10}\rangle) |11\rangle (|\beta_{00}\rangle + |\beta_{10}\rangle) + \\
& \beta\delta(|\beta_{00}\rangle - |\beta_{10}\rangle) |11\rangle (|\beta_{01}\rangle + |\beta_{11}\rangle) + \alpha\gamma(|\beta_{01}\rangle + |\beta_{11}\rangle) |10\rangle \\
& (|\beta_{01}\rangle - |\beta_{11}\rangle) + \alpha\delta(|\beta_{01}\rangle + |\beta_{11}\rangle) |10\rangle (|\beta_{00}\rangle - |\beta_{10}\rangle) + \\
& \beta\gamma(|\beta_{00}\rangle - |\beta_{10}\rangle) |10\rangle (|\beta_{01}\rangle - |\beta_{11}\rangle) + \beta\delta(|\beta_{00}\rangle - |\beta_{10}\rangle) |10\rangle \\
& (|\beta_{00}\rangle - |\beta_{10}\rangle) \Big] \tag{4.6}
\end{aligned}$$

Escolhendo o caso mais simples onde  $M_1, M_2, M_3$  e  $M_4$  são iguais a zero, e aplicando a expressão da lógica clássica sobre os qubits, ou seja

$$\left[ U_{CNOT} \left( Z^{M_1} X^{M_2} \otimes Z^{M_3} X^{M_4} \right) U_{CNOT} \right] |ab\rangle = \left( Z^{M_1} X^{M_2} \otimes Z^{M_3} X^{M_4} \right) |ab\rangle \tag{4.7}$$

Logo,  $M'_1, M'_2, M'_3$  e  $M'_4$  vão ser iguais a zero, sendo assim, temos que o estado de saída  $|S_1\rangle$  é

$$|S_1\rangle = \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |11\rangle + \beta\delta |10\rangle \tag{4.8}$$

que é análogo ao estado de referência observado na equação (4.2).

Considerando agora o caso em que  $M_1 = 1, M_2 = 1, M_3 = 0$  e  $M_4 = 1$ , temos que o estado de saída vai ser

$$|S_2\rangle = \alpha\gamma |10\rangle + \alpha\delta |11\rangle - \beta\gamma |01\rangle - \beta\delta |00\rangle \tag{4.9}$$

Aplicando o resultado da equação (4.7) na expressão (4.9), obtemos  $M'_1 = 1, M'_2 = 1, M'_3 = 0$  e  $M'_4 = 0$ , sendo assim, o estado de saída agora vai ser

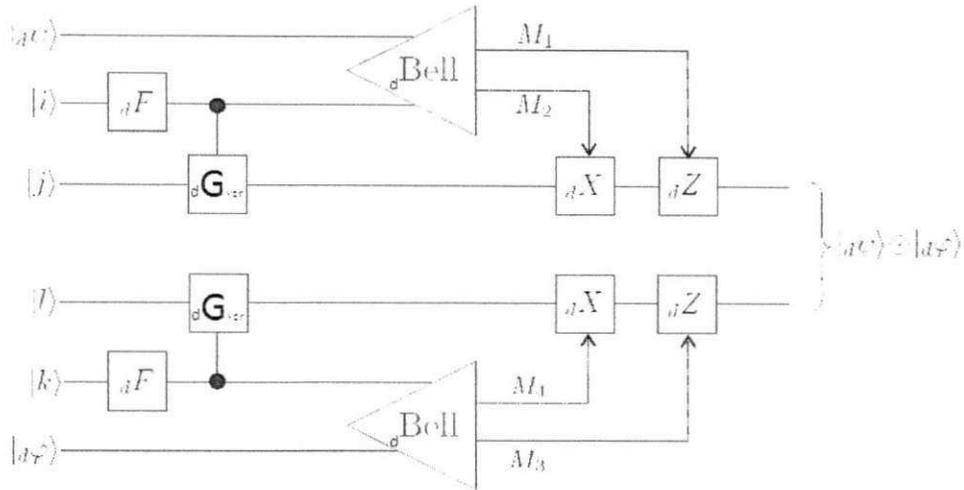
$$|S_2\rangle = \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |11\rangle + \beta\delta |10\rangle \tag{4.10}$$

que é equivalente a equação de referência (4.2).

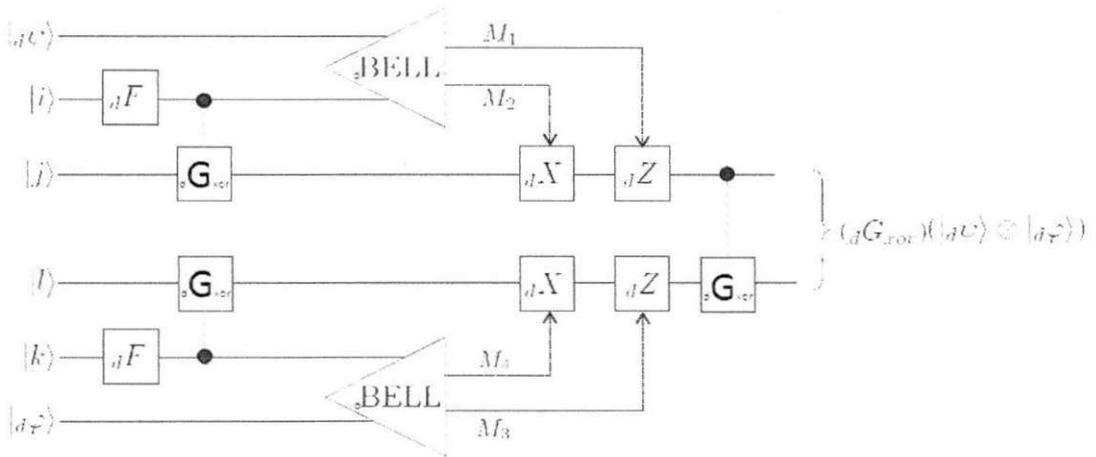
#### 4.4 Aplicação do teleporte quântico para correções de erros das portas quânticas generalizadas ( ${}_dG_{xor}$ )

De maneira análoga ao apresentado na seção (4.2), iremos generalizar a aplicação do teleporte para a construção de um esquema para teleporte da porta generalizada ( ${}_dG_{xor}$ ). As figuras (4.8–4.12) ilustram a aplicação do esquema no caso generalizado.

Colocando uma porta  ${}_dG_{xor}$  entre o par de qudits  $|{}_d\psi\rangle$  e  $|{}_d\varphi\rangle$  teleportados como mostra a figura (4.9), observou-se então que o efeito do conjunto sobre os estados de dois qudits é a operação da porta quântica  ${}_dG_{xor}$ , onde a porta  ${}_dG_{xor}$  atua em uma parte do teleporte como bit de controle e no outro como bit alvo.



**Figura 4.8** Circuito para teleportar dois estados quânticos generalizados  $|a\psi\rangle$  e  $|a\phi\rangle$ .



**Figura 4.9** A implementação de uma porta  $dG_{xor}$  entre o par de qudits, onde atua em uma parte como bit de controle e no outro como bit alvo.

Colocando agora um par de portas  $dG_{xor}$  no meio dos dois qudits, observamos que o comportamento geral do circuito não muda, já que a combinação das duas portas  $dG_{xor}$  sobre os qudits é o operador identidade como mostra a figura (4.10).

A figura (4.10) mostra o reagrupamento das portas  $dG_{xor}$  dentro das caixas tracejadas, onde o efeito da caixa tracejada a esquerda cria o estado emaranhado de quatro qudits.

