



UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM FÍSICA

**Estados Parcialmente Emaranhados em Comunicação
Quântica**

Raphael Fortes Infante Gomes

São Carlos
2012

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM FÍSICA

**Estados Parcialmente Emaranhados em Comunicação
Quântica**

Raphael Fortes Infante Gomes

Esta dissertação contém as correções e alterações
sugeridas pela Comissão Julgadora durante a defesa
realizada por Raphael Fortes Infante Gomes em 16/03/2012.

Universidade Federal de São Carlos.

Departamento de Física.

Área de Concentração: Física Estatística.

Orientador: Prof. Dr. Gustavo Garcia Rigolin.

São Carlos

2012

**Ficha catalográfica elaborada pelo DePT da
Biblioteca Comunitária da UFSCar**

G633ep

Gomes, Raphael Fortes Infante.

Estados parcialmente emaranhados em comunicação
quântica / Raphael Fortes Infante Gomes. -- São Carlos :
UFSCar, 2012.

112 f.

Dissertação (Mestrado) -- Universidade Federal de São
Carlos, 2012.

1. Física quântica. 2. Teletransporte de estados
quânticos. 3. Emaranhamento. 4. Teoria da informação
quântica. I. Título.

CDD: 539 (20^a)

Raphael Fortes Infante Gomes

Dissertação de Mestrado submetida à
Coordenação do Programa de Pós-
Graduação em Física, da Universidade
Federal de São Carlos, como requisito
parcial para a obtenção do título de
Mestre em Ciências.

Aprovada em 16/03/2012.

BANCA EXAMINADORA



Prof. Dr. Gustavo Garcia Rigolin
Universidade Federal de São Carlos - DF



Prof. Dr. Celso Jorge Villas-Boas
Universidade Federal de São Carlos - DF



Prof. Dr. Thiago Rodrigues de Oliveira
Universidade Federal Fluminense - IF

Agradecimentos

Agradeço de coração a meus pais, Ricardo e Regina, e a meu irmão Bernardo, por me fazerem acreditar que sonhos são possíveis. Sem eles, este trabalho não existiria.

Ao professor Gustavo Rigolin, por exercer com maestria o papel de orientador e contribuir com minha formação sob diversos aspectos.

Ao amigo Alexandre, que esteve presente em todos os momentos, principalmente nos mais difíceis.

À Mariana, que ajudou de formas que talvez nem ela imagine, me apoiando tanto no desenvolvimento do trabalho quanto em outras questões.

Aos pais da Mariana, Samuel e Sueli, pelos conselhos valiosos e ajuda em todas as circunstâncias.

À todos os meus familiares, em especial a meus tios João e Lúcia, que foram essenciais ao longo desta jornada.

Aos amigos Leonardo Guimarães, Thiago Freire, Matheus Piva, Flávio Lazzarotto, Richard Neil, Leonardo Rosa e Cíntia Marcellos, por contribuírem de forma tão especial, cada um à sua maneira.

Aos professores Gilmar Eugênio Marques, Celso Villas-Bôas e Fernando M. Araujo-Moreira, amigos verdadeiros presentes desde o início.

Aos professores João Chafi, João Batista de Oliveira, Luiz Henrique Barbosa, José Carlos Grizendi, Nelson Ragazzi, Niciléa Peixoto, Carlos Eduardo Noguères e Fabrício, por me fazerem acreditar sempre.

Aos amigos que não tiveram seus nomes citados e aos colegas na Universidade.

E, finalmente, à Capes, pelo auxílio financeiro durante estes dois anos de mestrado.

Resumo

Nesta dissertação abordamos o emaranhamento entre estados quânticos como um recurso a ser utilizado na transmissão de informação quântica, em especial no teletransporte quântico. Nosso foco foi direcionado para o estudo de estados quânticos parcialmente emaranhados, isto é, estados nos quais o teor de emaranhamento está aquém do máximo valor permitido pela mecânica quântica, visto que são mais prováveis de serem encontrados em dispositivos reais do que seriam estados maximamente emaranhados. Revisamos as propriedades e conceitos que caracterizam vetores e operadores sob a ótica da álgebra linear para em seguida apresentarmos formalmente os postulados da mecânica quântica. Introduzimos a noção de *qubits* e mostramos como estes podem ser aplicados em tarefas computacionais através de portas lógicas quânticas. Explicamos com detalhes os principais protocolos de teleporte quântico que originaram os métodos utilizados neste trabalho, destacando as vantagens e desvantagens de cada um. Apresentamos protocolos com arranjos inéditos e introduzimos técnicas que aperfeiçoaram alguns dos métodos de teleporte conhecidos, fornecendo alternativas para estes em relação à construção e arquitetura na disposição dos canais. Provamos que a probabilidade associada ao teleporte múltiplo de um *qubit* através de canais em série tende ao limite máximo para um caso especial. Mostramos que estados imperfeitos podem ser corrigidos e que é possível transmitir um *qubit* isolado ou um par de *qubits* empregando estados GHZ e modificações de estados da base de Bell. Discutimos a relação entre o valor da probabilidade de sucesso final e o grau de emaranhamento das bases e dos canais para cada método. Encerramos a dissertação com uma análise geral sobre todos os protocolos, destacando os mais eficientes com argumentos que englobam pontos de vista tanto teórico como prático.

Palavras-chave: Teleporte quântico. Emaranhamento. Teoria de informação quântica.

Abstract

In this master's thesis we approach the entanglement between quantum states as a resource to be used in the transmission of quantum information, particularly in quantum teleportation. Our focus was directed toward the study of partially entangled quantum states, that is, states in which the entanglement degree is below the maximum value allowed by quantum mechanics, since they are more likely to be found in actual devices than maximally entangled states. We review the properties and concepts that characterize vectors and operators from the viewpoint of linear algebra to formally present the postulates of quantum mechanics. We introduced the notion of qubits and showed how these can be applied to computing tasks via quantum logic gates. We explained in details the main quantum teleportation protocols that originated the methods used in this work, highlighting the advantages and disadvantages of each one. We presented protocols with new arrangements and introduced techniques that have improved some of the known methods, providing for those alternatives relating to construction and architecture in the arrangement of the channels. We proved that the probability associated with a multiple teleportation of a single qubit through channels in series tends to the maximum limit for a special case. We showed that imperfect states can be corrected and that it is possible to transmit a single qubit or a pair of qubits using GHZ states and modification of Bell basis' states. We discussed the relationship between the final success probability value and the bases and channels' degree of entanglement for each method. We concluded the thesis with a general analysis of all protocols, highlighting the most efficient ones with arguments that include theoretical and practical viewpoints.

Keywords: Quantum teleportation. Entanglement. Quantum information theory.

Sumário

Lista de Figuras	xiii
Lista de Tabelas	xvii
1 Introdução	1
1.1 Considerações Preliminares	2
1.2 Objetivos	2
1.3 Contribuições	2
1.4 Organização do Trabalho	3
2 Fundamentos	5
2.1 Vetores	5
2.2 Operadores	11
2.3 Representação Matricial	14
2.4 Os Postulados da Mecânica Quântica	21
2.4.1 Postulado I (Benenti et al., 2007)	21
2.4.2 Postulado II (Benenti et al., 2007)	22
2.4.3 Postulado III (Benenti et al., 2007)	25
2.5 Qubits e Sistemas de Dois Níveis	27
2.6 Operador e Matriz Densidade	30
2.7 Portas Lógicas	39
2.7.1 Portas de um <i>Qubit</i>	39
2.7.2 Portas de dois <i>Qubits</i>	41
3 Canais Perfeitamente Emaranhados: O Protocolo Original	45
3.1 O Protocolo Original	45
4 Canais Parcialmente Emaranhados	53
4.1 Teleporte com Evolução Unitária	53
4.2 Teleporte com Base de Bell Generalizada	56
4.3 Teleporte Múltiplo com Fidelidade Um	58
4.3.1 Protocolo 1	59

4.3.2	Protocolo 2	62
4.3.3	Protocolo 3	65
5	Teleporte de um <i>Qubit</i>: Novos Protocolos	69
5.1	Teleporte Múltiplo e Evolução Unitária	69
5.2	Teleporte Múltiplo com Sucesso Apenas no Fim	72
5.3	Base GHZ Generalizada	75
5.3.1	Correção dos estados restantes	79
6	Teleporte de Dois <i>Qubits</i>	81
6.1	Utilizando dois Canais Paralelos	81
6.1.1	Escolhendo $m_a=m_b=n$	84
6.1.2	Enviando $\alpha 00\rangle + \beta 11\rangle$	85
6.2	Base GHZ e Canal GHZ	89
6.3	Base Generalizada e Canal GHZ	93
6.4	Base GHZ e Canais Paralelos	97
7	Conclusões	101
A	Probabilidade Máxima Associada ao Teleporte Múltiplo em Série	105
	Referências Bibliográficas	111

Lista de Figuras

2.1	Representação de $ \Psi\rangle$ na Esfera de Bloch. Fonte: Figura adaptada de Nielsen and Chuang, 2004.	28
2.2	Portas que atuam em um qubit, suas respectivas nomenclaturas e representações matriciais. Fonte: Figura adaptada de Benenti et al., 2007.	41
2.3	Figura esquemática para portas de dois qubits. Em (a): controle no primeiro qubit. Em (b): controle no segundo qubit. O círculo menor preenchido representa a ativação da porta quando o qubit de controle for $ 1\rangle$, e o círculo menor vazio representa a ativação quando o qubit de controle for $ 0\rangle$. Fonte: Figura adaptada de Benenti et al., 2007.	42
2.4	Portas que atuam em dois qubit, suas respectivas nomenclaturas e representações matriciais. Fonte: Figura adaptada de Benenti et al., 2007.	43
2.5	Construindo portas de dois qubits a partir de portas de um qubit. Em (a): a porta <i>CNOT</i> com controle no segundo qubit. Em (b): a porta <i>Swap</i> . Em (c): a porta <i>Z – Controlada</i> com controle no primeiro qubit. Fonte: Figura adaptada de Benenti et al., 2007.	44
3.1	Teleporte de informação quântica entre dois pontos distintos utilizando um canal emaranhado. As cores vermelha e azul referem-se à Alice e Bob, respectivamente. As casas representam os pontos inicial e final do processo de teleporte. Os qubits que constituem o canal foram destacados para melhor visualização. A barra vermelha representa o canal formado pelo estado emaranhado entre estes qubits.	46
3.2	Canal formado pelo estado emaranhado entre o qubit de Alice (vermelho) e o de Bob (azul). No lado esquerdo, a informação original representada pelo qubit amarelo de Alice.	47
3.3	Elementos básicos de um protocolo de teleporte quântico: o qubit amarelo representa a informação original, e o canal emaranhado é representado pelo par de qubits vermelho (Alice) e azul (Bob). A barra vermelha e o sinal ondulatório em verde reforçam a idéia de que o canal é emaranhado. Os cabos pretos e os monitores em cinza representam respectivamente a base de medidas escolhida por Alice e o resultado destas medidas.	49

3.4 Procedimento padrão após Alice medir o sistema. Os dois qubits medidos são afetados e formam um estado emaranhado distinto do estado inicial que constituía o canal. Após a confirmação dos resultado das medidas de Alice através de um canal clássico, Bob sabe quais as transformações necessárias a serem aplicadas para que seu estado seja idêntico ao original enviado por Alice. 51

4.1 Teleporte de um qubit utilizando um canal maximamente emaranhado. A seta cinza indica que os qubits estão emaranhados. 54

4.2 Teleporte de um qubit utilizando um canal parcialmente emaranhado. A seta cinza é menor do que na figura 4.1 e está associada ao índice n , para reforçar a idéia de que o emaranhamento é inferior ao de estados maximamente emaranhados. 54

4.3 Disposição dos canais em série entre Alice e Bob. Neste modelo, Alice possui apenas o primeiro canal e Bob tem acesso a todos os outros e ao último qubit. 60

4.4 Para o protocolo 1: Do nível inferior até o topo, as curvas representam P_{suc}^{total} após $q= 2, 4, 6, 8, 10$ e 12 teleportes sucessivos. A linha tracejada mostra a probabilidade ótima ($1/2$) usando o protocolo apresentado na seção 4.2. Todas as grandezas são adimensionais. **Fonte:** Figura adaptada de Rigolin, 2009. 62

4.5 Para o protocolo 2: as curvas mostram P_{suc}^{total} após $q= 1, 2, 3, 4, 5$ e 6 teleportes sucessivos. A linha tracejada mostra a probabilidade ótima ($1/2$) usando o protocolo apresentado na seção 4.2. Todas as grandezas são adimensionais. **Fonte:** Figura adaptada de Rigolin, 2009. 65

4.6 Disposição dos canais em série entre Alice e Bob com o grau de emaranhamento diminuindo exponencialmente após o segundo canal. Neste modelo, Alice possui apenas o primeiro canal e Bob tem acesso a todos os outros e ao último qubit. 66

4.7 Do nível inferior até o topo, as curvas representam P_{suc}^{total} após $q= 2, 3, 4, 5$ e 6 teleportes sucessivos utilizando o protocolo 3. A linha tracejada mostra a probabilidade ótima ($1/2$) usando o protocolo apresentado na seção 4.2. **Fonte:** Figura adaptada de Rigolin, 2009. 68

5.1 Disposição dos canais em série entre Alice e Bob. Neste modelo, Alice possui apenas o primeiro canal e Bob só tem acesso ao último qubit. 73

5.2 Teleporte de um qubit utilizando dois canais paralelos e medidas na base GHZ generalizada. 76

6.1	Teleporte de dois qubits utilizando dois canais paralelos e medidas na base de Bell generalizada.	82
6.2	Teleporte de dois qubits utilizando um canal GHZ generalizado e medidas na base GHZ generalizada.	90
6.3	Teleporte de dois qubits utilizando um canal GHZ generalizado e medidas na base de Bell generalizada.	94
6.4	Teleporte de dois qubits utilizando canais paralelos e medidas na base GHZ generalizada.	98

Lista de Tabelas

3.1	Resultados possíveis para as medidas de Alice e as respectivas correções que Bob precisa aplicar.	50
4.1	Estrutura final dos qubits que não alcançaram fidelidade um após o segundo teleporte e os respectivos resultados das medidas associadas.	64
4.2	Estrutura final dos qubits que não alcançaram fidelidade um após o terceiro teleporte e as respectivas seqüências das medidas associadas.	64

Capítulo 1

Introdução

Foi somente anos depois da formulação da mecânica quântica e da teoria da informação e um bom tempo após o surgimento da computação digital em larga escala que finalmente percebeu-se que a física quântica poderia atuar sensivelmente sobre o processamento de informação e a computação digital. O início da teoria da informação quântica pode ser atribuído a Von Neumann, que, vinte anos antes de Shannon, introduziu a noção de entropia quântica através de um operador densidade.

Esta área da mecânica quântica lida com conceitos relacionados a estados quânticos, canais, medidas e entropia, e o teletransporte (ou teleporte) quântico é sem dúvida uma das linhas de pesquisa mais relevantes. Basicamente, o teleporte quântico é um processo em que uma determinada informação relacionada a um estado quântico é transmitida de um ponto a outro. Para isso, é necessário que exista um aparato de medidas disponível para o emissor (Alice) e que o receptor (Bob) consiga reconstruir o estado original ao fim do processo. Durante algum tempo, acreditou-se que o teleporte seria uma mera conjectura já que existem observáveis que não comutam e portanto não podem ser medidos simultaneamente em uma única cópia de um estado quântico. Bennett, Brassard, Crepeau, Jozsa, Peres, and Wootters (Bennett et al., 1993) demonstraram a viabilidade do teleporte utilizando um canal constituído de um par emaranhado semelhante a um estado da base de Bell. A idéia básica por trás do processo é a codificação e a divisão da informação em duas partes, uma quântica e outra clássica, enviadas separadamente por um canal quântico (o par emaranhado) e outro clássico, respectivamente. Este último nada mais é do que um meio de comunicação comum (como *e-mail*, telefone, etc;) pelo qual emissor e receptor podem intercambiar informações. Quanto ao par emaranhado, existe um problema associado à sua estrutura devido ao fato de o canal ser quântico: a decoerência. Quando ela ocorre, o emaranhamento é gradativamente destruído. Em vista disso, priorizamos neste trabalho o uso de estados parcialmente emaranhados, uma vez que simulam estados reais de forma mais eficaz. Nosso principal objetivo foi a utilização destes estados na construção de novos mecanismos de teleporte quântico.

1.1 Considerações Preliminares

O emaranhamento de sistemas quânticos desempenha um papel central na discussão de correlações não locais (Einstein et al., 1935) e é um dos ingredientes fundamentais para o bom funcionamento de alguns algoritmos em computação quântica (Shor, 1996; Grover, 1996) e também para a implementação de protocolos de comunicação quântica, tais como criptografia quântica (Ekert, 1991; Tittel et al., 1998) teletransporte (Bennett et al., 1993) e codificação superdensa (Bennett and Wiesner, 1992; Braunstein and Kimble, 2000). Junto com a computação e a comunicação quânticas, o emaranhamento quântico passou a ser um assunto muito investigado (Nielsen and Chuang, 2004; Braunstein and van Loock, 2005 e Dirk et al., 2000) no final da década de 1990 e início do século *XXI*, dando origem à teoria de informação quântica, uma nova área multidisciplinar envolvendo físicos, químicos, matemáticos e cientistas da computação.

Neste trabalho, priorizamos a reformulação de procedimentos conhecidos (relacionados a teleporte quântico) e a idealização de novos protocolos de teletransporte, visando sempre superar ou igualar a eficiência de métodos que já operam em dispositivos práticos e de outros que ainda não foram implementados no mercado. Para isso, direcionamos nosso foco para a análise do grau de emaranhamento (*entanglement*) dos estados envolvidos nestes procedimentos, visando obter resultados cada vez melhores para a probabilidade de sucesso no envio de informação quântica dos métodos propostos.

1.2 Objetivos

Temos dois objetivos centrais:

- (1) Descobrir novos protocolos e tarefas informacionais quânticos onde estados parcialmente emaranhados possam ser empregados em sua execução.
- (2) Superar a eficiência de protocolos conhecidos e analisar a viabilidade de substituí-los por aqueles que apresentaremos neste trabalho. Dessa forma introduziremos não somente novos resultados como também mecanismos e arranjos que podem ser empregados como alternativas aos protocolos de teleporte já existentes.

1.3 Contribuições

Ao redigir esta dissertação, acrescentamos as seguintes contribuições:

- (1) O melhor cenário em Rigolin, 2009 representava o método mais eficiente de teleporte múltiplo de um *qubit* com canais parcialmente emaranhados dispostos em série, onde o receptor (Bob) compartilhava um canal com o emissor (Alice) e mantinha os restantes em sua posse. Conseguimos aperfeiçoar este protocolo ao corrigir

estados imperfeitos gerados em qualquer etapa de teleporte e demonstramos que a probabilidade total de sucesso tende ao limite máximo permitido para teleportes de um *qubit* em série.

- (2) Quando os canais intermediários não estão em posse do emissor e nem do receptor, o melhor resultado para a transmissão de um *qubit* através de uma cadeia de pares emaranhados dispostos em série está em [Perseguers et al., 2008](#) e ocorre quando há uma seqüência de destilação entre estes pares. Construímos um protocolo de teleporte múltiplo que atinge a mesma eficiência, e, portanto, este último pode ser empregado para substituir o primeiro.
- (3) Finalmente, apresentamos nos capítulos [5](#) e [6](#) configurações alternativas que atingem a mesma eficiência dos protocolos restantes discutidos no capítulo [4](#).

1.4 Organização do Trabalho

O trabalho pode ser dividido em quatro etapas.

A primeira etapa é representada pelo capítulo [2](#) e consiste da formulação teórica de todos os conceitos necessários para a compreensão desta dissertação.

Na segunda etapa, concentramos nossa análise explicando o funcionamento de protocolos que envolvem canais perfeitamente emaranhados e parcialmente emaranhados. No capítulo [3](#) apresentaremos o teleporte quântico original seguindo a mesma estrutura do artigo que deu origem a este tema, e no capítulo [4](#) abordaremos canais parcialmente emaranhados explicando detalhadamente as fontes mais relevantes para este trabalho. Com isso, terminamos a segunda etapa.

Para a etapa seguinte, dividimos nossos resultados em dois capítulos. No capítulo [5](#) falaremos sobre teleportes que envolvem um único *qubit*, e no capítulo [6](#) encerraremos a terceira etapa estendendo estes conceitos ao construir protocolos que transmitam dois *qubits*.

No capítulo [7](#) concluiremos a quarta e última etapa reunindo os principais resultados obtidos e discutindo a relevância dos protocolos mais eficientes.

Capítulo 2

Fundamentos

Este capítulo apresenta os conceitos fundamentais para a compreensão de todo o trabalho (Nielsen and Chuang, 2004; Benenti et al., 2007; Mermin, 2007). Na primeira parte, introduziremos as ferramentas matemáticas necessárias para a análise dos postulados da mecânica quântica, dentre estas uma revisão de álgebra linear e a notação de "bra" e "ket". Na sequência falaremos de alguns tópicos mais específicos no ramo da informação quântica, como as diferentes notações para o produto tensorial e o conceito de fidelidade. De posse destas informações, estaremos aptos a discorrer sobre os protocolos básicos de transmissão de informação quântica nos capítulos seguintes.

2.1 Vetores

Iniciaremos esta seção revisando conceitos básicos relativos a vetores, que serão representados segundo a notação introduzida por Dirac. Para cada vetor existe uma representação simbólica $|\cdot\rangle$ conhecida como "ket" e um vetor associado $\langle\cdot|$ chamado de "bra", sendo este último a representação das componentes do primeiro vetor no espaço conhecido como dual.

Sejam dois vetores $|a\rangle = (a_1, \dots, a_n)$ e $|b\rangle = (b_1, \dots, b_n)$. Se $|c\rangle = |a\rangle + |b\rangle$, então

$$c_i = a_i + b_i, \quad (i = 1, \dots, n). \quad (2.1)$$

Exemplo:

$$|a\rangle = (2, 4, 6, 8), \quad |b\rangle = (1, 3, 5, 7).$$

$$\text{Então : } c_1 = 3, c_2 = 7, c_3 = 11, c_4 = 15.$$

$$\text{Logo, } |c\rangle = (3, 7, 11, 15). \quad (2.2)$$

Propriedades aditivas:

$$\begin{aligned}
|a\rangle + |b\rangle &= |b\rangle + |a\rangle; \\
|a\rangle + (|b\rangle + |c\rangle) &= (|a\rangle + |b\rangle) + |c\rangle.
\end{aligned}
\tag{2.3}$$

Propriedades multiplicativas:

Sejam dois números complexos quaisquer, m e n . Então:

$$\begin{aligned}
m(|a\rangle + |b\rangle) &= m|a\rangle + m|b\rangle; \\
(m + n)|a\rangle &= m|a\rangle + n|a\rangle; \\
(mn)|a\rangle &= m(n|a\rangle).
\end{aligned}
\tag{2.4}$$

Independência linear:

Um conjunto de vetores $|u_1\rangle, |u_2\rangle, |u_3\rangle, \dots, |u_n\rangle$ forma uma base linearmente independente quando a equação

$$m_1|u_1\rangle + m_2|u_2\rangle + m_3|u_3\rangle + \dots + m_n|u_n\rangle = 0
\tag{2.5}$$

é satisfeita se e somente se $m_i = 0$, ($i = 1, \dots, n$), para qualquer número complexo m_i .

Exemplo: para os vetores $|u_1\rangle = (1, 0, 0)$, $|u_2\rangle = (0, -1, 0)$ e $|u_3\rangle = (0, 0, i)$, a equação

$$\begin{aligned}
m_1|u_1\rangle + m_2|u_2\rangle + m_3|u_3\rangle = 0 &\Rightarrow m_1(1, 0, 0) + m_2(0, -1, 0) + m_3(0, 0, i) = (0, 0, 0) \Rightarrow \\
&\Rightarrow (m_1, -m_2, im_3) = (0, 0, 0)
\end{aligned}
\tag{2.6}$$

só possui a solução $m_1 = m_2 = m_3 = 0$. Portanto, $|u_1\rangle, |u_2\rangle$ e $|u_3\rangle$ são linearmente independentes.

Produto escalar:

Para dois vetores quaisquer $|a\rangle = (a_1, \dots, a_n)$ e $|b\rangle = (b_1, \dots, b_n)$, definimos o

produto escalar como

$$\langle a|b\rangle = a_1^*b_1 + a_2^*b_2 + a_3^*b_3 + \dots + a_n^*b_n = \sum_{i=1}^n a_i^*b_i; \quad (2.7)$$

onde $\langle a|$ é chamado de vetor dual de $|a\rangle$ e cada componente de $\langle a| = (a_1^*, \dots, a_n^*)$ é o complexo conjugado das componentes correspondentes de $|a\rangle$. Disso segue que (Benenti et al., 2007):

$$\begin{aligned} \langle a|b\rangle &= \langle b|a\rangle^*; \\ \langle a|mb\rangle &= m\langle a|b\rangle; \quad \langle ma|b\rangle = m^*\langle a|b\rangle; \\ \langle a|(m|b\rangle + n|c\rangle) &= m\langle a|b\rangle + n\langle a|c\rangle; \quad (\langle ma| + \langle nb|)|c\rangle = m^*\langle a|b\rangle + n^*\langle a|c\rangle; \\ \langle a|a\rangle &\geq 0; \quad \langle b|b\rangle \geq 0; \\ |\langle a|b\rangle|^2 &\leq \langle a|a\rangle\langle b|b\rangle; \end{aligned} \quad (2.8)$$

para dois números complexos quaisquer m e n . A última propriedade é conhecida como desigualdade de Cauchy-Schwarz. Alguns exemplos:

$$\begin{aligned} |a\rangle &= (2 + i, 4, 6), \quad |b\rangle = (1, 3, i). \\ \text{Então : } \langle a| &= (2 - i, 4, 6), \quad \langle b| = (1, 3, -i). \\ \langle a|a\rangle &= (4 + 1) + (16) + (36) = 57, \quad \langle b|b\rangle = (1) + (9) + (1) = 11, \quad \langle a|a\rangle\langle b|b\rangle = 627. \\ \langle a|b\rangle &= (2 - i) + (12) + (6i) = 14 + 5i, \quad |\langle a|b\rangle|^2 = (14)^2 + (5)^2 = 221 \leq 627. \end{aligned} \quad (2.9)$$

Normalização:

Adotaremos como convenção trabalhar com os vetores em sua forma normalizada, pois sempre nos deparamos com situações que exigem esta condição, como na definição da base de um espaço vetorial ou para satisfazer os postulados da mecânica quântica, sobre os quais falaremos na próxima seção. As situações em que mostrarmos vetores não-normalizados pertencerão a casos especiais nos quais a normalização foi omitida apenas para fins de clareza nas explicações.

Para um vetor qualquer $|v\rangle = (v_1, \dots, v_n)$ em um espaço de dimensão n , podemos normalizá-lo através da seguinte expressão:

$$|v'\rangle = \frac{|v\rangle}{|v|}, \quad (2.10)$$

onde $|v| = \sqrt{\langle v|v \rangle} = \sqrt{\sum_{i=1}^n |v_i|^2}$ é o módulo (ou norma) de $|v\rangle$.

Voltando ao exemplo anterior:

$|a\rangle = (2 + i, 4, 6)$, $\langle a|a \rangle = 57$. O vetor normalizado $|a'\rangle$ será

$$|a'\rangle = \frac{|a\rangle}{|a|} = \frac{1}{\sqrt{57}}(2 + i, 4, 6). \quad (2.11)$$

Ortogonalidade:

Dois vetores $|a\rangle = (a_1, \dots, a_n)$ e $|b\rangle = (b_1, \dots, b_n)$ são ortogonais se

$$\langle a|b \rangle = \sum_{i=1}^n a_i^* b_i = 0. \quad (2.12)$$

Exemplo: os vetores $|a\rangle = (1, 0, -1)$ e $|b\rangle = (1, 0, 1)$ são ortogonais.

$$\langle a|b \rangle = (1) + (0) + (-1) = 0. \quad (2.13)$$

Ortonormalidade:

Um conjunto de vetores $|u_1\rangle, |u_2\rangle, |u_3\rangle, \dots, |u_n\rangle$ forma uma base ortonormal quando

$$\begin{aligned} \langle u_i|u_j \rangle &= 0 \text{ se } i \neq j, \quad \langle u_i|u_j \rangle = 1 \text{ se } i = j; \text{ ou seja:} \\ \langle u_i|u_j \rangle &= \delta_{ij}, \end{aligned} \quad (2.14)$$

onde δ_{ij} é a delta de Kronecker.

Exemplo: para um espaço de dimensão 2, os vetores $|a\rangle = (1, 0)$ e $|b\rangle = (0, 1)$ formam uma base ortonormal:

$$\langle a|a \rangle = 1, \quad \langle b|b \rangle = 1, \quad \langle a|b \rangle = \langle b|a \rangle = 0. \quad (2.15)$$

Para construir um espaço vetorial de dimensão n , precisamos de uma base com n vetores $|u_1\rangle, |u_2\rangle, |u_3\rangle, \dots, |u_n\rangle$ que satisfaça à condição acima. Este conjunto de vetores não é único - de fato, existem infinitos - e cada um origina uma base específica. Uma vez escolhida a base, podemos expandir um vetor $|v\rangle$ de dimensão n em termos dos

vetores desta base através da relação

$$|v\rangle = \sum_{i=1}^n C_i^u |u_i\rangle, \quad (2.16)$$

na qual, devido à condição de ortonormalidade $\langle u_i | u_j \rangle = \delta_{ij}$, os coeficientes C_i^u são dados por

$$C_i^u = \langle u_i | v \rangle, \quad (2.17)$$

também conhecidos como amplitudes de probabilidade (veja a seção 2.4.1).

Uma propriedade que merece destaque é a da **Relação de Completeza**. Na próxima seção definiremos o conceito de operadores, mas podemos introduzi-lo através deste exemplo. Seja $|v\rangle$ um vetor de dimensão n e seja o operador

$$\sum_{i=1}^n |u_i\rangle \langle u_i|, \quad (2.18)$$

onde os vetores $|u_i\rangle$ são estados de uma base com a mesma dimensão de $|v\rangle$. Se aplicarmos este operador sobre o vetor $|v\rangle$, veremos que:

$$\left(\sum_{i=1}^n |u_i\rangle \langle u_i| \right) |v\rangle = \sum_{i=1}^n |u_i\rangle \langle u_i | v \rangle = \sum_{i=1}^n \langle u_i | v \rangle |u_i\rangle = \sum_{i=1}^n C_i^u |u_i\rangle = |v\rangle, \quad (2.19)$$

e, portanto,

$$\sum_{i=1}^n |u_i\rangle \langle u_i| = I. \quad (2.20)$$

A Relação de Completeza é válida independentemente da base de estados escolhida.

Produto Tensorial:

Todas as relações vistas até o momento abordaram propriedades de vetores que residiam em um mesmo espaço vetorial, e, logicamente, possuíam a mesma dimensão. Mas o que ocorre se precisarmos analisar vetores em espaços distintos e com dimensões que não sejam necessariamente as mesmas? Nesta situação, recorreremos ao uso do produto tensorial, que conecta os espaços vetoriais relacionados aos diferentes sistemas e une-os em apenas um, denominado sistema composto. O produto tensorial mantém algumas das propriedades e conceitos vistos em sistemas simples, como veremos a seguir.

Sejam $|v_1\rangle$ um vetor que reside em um espaço vetorial H_1 de dimensão N_1 e

$|v_2\rangle$ um vetor que reside em um espaço vetorial H_2 de dimensão N_2 . Se nosso sistema for composto e estivermos analisando os dois vetores simultaneamente, então ele pertence ao espaço $H = H_1 \otimes H_2$ e sua dimensão será $N = N_1 \times N_2$, onde as seguintes propriedades são válidas (Benenti et al., 2007):

$$\begin{aligned} m(|v_1\rangle \otimes |v_2\rangle) &= (m|v_1\rangle) \otimes |v_2\rangle = |v_1\rangle \otimes (m|v_2\rangle); \\ (|v_1\rangle + |a_1\rangle) \otimes |v_2\rangle &= |v_1\rangle \otimes |v_2\rangle + |a_1\rangle \otimes |v_2\rangle; \\ |v_1\rangle \otimes (|b_2\rangle + |v_2\rangle) &= |v_1\rangle \otimes |b_2\rangle + |v_1\rangle \otimes |v_2\rangle; \end{aligned} \tag{2.21}$$

para qualquer escalar complexo m onde $|a_1\rangle \in H_1$ e $|b_2\rangle \in H_2$.

Exemplo: Sejam $N_1 = 1$, $N_2 = 3$, $|v_1\rangle = |u_1\rangle$ e $|v_2\rangle = \frac{1}{\sqrt{3}}(|w_1\rangle + |w_2\rangle + |w_3\rangle)$. Se $|v\rangle = |v_1\rangle \otimes |v_2\rangle$, então

$$|v\rangle = |v_1\rangle \otimes |v_2\rangle = \frac{1}{\sqrt{3}}(|u_1\rangle \otimes |w_1\rangle + |u_1\rangle \otimes |w_2\rangle + |u_1\rangle \otimes |w_3\rangle). \tag{2.22}$$

Se $|g_a\rangle = \sum_{k=1}^{N_2} \sum_{i=1}^{N_1} D_{i,k}(|u_i\rangle \otimes |w_k\rangle)$ e $|g_b\rangle = \sum_{l=1}^{N_2} \sum_{j=1}^{N_1} E_{j,l}(|u_j\rangle \otimes |w_l\rangle)$ para coeficientes complexos $D_{i,k}$ e $E_{j,l}$ e algum conjunto de estados de base $|u_i\rangle$ em H_1 e $|w_k\rangle$ em H_2 , o produto escalar entre $|g_a\rangle$ e $|g_b\rangle$ é

$$\langle g_a | g_b \rangle = \sum_{k,l=1}^{N_2} \sum_{i,j=1}^{N_1} D_{i,k}^* E_{j,l}; \tag{2.23}$$

visto que $\langle u_i | u_j \rangle = \delta_{i,j}$ e $\langle w_k | w_l \rangle = \delta_{k,l}$.

Exemplo: Consideremos agora $|g_a\rangle$ e $|g_b\rangle$ dois vetores que residem no espaço $H = H_1 \otimes H_2$, com $|g_a\rangle = \frac{1}{\sqrt{2}}(|u_1\rangle \otimes |w_1\rangle + |u_2\rangle \otimes |w_2\rangle)$ e $|g_b\rangle = \frac{1}{\sqrt{2}}(|u_1\rangle \otimes |w_1\rangle - |u_2\rangle \otimes |w_2\rangle)$. O produto escalar entre ambos é

$$\begin{aligned} \langle g_a | g_b \rangle &= \left(\frac{1}{2}\right) \langle u_1 | u_1 \rangle \langle w_1 | w_1 \rangle - \left(\frac{1}{2}\right) \langle u_1 | u_2 \rangle \langle w_1 | w_2 \rangle + \left(\frac{1}{2}\right) \langle u_2 | u_1 \rangle \langle w_2 | w_1 \rangle - \left(\frac{1}{2}\right) \langle u_2 | u_2 \rangle \langle w_2 | w_2 \rangle \\ &= \left(\frac{1}{2}\right)(1)(1) - \left(\frac{1}{2}\right)(0)(0) + \left(\frac{1}{2}\right)(0)(0) - \left(\frac{1}{2}\right)(1)(1) = 0, \end{aligned} \tag{2.24}$$

e, dessa forma, $|g_a\rangle$ e $|g_b\rangle$ são ortogonais.

A próxima seção apresentará os conceitos relacionados a operadores, e retornaremos às propriedades do produto tensorial na seção 2.3.

2.2 Operadores

Seja $|v\rangle$ um vetor que reside em um espaço vetorial de dimensão N . Um operador \hat{O} é uma transformação que atua em $|v\rangle$ e substitui-o por outro vetor pertencente a este espaço, $\hat{O}(|v\rangle) = |u\rangle$, $|u\rangle \in N$.

Os operadores podem ser classificados como lineares ou não-lineares. Um operador é dito linear quando satisfaz as propriedades

$$\begin{aligned}\hat{O}(m|a\rangle) &= m\hat{O}|a\rangle; \\ \hat{O}(|a\rangle + |b\rangle) &= \hat{O}|a\rangle + \hat{O}|b\rangle; \\ (\hat{O}_1 + \hat{O}_2)|a\rangle &= \hat{O}_1|a\rangle + \hat{O}_2|a\rangle;\end{aligned}\tag{2.25}$$

para um número complexo qualquer m e dois operadores independentes \hat{O}_1 e \hat{O}_2 .

Projetores:

O produto entre um vetor qualquer $|u\rangle$ na forma "ket" e seu dual "bra" também é um operador, que pertence a uma classe especial chamada de projetores representados por \hat{P} . A ação de \hat{P}_u sobre um vetor $|v\rangle$ gera outro proporcional a $|u\rangle$, pois $\hat{P}_u(|v\rangle) = |u\rangle\langle u|(|v\rangle) = \langle u|v\rangle|u\rangle$. O coeficiente $\langle u|v\rangle$ é chamado de projeção de $|v\rangle$ sobre $|u\rangle$.

A relação de completeza apresentada na Eq. (2.18) pode ser associada a um operador linear. Veja que

$$\sum_{i=1}^n |u_i\rangle\langle u_i|v\rangle = |v\rangle,\tag{2.26}$$

e, portanto, sua ação sobre qualquer vetor é equivalente à operação identidade I , mantendo o vetor inalterado após a transformação.

Comutadores e AntiComutadores:

A relação de comutação também pode ser associada ao conceito de operadores. Sejam \hat{O}_a , \hat{O}_b e \hat{O}_c três operadores quaisquer. Um comutador é definido como

$$[\hat{O}_a, \hat{O}_b] = \hat{O}_a\hat{O}_b - \hat{O}_b\hat{O}_a\tag{2.27}$$

e satisfaz as seguintes propriedades:

$$[\hat{O}_a, \hat{O}_b] = -[\hat{O}_b, \hat{O}_a];$$

$$[\hat{O}_a \hat{O}_b, \hat{O}_c] = \hat{O}_a [\hat{O}_b, \hat{O}_c] + [\hat{O}_a, \hat{O}_c] \hat{O}_b. \quad (2.28)$$

Já o anti-comutador é definido como

$$\{\hat{O}_a, \hat{O}_b\} = \hat{O}_a \hat{O}_b + \hat{O}_b \hat{O}_a. \quad (2.29)$$

Dizemos que \hat{O}_a e \hat{O}_b comutam se $\hat{O}_a \hat{O}_b = \hat{O}_b \hat{O}_a$ e anticomutam se $\hat{O}_a \hat{O}_b = -\hat{O}_b \hat{O}_a$, mas, como observaremos nos próximos capítulos, geralmente os operadores quânticos não obedecem à estas condições. Quando isso ocorre, no entanto, surgem propriedades interessantes como a reversibilidade nas operações lógicas (seção 2.7) e a possibilidade de realizar medidas sem afetarmos o estado quântico em questão (seção 2.4).

Autovalores e Autovetores:

Quando um operador \hat{O} atua sobre um vetor $|a\rangle$ e o vetor gerado é proporcional a $|a\rangle$, dizemos que este é um autovetor de \hat{O} com autovalor s_a , também conhecido como coeficiente de proporcionalidade. A operação é descrita por

$$\hat{O}|a\rangle = s_a|a\rangle. \quad (2.30)$$

Um operador que reside em um espaço vetorial de dimensão n possui no máximo n autovalores distintos. Quando os autovalores são iguais, dizemos que estes são degenerados. Existem algumas técnicas para calcular os autovalores, sendo a mais comum através de determinantes, que mostraremos na seção seguinte. Também veremos que um operador pode ser representado através de vetores pertencentes a um conjunto de estados de base, desde que se conheça a relação entre estes vetores e o operador em questão. Nas seções 2.3 e 2.4.2 retornaremos à discussão destas propriedades.

Operadores Hermitianos:

Na seção 2.4.2 mostraremos que as medidas de um parâmetro observável são associadas a operadores conhecidos como hermitianos. Por enquanto, vamos nos concentrar apenas em sua definição. Para qualquer operador \hat{O} , existe um operador correspondente \hat{O}^\dagger tal que

$$\langle b|\hat{O}a\rangle = \langle a\hat{O}^\dagger|b\rangle, \quad (2.31)$$

onde \hat{O}^\dagger é chamado de operador auto-adjunto ou hermitiano conjugado de \hat{O} . Um operador \hat{O} é hermitiano se $\hat{O} = \hat{O}^\dagger$.

Para dois operadores \hat{O}_1 e \hat{O}_2 quaisquer, temos que (Benenti et al., 2007)

$$\begin{aligned}(\hat{O}^\dagger)^\dagger &= \hat{O}; \\ (\hat{O}_1 + \hat{O}_2)^\dagger &= \hat{O}_2^\dagger + \hat{O}_1^\dagger = \hat{O}_1^\dagger + \hat{O}_2^\dagger; \\ (\hat{O}_1\hat{O}_2)^\dagger &= \hat{O}_2^\dagger\hat{O}_1^\dagger;\end{aligned}\tag{2.32}$$

e, para dois vetores quaisquer $|a\rangle$ e $|b\rangle$,

$$\begin{aligned}|a\rangle^\dagger &= \langle a|, \quad \langle a|^\dagger = |a\rangle; \\ (|a\rangle\langle b|)^\dagger &= |b\rangle\langle a|; \\ |\hat{O}a\rangle^\dagger &= \langle a\hat{O}^\dagger|.\end{aligned}\tag{2.33}$$

Um caso particular de operadores hermitianos ocorre quando estes são unitários. Um operador U é dito unitário se

$$UU^\dagger = U^\dagger U = I.\tag{2.34}$$

Na definição acima podemos inferir que $U^\dagger = U^{-1}$, onde U^{-1} é o operador inverso de U . Uma propriedade importante reside no fato de que a ação de U sobre dois vetores quaisquer não altera o produto escalar entre os mesmos, pois se $|a'\rangle = U|a\rangle$ e $|b'\rangle = U|b\rangle$,

$$\langle a'|b'\rangle = \langle aU^\dagger|Ub\rangle = \langle a|I|b\rangle = \langle a|b\rangle;\tag{2.35}$$

e, conseqüentemente, a norma entre os vetores também permanece inalterada. Isso independe do tipo de transformação unitária e dos parâmetros envolvidos. Exploraremos esta propriedade na seção 2.4.2 ao analisarmos a evolução de estados quânticos no tempo e a ação de operadores de medidas sobre estes estados, enquanto outras propriedades relevantes são discutidas ao longo do capítulo.

Produto Tensorial:

No final da seção 2.1 introduzimos a noção de produto tensorial, e apresentamos as propriedades relacionadas a vetores que residiam em espaços independentes H_1 (com dimensão N_1) e H_2 (com dimensão N_2). Agora, mostraremos como se comportam os operadores que atuam em um sistema composto no espaço $H = H_1 \otimes H_2$.

Se $\{\hat{O}_1, |u_i\rangle\} \in H_1$ e $\{\hat{O}_2, |w_k\rangle\} \in H_2$, onde \hat{O}_1 e \hat{O}_2 são operadores lineares

e $|u_i\rangle$ e $|w_k\rangle$ estados de base, a ação destes operadores em um estado composto como $|g_a\rangle = \sum_{k=1}^{N_2} \sum_{i=1}^{N_1} D_{i,k}(|u_i\rangle \otimes |w_k\rangle)$ é expressa por

$$(\hat{O}_1 \otimes \hat{O}_2)|g_a\rangle = \sum_{k=1}^{N_2} \sum_{i=1}^{N_1} D_{i,k}(\hat{O}_1|u_i\rangle \otimes \hat{O}_2|w_k\rangle), \quad (2.36)$$

onde cada operador atua separadamente no estado de base que pertence ao seu espaço vetorial. Na próxima seção, mostraremos como representar vetores e operadores através de matrizes e retornaremos novamente às propriedades do produto tensorial.

2.3 Representação Matricial

Até agora, apresentamos vetores e operadores como objetos com propriedades bem definidas e mostramos como se comportam suas componentes quando submetidas a operações algébricas. Nesta seção, mostraremos que é possível associar a estes conceitos uma representação matricial.

Consideremos novamente as definições de vetores que estabelecemos no início da seção 2.1. Cada vetor de dimensão n que chamamos de "ket" será representado por uma matriz coluna e seu dual "bra" será descrito por uma matriz linha, todos com dimensão n . Assim, para um vetor qualquer $|a\rangle = (a_1, \dots, a_n)$, podemos descrevê-lo como

$$|a\rangle = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix},$$

e seu vetor dual como

$$\langle a| = \left[a_1^*, a_2^*, a_3^*, \dots, a_n^* \right].$$

É fácil verificar que todas as propriedades descritas na seção 2.1 obedecem à definição acima. Para exemplificar, vamos calcular o produto escalar entre dois vetores quaisquer $|a\rangle = (a_1, \dots, a_n)$ e $|b\rangle = (b_1, \dots, b_n)$,

$$\langle a|b\rangle = \left[a_1^*, a_2^*, a_3^*, \dots, a_n^* \right] \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{bmatrix} = [a_1^*b_1 + a_2^*b_2 + a_3^*b_3 + \dots + a_n^*b_n] = \left[\sum_{i=1}^n a_i^*b_i \right],$$

(2.37)

que concorda com a definição 2.7.

Por sua vez, os operadores são representados por matrizes quadradas. Um operador \hat{O} que atua sobre um vetor cuja dimensão é n possui $n \times n = n^2$ elementos,

$$\hat{O} = \begin{bmatrix} \hat{O}_{1,1} & \hat{O}_{1,2} & \cdots & \hat{O}_{1,n} \\ \hat{O}_{2,1} & \hat{O}_{2,2} & \cdots & \hat{O}_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ \hat{O}_{n,1} & \hat{O}_{n,2} & \cdots & \hat{O}_{n,n} \end{bmatrix}.$$

Para representar um operador em uma matriz é necessário escolher um conjunto de vetores pertencente a alguma base específica, pois para cada base há uma representação única. Uma vez escolhido o conjunto, cada elemento na linha i e coluna j da matriz será determinado pela expressão $\hat{O}_{i,j} = \langle u_i | \hat{O} u_j \rangle$, onde $|u_1\rangle, |u_2\rangle, |u_3\rangle, \dots, |u_n\rangle$ são os vetores que formam a base.

Quando falamos sobre os auto-vetores de um operador, vimos que a estes vetores havia um autovalor associado. Se reescrevermos a Eq. (2.30) na representação matricial,

$$\hat{O}|a\rangle = s_a|a\rangle \Rightarrow \begin{bmatrix} \hat{O}_{1,1} & \hat{O}_{1,2} & \cdots & \hat{O}_{1,n} \\ \hat{O}_{2,1} & \hat{O}_{2,2} & \cdots & \hat{O}_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ \hat{O}_{n,1} & \hat{O}_{n,2} & \cdots & \hat{O}_{n,n} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = s_a \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix}, \quad (2.38)$$

obtemos o autovalor s_a resolvendo a expressão

$$\det \begin{bmatrix} \hat{O}_{1,1} - s_a & \hat{O}_{1,2} & \cdots & \hat{O}_{1,n} \\ \hat{O}_{2,1} & \hat{O}_{2,2} - s_a & \cdots & \hat{O}_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ \hat{O}_{n,1} & \hat{O}_{n,2} & \cdots & \hat{O}_{n,n} - s_a \end{bmatrix} = 0. \quad (2.39)$$

Como afirmamos na seção 2.2, para cada autoestado há um autovalor correspondente, e nada impede que autoestados distintos possuam o mesmo autovalor. Na seção 2.4.2, mostraremos que esta característica é conhecida como degenerescência e está intimamente ligada aos postulados da Mecânica Quântica.

Um operador também pode ser representado através de projetores. Se a

cada elemento $\hat{O}_{i,j}$ da matriz associamos o projetor $|u_j\rangle\langle u_i|$, \hat{O} será descrito por

$$\hat{O} = \sum_{j=1}^n \sum_{i=1}^n \hat{O}_{i,j} |u_j\rangle\langle u_i|, \quad (2.40)$$

cuja expressão é denominada decomposição espectral. Se a matriz que representa o operador for diagonal,

$$\begin{bmatrix} \hat{O}_{1,1} & 0 & \dots & 0 \\ 0 & \hat{O}_{2,2} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \hat{O}_{n,n} \end{bmatrix}, \quad (2.41)$$

sua decomposição espectral será função apenas de seus autovalores;

$$\hat{O} = \sum_{i=1}^n s_{u_i} |u_i\rangle\langle u_i|, \quad (2.42)$$

onde cada $|u_i\rangle$ é autoestado de \hat{O} com autovalor s_{u_i} .

Exemplo: sejam $\hat{O} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Então:

$$\det(\hat{O} - s_{u_i} I) = 0 \Rightarrow \begin{vmatrix} 1 - s_{u_i} & 0 \\ 0 & -1 - s_{u_i} \end{vmatrix} = 0, \quad (2.43)$$

que tem como soluções $s_{u_1} = +1$ e $s_{u_2} = -1$. Resolvendo a equação

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = s_{u_i} \begin{pmatrix} x \\ y \end{pmatrix}, \quad (2.44)$$

encontramos $|u_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ para $s_{u_1} = +1$ e $|u_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ para $s_{u_2} = -1$. Como \hat{O} é diagonal, sua decomposição espectral é expressa em termos de seus autovalores e autovetores, ou seja,

$$\hat{O} = (+1)|u_1\rangle\langle u_1| + (-1)|u_2\rangle\langle u_2|. \quad (2.45)$$

Operador Inverso:

Um operador inverso \hat{O}^{-1} é aquele que satisfaz à relação

$$\hat{O}\hat{O}^{-1} = \hat{O}^{-1}\hat{O} = I. \quad (2.46)$$

A condição necessária para que \hat{O}^{-1} exista e satisfaça a relação acima é $\det \hat{O} \neq 0$ para qualquer matriz que represente o operador \hat{O} . Veremos na seção 2.7 que os operadores inversos estão intrinsecamente ligados às portas lógicas de circuitos quânticos.

Produto Tensorial:

Já vimos como aplicar o produto tensorial a vetores (seção 2.1) e operadores (seção 2.2). Neste tópico, veremos como representá-lo em uma estrutura matricial.

Para dois operadores lineares quaisquer $\hat{O}_1 \in H_1$ e $\hat{O}_2 \in H_2$, o produto $\hat{O} = \hat{O}_1 \otimes \hat{O}_2$ assume a forma matricial de (Benenti et al., 2007)

$$\begin{bmatrix} \langle u_1 | \hat{O}_1 u_1 \rangle (\hat{O}_2) & \langle u_1 | \hat{O}_1 u_2 \rangle (\hat{O}_2) & \dots & \langle u_1 | \hat{O}_1 u_{N_1} \rangle (\hat{O}_2) \\ \langle u_2 | \hat{O}_1 u_1 \rangle (\hat{O}_2) & \langle u_2 | \hat{O}_1 u_2 \rangle (\hat{O}_2) & \dots & \langle u_2 | \hat{O}_1 u_{N_1} \rangle (\hat{O}_2) \\ \vdots & \vdots & \vdots & \vdots \\ \langle u_{N_1} | \hat{O}_1 u_1 \rangle (\hat{O}_2) & \langle u_{N_1} | \hat{O}_1 u_2 \rangle (\hat{O}_2) & \dots & \langle u_{N_1} | \hat{O}_1 u_{N_1} \rangle (\hat{O}_2) \end{bmatrix}, \quad (2.47)$$

cujos estados de base são resultantes do produto tensorial $|u_i\rangle \otimes |w_k\rangle$, onde $|u_i\rangle \in H_1$ e $|w_k\rangle \in H_2$. Assim, se H_1 possui dimensão N_1 e H_2 dimensão N_2 , a matriz que representa \hat{O} possuirá $N = N_1 \times N_2$ estados de base e N^2 elementos.

O produto tensorial entre vetores também possui uma forma matricial. Se $|v_1\rangle \in H_1$ e $|v_2\rangle \in H_2$ são dois vetores quaisquer, com $|v_1\rangle = \sum_{i=1}^{N_1} C_{u_i} |u_i\rangle$ e $|v_2\rangle = \sum_{k=1}^{N_2} D_{w_k} |w_k\rangle$, então o produto $|v\rangle = |v_1\rangle \otimes |v_2\rangle$ é representado por

$$|v\rangle = \begin{bmatrix} C_{u_1} \begin{pmatrix} D_{u_1} \\ D_{u_2} \\ \vdots \\ D_{u_{N_2}} \end{pmatrix} \\ C_{u_2} \begin{pmatrix} D_{u_1} \\ D_{u_2} \\ \vdots \\ D_{u_{N_2}} \end{pmatrix} \\ \vdots \\ C_{u_{N_1}} \begin{pmatrix} D_{u_1} \\ D_{u_2} \\ \vdots \\ D_{u_{N_2}} \end{pmatrix} \end{bmatrix},$$

que apresenta uma coluna e $N = N_1 \times N_2$ elementos. Quando estudarmos estados quânticos que residem em diferentes sistemas, faremos uso freqüente do produto tensorial. Veremos este assunto com detalhes nas seções 2.4 e 2.7.

$$\text{Exemplo: seja } \hat{O}_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \hat{O}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, |u_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ e}$$

$$|u_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

$$\text{Então } \hat{O} = \hat{O}_1 \otimes \hat{O}_2 =$$

$$= \begin{bmatrix} \langle u_1 | \hat{O}_1 u_1 \rangle \langle \hat{O}_2 & \langle u_1 | \hat{O}_1 u_2 \rangle \langle \hat{O}_2 \\ \langle u_2 | \hat{O}_1 u_1 \rangle \langle \hat{O}_2 & \langle u_2 | \hat{O}_1 u_2 \rangle \langle \hat{O}_2 \end{bmatrix} = \begin{bmatrix} (1) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & (0) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ (0) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & (-1) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \quad (2.48)$$

$$\text{e } |u\rangle = |u_1\rangle \otimes |u_2\rangle =$$

$$= \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}. \quad (2.49)$$

Operadores Hermitianos:

Na seção anterior, definimos o operador hermitiano através da relação

$$\langle a|\hat{O}b\rangle = \langle a\hat{O}^\dagger|b\rangle. \quad (2.50)$$

Se transcrevermos esta expressão para a álgebra matricial, veremos que é possível construir a matriz do operador auto-adjunto de forma bem simples. Observe que $\langle a\hat{O}^\dagger|b\rangle = (\langle b|\hat{O}^\dagger a\rangle)^*$. Logo, se o operador \hat{O} for representado na base $|u_1\rangle, |u_2\rangle, |u_3\rangle, \dots, |u_n\rangle$, os elementos da matriz hermitiana podem ser encontrados a partir dos constituintes da matriz do operador \hat{O} , como revela a expressão

$$\langle u_i|\hat{O}u_j\rangle = \langle u_i\hat{O}^\dagger|u_j\rangle \Rightarrow \langle u_i|\hat{O}u_j\rangle = (\langle u_j|\hat{O}^\dagger u_i\rangle)^* \Rightarrow \hat{O}_{i,j} = (\hat{O}_{j,i}^\dagger)^* \Rightarrow (\hat{O}_{i,j})^* = \hat{O}_{j,i}^\dagger. \quad (2.51)$$

Desse modo, cada termo na forma $\hat{O}_{j,i}^\dagger$ da matriz hermitiana corresponde ao conjugado do elemento $\hat{O}_{i,j}$ na matriz do operador \hat{O} . Sendo assim, podemos afirmar que

$$\hat{O}^\dagger = (\hat{O}^T)^*. \quad (2.52)$$

Dissemos na seção 2.2 que um operador é hermitiano quando $\hat{O} = \hat{O}^\dagger$. Neste caso, \hat{O} e \hat{O}^\dagger devem possuir os mesmo elementos na diagonal principal e estes são números reais, já que $\hat{O}_{i,i} = (\hat{O}_{i,i}^T)^* \Rightarrow \hat{O}_{i,i} = \hat{O}_{i,i}^*$. Mas $\hat{O}|u_i\rangle = s_{u_i}|u_i\rangle$. Logo, $\langle u_i|\hat{O}|u_i\rangle = s_{u_i}\langle u_i|u_i\rangle$, e, como o produto escalar $\langle u_i|u_i\rangle$ é sempre real, os autovalores s_{u_i} de um operador hermitiano também são reais.

Para os operadores unitários, uma outra propriedade envolvendo autovalores é satisfeita. Vimos na seção 2.2 que o produto escalar entre dois vetores não é afetado pela ação de U . Logo, se analisarmos esta propriedade para um autoestado deste operador, veremos que

$$\langle u'_i|u'_i\rangle = \langle u_i\hat{O}^\dagger|\hat{O}u_i\rangle = \langle u_i|(s_{u_i})^*(s_{u_i})|u_i\rangle = |s_{u_i}|^2\langle u_i|u_i\rangle. \quad (2.53)$$

Como $\langle u'_i|u'_i\rangle = \langle u_i|u_i\rangle$, $|s_{u_i}|^2 = 1$ e os autovalores possuem módulo unitário.

Há uma classe especial de operadores unitários que constitui uma ferramenta vital para a correção de *qubits* (os quais definiremos na seção seguinte) durante a transmissão de informação quântica: as matrizes de Pauli. Estas matrizes representam transformações unitárias que atuam linearmente sobre os *qubits*, corrigindo-os localmente. Junto com a matriz identidade I , formam uma base completa para a representação de qualquer matriz de dimensão 2×2 , e são representadas por $\sigma_x, \sigma_y, \sigma_z$. Por ora, apresentaremos

apenas algumas propriedades destes operadores. As três matrizes de Pauli são

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Se pensarmos em uma analogia com a condição para que um conjunto de vetores seja linearmente independente, veremos que $a(\sigma_x) + b(\sigma_y) + c(\sigma_z) + d(I) = 0 \Rightarrow$

$$\begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} + \begin{bmatrix} 0 & -ib \\ ib & 0 \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & -c \end{bmatrix} + \begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} c+d & a-ib \\ a+ib & -c+d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad (2.54)$$

só é satisfeita se $a = b = c = d = 0$. Portanto, as três matrizes de Pauli são linearmente independentes e ao lado da matriz identidade podem ser utilizadas para representar qualquer matriz 2×2 , da mesma maneira que um conjunto de vetores L.I. pode ser utilizado para representar qualquer vetor (contanto que todos residam no mesmo espaço de Hilbert). Outras relações satisfeitas por essas matrizes:

$$\begin{aligned} \sigma_x^2 &= \sigma_y^2 = \sigma_z^2 = I; \\ \sigma_x \sigma_y &= -\sigma_y \sigma_x = i\sigma_z; \\ \sigma_y \sigma_z &= -\sigma_z \sigma_y = i\sigma_x; \\ \sigma_z \sigma_x &= -\sigma_x \sigma_z = i\sigma_y; \end{aligned} \quad (2.55)$$

que podem ser reduzidas a

$$\sigma_k^2 = I, \quad \sigma_k \sigma_l = \epsilon_{klm} i \sigma_m \quad \text{para } k \neq l \neq m; \quad (2.56)$$

sendo ϵ_{klm} o símbolo de Levi-Civita onde $\epsilon_{klm} = \epsilon_{mkl} = \epsilon_{lmk} = 1$, $\epsilon_{kml} = \epsilon_{lkm} = \epsilon_{mlk} = -1$ e $\epsilon_{klm} = 0$ quando dois ou mais índices forem iguais.

Repare que as matrizes de Pauli são hermitianas e possuem $+1$ e -1 como autovalores, comprovando sua unitariedade, e, além disso, possuem a propriedade de serem anticomutativas, conceito que retomaremos na próxima seção. Voltaremos às propriedades das matrizes de Pauli na seção 2.7.

Comutadores e AntiComutadores:

Outra característica que reforça a associação entre operadores na mecânica quântica e sua representação matricial deve-se ao fato de que geralmente duas matrizes aleatórias não obedecem à comutatividade e à anti-comutatividade. Para verificar esta

afirmação, basta efetuar os produtos $M_a M_b$ e $M_b M_a$ para duas matrizes M_a e M_b quaisquer e conferir o resultado. Quando dois operadores comutam, é possível encontrar uma base cujos estados sejam autoestados de ambos os operadores (se os autovalores não forem degenerados), e, neste caso, podemos representar estes operadores como matrizes em função da mesma base de estados.

Na seção seguinte falaremos sobre o Princípio da Incerteza, e as relações de comutatividade serão essenciais para entendermos os conceitos que serão introduzidos neste tópico.

2.4 Os Postulados da Mecânica Quântica

2.4.1 Postulado I (Benenti et al., 2007)

O estado S de um sistema físico é completamente descrito por um vetor unitário $|\Psi\rangle$ que reside no espaço de Hilbert H_s associado ao sistema. Este vetor é conhecido como vetor de estado ou função de onda, cuja evolução temporal é governada pela equação de Schrödinger,

$$i\hbar \frac{d}{dt} |\Psi(t)\rangle = H |\Psi(t)\rangle, \quad (2.57)$$

onde H é um operador auto-adjunto conhecido como Hamiltoniano do sistema e $\hbar = h/2\pi$, sendo h a constante conhecida como constante de Planck cujo valor determinado experimentalmente é de $h \approx 6,626 \times 10^{-34} \text{ J.s}$.

Como a Eq. (2.57) é uma equação diferencial linear de primeira ordem, qualquer combinação linear de soluções particulares também é uma solução. Isso indica que H pode ser associado a um operador linear que atua sobre um vetor de estado $|\Psi\rangle$, e, de fato, todas as representações e propriedades vistas para vetores e operadores nas seções 2.1, 2.2 e 2.3 são compatíveis com a Eq. de Schrödinger e suas soluções. O uso de matrizes para descrever estes objetos foi introduzido pela primeira vez por Heisenberg e sua proposta ficou conhecida como mecânica matricial. No início, esta abordagem para a mecânica quântica gerava inconsistências com a visão na época decorrente da formulação de Schrödinger; mas, alguns anos depois, foi demonstrado que ambas explicavam os mesmos fenômenos e eram equivalentes.

A natureza da função de onda é definida pelo espaço de Hilbert, que pode ser discreto ou contínuo. Para o primeiro caso, $|\Psi\rangle$ possui dimensão finita e o número de coordenadas que o define é limitado, e, dessa forma, podemos associar à função de onda as mesmas propriedades vistas para vetores na seção 2.1. Para o segundo, entretanto, $|\Psi\rangle$ é visto como uma função contínua de parâmetros específicos (como as coordenadas de posição x, y, z) e o espaço de Hilbert assume dimensão infinita. O foco do presente

trabalho está no primeiro caso, e, portanto, em sistemas com dimensão finita e coordenadas bem definidas. Deste ponto em diante, assumimos que nosso espaço de Hilbert H_s é sempre limitado. Vejamos agora como determinar a função de onda com estas restrições.

Todo sistema quântico é governado por uma dinâmica intrínseca que dita seu comportamento ao longo do tempo através da relação (Benenti et al., 2007)

$$|\Psi(t)\rangle = U(t, t_0)|\Psi(t_0)\rangle, \quad (2.58)$$

onde $|\Psi(t_0)\rangle$ é o estado do sistema em algum instante t_0 e $U(t, t_0)$ é chamado de operador de evolução. O cenário mais simples ocorre quando o sistema é estacionário: $|\Psi(t)\rangle \propto |\Psi(t_0)\rangle$ e $U(t, t_0) \propto I$. Para outros tipos de dinâmica, é preciso conhecer $U(t, t_0)$ a fim de prever a forma de $|\Psi(t)\rangle$. Quando o Hamiltoniano for independente do tempo, a solução da Eq. (2.57) é

$$|\Psi(t)\rangle = e^{[-\frac{i}{\hbar}(t-t_0)H]}|\Psi(t_0)\rangle = \left(\sum_{n=0}^{\infty} \frac{1}{n!} \left[-\frac{i}{\hbar}(t-t_0) \right]^n H^n \right) \Psi(t_0), \quad (2.59)$$

sendo $U(t, t_0) = e^{[-\frac{i}{\hbar}(t-t_0)H]}$. Para determinar $|\Psi(t)\rangle$ quando H for dependente do tempo é necessário recorrer a outras técnicas, e uma delas consiste em obter aproximações da matriz H através de métodos semelhantes à expansão de uma função em série de Taylor. O próximo postulado relaciona os coeficientes do estado quântico que representa o sistema às probabilidades de obter resultados para uma determinada medida.

2.4.2 Postulado II (Benenti et al., 2007)

Associa-se a cada observável O um operador auto-adjunto \hat{O} que reside em um espaço de Hilbert H_s . Se uma medida de O for realizada sobre um sistema, os únicos resultados possíveis são os autovalores do operador \hat{O} ,

$$\hat{O}|u_i\rangle = s_{u_i}|u_i\rangle, \quad (2.60)$$

onde $|u_1\rangle, |u_2\rangle, |u_3\rangle, \dots$ é uma base ortonormal de autoestados de \hat{O} . Se o vetor de estado do sistema for expandido sobre esta base,

$$|\Psi(t)\rangle = \sum_i C_{u_i}(t)|u_i\rangle, \quad (2.61)$$

a probabilidade de a medida do observável O em um instante t ser s_{u_i} é dada por

$$prob(s = s_{u_i}|t) = |\langle u_i|\Psi(t)\rangle|^2 = |C_{u_i}(t)|^2. \quad (2.62)$$

O coeficiente $C_{u_i}(t)$ é chamado de amplitude de probabilidade, e a unitarie-

dade de $|\Psi\rangle$ imposta pelo Postulado I agora pode ser compreendida. Repare que a probabilidade para cada resultado possível das medidas de \hat{O} está relacionada ao coeficiente $C_{u_i}(t)$, e, se considerarmos todas as possibilidades de medida, a soma de todas as probabilidades deve ser necessariamente igual a um. Como $\text{prob}(s = s_{u_i}|t) = |\langle u_i|\Psi(t)\rangle|^2 = |C_{u_i}(t)|^2$, então a condição

$$\|\Psi(t)\| = \sum_i |C_{u_i}(t)|^2 = 1 \quad (2.63)$$

é necessária. Logo, se $|\Psi(t)\rangle$ representa o estado de um sistema, ele é obrigatoriamente unitário.

Os observáveis quânticos representados por operadores são análogos às variáveis dinâmicas clássicas, como posição, energia, momentos linear e angular, dentre outros. Há, porém, observáveis quânticos que não possuem análogos clássicos, como é o caso do operador de *spin* S , sendo este um dos fatores que contribuem para que a mecânica quântica forneça uma descrição mais completa da natureza do que a mecânica clássica. Os operadores não devem ser confundidos com parâmetros intrínsecos do sistema observado, como a carga elétrica e a massa de seus constituintes, que, em situações não-relativísticas, são independentes do referencial de observação.

Vimos na seção anterior que se o Hamiltoniano for independente do tempo a solução para $|\Psi(t)\rangle$ na Eq. (2.57) é a Eq. (2.59) em que $|\Psi(t)\rangle = e^{[-\frac{i}{\hbar}(t-t_0)H]}|\Psi(t_0)\rangle$. Como o Postulado II afirma que os possíveis resultados da medida de um operador são seus autovalores, podemos expressar $|\Psi(t)\rangle$ em termos dos autoestados de H e simplificar a expressão (2.59). Os autoestados e os autovalores de H são representados respectivamente por $|n\rangle$ e E_n , onde n é um parâmetro que define a energia E_n do sistema. Dizemos então que

$$H|n\rangle = E_n|n\rangle, \quad n \in N, \quad (2.64)$$

e, por, conseguinte,

$$\sum_{n=0}^{\infty} \left(\frac{1}{n!} \left[-\frac{i}{\hbar}(t-t_0) \right]^n H^n |n\rangle \right) = \sum_{n=0}^{\infty} \left(\frac{1}{n!} \left[-\frac{i}{\hbar}(t-t_0) \right]^n (E_n)^n |n\rangle \right) = e^{[-\frac{i(t-t_0)}{\hbar}E_n]} |n\rangle. \quad (2.65)$$

Após expandir $|\Psi(t)\rangle = \sum_n C_n(t)|n\rangle$ e submeter este estado à ação do operador H , observamos que

$$|\Psi(t)\rangle = e^{[-\frac{i}{\hbar}(t-t_0)H]}|\Psi(t_0)\rangle = \sum_n C_n(t_0) e^{[-\frac{i(t-t_0)}{\hbar}E_n]} |n\rangle. \quad (2.66)$$

Vejamos um exemplo: sejam $|\Psi(0)\rangle = \frac{1}{3}|a\rangle + \frac{2}{3}|b\rangle + \frac{2}{3}|c\rangle$, $H|a\rangle = |a\rangle$, $H|b\rangle =$

$2|b\rangle$ e $H|c\rangle = 3|c\rangle$. Assim, se o operador \hat{O} atuar sobre o sistema, as probabilidades de obter os resultados $E_1 = 1$, $E_2 = 2$ ou $E_3 = 3$ associados aos estados $|a\rangle$, $|b\rangle$ e $|c\rangle$, respectivamente, são:

$$\begin{aligned} \text{prob}(s = E_1 = 1|t_0 = 0) &= |\langle a|\Psi(0)\rangle|^2 = \left|\frac{1}{3}\right|^2, \\ \text{prob}(s = E_2 = 2|t_0 = 0) &= |\langle b|\Psi(0)\rangle|^2 = \left|\frac{2}{3}\right|^2, \\ \text{prob}(s = E_3 = 3|t_0 = 0) &= |\langle c|\Psi(0)\rangle|^2 = \left|\frac{2}{3}\right|^2, \end{aligned} \quad (2.67)$$

e, após um determinado tempo t ,

$$|\Psi(t)\rangle = \sum_n C_n(0) e^{-\frac{i(t-0)E_n}{\hbar}} |n\rangle = \frac{1}{3} e^{-\frac{it}{\hbar}} |a\rangle + \frac{2}{3} e^{-\frac{2it}{\hbar}} |b\rangle + \frac{2}{3} e^{-\frac{3it}{\hbar}} |c\rangle. \quad (2.68)$$

Para o caso particular em que $|\Psi(t_0)\rangle = |n\rangle$, ou seja, quando o estado inicial coincide com um dos autoestados de H , $|\Psi(t)\rangle$ é simplesmente

$$|\Psi(t)\rangle = e^{\left[-\frac{i(t-t_0)E_n}{\hbar}\right]} |n\rangle, \quad (2.69)$$

e, como

$$|e^{i\theta}| \equiv 1 \quad (2.70)$$

para qualquer parâmetro θ , a norma de $|\Psi(t)\rangle$ é

$$\| |\Psi(t)\rangle \| = \left| e^{\left[-\frac{i(t-t_0)E_n}{\hbar}\right]} \right| \times \| |n\rangle \| = \| |n\rangle \|. \quad (2.71)$$

Neste caso, o estado do sistema ao longo do tempo é estacionário e a transformação $U(t) \propto I$ é unitária. Isso equivale a afirmar que a norma de $|\Psi(t)\rangle$ não muda com o tempo (2.35) e que a probabilidade de o sistema ser encontrado em algum dos estados de base permanece inalterada. Para o caso do operador \hat{H} , é o mesmo que afirmar que a chance de que o sistema esteja em algum estado de energia E_n não se altera com o passar do tempo, e, comparando com o conceito análogo clássico, dizemos que o sistema é conservativo. Repare ainda que sistemas que diferem pelo fator $e^{i\theta}$ são equivalentes, já que as previsões relativas às probabilidades de colapso para um determinado estado são idênticas para ambos. Assim, dizemos que dois sistemas $|\Psi(t)\rangle$ e $|\Psi'(t)\rangle$ são semelhantes se a única diferença entre eles for um fator multiplicativo igual a $e^{i\theta}$, onde θ é uma fase real qualquer.

2.4.3 Postulado III (Benenti et al., 2007)

Se o sistema é descrito pelo vetor de estado $|\Psi\rangle$ e sobre ele é realizada uma medida do observável \hat{O} com resultado s_{u_i} , imediatamente após a medida o sistema assume o estado

$$\frac{\hat{P}_{u_i}|\Psi(t)\rangle}{\sqrt{\langle\Psi(t)|\hat{P}_{u_i}|\Psi(t)\rangle}}, \quad (2.72)$$

onde \hat{P}_{u_i} é o operador de projeção sobre o subespaço correspondente a s_{u_i} .

Vejam os que diz o postulado. Primeiramente, vamos supor que s_{u_i} é não degenerado. Assim, a expressão $\hat{O}|u_i\rangle = s_{u_i}|u_i\rangle$ é válida para algum autoestado $|u_i\rangle$ de \hat{O} . Se a medida \hat{O} sobre o sistema forneceu s_{u_i} como resultado, o novo estado do sistema é $|u_i\rangle$, que, por definição, é normalizado. Dizemos assim que o sistema colapsou para um dos autoestados do operador \hat{O} .

Para verificar esta afirmação, observe a Eq. (2.72). Como s_{u_i} é único, só o estado $|u_i\rangle$ está associado a este autovalor no projetor \hat{P}_{u_i} . Assim, $\hat{P}_{u_i} = |u_i\rangle\langle u_i|$, e, ao substituir este termo em (2.72), notamos que

$$\frac{\hat{P}_{u_i}|\Psi(t)\rangle}{\sqrt{\langle\Psi(t)|\hat{P}_{u_i}|\Psi(t)\rangle}} = \frac{|u_i\rangle\langle u_i|\Psi(t)\rangle}{\sqrt{\langle\Psi(t)|u_i\rangle\langle u_i|\Psi(t)\rangle}} = \frac{|u_i\rangle\langle u_i|\Psi(t)\rangle}{\sqrt{|\langle u_i|\Psi(t)\rangle|^2}} = \frac{\langle u_i|\Psi(t)\rangle}{|\langle u_i|\Psi(t)\rangle|}|u_i\rangle = e^{i\theta_i}|u_i\rangle, \quad (2.73)$$

confirmando a afirmação de que o sistema se encontra no estado unitário $|u_i\rangle$ a menos de uma fase global θ_i .

Mas e se o autovalor s_{u_i} for degenerado? Neste caso, há um subespaço de \hat{O} associado a s_{u_i} e o projetor \hat{P}_{u_i} é dado por $\hat{P}_{u_i} = \sum_{g=1}^k |u_{g_i}\rangle\langle u_{g_i}|$, onde k é o número de degenerescências associado a este autovalor. A Eq. (2.72) pode então ser expressa por

$$\frac{\hat{P}_{u_i}|\Psi(t)\rangle}{\sqrt{\langle\Psi(t)|\hat{P}_{u_i}|\Psi(t)\rangle}} = \frac{\left(\sum_{g=1}^k |u_{g_i}\rangle\langle u_{g_i}|\right)|\Psi(t)\rangle}{\sqrt{\left(\sum_{g=1}^k \langle\Psi(t)|u_{g_i}\rangle\langle u_{g_i}|\Psi(t)\rangle\right)}} = \frac{\sum_{g=1}^k |u_{g_i}\rangle\langle u_{g_i}|\Psi(t)\rangle}{\sqrt{\sum_{g=1}^k |\langle u_{g_i}|\Psi(t)\rangle|^2}} \quad (2.74)$$

onde podemos notar que o novo sistema será um estado unitário formado pela combinação dos estados $|u_{g_i}\rangle$, como mostra o próximo exemplo.