Para encontrarmos este estado emaranhado, observe os seguintes passos, onde o estado de entrada é dado por

$$|au_0\rangle = |i\rangle \otimes |j\rangle \otimes |l\rangle \otimes |k\rangle = |ijkl\rangle \tag{4.11}$$

A ação das portas de fourier sobre os qudits pode ser encontrada utilizando a expressão

$$|au_1\rangle = {}_d F |i\rangle \otimes |j\rangle \otimes |l\rangle \otimes {}_d F |k\rangle \tag{4.12}$$

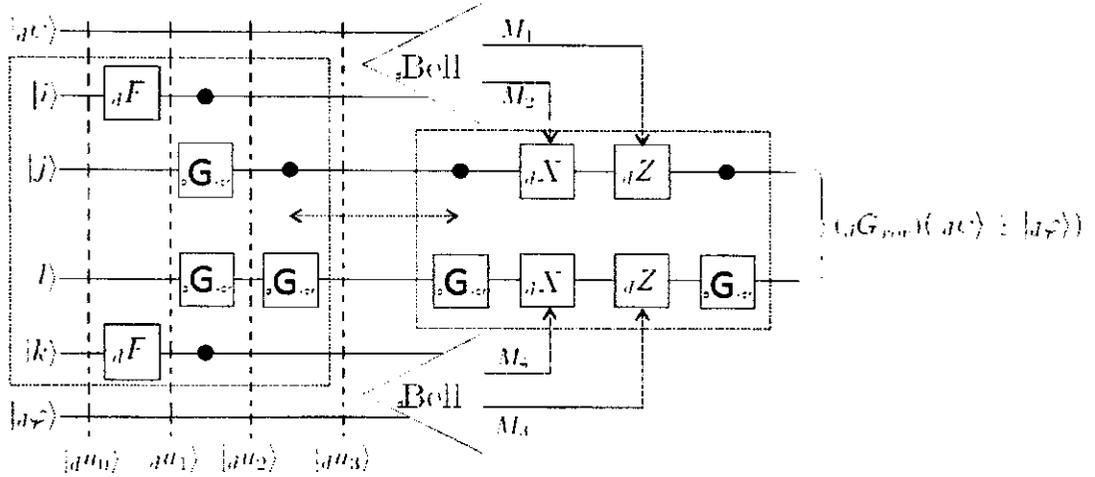


Figura 4.10 Um par de porta  ${}_dG_{xor}$  adicionados no circuito que não causa nenhum efeito.

e a ação das portas  ${}_dG_{xor}$  sobre o qudits pode ser obtida da seguinte maneira

$$|{}_du_2\rangle = \left( G_{xor}^{1 \rightarrow 3} \otimes G_{xor}^{4 \rightarrow 3} \right) |{}_du_1\rangle \tag{4.13}$$

onde o índice  $1 \rightarrow 3$  indica que o qudit 1 é o controle e o qudite 3 é o alvo, assim como para o índice  $4 \rightarrow 3$ .

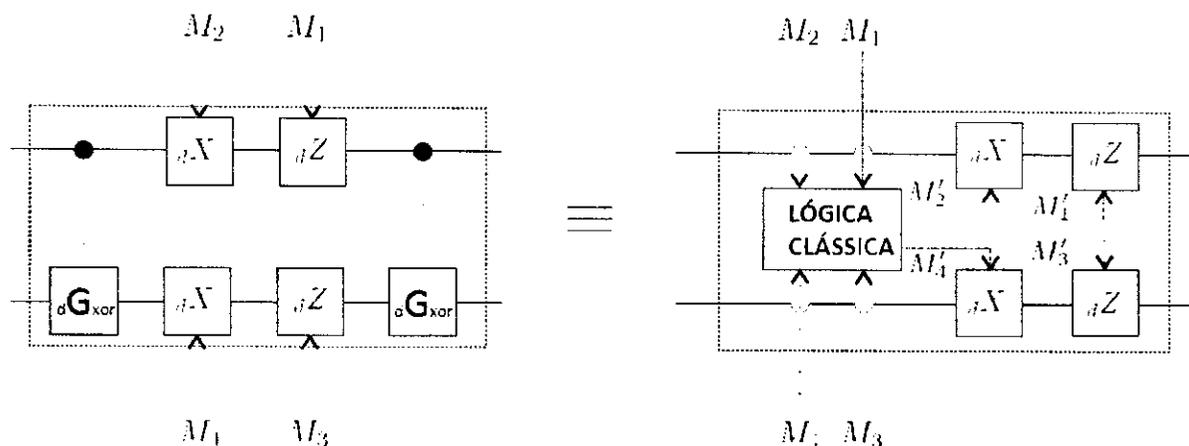
Logo o estado emaranhado da caixa tracejada a esquerda pode ser encontrada pela expressão

$$|{}_du_3\rangle = \left( G_{xor}^{2 \rightarrow 3} \right) |{}_du_2\rangle \tag{4.14}$$

A caixa tracejada a direita como mostra a figura (4.10), a porta  ${}_dG_{xor}$  altera as condições em que as portas  ${}_dX$  e  ${}_dZ$  são aplicadas separadamente para os dois qudits. Então, para qualquer combinação de  $M_1, M_2, M_3$  e  $M_4$ , o efeito desejado pode ser alcançado através de uma aplicação de uma combinação apropriada das portas  ${}_dX$  e  ${}_dZ$  individualmente para os dois qudits na caixa tracejada. Logo, podemos remover a porta  ${}_dG_{xor}$  da caixa tracejada se modificarmos a lógica clássica controlando as portas  ${}_dX$  e  ${}_dZ$ , como mostra a figura (4.11). Observe que estamos fazendo apenas a medida na base de Bell generalizada que nos fornece os resultados clássicos, e sabemos que essa medida na base de Bell generalizada não necessita de implementações de portas  ${}_dG_{xor}$ .

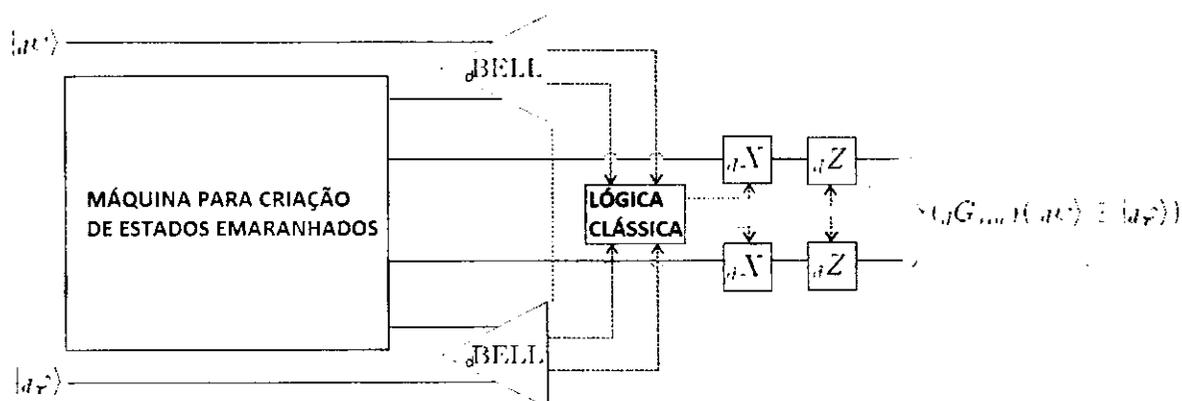
Após removermos o par de portas quântica  ${}_dG_{xor}$  a lógica clássica aplicada sobre os qudits é dada pela expressão

$$\left[ \left( \omega^{j \oplus M_2} \right)^{M_1} \left( \omega^{(j \ominus l) \oplus M_2} \right)^{M_3} \right] |j \oplus M_2, j \oplus M_2 \ominus [(j \ominus l) \oplus M_4]\rangle \tag{4.15}$$



**Figura 4.11** O par de portas  $dG_{xor}$  removido depois da modificação da lógica clássica controlando as aplicações das portas  $dX$  e  $dZ$ .

Logo, um circuito que contém a aplicação de uma porta  $dG_{xor}$  entre dois qudits na computação quântica, sem que haja o risco de destruição do estado dos dois qudits se a porta  $dG_{xor}$  falhar é mostrado na figura (4.12).



**Figura 4.12** Aplicação da porta  $dG_{xor}$  entre os dois qudits em uma computação quântica, sem o risco de destruir o estado dos dois qudits se a porta quântica  $dG_{xor}$  falhar.

Observamos na figura (4.12) que na primeira caixa tracejada a esquerda serviu para criar os estados emaranhados, no entanto, basta ter algum dispositivo que gere estes estados e algum meio seguro para verificar que ela conseguiu, e se ela não conseguir criar esses estados, o nosso processo de verificação nos dirá isso, e logo poderemos preparar a máquina novamente com quatro estados de qudits. Portanto, poderemos substituir a primeira caixa por uma máquina genérica para a criação dos estados, e que assumiremos também que essa máquina possui um procedimento de verificação que o estado foi criado com sucesso.