Exemplo: sejam $|\Psi(0)\rangle = \frac{1}{3}|a\rangle + \frac{2}{3}|b\rangle + \frac{2}{3}|c\rangle$, $H|a\rangle = |a\rangle$, $H|b\rangle = |b\rangle$ e $H|c\rangle = 5|c\rangle$. Logo, só existem dois autovalores possíveis, onde um deles é igual a +5 e o outro é igual a +1 com degenerescência dupla. De acordo com a Eq. (2.74), se o resultado após a medida do operador \hat{O} sobre o sistema for +1, o novo sistema será formado pela

combinação dos estados $|a\rangle$ e $|b\rangle$ segundo a relação

$$\begin{aligned} \frac{\hat{P}_{u_i}|\Psi(t)\rangle}{\sqrt{\langle\Psi(t)|\hat{P}_{u_i}|\Psi(t)\rangle}} &= \frac{\sum_{g=1}^k |u_{g_i}\rangle\langle u_{g_i}|\Psi(t)\rangle}{\sqrt{\sum_{g=1}^k |\langle u_{g_i}|\Psi(t)\rangle|^2}} = \frac{|a\rangle\langle a|\Psi(t)\rangle + |b\rangle\langle b|\Psi(t)\rangle}{\sqrt{|\langle a|\Psi(t)\rangle|^2 + |\langle b|\Psi(t)\rangle|^2}} \\ &= \frac{\frac{1}{3}|a\rangle + \frac{2}{3}|b\rangle}{\sqrt{|\frac{1}{3}|^2 + |\frac{2}{3}|^2}} = \frac{3}{\sqrt{5}} \left(\frac{1}{3}|a\rangle + \frac{2}{3}|b\rangle \right). \end{aligned} \quad (2.75)$$

Note na Eq. (2.74) que a probabilidade de o sistema colapsar para o estado $|u_{g_i}\rangle$ pode ser expressa através do projetor \hat{P}_{u_i} ,

$$p_{u_i} = \sum_{g=1}^k |\langle u_{g_i}|\Psi(t)\rangle|^2 = \sum_{g=1}^k \langle\Psi(t)|u_{g_i}\rangle\langle u_{g_i}|\Psi(t)\rangle = \langle\Psi(t)|\hat{P}_{u_i}|\Psi(t)\rangle, \quad (2.76)$$

e que (2.42) e (2.76) podem ser usadas para calcular o valor médio sobre todos os resultados possíveis da medida do operador \hat{O} sobre o estado $|\Psi\rangle$,

$$\begin{aligned} \langle\hat{O}\rangle &= \sum_{i=1}^N s_{u_i} p_{u_i} = \sum_{i=1}^N s_{u_i} \langle\Psi(t)|\hat{P}_{u_i}|\Psi(t)\rangle = \sum_{i=1}^N s_{u_i} \langle\Psi(t)| \left(\sum_{g=1}^k |u_{g_i}\rangle\langle u_{g_i}| \right) |\Psi(t)\rangle \\ &= \sum_{i=1}^N \langle\Psi(t)| \left(\sum_{g=1}^k s_{u_i} |u_{g_i}\rangle\langle u_{g_i}| \right) |\Psi(t)\rangle = \langle\Psi(t)| \left(\sum_{i=1}^N \sum_{g=1}^k s_{u_i} |u_{g_i}\rangle\langle u_{g_i}| \right) |\Psi(t)\rangle \\ &= \langle\Psi(t)|\hat{O}|\Psi(t)\rangle. \end{aligned} \quad (2.77)$$

Sabemos que a toda medida existe um erro associado, e os sistemas quânticos não são uma exceção à regra. Felizmente, o erro relativo às medidas de um operador quântico são facilmente calculados através da expressão

$$\Delta\hat{O} = \sqrt{\langle\hat{O}^2\rangle - \langle\hat{O}\rangle^2}, \quad (2.78)$$

onde \hat{O} é dado pela Eq. (2.77). Se quisermos medir dois parâmetros simultaneamente e saber o quão confiável é o resultado final, a expressão

$$\Delta\hat{O}_a\Delta\hat{O}_b = \frac{|\langle\Psi|[\hat{O}_a, \hat{O}_b]|\Psi\rangle|}{2} \quad (2.79)$$

fornece o limite mínimo do produto dos desvios padrão de dois operadores quaisquer \hat{O}_a e \hat{O}_b e é conhecida como Princípio da Incerteza. Se \hat{O}_a e \hat{O}_b comutam, é possível obter $\Delta\hat{O}_a\Delta\hat{O}_b = 0$ e as duas medidas não perturbam o estado do sistema medido. Se, por outro lado, $[\hat{O}_a, \hat{O}_b] \neq 0$, então $\Delta\hat{O}_a \neq 0$, $\Delta\hat{O}_b \neq 0$ e as duas medidas não podem ser obtidas simultaneamente com erro zero. Neste caso, quanto maior a informação sobre uma das medidas maior é a incerteza associada à outra. Como exemplo, podemos citar a relação entre o momento linear em um determinado eixo de direção e a posição de uma partícula sobre este eixo. Como o resultado é válido para qualquer escolha de coordenadas, suponha

que o eixo em questão seja z . Assim, o Princípio da Incerteza nos diz que

$$\Delta\hat{z}\Delta\hat{p}_z \geq \frac{\hbar}{2}, \quad (2.80)$$

e, portanto, o valor mínimo associado ao produto das incertezas do momento p_z e da posição z é $\hbar/2$. Desse modo, não é possível obter acesso ao resultado de ambas sem que exista uma determinada margem de erro associada a cada uma.

2.5 Qubits e Sistemas de Dois Níveis

A palavra *qubit* é oriunda do termo *quantum-bit* e é empregada para distinguir *bits* clássicos de quânticos. Em sistemas computacionais, um *bit* representa a menor unidade de informação que pode ser implementada e é representada por dígitos binários como 0 e 1. Por sua vez, um *qubit* representa qualquer sistema físico de dois níveis, que são encontrados sob diversas formas. Como exemplo, podemos citar fótons polarizados em eixos perpendiculares, o conjunto que engloba o estado fundamental e o primeiro estado excitado do átomo de hidrogênio, as duas orientações do spin de um elétron em uma determinada direção (*up* e *down*), dentre outros. Matematicamente, representamos um *qubit* como um vetor de duas dimensões em um espaço de Hilbert H onde qualquer escolha de base é válida, desde que os vetores que a constituam sejam ortonormais. Geralmente, a representação matricial padrão para os vetores que definem o espaço vetorial de um *qubit* é

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

e a forma geral que associamos a qualquer *qubit* é

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.81)$$

onde $|\alpha|^2 + |\beta|^2 = 1$. Essa condição é semelhante à relação $\cos^2 x + \sin^2 x \equiv 1$, onde x é um parâmetro real qualquer. Assim, α e β podem ser igualados a estas funções trigonométricas a menos de uma diferença de fase multiplicando-os e que desapareça ao tomarmos o quadrado de cada módulo. Vimos que diferenças de fase deste tipo são expressas por $e^{i\phi}$, onde ϕ é um parâmetro real qualquer. Dito isso, uma outra forma de representar um *qubit* é

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle. \quad (2.82)$$

Se multiplicarmos $|\Psi\rangle$ pelo fator $e^{-\frac{i\phi}{2}}$, sabemos que o novo estado representa o mesmo sistema (seção 2.4.1). Então

$$|\Psi\rangle = \cos \frac{\theta}{2} e^{-\frac{i\phi}{2}} |0\rangle + \sin \frac{\theta}{2} e^{\frac{i\phi}{2}} |1\rangle \quad (2.83)$$

é a forma mais utilizada para representar um *qubit* em função de θ e ϕ , dada a simetria entre seus coeficientes. Na figura 2.1 podemos visualizar a representação geométrica das Eqs. (2.82) e (2.83). O valor dos parâmetros reais θ e ϕ determina a posição de $|\Psi\rangle$ na superfície conhecida como esfera de *Bloch*. O vetor geométrico que indica a posição do vetor de estado $|\Psi\rangle$ é denominado de r , que pode ser expresso tanto em coordenadas esféricas como cartesianas. Outro conceito essencial para a compreensão dos cálculos neste

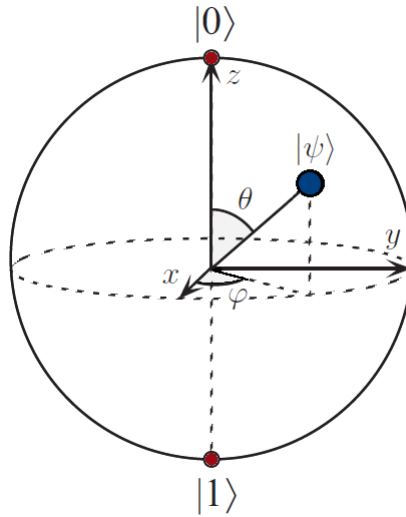


Figura 2.1: Representação de $|\Psi\rangle$ na Esfera de Bloch.
Fonte: Figura adaptada de Nielsen and Chuang, 2004.

trabalho está relacionado à fidelidade entre dois estados quânticos, que pode ser classificada como uma medida da “similaridade” entre estes estados. Como exemplo, sejam dois estados puros, $|\Psi^{inicial}\rangle$ e $|\Psi^{final}\rangle$, sendo $|\Psi^{inicial}\rangle$ um estado qualquer e $|\Psi^{final}\rangle$ a forma final do estado anterior após uma determinada transformação. A fidelidade será expressa por

$$F = \langle \Psi^{inicial} | (|\Psi^{final}\rangle \langle \Psi^{final}|) | \Psi^{inicial} \rangle = |\langle \Psi^{final} | \Psi^{inicial} \rangle|^2 = |\langle \Psi^{inicial} | \Psi^{final} \rangle|^2. \quad (2.84)$$

Observando esta expressão, é fácil notar que se $|\Psi^{inicial}\rangle$ e $|\Psi^{final}\rangle$ forem iguais, a fidelidade resultante é igual a um; ou seja, o estado final é igual ao inicial. Se, por outro lado, $|\Psi^{inicial}\rangle$ e $|\Psi^{out}\rangle$ forem ortogonais, a fidelidade resultante é nula. De uma forma geral, a fidelidade fica situada entre 0 e 1. Isto é fácil de perceber se definirmos um

dos estados como $|\Psi'_{inicial}\rangle = |0\rangle$ e o outro como

$$|\Psi'_{final}\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle \quad (2.85)$$

e recorreremos às representações matriciais de ambos. Com isso, a fidelidade assume a forma de

$$F = |\langle\Psi'_{inicial}|\Psi'_{final}\rangle|^2 = \left| \begin{bmatrix} 1, & 0 \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}e^{i\phi} \end{bmatrix} \right|^2 = \left| \begin{bmatrix} \cos\frac{\theta}{2} \end{bmatrix} \right|^2 = \cos^2\frac{\theta}{2}. \quad (2.86)$$

Vimos que a representação completa de um *qubit* exige apenas o conhecimento de dois parâmetros; α e β ou θ e ϕ . Para descrever sistemas que possuem mais de um *qubit*, precisamos de uma expressão geral que leve em conta todos os elementos presentes neste sistema. Neste caso, um sistema com n -*qubits* é representado por um produto tensorial através da expressão

$$|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes |x_4\rangle \otimes \dots \otimes |x_n\rangle = |x_1\rangle|x_2\rangle|x_3\rangle|x_4\rangle, \dots, |x_n\rangle = |x_1x_2x_3x_4\dots x_n\rangle. \quad (2.87)$$

A forma condensada mostrada no último termo da Eq. (2.87) é a mais comum de ser encontrada em textos da área, e, por isso, será adotada como padrão neste trabalho. Quando julgarmos necessário, recorreremos à expressão completa para este produto.

A Eq. (2.87) pode ser utilizada também para representar qualquer número inteiro. Para isto, basta escrever o número em questão em sua forma binária e efetuar o produto tensorial de todos os bits. Como exemplo, vamos representar o número 5 com três dígitos binários:

$$|5\rangle_{10} = |101\rangle_2 = |1\rangle \otimes |0\rangle \otimes |1\rangle. \quad (2.88)$$

Efetuando o produto tensorial entre as matrizes $|1\rangle$, $|0\rangle$ e $|1\rangle$, ficamos com:

$$|5\rangle_{10} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Repare que apenas o sexto elemento da matriz $|101\rangle$ não é nulo. Para um inteiro qualquer n , sua representação sob a forma matricial é

$$|n\rangle_{10} = \begin{pmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \end{pmatrix},$$

onde a posição do dígito 1 após n dígitos nulos equivale à representação de n em sua forma decimal. Em um espaço de dimensão n , podemos representar 2^n números inteiros entre 0 e $2^n - 1$.

Finalmente, podemos utilizar a Eq. (2.87) para distinguir *qubits* emaranhados de estados separáveis. Um estado puro é dito emaranhado se não puder ser escrito a menos de uma constante multiplicativa sob a forma reduzida

$$|\Psi\rangle = |x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes |x_4\rangle \otimes \dots \otimes |x_n\rangle, \quad (2.89)$$

onde cada estado $|x_i\rangle$ reside em um único espaço de Hilbert. Assim, um estado da forma $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |0_B\rangle) = \frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle) \otimes |0_B\rangle$ é separável, mas um estado $|\Psi'\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle \otimes |0_B\rangle + |1_A\rangle \otimes |1_B\rangle)$ está emaranhado.

2.6 Operador e Matriz Densidade

Até o momento analisamos estados quânticos em que todos os coeficientes associados a estados de uma determinada base são conhecidos, segundo a relação $|\Psi(t)\rangle = \sum_i C_{u_i}(t)|u_i\rangle$. Nesta seção abordaremos sistemas sobre os quais não dispomos de informações suficientes para determinar seu vetor de estado. Um exemplo é o estado oriundo de um forno que produz l estados aleatórios quaisquer $|\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle, \dots, |\Psi_l\rangle$ não necessariamente ortonormais. Em cenários como este, que chamamos de mistura estatística, só podemos supor que há uma probabilidade de que o sistema se encontre em algum dos possíveis estados $|\Psi_k\rangle$. Assim, precisamos descrever o sistema como uma mistura entre estes diferentes estados $|\Psi_k\rangle$ dispondo apenas do conhecimento da probabilidade p_k . Para

tanto, vamos introduzir o operador densidade

$$\rho = p_1|\Psi_1\rangle\langle\Psi_1| + p_2|\Psi_2\rangle\langle\Psi_2| + \dots + p_l|\Psi_l\rangle\langle\Psi_l| = \sum_{k=1}^l p_k|\Psi_k\rangle\langle\Psi_k|, \quad (2.90)$$

que representa a chance p_k de o sistema ser encontrado em um algum dos estados $|\Psi_k\rangle$. Se o estado do sistema for $|\Psi_k\rangle$ e esta informação estiver disponível, então o operador densidade é simplesmente $\rho = |\Psi_k\rangle\langle\Psi_k|$ e dizemos que o sistema está em um estado puro.

Embora aparentemente a expressão que defina ρ seja mais complicada do que a de um estado $|\Psi\rangle$ expresso em termos de suas componentes, as propriedades discutidas nos Postulados da seção 2.4 continuam sendo válidas nesta configuração. Se aplicarmos um operador sobre o sistema e mensurarmos a probabilidade de obter o resultado s_{u_i} associado a algum estado de base, a probabilidade total e o valor médio das medidas relacionadas ao operador podem ser calculados e expressos em função de ρ . Se o estado do sistema for $|\Psi_k\rangle$, sabemos da Eq. (2.76) que

$$p_{u_i} = \langle\Psi_k|\hat{P}_{u_i}|\Psi_k\rangle \quad (2.91)$$

é a probabilidade de obtermos o resultado s_{u_i} e o sistema colapsar para o estado $|u_i\rangle$. Portanto, uma vez que a chance de que o sistema esteja em $|\Psi_k\rangle$ é p_k , a probabilidade total de o resultado da medida ser s_{u_i} levando em conta todos os l estados $|\Psi_k\rangle$ é

$$p(i) = \sum_{k=1}^l p_k \langle\Psi_k|\hat{P}_{u_i}|\Psi_k\rangle. \quad (2.92)$$

Ao efetuar o traço sobre $\rho\hat{P}_{u_i}$ verificamos que

$$\begin{aligned} \text{Tr}(\rho\hat{P}_{u_i}) &= \sum_{j=1}^n \langle u_j|\rho\hat{P}_{u_i}|u_j\rangle = \sum_{j=1}^n \langle u_j|\left(\sum_{k=1}^l p_k|\Psi_k\rangle\langle\Psi_k|\right)\hat{P}_{u_i}|u_j\rangle \\ &= \sum_{j=1}^n \left(\sum_{k=1}^l p_k \langle u_j|\Psi_k\rangle\langle\Psi_k|\hat{P}_{u_i}|u_j\rangle\right) = \sum_{k=1}^l \left(\sum_{j=1}^n p_k \langle\Psi_k|\hat{P}_{u_i}|u_j\rangle\langle u_j|\Psi_k\rangle\right) \\ &= \sum_{k=1}^l p_k \langle\Psi_k|\hat{P}_{u_i}\left(\sum_{j=1}^n |u_j\rangle\langle u_j|\right)|\Psi_k\rangle = \sum_{k=1}^l p_k \langle\Psi_k|\hat{P}_{u_i}|\Psi_k\rangle = p(i). \end{aligned} \quad (2.93)$$

Conseqüentemente, $p(i) = \text{Tr}(\rho\hat{P}_{u_i})$. Por sua vez, de acordo com a Eq. (2.77) o valor médio de \hat{O} é

$$\langle\hat{O}\rangle = \sum_{i=1}^n s_{u_i}p(i) = \sum_{i=1}^n s_{u_i}\left(\sum_{k=1}^l p_k \langle\Psi_k|\hat{P}_{u_i}|\Psi_k\rangle\right) = \sum_{i=1}^n \left(\sum_{k=1}^l s_{u_i}p_k \langle\Psi_k|\hat{P}_{u_i}|\Psi_k\rangle\right)$$

$$= \sum_{k=1}^l p_k \left(\sum_{i=1}^n s_{u_i} \langle \Psi_k | \hat{P}_{u_i} | \Psi_k \rangle \right) = \sum_{k=1}^l p_k \langle \Psi_k | \hat{O} | \Psi_k \rangle, \quad (2.94)$$

e, ao calcular o traço do operador $\rho \hat{O}$, concluimos que

$$\begin{aligned} \text{Tr}(\rho \hat{O}) &= \sum_{i=1}^n \langle u_i | \rho \hat{O} | u_i \rangle = \sum_{i=1}^n \langle u_i | \left(\sum_{k=1}^l p_k | \Psi_k \rangle \langle \Psi_k | \right) \hat{O} | u_i \rangle \\ &= \sum_{i=1}^n \left(\sum_{k=1}^l p_k \langle u_i | \Psi_k \rangle \langle \Psi_k | \hat{O} | u_i \rangle \right) = \sum_{k=1}^l \left(\sum_{i=1}^n p_k \langle \Psi_k | \hat{O} | u_i \rangle \langle u_i | \Psi_k \rangle \right) \\ &= \sum_{k=1}^l p_k \langle \Psi_k | \hat{O} \left(\sum_{i=1}^n | u_i \rangle \langle u_i | \right) | \Psi_k \rangle = \sum_{k=1}^l p_k \langle \Psi_k | \hat{O} | \Psi_k \rangle = \langle \hat{O} \rangle. \end{aligned} \quad (2.95)$$

Portanto, continuamos aptos a realizar previsões sobre o comportamento do sistema calculando as probabilidades $p(i)$ e o valor médio de \hat{O} através das relações $p(i) = \text{Tr}(\rho \hat{P}_{u_i})$ e $\langle \hat{O} \rangle = \text{Tr}(\rho \hat{O})$, cujos conceitos foram introduzidos nas seções 2.4.2 e 2.4.3.

Na seção 2.4.1 vimos a equação de Schrödinger (Eq. (2.57)) e a relação que fornecia a evolução no tempo de um estado $|\Psi(t_0)\rangle$ em $t = t_0$ para $|\Psi(t)\rangle$ em $t = t$ (Eq. (2.58)). Da mesma forma, existem equações análogas tanto para a dinâmica do operador ρ (Benenti et al., 2007)

$$i\hbar \frac{d}{dt} \rho(t) = [H, \rho(t)] \quad (2.96)$$

como para sua evolução no tempo quando $|\Psi(t)\rangle$ está sujeito à ação de um operador unitário $U(t, t_0)$,

$$\rho(t) = \sum_{k=1}^l p_k |\Psi(t)\rangle \langle \Psi(t)| = \sum_{k=1}^l p_k U(t, t_0) |\Psi(t_0)\rangle \langle \Psi(t_0)| U(t, t_0)^\dagger = U(t, t_0) \rho(t_0) U(t, t_0)^\dagger. \quad (2.97)$$

Existe ainda uma analogia com a Eq. (2.72) que revela o que ocorre quando o sistema é medido e fornece o autovalor s_{u_i} . Neste caso, há o colapso para o estado $|u_i\rangle$ associado a s_{u_i} , e a nova configuração assumida por ρ é

$$\rho'(t) = \frac{\hat{P}_{u_i} \rho(t) \hat{P}_{u_i}}{\text{Tr}(\rho \hat{P}_{u_i})}. \quad (2.98)$$

Assim, mesmo que no início não tenhamos conhecimento sobre qual estado o sistema reside, sabemos como será o novo operador $\rho'(t)$ após a medida de um determinado operador \hat{O} .

A seguir, demonstraremos as principais propriedades do operador densidade que nos permitirão distinguir sistemas puros de estados mistos.

(1) ρ é hermitiano (consulte a Eq. (2.33)).

$$\rho^\dagger = \left(\sum_{k=1}^l p_k |\Psi_k\rangle \langle \Psi_k| \right)^\dagger = \sum_{k=1}^l p_k (|\Psi_k\rangle)^\dagger (\langle \Psi_k|)^\dagger = \sum_{k=1}^l p_k |\Psi_k\rangle \langle \Psi_k| = \rho. \quad (2.99)$$

(2) $\text{Tr}\rho = 1$.

$$\begin{aligned} \text{Tr}\rho &= \sum_{i=1}^n \langle u_i | \rho | u_i \rangle = \sum_{i=1}^n \langle u_i | \left(\sum_{k=1}^l p_k |\Psi_k\rangle \langle \Psi_k| \right) | u_i \rangle \\ &= \sum_{i=1}^n \langle u_i | \left(\sum_{k=1}^l p_k \langle \Psi_k | u_i \rangle | \Psi_k \rangle \right) = \sum_{i=1}^n \left(\sum_{k=1}^l p_k \langle \Psi_k | u_i \rangle \langle u_i | \Psi_k \rangle \right) \\ &= \sum_{i=1}^n \left(\sum_{k=1}^l p_k |\langle u_i | \Psi_k \rangle|^2 \right) = \sum_{i=1}^n p(i) = 1. \end{aligned} \quad (2.100)$$

(3) ρ é um operador não-negativo, ou seja, o valor médio associado aos possíveis resultados após sua ação sobre um estado $|\Phi(t)\rangle$ nunca é negativo.

$$\begin{aligned} \langle \Phi(t) | \rho | \Phi(t) \rangle &= \langle \Phi(t) | \left(\sum_{k=1}^l p_k |\Psi_k\rangle \langle \Psi_k| \right) | \Phi(t) \rangle = \langle \Phi(t) | \left(\sum_{k=1}^l p_k \langle \Psi_k | \Phi(t) \rangle | \Psi_k \rangle \right) \\ &= \sum_{k=1}^l p_k \langle \Psi_k | \Phi(t) \rangle \langle \Phi(t) | \Psi_k \rangle = \sum_{k=1}^l p_k |\langle \Phi(t) | \Psi_k \rangle|^2 \geq 0. \end{aligned} \quad (2.101)$$

Agora, se analisarmos a matriz que representa o operador densidade em uma base qualquer e aplicarmos estas propriedades, podemos determinar se o sistema encontra-se em um estado puro ou misto. Considere a decomposição espectral de ρ em termos de seus autoestados $|u_i\rangle$,

$$\rho = \sum_{i=1}^n s_{u_i} |u_i\rangle \langle u_i|. \quad (2.102)$$

De acordo com a Eq. (2.101), $\langle \Phi(t) | \rho | \Phi(t) \rangle \geq 0$ para qualquer estado $|\Phi(t)\rangle$. Então, se $|\Phi(t)\rangle = |u_i\rangle$, $\langle u_i | \rho | u_i \rangle \geq 0$, e disso segue que

$$s_{u_i} \geq 0 \quad (2.103)$$

para qualquer autovalor de ρ . Sua representação matricial na base $|u_1\rangle, |u_2\rangle, |u_3\rangle, \dots, |u_n\rangle$ será

$$\rho = \begin{bmatrix} s_{u_1} & 0 & \dots & 0 \\ 0 & s_{u_2} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & s_{u_n} \end{bmatrix}. \quad (2.104)$$

Como $\text{Tr}\rho = 1$, os autovalores estão restritos ao vínculo

$$\sum_{i=1}^n s_{u_i} = 1, \quad (2.105)$$

e, visto que $s_{u_i} \geq 0$, então $0 \leq s_{u_i} \leq 1$. Por outro lado,

$$\rho^2 = \begin{bmatrix} s_{u_1}^2 & 0 & \dots & 0 \\ 0 & s_{u_2}^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & s_{u_n}^2 \end{bmatrix}, \quad (2.106)$$

e, dessa forma,

$$\sum_{i=1}^n s_{u_i}^2 \leq 1. \quad (2.107)$$

Assim, $\text{Tr}\rho^2 \leq 1$. Um caso especial ocorre quando $s_{u_i} = 1$, $s_{u_j} = 0$ para $j \neq i$ e $\text{Tr}\rho^2 = 1$. Mas se $s_{u_i} = 1$ para um único autovalor, o estado do sistema é puro, pois $\rho = |u_i\rangle\langle u_i|$. Visto que o traço é uma propriedade que não depende da representação matricial em questão, basta computar $\text{Tr}\rho^2$ se quisermos distinguir sistemas puros de misturas estatísticas. Para sistemas puros,

$$\text{Tr}\rho^2 = 1, \quad (2.108)$$

e, para misturas estatísticas,

$$\text{Tr}\rho^2 < 1. \quad (2.109)$$

Mostraremos a seguir como aplicar as propriedades do operador densidade para sistemas de um *qubit*.

Operador Densidade para um *Qubit*:

Retornemos à Eq. (2.82) na qual vimos uma das possíveis representações para um *qubit* em função dos parâmetros θ e ϕ ,

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle. \quad (2.110)$$

A matriz do operador densidade relativo a este estado é

$$\rho = |\Psi\rangle\langle\Psi| = \begin{bmatrix} \cos^2\frac{\theta}{2} & \sin\frac{\theta}{2}\cos\frac{\theta}{2}e^{-i\phi} \\ \sin\frac{\theta}{2}\cos\frac{\theta}{2}e^{i\phi} & \sin^2\frac{\theta}{2} \end{bmatrix}. \quad (2.111)$$

Na Eq. (2.54), mostramos que qualquer matriz pode ser expressa como uma combinação de I , σ_x , σ_y e σ_z . Assim, a matriz de ρ pode ser escrita como

$$\rho = a(I) + b(\sigma_x) + c(\sigma_y) + d(\sigma_z). \quad (2.112)$$

Visto que $\text{Tr}\rho = 1$, $\text{Tr}(I) = 2$ e $\text{Tr}(\sigma_x) = \text{Tr}(\sigma_y) = \text{Tr}(\sigma_z) = 0$, o coeficiente a deve ser igual a $1/2$. Logo, a matriz de ρ pode ser reescrita em termos dos parâmetros x , y , z das matrizes de Pauli,

$$\rho = \frac{1}{2}(I + x(\sigma_x) + y(\sigma_y) + z(\sigma_z)), \quad (2.113)$$

onde $x = 2b$, $y = 2c$, $z = 2d$, e sua forma matricial passa a ser representada por

$$\rho = \begin{bmatrix} 1+z & x-iy \\ x+iy & 1-z \end{bmatrix}. \quad (2.114)$$

Ao calcular o determinante na expressão (2.114), vemos que

$$\det\rho = \frac{1}{4}(1 - x^2 - y^2 - z^2). \quad (2.115)$$

Se associarmos o vetor r da esfera de Bloch de raio unitário (Fig. 2.1) às coordenadas x , y , z então $|r|^2 = x^2 + y^2 + z^2$ e

$$\det\rho = \frac{1}{4}(1 - |r|^2). \quad (2.116)$$

Por outro lado, de acordo com a Eq. (2.103), os autovalores s_{u_1} e s_{u_2} de ρ são positivos ou nulos. Como $\det\rho = s_{u_1} \times s_{u_2}$ na representação matricial em (2.104), segue que $\det\rho \geq 0$ e $0 \leq |r| \leq 1$.

Assim, podemos mapear qualquer sistema quântico associando-o às coor-

denadas x , y , z do vetor r na esfera de Bloch de raio unitário. Se o sistema estiver em um estado puro, então $s_{u_1} = 1$ e $s_{u_2} = 0$ (ou o inverso) e $|r| = 1$. Para qualquer outra condição, $|r| < 1$. Desse modo, um ponto na superfície da esfera representa um estado puro e os pontos para os quais $|r| < 1$ representam estados mistos.

Considere agora um caso especial. Suponha que o *qubit* possa estar em qualquer um dos estados relativos aos parâmetros θ e ϕ com a mesma probabilidade. Desta forma, para construir a matriz do operador densidade devemos integrar a Eq. (2.111) sobre todas as direções do espaço

$$\int_0^{2\pi} d\phi \int_0^\pi d\theta \sin \theta \begin{bmatrix} \cos^2 \frac{\theta}{2} & \sin \frac{\theta}{2} \cos \frac{\theta}{2} e^{-i\phi} \\ \sin \frac{\theta}{2} \cos \frac{\theta}{2} e^{i\phi} & \sin^2 \frac{\theta}{2} \end{bmatrix}. \quad (2.117)$$

Antes de prosseguir, é preciso verificar se expressão (2.117) possui norma unitária. O cálculo de $\int_0^{2\pi} d\phi \int_0^\pi d\theta \sin \theta$ fornece 4π como resultado, logo,

$$\rho = \frac{1}{4\pi} \int_0^{2\pi} d\phi \int_0^\pi d\theta \sin \theta \begin{bmatrix} \cos^2 \frac{\theta}{2} & \sin \frac{\theta}{2} \cos \frac{\theta}{2} e^{-i\phi} \\ \sin \frac{\theta}{2} \cos \frac{\theta}{2} e^{i\phi} & \sin^2 \frac{\theta}{2} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2} I. \quad (2.118)$$

Repare na Eq. (2.118) que $\rho^2 = \frac{1}{4} I \Rightarrow \text{Tr} \rho^2 < 1$ (confirmando o fato de o estado ser misto) e que $x = y = z = 0$ em (2.114). Assim, o sistema em questão está localizado no centro da esfera de Bloch. Se calcularmos o valor médio de qualquer um dos operadores de Pauli, veremos que

$$\langle \sigma_k \rangle = \text{Tr}(\rho \sigma_k) = \text{Tr}\left(\frac{1}{2} I \sigma_k\right) = \frac{1}{2} \text{Tr}(\sigma_k) = 0. \quad (2.119)$$

Dizemos que neste caso o sistema está despolarizado. Um sistema polarizado é aquele em que pelo menos uma das componentes $\langle \sigma_k \rangle$ ($k = x, y, z$) não é nula. Para um estado qualquer na forma da Eq. (2.113), o valor médio do operador σ_k é dado por

$$\langle \sigma_k \rangle = \text{Tr}(\rho \sigma_k) = \text{Tr} \left[\frac{1}{2} (I + x\sigma_x + y\sigma_y + z\sigma_z) \sigma_k \right] = \text{Tr} \left[\frac{1}{2} (x\sigma_x + y\sigma_y + z\sigma_z) \sigma_k \right] = k. \quad (2.120)$$

Observe com atenção o resultado final da Eq. (2.120). O valor médio do operador $\langle \sigma_k \rangle$ ($k = x, y, z$) de um determinado sistema é igual à própria componente k . Se forem preparados vários sistemas idênticos descritos pelo mesmo operador densidade sobre o qual não há nenhuma informação, podemos obter com boa aproximação os valores das componentes x , y , z ao efetuarmos um extenso número de medidas de $\langle \sigma_x \rangle$, $\langle \sigma_y \rangle$ e $\langle \sigma_z \rangle$ aleatoriamente. De posse destes dados, podemos determinar ρ e o operador densidade que descreve igualmente cada sistema. No próximo tópico discutiremos a relação do

operador densidade com sistemas que possuem mais de um *qubit*.

Operador Densidade para Sistemas Compostos:

Finalizaremos esta seção mostrando como obter informações relativas a um único sistema quando o vetor de estado envolve mais de um *qubit*. Sejam os operadores lineares e os estados de base $\{\hat{O}_1, |u_i\rangle\} \in H_1$, $\{\hat{O}_2, |w_a\rangle\} \in H_2$ e seja o sistema constituído pelo vetor de estado $|\psi\rangle$ em $H = H_1 \otimes H_2$ tal que $|\psi\rangle = \sum_{a=1}^{N_2} \sum_{i=1}^{N_1} D_{i,a}(|u_i\rangle \otimes |w_a\rangle)$, onde H_1 e H_2 são espaços vetoriais de dimensão N_1 e N_2 , respectivamente. O operador densidade deste sistema é dado por

$$\rho = |\Psi\rangle\langle\Psi| = \sum_{j,b=1}^{N_1,N_2} \sum_{i,a=1}^{N_1,N_2} D_{i,a} D_{j,b}^* (|u_i\rangle \otimes |w_a\rangle) (\langle u_j| \otimes \langle w_b|). \quad (2.121)$$

Deste ponto em diante, omitiremos os limites nas somas e condensaremos o produto tensorial $|\cdot\rangle \otimes |\cdot\rangle$ na forma $|\cdot\rangle|\cdot\rangle$ para que as expressões apareçam em uma notação mais compacta. Se definirmos o produto $D_{i,a} D_{j,b}^*$ como

$$D_{i,a} D_{j,b}^* = \rho_{ia,jb} = \langle u_i | \langle w_a | \rho | u_j \rangle | w_b \rangle, \quad (2.122)$$

a Eq. (2.121) pode ser escrita como

$$\rho = |\Psi\rangle\langle\Psi| = \sum_{j,b} \sum_{i,a} \rho_{ia,jb} |u_i\rangle |w_a\rangle \langle u_j| \langle w_b|. \quad (2.123)$$

Agora, suponha que apliquemos sobre o sistema um operador \hat{O}_1 que só atua sobre os vetores pertencentes a H_1 . Assim, podemos expressá-lo como um operador em H através de

$$\hat{O} = \hat{O}_1 \otimes I_2, \quad (2.124)$$

visto que o operador I_2 não afeta os vetores pertencentes a H_2 . Se quisermos descobrir o valor esperado de \hat{O}_1 , devemos calcular

$$\begin{aligned} \langle \hat{O}_1 \rangle &= \text{Tr}(\rho \hat{O}) = \sum_{k,c} \langle u_k | \langle w_c | \rho \hat{O} | u_k \rangle | w_c \rangle \\ &= \sum_{k,c} \langle u_k | \langle w_c | \left(\sum_{j,b} \sum_{i,a} \rho_{ia,jb} |u_i\rangle |w_a\rangle \langle u_j| \langle w_b| \right) (\hat{O}_1 \otimes I_2) | u_k \rangle | w_c \rangle. \end{aligned} \quad (2.125)$$

Como $\langle u_k | u_i \rangle = \delta_{k,i}$, $\langle w_c | w_a \rangle = \delta_{c,a}$ e $\langle w_b | w_c \rangle = \delta_{b,c}$, a Eq. (2.125) se reduz a

$$\langle \hat{O}_1 \rangle = \sum_{i,j,a} \rho_{ia,ja} \langle u_j | \hat{O}_1 | u_i \rangle. \quad (2.126)$$

Neste momento, faremos uma breve digressão para introduzir o conceito de traço parcial. Em um sistema cujos estados de base sejam combinações de vetores pertencentes a espaços vetoriais distintos 1 e 2, o operador densidade relativo ao subsistema 1 é definido como

$$\rho_1 \equiv \text{Tr}_2 \rho \equiv \sum_a \langle w_a | \rho | w_a \rangle, \quad (2.127)$$

e, analogamente, o operador densidade relativo ao subsistema 2 é definido como

$$\rho_2 \equiv \text{Tr}_1 \rho \equiv \sum_i \langle u_i | \rho | u_i \rangle. \quad (2.128)$$

Por outro lado, segundo as Eqs. (2.123) e (2.127), o elemento de matriz $(\rho_1)_{i,j}$ é dado por

$$\begin{aligned} (\rho_1)_{i,j} &= \langle u_i | \rho_1 | u_j \rangle = \langle u_i | (\sum_a \langle w_a | \rho | w_a \rangle) | u_j \rangle \\ &= \langle u_i | \left\{ \sum_a \langle w_a | \left(\sum_{j,b} \sum_{i,a} \rho_{ia,jb} |u_i\rangle |w_a\rangle \langle u_j| \langle w_b| \right) |w_a\rangle \right\} | u_j \rangle = \sum_a \rho_{ia,ja}. \end{aligned} \quad (2.129)$$

Com os resultados fornecido pelas Eq. (2.129), podemos retornar à Eq. (2.126) e calcular o valor esperado de \hat{O}_1 ,

$$\langle \hat{O}_1 \rangle = \sum_{i,j} \langle u_i | \rho_1 | u_j \rangle \langle u_j | \hat{O}_1 | u_i \rangle = \sum_i \langle u_i | \rho_1 \hat{O}_1 | u_i \rangle = \text{Tr}(\rho_1 \hat{O}_1). \quad (2.130)$$

e, analogamente,

$$\langle \hat{O}_2 \rangle = \text{Tr}(\rho_2 \hat{O}_2). \quad (2.131)$$

Portanto, se $|\psi\rangle \in H = H_A \otimes H_B$ é um vetor de estado de um sistema composto, ρ é o operador densidade deste sistema e desejarmos reduzir este último para que fique somente em função do subsistema A , aplicamos

$$\rho_A = \text{Tr}_B \rho = \sum_l \langle w_l | \rho | w_l \rangle \quad (2.132)$$

sobre os estados de base $|w_l\rangle$ de B .

Se, por outro lado, quisermos saber a probabilidade de este sistema reduzido estar associado a algum dos estados de base $|u_i\rangle$ de A , calculamos

$$p(i) = \langle u_i | \rho_A | u_i \rangle. \quad (2.133)$$

E, finalmente, se desejarmos calcular o valor esperado de um operador \hat{O}_A

que atua somente em estados pertencentes ao espaço vetorial H_A , basta efetuar a operação

$$\langle \hat{O}_A \rangle = \text{Tr}(\rho_A \hat{O}_A). \quad (2.134)$$

Note que os subsistemas A e B também podem ser compostos, pois em momento algum mencionamos que estes são formados por estados de base de um *qubit*. Estas propriedades são fundamentais para o cálculo das probabilidades associadas aos sistemas compostos que serão analisados nos próximos capítulos.

2.7 Portas Lógicas

Encerraremos este capítulo apresentado conceitos relacionados à computação quântica e as operações lógicas mais comuns que podem ser implementadas sobre *qubits*, mostrando como operar sobre *qubits* simples e sistemas compostos de pares do tipo $H_s = H_a \otimes H_b$. O papel dos *qubits* sob a ótica de operações lógicas é compatível com o de *bits* clássicos presentes em sistemas de informação, e muitas destas portas são utilizadas em sistemas eletrônicos atuais. O leitor deve analisar atentamente cada item para que consiga compreender a função destas operações e o motivo de sua utilização quando aplicarmos correções de estados quânticos imperfeitos, ou, em outras palavras, com fidelidade menor do que um; e notar que todas são reversíveis e atuam como operadores lineares, sejam em estados normalizados de um *qubit* como $\alpha|0\rangle + \beta|1\rangle$ ou de dois *qubits* como $\alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}$.

As principais portas lógicas simples são as portas X , Y , Z , H e $Fase$; e para sistemas compostos de dois *qubits* merecem destaque as portas $CNOT$, $Z - Controlada$, $Fase - Controlada$ e $Swap$. Para todas elas, mostraremos que o estado final de cada *qubit* está relacionado a seu valor inicial de forma única para cada operação.

Discutiremos a seguir o mecanismo de funcionamento das portas simples e sua relação com os operadores de Pauli.

2.7.1 Portas de um *Qubit*

Os Operadores de Pauli:

Os operadores de Pauli podem ser associados às portas lógicas x , y , z e seus componentes físicos da mesma maneira que operadores algébricos representam ferramentas de medição em sistemas práticos. Vimos na seção 2.5 a forma matricial padrão para *qubits* e em 2.3 como representar matricialmente os operadores de Pauli, mas ainda não havíamos comentado o que ocorria quando algum destes operadores atuava nos estados de base $|0\rangle$ e $|1\rangle$. Vejamos então como funcionam estes operadores:

Porta X (NOT):

A porta X ou NOT inverte o valor do *qubit*, seja ele $|0\rangle$ ou $|1\rangle$.

$$\begin{aligned}\sigma_x|0\rangle &= |1\rangle, \\ \sigma_x|1\rangle &= |0\rangle, \\ \sigma_x(\alpha|0\rangle + \beta|1\rangle) &= \alpha|1\rangle + \beta|0\rangle.\end{aligned}\tag{2.135}$$

Porta Z:

A porta Z mantém o *qubit* $|0\rangle$ inalterado e inverte o sinal de $|1\rangle$.

$$\begin{aligned}\sigma_z|0\rangle &= |0\rangle, \\ \sigma_z|1\rangle &= -|1\rangle, \\ \sigma_z(\alpha|0\rangle + \beta|1\rangle) &= \alpha|0\rangle - \beta|1\rangle.\end{aligned}\tag{2.136}$$

Porta Y:

A porta Y acrescenta a fase i e troca o valor tanto de $|0\rangle$ como de $|1\rangle$, invertendo o sinal apenas para este último.

$$\begin{aligned}\sigma_y|0\rangle &= i|1\rangle, \\ \sigma_y|1\rangle &= -i|0\rangle, \\ \sigma_y(\alpha|0\rangle + \beta|1\rangle) &= i\alpha|1\rangle - i\beta|0\rangle.\end{aligned}\tag{2.137}$$

Hadamard:

A porta H produz uma combinação entre $|0\rangle$ e $|1\rangle$.

$$\begin{aligned}H|0\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \\ H|1\rangle &= \frac{|0\rangle-|1\rangle}{\sqrt{2}}, \\ H(\alpha|0\rangle + \beta|1\rangle) &= \alpha\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right).\end{aligned}\tag{2.138}$$

Fase:

A porta de *Fase* mantém o estado $|0\rangle$ inalterado e acrescenta a fase i em $|1\rangle$.

$$S|0\rangle = |0\rangle,$$

$$\begin{aligned}
 S|1\rangle &= i|1\rangle, \\
 S(\alpha|0\rangle + \beta|1\rangle) &= \alpha|0\rangle + i\beta|1\rangle.
 \end{aligned}
 \tag{2.139}$$

A figura 2.2 mostra as principais portas simples com suas respectivas nomenclaturas e representações matriciais.


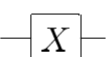
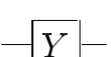
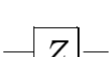

Hadamard		$\frac{1}{\sqrt{2}}$	$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X			$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y			$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z			$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Fase			$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

Figura 2.2: Portas que atuam em um qubit, suas respectivas nomenclaturas e representações matriciais.

Fonte: Figura adaptada de *Benenti et al., 2007*.

2.7.2 Portas de dois Qubits

As portas de dois *qubits* operam sobre o conjunto de estados $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ e $|1\rangle|1\rangle$. Quando uma porta é classificada como "controlada", o estado final dos dois *qubits* só é alterado se o *qubit* de controle estiver ativo. Geralmente, estas portas são projetadas para utilizar o primeiro *qubit* como controle e só entrarem em ação caso seu valor seja $|1\rangle$. A figura 2.3 mostra um exemplo para a porta *CNOT*. O círculo menor está posicionado sobre o *qubit* de controle, e a operação da porta é ativada de acordo com seu preenchimento. Para o círculo vazio a porta entra em ação quando o controle for igual a $|0\rangle$, e para o círculo cheio a ativação ocorre se o controle for $|1\rangle$. Adotaremos a convenção padrão que considera o controle no primeiro *qubit* e a ativação da porta para o estado $|1\rangle$.

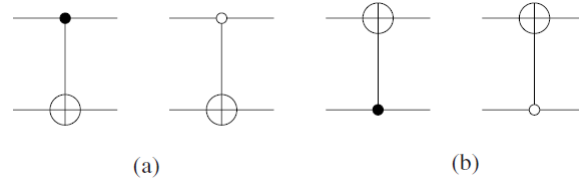


Figura 2.3: Figura esquemática para portas de dois qubits. Em (a): controle no primeiro qubit. Em (b): controle no segundo qubit. O círculo menor preenchido representa a ativação da porta quando o qubit de controle for $|1\rangle$, e o círculo menor vazio representa a ativação quando o qubit de controle for $|0\rangle$.

Fonte: Figura adaptada de *Benenti et al., 2007*.

Not-Controlada:

A porta *CNOT* inverte o valor do segundo *qubit* apenas quando o controle for igual a $|1\rangle$.

$$\begin{aligned}
 CNOT_{1,2}|0\rangle|0\rangle &= |0\rangle|0\rangle, \\
 CNOT_{1,2}|0\rangle|1\rangle &= |0\rangle|1\rangle, \\
 CNOT_{1,2}|1\rangle|0\rangle &= |1\rangle|1\rangle, \\
 CNOT_{1,2}|1\rangle|1\rangle &= |1\rangle|0\rangle, \\
 CNOT_{1,2}(\alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}) \\
 &= \alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|11\rangle_{1,2} + \delta'|10\rangle_{1,2}.
 \end{aligned} \tag{2.140}$$

Swap(Troca):

A porta *Swap* permuta os valores dos dois *qubits*.

$$\begin{aligned}
 (Swap)_{1,2}|0\rangle|0\rangle &= |0\rangle|0\rangle, \\
 (Swap)_{1,2}|0\rangle|1\rangle &= |1\rangle|0\rangle, \\
 (Swap)_{1,2}|1\rangle|0\rangle &= |0\rangle|1\rangle, \\
 (Swap)_{1,2}|1\rangle|1\rangle &= |1\rangle|1\rangle, \\
 (Swap)_{1,2}(\alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}) \\
 &= \alpha'|00\rangle_{1,2} + \beta'|10\rangle_{1,2} + \gamma'|01\rangle_{1,2} + \delta'|11\rangle_{1,2}.
 \end{aligned} \tag{2.141}$$

Z-Controlada:

A porta *Z* inverte o sinal global entre os dois *qubits* apenas quando o controle e o alvo forem iguais a $|1\rangle$.

$$Z_{1,2}|0\rangle|0\rangle = |0\rangle|0\rangle,$$

$$\begin{aligned}
Z_{1,2}|0\rangle|1\rangle &= |0\rangle|1\rangle, \\
Z_{1,2}|1\rangle|0\rangle &= |1\rangle|0\rangle, \\
Z_{1,2}|1\rangle|1\rangle &= -|1\rangle|1\rangle, \\
Z_{1,2}(\alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}) \\
&= \alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} - \delta'|11\rangle_{1,2}.
\end{aligned} \tag{2.142}$$

Fase-Controlada:

A porta de *Fase* acrescenta a fase i entre os dois *qubits* apenas quando o controle e o alvo forem iguais a $|1\rangle$.

$$\begin{aligned}
S_{1,2}|0\rangle|0\rangle &= |0\rangle|0\rangle, \\
S_{1,2}|0\rangle|1\rangle &= |0\rangle|1\rangle, \\
S_{1,2}|1\rangle|0\rangle &= |1\rangle|0\rangle, \\
S_{1,2}|1\rangle|1\rangle &= i|1\rangle|1\rangle, \\
S_{1,2}(\alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}) \\
&= \alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + i\delta'|11\rangle_{1,2}.
\end{aligned} \tag{2.143}$$

A figura 2.4 mostra as principais portas de dois *qubits* com suas respectivas nomenclaturas e representações matriciais, e a fig 2.5 revela como construí-las a partir de portas simples de um *qubit* e da porta *CNOT*.

NOT-controlada		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Swap (troca)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Z-controlada		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
Fase-controlada		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$

Figura 2.4: Portas que atuam em dois *qubit*, suas respectivas nomenclaturas e representações matriciais.

Fonte: Figura adaptada de *Benenti et al., 2007*.

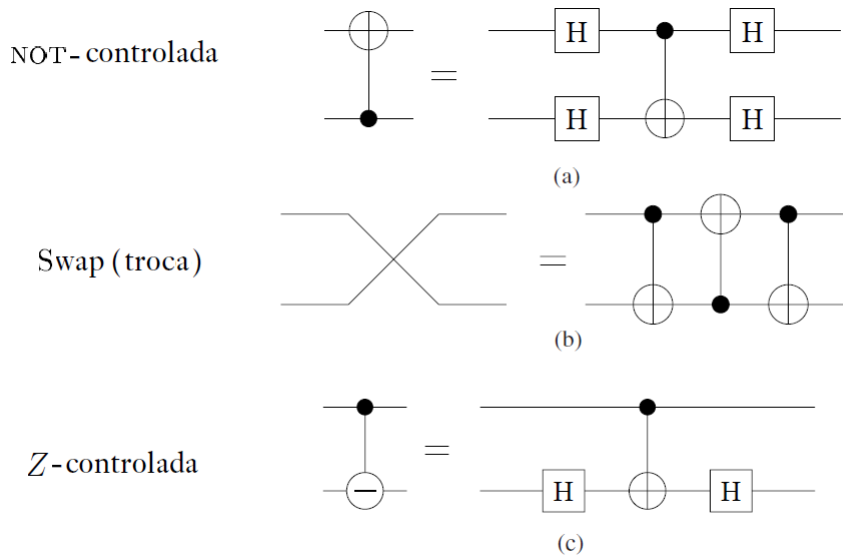


Figura 2.5: Construindo portas de dois qubits a partir de portas de um qubit. Em (a): a porta CNOT com controle no segundo qubit. Em (b): a porta Swap. Em (c): a porta Z – Controlada com controle no primeiro qubit.
 Fonte: Figura adaptada de Benenti et al., 2007.

Capítulo 3

Canais Perfeitamente Emaranhados: O Protocolo Original

3.1 O Protocolo Original

A primeira vez que o teletransporte (ou teleporte) quântico foi proposto como um método prático ocorreu em um artigo de Charles Bennet e colaboradores publicado em 1993, que será explicado nesta seção. Desde então, muitos métodos foram propostos mas todos se baseiam no princípio fundamental introduzido por este artigo: a transmissão de um **estado quântico** entre partículas separadas por uma determinada distância, sem que ambas interajam diretamente. Muitos pensam que o teleporte só envolve partículas, mas não é este o caso que abordaremos neste trabalho. Sabemos como teleportar estados, ou, em outras palavras, informação quântica, mas não sabemos ainda como transportar elementos portadores de massa. A idéia principal de qualquer teletransporte é a transmissão de algum tipo de informação (seja o estado de átomos em um certo ordenamento ou o estado de spin de um elétron) de um ponto a outro sem que haja um meio contínuo entre eles. Portanto, nosso foco será sempre o envio de estados quânticos de uma partícula a outra, sem que a partícula original seja enviada no processo. A seguir, descreveremos as principais propriedades relacionadas a estados quânticos e ao emaranhamento.

Em linhas gerais, queremos que um emissor (que chamaremos de Alice) “teleporte” um estado quântico para um receptor (que chamaremos de Bob) fazendo uso de uma característica peculiar de sistemas quânticos: o emaranhamento. De uma forma bem simples, o emaranhamento pode ser entendido como uma propriedade eminentemente quântica entre duas partículas que pode ser mantida mesmo em grandes distâncias na ausência de efeitos dissipativos, como ilustra a figura 3.1 (já existem dispositivos operando com partículas separadas por distâncias superiores a 100 km). A grande dificuldade em manter um sistema emaranhado deve-se ao fato de o mesmo ser extremamente sensível às

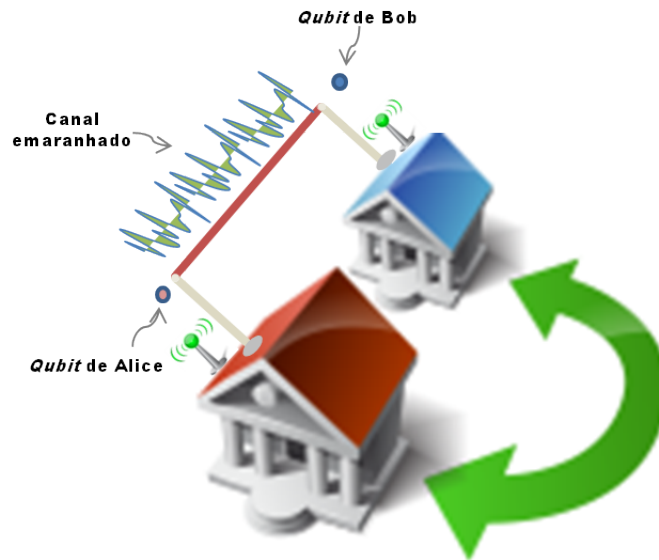


Figura 3.1: Teleporte de informação quântica entre dois pontos distintos utilizando um canal emaranhado. As cores vermelha e azul referem-se à Alice e Bob, respectivamente. As casas representam os pontos inicial e final do processo de teleporte. Os qubits que constituem o canal foram destacados para melhor visualização. A barra vermelha representa o canal formado pelo estado emaranhado entre estes qubits.

flutuações térmicas do ambiente, fenômeno que é conhecido como decoerência. Quando isto ocorre, o emaranhamento rapidamente é destruído.

Outra propriedade importante de estados quânticos está relacionada ao colapso dos estados quando estes são submetidos a algum tipo de medida externa. Se estivermos operando um sistema clássico, é possível que determinados bits consigam ser “copiados” sem afetar o sistema que os comporta. Para sistemas quânticos, entretanto, não é possível clonar um estado (ou melhor dizendo, um *qubit*) sem que o sistema seja perturbado. Esta característica é conhecida como o teorema da não-clonagem (?; Dieks, 1982), e é de suma importância na área de criptografia quântica. Dito isso, podemos inferir que este protocolo apresenta vantagens em relação aos protocolos clássicos: além de poder transmitir a informação desejada, evitando que o estado original seja enviado diretamente a Bob, não é preciso que nenhum dos participantes saiba o conteúdo da informação antes do procedimento. Para que o conteúdo da mensagem fosse descoberto, seria necessário realizar uma medida sobre o sistema, que, por sua vez, seria perturbado e colapsaria para um de seus auto-estados, perdendo sua configuração original. Assim, nem Alice e nem Bob têm conhecimento prévio da mensagem que estão compartilhando, salvo o cenário em que Alice prepara conscientemente um estado (como $|0\rangle$) e deseja enviá-lo a Bob. Neste caso, Bob poderia contactar Alice e reproduzir facilmente o estado em seu laboratório, evitando recorrer a este procedimento. Portanto, o teleporte quântico justifica-se principalmente

pela transmissão de estados desconhecidos, cabendo ao transmissor e receptor partilharem os motivos que envolvam sua utilização.

Mostraremos ainda que o processo completo garante fidelidade um (ou seja, a estrutura do estado final recebido será idêntica àquela do estado enviado) e probabilidade um (em todas as vezes que o protocolo for aplicado, a informação chegará a seu destino, com 100% de chance de sucesso).

Iniciaremos agora a descrição do protocolo. O estado que Alice deseja transmitir pode ser representado por um *qubit*, cuja forma geral é

$$|\phi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1. \quad (3.1)$$

Nesta representação, o estado inicial está expresso em termos da superposição dos estados $|0\rangle_1$ e $|1\rangle_1$. Os coeficientes α e β podem assumir qualquer valor, desde que a condição de normalização $|\alpha|^2 + |\beta|^2 = 1$ seja obedecida. Simplificaremos os cálculos deste texto ao considerar valores reais para α e β e frisamos que tal restrição não acarreta perda de generalidade, uma vez que valores complexos associados a estes coeficientes geram os mesmos resultados. Alice e Bob precisam ter à sua disposição um canal, que neste

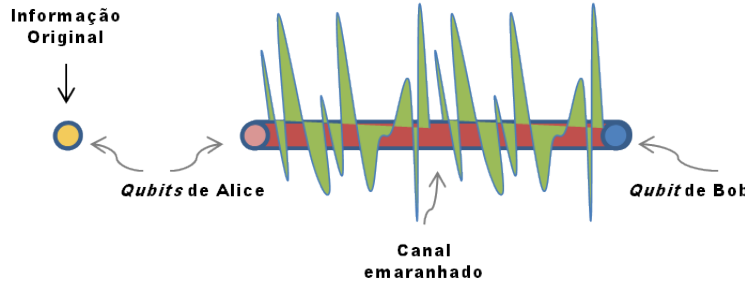


Figura 3.2: Canal formado pelo estado emaranhado entre o qubit de Alice (vermelho) e o de Bob (azul). No lado esquerdo, a informação original representada pelo qubit amarelo de Alice.

caso é um par emaranhado do tipo EPR (Einstein et al., 1935). Uma das representações possíveis para o canal é

$$|\Phi^+\rangle_{2,3} = \frac{|00\rangle_{2,3} + |11\rangle_{2,3}}{\sqrt{2}}, \quad (3.2)$$

onde o estado $|\Phi^+\rangle$ pertence ao conjunto dos estados da base de Bell, que listamos logo abaixo:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad |\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \quad (3.3)$$

Assim como os estados da base de Bell, os estados $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$ também formam uma base completa de dimensão 4. Os índices 1, 2, e 3 referem-se às partículas envolvidas no processo. Alice possui o *qubit* original, representado por 1, e um dos pares do canal, que será associado ao índice 2. O outro constituinte do par que está

em posse de Bob será descrito pelo índice 3.

O sistema formado pelo *qubit* original e o canal pode ser expresso pelo produto tensorial entre $|\phi\rangle_1$ e $|\Phi^+\rangle_{2,3}$,

$$|\phi\rangle_1|\Phi^+\rangle_{2,3} = \frac{\alpha}{\sqrt{2}}|000\rangle_{1,2,3} + \frac{\alpha}{\sqrt{2}}|011\rangle_{1,2,3} + \frac{\beta}{\sqrt{2}}|100\rangle_{1,2,3} + \frac{\beta}{\sqrt{2}}|111\rangle_{1,2,3}, \quad (3.4)$$

onde englobamos todos os constituintes do sistema.

Antes de prosseguirmos com o protocolo, precisamos fazer mais uma consideração. Uma vez que as medidas de Alice serão realizadas na base de Bell, podemos reescrever a Eq. (3.3) rearranjando os estados da base computacional em função dos estados da base de Bell:

$$|00\rangle = \frac{|\Phi^+\rangle + |\Phi^-\rangle}{\sqrt{2}}, \quad |01\rangle = \frac{|\Psi^+\rangle + |\Psi^-\rangle}{\sqrt{2}}, \quad |10\rangle = \frac{|\Psi^+\rangle - |\Psi^-\rangle}{\sqrt{2}}, \quad |11\rangle = \frac{|\Phi^+\rangle - |\Phi^-\rangle}{\sqrt{2}}. \quad (3.5)$$

Com isso, podemos expressar o estado geral do sistema em função destes estados, que será

$$\begin{aligned} |\text{Estado Geral}\rangle &= |\phi\rangle_1|\Phi^+\rangle_{2,3} \\ &= \frac{\alpha}{\sqrt{2}} \left(\frac{|\Phi^+\rangle_{1,2} + |\Phi^-\rangle_{1,2}}{\sqrt{2}} \right) |0\rangle_3 + \frac{\alpha}{\sqrt{2}} \left(\frac{|\Psi^+\rangle_{1,2} + |\Psi^-\rangle_{1,2}}{\sqrt{2}} \right) |1\rangle_3 \\ &\quad + \frac{\beta}{\sqrt{2}} \left(\frac{|\Psi^+\rangle_{1,2} - |\Psi^-\rangle_{1,2}}{\sqrt{2}} \right) |0\rangle_3 + \frac{\beta}{\sqrt{2}} \left(\frac{|\Phi^+\rangle_{1,2} - |\Phi^-\rangle_{1,2}}{\sqrt{2}} \right) |1\rangle_3 \\ &= \frac{1}{2} (|\Phi^+\rangle_{1,2}[\alpha|0\rangle_3 + \beta|1\rangle_3]) + \frac{1}{2} (|\Phi^-\rangle_{1,2}[\alpha|0\rangle_3 - \beta|1\rangle_3]) \\ &\quad + \frac{1}{2} (|\Psi^+\rangle_{1,2}[\beta|0\rangle_3 + \alpha|1\rangle_3]) + \frac{1}{2} (|\Psi^-\rangle_{1,2}[-\beta|0\rangle_3 + \alpha|1\rangle_3]), \end{aligned} \quad (3.6)$$

e o operador densidade associado ao estado geral,

$$\begin{aligned} \rho &= |\text{Estado Geral}\rangle\langle\text{Estado Geral}| = |\phi\rangle_1|\Phi^+\rangle_{2,3} {}_{2,3}\langle\Phi^+|_1\langle\phi| \\ &= \frac{1}{4} (|\Phi^+\rangle_{1,2} {}_{1,2}\langle\Phi^+|) (\alpha|0\rangle_3 + \beta|1\rangle_3) (\alpha^* {}_3\langle 0| + \beta^* {}_3\langle 1|) \\ &\quad + \frac{1}{4} (|\Phi^-\rangle_{1,2} {}_{1,2}\langle\Phi^-|) (\alpha|0\rangle_3 - \beta|1\rangle_3) (\alpha^* {}_3\langle 0| - \beta^* {}_3\langle 1|) \\ &\quad + \frac{1}{4} (|\Psi^+\rangle_{1,2} {}_{1,2}\langle\Psi^+|) (\beta|0\rangle_3 + \alpha|1\rangle_3) (\beta^* {}_3\langle 0| + \alpha^* {}_3\langle 1|) \\ &\quad + \frac{1}{4} (|\Psi^-\rangle_{1,2} {}_{1,2}\langle\Psi^-|) (-\beta|0\rangle_3 + \alpha|1\rangle_3) (-\beta^* {}_3\langle 0| + \alpha^* {}_3\langle 1|), \\ &\quad + \text{termos cruzados do tipo } |\Phi^+\rangle_{2,3} {}_{2,3}\langle\Phi^-|, |\Phi^-\rangle_{2,3} {}_{2,3}\langle\Phi^+|, \dots \end{aligned} \quad (3.7)$$

Munidos destas informações, agora podemos iniciar a descrição deste método. A primeira etapa consiste em Alice medir o sistema na base de Bell. Observe nas Eqs. (3.6) e (3.7) que cada um dos quatro estados tem a mesma probabilidade de ser

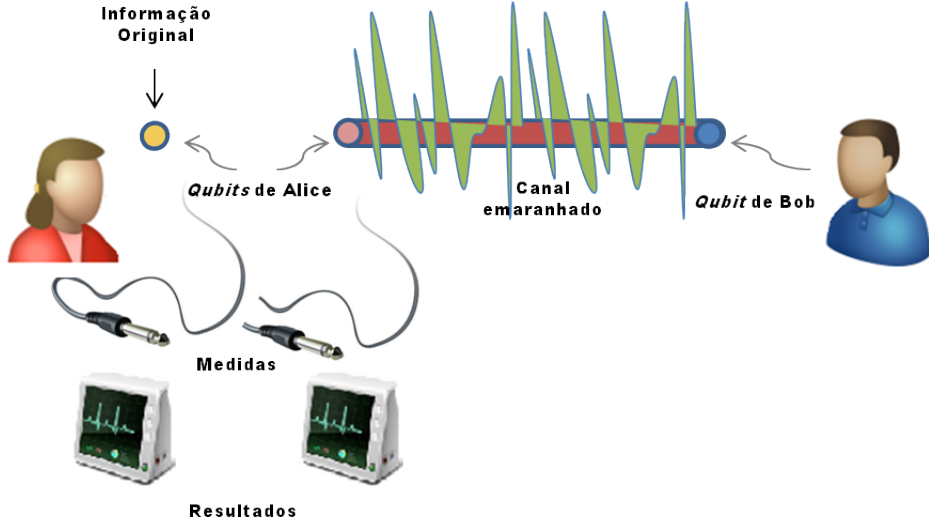


Figura 3.3: Elementos básicos de um protocolo de teleporte quântico: o qubit amarelo representa a informação original, e o canal emaranhado é representado pelo par de qubits vermelho (Alice) e azul (Bob). A barra vermelha e o sinal ondulatório em verde reforçam a idéia de que o canal é emaranhado. Os cabos pretos e os monitores em cinza representam respectivamente a base de medidas escolhida por Alice e o resultado destas medidas.

obtido, pois todos estão normalizados e possuem o mesmo coeficiente. De fato, de acordo com a Eq. (2.134) do capítulo 2, as probabilidades são dadas por

$$\begin{aligned}
 P_{suc} \rightarrow (\alpha|0\rangle_3 + \beta|1\rangle_3) &= {}_{1,2}\langle\Phi^+|\rho_{1,2}|\Phi^+\rangle_{1,2} = \frac{1}{4}, \\
 P_{suc} \rightarrow (\alpha|0\rangle_3 - \beta|1\rangle_3) &= {}_{1,2}\langle\Phi^-|\rho_{1,2}|\Phi^-\rangle_{1,2} = \frac{1}{4}, \\
 P_{suc} \rightarrow (\beta|0\rangle_3 + \alpha|1\rangle_3) &= {}_{1,2}\langle\Psi^+|\rho_{1,2}|\Psi^+\rangle_{1,2} = \frac{1}{4}, \\
 P_{suc} \rightarrow (-\beta|0\rangle_3 + \alpha|1\rangle_3) &= {}_{1,2}\langle\Psi^-|\rho_{1,2}|\Psi^-\rangle_{1,2} = \frac{1}{4}.
 \end{aligned} \tag{3.8}$$

Contudo, note que poderíamos elevar ao quadrado o módulo de cada coeficiente em (3.6) que o resultado seria o mesmo. Faremos isto nos próximos capítulos para evitar estender os cálculos demasiadamente.

Uma vez realizada a medida, Alice precisa informar o resultado a Bob. Para isso, a cada um dos quatro estados pode ser associada uma representação binária extra, com o intuito de distingui-los. Por convenção, utiliza-se

$$|\Phi^+\rangle = 00, \quad |\Phi^-\rangle = 01, \quad |\Psi^+\rangle = 10, \quad |\Psi^-\rangle = 11. \tag{3.9}$$

Assim, de acordo com o resultado obtido, Alice pode enviar separadamente dois bits clássicos a Bob, e este, por sua vez, saberá para qual estado o sistema colapsou. Em seguida, basta que seja aplicada uma transformação unitária adequada, e o *qubit*

Resultado obtido por Alice	<i>Qubit</i> de Bob	Correção
$ \Phi^+\rangle$	$\alpha 0\rangle + \beta 1\rangle$	I
$ \Phi^-\rangle$	$\alpha 0\rangle - \beta 1\rangle$	σ_z
$ \Psi^+\rangle$	$\alpha 1\rangle + \beta 0\rangle$	σ_x
$ \Psi^-\rangle$	$\alpha 1\rangle - \beta 0\rangle$	$i\sigma_y$ ou $\sigma_z\sigma_x$

Tabela 3.1: Resultados possíveis para as medidas de Alice e as respectivas correções que Bob precisa aplicar.

original será recuperado, como mostra a tabela 3.1. Vamos recorrer às matrizes de Pauli e mostrar um exemplo, lembrando que

$$\sigma_x|0\rangle = |1\rangle, \quad \sigma_x|1\rangle = |0\rangle, \quad \sigma_z|0\rangle = |0\rangle, \quad \sigma_z|1\rangle = -|1\rangle, \quad \sigma_y|0\rangle = i|1\rangle, \quad \sigma_y|1\rangle = -i|0\rangle. \quad (3.10)$$

Vamos supor que a medida inicial de Alice fosse $|\Phi^-\rangle$. Assim, o sistema iria colapsar para o estado $\alpha|0\rangle_3 - \beta|1\rangle_3$, e os bits clássicos enviados a Bob seriam 0 e 1, nesta ordem. Este, então, aplicaria a transformação unitária σ_z e recuperaria a informação original igual a $\alpha|0\rangle_3 + \beta|1\rangle_3$. Visto que é sempre possível corrigir estes estados para que a informação original seja recuperada, e Alice e Bob sabem como fazê-lo, o protocolo funcionará todas as vezes em que ambos desejarem transmitir uma informação quântica semelhante à Eq. (3.1). Logo, concluímos que o protocolo garante fidelidade e probabilidade iguais a um.

Antes de encerrar a descrição deste método, é importante ressaltar que todo o processo é condizente com as leis da física - mesmo sob o ponto de vista relativístico - e que o princípio da relatividade não é violado. Embora exista a hipótese de que o efeito da medida de uma partícula emaranhada seja instantaneamente transmitido ao seu par, Bob não sabe qual o resultado da medida de Alice até que esta o informe. Observe que

$$\rho_B = \text{Tr}_A \rho \quad (3.11)$$

onde A é o subsistema formado pelos *qubits* 1 e 2 e B é o estado associado ao *qubit* 3. Desse modo, considerando a Eq. (3.7), sabendo que $|\alpha|^2 + |\beta|^2 = 1$ e que os termos cruzados não contribuem para o cálculo do traço sobre ρ , ρ_B é igual a

$$\begin{aligned} \rho_3 &= {}_{1,2}\langle\Phi^+|\rho|\Phi^+\rangle_{1,2} + {}_{1,2}\langle\Phi^-|\rho|\Phi^-\rangle_{1,2} + {}_{1,2}\langle\Psi^+|\rho|\Psi^+\rangle_{1,2} + {}_{1,2}\langle\Psi^-|\rho|\Psi^-\rangle_{1,2} \\ &= \frac{1}{4} \{|\alpha|^2(|0\rangle_{33}\langle 0|) + |\beta|^2(|1\rangle_{33}\langle 1|)\} + \frac{1}{4} \{|\alpha|^2(|0\rangle_{33}\langle 0|) + |\beta|^2(|1\rangle_{33}\langle 1|)\} \\ &\quad + \frac{1}{4} \{|\alpha|^2(|1\rangle_{33}\langle 1|) + |\beta|^2(|0\rangle_{33}\langle 0|)\} + \frac{1}{4} \{|\alpha|^2(|1\rangle_{33}\langle 1|) + |\beta|^2(|0\rangle_{33}\langle 0|)\} \\ &= \frac{1}{2}(|\alpha|^2 + |\beta|^2)(|0\rangle_{33}\langle 0|) + \frac{1}{2}(|\alpha|^2 + |\beta|^2)(|1\rangle_{33}\langle 1|) = \frac{1}{2}I. \end{aligned}$$

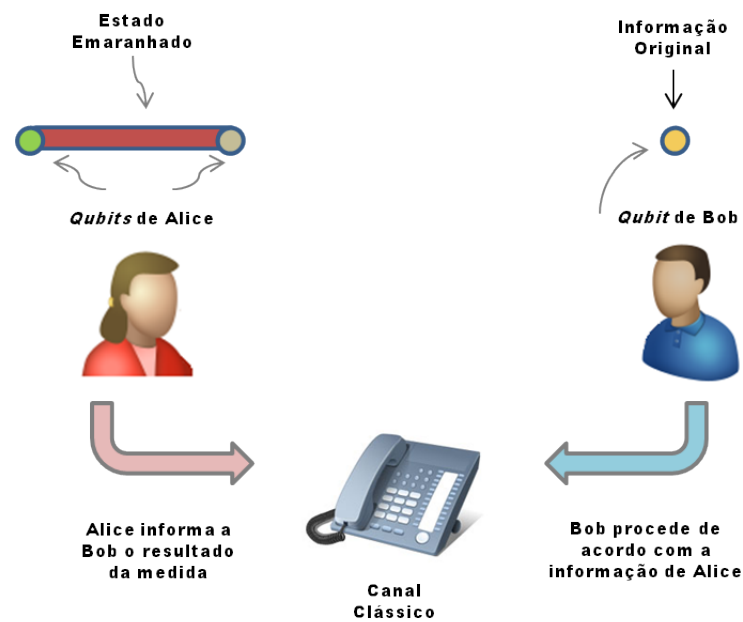


Figura 3.4: Procedimento padrão após Alice medir o sistema. Os dois qubits medidos são afetados e formam um estado emaranhado distinto do estado inicial que constituía o canal. Após a confirmação dos resultados das medidas de Alice através de um canal clássico, Bob sabe quais as transformações necessárias a serem aplicadas para que seu estado seja idêntico ao original enviado por Alice.

(3.12)

Assim, Bob não possui nenhuma pista sobre o resultado da medida de Alice até que os bits clássicos sejam enviados e o recebimento dos mesmos confirmado; e esta operação é feita através de um canal clássico. Dessa forma, até que todo o processo seja finalizado, concluímos que o tempo decorrido seria maior do que aquele que um feixe de luz gastaria atravessando a distância que separa Alice de Bob, não violando portanto o princípio da relatividade.

Capítulo 4

Canais Parcialmente Emaranhados

Para protocolos que utilizam canais parcialmente emaranhados, a probabilidade de sucesso ao fim do processo é menor do que um. Dessa forma, a eficiência destes métodos pode ser atribuída à probabilidade final para que a informação chegue a Bob em sua forma original (fidelidade um). Nesta seção, vamos apresentar três protocolos que buscam eficiência máxima, e, no final, faremos um comparativo entre os mesmos, destacando as vantagens e desvantagens de cada um.

4.1 Teleporte com Evolução Unitária

Este método apresenta uma ferramenta interessante descrita por uma matriz de correção que atua sobre a forma final do *qubit*, e foi primeiramente descrito por [Li et al., 2000](#). O artigo mostra ser possível teleportar um *qubit* através de um canal parcialmente emaranhado com uma determinada probabilidade, que dependerá do grau de emaranhamento do canal e do tipo de medida realizada. A forma geral do *qubit* continua sendo

$$|\phi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1, \quad (4.1)$$

e, novamente, Alice deseja teleportar o *qubit* para Bob. Entretanto, ao contrário do protocolo original, o canal utilizado para a transmissão do *qubit* não está maximamente emaranhado. Sua representação será

$$|\Phi_n^+\rangle_{2,3} = \frac{|00\rangle_{2,3} + n|11\rangle_{2,3}}{\sqrt{1+n^2}}, \quad (4.2)$$

onde $0 < n < 1$. Na forma mostrada acima, o emaranhamento pode aumentar continuamente desde $n = 0$ até $n = 1$. Para $n = 0$ não há emaranhamento e para $n = 1$ o canal está maximamente emaranhado. Qualquer outra configuração caracteriza um estado parcialmente emaranhado, como mostra a figura 4.2.