## 4.5 Exemplo

Para ilustrar o esquema apresentado, consideraremos o circuito mostrado na figura (4.12) com dois estados quânticos generalizados  $|_3\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$  e  $|_3\varphi\rangle = \gamma_0|0\rangle + \gamma_1|1\rangle + \gamma_2|2\rangle$  a serem teletransportados para aplicação de uma porta  $_dG_{xor}$  entre os dois qutrites na computação quântica, sem correr o risco de destruir o estado se a porta  $_dG_{xor}$  falhar. Logo, podemos dizer que nosso estado de referência para um qutrite na saída é dada por

$$\begin{aligned} {}_3G_{xor}(|_3\psi\rangle \otimes |_3\varphi\rangle) = & \alpha_0\gamma_0|00\rangle + \alpha_0\gamma_1|02\rangle + \alpha_0\gamma_2|01\rangle + \\ & \alpha_1\gamma_0|11\rangle + \alpha_1\gamma_1|10\rangle + \alpha_1\gamma_2|12\rangle + \alpha_2\gamma_0|22\rangle + \alpha_2\gamma_1|21\rangle + \alpha_2\gamma_2|20\rangle \end{aligned} \quad (4.16)$$

Adotando  $i, j, l$  e  $k$  iguais a zero e utilizando as expressões (4.11), (4.12), (4.13) e (4.14) a máquina cria o seguinte estado emaranhado

$$|_3u_3\rangle = \frac{1}{3} \left[ |0000\rangle + |0021\rangle + |0012\rangle + |1110\rangle + |1101\rangle + |1122\rangle + |2220\rangle + |2211\rangle + |2202\rangle \right] \quad (4.17)$$

Fazendo o teleporte dos qutrites, temos que

$$\begin{aligned} |_3\psi\rangle |_3u_3\rangle |_3\varphi\rangle = & \left( \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle \right) \frac{1}{3} \left[ |0000\rangle + |0021\rangle + |0012\rangle + \right. \\ & \left. |1110\rangle + |1101\rangle + |1122\rangle + |2220\rangle + |2211\rangle + |2202\rangle \right] \left( \gamma_0|0\rangle + \gamma_1|1\rangle + \gamma_2|2\rangle \right) \end{aligned} \quad (4.18)$$

Resolvendo o produto tensorial, obtemos

$$\begin{aligned} |_3\psi\rangle |_3u_3\rangle |_3\varphi\rangle = & \frac{1}{3} \left[ \alpha_0\gamma_0|000000\rangle + \alpha_0\gamma_1|000001\rangle + \alpha_0\gamma_2|000002\rangle + \alpha_1\gamma_0|100000\rangle + \right. \\ & \alpha_1\gamma_1|100001\rangle + \alpha_1\gamma_2|100002\rangle + \alpha_2\gamma_0|200000\rangle + \alpha_2\gamma_1|200001\rangle + \alpha_2\gamma_2|200002\rangle + \\ & \alpha_0\gamma_0|000210\rangle + \alpha_0\gamma_1|000211\rangle + \alpha_0\gamma_2|000212\rangle + \alpha_1\gamma_0|100210\rangle + \alpha_1\gamma_1|100211\rangle + \\ & \alpha_1\gamma_2|100212\rangle + \alpha_2\gamma_0|200210\rangle + \alpha_2\gamma_1|200211\rangle + \alpha_2\gamma_2|200212\rangle + \alpha_0\gamma_0|000120\rangle + \\ & \alpha_0\gamma_1|000121\rangle + \alpha_0\gamma_2|000122\rangle + \alpha_1\gamma_0|100120\rangle + \alpha_1\gamma_1|100121\rangle + \alpha_1\gamma_2|100122\rangle + \\ & \alpha_2\gamma_0|200120\rangle + \alpha_2\gamma_1|200121\rangle + \alpha_2\gamma_2|200122\rangle + \alpha_0\gamma_0|011100\rangle + \alpha_0\gamma_1|011101\rangle + \\ & \alpha_0\gamma_2|011102\rangle + \alpha_1\gamma_0|111100\rangle + \alpha_1\gamma_1|111101\rangle + \alpha_1\gamma_2|111102\rangle + \alpha_2\gamma_0|211100\rangle + \\ & \alpha_2\gamma_1|211101\rangle + \alpha_2\gamma_2|211102\rangle + \alpha_0\gamma_0|011010\rangle + \alpha_0\gamma_1|011011\rangle + \alpha_0\gamma_2|011012\rangle + \\ & \alpha_1\gamma_0|111010\rangle + \alpha_1\gamma_1|111011\rangle + \alpha_1\gamma_2|111012\rangle + \alpha_2\gamma_0|211010\rangle + \alpha_2\gamma_1|211011\rangle + \\ & \alpha_2\gamma_2|211012\rangle + \alpha_0\gamma_0|011220\rangle + \alpha_0\gamma_1|011221\rangle + \alpha_0\gamma_2|011222\rangle + \alpha_1\gamma_0|111220\rangle + \\ & \alpha_1\gamma_1|111221\rangle + \alpha_1\gamma_2|111222\rangle + \alpha_2\gamma_0|211220\rangle + \alpha_2\gamma_1|211221\rangle + \alpha_2\gamma_2|211222\rangle + \end{aligned}$$

$$\begin{aligned}
& \alpha_0 \gamma_0 |022200\rangle + \alpha_0 \gamma_1 |022201\rangle + \alpha_0 \gamma_2 |022202\rangle + \alpha_1 \gamma_0 |122200\rangle + \alpha_1 \gamma_1 |122201\rangle + \\
& \alpha_1 \gamma_2 |122202\rangle + \alpha_2 \gamma_0 |222200\rangle + \alpha_2 \gamma_1 |222201\rangle + \alpha_2 \gamma_2 |222202\rangle + \alpha_0 \gamma_0 |022110\rangle + \\
& \alpha_0 \gamma_1 |022111\rangle + \alpha_0 \gamma_2 |022112\rangle + \alpha_1 \gamma_0 |122110\rangle + \alpha_1 \gamma_1 |122111\rangle + \alpha_1 \gamma_2 |122112\rangle + \\
& \alpha_2 \gamma_0 |222110\rangle + \alpha_2 \gamma_1 |222111\rangle + \alpha_2 \gamma_2 |222112\rangle + \alpha_0 \gamma_0 |022020\rangle + \alpha_0 \gamma_1 |022021\rangle + \\
& \alpha_0 \gamma_2 |022022\rangle + \alpha_1 \gamma_0 |122020\rangle + \alpha_1 \gamma_1 |122021\rangle + \alpha_1 \gamma_2 |122022\rangle + \alpha_2 \gamma_0 |222020\rangle + \\
& \alpha_2 \gamma_1 |222021\rangle + \alpha_2 \gamma_2 |222022\rangle \Big]
\end{aligned} \tag{4.19}$$

Colocando os dois termos iniciais e finais da equação (4.19) na base de Bell para um qutrite, temos

$$\begin{aligned}
|_3\psi\rangle |_3u_3\rangle |_3\varphi\rangle = & \frac{1}{9} \Big[ \alpha_0 \gamma_0 (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + |_3\beta_{20}\rangle) |00\rangle \\
& (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + |_3\beta_{20}\rangle) + \dots + \alpha_0 \gamma_1 (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + |_3\beta_{20}\rangle) \\
& |02\rangle (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle + \omega |_3\beta_{20}\rangle) + \dots + \alpha_0 \gamma_2 (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + \\
& |_3\beta_{20}\rangle) |01\rangle (|_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle + \omega^2 |_3\beta_{20}\rangle) + \dots + \alpha_1 \gamma_0 \\
& (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle + \omega |_3\beta_{20}\rangle) |11\rangle (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + |_3\beta_{20}\rangle) + \dots + \\
& \alpha_1 \gamma_1 (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle + \omega |_3\beta_{20}\rangle) |10\rangle (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle \\
& + \omega |_3\beta_{20}\rangle) + \dots + \alpha_1 \gamma_2 (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle + \omega |_3\beta_{20}\rangle) |12\rangle \\
& (|_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle + \omega^2 |_3\beta_{20}\rangle) + \dots + \alpha_2 \gamma_0 (|_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle \\
& + \omega^2 |_3\beta_{20}\rangle) |22\rangle (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + |_3\beta_{20}\rangle) + \dots + \alpha_2 \gamma_1 (|_3\beta_{00}\rangle + \\
& \omega |_3\beta_{10}\rangle + \omega^2 |_3\beta_{20}\rangle) |21\rangle (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle + \omega |_3\beta_{20}\rangle) + \dots + \\
& \alpha_2 \gamma_2 (|_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle + \omega^2 |_3\beta_{20}\rangle) |20\rangle (|_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle \\
& + \omega^2 |_3\beta_{20}\rangle) \Big]
\end{aligned} \tag{4.20}$$

Multiplicando termo à termo da equação (4.20), obteremos

$$\begin{aligned}
|_3\psi\rangle |_3u_3\rangle |_3\varphi\rangle = & \frac{1}{9} \Big[ \alpha_0 \gamma_0 |_3\beta_{00}\rangle |00\rangle (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + \\
& |_3\beta_{20}\rangle) + \alpha_0 \gamma_0 |_3\beta_{10}\rangle |00\rangle (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + |_3\beta_{20}\rangle) + \alpha_0 \gamma_0 \\
& |_3\beta_{20}\rangle (|_3\beta_{00}\rangle + |_3\beta_{10}\rangle + |_3\beta_{20}\rangle) + \dots + \alpha_0 \gamma_1 |_3\beta_{00}\rangle |02\rangle (|_3\beta_{00}\rangle \\
& + \omega^2 |_3\beta_{10}\rangle + \omega |_3\beta_{20}\rangle) + \alpha_0 \gamma_1 |_3\beta_{10}\rangle |02\rangle (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle + \\
& \omega |_3\beta_{20}\rangle) + \alpha_0 \gamma_1 |_3\beta_{20}\rangle |02\rangle (|_3\beta_{00}\rangle + \omega^2 |_3\beta_{10}\rangle + \omega |_3\beta_{20}\rangle) + \dots + \\
& \alpha_0 \gamma_2 |_3\beta_{00}\rangle |01\rangle (|_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle + \omega^2 |_3\beta_{20}\rangle) + \alpha_0 \gamma_2 |_3\beta_{10}\rangle \\
& |01\rangle (|_3\beta_{00}\rangle + \omega |_3\beta_{10}\rangle + \omega^2 |_3\beta_{20}\rangle) + \alpha_0 \gamma_2 |_3\beta_{20}\rangle |01\rangle (|_3\beta_{00}\rangle +
\end{aligned}$$

$$\begin{aligned}
 & \omega |{}_3\beta_{10}\rangle + \omega^2 |{}_3\beta_{20}\rangle) + \dots + \alpha_1 \gamma_0 |{}_3\beta_{00}\rangle |11\rangle (|{}_3\beta_{00}\rangle + |{}_3\beta_{10}\rangle + \\
 & |{}_3\beta_{20}\rangle) + \alpha_1 \gamma_0 \omega^2 |{}_3\beta_{10}\rangle |11\rangle (|{}_3\beta_{00}\rangle + |{}_3\beta_{10}\rangle + |{}_3\beta_{20}\rangle) + \alpha_1 \gamma_0 \\
 & \omega |{}_3\beta_{20}\rangle |11\rangle (|{}_3\beta_{00}\rangle + |{}_3\beta_{10}\rangle + |{}_3\beta_{20}\rangle) + \dots + \alpha_1 \gamma_1 |{}_3\beta_{00}\rangle |10\rangle \\
 & (|{}_3\beta_{00}\rangle + \omega^2 |{}_3\beta_{10}\rangle + \omega |{}_3\beta_{20}\rangle) + \alpha_1 \gamma_1 \omega^2 |{}_3\beta_{10}\rangle |10\rangle (|{}_3\beta_{00}\rangle + \\
 & \omega^2 |{}_3\beta_{10}\rangle + \omega |{}_3\beta_{20}\rangle) + \alpha_1 \gamma_1 \omega |{}_3\beta_{20}\rangle |10\rangle (|{}_3\beta_{00}\rangle + \omega^2 |{}_3\beta_{10}\rangle + \\
 & \omega |{}_3\beta_{20}\rangle) + \alpha_1 \gamma_2 |{}_3\beta_{00}\rangle |12\rangle (|{}_3\beta_{00}\rangle + \omega |{}_3\beta_{10}\rangle + \omega^2 |{}_3\beta_{20}\rangle) + \\
 & \alpha_1 \gamma_2 \omega^2 |{}_3\beta_{10}\rangle |12\rangle (|{}_3\beta_{00}\rangle + \omega |{}_3\beta_{10}\rangle + \omega^2 |{}_3\beta_{20}\rangle) + \alpha_1 \gamma_2 \omega \\
 & |{}_3\beta_{20}\rangle |12\rangle (|{}_3\beta_{00}\rangle + \omega |{}_3\beta_{10}\rangle + \omega^2 |{}_3\beta_{20}\rangle) + \dots + \alpha_2 \gamma_0 |{}_3\beta_{00}\rangle |22\rangle \\
 & (|{}_3\beta_{00}\rangle + |{}_3\beta_{10}\rangle + |{}_3\beta_{20}\rangle) + \alpha_2 \gamma_0 \omega |{}_3\beta_{10}\rangle |22\rangle (|{}_3\beta_{00}\rangle + |{}_3\beta_{10}\rangle + \\
 & |{}_3\beta_{20}\rangle) + \alpha_2 \gamma_0 \omega^2 |{}_3\beta_{20}\rangle |22\rangle (|{}_3\beta_{00}\rangle + |{}_3\beta_{10}\rangle + |{}_3\beta_{20}\rangle) + \dots + \\
 & \alpha_2 \gamma_1 |{}_3\beta_{00}\rangle |21\rangle (|{}_3\beta_{00}\rangle + \omega^2 |{}_3\beta_{10}\rangle + \omega |{}_3\beta_{20}\rangle) + \alpha_2 \gamma_1 \\
 & \omega |{}_3\beta_{10}\rangle |21\rangle (|{}_3\beta_{00}\rangle + \omega^2 |{}_3\beta_{10}\rangle + \omega |{}_3\beta_{20}\rangle) + \alpha_2 \gamma_1 \omega^2 |{}_3\beta_{20}\rangle \\
 & |21\rangle (|{}_3\beta_{00}\rangle + \omega^2 |{}_3\beta_{10}\rangle + \omega |{}_3\beta_{20}\rangle) + \dots + \alpha_2 \gamma_2 |{}_3\beta_{00}\rangle |20\rangle (|{}_3\beta_{00}\rangle \\
 & + \omega |{}_3\beta_{10}\rangle + \omega^2 |{}_3\beta_{20}\rangle) + \alpha_2 \gamma_2 \omega |{}_3\beta_{10}\rangle |20\rangle (|{}_3\beta_{00}\rangle + \omega |{}_3\beta_{10}\rangle + \\
 & \omega^2 |{}_3\beta_{20}\rangle) + \alpha_2 \gamma_2 \omega^2 |{}_3\beta_{20}\rangle |20\rangle (|{}_3\beta_{00}\rangle + \omega |{}_3\beta_{10}\rangle + \omega^2 |{}_3\beta_{20}\rangle) \Big] \quad (4.21)
 \end{aligned}$$

Escolhendo o caso mais simples onde  $M_1, M_2, M_3$  e  $M_4$  são iguais a zero, e aplicando a lógica clássica sobre os qudits conforme a equação (4.15), temos

$$1.1 |j \oplus 0, j \oplus 0 \ominus [(j \ominus l) \oplus 0]\rangle = |j, j \oplus (j \ominus l)\rangle = |j, l\rangle \quad (4.22)$$