Prosseguindo com a descrição do procedimento, podemos escrever o estado

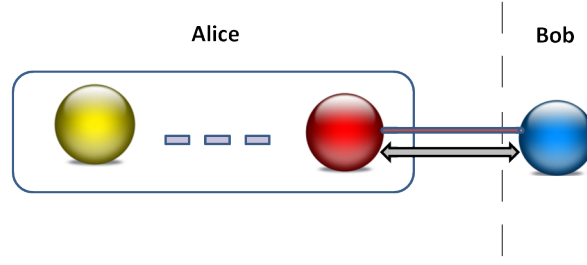


Figura 4.1: Teleporte de um qubit utilizando um canal maximamente emaranhado. A seta cinza indica que os qubits estão emaranhados.

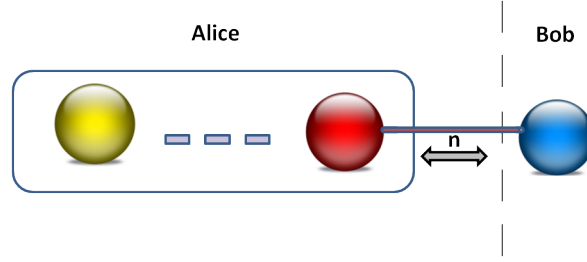


Figura 4.2: Teleporte de um qubit utilizando um canal parcialmente emaranhado. A seta cinza é menor do que na figura 4.1 e está associada ao índice n , para reforçar a idéia de que o emaranhamento é inferior ao de estados maximamente emaranhados.

geral do sistema, o *qubit* a ser teleportado e o canal como

$$|\phi\rangle_1 |\Phi_n^+\rangle_{2,3} = \frac{\alpha}{\sqrt{1+n^2}} |000\rangle_{1,2,3} + \frac{n\alpha}{\sqrt{1+n^2}} |011\rangle_{1,2,3} + \frac{\beta}{\sqrt{1+n^2}} |100\rangle_{1,2,3} + \frac{n\beta}{\sqrt{1+n^2}} |111\rangle_{1,2,3}. \quad (4.3)$$

O início deste protocolo será idêntico ao do protocolo original: Alice realiza uma medida de Bell e informa o resultado a Bob. Para que possamos ter uma melhor visualização dos resultados possíveis, vamos reescrever o estado geral do sistema em termos da base de Bell, usando a Eq. (3.5).

$$\begin{aligned} |\phi\rangle_1 |\Phi_n^+\rangle_{2,3} &= \frac{\alpha}{\sqrt{1+n^2}} \left(\frac{|\Phi^+\rangle_{1,2} + |\Phi^-\rangle_{1,2}}{\sqrt{2}} \right) |0\rangle_3 + \frac{n\alpha}{\sqrt{1+n^2}} \left(\frac{|\Psi^+\rangle_{1,2} + |\Psi^-\rangle_{1,2}}{\sqrt{2}} \right) |1\rangle_3 \\ &\quad + \frac{\beta}{\sqrt{1+n^2}} \left(\frac{|\Psi^+\rangle_{1,2} - |\Psi^-\rangle_{1,2}}{\sqrt{2}} \right) |0\rangle_3 + \frac{n\beta}{\sqrt{1+n^2}} \left(\frac{|\Phi^+\rangle_{1,2} - |\Phi^-\rangle_{1,2}}{\sqrt{2}} \right) |1\rangle_3 \\ &= |\Phi^+\rangle_{1,2} \sqrt{\frac{(\alpha)^2 + (n\beta)^2}{2(1+n^2)}} \left[\frac{\alpha|0\rangle_3 + n\beta|1\rangle_3}{\sqrt{(\alpha)^2 + (n\beta)^2}} \right] + |\Phi^-\rangle_{1,2} \sqrt{\frac{(\alpha)^2 + (n\beta)^2}{2(1+n^2)}} \left[\frac{\alpha|0\rangle_3 - n\beta|1\rangle_3}{\sqrt{(\alpha)^2 + (n\beta)^2}} \right] \\ &\quad + |\Psi^+\rangle_{1,2} \sqrt{\frac{(n\alpha)^2 + (\beta)^2}{2(1+n^2)}} \left[\frac{\beta|0\rangle_3 + n\alpha|1\rangle_3}{\sqrt{(n\alpha)^2 + (\beta)^2}} \right] + |\Psi^-\rangle_{1,2} \sqrt{\frac{(n\alpha)^2 + (\beta)^2}{2(1+n^2)}} \left[\frac{-\beta|0\rangle_3 + n\alpha|1\rangle_3}{\sqrt{(n\alpha)^2 + (\beta)^2}} \right]. \end{aligned} \quad (4.4)$$

Os estados mostrados na Eq. (4.4) foram ajustados de forma que apareçam normalizados.

Após a medida de Alice na base de Bell, o estado do *qubit* em posse de Bob ficará alterado, mas, como podemos observar na última equação, nenhum dos *qubits* será

recebido com fidelidade um. Os resultados possíveis (sem a respectiva normalização) serão

$$\alpha|0\rangle_3 + n\beta|1\rangle_3; \quad \alpha|0\rangle_3 - n\beta|1\rangle_3; \quad \beta|0\rangle_3 + n\alpha|1\rangle_3; \quad -\beta|0\rangle_3 + n\alpha|1\rangle_3. \quad (4.5)$$

Para obter o estado original na forma $\alpha|0\rangle_3 + \beta|1\rangle_3$ (ou qualquer um dos estados na Tabela 3.1, que estão apenas a uma diferença de fase em relação ao original) Bob recorre a uma nova estratégia: introduz um *qubit* auxiliar, $|0\rangle_{aux}$. Assim, o sistema possui um novo elemento, e os *qubits* de Bob na Eq. (4.5) passam a ser descritos por

$$\begin{aligned} &\alpha|0\rangle_3|0\rangle_{aux} + n\beta|1\rangle_3|0\rangle_{aux}; \quad \alpha|0\rangle_3|0\rangle_{aux} - n\beta|1\rangle_3|0\rangle_{aux}; \\ &\beta|0\rangle_3|0\rangle_{aux} + n\alpha|1\rangle_3|0\rangle_{aux}; \quad -\beta|0\rangle_3|0\rangle_{aux} + n\alpha|1\rangle_3|0\rangle_{aux}; \end{aligned} \quad (4.6)$$

Em seguida, Bob irá aplicar uma transformação unitária no seu sistema (formado pelo *qubit* teleportado e o *qubit* auxiliar) de acordo com o resultado obtido por Alice. Cada transformação é distinta e pode ser expressa por uma matriz. Se, por exemplo, o resultado fosse $|\Phi^+\rangle_{1,2}$, a matriz de evolução unitária teria a seguinte forma

$$U_{corr} = \begin{bmatrix} n & 0 & \sqrt{1-n^2} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ \sqrt{1-n^2} & 0 & -n & 0 \end{bmatrix},$$

onde usamos como base o conjunto de estados $\{|0\rangle_3|0\rangle_{aux}, |1\rangle_3|0\rangle_{aux}, |0\rangle_3|1\rangle_{aux}, |1\rangle_3|1\rangle_{aux}\}$ para descrevê-la.

Após a transformação sobre $(\alpha|0\rangle_3|0\rangle_{aux} + n\beta|1\rangle_3|0\rangle_{aux}) / \sqrt{(\alpha^2) + (n\beta)^2}$, o sistema pode ser expresso por

$$U_{corr} \left(\frac{\alpha|0\rangle_3|0\rangle_{aux} + n\beta|1\rangle_3|0\rangle_{aux}}{\sqrt{(\alpha^2) + (n\beta)^2}} \right) = \frac{n}{\sqrt{(\alpha^2) + (n\beta)^2}} (\alpha|0\rangle_3 + \beta|1\rangle_3) |0\rangle_{aux} + \sqrt{\frac{1-n^2}{(\alpha^2) + (n\beta)^2}} \alpha|1\rangle_3 |1\rangle_{aux}. \quad (4.7)$$

Ao medir o *qubit* auxiliar, os possíveis resultados serão $|0\rangle_{aux}$ e $|1\rangle_{aux}$. No nosso exemplo, se o resultado fosse $|0\rangle_{aux}$, o *qubit* original seria recebido com fidelidade um.

Para calcular a probabilidade relacionada a este processo, precisamos analisar duas etapas. A probabilidade de se obter $|0\rangle_{aux}$ na Eq. (4.7) após a correção pela matriz é

$$\left| \frac{n}{\sqrt{(\alpha^2) + (n\beta)^2}} \right|^2, \quad (4.8)$$

segundo nossa análise após a Eq. (3.8). Porém, antes desta correção, existe a probabilidade associada ao resultado das medidas nas bases generalizadas. Como pode ser visto na Eq.

(4.4), a probabilidade de se obter $|\Phi^+\rangle_{1,2}$ é

$$\left| \sqrt{\frac{(\alpha)^2 + (n\beta)^2}{2(1+n^2)}} \right|^2. \quad (4.9)$$

Logo, a probabilidade de se obter $|\Phi^+\rangle_{1,2}$ e $|0\rangle_{aux}$ nesta ordem é

$$\left| \sqrt{\frac{(\alpha)^2 + (n\beta)^2}{2(1+n^2)}} \right|^2 \times \left| \frac{n}{\sqrt{(\alpha)^2 + (n\beta)^2}} \right|^2 = \frac{n^2}{2(1+n^2)}. \quad (4.10)$$

Se o resultado da medida final revelasse $|1\rangle_{aux}$, o *qubit* seria destruído e a informação estaria perdida.

Para cada uma das configurações, a probabilidade de se obter o *qubit* original após as medidas nas bases generalizadas e do *qubit* auxiliar é a mesma encontrada na Eq. (4.10). Como existem quatro possibilidades para as medidas nas bases generalizadas, a probabilidade total de sucesso é calculada somando-se as quatro probabilidades parciais,

$$P_{suc} = 4 \times \frac{n^2}{2(1+n^2)} = \frac{2n^2}{1+n^2}. \quad (4.11)$$

Este importante resultado representa a maior eficiência possível para teleportes probabilísticos que operam com transmissão serial de informação quântica, (Vidal, 1999) e aparecerá novamente em outros protocolos. É necessário frisar que o resultado é válido apenas para os casos em que Bob possui acesso a todos os canais envolvidos no processo.

4.2 Teleporte com Base de Bell Generalizada

Neste método, apresentado em Agrawal and Pati, 2002, as estruturas do *qubit* que será transmitido e do canal utilizado são iguais às do protocolo visto na seção 4.1, Eqs. (4.1) e (4.2). Porém, desta vez, Bob não irá utilizar um *qubit* auxiliar seguido de uma evolução unitária, e Alice não mais projetará seus *qubits* com medida na base de Bell. Ela realizará um outro tipo de medida projetiva, a qual pode ser vista como uma generalização de medida na base de Bell. Estes estados de Bell generalizados são vetores ortonormais de estrutura semelhante ao canal que transmitirá a informação do *qubit*,

$$|\Phi_m^+\rangle = \frac{|00\rangle + m|11\rangle}{\sqrt{1+m^2}}, \quad |\Phi_m^-\rangle = \frac{m|00\rangle - |11\rangle}{\sqrt{1+m^2}}, \quad |\Psi_m^+\rangle = \frac{|01\rangle + m|10\rangle}{\sqrt{1+m^2}}, \quad |\Psi_m^-\rangle = \frac{m|01\rangle - |10\rangle}{\sqrt{1+m^2}}, \quad (4.12)$$

onde $0 < m < 1$.

Como já vimos, o estado geral do sistema pode ser expresso por

$$|\phi\rangle_1|\Phi_n^+\rangle_{2,3} = \frac{\alpha}{\sqrt{1+n^2}}|000\rangle_{1,2,3} + \frac{\alpha n}{\sqrt{1+n^2}}|011\rangle_{1,2,3} + \frac{\beta}{\sqrt{1+n^2}}|100\rangle_{1,2,3} + \frac{\beta n}{\sqrt{1+n^2}}|111\rangle_{1,2,3}. \quad (4.13)$$

Agora, podemos reescrever a base computacional e o estado geral do sistema em função dos estados da base generalizada. Para a base computacional, as expressões são:

$$\begin{aligned} |00\rangle &= \frac{|\Phi_m^+\rangle + m|\Phi_m^-\rangle}{\sqrt{1+m^2}}, & |01\rangle &= \frac{|\Psi_m^+\rangle + m|\Psi_m^-\rangle}{\sqrt{1+m^2}}, \\ |10\rangle &= \frac{m|\Psi_m^+\rangle - |\Psi_m^-\rangle}{\sqrt{1+m^2}}, & |11\rangle &= \frac{m|\Phi_m^+\rangle - |\Phi_m^-\rangle}{\sqrt{1+m^2}}; \end{aligned} \quad (4.14)$$

e, para o estado geral do sistema, $|\phi\rangle_1|\Phi_n^+\rangle_{2,3}$ torna-se

$$\begin{aligned} |\phi\rangle_1|\Phi_n^+\rangle_{2,3} &= \frac{\alpha}{\sqrt{1+n^2}} \left(\frac{|\Phi_m^+\rangle + m|\Phi_m^-\rangle}{\sqrt{1+m^2}} \right) |0\rangle_3 + \frac{n\alpha}{\sqrt{1+n^2}} \left(\frac{|\Psi_m^+\rangle + m|\Psi_m^-\rangle}{\sqrt{1+m^2}} \right) |1\rangle_3 \\ &\quad + \frac{\beta}{\sqrt{1+n^2}} \left(\frac{m|\Psi_m^+\rangle - |\Psi_m^-\rangle}{\sqrt{1+m^2}} \right) |0\rangle_3 + \frac{n\beta}{\sqrt{1+n^2}} \left(\frac{m|\Phi_m^+\rangle - |\Phi_m^-\rangle}{\sqrt{1+m^2}} \right) |1\rangle_3 \\ &= |\Phi_m^+\rangle_{1,2} \sqrt{\frac{(\alpha)^2 + (mn\beta)^2}{(1+m^2)(1+n^2)}} \left[\frac{\alpha|0\rangle_3 + mn\beta|1\rangle_3}{\sqrt{(\alpha)^2 + (mn\beta)^2}} \right] + |\Phi_m^-\rangle_{1,2} \sqrt{\frac{(m\alpha)^2 + (n\beta)^2}{(1+m^2)(1+n^2)}} \left[\frac{m\alpha|0\rangle_3 - n\beta|1\rangle_3}{\sqrt{(m\alpha)^2 + (n\beta)^2}} \right] \\ &\quad + |\Psi_m^+\rangle_{1,2} \sqrt{\frac{(n\alpha)^2 + (m\beta)^2}{(1+m^2)(1+n^2)}} \left[\frac{m\beta|0\rangle_3 + n\alpha|1\rangle_3}{\sqrt{(n\alpha)^2 + (m\beta)^2}} \right] + |\Psi_m^-\rangle_{1,2} \sqrt{\frac{(mn\alpha)^2 + (\beta)^2}{(1+m^2)(1+n^2)}} \left[\frac{\beta|0\rangle_3 - mn\alpha|1\rangle_3}{\sqrt{(mn\alpha)^2 + (\beta)^2}} \right]. \end{aligned} \quad (4.15)$$

Se olharmos atentamente, podemos notar que para $m = n$ o sistema passa a ser descrito por

$$\begin{aligned} |\phi\rangle_1|\Phi_n^+\rangle_{2,3} &= |\Phi_m^+\rangle_{1,2} \frac{\sqrt{(\alpha)^2 + (n^2\beta)^2}}{1+n^2} \left[\frac{\alpha|0\rangle_3 + n^2\beta|1\rangle_3}{\sqrt{(\alpha)^2 + (n^2\beta)^2}} \right] + |\Phi_m^-\rangle_{1,2} \frac{n}{1+n^2} [\alpha|0\rangle_3 - \beta|1\rangle_3] + \\ &\quad + |\Psi_m^+\rangle_{1,2} \frac{n}{1+n^2} [\beta|0\rangle_3 + \alpha|1\rangle_3] + |\Psi_m^-\rangle_{1,2} \frac{\sqrt{(n^2\alpha)^2 + (\beta)^2}}{1+n^2} \left[\frac{\beta|0\rangle_3 - n^2\alpha|1\rangle_3}{\sqrt{(n^2\alpha)^2 + (\beta)^2}} \right]. \end{aligned} \quad (4.16)$$

Assim, supondo que Alice meça seus estados na base generalizada e imponha a condição $m = n$, teremos as seguintes possibilidades: se os resultados forem $|\Phi_m^-\rangle_{1,2}$ ou $|\Psi_m^+\rangle_{1,2}$, basta que Bob aplique a transformação unitária adequada (σ_z ou σ_x , respectivamente) e o *qubit* será recebido com fidelidade um. Se, por outro lado, as medidas de Alice revelarem $|\Phi_m^+\rangle_{1,2}$ e $|\Psi_m^-\rangle_{1,2}$, Bob não receberá com perfeição o estado inicial $|\phi\rangle_1$ do *qubit* e o protocolo terá falhado. Para qualquer outra hipótese ($m \neq n$), não há possibilidade de que $|\phi\rangle_1$ seja recebido com fidelidade um.

Dessa forma, a probabilidade total de sucesso pode ser calculada considerando-se apenas os coeficientes associados a cada estado na Eq. (4.29). Para as duas primeiras possibilidades, a probabilidade de sucesso tanto para $|\Phi_m^-\rangle_{1,2}$ como para $|\Psi_m^+\rangle_{1,2}$ é

$$P_{|\Phi_m^-\rangle} = P_{|\Psi_m^+\rangle} = \frac{n^2}{(1+n^2)^2}. \quad (4.17)$$

Somando-se estes dois valores, a probabilidade total de sucesso é igual a

$$P_{suc} = P_{|\Phi_m^-\rangle} + P_{|\Psi_m^+\rangle} = \frac{2n^2}{(1+n^2)^2}. \quad (4.18)$$

Para finalizar o protocolo, basta que Alice e Bob se comuniquem através de um canal clássico e confirmam o resultado das medidas. Em caso de sucesso, como dito anteriormente, Bob aplica as transformações unitárias corretas, e, em caso de falha, o protocolo deve ser repetido até que alguma das medidas revele $|\Phi_m^-\rangle$ ou $|\Psi_m^+\rangle$.

Se observarmos a expressão final para a probabilidade total na Eq. (4.18), deduziremos que o valor de P_{suc} pertence ao intervalo $0 < P_{suc} < 0,5$. Se não houvesse emaranhamento ($n = 0$), teríamos $P_{suc} = 0$. Para $n = 1$, deveríamos obter $P_{suc} = 1$, pois voltaríamos ao caso analisado na seção 3.1 em que o canal seria um estado da base de Bell. Porém, como estamos desconsiderando as medidas de $|\Phi_m^-\rangle$ e $|\Psi_m^+\rangle$, manteremos sempre $n < 1$. Assim, de acordo com a Eq. (4.18), o máximo valor que P_{suc} atinge neste protocolo para $n \simeq 1$ é 0,5.

Podem ser considerados outros valores para m que sejam diferentes de n . Nestas condições, entretanto, não conseguiremos obter o *qubit* de Bob como sendo $\alpha|0\rangle + \beta|1\rangle$. Sempre teremos nestes casos ou α e/ou β multiplicados por m ou n . Quando a condição $m = n$ é atingida, denominamos esta configuração de *matching*; ou seja, um casamento entre o grau de emaranhamento da base de medida (m) e do canal (n). Antes de encerrar este método, é importante ressaltar que o resultado encontrado para P_{suc} é parecido com o do protocolo com correção via evolução unitária, diferindo deste último apenas por um fator $(1+n^2)$ no denominador. Como $1+n^2 > 1$, a Eq. (4.11) representa o melhor resultado obtido até agora.

4.3 Teleporte Múltiplo com Fidelidade Um

Todos os artigos que mostramos até agora apresentavam apenas um método para teleportar o *qubit* inicial com fidelidade um. Nesta seção, vamos analisar o artigo [Rigolin, 2009](#) no qual são propostos três protocolos distintos que possuem uma característica em comum: a utilização de canais em série para teleportar o *qubit* mais de uma vez. Estes protocolos representam uma generalização de outro método ([Modławska and Grudka, 2008](#)) contido na referência deste mesmo artigo. Cada vez que o resultado da medida

em uma base específica (seja na base de Bell ou na base generalizada) não permitir que seja possível acessar o *qubit* em sua forma original, um novo teleporte é realizado. Assim, surgirão novas possibilidades de medidas, e, para algumas destas, será possível obter com uma certa probabilidade o *qubit* com fidelidade um. Esta idéia representa um avanço em relação aos protocolos anteriores, nos quais Alice abandonava a operação quando o resultado de uma das medidas não era o esperado. Para fins de clareza, omitiremos a normalização dos estados quando julgarmos necessário. Prosseguiremos então à descrição do primeiro dos três novos protocolos:

4.3.1 Protocolo 1

O primeiro protocolo é baseado no método apresentado na seção 4.1. A base de medida será somente a base de Bell ($m = 1$) e o canal será idêntico ao da Eq. (4.2). Após a etapa inicial, nenhuma das medidas consegue fornecer o *qubit* em sua forma original. Restava a Alice apenas abandonar esta tentativa e reiniciar o processo com outro *qubit* preparado de forma idêntica. Entretanto, se desta vez Bob realizar um novo teleporte sobre qualquer um dos possíveis resultados finais para o *qubit*, através de um canal do tipo

$$|\Phi_n^+\rangle_{2,3} = \frac{|00\rangle_{2,3} + n|11\rangle_{2,3}}{\sqrt{1+n^2}}, \quad (4.19)$$

onde $0 < n < 1$, surgirão novas configurações e possibilidades para que o *qubit* original alcance fidelidade um. Para simplificar as equações, vamos evitar apresentar os estados em sua forma normalizada e já, quando for o caso, com a transformação unitária σ_z implementada. Isto representa apenas uma mudança de fase em relação ao estado real do *qubit* e não altera a probabilidade de o mesmo ser acessado. De acordo com a Eq. (4.4), o estado inicial em que o sistema se encontrava após o primeiro teleporte era:

$$\begin{aligned} & \frac{1}{\sqrt{2(1+n^2)}} |\Phi^+\rangle [\alpha|0\rangle + n\beta|1\rangle] + \frac{1}{\sqrt{2(1+n^2)}} |\Phi^-\rangle [\alpha|0\rangle + n\beta|1\rangle] + \\ + & \frac{1}{\sqrt{2(1+n^2)}} |\Psi^+\rangle [\beta|0\rangle + n\alpha|1\rangle] + \frac{1}{\sqrt{2(1+n^2)}} |\Psi^-\rangle [\beta|0\rangle + n\alpha|1\rangle]. \end{aligned} \quad (4.20)$$

A figura 4.3 mostra como é a disposição dos canais. Alice mantém a posse de um *qubit* do primeiro canal, enquanto Bob tem acesso ao outro *qubit* e aos canais restantes. Se Bob efetuar um novo teleporte sobre qualquer um destes estados ($\alpha|0\rangle + n\beta|1\rangle$ ou $\beta|0\rangle + n\alpha|1\rangle$), obterá quatro novos possíveis resultados, dentre os quais estarão $\alpha|0\rangle + \beta|1\rangle$ ou $\alpha|1\rangle + \beta|0\rangle$. O estado do sistema após o segundo teleporte para cada uma das quatro medidas possíveis na primeira etapa pode ser conferido nas expressões a seguir:

Após a medida de $|\Phi^+\rangle$:

$$\frac{1}{2(1+n^2)} |\Phi^+\rangle [\alpha|0\rangle + n^2\beta|1\rangle] + \frac{1}{2(1+n^2)} |\Phi^-\rangle [\alpha|0\rangle + n^2\beta|1\rangle]$$

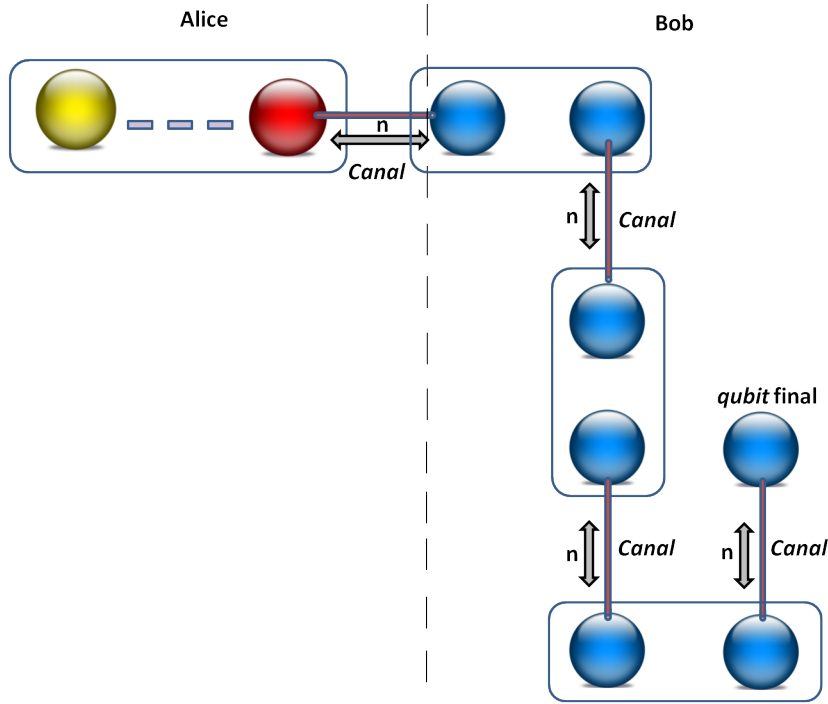


Figura 4.3: Disposição dos canais em série entre Alice e Bob. Neste modelo, Alice possui apenas o primeiro canal e Bob tem acesso a todos os outros e ao último qubit.

$$+ \frac{n}{2(1+n^2)} |\Psi^+\rangle [\beta|0\rangle + \alpha|1\rangle] + \frac{n}{2(1+n^2)} |\Psi^-\rangle [\beta|0\rangle + \alpha|1\rangle]. \quad (4.21)$$

Após a medida de $|\Phi^-\rangle$:

$$\begin{aligned} & \frac{1}{2(1+n^2)} |\Phi^+\rangle [\alpha|0\rangle + n^2\beta|1\rangle] + \frac{1}{2(1+n^2)} |\Phi^-\rangle [\alpha|0\rangle + n^2\beta|1\rangle] \\ + & \frac{n}{2(1+n^2)} |\Psi^+\rangle [\beta|0\rangle + \alpha|1\rangle] + \frac{n}{2(1+n^2)} |\Psi^-\rangle [\beta|0\rangle + \alpha|1\rangle]. \end{aligned} \quad (4.22)$$

Após a medida de $|\Psi^+\rangle$:

$$\begin{aligned} & \frac{n}{2(1+n^2)} |\Phi^+\rangle [\alpha|0\rangle + \beta|1\rangle] + \frac{n}{2(1+n^2)} |\Phi^-\rangle [\alpha|0\rangle + \beta|1\rangle] \\ + & \frac{1}{2(1+n^2)} |\Psi^+\rangle [\beta|0\rangle + n^2\alpha|1\rangle] + \frac{1}{2(1+n^2)} |\Psi^-\rangle [\beta|0\rangle + n^2\alpha|1\rangle]. \end{aligned} \quad (4.23)$$

Após a medida de $|\Psi^-\rangle$:

$$\begin{aligned} & \frac{n}{2(1+n^2)} |\Phi^+\rangle [\alpha|0\rangle + \beta|1\rangle] + \frac{n}{2(1+n^2)} |\Phi^-\rangle [\alpha|0\rangle + \beta|1\rangle] \\ + & \frac{1}{2(1+n^2)} |\Psi^+\rangle [\beta|0\rangle + n^2\alpha|1\rangle] + \frac{1}{2(1+n^2)} |\Psi^-\rangle [\beta|0\rangle + n^2\alpha|1\rangle]. \end{aligned} \quad (4.24)$$

Com isso, ao medir o sistema após o segundo teleporte, Alice e Bob podem ter êxito no procedimento se obtiverem como resultado de suas medidas qualquer uma

das seguintes seqüências: $|\Phi^+\rangle|\Psi^+\rangle$, $|\Phi^+\rangle|\Psi^-\rangle$, $|\Phi^-\rangle|\Psi^+\rangle$, $|\Phi^-\rangle|\Psi^-\rangle$, $|\Psi^+\rangle|\Phi^+\rangle$, $|\Psi^+\rangle|\Phi^-\rangle$, $|\Psi^-\rangle|\Phi^+\rangle$, $|\Psi^-\rangle|\Phi^-\rangle$. É fácil verificar que a probabilidade de sucesso para cada caso é

$$\begin{aligned} P_{|\Phi^+\rangle|\Psi^+\rangle} &= P_{|\Phi^+\rangle|\Psi^-\rangle} = P_{|\Phi^-\rangle|\Psi^+\rangle} = P_{|\Phi^-\rangle|\Psi^-\rangle} = P_{|\Psi^+\rangle|\Phi^+\rangle} \\ &= P_{|\Psi^+\rangle|\Phi^-\rangle} = P_{|\Psi^-\rangle|\Phi^+\rangle} = P_{|\Psi^-\rangle|\Phi^-\rangle} = \frac{n^2}{4(1+n^2)^2}, \end{aligned} \quad (4.25)$$

e, assim, a probabilidade total de sucesso após o segundo teleporte é

$$P_{suc}^{(2)} = 8 \times \frac{n^2}{4(1+n^2)} = \frac{2n^2}{(1+n^2)^2}. \quad (4.26)$$

Repare que este resultado é o mesmo encontrado no final da seção 4.2.

Vimos que para o primeiro teleporte não há nenhum caso bem-sucedido de imediato, mas na etapa seguinte encontramos várias opções em que o estado original é transmitido com fidelidade um. Isso ocorre devido à relação entre o canal $|\Phi_n^+\rangle_{2,3}$ e a estrutura algébrica de cada um dos estados da base, gerando um padrão que nos permite associar o estado final de Bob com o resultado das sucessivas medidas na base de Bell. Para resultados iguais a $|\Phi^+\rangle_{1,2}$ e $|\Phi^-\rangle_{1,2}$ o coeficiente β do *qubit* de Bob é multiplicado por n , e para $|\Psi^+\rangle_{1,2}$ e $|\Psi^-\rangle_{1,2}$ o mesmo ocorre com α . Como só havia estados nas formas $\alpha|0\rangle_3 + n\beta|1\rangle_3$ e $\beta|0\rangle_3 + n\alpha|1\rangle_3$ em proporções iguais após o fim da primeira etapa, a medida de $|\Psi^+\rangle$ ou $|\Psi^-\rangle$ na primeira etapa e a de $|\Phi^+\rangle$ ou $|\Phi^-\rangle$ na segunda faz com que metade dos casos na etapa seguinte assumam a forma $n\alpha|0\rangle_3 + n\beta|1\rangle_3$ (já incluindo a ação de σ_x). Os estados restantes ficam divididos em partes iguais nas formas $\alpha|0\rangle_3 + n^2\beta|1\rangle_3$ e $\beta|0\rangle_3 + n^2\alpha|1\rangle_3$.

Seguindo esta lógica, nunca transmitiremos $\alpha|0\rangle_3 + \beta|1\rangle_3$ em um número ímpar de tentativas, mas sempre teremos sucesso para um número par de teleportes. Podemos ainda estabelecer uma regra geral para a probabilidade total em uma etapa q , sendo q um inteiro par. Como precisamos obter o mesmo número de combinações entre $|\Phi^\pm\rangle$ e $|\Psi^\pm\rangle$ após as medidas, $\alpha|0\rangle_3 + \beta|1\rangle_3$ será proporcional a $n^{\frac{q}{2}}$. Além disso, a cada nova etapa todos os estados são multiplicados por um fator igual a $1/\sqrt{2(1+n^2)}$, e, dessa forma, um estado na q -ésima etapa seria proporcional a $1/\sqrt{2^q(1+n^2)^q}$. Logo, a probabilidade total será proporcional a $n^q/2^q(1+n^2)^q$. A expressão correta para este resultado é (Rigolin, 2009)

$$P_{suc}^{(q)} = \frac{A(q)n^q}{2^q(1+n^2)^q}, \quad (4.27)$$

onde $A(q)$ é o número total de combinações possíveis para valores pares de q em que $|\Phi^\pm\rangle$ e $|\Psi^\pm\rangle$ ocorrem em igual número ($A(q) = 0$ quando q for ímpar). É importante ressaltar que nessa expressão só são consideradas as possibilidades em que não houve sucesso em etapas anteriores a q , pois, se este fosse o caso, já alcançaríamos nosso objetivo em uma

etapa prévia e não haveria sentido em realizar um novo teleporte.

Por outro lado, podemos calcular a probabilidade total de sucesso até uma determinada etapa q levando em conta todas as probabilidades individuais para etapas anteriores a q e somando-as, incluindo a última. Com isso, queremos um cenário em que seja possível transmitir o *qubit* original em até q etapas, sem excluir as possibilidades em que o objetivo é alcançado em alguma etapa anterior, ou seja

$$P_{suc}^{total} = \sum_{j=1}^q P_{suc}^{(j)}. \quad (4.28)$$

Foram efetuados cálculos para valores de q entre 1 e 12. A figura 4.4 mostra o comportamento de P_{suc}^{total} para estes parâmetros em função do grau de emaranhamento do canal, onde os valores para $A(q)$ até a etapa 12 são: $A(2) = 8$, $A(4) = 32$, $A(6) = 256$, $A(8) = 2560$, $A(10) = 28672$ e $A(12) = 344064$.

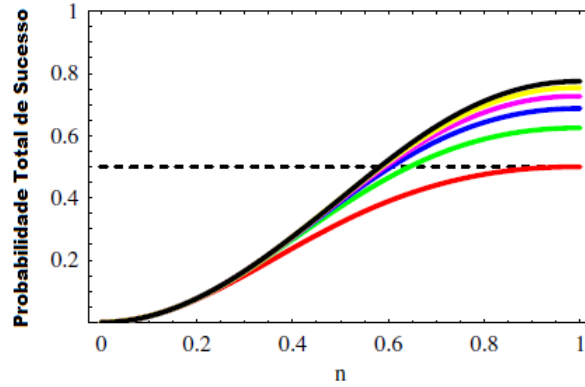


Figura 4.4: Para o protocolo 1: Do nível inferior até o topo, as curvas representam P_{suc}^{total} após $q= 2, 4, 6, 8, 10$ e 12 teleportes sucessivos. A linha tracejada mostra a probabilidade ótima ($1/2$) usando o protocolo apresentado na seção 4.2. Todas as grandezas são adimensionais.

Fonte: Figura adaptada de *Rigolin, 2009*.

Ao analisar atentamente o gráfico da figura 4.4, notamos que há dois pontos que precisam ser ressaltados. De imediato, podemos observar que a curva passa a ser estável para valores acima de $q = 10$, o que nos leva a concluir que novos teleportes acima deste valor não farão com que a eficiência do protocolo aumente. A segunda observação é referente ao fato de que, mesmo para altos valores de n , a probabilidade total de sucesso não chega a um, pois estamos sempre descartando resultados em que o número das combinações envolvendo $|\Phi^\pm\rangle$ e $|\Psi^\pm\rangle$ é distinto. Nos protocolos seguintes veremos como aperfeiçoar este método.