Logo,  $M'_1, M'_2, M'_3$  e  $M'_4$  vão ser iguais a zero, sendo assim, temos que o estado de saída  $|S_1\rangle$  vai ser igual o estado de referência mostrado na equação (4.16), ou seja:

$$\begin{aligned}
 |{}_3S_1\rangle = & \alpha_0 \gamma_0 |00\rangle + \alpha_0 \gamma_1 |02\rangle + \alpha_0 \gamma_2 |01\rangle + \alpha_1 \gamma_0 |11\rangle + \alpha_1 \gamma_1 |10\rangle + \alpha_1 \gamma_2 |12\rangle \\
 & + \alpha_2 \gamma_0 |22\rangle + \alpha_2 \gamma_1 |21\rangle + \alpha_2 \gamma_2 |20\rangle \quad (4.23)
 \end{aligned}$$

Consideremos agora o caso em que  $M_1 = 0, M_2 = 0, M_3 = 1$  e  $M_4 = 0$ , temos que o estado de saída é dado por

$$\begin{aligned}
 |{}_3S_2\rangle = & \alpha_0 \gamma_0 |00\rangle + \alpha_0 \gamma_1 \omega^2 |02\rangle + \alpha_0 \gamma_2 \omega |01\rangle + \alpha_1 \gamma_0 |11\rangle + \alpha_1 \gamma_1 \omega^2 \\
 & |10\rangle + \alpha_1 \gamma_2 \omega |12\rangle + \alpha_2 \gamma_0 |22\rangle + \alpha_2 \gamma_1 \omega^2 |21\rangle + \alpha_2 \gamma_2 \omega |20\rangle \quad (4.24)
 \end{aligned}$$

Considerando a lógica clássica sobre o qudite, obtemos

$$[\omega^{(j \ominus l)}] |j \oplus 0, j \oplus 0 \ominus [(j \ominus l) \oplus 0]\rangle = [\omega^{(j \ominus l)}] |j, l\rangle \quad (4.25)$$

De acordo com o resultado acima temos que  $M'_1 = 0$ ,  $M'_2 = 0$ ,  $M'_3 = 1$  e  $M'_4 = 0$ , logo o estado de saída  $|{}_3S_2\rangle$  vai ser

$$\begin{aligned} |{}_3S_2\rangle = & \alpha_0\gamma_0\omega^{(0\ominus 0)} |00\rangle + \alpha_0\gamma_1\omega^2\omega^{(0\ominus 2)} |02\rangle + \alpha_0\gamma_2\omega\omega^{(0\ominus 1)} \\ & |01\rangle + \alpha_1\gamma_0\omega^{(1\ominus 1)} |11\rangle + \alpha_1\gamma_1\omega^2\omega^{(1\ominus 0)} |10\rangle + \alpha_1\gamma_2\omega\omega^{(1\ominus 2)} \\ & |12\rangle + \alpha_2\gamma_0\omega^{(2\ominus 2)} |22\rangle + \alpha_2\gamma_1\omega^2\omega^{(2\ominus 1)} |21\rangle + \alpha_2\gamma_2\omega\omega^{(2\ominus 0)} |20\rangle \end{aligned} \quad (4.26)$$

Por fim podemos reescrever o estado de saída  $|{}_3S_2\rangle$  da seguinte maneira

$$\begin{aligned} |{}_3S_2\rangle = & \alpha_0\gamma_0 |00\rangle + \alpha_0\gamma_1 |02\rangle + \alpha_0\gamma_2 |01\rangle + \alpha_1\gamma_0 |11\rangle + \alpha_1\gamma_1 |10\rangle + \alpha_1\gamma_2 \\ & |12\rangle + \alpha_2\gamma_0 |22\rangle + \alpha_2\gamma_1 |21\rangle + \alpha_2\gamma_2 |20\rangle \end{aligned} \quad (4.27)$$

que também é analogo ao estado de referência.

Escolhendo agora  $M_1 = 0$ ,  $M_2 = 0$ ,  $M_3 = 2$  e  $M_4 = 0$ , temos que o estado de saída vai ser

$$\begin{aligned} |{}_3S_3\rangle = & \alpha_0\gamma_0 |00\rangle + \alpha_0\gamma_1\omega |02\rangle + \alpha_0\gamma_2\omega^2 |01\rangle + \alpha_1\gamma_0 |11\rangle + \alpha_1\gamma_1\omega \\ & |10\rangle + \alpha_1\gamma_2\omega^2 |12\rangle + \alpha_2\gamma_0 |22\rangle + \alpha_2\gamma_1\omega |21\rangle + \alpha_2\gamma_2\omega^2 |20\rangle \end{aligned} \quad (4.28)$$

A lógica clássica sobre o qutrite vai ser dado por

$$[\omega^{(j\ominus l)}] |j \oplus 0, j \oplus 0 \ominus [(j \ominus l) \oplus 0]\rangle = [\omega^{(j\ominus l)}]^2 |j, l\rangle \quad (4.29)$$

De acordo com a lógica clássica atuando no qutrite temos que  $M'_1 = 0$ ,  $M'_2 = 0$ ,  $M'_3 = 2$  e  $M'_4 = 0$ , logo, podemos aplicar o resultado da equação (4.29) na expressão (4.30) e o estado de saída vai ser agora dado por

$$\begin{aligned} |{}_3S_3\rangle = & \alpha_0\gamma_0 [\omega^{(0\ominus 0)}]^2 |00\rangle + \alpha_0\gamma_1\omega [\omega^{(0\ominus 2)}]^2 |02\rangle + \alpha_0\gamma_2 \\ & \omega^2 [\omega^{(0\ominus 1)}]^2 |01\rangle + \alpha_1\gamma_0 [\omega^{(1\ominus 1)}]^2 |11\rangle + \alpha_1\gamma_1\omega \\ & [\omega^{(1\ominus 0)}]^2 |10\rangle + \alpha_1\gamma_2\omega^2 [\omega^{(1\ominus 2)}]^2 |12\rangle + \alpha_2\gamma_0 \\ & [\omega^{(2\ominus 2)}]^2 |22\rangle + \alpha_2\gamma_1\omega [\omega^{(2\ominus 1)}]^2 |21\rangle + \alpha_2\gamma_2\omega^2 \\ & [\omega^{(2\ominus 0)}]^2 |20\rangle \end{aligned} \quad (4.30)$$

Por fim podemos reescrever o estado de saída  $|{}_3S_3\rangle$  da seguinte maneira

$$\begin{aligned} |{}_3S_3\rangle = & \alpha_0\gamma_0 |00\rangle + \alpha_0\gamma_1 |02\rangle + \alpha_0\gamma_2 |01\rangle + \alpha_1\gamma_0 |11\rangle + \alpha_1\gamma_1 |10\rangle + \\ & \alpha_1\gamma_2 |12\rangle + \alpha_2\gamma_0 |22\rangle + \alpha_2\gamma_1 |21\rangle + \alpha_2\gamma_2 |20\rangle \end{aligned} \quad (4.31)$$

Observamos que os três estados de saída  $|S_1\rangle$ ,  $|S_2\rangle$  e  $|S_3\rangle$  são iguais ao estado de referência para o teleporte dos dois qutrites com a aplicação da porta  $_dG_{xor}$  quando utilizamos a nossa lógica clássica para eliminação das portas  $_dG_{xor}$ , no entanto, aplicamos a lógica para não correremos o risco de uma das portas falharem e termos confiabilidade nos dados obtidos.

## 4.6 Conclusões

Neste capítulo foi construído a partir da idéia proposta por [2] um esquema para teleportação de estados quânticos arbitrários no espaço de Hilbert de dimensão- $d$ , por meio de uma lógica clássica segura construída passo a passo para podermos eliminar as portas quânticas  $_dG_{xor}$  generalizadas para o esquema não correr nenhum risco da informação ser modificada se uma dessas portas falhassem durante as suas respectivas ações sobre os qudits. De bônus fizemos um exemplo do esquema teletransportando dois qutrites com a aplicação da lógica clássica para tornarmos a nossa proposta confiável.

## CAPÍTULO 5

---

# Considerações Finais

---

O principal objetivo da computação quântica tolerante a falhas é a realização de operações lógicas usando portas quânticas que evitem a propagação de erros entre os qubits físicos.

A construção de portas quânticas tolerantes a falhas usando o teleporte quântico, oferece um valioso recurso à computação quântica, pois possibilita realizar experiências à sua implementação física.