4.3.2 Protocolo 2

Passemos agora para o segundo protocolo. Assim como o Protocolo 1, que foi caracterizado como uma extensão de um método anterior (visto na seção 4.1), este

pode ser classificado como extensão do procedimento apresentado na seção 4.2. Neste procedimento, os resultados desejados ocorriam quando Alice obtinha $|\Phi_m^-\rangle$ ou $|\Psi_m^+\rangle$ após a primeira medida do sistema. Para $|\Phi_m^+\rangle$ ou $|\Psi_m^-\rangle$, o protocolo era interrompido e o processo poderia ser classificado como falho. No método que vamos descrever a seguir, o processo continua após a primeira medida, e Bob faz um novo teleporte utilizando uma base e um canal semelhantes aos da seção 4.2, sempre ajustando-os para a condição de *matching* ($m = n$). Recordemos que, após a primeira etapa, o estado geral do sistema era igual a

$$\begin{aligned} |\phi\rangle_1 |\Phi_n^+\rangle_{2,3} = & |\Phi_m^+\rangle_{1,2} \frac{\sqrt{(\alpha)^2 + (n^2\beta)^2}}{1+n^2} \left[\frac{\alpha|0\rangle_3 + n^2\beta|1\rangle_3}{\sqrt{(\alpha)^2 + (n^2\beta)^2}} \right] + |\Phi_m^-\rangle_{1,2} \frac{n}{1+n^2} [\alpha|0\rangle_3 - \beta|1\rangle_3] \\ & + |\Psi_m^+\rangle_{1,2} \frac{n}{1+n^2} [\beta|0\rangle_3 + \alpha|1\rangle_3] + |\Psi_m^-\rangle_{1,2} \frac{\sqrt{(n^2\alpha)^2 + (\beta)^2}}{1+n^2} \left[\frac{\beta|0\rangle_3 - n^2\alpha|1\rangle_3}{\sqrt{(n^2\alpha)^2 + (\beta)^2}} \right]. \end{aligned} \quad (4.29)$$

É interessante notar na expressão (4.29) a influência que cada estado da base de medida possui sobre a estrutura final do *qubit* 3 de Bob. A fidelidade máxima em relação ao *qubit* inicial ocorre se os resultados das medidas forem $|\Phi_m^-\rangle$ ou $|\Psi_m^+\rangle$. Para $|\Phi_m^+\rangle$ e $|\Psi_m^-\rangle$, entretanto, os coeficientes β e α ganham, respectivamente, um fator n^2 multiplicando-os. Assim, se for realizado um segundo teleporte, os casos bem-sucedidos serão aqueles em que os estados se "compensarão", e tanto α quanto β terão adquirido um fator multiplicativo igual a n^2 . Se utilizarmos uma seqüência de canais semelhantes à da figura 4.3 para este modelo, podemos afirmar que as combinações desejadas ocorrerão para as medidas de $|\Phi_m^+\rangle|\Psi_m^-\rangle$ e $|\Psi_m^-\rangle|\Phi_m^+\rangle$, e ainda prever o que acontece após o segundo teleporte para calcular as novas probabilidades de sucesso. Cada um destes estados terá um coeficiente proporcional a $\frac{1}{1+n^2} \times \frac{1}{1+n^2} = \left(\frac{1}{1+n^2}\right)^2$, e sua estrutura será igual a

$$\frac{n^2}{(1+n^2)^2} |\Phi_m^+\rangle|\Psi_m^-\rangle [\alpha|0\rangle + \beta|1\rangle] \text{ e } \frac{n^2}{(1+n^2)^2} |\Psi_m^-\rangle|\Phi_m^+\rangle [\alpha|0\rangle + \beta|1\rangle], \quad (4.30)$$

após as devidas correções com as matrizes de Pauli. A probabilidade de sucesso para cada caso é

$$P_{|\Phi_m^+\rangle|\Psi_m^-\rangle} = P_{|\Psi_m^-\rangle|\Phi_m^+\rangle} = \frac{n^4}{(1+n^2)^4}, \quad (4.31)$$

e a probabilidade de sucesso total após o segundo teleporte é

$$P_{suc}^{(2)} = P_{|\Phi_m^+\rangle|\Psi_m^-\rangle} + P_{|\Psi_m^-\rangle|\Phi_m^+\rangle} = \frac{2n^4}{(1+n^2)^4}. \quad (4.32)$$

Se houver falha, podemos prosseguir com os cálculos até a terceira etapa. A tabela 4.1 mostra a estrutura final dos *qubits* para os resultados que não obtiveram

Estrutura do <i>Qubit</i>	Estados Associados
$\alpha 0\rangle_3 + n^4\beta 1\rangle_3$	$ \Phi_m^+\rangle \Phi_m^+\rangle$
$\alpha 0\rangle_3 + n^2\beta 1\rangle_3$	$ \Phi_m^+\rangle \Phi_m^-\rangle, \Phi_m^+\rangle \Psi_m^+\rangle$
$n^2\alpha 0\rangle_3 + \beta 1\rangle_3$	$ \Psi_m^-\rangle \Phi_m^-\rangle, \Psi_m^-\rangle \Psi_m^+\rangle$
$n^4\alpha 0\rangle_3 + \beta 1\rangle_3$	$ \Psi_m^-\rangle \Psi_m^-\rangle$

Tabela 4.1: Estrutura final dos qubits que não alcançaram fidelidade um após o segundo teleporte e os respectivos resultados das medidas associadas.

Estrutura do <i>Qubit</i>	Estados Associados
$\alpha 0\rangle_3 + n^6\beta 1\rangle_3$	$ \Phi_m^+\rangle \Phi_m^+\rangle \Phi_m^+\rangle$
$\alpha 0\rangle_3 + n^4\beta 1\rangle_3$	$ \Phi_m^+\rangle \Phi_m^+\rangle \Phi_m^-\rangle, \Phi_m^+\rangle \Phi_m^+\rangle \Psi_m^+\rangle, \Phi_m^+\rangle \Phi_m^-\rangle \Phi_m^+\rangle, \Phi_m^+\rangle \Psi_m^+\rangle \Phi_m^+\rangle$
$n^2(\alpha 0\rangle_3 + n^2\beta 1\rangle_3)$	$ \Phi_m^+\rangle \Phi_m^+\rangle \Psi_m^-\rangle, \Phi_m^+\rangle \Phi_m^-\rangle \Phi_m^-\rangle, \Phi_m^+\rangle \Phi_m^-\rangle \Psi_m^+\rangle, \Phi_m^+\rangle \Psi_m^+\rangle \Psi_m^-\rangle, \Phi_m^+\rangle \Psi_m^+\rangle \Psi_m^+\rangle$
$n^2(n^2\alpha 0\rangle_3 + \beta 1\rangle_3)$	$ \Psi_m^-\rangle \Phi_m^-\rangle \Phi_m^-\rangle, \Psi_m^-\rangle \Phi_m^-\rangle \Psi_m^+\rangle, \Psi_m^-\rangle \Psi_m^+\rangle \Phi_m^-\rangle, \Psi_m^-\rangle \Psi_m^+\rangle \Psi_m^+\rangle, \Psi_m^-\rangle \Psi_m^-\rangle \Phi_m^+\rangle$
$n^4\alpha 0\rangle_3 + \beta 1\rangle_3$	$ \Psi_m^-\rangle \Phi_m^-\rangle \Psi_m^-\rangle, \Psi_m^-\rangle \Psi_m^+\rangle \Psi_m^-\rangle, \Psi_m^-\rangle \Psi_m^-\rangle \Phi_m^-\rangle, \Psi_m^-\rangle \Psi_m^-\rangle \Psi_m^+\rangle$
$n^6\alpha 0\rangle_3 + \beta 1\rangle_3$	$ \Psi_m^-\rangle \Psi_m^-\rangle \Psi_m^-\rangle$

Tabela 4.2: Estrutura final dos qubits que não alcançaram fidelidade um após o terceiro teleporte e as respectivas seqüências das medidas associadas.

fidelidade um após o segundo teleporte. Os seis estados mostrados na tabela 4.1 dão origem a 24 novos estados para um novo teleporte. Para que Bob consiga finalizar o protocolo na terceira etapa, alguma das seqüências de medidas abaixo deve ser obtida:

$$|\Phi_m^+\rangle|\Phi_m^-\rangle|\Psi_m^-\rangle, |\Phi_m^+\rangle|\Psi_m^+\rangle|\Psi_m^-\rangle, |\Psi_m^-\rangle|\Phi_m^-\rangle|\Psi_m^+\rangle, |\Psi_m^-\rangle|\Psi_m^+\rangle|\Phi_m^+\rangle, \quad (4.33)$$

lembrando que a presença de $|\Phi_m^-\rangle$ ou $|\Psi_m^+\rangle$ na segunda etapa não interfere na estrutura do *qubit* recebido após o primeiro teleporte (pois tanto α quanto β são multiplicados por n). Assim, levando em conta os quatro casos acima, a probabilidade total de sucesso após o terceiro teleporte será

$$P_{suc}^{(3)} = 4 \times \left| \frac{n^2}{(1+n^2)^2} \times \frac{n}{(1+n^2)} \right|^2 = 4 \times \left| \frac{(n)^3}{(1+n^2)^3} \right|^2 = \frac{4n^6}{(1+n^2)^6}, \quad (4.34)$$

e na tabela 4.2 listamos os 20 estados associados às falhas após o terceiro teleporte.

Para a quarta etapa, as 10 combinações que resultam em sucesso (originadas no teleporte dos estados referentes à $n^2(\alpha|0\rangle_3 + n^2\beta|1\rangle_3)$ e $n^2(n^2\alpha|0\rangle_3 + \beta|1\rangle_3)$) geram $P_{suc}^{(4)} = 10n^8/(1+n^2)^8$, e, de maneira geral (Rigolin, 2009), após o q -ésimo teleporte, a probabilidade total de sucesso é

$$P_{suc}^{(q)} = \frac{B(q)n^{2q}}{(1+n^2)^{2q}}, \quad (4.35)$$

onde $B(q)$ representa o total de combinações possíveis envolvendo $|\Phi_m^+\rangle$ e $|\Psi_m^-\rangle$ com os

dois estados presentes em igual número (obviamente, com a restrição de que esta condição só possa ser atingida após q vezes, para que não sejam considerados os casos em que o teleporte já teria ocorrido com sucesso em alguma etapa anterior).

Encerraremos este método analisando a probabilidade total de sucesso envolvendo todos os valores possíveis para q . A figura 4.5 mostra $P_{suc}^{total} = \sum_{j=1}^q P_{suc}^{(j)}$ para vários valores de q e n . Podemos notar que este protocolo atinge a mesma eficiência que o anterior na metade do número de passos, comprovando a superioridade do Protocolo 2 em relação ao Protocolo 1.

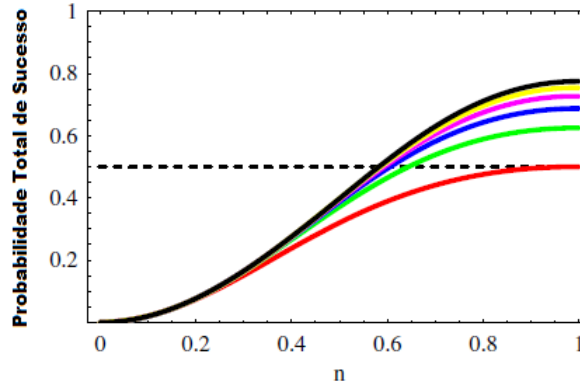


Figura 4.5: Para o protocolo 2: as curvas mostram P_{suc}^{total} após $q=1, 2, 3, 4, 5$ e 6 teleportes sucessivos. A linha tracejada mostra a probabilidade ótima ($1/2$) usando o protocolo apresentado na seção 4.2. Todas as grandezas são adimensionais.

Fonte: Figura adaptada de *Rigolin, 2009*.

4.3.3 Protocolo 3

Para finalizar, vamos apresentar o terceiro e último protocolo, e, ao final da seção, demonstraremos que este será o mais eficiente dentre os três métodos relacionados ao Teleporte Múltiplo com Fidelidade Um. Este método possui as duas primeiras etapas iguais às do Protocolo 1, mas, da terceira em diante, o grau de emaranhamento do canal diminui exponencialmente de n^2 até $n^{2^{q-2}}$ para o q -ésimo teleporte. Verificaremos que após algumas etapas e considerando valores de n próximos de um, a probabilidade total de sucesso será maior do que a dos dois protocolos anteriores e atingirá um valor próximo do máximo ($P_{suc}^{total} \approx 1$), aproximando-se dos resultados do Protocolo Original. Inicialmente, podemos repetir as duas primeiras etapas do Protocolo 1 e observar o resultado das medidas de Bob. Se não houver sucesso após o segundo teleporte, transmitiremos o estado novamente, mas, dessa vez, utilizando um canal igual a

$$|\Phi_{n^2}^+\rangle_{2,3} = \frac{|00\rangle_{2,3} + n^2|11\rangle_{2,3}}{\sqrt{1+n^4}}, \quad (4.36)$$

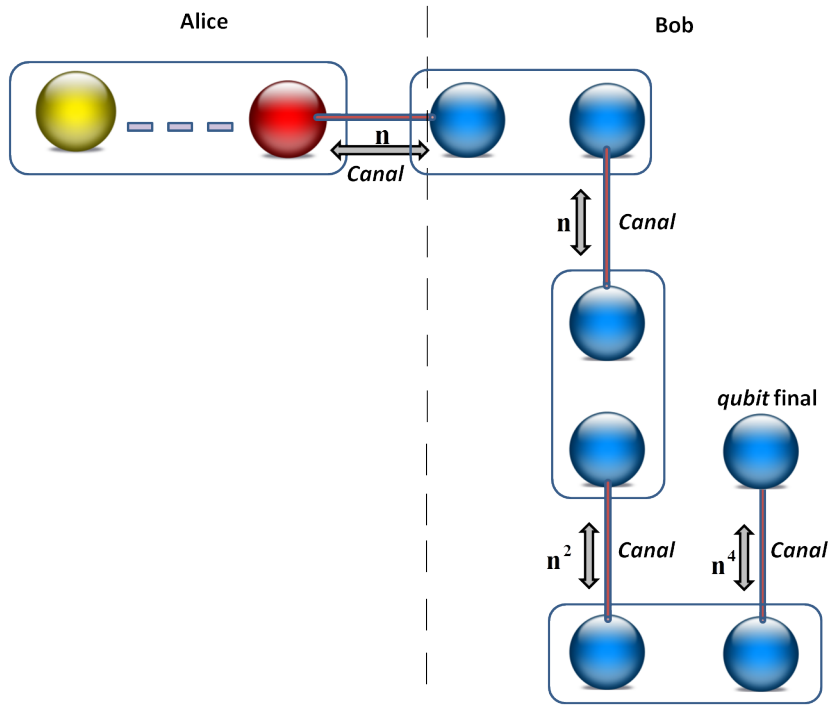


Figura 4.6: Disposição dos canais em série entre Alice e Bob com o grau de emaranhamento diminuindo exponencialmente após o segundo canal. Neste modelo, Alice possui apenas o primeiro canal e Bob tem acesso a todos os outros e ao último qubit.

onde $0 < n < 1$. Para compreender o que ocorrerá, vamos observar os possíveis resultados para a segunda etapa do Protocolo 1, mais precisamente nas equações (4.21), (4.22), (4.23) e (4.24). Observe que os casos em que houve falha apresentavam os *qubits* nas seguintes formas:

$$\alpha|0\rangle_3 + n^2\beta|1\rangle_3 \quad \text{ou} \quad n^2\alpha|0\rangle_3 + \beta|1\rangle_3. \quad (4.37)$$

Observe a figura 4.6. Com o grau de emaranhamento do canal alterado de n para n^2 , o estado de cada *qubit* após o novo teleporte também será afetado. Se o canal fosse do tipo n , o *qubit* apresentaria alguma das estruturas abaixo após o terceiro teleporte, de acordo com o resultado da medida de Bob ($|\Phi^\pm\rangle$ ou $|\Psi^\pm\rangle$):

$$\alpha|0\rangle_3 + n^3\beta|1\rangle_3, \quad n\alpha|0\rangle_3 + n^2\beta|1\rangle_3, \quad n^3\alpha|0\rangle_3 + \beta|1\rangle_3, \quad n^2\alpha|0\rangle_3 + n\beta|1\rangle_3. \quad (4.38)$$

Para um canal do tipo n^2 , entretanto, as possíveis formas que poderiam ser assumidas são

$$\alpha|0\rangle_3 + n^4\beta|1\rangle_3, \quad n^2\alpha|0\rangle_3 + n^2\beta|1\rangle_3, \quad n^4\alpha|0\rangle_3 + \beta|1\rangle_3, \quad n^2\alpha|0\rangle_3 + n^2\beta|1\rangle_3. \quad (4.39)$$

Note que a segunda e a quarta estrutura são iguais, e podem ser escritas como $n^2(\alpha|0\rangle_3 + \beta|1\rangle_3)$. Isso significa que o estado original pode ser recebido com fidelidade

um em alguns dos casos. Jamais poderíamos obter sucesso na terceira etapa do Protocolo 1, mas, com esta modificação no grau de emaranhamento de n para n^2 , o *qubit* $\alpha|0\rangle_3 + \beta|1\rangle_3$ agora pode ser recebido por Bob. Logo, tal mudança já torna este método mais eficiente do que o primeiro. Se seguirmos este raciocínio, podemos adaptar o grau de emaranhamento do canal nas etapas seguintes de forma que sempre consigamos sucesso em alguma etapa q , seja ela par ou ímpar. Para tanto, é necessário conhecer todas as formas possíveis para o *qubit* 3 na etapa $q - 1$.

Vamos tentar entender como isso ocorreu. Já vimos anteriormente que a forma do canal influencia a estrutura do *qubit* após o teleporte. Assim, se observarmos atentamente para a Eq. (4.20), podemos prever quais seriam os estados bem-sucedidos após a terceira etapa e seus respectivos coeficientes. Quando o grau do canal for igual a n , o ato de medir $|\Phi^+\rangle$ ou $|\Phi^-\rangle$ faz com que β seja multiplicado por um fator igual a n , enquanto que medir $|\Psi^+\rangle$ e $|\Psi^-\rangle$ faz com que α adquira este fator. Se o grau de emaranhamento for igual a n^2 , basta substituir o fator n que seria introduzido na etapa seguinte em β ou α por n^2 . Desse modo, fica fácil prever as possíveis combinações que resultariam em sucesso: $|\Phi^\pm\rangle|\Phi^\pm\rangle|\Psi^\pm\rangle$ e $|\Psi^\pm\rangle|\Psi^\pm\rangle|\Phi^\pm\rangle$. Os coeficientes destes estados seriam iguais a

$$\frac{1}{2(1+n^2)} \times \frac{n^2}{\sqrt{2(1+n^4)}} = \frac{n^2}{2(1+n^2)\sqrt{2(1+n^4)}}, \quad (4.40)$$

onde o fator $1/2(1+n^2)$ está relacionado aos dois primeiros teleportes, e a forma final assumida por estes estados seria

$$\frac{n^2}{2(1+n^2)\sqrt{2(1+n^4)}}|\Phi^\pm\rangle|\Phi^\pm\rangle|\Psi^\pm\rangle(\alpha|0\rangle + \beta|1\rangle) \text{ ou } \frac{n^2}{2(1+n^2)\sqrt{2(1+n^4)}}|\Psi^\pm\rangle|\Psi^\pm\rangle|\Phi^\pm\rangle(\alpha|0\rangle + \beta|1\rangle), \quad (4.41)$$

respectivamente. Se quisermos calcular a probabilidade total de sucesso nesta etapa, basta somar as 16 combinações acima:

$$P_{suc}^{(3)} = 16 \times \frac{n^4}{8(1+n^2)^2(1+n^4)} = \frac{2n^4}{(1+n^2)^2(1+n^4)}. \quad (4.42)$$

Para ilustrar o que aconteceria na quarta etapa, só precisamos conhecer os resultados que falharam na etapa 3. De acordo com a análise anterior, poderíamos teleportar $\alpha|0\rangle_3 + n^4\beta|1\rangle_3$ ou $n^4\alpha|0\rangle_3 + \beta|1\rangle_3$ e utilizar um canal com um grau de emaranhamento igual a n^4 . Assim, o processo seria bem-sucedido se medíssemos $|\Psi^\pm\rangle$ após $|\Phi^\pm\rangle|\Phi_m^\pm\rangle|\Phi^\pm\rangle$ ou $|\Phi^\pm\rangle$ após $|\Phi^\pm\rangle|\Phi_m^\pm\rangle|\Phi^\pm\rangle$, cujos coeficientes seriam iguais a

$$\frac{n^4}{2(1+n^2)\sqrt{2(1+n^4)}\sqrt{2(1+n^8)}} \quad (4.43)$$

e

$$P_{suc}^{(4)} = 32 \times \frac{n^8}{16(1+n^2)^2(1+n^4)(1+n^8)} = \frac{2n^8}{(1+n^2)^2(1+n^4)(1+n^8)}. \quad (4.44)$$

Seguindo este raciocínio, utilizaríamos um canal de grau n^8 para o quinto teleporte, n^{16} para o sexto e toda vez que o processo falhar podemos teleportar o estado obtido quantas vezes forem necessárias, usando um canal apropriadamente emaranhado cujo teor de emaranhamento é dado pelo decréscimo exponencial igual a $n^{2^{q-2}}$ para cada etapa q . Assim, em nenhum momento deixamos de ter resultados válidos (com exceção do primeiro teleporte) e o objetivo de atingir um valor alto para a probabilidade total de sucesso em poucos passos pode ser alcançado. A expressão geral para $P_{suc}^{(q)}$ é (Rigolin, 2009)

$$P_{suc}^{(q)} = \frac{2n^{2^{q-1}}}{(1+n^2)^2(1+n^4)(1+n^8)\dots(1+n^{2^{q-1}})} = \frac{2n^{2^{q-1}}(1-n^2)}{(1+n^2)(1-n^{2^q})}, \quad (4.45)$$

e a figura 4.7 mostra o comportamento de $P_{suc}^{total} = \sum_{j=1}^q P_{suc}^{(j)}$ para vários valores de q e n , onde podemos observar claramente as vantagens introduzidas por este protocolo.

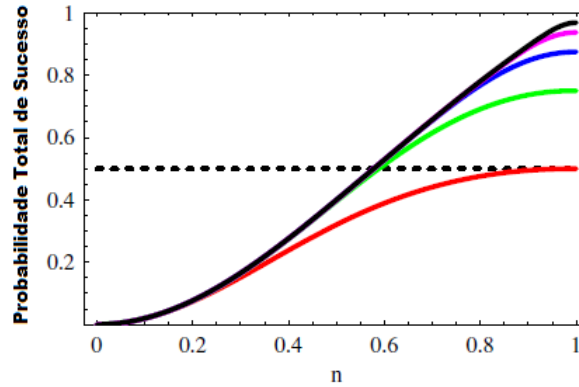


Figura 4.7: Do nível inferior até o topo, as curvas representam P_{suc}^{total} após $q=2, 3, 4, 5$ e 6 teleportes sucessivos utilizando o protocolo 3. A linha tracejada mostra a probabilidade ótima ($1/2$) usando o protocolo apresentado na seção 4.2.

Fonte: Figura adaptada de Rigolin, 2009.

Como era de se esperar, P_{suc}^{total} atinge seu valor máximo para a metade do número de teleportes em comparação com o protocolo 1. Além disso, para valores de n próximos de 0,9, temos $P_{suc}^{total} \approx 1$, algo que nenhum dos protocolos anteriores alcança. Portanto, este método é o mais eficiente dos três.

Podemos ainda destacar que o gasto de recursos requeridos pelo Protocolo 3 também é menor, já que o número de canais necessários para implementar este método é menor do que no primeiro protocolo e o grau de emaranhamento utilizado é inferior ao dos dois protocolos precedentes. Visto que o emaranhamento é um recurso de custo elevado, esta propriedade pode ser muito útil em aplicações práticas.

Capítulo 5

Teleporte de um *Qubit*: Novos Protocolos

Já analisamos o protocolo original (Bennett et al., 1993), os principais modelos de teleporte que utilizam canais parcialmente emaranhados (Li et al., 2000; Agrawal and Pati, 2002; Rigolin, 2009) e as respectivas probabilidades de sucesso associadas a cada um destes. Agora, podemos explorar as possibilidades introduzidas por estes modelos e construir novos protocolos com canais imperfeitos, visando superar estas probabilidades, e, em especial, o valor de $P_{suc}^{total} = \frac{2n^2}{1+n^2}$. Neste capítulo, abordaremos métodos de transmissão em que apenas um *qubit* é enviado. O primeiro modelo que vamos apresentar é uma combinação das seções 4.1, 4.2 e 4.3. Nos modelos seguintes exploraremos as propriedades das bases GHZ modificadas (Rigolin, 2005 e Rigolin, 2004) utilizando diferentes canais. No próximo capítulo, trataremos de teleportes envolvendo mais de um *qubit*.

5.1 Teleporte Múltiplo e Evolução Unitária

Vamos revisar algumas das técnicas vistas até o momento para obter fidelidade um através de um estado imperfeito. Para o Teleporte com Evolução Unitária (seção 4.1), estabelecemos o seguinte procedimento para Bob:

- (1) Adicionar ao sistema o *qubit* $|0\rangle_{aux}$.
- (2) Aplicar uma transformação unitária.
- (3) Realizar uma nova medida.
- (4) Para um determinado resultado da nova medida, o objetivo é atingido. Em caso contrário, reiniciar o procedimento com outro *qubit* semelhante ao original.

Para o Teleporte Múltiplo com Fidelidade Um (seção 4.3), a seqüência vista foi:

- (1) Escolher o tipo de canal que será usado no próximo teleporte.
- (2) Reenviar o estado imperfeito através deste canal.
- (3) Realizar uma nova medida.
- (4) Para determinados resultados da nova medida, o objetivo é atingido. Em caso contrário, retornar para o passo 1.

No modelo que apresentaremos em seguida, retomamos a idéia de teleportar sucessivas vezes estados imperfeitos até uma determinada etapa previamente escolhida que denotaremos por $q-1$ (utilizando a mesma notação da seção 4.3). Nesta etapa, o sistema é medido em uma base específica. Se após a medida o estado obtido ainda não for o desejado, ao invés de reenviá-lo através de um novo canal introduzimos um *qubit* auxiliar igual a $|0\rangle_{aux}$ na etapa seguinte e aplicamos uma transformação unitária adequada (seção 4.1). Em seguida, medimos o sistema na base formada por $|0\rangle_3|0\rangle_{aux}$, $|1\rangle_3|0\rangle_{aux}$, $|0\rangle_3|1\rangle_{aux}$, $|1\rangle_3|1\rangle_{aux}$ e observamos o resultado. Se o estado final do *qubit* de Bob não apresentar fidelidade um, o procedimento é abandonado e o protocolo é reiniciado com outro *qubit* semelhante ao original.

De uma forma geral, qualquer estado pode ser corrigido pelo procedimento descrito no parágrafo anterior. Seja

$$\frac{\alpha|0\rangle + T\beta|1\rangle}{\sqrt{(\alpha)^2 + (T\beta)^2}} \quad (5.1)$$

um estado imperfeito qualquer. Para que tenhamos

$$\frac{T}{\sqrt{(\alpha^2) + (T\beta)^2}}(\alpha|0\rangle + \beta|1\rangle)|0\rangle_{aux} + \sqrt{\frac{1-T^2}{(\alpha^2) + (T\beta)^2}}\alpha|1\rangle|1\rangle_{aux} \quad (5.2)$$

como um novo estado após a correção, basta construir uma matriz semelhante à vista na Eq. (4.1), com T no lugar de n . Assim, uma dentre as possíveis estruturas para a matriz que corrige o estado acima seria a seguinte,

$$U_{corr} = \begin{bmatrix} T & 0 & \sqrt{1-T^2} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ \sqrt{1-T^2} & 0 & -T & 0 \end{bmatrix},$$

com a qual obteríamos o resultado desejado. Para estados iniciais do tipo

$$\frac{T\alpha|0\rangle + \beta|1\rangle}{\sqrt{(T\alpha)^2 + (\beta)^2}} \quad (5.3)$$

construiríamos uma matriz semelhante à anterior ao permutar apenas alguns elementos,

$$U_{corr} = \begin{bmatrix} 0 & T & 0 & \sqrt{1-T^2} \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & \sqrt{1-T^2} & 0 & -T \end{bmatrix}.$$

Com isso, nosso estado após a aplicação desta matriz seria

$$\frac{T}{\sqrt{(\beta^2) + (T\alpha)^2}}(\alpha|1\rangle + \beta|0\rangle)|0\rangle_{aux} + \sqrt{\frac{1-T^2}{(\beta^2) + (T\alpha)^2}}\beta|1\rangle|1\rangle_{aux}. \quad (5.4)$$

Se medíssemos $|0\rangle_{aux}$ e aplicássemos σ_x em $\alpha|1\rangle + \beta|0\rangle$, recuperaríamos o estado original $\alpha|0\rangle + \beta|1\rangle$. Como T é arbitrário, provamos que podemos corrigir qualquer estado com esta técnica.

Retomemos a descrição deste protocolo. Para a escolha das bases de medida utilizadas até a etapa $q-1$ (antes da introdução de $|0\rangle_{aux}$) adaptamos as técnicas mostradas nos dois últimos protocolos vistos na seção 4.3: teleportes utilizando base de grau m com canais de grau n (e adotando $m=n$) e base de Bell com canais de grau $n^{2^{q-2}}$ ($q \geq 2$). Na etapa q , as matrizes de correção que atuam após a introdução de $|0\rangle_{aux}$ foram construídas para se adequar à cada forma específica assumida pelos *qubits* de interesse na etapa $q-1$. Após aplicá-las sobre os últimos, medimos o *qubit* auxiliar e efetuamos as últimas correções com as matrizes de Pauli, calculamos os valores de $P_{suc}^{(q)}$ e comparamos os resultados com os encontrados nos protocolos mencionados. Dado o excessivo número de estados gerados nos cálculos para teleportes com valores de $q \geq 4$, foram realizados cálculos até $q=4$.

Vamos apresentar primeiro os resultados referentes às probabilidades calculadas após o término da etapa q , na qual usamos a técnica de correção via *qubit* auxiliar e transformação unitária e que denotaremos por $P_{suc}^{(q)}$. Encontramos as seguintes expressões:

(1) base de grau m e canais de grau n , com $m=n$:

$$\begin{aligned} P_{suc}^{(1)} &= \frac{2n^2}{(1+n^2)^2}, & P_{suc}^{(2)} &= \frac{2n^4}{(1+n^2)^2}, & P_{suc}^{(3)} &= \frac{4n^6}{(1+n^2)^4} + \frac{2n^8}{(1+n^2)^4}, \\ P_{suc}^{(4)} &= \frac{10n^8}{(1+n^2)^6} + \frac{8n^{10}}{(1+n^2)^6} + \frac{2n^{12}}{(1+n^2)^6}. \end{aligned} \quad (5.5)$$

(2) base de Bell e canais de grau $n^{2^{q-2}}$ ($q \geq 2$):

$$P_{suc}^{(1)} = 0, \quad P_{suc}^{(2)} = \frac{2n^2}{1+n^2}, \quad P_{suc}^{(3)} = \frac{2n^4}{(1+n^2)^2}, \quad P_{suc}^{(4)} = \frac{2n^8}{(1+n^2)^2(1+n^4)}. \quad (5.6)$$

De posse destes valores, calculamos a probabilidade total envolvendo todas as possibilidades de teleporte. Para isso, basta somar as probabilidades até a j -ésima etapa, com j assumindo valores inteiros desde $j = 1$ até $j = q$. Para as probabilidades calculadas até a etapa $j - 1$, retomamos as expressões $P_{suc}^{(j)}$ calculadas na seção 4.3, e a estes valores somamos os resultados encontrados na etapa q listados nas equações acima ($P_{suc}^{(q)}$). Assim, temos que:

$$P_{suc}^{total} = \sum_{j=1}^{q-1} P_{suc}^{(j)} + P_{suc}^{(q)}, \quad q \in [1, 4]. \quad (5.7)$$

Para os dois métodos analisados, um fato notável foi a descoberta de que P_{suc}^{total} resultava sempre na mesma expressão, independente dos valores de q considerados. No Apêndice A, demonstramos que essa soma revela o melhor resultado obtido até agora, para qualquer valor de q . A expressão encontrada para P_{suc}^{total} foi

$$P_{suc}^{total} = \sum_{j=1}^{q-1} P_{suc}^{(j)} + P_{suc}^{(q)} = \frac{2n^2}{1 + n^2}, \quad (5.8)$$

o mesmo resultado encontrado na Eq. (4.11). Ou seja, efetuar sucessivos teleportes e aplicar a correção via transformação unitária na última etapa resulta na mesma probabilidade de sucesso oriunda do caso em que efetuamos apenas um teleporte seguido da correção via transformação unitária.

Na próxima seção veremos um outro tipo de teleporte múltiplo com correção de estados imperfeitos.

5.2 Teleporte Múltiplo com Sucesso Apenas no Fim

O Teleporte Múltiplo abordado na seção 5.1 era constituído de canais em série através dos quais o estado enviado por Alice era teleportado seguidamente até uma etapa q escolhida. Após a interrupção do processo e a subsequente medida do sistema, Bob aplicava as correções necessárias para que o *qubit* final assumisse as características da informação original. Desta forma, Bob poderia escolher arbitrariamente em qual etapa desejava interromper o teleporte já que dispunha de todos os canais. Se, por exemplo, a etapa escolhida fosse a quarta, o estado era teleportado entre os próprios canais de Bob até $q = 4$ a menos que houvesse sucesso em alguma etapa anterior. Vimos que a probabilidade final após a implementação das correções era independente do número de vezes que Bob teleportava o mesmo estado (Eq. (5.8)), tornando desnecessário na prática o uso de mais de um canal para enviar o estado inicial já que isso acarretaria um aumento de recursos financeiros e materiais.

Nesta seção, introduziremos um protocolo de teleporte múltiplo que opera

sob outro mecanismo. O estado será enviado através de canais em série mas Alice e Bob só têm acesso ao primeiro e último, respectivamente, pois os canais intermediários ficam isolados. Assim, esperamos que surja um novo padrão na distribuição de probabilidades, pois agora Bob não pode interromper o processo mesmo que algum caso seja bem-sucedido antes de atingir a etapa final q , e, por isso, a probabilidade total de sucesso para qualquer valor de q será menor do que a expressão $P_{suc}^{total} = \sum_{j=1}^q P_{suc}^{(j)}$ para os modelos discutidos nas seções 4.3 e 5.1, uma vez que o estado original deve ser obtido em um número fixo de etapas pré-determinado. Todavia, como constataremos ao final desta seção, tal fato não diminui a importância deste modelo.

Vejamos então como funciona o processo. A figura 5.1 ilustra o mecanismo

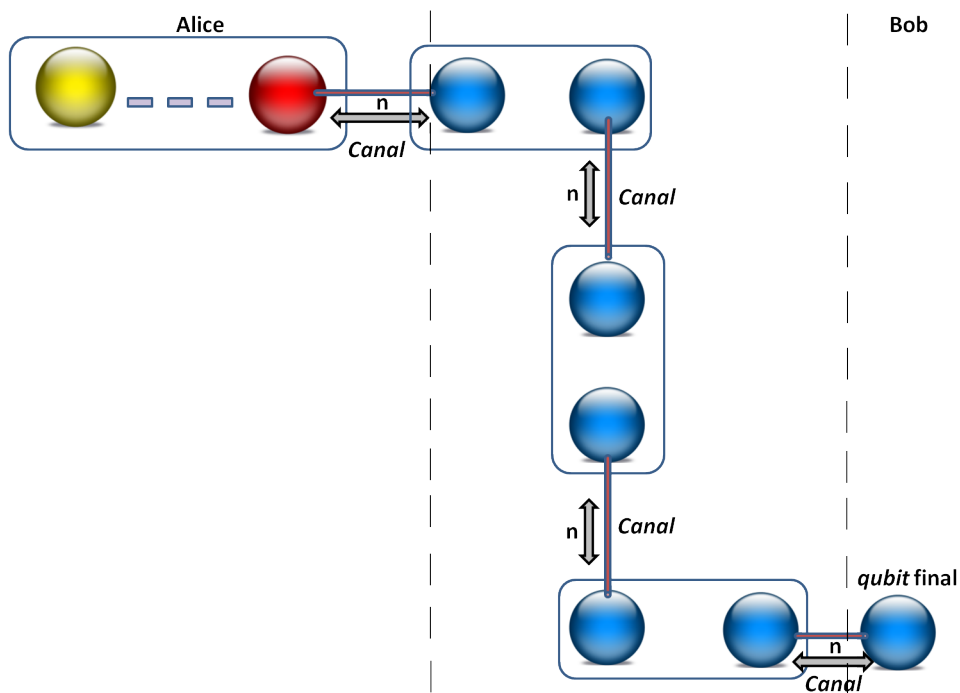


Figura 5.1: Disposição dos canais em série entre Alice e Bob. Neste modelo, Alice possui apenas o primeiro canal e Bob só tem acesso ao último qubit.

deste protocolo. Repare que o estado é transmitido através de um número fixo de canais, e Bob só tem acesso ao último da seqüência. Após a revelação das medidas do par em posse de Alice e dos *qubits* restantes através de algum dispositivo acoplado aos canais intermediários, Bob sabe qual estado possui em mãos e quais as correções unitárias necessárias para equipará-lo ao estado original. Portanto, para cada etapa q vista na seção 5.1, adicionamos os estados que haviam sido descartados por alcançarem êxito previamente e recalculamos os estados finais. Foram realizados testes para $m = n$ e $m = 1$, e a segunda escolha forneceu os melhores resultados, e, devido à semelhança destes últimos com uma expressão conhecida (Perseguers et al., 2008), decidimos estender os cálculos para este cenário até $q = 8$. Os resultados podem ser conferidos a seguir.

(1) $m = n$:

$$P'_{suc}(1) = \frac{2n^2}{1+n^2}, \quad P'_{suc}(2) = \left(\frac{2n^2}{1+n^2}\right)^2 \frac{n^2(3+n^2)}{(1+n^2)^2}, \quad P'_{suc}(3) = \left(\frac{2n^2}{1+n^2}\right)^2 \frac{n^4(10+5n^2+n^4)}{(1+n^2)^4}. \quad (5.9)$$

(2) $m = 1$:

$$\begin{aligned} P'_{suc}(1) &= \frac{2n^2}{1+n^2}, \quad P'_{suc}(2) = \frac{2n^2}{1+n^2}, \quad P'_{suc}(3) = \left(\frac{2n^2}{1+n^2}\right)^2 \frac{3+n^2}{2(1+n^2)}, \quad P'_{suc}(4) = \left(\frac{2n^2}{1+n^2}\right)^2 \frac{3+n^2}{2(1+n^2)}, \\ P'_{suc}(5) &= \frac{2n^6(10+5n^2+n^4)}{(1+n^2)^5}, \quad P'_{suc}(6) = \frac{2n^6(10+5n^2+n^4)}{(1+n^2)^5}, \quad P'_{suc}(7) = \frac{2n^8(35+21n^2+7n^4+n^6)}{(1+n^2)^7}, \\ P'_{suc}(8) &= \frac{2n^8(35+21n^2+7n^4+n^6)}{(1+n^2)^7}. \end{aligned} \quad (5.10)$$

Para $m = 1$, o valor das probabilidades se repete para as etapas q e $q + 1$ onde q é um inteiro ímpar.

Construímos por indução a expressão geral para as probabilidades calculadas nas duas situações. Para $m = n$, encontramos

$$P_{suc}^{total} = \frac{1}{(1+n^2)^q} \left\{ \sum_{j=1}^q \binom{2q}{q-j} n^{2(q+j)} + \sum_{j=0}^q \binom{2q}{q+j} n^{2(q+j)} \right\}, \quad (5.11)$$

onde $\binom{m}{n} = m!/\{(n!)(m-n)!\}$. Para $m = 1$, entretanto, a expressão encontrada para a probabilidade total de sucesso foi

$$P_{suc}^{total} = 1 - (f_n^{2j} - g_n^{2j}) \sum_{j=0}^{\frac{q-1}{2}} f_n^{2j} g_n^{2j} \binom{2j}{j} \quad (5.12)$$

a qual, por sua vez, é idêntica à expressão

$$P_{swap} = 1 - (f_n^{2j} - g_n^{2j}) \sum_{j=0}^{\frac{N}{2}} f_n^{2j} g_n^{2j} \binom{2j}{j} \quad (5.13)$$

calculada em [Perseguers et al., 2008](#) e citada no final de [Rigolin, 2009](#), onde $f_n = 1/(\sqrt{1+n^2})$ e $g_n = n/(\sqrt{1+n^2})$. A Eq. 5.13 fora obtida calculando-se a destilação de uma cadeia de n qubits em série onde Alice e Bob só possuíam o primeiro e último qubit, respectivamente. O número de destilações realizadas é associado ao índice inteiro N , o qual, por sua vez, está defasado de uma unidade em relação ao valor do índice q que representa o número de teleportes em 5.12. Este resultado era o melhor até o momento e não havia outro método que atingisse o mesmo valor. Assim, mostramos com os resultados em 5.12 que uma cadeia de qubits em série também pode ser utilizada para sucessivos teleportes de um mesmo

estado (com a condição de que não ocorra interferência antes do fim do processo) e a eficiência ao fim do procedimento será a mesma da Eq. (5.13). Logo, este método possui aplicação direta para o mercado, pois serve como alternativa à destilação proposta por [Perseguers et al., 2008](#).

Na próxima seção vamos abordar um caso em que apenas um teleporte é realizado e a correção via *qubit* auxiliar é aplicada em seguida.

5.3 Base GHZ Generalizada

Vamos mostrar agora como teleportar um único *qubit* utilizando dois canais paralelos. O processo todo envolve cinco *qubits*, onde os três primeiros estão englobados na base de medida e os dois restantes em posse de Bob. Após a medida de Alice e o colapso dos dois últimos para um novo estado, mostraremos que é possível separá-los em dois *qubits* distintos aplicando transformações unitárias simples, onde um destes será idêntico ao *qubit* original.

Um exemplo de uma estrutura que envolve três *qubits* emaranhados é o estado conhecido como GHZ ([Greenberger et al., 2010](#); [Rigolin, 2005](#)):

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \quad (5.14)$$

Se observarmos a base de Bell generalizada na Eq. (4.12) da seção (4.2), podemos construir uma base GHZ modificada de forma que seus estados dependam apenas de um único parâmetro m . Em [Rigolin, 2005](#) encontramos a forma explícita destes estados, mostrada a seguir:

$$\begin{aligned} |G_m^+\rangle &= \frac{|010\rangle + m|101\rangle}{\sqrt{1+m^2}}, & |G_m^-\rangle &= \frac{m|010\rangle - |101\rangle}{\sqrt{1+m^2}}, & |H_m^+\rangle &= \frac{|100\rangle + m|011\rangle}{\sqrt{1+m^2}}, \\ |H_m^-\rangle &= \frac{m|100\rangle - |011\rangle}{\sqrt{1+m^2}}, & |Z_m^+\rangle &= \frac{|110\rangle + m|001\rangle}{\sqrt{1+m^2}}, & |Z_m^-\rangle &= \frac{m|110\rangle - |001\rangle}{\sqrt{1+m^2}}, \end{aligned} \quad (5.15)$$

onde $0 < m < 1$.

Os seis estados mostrados acima são ortonormais, mas não formam uma base completa. Para descrever qualquer vetor que envolva 3 *qubits*, onde cada *qubit* reside em um espaço de *Hilbert* de duas dimensões, são necessários $2^3 = 8$ estados ortonormais. Se adicionarmos dois novos estados ([Rigolin, 2005](#)) representados por $|GHZ_m^+\rangle = (|000\rangle + m|111\rangle) / \sqrt{1+m^2}$ e $|GHZ_m^-\rangle = (m|000\rangle - |111\rangle) / \sqrt{1+m^2}$, teremos agora um conjunto ortonormal que forma uma base completa de oito estados, e, com isso, podemos projetar um determinado sistema de três *qubits* que possa ser medido nesta base. A figura 5.2 mostra como será realizado o procedimento de envio do *qubit* original de Alice. Serão utilizados dois canais no processo, e vamos representá-los pela mesma estrutura $|\Phi_n^+\rangle$

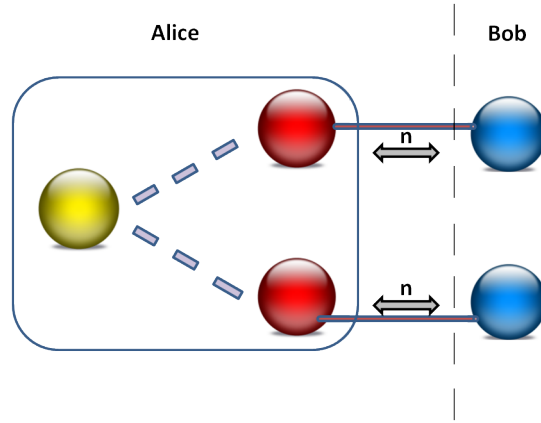


Figura 5.2: Teleporte de um qubit utilizando dois canais paralelos e medidas na base GHZ generalizada.

utilizada nos outros protocolos. Poderíamos muito bem ter escolhido $|\Phi_n^-\rangle$, $|\Psi_n^+\rangle$ ou $|\Psi_n^-\rangle$, mas da mesma forma que um estado da base de Bell pode ser alterado para outro através de transformações locais, o mesmo ocorre com os estados da base generalizada, e a escolha inicial da forma dos canais não interfere no resultado final.

De um modo geral, o processo relacionado à transmissão de informação quântica é semelhante ao que já vimos até aqui. Alice prepara um estado, faz uma medida conjunta entre seu *qubit* e uma parte dos constituintes dos canais e informa o resultado a Bob. Uma vez que os dois participantes saibam a relação entre o resultado das medidas e as respectivas transformações unitárias que devem ser aplicadas, basta a Bob aplicar a transformação correta ou que o processo seja repetido até que haja sucesso. A diferença, neste caso, é que serão utilizados dois canais para o envio do estado original, e ambos pertencem ao processo de medida de Alice. Vamos explicar como isso será realizado, lembrando que se desejarmos escrever o estado geral do sistema, precisaremos levar em conta todos os elementos presentes no momento da análise.

No início do processo, havia o *qubit* 1 de Alice e dois canais que denotaremos por $|\Phi_n^+\rangle_{3,5}$ e $|\Phi_n^+\rangle_{4,6}$, com os *qubits* 3 e 4 em posse de Alice e *qubits* 5 e 6 em posse de Bob. Então, inicialmente, nosso estado geral assumia a seguinte configuração:

$$|\phi\rangle_1|\Phi_n^+\rangle_{3,5}|\Phi_n^+\rangle_{4,6} = \frac{(\alpha|0\rangle_1 + \beta|1\rangle_1)}{1+n^2}(|0000\rangle_{3,5,4,6} + n|0011\rangle_{3,5,4,6} + n|1100\rangle_{3,5,4,6} + n^2|1111\rangle_{3,5,4,6}). \quad (5.16)$$

Ao expandir o produto acima e rearranjar os índices na ordem $|13456\rangle$, ficamos com $|\phi\rangle_1|\Phi_n^+\rangle_{3,5}|\Phi_n^+\rangle_{4,6} =$

$$\begin{aligned} &= N^2(\alpha|00000\rangle_{1,3,4,5,6} + n\alpha|00101\rangle_{1,3,4,5,6} + n\alpha|01010\rangle_{1,3,4,5,6} + n^2\alpha|01111\rangle_{1,3,4,5,6}) \\ &+ N^2(\beta|10000\rangle_{1,3,4,5,6} + n\beta|10101\rangle_{1,3,4,5,6} + n\beta|11010\rangle_{1,3,4,5,6} + n^2\beta|11111\rangle_{1,3,4,5,6}). \end{aligned} \quad (5.17)$$

Se escrevermos os oito estados da base computacional de três *qubits* em função dos estados GHZ generalizados, poderemos inserir estes últimos na estrutura do estado geral do sistema. Assim, considerando que

$$\begin{aligned} |000\rangle &= \frac{|GHZ_m^+\rangle + m|GHZ_m^-\rangle}{\sqrt{1+m^2}}, & |001\rangle &= \frac{m|Z_m^+\rangle - |Z_m^-\rangle}{\sqrt{1+m^2}}, & |010\rangle &= \frac{|G_m^+\rangle + m|G_m^-\rangle}{\sqrt{1+m^2}}, & |011\rangle &= \frac{m|H_m^+\rangle - |H_m^-\rangle}{\sqrt{1+m^2}}, \\ |100\rangle &= \frac{|H_m^+\rangle + m|H_m^-\rangle}{\sqrt{1+m^2}}, & |101\rangle &= \frac{m|G_m^+\rangle - |G_m^-\rangle}{\sqrt{1+m^2}}, & |110\rangle &= \frac{|Z_m^+\rangle + m|Z_m^-\rangle}{\sqrt{1+m^2}}, & |111\rangle &= \frac{m|GHZ_m^+\rangle - |GHZ_m^-\rangle}{\sqrt{1+m^2}}, \end{aligned} \quad (5.18)$$

o estado geral do sistema será $|\phi\rangle_1 |\Phi_n^+\rangle_{3,5} |\Phi_n^+\rangle_{4,6} =$

$$\begin{aligned} &= \alpha \left(\frac{|GHZ_m^+\rangle + m|GHZ_m^-\rangle}{(1+n^2)\sqrt{1+m^2}} \right) |00\rangle_{56} + n\alpha \left(\frac{m|Z_m^+\rangle - |Z_m^-\rangle}{(1+n^2)\sqrt{1+m^2}} \right) |01\rangle_{56} + n\alpha \left(\frac{|G_m^+\rangle + m|G_m^-\rangle}{(1+n^2)\sqrt{1+m^2}} \right) |10\rangle_{56} \\ &+ n^2\alpha \left(\frac{m|H_m^+\rangle - |H_m^-\rangle}{(1+n^2)\sqrt{1+m^2}} \right) |11\rangle_{56} + \beta \left(\frac{|H_m^+\rangle + m|H_m^-\rangle}{(1+n^2)\sqrt{1+m^2}} \right) |00\rangle_{56} + n\beta \left(\frac{m|G_m^+\rangle - |G_m^-\rangle}{(1+n^2)\sqrt{1+m^2}} \right) |01\rangle_{56} \\ &+ n\beta \left(\frac{|Z_m^+\rangle + m|Z_m^-\rangle}{(1+n^2)\sqrt{1+m^2}} \right) |10\rangle_{56} + n^2\beta \left(\frac{m|GHZ_m^+\rangle - |GHZ_m^-\rangle}{(1+n^2)\sqrt{1+m^2}} \right) |11\rangle_{56}. \end{aligned} \quad (5.19)$$

Deste ponto em diante, já sabemos como proceder. Como os estados GHZ generalizados são ortogonais, basta que o sistema seja medido em uma base que contenha apenas estes oito estados. Para cada possível resultado relacionado à uma destas medidas, os *qubits* 5 e 6 serão modificados para uma determinada estrutura particular, e esperamos que algumas sejam semelhantes à original enviada por Alice. No arranjo abaixo, reescrevemos o estado geral e mostramos os possíveis resultados associados à estas medidas (onde incluímos as respectivas normalizações). $|\phi\rangle_1 |\Phi_n^+\rangle_{3,5} |\Phi_n^+\rangle_{4,6} =$

$$\begin{aligned} &= |GHZ_m^+\rangle \left[\frac{\sqrt{(\alpha)^2 + (mn^2\beta)^2}}{(1+n^2)\sqrt{1+m^2}} \right] \left(\frac{\alpha|00\rangle_{56} + mn^2\beta|11\rangle_{56}}{\sqrt{(\alpha)^2 + (mn^2\beta)^2}} \right) + |GHZ_m^-\rangle \left[\frac{\sqrt{(m\alpha)^2 + (n^2\beta)^2}}{(1+n^2)\sqrt{1+m^2}} \right] \left(\frac{m\alpha|00\rangle_{56} - n^2\beta|11\rangle_{56}}{\sqrt{(m\alpha)^2 + (n^2\beta)^2}} \right) \\ &+ |Z_m^+\rangle \left[\frac{\sqrt{(mn\alpha)^2 + (n\beta)^2}}{(1+n^2)\sqrt{1+m^2}} \right] \left(\frac{mn\alpha|01\rangle_{56} + n\beta|10\rangle_{56}}{\sqrt{(mn\alpha)^2 + (n\beta)^2}} \right) + |Z_m^-\rangle \left[\frac{\sqrt{(-n\alpha)^2 + (mn\beta)^2}}{(1+n^2)\sqrt{1+m^2}} \right] \left(\frac{-n\alpha|01\rangle_{56} + mn\beta|10\rangle_{56}}{\sqrt{(-n\alpha)^2 + (mn\beta)^2}} \right) \\ &+ |G_m^+\rangle \left[\frac{\sqrt{(n\alpha)^2 + (mn\beta)^2}}{(1+n^2)\sqrt{1+m^2}} \right] \left(\frac{n\alpha|10\rangle_{56} + mn\beta|01\rangle_{56}}{\sqrt{(n\alpha)^2 + (mn\beta)^2}} \right) + |G_m^-\rangle \left[\frac{\sqrt{(mn\alpha)^2 + (-n\beta)^2}}{(1+n^2)\sqrt{1+m^2}} \right] \left(\frac{mn\alpha|10\rangle_{56} - n\beta|01\rangle_{56}}{\sqrt{(mn\alpha)^2 + (-n\beta)^2}} \right) \\ &+ |H_m^+\rangle \left[\frac{\sqrt{(mn^2\alpha)^2 + (\beta)^2}}{(1+n^2)\sqrt{1+m^2}} \right] \left(\frac{mn^2\alpha|11\rangle_{56} + \beta|00\rangle_{56}}{\sqrt{(mn^2\alpha)^2 + (\beta)^2}} \right) + |H_m^-\rangle \left[\frac{\sqrt{(-n^2\alpha)^2 + (m\beta)^2}}{(1+n^2)\sqrt{1+m^2}} \right] \left(\frac{-n^2\alpha|11\rangle_{56} + m\beta|00\rangle_{56}}{\sqrt{(-n^2\alpha)^2 + (m\beta)^2}} \right). \end{aligned} \quad (5.20)$$

Nosso próximo passo diz respeito à escolha do grau de emaranhamento m da base de medidas. Existem inúmeras opções válidas, mas o que nos interessa é a escolha que maximize a probabilidade total associada ao sucesso no envio do *qubit* original. De todas as opções testadas, a única que atinge o máximo valor possível é escolha de $m = 1$, e, nesta condição, o estado geral do sistema pode ser reduzido à seguinte estrutura:

$$\begin{aligned} &|GHZ_m^+\rangle \left[\frac{\sqrt{(\alpha)^2 + (n^2\beta)^2}}{(1+n^2)\sqrt{2}} \right] \left(\frac{\alpha|00\rangle_{56} + n^2\beta|11\rangle_{56}}{\sqrt{(\alpha)^2 + (n^2\beta)^2}} \right) + |GHZ_m^-\rangle \left[\frac{\sqrt{(\alpha)^2 + (n^2\beta)^2}}{(1+n^2)\sqrt{2}} \right] \left(\frac{\alpha|00\rangle_{56} - n^2\beta|11\rangle_{56}}{\sqrt{(\alpha)^2 + (n^2\beta)^2}} \right) \\ &+ |Z_m^+\rangle \left[\frac{n}{(1+n^2)\sqrt{2}} \right] (\alpha|01\rangle_{56} + \beta|10\rangle_{56}) + |Z_m^-\rangle \left[\frac{n}{(1+n^2)\sqrt{2}} \right] (-\alpha|01\rangle_{56} + \beta|10\rangle_{56}) \end{aligned}$$

$$\begin{aligned}
& + |G_m^+\rangle \left[\frac{n}{(1+n^2)\sqrt{2}} \right] (\alpha|10\rangle_{56} + \beta|01\rangle_{56}) + |G_m^-\rangle \left[\frac{n}{(1+n^2)\sqrt{2}} \right] (\alpha|10\rangle_{56} - \beta|01\rangle_{56}) \\
& + |H_m^+\rangle \left[\frac{\sqrt{(n^2\alpha)^2 + (\beta)^2}}{(1+n^2)\sqrt{2}} \right] \left(\frac{n^2\alpha|11\rangle_{56} + \beta|00\rangle_{56}}{\sqrt{(n^2\alpha)^2 + (\beta)^2}} \right) + |H_m^-\rangle \left[\frac{\sqrt{(-n^2\alpha)^2 + (\beta)^2}}{(1+n^2)\sqrt{2}} \right] \left(\frac{-n^2\alpha|11\rangle_{56} + \beta|00\rangle_{56}}{\sqrt{(-n^2\alpha)^2 + (\beta)^2}} \right).
\end{aligned} \tag{5.21}$$

Para esta escolha de base, percebemos que o protocolo funciona de imediato se os resultados medidos por Alice forem $|Z_m^+\rangle$, $|Z_m^-\rangle$, $|G_m^+\rangle$ ou $|G_m^-\rangle$, com os estados finais obtidos assumindo as formas de

$$\alpha|01\rangle_{56} + \beta|10\rangle_{56}, \quad -\alpha|01\rangle_{56} + \beta|10\rangle_{56}, \quad \alpha|10\rangle_{56} + \beta|01\rangle_{56}, \quad \text{ou} \quad \alpha|10\rangle_{56} - \beta|01\rangle_{56}, \tag{5.22}$$

respectivamente. Para cada um destes estados, aplicamos uma porta *CNOT* com o controle no *qubit* 5 e o alvo no *qubit* 6. Desta forma, as novas possibilidades passam a ser

$$\alpha|01\rangle_{56} + \beta|11\rangle_{56}, \quad -\alpha|01\rangle_{56} + \beta|11\rangle_{56}, \quad \alpha|11\rangle_{56} + \beta|01\rangle_{56}, \quad \text{ou} \quad \alpha|11\rangle_{56} - \beta|01\rangle_{56}, \tag{5.23}$$

ou, escrevendo de outra maneira,

$$(\alpha|0\rangle_5 + \beta|1\rangle_5)|1\rangle_6, \quad (-\alpha|0\rangle_5 + \beta|1\rangle_5)|1\rangle_6, \quad (\alpha|1\rangle_5 + \beta|0\rangle_5)|1\rangle_6, \quad \text{ou} \quad (\alpha|1\rangle_5 - \beta|0\rangle_5)|1\rangle_6. \tag{5.24}$$

Se neste ponto medirmos o *qubit* 6, encontraremos $|1\rangle$ como resultado, e os estados relacionados ao *qubit* 5 serão

$$\alpha|0\rangle_5 + \beta|1\rangle_5, \quad -\alpha|0\rangle_5 + \beta|1\rangle_5, \quad \alpha|1\rangle_5 + \beta|0\rangle_5, \quad \text{ou} \quad \alpha|1\rangle_5 - \beta|0\rangle_5. \tag{5.25}$$

Aplicando as transformações unitárias básicas necessárias (I , $\sigma_x\sigma_z\sigma_x$, σ_x , ou $\sigma_z\sigma_x$, respectivamente), conseguimos transmitir o estado original e constatamos que o procedimento funciona. Poderíamos ter aplicado uma porta *CNOT* com o controle no *qubit* 6 e o alvo no *qubit* 5, e, medindo este, verificaríamos que seu valor seria igual a $|1\rangle$, mas as probabilidades ao final do processo seriam as mesmas. Para calculá-las, repare que as probabilidades de sucesso para cada caso são iguais e que, quando somadas, resultam em

$$P_{suc}^{total} = 4 \times \frac{n^2}{2(1+n^2)^2} = \frac{2n^2}{(1+n^2)^2}. \tag{5.26}$$

A primeira vez que vimos este resultado foi na Eq. (4.18) da seção (4.2). Naquele momento, mostramos que as possibilidades de sucesso direto forneciam este valor e não nos preocupamos com as medidas restantes, e, na seção (5.1), mostramos que a

correção destes estados alteravam o valor de P_{suc}^{total} para $2n^2/1+n^2$. Como ainda nos resta metade dos casos para analisar, existe a chance de podermos atingir este último resultado, como veremos a seguir.

5.3.1 Correção dos estados restantes

Podemos corrigir os estados

$$\frac{\alpha|00\rangle + n^2\beta|11\rangle}{\sqrt{(\alpha)^2 + (n^2\beta)^2}}, \quad \frac{\alpha|00\rangle - n^2\beta|11\rangle}{\sqrt{(\alpha)^2 + (n^2\beta)^2}}, \quad \frac{n^2\alpha|11\rangle + \beta|00\rangle}{\sqrt{(n^2\alpha)^2 + (\beta)^2}}, \quad \text{e} \quad \frac{-n^2\alpha|11\rangle + \beta|00\rangle}{\sqrt{(n^2\alpha)^2 + (\beta)^2}} \quad (5.27)$$

associados às medidas de $|GHZ_m^+\rangle$, $|GHZ_m^-\rangle$, $|H_m^+\rangle$ e $|H_m^-\rangle$, respectivamente, através da técnica da Matriz de Evolução Unitária. O procedimento é o mesmo descrito na seção (5.1) para corrigir um *qubit* simples, desde que trabalhemos com somente um. Para isso, basta reduzir o estado final de dois *qubits* para um, como mostramos no final da seção anterior. Aplicamos uma porta *CNOT* com o controle no *qubit* 5 e o alvo no *qubit* 6 e em seguida medimos este último, que agora assumirá o valor $|0\rangle$. Dessa forma, os estados que falharam passam a ser descritos por

$$\frac{\alpha|0\rangle + n^2\beta|1\rangle}{\sqrt{(\alpha)^2 + (n^2\beta)^2}}, \quad \frac{\alpha|0\rangle - n^2\beta|1\rangle}{\sqrt{(\alpha)^2 + (n^2\beta)^2}}, \quad \frac{n^2\alpha|1\rangle + \beta|0\rangle}{\sqrt{(n^2\alpha)^2 + (\beta)^2}}, \quad \text{e} \quad \frac{-n^2\alpha|1\rangle + \beta|0\rangle}{\sqrt{(n^2\alpha)^2 + (\beta)^2}}. \quad (5.28)$$

Por outro lado, já vimos como a matriz de correção atua. Sabendo que os estados podem diferir uns dos outros apenas pelas transformações unitárias básicas, as estruturas do tipo $\alpha|0\rangle + T\beta|1\rangle/\sqrt{(\alpha)^2 + (T\beta)^2}$ serão modificadas para

$$\frac{T}{\sqrt{(\alpha^2) + (T\beta)^2}}(\alpha|0\rangle + \beta|1\rangle)|0\rangle_{aux} + \sqrt{\frac{1-T^2}{(\alpha^2) + (T\beta)^2}}\alpha|1\rangle|1\rangle_{aux}, \quad (5.29)$$

e, da mesma forma, as do tipo $(T\alpha|0\rangle + \beta|1\rangle)/\sqrt{(T\alpha)^2 + (\beta)^2}$ serão modificadas para

$$\frac{T}{\sqrt{(\beta^2) + (T\alpha)^2}}(\alpha|1\rangle + \beta|0\rangle)|0\rangle_{aux} + \sqrt{\frac{1-T^2}{(\beta^2) + (T\alpha)^2}}\beta|1\rangle|1\rangle_{aux}. \quad (5.30)$$

Com $T = n^2$, a probabilidade de obter $|0\rangle_{aux}$ para as estruturas do tipo $(\alpha|0\rangle + n^2\beta|1\rangle)/\sqrt{(\alpha)^2 + (n^2\beta)^2}$ é

$$\left| \frac{n^2}{\sqrt{(\alpha^2) + (n^2\beta^2)}} \right|^2, \quad (5.31)$$

e a probabilidade de obter cada um dos estados da base GHZ generalizada é

$$\left| \sqrt{\frac{(\alpha)^2 + (n^2\beta)^2}{2(1+n^2)^2}} \right|^2. \quad (5.32)$$

Assim, a probabilidade relativa a este caso é

$$\left| \sqrt{\frac{(\alpha)^2 + (n^2\beta)^2}{2(1+n^2)^2}} \right|^2 \times \left| \frac{n^2}{\sqrt{(\alpha)^2 + (n^2\beta)^2}} \right|^2 = \frac{n^4}{2(1+n^2)^2}, \quad (5.33)$$

e, como o resultado é idêntico para qualquer um dos quatro estados após as correção dos mesmos, a probabilidade associada aos estados corrigidos será de

$$4 \times \frac{n^4}{2(1+n^2)^2} = \frac{2n^4}{(1+n^2)^2}. \quad (5.34)$$

Somando este resultado ao encontrado no final da seção anterior, determinamos que P_{suc}^{total} é igual a

$$P_{suc}^{total} = \frac{2n^4}{(1+n^2)^2} + \frac{2n^2}{(1+n^2)^2} = \frac{2n^2}{1+n^2}, \quad (5.35)$$

e, mais uma vez, atingimos o valor dado pela Eq. (4.11), como previmos antes do início desta seção.

Capítulo 6

Teleporte de Dois *Qubits*

No capítulo anterior, apresentamos três métodos distintos para teleportar probabilisticamente um *qubit* com fidelidade um, e provamos que ambos atingem a mesma eficiência. Neste capítulo, mostraremos como teleportar dois *qubits* através de diferentes arranjos envolvendo os canais e a base de medidas, e, para cada configuração, revelaremos ao menos uma situação na qual cada protocolo atinge o valor de $P_{suc}^{total} = \frac{2n^2}{1+n^2}$.

6.1 Utilizando dois Canais Paralelos

O estado geral de dois *qubits* pode ser construído a partir da definição para o caso de um *qubit*. Existem quatro estados de base, e, portanto, são necessários quatro coeficientes sujeitos ao vínculo de normalização,

$$|\phi\rangle_{1,2} = \alpha' |00\rangle_{1,2} + \beta' |01\rangle_{1,2} + \gamma' |10\rangle_{1,2} + \delta' |11\rangle_{1,2}, \quad (6.1)$$

com $|\alpha'|^2 + |\beta'|^2 + |\gamma'|^2 + |\delta'|^2 = 1$.

Alice e Bob agora compartilharão dois canais paralelos, que representaremos por $|\Phi_{n1}^+\rangle_{3,5}$ e $|\Phi_{n2}^+\rangle_{4,6}$. Lembre-se de que a escolha dos canais é arbitrária e não afeta o valor das probabilidades calculadas ao final do processo, e os cálculos seriam os mesmos se tivéssemos escolhido qualquer outra combinação (como $|\Phi_{n1}^-\rangle_{3,5}$ e $|\Psi_{n2}^+\rangle_{4,6}$, por exemplo). As medidas iniciais de Alice serão realizadas sobre dois pares de *qubits*, representados pelos índices 1 e 3 para o primeiro par e 2 e 4 para o segundo. Cada base de medida possui um grau de emaranhamento próprio, que denotaremos por m_a e m_b , e obedecem à mesma estrutura vista para a base generalizada de grau m trabalhada nos protocolos anteriores.

A figura 6.1 ilustra o mecanismo deste método. Alice possui o estado inicial de dois *qubits* (representados pelos índices 1 e 2) e um *qubit* de cada canal (índices 3 e 4), enquanto Bob recebe os outros dois *qubits* restantes (5 e 6). A escolha do grau de emaranhamento dos canais foi feita de forma que $n_1=n_2$, uma vez que esta condição

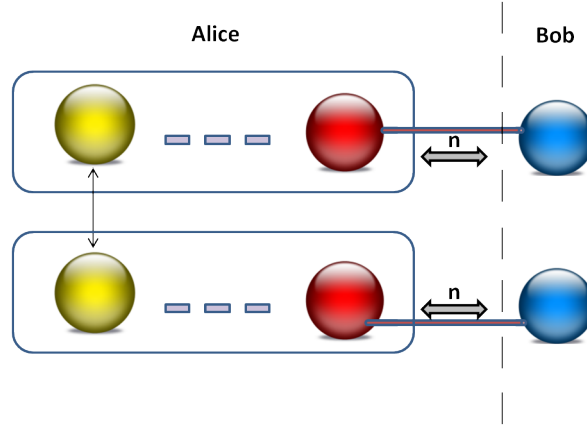


Figura 6.1: Teleporte de dois qubits utilizando dois canais paralelos e medidas na base de Bell generalizada.

forneceu a maior eficiência dentre todos os testes realizados. A princípio, as bases de medidas serão mantidas com graus de emaranhamento distintos - m_a e m_b - e, após o cálculo do estado geral do sistema, analisaremos os principais casos envolvendo estes dois parâmetros.

Começaremos mais uma vez calculando o estado geral do sistema, respeitando a ordem $|12\rangle|35\rangle|46\rangle$. Sua forma será $|\phi\rangle_1|\Phi_n^+\rangle_{3,5}|\Phi_n^+\rangle_{4,6} =$

$$= N^2(\alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}) \times \\ (|0000\rangle_{3,5,4,6} + n|0011\rangle_{3,5,4,6} + n|1100\rangle_{3,5,4,6} + n^2|1111\rangle_{3,5,4,6}), \quad (6.2)$$

onde $N^2 = 1/\sqrt{1+n^2}$ e os quatro últimos qubits seguem o ordenamento $|35\rangle|46\rangle$. Expandindo o produto acima, ficamos com $|\phi\rangle_1|\Phi_n^+\rangle_{3,5}|\Phi_n^+\rangle_{4,6} =$

$$= N^2(\alpha'|000000\rangle + n\alpha'|000011\rangle + n\alpha'|001100\rangle + n^2\alpha'|001111\rangle)_{1,2,3,5,4,6} \\ + N^2(\beta'|010000\rangle + n\beta'|010011\rangle + n\beta'|011100\rangle + n^2\beta'|011111\rangle)_{1,2,3,5,4,6} \\ + N^2(\gamma'|100000\rangle + n\gamma'|100011\rangle + n\gamma'|101100\rangle + n^2\gamma'|101111\rangle)_{1,2,3,5,4,6} \\ + N^2(\delta'|110000\rangle + n\delta'|110011\rangle + n\delta'|111100\rangle + n^2\delta'|111111\rangle)_{1,2,3,5,4,6} . \quad (6.3)$$

Entretanto, queremos que as medidas de Alice sejam realizadas sobre os qubits $|13\rangle$ e $|24\rangle$. Assim, reescreveremos o estado acima na ordenação $|13\rangle|24\rangle|56\rangle$, com $|\phi\rangle_1|\Phi_n^+\rangle_{3,5}|\Phi_n^+\rangle_{4,6} =$

$$= N^2(\alpha'|000000\rangle + n\alpha'|000101\rangle + n\alpha'|010010\rangle + n^2\alpha'|010111\rangle)_{1,3,2,4,5,6} \\ + N^2(\beta'|001000\rangle + n\beta'|001101\rangle + n\beta'|011010\rangle + n^2\beta'|011111\rangle)_{1,3,2,4,5,6} \\ + N^2(\gamma'|100000\rangle + n\gamma'|100101\rangle + n\gamma'|110010\rangle + n^2\gamma'|110111\rangle)_{1,3,2,4,5,6}$$

$$+ N^2(\delta'|101000\rangle + n\delta'|101101\rangle + n\delta'|111010\rangle + n^2\delta'|111111\rangle)_{1,3,2,4,5,6} \quad . \quad (6.4)$$

Nosso próximo passo será apresentar o estado geral em função das medidas das bases generalizadas m_a e m_b , e o leitor já deve ter uma idéia de como fazê-lo. Tudo o que precisamos é saber como expandir o produto dos quatro primeiros *qubits* em termos destas bases, substituindo os pares $|13\rangle$ e $|24\rangle$ pelo produto tensorial das respectivas combinações associadas aos estados de m_a e m_b . Faremos um exemplo para o primeiro caso.

Vejamos o estado $|00\rangle|00\rangle$. Sabemos que cada par deste estado pode ser reescrito em termos de combinações para uma base generalizada de grau m . De acordo com a Eq. (4.14), as possíveis combinações são

$$\begin{aligned} |00\rangle &= \frac{|\Phi_m^+\rangle + m|\Phi_m^-\rangle}{\sqrt{1+m^2}}, & |01\rangle &= \frac{|\Psi_m^+\rangle + m|\Psi_m^-\rangle}{\sqrt{1+m^2}}, \\ |10\rangle &= \frac{m|\Psi_m^+\rangle - |\Psi_m^-\rangle}{\sqrt{1+m^2}}, & |11\rangle &= \frac{m|\Phi_m^+\rangle - |\Phi_m^-\rangle}{\sqrt{1+m^2}}. \end{aligned} \quad (6.5)$$

Assim, se quisermos reescrever o produto tensorial de $|00\rangle|00\rangle$ em termos de uma base com grau m_a e outra com grau m_b , basta expandir os termos associados a cada par,

$$\begin{aligned} |00\rangle|00\rangle &= \left(\frac{|\Phi_{m_a}^+\rangle + m_a|\Phi_{m_a}^-\rangle}{\sqrt{1+m_a^2}} \right) \left(\frac{|\Phi_{m_b}^+\rangle + m_b|\Phi_{m_b}^-\rangle}{\sqrt{1+m_b^2}} \right) \\ &= M_a M_b (|\Phi_{m_a}^+\rangle|\Phi_{m_b}^+\rangle + (m_b)|\Phi_{m_a}^+\rangle|\Phi_{m_b}^-\rangle + (m_a)|\Phi_{m_a}^-\rangle|\Phi_{m_b}^+\rangle + (m_a)(m_b)|\Phi_{m_a}^-\rangle|\Phi_{m_b}^-\rangle), \end{aligned} \quad (6.6)$$

onde $M_a = 1/\sqrt{1+m_a^2}$ e $M_b = 1/\sqrt{1+m_b^2}$.