Apresentamos um esquema utilizando o teleporte quântico com portas quânticas generalizadas  ${}_dG_{xor}$  tolerantes a falhas operacionais. Nosso esquema é uma adaptação daquele apresentado por Gottesman e Chuang [12], no espaço de Hilbert de qudits. Esse esquema permite a construção tolerante à falhas de portas unitárias (U) satisfazendo  $U \in C_k$ ,  $C_k = \{U|UC_1U^\dagger \subseteq C_{k-1}\}$ , sendo  $C_1$  a representação do grupo de Pauli e  $C_2$  a representação do grupo de Clifford. Verificamos que a porta  ${}_dG_{xor}$  obedece (como é de se esperar) a relação  ${}_dG_{xor} \in {}_dC_2$ ,  ${}_dC_2 = \{U|UC_1U^\dagger \subseteq C_1\}$ , sendo  ${}_dC_2$  o grupo de Clifford em d-dimensional.

O esquema apresentado nesse trabalho pode ser utilizado para outras portas quânticas universais reconhecidamente de difícil implementação [12], como por exemplo, a porta quântica Toffoli, a  $\pi/8$  e a a porta de fase controlada (S).

---

---

## Referências Bibliográficas

---

- [1] K. J. Resch T. C. Ralph and A. Gilchrist. Efficient toffoli gates using qudits. *Phys. Rev. A* 75, 022313, 75:5, 2007.
- [2] R. Laflamme P. Kaye and M. Mosca. *An Introduction to Quantum Computing*. 2007.
- [3] Diney Soares Ether Júnior. *Teletransporte Quântico em múltiplos Graus de Liberdade de um Fóton*. PhD thesis, Universidade Federal do Rio de Janeiro, 2009.
- [4] Mário Ferreira dos Santos. *Dicionário de Filosofia e Ciências Culturais*, volume 3. Editora Matese, 1963.
- [5] M. A. Nielsen and I. L. Chuang. *Quantum computation and Quantum Information*. Cambridge University Press, 2000.
- [6] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661 – 663, Aug 1991.
- [7] RAIMOND J. M. HAROCHE, S. *Exploring the Quantum*. Oxford University Press, 2006.
- [8] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys. Rev. Lett.*, 78:221–3224, Apr 1997.
- [9] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895 –1899, Mar 1993.
- [10] Horodecki P. Horodecki R. Horodecki, M. General teleportation channel, singlet fraction and quasi-distillation. *Physical Review A*, v.60,:p.1898., 1999.
- [11] Kimble H. J Braunstein, S. L. A posteriori teleportation. *Nature*, v.394:840–841, 1998.
- [12] Chuang I. L. Gottesman, D. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, v.402:390–393, 1999.

- 
- [13] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 80:1121–1125, 1998.
- [14] Chiaverini J. Schaetz T. et al. Barrett, M. D. Deterministic quantum teleportation of atomic qubits. *Nature*, v.429:737–739, 2004.
- [15] M. A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation using nuclear magnetic resonance. *Nature*, 395:52–55, October 1998.
- [16] W. Tittel H. Zbinden I. Marcikic, H. de Riedmatten and N. Gisin. Long-distance teleportation of qubits at telecommunication wavelengths. *Nature*, 421:509–513, 2002.
- [17] Benjamin Schumacher. Quantum coding. *Phys. Rev. A*, 51:2738–2747, 1995.
- [18] Gustavo Lima Chaves e Peterson Katagiri Zilli Felipe Portavales Goldstein. Breve introdução a computação quântica, Agosto 2011.
- [19] Marco Genovese and Paolo Trainay. Review on qudits production and their application to quantum communication and studies on local realism. *ADV.SCI.LETT.*, 1:153, 2008.
- [20] John Martinis and Matthew Neeley. Experiments at ucsb push quantum mechanics to higher levels, August 2009.
- [21] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, 1995.
- [22] Ch. Roos, Th. Zeiger, H. Rohde, H. C. Nägerl, J. Eschner, D. Leibfried, F. Schmidt-Kaler, and R. Blatt. Quantum state engineering on an optical transition and decoherence in a paul trap. *Phys. Rev. Lett.*, 83, 1999.
- [23] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time bell states. *Phys. Rev. Lett.*, 84:4737–4740, 2000.
- [24] E. Knill. Group representations, error bases and quantum codes. *LANL REPORT*, pages 96–2807, 1996.
- [25] D. Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *LANL REPORT*, 1:302–313, 1998.
- [26] FERNANDO VASCONCELOS MENDES. *Esquemas para Teleportação de Portas Quânticas*. PhD thesis, Universidade Federal do Ceará, 2010.

- 
- [27] Nicolas Gisin Igor Jex Gernot Alber, Aldo Delgado. Generalized quantum xor-gate for quantum teleportation and state purification in arbitrary dimensional hilbert spaces. *Cornel University Library*, 1:4, 2000.
- [28] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.
- [29] Klaus Mattle Manfred Eibl Harald Weinfurter Dik Bouwmeester, Jian-Wei Pan and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, November 1997.
- [30] Helle Bechmann-Pasquinucci and Asher Peres. Quantum cryptography with 3-state systems. *Phys. Rev. Lett.*, 85:3313–3316, 2000.
- [31] D. M. BURTON. *Elementary Number Theory*. McGraw-Hill Companies, 1997.
- [32] R. K. CONWAY, J. H.; GUY. *The Book of Numbers*. Springer, 1995.
- [33] J. M JONES, G. A.; JONES. *Elementary Number Theory*. Springer, 1998.
- [34] J. J. TATTERSALL. *Elementary Number Theory in Nine Chapters*. Cambridge University Press, 2005.
- [35] Flávio Luís Alves. Computação quântica: Fundamentos físicos e perspectivas. Master's thesis, Universidade Federal de Lavras, 2003.
- [36] Ana Rute Cerveira Esteves. Teoria de fredholm em espaços de hilbert. Master's thesis, Universidade de Aveiro, 2007.

## APÊNDICE A

---

# Noções de aritmética modular

---

Neste apêndice mostraremos algumas noções básicas da aritmética modular, que é um tema bastante explorado dentro da teoria moderna dos números, cuja a aderência com esse trabalho advém da ação das portas lógicas quânticas generalizadas atuando sobre qudits de dimensões arbitrárias.

### A.1 Introdução

Introduzida pelo matemático Karl Friedrich Gauss, em seu seminal trabalho *Disquisitiones Arithmeticae* de 1801, a aritmética modular [31, 32] não apenas está no centro da moderna teoria dos números como também possui muitas aplicações práticas em ciência da computação.

O método aplicado ao desenvolvimento da generalização das portas lógicas quânticas empregou alguns conceitos envolvendo aritmética modular, portanto, embora esteja fora do escopo deste trabalho fornecer uma ampla discussão sobre o tema serão discutidas as propriedades necessárias ao entendimento da abordagem aplicada.

O restante deste apêndice está organizado da seguinte forma: A discussão é iniciada na Seção A.2 com uma breve discussão sobre a operação do módulo e apresentação de exemplos. Na sequência tem-se na Seção A.3 o tema central aritmética modular: a teoria das congruências. Por fim, a seção A.4 apresenta as conclusões.

### A.2 Noções básicas

A aritmética modular mostra-se como uma importante ferramenta na solução de muitos problemas envolvendo números inteiros, a idéia central consiste em substituir cada número inteiro de um dado problema pelo resto de sua divisão por um número fixo, por exemplo  $n$ . O mais proeminente benefício direto dessa abordagem é reduzir o conjunto infinito  $\mathbb{Z}$ , sobre o qual se trabalha, para  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ , um conjunto finito de  $n$  elementos [33].

Para a consolidação da idéia pode-se tomar como exemplo o seguinte problema: Qual dia da semana será daqui a 1000 dias? Uma primeira escolha para essa solução pode ser contar, a partir de hoje, os mil dias à frente e verificar em qual dia resultará. Por outro lado, pode-se observar que os dias da semana formam um ciclo com sete elementos, assim, escrevendo o número 1000 na forma

$$1000 = 142 \times 7 + 6 \quad (\text{A.1})$$

perceber-se-á que bastará buscar que dia da semana será daqui a seis dias e se terá a resposta para o problema colocado. Dada essa explicação pode-se agora expressar uma definição de maneira mais formal como se segue.

**Definição A.1.** Para  $a$  um inteiro positivo e  $n \in \mathbb{Z}$ , diz-se que a divisão inteira de  $a$  por  $n$  fornecerá como resto

$$a \bmod n,$$

cujo valor estará entre 0 e  $n - 1$ .

Para ilustrar seguem alguns exemplos:

- $4 \bmod 3 = 1$ ,  $17 \bmod 3 = 2$ ,  $38 \bmod 3 = 2$
- $5 \bmod 6 = 5$ ,  $23 \bmod 6 = 5$ ,  $57 \bmod 6 = 3$
- $8 \bmod 11 = 8$ ,  $18 \bmod 11 = 7$ ,  $82 \bmod 11 = 5$
- $49 \bmod 37 = 12$ ,  $392 \bmod 37 = 22$ ,  $4459 \bmod 37 = 19$

### A.3 Congruência modular

Dentre algumas denominações encontradas para a aritmética modular talvez a mais aderente à sua própria natureza seja a de aritmética dos restos<sup>1</sup>, pois como já pode ser percebido a partir da Definição A.1 ela está intimamente relacionada com a operação de divisão. Dessa maneira, será enunciado o teorema<sup>2</sup> da divisão que será útil à discussão desenvolvida no decorrer desta seção.

**Teorema A.1.** Se  $a$  e  $b$  são números inteiros com  $b > 0$  então existe um único par de inteiros  $q$  e  $r$  tais que

$$a = qb + r \quad \text{com} \quad 0 \leq r < b,$$

<sup>1</sup>Nesse contexto o termo significa o resto de uma divisão em  $\mathbb{Z}$ .

<sup>2</sup>A demonstração não será reproduzida aqui, mas uma versão didática pode ser encontrada em [34]

Uma vez apresentada a definição sobre a operação de módulo e revisto o teorema da divisão pode-se partir para o tema central da aritmética modular, a teoria das congruências definida a seguir.

**Definição A.2.** Tomando  $n$  como um número inteiro fixo, diz-se que dois inteiros  $a$  e  $b$  são congruentes módulo  $n$ , denotado por

$$a \equiv b \pmod{n},$$

se  $n$  divide a diferença  $a - b$ , ou seja,  $a - b = kn$  para algum inteiro  $k$ .

Logo, para  $n$  um inteiro positivo e  $a, b \in \mathbb{Z}$ , tem-se que  $a$  é congruente a  $b$  módulo  $n$  se  $n|(a - b)$ , ou seja, se  $n$  divide  $(a - b)$ . Por outro lado, se  $n \nmid (a - b)$  dizemos que  $a$  e  $b$  não são congruentes módulo  $n$ , denotado por  $a \not\equiv b \pmod{n}$ . Assim, fixando  $n = 4$  seriam exemplos de congruências:

$$6 \equiv 2, 14 \equiv 2, 3 \equiv 7, 21 \equiv 1, 16 \equiv 0 \quad (\text{A.2})$$

Colocando na forma de teorema tal qual proposto em [31] tem-se:

**Teorema A.1.** Para inteiros arbitrários  $a$  e  $b$ ,  $a \equiv b \pmod{n}$  se e somente se  $a$  e  $b$  levam ao mesmo resto não negativo quando divididos por  $n$ .

*Demonstração.* Primeiro, toma-se  $a \equiv b \pmod{n}$ , então se tem que  $a = b + kn$  para algum inteiro  $k$ . A divisão por  $n$  deixará um certo resto  $r : b = qn + r$ , onde  $0 \leq r < n$ . Portanto,

$$a = b + kn = (qn + r) + kn = (q + k)n + r,$$

o que indica que  $a$  tem o mesmo resto que  $b$ .

Por último, finalizando essa breve discussão sobre aritmética modular, na sequência é apresentado um conjunto de propriedades importante à manipulação dos conceitos apresentados. É assumido um  $n$  fixo, portanto para reduzir a notação será omitido o " $\pmod{n}$ ".

1.  $a \equiv a$
2. Se  $a \equiv b$ , então  $b \equiv a$ .
3. Se  $a \equiv b$  e  $b \equiv c$ , então  $a \equiv c$ .
4. Se  $a \equiv b$  e  $c \equiv d$ , então  $a + c \equiv b + d$  e  $ac \equiv bd$ .
5. Se  $a \equiv b$ , então  $a + c \equiv b + c$ .

---

6.  $(-x) \equiv N - x$

7. Se  $a \equiv b$ , então  $a^k \equiv b^k$  para todo  $k$  inteiro positivo.

## A.4 Conclusão

Neste apêndice foram apresentados alguns conceitos sobre a aritmética modular. No centro da moderna teoria dos números sua aderência com o trabalho advém da ação das portas lógicas generalizadas atuando sobre qudits de dimensão arbitrária. Foram portanto revisadas as definições sobre a operação módulo, posteriormente entrando na teoria das congruências. Para finalizar foi apresentada algumas propriedades úteis para resolução de problemas envolvendo aritmética modular.

## APÊNDICE B

---

---

# Breve Introdução a Álgebra e Notação da Mecânica Quântica

---

Mostraremos nesse apêndice uma breve discussão sobre a álgebra e notação da Mecânica Quântica, fazendo uma breve introdução sobre estados quânticos, espaço de Hilbert ( $\mathcal{H}$ ) e por fim sobre sistemas compostos como pode ser visto nas seções 3.2, 3.2 e 3.3 respectivamente.

### B.1 Estados

Duas das noções mais importantes nas teorias físicas são as de estado e a de grandeza, quantidade ou magnitude física. De um modo geral, estados são caracterizações básicas dos objetos físicos tratados pela teoria. As grandezas físicas são as propriedades mensuráveis desses objetos. Um estado de um sistema clássico (governado pela mecânica clássica) é caracterizado por valores bem definidos das grandezas físicas mensuráveis. Posição, velocidade, energia, todas têm valores bem definidos a todo instante. Determinar o estado de um sistema quântico corresponde a especificar probabilidades de encontrar determinados valores para as grandezas físicas mensuráveis. Existe uma incerteza intrínseca ao sistema, e essa incerteza é descrita matematicamente como uma superposição coerente de estados distintos. Essa superposição corresponderia, grosso modo, ao sistema estar, ao mesmo tempo, em vários estados clássicos diferentes, onde o estado clássico de uma partícula é representado matematicamente por um ponto no espaço de fases, formado pelas componentes da posição e da velocidade da partícula. Na mecânica quântica, o estado de uma partícula é representado matematicamente por um vetor num espaço vetorial complexo, chamado espaço de Hilbert [35].

### B.2 Espaço de Hilbert

Para entendermos um pouco da mecânica quântica necessária para a computação quântica e informação quântica, precisamos ter uma compreensão minuciosa de alguns conceitos

básicos da álgebra linear. Logo, apresentaremos os elementos básicos da álgebra linear para se ter uma melhor compreensão dos conceitos fundamentais da computação quântica e informação quântica. Sabemos que a Álgebra Linear estuda operações lineares em espaços vetoriais, mas na Mecânica Quântica o espaço vetorial utilizado é o famoso espaço de Hilbert ( $\mathcal{H}$ ) ou espaço vetorial complexo  $\mathbb{C}^n$  e linear. Complexo, porque as componentes de um vetor de estado tem valores complexos e linear, porque a soma dos vetores e a multiplicação de vetores por números produzem vetores no mesmo espaço.

Espaços de Hilbert são uma classe especial de espaços normados ou espaços de Banach, mas historicamente os espaços de Hilbert surgiram primeiro. Toda a teoria destes espaços foram criados pelo matemático alemão David Hilbert por volta de 1912, onde os elementos abstratos do espaço de Hilbert são denominados de vetores [36]. Esse espaço vetorial é dotado de um produto interno, ou seja, noções de distância e ângulos e obedece a relação de completude, garantindo que os limites existem quando esperados, o que permite e facilita diversas definições de análise. Logo na mecânica quântica um sistema físico é descrito por um espaço de Hilbert complexo que contém os vetores de estado, que contém todas as informações do sistema.

Observemos algumas propriedades fundamentais que constituem o espaço de Hilbert [35], são elas:

**1ª propriedade :** É um espaço vetorial sobre números complexos  $\mathbb{C}$ , os vetores são denotados por  $|\psi\rangle$ , conhecido como notação ket de Dirac.

**2ª propriedade :**  $\mathcal{H}$  é um conjunto de objetos chamados vetores, com uma operação de soma de vetores definida de tal forma que:

- i) se dois vetores  $|f\rangle, |g\rangle \in \mathcal{H}$ , então a soma  $|f\rangle + |g\rangle$  também é um vetor de  $\mathcal{H}$ ;
- ii) a soma é comutativa e associativa:  $|f\rangle + |g\rangle = |g\rangle + |f\rangle$  e  $(|f\rangle + |g\rangle) + |h\rangle = |f\rangle + (|g\rangle + |h\rangle)$ ;
- iii) existe em  $\mathcal{H}$  um vetor chamado nulo, tal que  $|f\rangle + 0 = |f\rangle \forall |f\rangle \in \mathcal{H}$ ;
- iv) Definida também uma operação de produto por escalar sendo que  $\alpha$  e  $\beta$  pertencem ao conjunto dos complexos, e  $|f\rangle$  e  $|g\rangle$  são elementos de  $\mathcal{H}$ , logo:

- a)  $\alpha|f\rangle \in \mathcal{H}$
- b)  $(\alpha\beta)|f\rangle = \alpha(\beta|f\rangle)$
- c)  $(\alpha + \beta)|f\rangle = \alpha|f\rangle + \beta|f\rangle$
- d)  $\alpha(|f\rangle + |g\rangle) = \alpha|f\rangle + \alpha|g\rangle$
- e)  $1|f\rangle = |f\rangle$

**3ª propriedade :** O espaço de Hilbert  $\mathcal{H}$  tem um produto interno que é uma função que tem como entrada dois vetores e que produz na saída um número complexo (escalar). O produto interno pode ser escrito pela notação alternativa  $(|f\rangle, |g\rangle)$  ou na notação padrão da mecânica quântica como  $\langle f|g\rangle$  que mapeia um par ordenado de vetores para  $\mathbb{C}$ , definidos por

Sejam  $|f\rangle$  e  $|g\rangle \in \mathcal{H}$ , temos:

- i)  $(|f\rangle, |g\rangle) = (|g\rangle, |f\rangle)^*$  ou  $\langle f|g\rangle = \langle g|f\rangle^*$ ;
- ii)  $(|f\rangle, |g\rangle + |h\rangle) = (|f\rangle, |g\rangle) + (|f\rangle, |h\rangle)$  ou  $\langle f|( |g\rangle + |h\rangle) = \langle f|g\rangle + \langle f|h\rangle$ ;

- iii)  $(|f\rangle, \alpha|g\rangle) = \alpha(|f\rangle, |g\rangle)$  ou  $\langle f|\alpha|g\rangle = \alpha\langle f|g\rangle$ ;  
 iv)  $(\alpha|f\rangle, |g\rangle) = \alpha^*(|f\rangle, |g\rangle)$   
 v)  $(|f\rangle, |f\rangle) \geq 0$ , e  $(|f\rangle, |f\rangle) = 0$  ou  $\langle f|f\rangle \geq 0$  e  $\langle f|f\rangle = 0$  se e somente se  $|f\rangle = 0$  (vetor nulo).

A existência do produto interno em  $\mathcal{H}$  dota o espaço de uma noção natural de distância. Diz-se então que  $\mathcal{H}$  é um espaço métrico. Definimos a norma de um vetor de  $\mathcal{H}$  por  $\| |f\rangle \| = \langle f|f\rangle^{1/2}$ .

Dados dois vetores  $x$  e  $y$  em um Espaço de Hilbert  $\mathcal{H}$ , diz-se que são ortogonais se seu produto interno é zero, ou seja,

$$\langle x|y\rangle = 0 \Rightarrow |x\rangle \perp |y\rangle$$

Uma base de  $\mathcal{H}$  é o menor subconjunto  $\{|e_1\rangle, |e_2\rangle, \dots, |e_N\rangle\}$  de  $\mathcal{H}$  que varre o espaço todo, ou seja, qualquer vetor de  $\mathcal{H}$  pode ser escrito como uma combinação linear dos vetores deste conjunto:

$$|\psi\rangle = \sum_{i=1}^N \alpha_i |e_i\rangle \quad (\text{B.1})$$

Onde dizemos que  $N$  é a dimensão de  $\mathcal{H}$ . Se este conjunto for ortonormal, dizemos que ele é uma base ortonormal de  $\mathcal{H}$ . Bases ortonormais são muito convenientes para expressar vetores de  $\mathcal{H}$ .

### B.3 Sistemas Compostos

Suponha que estejamos interessados em dois sistema quânticos  $A$  e  $B$  descritos por estados nos espaços de Hilbert  $\mathcal{H}_A$  e  $\mathcal{H}_B$ , respectivamente. Sendo assim, o espaço de Hilbert do sistema composto  $(A + B)$  é dado pelo produto tensorial dos espaços  $\mathcal{H}_A$  e  $\mathcal{H}_B$ , ou seja:

$$\mathcal{H} = \mathcal{H}^{\otimes(A+B)} \equiv \mathcal{H}_A \otimes \mathcal{H}_B \quad (\text{B.2})$$

Onde seus estados atuam no espaço de Hilbert  $\mathcal{H}$ . Logo, o produto tensorial é uma forma de juntar os espaços vetoriais maiores, sendo essa tecnica importante na mecânica quântica para sistemas com muitas partículas.

Consideremos  $|\psi_1\rangle$  e  $|\psi_2\rangle$  estados puros (Um ensemble que pode ser descrito por um único vetor de estado  $|\psi\rangle$ , se diz que está num estado puro) do sistema  $A$ , e  $|\phi_1\rangle$  e  $|\phi_2\rangle$  estados puros do sistema  $B$ , logo:

$$|\psi\rangle \equiv \alpha |\psi_1\rangle \otimes |\phi_1\rangle + \beta |\psi_1\rangle \otimes |\phi_2\rangle, \quad |\alpha|^2 + |\beta|^2 = 1 \quad (\text{B.3})$$

Que é um estado do sistema composto de 'A + B', não sendo ainda o estado mais geral. De forma genérica, vamos considerar  $\{|e_i\rangle\}$ , com  $i = 1, \dots, m$  sendo a base de  $\mathcal{H}_A$  e  $\{|f_j\rangle\}$ , com  $j = 1, \dots, n$  sendo a base de  $\mathcal{H}_B$ , então cada vetor (estado puro) em  $\mathcal{H}$  pode ser escrito da seguinte maneira:

$$|\psi\rangle = \sum_{ij} c_{ij} |e_i\rangle \otimes |f_j\rangle \quad (\text{B.4})$$

para alguns coeficientes complexos  $c_{ij}$ . Notoriamente a mecânica quântica admite mais estados para um sistema composto do que a mecânica clássica. De fato, no caso clássico, se os estados dos subsistemas A e B são descritos por conjuntos de coordenadas  $x_\mu^{(A)}$  e  $x_\nu^{(B)}$ , então o estado do sistema composto está caracterizado por o conjunto de coordenadas  $\{x_\mu^{(A)}, x_\nu^{(B)}\}$ . Isto significa que o espaço do sistema composto tem uma estrutura de produto cartesiano dos espaços dos subsistemas, distinta daquela de produto tensorial no caso quântico. Os estados produto da forma:

$$|\psi\rangle \otimes |\phi\rangle, |\phi\rangle \in \mathcal{H}_B \quad (\text{B.5})$$

são chamados de separáveis; todos os outros estados, ou seja, aqueles que não podem ser escritos como um produto tensorial simples (por exemplo, de dois estados) são chamados de emaranhados.

## B.4 Conclusão

Neste apêndice foram mostrados resumidamente alguns conceitos de estados quânticos, espaço de Hilbert e suas respectivas propriedades, e por último, um pouco do conceito de sistemas compostos.