Após reescrever o produto dos estados computacionais em função das bases generalizadas para todas as 16 combinações possíveis, encontramos a forma final para o estado geral; $|\phi\rangle_1|\Phi_n^+\rangle_{3,5}|\Phi_n^+\rangle_{4,6} =$

$$\begin{aligned} &= N^2 M_a M_b |\Phi_{m_a}^+\rangle_{1,3} |\Phi_{m_b}^+\rangle_{2,4} (\alpha'|00\rangle + (n)(m_b)\beta'|01\rangle + (n)(m_a)\gamma'|10\rangle + (n^2)(m_a)(m_b)\delta'|11\rangle)_{5,6} \\ &+ N^2 M_a M_b |\Phi_{m_a}^+\rangle_{1,3} |\Phi_{m_b}^-\rangle_{2,4} ((m_b)\alpha'|00\rangle - (n)\beta'|01\rangle + (n)(m_a)(m_b)\gamma'|10\rangle - (n^2)(m_a)\delta'|11\rangle)_{5,6} \\ &+ N^2 M_a M_b |\Phi_{m_a}^-\rangle_{1,3} |\Phi_{m_b}^+\rangle_{2,4} ((m_a)\alpha'|00\rangle + (n)(m_a)(m_b)\beta'|01\rangle - (n)\gamma'|10\rangle - (n^2)(m_b)\delta'|11\rangle)_{5,6} \\ &+ N^2 M_a M_b |\Phi_{m_a}^-\rangle_{1,3} |\Phi_{m_b}^-\rangle_{2,4} ((m_a)(m_b)\alpha'|00\rangle - (n)(m_a)\beta'|01\rangle - (n)(m_b)\gamma'|10\rangle + (n^2)\delta'|11\rangle)_{5,6} \\ &+ N^2 M_a M_b |\Phi_{m_a}^+\rangle_{1,3} |\Psi_{m_b}^+\rangle_{2,4} ((n)\alpha'|01\rangle + (m_b)\beta'|00\rangle + (n^2)(m_a)\gamma'|11\rangle + (n)(m_a)(m_b)\delta'|10\rangle)_{5,6} \\ &+ N^2 M_a M_b |\Phi_{m_a}^+\rangle_{1,3} |\Psi_{m_b}^-\rangle_{2,4} ((n)(m_b)\alpha'|01\rangle - \beta'|00\rangle + (n^2)(m_a)(m_b)\gamma'|11\rangle - (n)(m_a)\delta'|10\rangle)_{5,6} \\ &+ N^2 M_a M_b |\Phi_{m_a}^-\rangle_{1,3} |\Psi_{m_b}^+\rangle_{2,4} ((n)(m_a)\alpha'|01\rangle + (m_a)(m_b)\beta'|00\rangle - (n^2)\gamma'|11\rangle - (n)(m_b)\delta'|10\rangle)_{5,6} \\ &+ N^2 M_a M_b |\Phi_{m_a}^-\rangle_{1,3} |\Psi_{m_b}^-\rangle_{2,4} ((n)(m_a)(m_b)\alpha'|01\rangle - (m_a)\beta'|00\rangle - (n^2)(m_b)\gamma'|11\rangle + (n)\delta'|10\rangle)_{5,6} \end{aligned}$$

$$\begin{aligned}
& +N^2M_aM_b|\Psi_{m_a}^+\rangle_{1,3}|\Phi_{m_b}^+\rangle_{2,4} \left((n)\alpha'|10\rangle + (n^2)(m_b)\beta'|11\rangle + (m_a)\gamma'|00\rangle + (n)(m_a)(m_b)\delta'|01\rangle \right)_{5,6} \\
& +N^2M_aM_b|\Psi_{m_a}^+\rangle_{1,3}|\Phi_{m_b}^-\rangle_{2,4} \left((n)(m_b)\alpha'|10\rangle - (n^2)\beta'|11\rangle + (m_a)(m_b)\gamma'|00\rangle - (n)(m_a)\delta'|01\rangle \right)_{5,6} \\
& +N^2M_aM_b|\Psi_{m_a}^-\rangle_{1,3}|\Phi_{m_b}^+\rangle_{2,4} \left((n)(m_a)\alpha'|10\rangle + (n^2)(m_a)(m_b)\beta'|11\rangle - \gamma'|00\rangle - (n)(m_b)\delta'|01\rangle \right)_{5,6} \\
& +N^2M_aM_b|\Psi_{m_a}^-\rangle_{1,3}|\Phi_{m_b}^-\rangle_{2,4} \left((m_a)(m_b)(n)\alpha'|10\rangle - (n^2)(m_a)\beta'|11\rangle - (m_b)\gamma'|00\rangle + (n)\delta'|01\rangle \right)_{5,6} \\
& +N^2M_aM_b|\Psi_{m_a}^+\rangle_{1,3}|\Psi_{m_b}^+\rangle_{2,4} \left((n^2)\alpha'|11\rangle + (n)(m_b)\beta'|10\rangle + (n)(m_a)\gamma'|01\rangle + (m_a)(m_b)\delta'|00\rangle \right)_{5,6} \\
& +N^2M_aM_b|\Psi_{m_a}^+\rangle_{1,3}|\Psi_{m_b}^-\rangle_{2,4} \left((n^2)(m_b)\alpha'|11\rangle - (n)\beta'|10\rangle + (n)(m_a)(m_b)\gamma'|01\rangle - (m_a)\delta'|00\rangle \right)_{5,6} \\
& +N^2M_aM_b|\Psi_{m_a}^-\rangle_{1,3}|\Psi_{m_b}^+\rangle_{2,4} \left((n^2)(m_a)\alpha'|11\rangle + (n)(m_a)(m_b)\beta'|10\rangle - (n)\gamma'|01\rangle - (m_b)\delta'|00\rangle \right)_{5,6} \\
& +N^2M_aM_b|\Psi_{m_a}^-\rangle_{1,3}|\Psi_{m_b}^-\rangle_{2,4} \left((n^2)(m_a)(m_b)\alpha'|11\rangle - (n)(m_a)\beta'|10\rangle - (n)(m_b)\gamma'|01\rangle_{5,6} + \delta'|00\rangle \right)_{5,6}.
\end{aligned} \tag{6.7}$$

A expressão acima pode parecer complicada, mas ainda não fizemos nenhuma consideração para casos particulares. Ao escolher devidamente os parâmetros das bases e dos *qubits* originais, reduzimos o estado geral para formas mais simples de serem trabalhadas e elaboramos protocolos tão eficientes quanto os dos capítulo 5. Muitos testes foram realizados, e mostraremos aqueles que obtiveram os melhores resultados nas seções a seguir. Ao final do capítulo, comentaremos sobre outras alternativas.

6.1.1 Escolhendo $m_a=m_b=n$.

Embora a eficiência deste cenário esteja aquém do valor que buscamos ($P_{suc}^{total} = 2n^2/1+n^2$), escolhemos comentá-lo primeiro para destacar uma característica que não será encontrada em nenhum outro caso para dois *qubits*. Para uma condição especial, existem quatro opções possíveis para o teleporte direto do estado original com fidelidade um, e, nestes casos, o processo pode chegar ao fim sem que em momento algum tenhamos qualquer informação sobre o estado inicial de Alice. Em outras palavras, o teleporte ocorre para qualquer estado arbitrário de dois *qubits*, e a escolha de parâmetros $m_a=m_b=n$ é a única que viabiliza esta condição. Nos modelos seguintes, precisaremos manipular um estado de um *qubit* para associá-lo a outro conhecido, e o resultado será o estado original de Alice. Só o fato de conhecermos um dos *qubits* já revela que estado seguinte não pode ser totalmente arbitrário, e o número de parâmetros livres será menor. Portanto, se quisermos teleportar um estado de dois *qubits* sobre o qual não temos conhecimento de sua origem devemos utilizar este método, cujo sucesso está associado às medidas de $|\Phi_{m_a}^-\rangle_{1,3}|\Phi_{m_b}^-\rangle_{2,4}$, $|\Phi_{m_a}^-\rangle_{1,3}|\Psi_{m_b}^+\rangle_{2,4}$, $|\Psi_{m_a}^+\rangle_{1,3}|\Phi_{m_b}^-\rangle_{2,4}$, ou $|\Psi_{m_a}^+\rangle_{1,3}|\Psi_{m_b}^+\rangle_{2,4}$. A probabilidade total é igual a

$$\begin{aligned}
P_{suc}^{total} &= 4 \times |N^2M_aM_b \times n^2|^2 = 4 \times \left| \frac{n^2}{(1+n^2)\sqrt{(1+n^2)}\sqrt{(1+n^2)}} \right|^2 = 4 \times \left| \frac{n^2}{(1+n^2)^2} \right|^2 = \frac{4n^4}{(1+n^2)^4} \\
&= \left(\frac{2n^2}{(1+n^2)^2} \right)^2, \tag{6.8}
\end{aligned}$$

lembrando que $2n^2/(1+n^2)^2$ é o resultado obtido na Eq. (4.18) para o teleporte de um único *qubit* em apenas um canal.

A relação entre estas expressões não ocorre por acaso, já que agora estamos teleportando dois *qubits* e desejamos que ocorra êxito em ambos os canais. Dessa forma, a probabilidade final será o produto das probabilidades individuais associadas a cada canal, o que concorda com o resultado que acabamos de mostrar.

Para os estados restantes, tentamos aplicar as técnicas de correção com matrizes apresentadas no capítulo 5 adaptadas para o caso de dois *qubits*, e não foi possível determinar uma transformação que corrigisse estes estados em sua forma geral, visto que as condições de unitariedade que a transformação deveria obedecer não eram totalmente satisfeitas. Todavia, obtivemos êxito para casos particulares que comentaremos nas próximas seções.

6.1.2 Enviando $\alpha|00\rangle + \beta|11\rangle$.

Se nosso objetivo for maximizar a probabilidade de sucesso, não podemos trabalhar com um estado qualquer como no cenário anterior, pois precisamos reduzir o número de parâmetros desconhecidos na Eq. (6.7). Uma maneira viável seria construir o estado de dois *qubits* a partir de outros mais simples, para, então, ponderar sobre as escolhas adequadas de m_a e m_b em cada modelo específico. Nesta seção e na próxima, vamos mostrar que é possível construir estados emaranhados a partir de $\alpha|0\rangle + \beta|1\rangle$ e como atingir o valor de $P_{suc}^{total} = 2n^2/1+n^2$.

Suponha que temos posse de um *qubit* qualquer representado por $\alpha|0\rangle_1 + \beta|1\rangle_1$ e acrescentamos ao sistema um novo *qubit* que seja conhecido, como $|0\rangle_2$. Assumindo que o sistema esteja isolado, seu estado geral será $\alpha|00\rangle_{1,2} + \beta|10\rangle_{1,2}$. Aplicando então uma porta $CNOT_{1,2}$ com o controle no primeiro *qubit* e o alvo no segundo, nosso estado agora passa a ser $\alpha|00\rangle_{1,2} + \beta|11\rangle_{1,2}$. Se compararmos esta expressão com a Eq. (6.1),

$$|\phi\rangle_1 = \alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}, \quad (6.9)$$

perceberemos que ambas representam o mesmo estado quando $\alpha = \alpha'$, $\beta = \delta'$ e $\beta' = \gamma' = 0$.

Nestas condições, é fácil perceber que a Eq. (6.7) assume uma forma mais simples. Vários testes foram realizados com m_a e m_b assumindo diferentes valores, e aqueles que maximizam a probabilidade total ocorrem para $m_a = m_b = 1$, ou seja, quando Alice mede os dois pares na Base de Bell. Com estas considerações, o sistema é reduzido a $|\phi\rangle_1 |\Phi_n^+\rangle_{3,5} |\Phi_n^+\rangle_{4,6} =$

$$\begin{aligned} &= N^2 |\Phi_{m_a}^+\rangle_{1,3} |\Phi_{m_b}^+\rangle_{2,4} (\alpha|00\rangle + (n^2)\beta|11\rangle)_{5,6} + N^2 |\Phi_{m_a}^+\rangle_{1,3} |\Phi_{m_b}^-\rangle_{2,4} (\alpha|00\rangle - (n^2)\beta|11\rangle)_{5,6} \\ &+ N^2 |\Phi_{m_a}^-\rangle_{1,3} |\Phi_{m_b}^+\rangle_{2,4} (\alpha|00\rangle - (n^2)\beta|11\rangle)_{5,6} + N^2 |\Phi_{m_a}^-\rangle_{1,3} |\Phi_{m_b}^-\rangle_{2,4} (\alpha|00\rangle + (n^2)\beta|11\rangle)_{5,6} \end{aligned}$$

$$\begin{aligned}
& +N^2|\Phi_{ma}^+\rangle_{1,3}|\Psi_{mb}^+\rangle_{2,4}((n)\alpha|01\rangle + (n)\beta|10\rangle)_{5,6} + N^2|\Phi_{ma}^+\rangle_{1,3}|\Psi_{mb}^-\rangle_{2,4}((n)\alpha|01\rangle - (n)\beta|10\rangle)_{5,6} \\
& +N^2|\Phi_{ma}^-\rangle_{1,3}|\Psi_{mb}^+\rangle_{2,4}((n)\alpha|01\rangle - (n)\beta|10\rangle)_{5,6} + N^2|\Phi_{ma}^-\rangle_{1,3}|\Psi_{mb}^-\rangle_{2,4}((n)\alpha|01\rangle + (n)\beta|10\rangle)_{5,6} \\
& +N^2|\Psi_{ma}^+\rangle_{1,3}|\Phi_{mb}^+\rangle_{2,4}((n)\alpha|10\rangle + (n)\beta|01\rangle)_{5,6} + N^2|\Psi_{ma}^+\rangle_{1,3}|\Phi_{mb}^-\rangle_{2,4}((n)\alpha|10\rangle - (n)\beta|01\rangle)_{5,6} \\
& +N^2|\Psi_{ma}^-\rangle_{1,3}|\Phi_{mb}^+\rangle_{2,4}((n)\alpha|10\rangle - (n)\beta|01\rangle)_{5,6} + N^2|\Psi_{ma}^-\rangle_{1,3}|\Phi_{mb}^-\rangle_{2,4}((n)\alpha|10\rangle + (n)\beta|01\rangle)_{5,6} \\
& +N^2|\Psi_{ma}^+\rangle_{1,3}|\Psi_{mb}^+\rangle_{2,4}((n^2)\alpha|11\rangle + \beta|00\rangle)_{5,6} + N^2|\Psi_{ma}^+\rangle_{1,3}|\Psi_{mb}^-\rangle_{2,4}((n^2)\alpha|11\rangle - \beta|00\rangle)_{5,6} \\
& +N^2|\Psi_{ma}^-\rangle_{1,3}|\Psi_{mb}^+\rangle_{2,4}((n^2)\alpha|11\rangle - \beta|00\rangle)_{5,6} + N^2|\Psi_{ma}^-\rangle_{1,3}|\Psi_{mb}^-\rangle_{2,4}((n^2)\alpha|11\rangle + \beta|00\rangle)_{5,6}.
\end{aligned} \tag{6.10}$$

Se o leitor analisar rapidamente a expressão acima notará que as medidas de

$$\begin{aligned}
& |\Phi_{ma}^+\rangle_{1,3}|\Psi_{mb}^+\rangle_{2,4}, |\Phi_{ma}^+\rangle_{1,3}|\Psi_{mb}^-\rangle_{2,4}, |\Phi_{ma}^-\rangle_{1,3}|\Psi_{mb}^+\rangle_{2,4}, |\Phi_{ma}^-\rangle_{1,3}|\Psi_{mb}^-\rangle_{2,4}, \\
& |\Psi_{ma}^+\rangle_{1,3}|\Phi_{mb}^+\rangle_{2,4}, |\Psi_{ma}^+\rangle_{1,3}|\Phi_{mb}^-\rangle_{2,4}, |\Psi_{ma}^-\rangle_{1,3}|\Phi_{mb}^+\rangle_{2,4}, |\Psi_{ma}^-\rangle_{1,3}|\Phi_{mb}^-\rangle_{2,4}.
\end{aligned} \tag{6.11}$$

estão associadas à transmissão direta do estado inicial. Para estes casos, o teleporte ocorre com sucesso sem que Alice e Bob precisem conhecer o grau de emaranhamento dos canais, desde que estes possuam o mesmo valor. Este fato merece destaque visto que em nenhum dos protocolos discutidos nos outros capítulos tal cenário poderia ocorrer. Se estivermos trabalhando com dispositivos reais e a única informação disponível sobre os canais é a de que ambos sejam semelhantes, saberemos que o teleporte ocorrerá perfeitamente para qualquer uma das seqüências de medidas descritas.

Uma análise mais cuidadosa revela que existem somente dois tipos de estrutura; a primeira, com grau de emaranhamento igual a n^2 , e a segunda, que nos remete a um estado semelhante à $\alpha|0\rangle + \beta|1\rangle$ (não fosse a presença do segundo *qubit* em cada coeficiente) e que está associada às medidas citadas acima. Neste ponto é preciso destacar uma característica deste método que não poderia ser discutida em outras seções. Podemos extrair facilmente o estado de dois *qubits* enviado por Alice e - se quisermos ir além - refiná-lo até obter o primeiro estado utilizado em todo o processo, $\alpha|0\rangle + \beta|1\rangle$. Portanto, o método funciona para o envio tanto de dois como para o de um único *qubit*, e, a princípio, podemos utilizá-lo como substituto para os mecanismos que utilizam somente um canal. Contudo, precisamos saber primeiro se as eficiências de ambos serão semelhantes.

Vamos mostrar inicialmente como recuperar o estado de Alice nas duas formas que acabamos de discutir através de um exemplo. Suponha que o resultado da medida tenha fornecido $|\Psi_{ma}^-\rangle_{1,3}|\Phi_{mb}^-\rangle_{2,4}$, o qual está associado a $\alpha|10\rangle_{5,6} + \beta|01\rangle_{5,6}$. Aplicando uma porta *NOT* simples (σ_x) no *qubit* 5, modificamos o estado final para $\alpha|00\rangle_{5,6} + \beta|11\rangle_{5,6}$: esta já é a informação enviada por Alice.

Se quisermos refiná-la ainda mais, aplicamos uma $CNOT_{5,6}$ com o controle em 5 e o alvo em 6 para obter $\alpha|00\rangle_{5,6} + \beta|10\rangle_{5,6} \Rightarrow (\alpha|0\rangle_5 + \beta|1\rangle_5)|0\rangle_6$. Ao medir o

qubit 6, colapsamos este para $|0\rangle_6$ e o estado anterior para $\alpha|0\rangle_5 + \beta|1\rangle_5$. Assim, Bob pode ter acesso tanto ao primeiro estado manipulado por Alice como à informação final enviada pela mesma na forma de dois *qubits*, e a seqüência total de operações dependerá do objetivo de ambos. Neste caso, se tivéssemos aplicado a porta *CNOT* antes de σ_x sobre os mesmos índices também encontraríamos $\alpha|0\rangle_5 + \beta|1\rangle_5$.

Outro fato que merece destaque é o de que a probabilidade de obter $\alpha|00\rangle_{5,6} + \beta|11\rangle_{5,6}$ é a mesma de obter $\alpha|0\rangle_5 + \beta|1\rangle_5$. A explicação reside no exemplo que acabamos de mostrar: para reduzir o estado de dois *qubits* a dois estados separáveis de um *qubit* utilizamos apenas transformações unitárias simples, sem afetar a norma e a fidelidade do estado. Dessa forma, para qualquer uma das duas análises, só precisamos calcular a probabilidade final uma vez. Para determiná-la, observe que as oito probabilidades individuais de sucesso direto são iguais. Seu respectivo valor é de

$$\frac{n^2}{4(1+n^2)^2}. \quad (6.12)$$

Ao multiplicar este valor por 8, determinamos a probabilidade total de sucesso, que é igual a

$$P_{suc} = \frac{2n^2}{(1+n^2)^2}, \quad (6.13)$$

e novamente nos deparamos com a expressão encontrada na Eq. (4.18).

Se quisermos elaborar uma analogia com o caso de um *qubit*, precisamos retornar à seção 4.3.1. Lembre-se de que a primeira etapa consistia de um teleporte através de um canal com grau n e medidas na base de Bell. Entretanto, não havia êxito direto para nenhuma das quatro possibilidades, algo que só foi ocorrer na etapa seguinte. Como mostramos anteriormente, o protocolo desta seção é bem-sucedido para metade dos casos após o primeiro teleporte.

Agora que já sabemos como corrigir estados imperfeitos, podemos prosseguir com nossa análise e aplicar as técnicas mostradas no capítulo 5 sobre os estados restantes. Após reduzi-los a estados de um *qubit*, o procedimento será o mesmo utilizado nas Eqs. (5.30),(5.31),(5.32),(5.33) e (5.34), cujo resultado final é de

$$P_{suc}^{corr} = \frac{2n^4}{(1+n^2)^2}. \quad (6.14)$$

Somando-se os dois valores, encontramos

$$P_{suc}^{total} = P_{suc} + P_{suc}^{corr} = \frac{2n^2}{(1+n^2)^2} + \frac{2n^4}{(1+n^2)^2} = \frac{2n^2}{1+n^2}. \quad (6.15)$$

Se basearmos nossa análise apenas na eficiência deste protocolo, o resultado

acima comprova que este método pode substituir os procedimentos vistos em outros capítulos. Para fins práticos, no entanto, um dispositivo que opere com dois canais seria mais difícil de ser construído e controlado, e seriam necessários alguns argumentos que justificasse sua utilização. Um deles seria a capacidade de teleportar não somente um mas dois *qubits*.

Outros valores para m_a e m_b .

Ao testar outros valores para m_a e m_b relacionados ao envio do estado $\alpha|00\rangle + \beta|11\rangle$, encontramos resultados sempre inferiores a $P_{suc}^{total} = 2n^2/1 + n^2$. Listaremos a seguir os principais testes, que foram divididos em três categorias. O caso em que $m_a = m_b = 1$ também foi incluído.

Para $m_a = 1$:

- (1) $m_a = 1$ e $m_b = 1$, com $P_{suc}^{total} = 2n^2/1 + n^2$.
- (2) $m_a = 1$ e $m_b = n$, com $P_{suc}^{total} = 6n^4 + 2n^6/(1 + n^2)^3$.
- (3) $m_a = 1$ e $m_b = n^2$, com $P_{suc}^{total} = 2n^4/1 + n^4$.

Para $m_a = n$:

- (1) $m_a = n$ e $m_b = 1$, com $P_{suc}^{total} = 6n^4 + 2n^6/(1 + n^2)^3$.
- (2) $m_a = n$ e $m_b = n$, com $P_{suc}^{total} = 6n^4 + 2n^6/(1 + n^2)^3$.
- (3) $m_a = n$ e $m_b = n^2$, com $P_{suc}^{total} = 8n^6 + 6n^8 + 2n^{10}/(1 + n^2)^3(1 + n^4)$.

Para $m_a = n^2$:

- (1) $m_a = n^2$ e $m_b = 1$, com $P_{suc}^{total} = 2n^4/1 + n^4$.
- (2) $m_a = n^2$ e $m_b = n$, com $P_{suc}^{total} = 8n^6 + 6n^8 + 2n^{10}/(1 + n^2)^3(1 + n^4)$.
- (3) $m_a = n^2$ e $m_b = n^2$, com $P_{suc}^{total} = 4n^6 + 6n^8 + 4n^{10} + 2n^{12}/(1 + n^2)^2(1 + n^4)$.

Realizamos testes numéricos para diferentes valores de P_{suc}^{total} no intervalo $0 < n < 1$ e nenhum resultado supera aquele em que escolhemos a base de Bell para m_a e m_b . Porém, consideramos em todos os testes medidas independentes dos pares de *qubits* relacionados aos índices 1, 3 e 2, 4, e, na seção seguinte, mostraremos que estas podem ser realizadas em momentos distintos, no qual a segunda medida é condicionada ao resultado da primeira.

Condiccionando a segunda medida ao resultado da primeira.

Os resultados dos testes acima mostram a ineficiência na escolha de outros valores para m_a e m_b . Entretanto, havíamos sempre considerado medidas independentes dos dois pares em posse de Alice. Mas e se as medidas fossem feitas em momentos distintos? Alice poderia medir o primeiro par e observar o resultado para decidir posteriormente que tipo de medida implementaria no segundo par. Se houvesse uma mudança no valor de m_b para cada resultado individual obtido na primeira medida ($|\Phi_{m_a}^+\rangle_{1,3}$, $|\Phi_{m_a}^-\rangle_{1,3}$, $|\Psi_{m_a}^+\rangle_{1,3}$, $|\Psi_{m_a}^-\rangle_{1,3}$), talvez a probabilidade final fosse diferente. Se este fosse o caso, Alice poderia montar uma tabela condicionando a melhor escolha para o valor de m_b dado o estado obtido ao medir o primeiro par.

Façamos um exemplo. Suponha que quatro tentativas tenham sido realizadas independentemente e que a ordem dos resultados foi de $|\Phi_{m_a}^-\rangle_{1,3}$, $|\Psi_{m_a}^+\rangle_{1,3}$, $|\Phi_{m_a}^+\rangle_{1,3}$ e $|\Psi_{m_a}^-\rangle_{1,3}$. Ora, se escolhêssemos $m_b = 1$ para todos os casos sabemos que $P_{suc}^{total} = 2n^2/1 + n^2$. Mas e se ajustássemos $m_b = 1$ para os dois primeiros e $m_b = n$ para os restantes?

Diante dessa questão, calculamos todas as possibilidades envolvendo os valores de m_a e m_b mostrados na seção 6.1.2 e realizamos testes numéricos que indicaram quais seriam as melhores escolhas para o valor de m_b depois de conhecer o estado associado à medida na base com grau m_a . Mesmo para esta abordagem, não houve melhora no valor da probabilidade final de sucesso com a mudança de parâmetros, e a escolha de $m_a = m_b = 1$ continua sendo a mais vantajosa.

Nas duas seções seguintes abordaremos novamente protocolos que envolvam estados GHZ.

6.2 Base GHZ e Canal GHZ

Em todas as considerações feitas desde o início deste capítulo utilizamos os canais (com grau n) e as bases de medidas (com grau m) com a mesma estrutura vista nos primeiros protocolos do capítulo 4. Retomaremos nesta seção e na próxima o uso de estados GHZ vistos na seção 5.3 para testá-los em novas aplicações, sempre tendo em vista o envio do estado em sua forma geral,

$$|\phi\rangle_{1,2} = \alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}. \quad (6.16)$$

O método que mostraremos a seguir têm uma ligação direta com aquele que apresentamos na seção 5.3. Enquanto o último utilizava um canal GHZ de três *qubits* para transmitir o estado $\alpha|0\rangle_1 + \beta|1\rangle_1$, o atual dispõe de um canal com quatro *qubits* para enviar o estado $\alpha|00\rangle_{1,2} + \beta|11\rangle_{1,2}$. De uma forma geral, os procedimentos são semelhantes, e a diferença básica reside no número de *qubits* envolvidos no processo e nos cálculos. Na

figura 6.2 podemos entender com mais clareza como o processo funciona. Visto que o

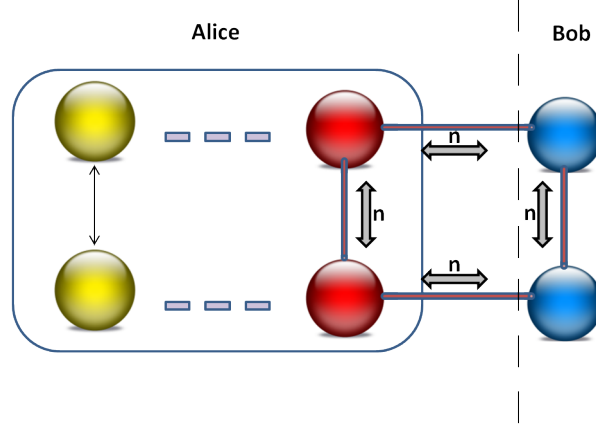


Figura 6.2: Teleporte de dois qubits utilizando um canal GHZ generalizado e medidas na base GHZ generalizada.

canal é constituído por quatro *qubits*, precisamos de $2^4 = 16$ estados ortonormais para estabelecer a base de medidas que será utilizada por Alice. Para não haver confusão com os oito estados mostrados na Eq. (5.15), vamos atribuir a cada um dos novos uma notação que ainda não tenha sido utilizada. O canal agora será descrito por

$$|A_n^+\rangle_{3,5,4,6} = \frac{|0000\rangle_{3,5,4,6} + n|1111\rangle_{3,5,4,6}}{\sqrt{1+n^2}}. \quad (6.17)$$

e a forma destes 16 novos estados e suas respectivas denominações escolhidas estão listadas abaixo:

$$\begin{aligned} |A_m^+\rangle &= \frac{|0000\rangle + m|1111\rangle}{\sqrt{1+m^2}}, & |A_m^-\rangle &= \frac{m|0000\rangle - |1111\rangle}{\sqrt{1+m^2}}, & |B_m^+\rangle &= \frac{|1110\rangle + m|0001\rangle}{\sqrt{1+m^2}}, & |B_m^-\rangle &= \frac{m|1110\rangle - |0001\rangle}{\sqrt{1+m^2}}, \\ |C_m^+\rangle &= \frac{|0010\rangle + m|1101\rangle}{\sqrt{1+m^2}}, & |C_m^-\rangle &= \frac{m|0010\rangle - |1101\rangle}{\sqrt{1+m^2}}, & |D_m^+\rangle &= \frac{|1100\rangle + m|0011\rangle}{\sqrt{1+m^2}}, & |D_m^-\rangle &= \frac{m|1100\rangle - |0011\rangle}{\sqrt{1+m^2}}, \\ |E_m^+\rangle &= \frac{|0100\rangle + m|1011\rangle}{\sqrt{1+m^2}}, & |E_m^-\rangle &= \frac{m|0100\rangle - |1011\rangle}{\sqrt{1+m^2}}, & |F_m^+\rangle &= \frac{|1010\rangle + m|0101\rangle}{\sqrt{1+m^2}}, & |F_m^-\rangle &= \frac{m|1010\rangle - |0101\rangle}{\sqrt{1+m^2}}, \\ |J_m^+\rangle &= \frac{|0110\rangle + m|1001\rangle}{\sqrt{1+m^2}}, & |J_m^-\rangle &= \frac{m|0110\rangle - |1001\rangle}{\sqrt{1+m^2}}, & |K_m^+\rangle &= \frac{|1000\rangle + m|0111\rangle}{\sqrt{1+m^2}}, & |K_m^-\rangle &= \frac{m|1000\rangle - |0111\rangle}{\sqrt{1+m^2}}; \end{aligned} \quad (6.18)$$

onde $0 < m < 1$. Efetuando o produto tensorial entre o *qubit* $|\phi\rangle_{1,2}$ e o canal $|A_n^+\rangle_{3,5,4,6}$, determinamos o estado geral do sistema,

$$|\phi\rangle_{1,2}|A_n^+\rangle_{3,5,4,6} = N^2(\alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2})(|0000\rangle_{3,5,4,6} + n|1111\rangle_{3,5,4,6}). \quad (6.19)$$

Já vimos que a ordem dos índices deve ser alterada para que estes fiquem de acordo com os *qubits* que Alice irá medir. Seguindo os mesmos passos da seção 5.3,

escolhemos a ordem $|132456\rangle$, em que $|\phi\rangle_{1,2}|A_n^+\rangle_{3,5,4,6} =$

$$\begin{aligned} &= N^2(\alpha'|000000\rangle + n\alpha'|001111\rangle)_{1,3,2,4,5,6} + N^2(\beta'|010000\rangle + n\beta'|011111\rangle)_{1,3,2,4,5,6}, \\ &+ N^2(\gamma'|100000\rangle + n\gamma'|101111\rangle)_{1,3,2,4,5,6} + N^2(\delta'|110000\rangle + n\delta'|111111\rangle)_{1,3,2,4,5,6}. \end{aligned} \quad (6.20)$$

Ao ordenar os 16 estados da base computacional em função dos estados GHZ,

$$\begin{aligned} |0000\rangle &= \frac{|A_m^+\rangle + m|A_m^-\rangle}{\sqrt{1+m^2}}, & |0001\rangle &= \frac{m|B_m^+\rangle - |B_m^-\rangle}{\sqrt{1+m^2}}, & |0010\rangle &= \frac{|C_m^+\rangle + m|C_m^-\rangle}{\sqrt{1+m^2}}, & |0011\rangle &= \frac{m|D_m^+\rangle - |D_m^-\rangle}{\sqrt{1+m^2}}, \\ |0100\rangle &= \frac{|E_m^+\rangle + m|E_m^-\rangle}{\sqrt{1+m^2}}, & |0101\rangle &= \frac{m|F_m^+\rangle - |F_m^-\rangle}{\sqrt{1+m^2}}, & |0110\rangle &= \frac{|J_m^+\rangle + m|J_m^-\rangle}{\sqrt{1+m^2}}, & |0111\rangle &= \frac{m|K_m^+\rangle - |K_m^-\rangle}{\sqrt{1+m^2}}, \\ |1000\rangle &= \frac{|K_m^+\rangle + m|K_m^-\rangle}{\sqrt{1+m^2}}, & |1001\rangle &= \frac{m|J_m^+\rangle - |J_m^-\rangle}{\sqrt{1+m^2}}, & |1010\rangle &= \frac{|F_m^+\rangle + m|F_m^-\rangle}{\sqrt{1+m^2}}, & |1011\rangle &= \frac{m|E_m^+\rangle - |E_m^-\rangle}{\sqrt{1+m^2}}, \\ |1100\rangle &= \frac{|D_m^+\rangle + m|D_m^-\rangle}{\sqrt{1+m^2}}, & |1101\rangle &= \frac{m|C_m^+\rangle - |C_m^-\rangle}{\sqrt{1+m^2}}, & |1110\rangle &= \frac{|B_m^+\rangle + m|B_m^-\rangle}{\sqrt{1+m^2}}, & |1111\rangle &= \frac{m|A_m^+\rangle - |A_m^-\rangle}{\sqrt{1+m^2}}, \end{aligned} \quad (6.21)$$

temos condições de reescrever o estado geral do sistema, que agora será $|\phi\rangle_{1,2}|A_n^+\rangle_{3,5,4,6} =$

$$\begin{aligned} &= MN\alpha' (|A_m^+\rangle + m|A_m^-\rangle) |00\rangle_{56} + MNn\alpha' (m|F_m^+\rangle - |F_m^-\rangle) |11\rangle_{56} \\ &+ MN\beta' (|C_m^+\rangle + m|C_m^-\rangle) |00\rangle_{56} + MNn\beta' (m|K_m^+\rangle - |K_m^-\rangle) |11\rangle_{56} \\ &+ MN\gamma' (|K_m^+\rangle + m|K_m^-\rangle) |00\rangle_{56} + MNn\gamma' (m|C_m^+\rangle - |C_m^-\rangle) |11\rangle_{56} \\ &+ MN\delta' (|F_m^+\rangle + m|F_m^-\rangle) |00\rangle_{56} + MNn\delta' (m|A_m^+\rangle - |A_m^-\rangle) |11\rangle_{56} \quad . \end{aligned} \quad (6.22)$$

Sabemos que os estados GHZ generalizados são ortogonais, e que a base de medida escolhida por Alice deve conter todos os 16 estados. Nosso próximo passo será reagrupá-los em função dos *qubits* 5 e 6 de Bob, mas, antes, é preciso fazer uma observação. Note que se olharmos para os quatro primeiros *qubits* em todos os "kets" na Eq. (6.20), veremos que apenas metade dos estados da base computacional aparecem na expressão, pois somente oito estão associados a algum coeficiente (α' e β' ou γ' e δ') oriundos do estado enviado por Alice. Sendo assim, não podemos esperar que nos cálculos seguintes todos os coeficientes estejam associados a algum estado da base GHZ generalizada, e, de fato, a expressão seguinte valida esta afirmação. O estado geral com as normalizações agora se apresenta como $|\phi\rangle_{1,2}|A_n^+\rangle_{3,5,4,6} =$

$$\begin{aligned} &= \left[\frac{\sqrt{(\alpha')^2 + (mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |A_m^+\rangle \left(\frac{\alpha'|00\rangle_{56} + mn\delta'|11\rangle_{56}}{\sqrt{(\alpha')^2 + (mn\delta')^2}} \right) + \left[\frac{\sqrt{(m\alpha')^2 + (-n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |A_m^-\rangle \left(\frac{m\alpha'|00\rangle_{56} - n\delta'|11\rangle_{56}}{\sqrt{(m\alpha')^2 + (-n\delta')^2}} \right) \\ &+ \left[\frac{\sqrt{(mn\alpha')^2 + (\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |F_m^+\rangle \left(\frac{mn\alpha'|00\rangle_{56} + \delta'|11\rangle_{56}}{\sqrt{(mn\alpha')^2 + (\delta')^2}} \right) + \left[\frac{\sqrt{(-n\alpha')^2 + (m\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |F_m^-\rangle \left(\frac{-n\alpha'|00\rangle_{56} + m\delta'|11\rangle_{56}}{\sqrt{(-n\alpha')^2 + (m\delta')^2}} \right) \\ &+ \left[\frac{\sqrt{(\beta')^2 + (mn\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |C_m^+\rangle \left(\frac{\beta'|00\rangle_{56} + mn\gamma'|11\rangle_{56}}{\sqrt{(\beta')^2 + (mn\gamma')^2}} \right) + \left[\frac{\sqrt{(m\beta')^2 + (-n\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |C_m^-\rangle \left(\frac{m\beta'|00\rangle_{56} - n\gamma'|11\rangle_{56}}{\sqrt{(m\beta')^2 + (-n\gamma')^2}} \right) \end{aligned}$$

$$+ \left[\frac{\sqrt{(mn\beta')^2 + (\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |K_m^+\rangle \left(\frac{mn\beta' |00\rangle_{56} + \gamma' |11\rangle_{56}}{\sqrt{(mn\beta')^2 + (\gamma')^2}} \right) + \left[\frac{\sqrt{(-n\beta')^2 + (m\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |K_m^-\rangle \left(\frac{-n\beta' |00\rangle_{56} + m\gamma' |11\rangle_{56}}{\sqrt{(-n\beta')^2 + (m\gamma')^2}} \right); \quad (6.23)$$

e repare que apenas dois dos coeficientes do estado inicial (α' e β' ou γ' e δ') aparecem associados a um único estado da base de medida.

Agora, é preciso efetuar novas considerações. Para qualquer que seja a medida de Alice, jamais o estado $|\phi\rangle_{1,2} = \alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}$ será transmitido integralmente, ou, em outras palavras, com fidelidade um. Não existe correção para este caso. Tudo o que podemos fazer é particularizar esta forma geral para algum caso conhecido, e então refazer os cálculos desde o início visando a transmissão deste estado particular.

Uma opção viável seria considerarmos novamente o estado $\alpha|00\rangle_{1,2} + \beta|11\rangle_{1,2}$, e já vimos que para que exista correspondência entre este caso e a expressão geral as condições $\alpha = \alpha'$, $\beta = \delta'$ e $\beta' = \gamma' = 0$ devem ser satisfeitas. Neste cenário, o estado geral do sistema será somente $|\phi\rangle_{1,2} |A_n^+\rangle_{3,5,4,6} =$

$$= \left[\frac{\sqrt{(\alpha')^2 + (mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |A_m^+\rangle \left(\frac{\alpha' |00\rangle_{56} + mn\delta' |11\rangle_{56}}{\sqrt{(\alpha')^2 + (mn\delta')^2}} \right) + \left[\frac{\sqrt{(m\alpha')^2 + (-n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |A_m^-\rangle \left(\frac{m\alpha' |00\rangle_{56} - n\delta' |11\rangle_{56}}{\sqrt{(m\alpha')^2 + (-n\delta')^2}} \right) \\ + \left[\frac{\sqrt{(mn\alpha')^2 + (\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |F_m^+\rangle \left(\frac{mn\alpha' |00\rangle_{56} + \delta' |11\rangle_{56}}{\sqrt{(mn\alpha')^2 + (\delta')^2}} \right) + \left[\frac{\sqrt{(-n\alpha')^2 + (m\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |F_m^-\rangle \left(\frac{-n\alpha' |00\rangle_{56} + m\delta' |11\rangle_{56}}{\sqrt{(-n\alpha')^2 + (m\delta')^2}} \right), \quad (6.24)$$

já que os coeficientes β' e γ' são nulos. Assim, nos deparamos com apenas quatro tipos de estrutura que Bob pode receber: $\alpha|00\rangle_{56} + mn\delta'|11\rangle_{56}$, $m\alpha|00\rangle_{56} - n\delta'|11\rangle_{56}$, $n\alpha|00\rangle_{56} + m\delta'|11\rangle_{56}$, $mn\alpha|00\rangle_{56} - \delta'|11\rangle_{56}$. Vamos analisar então duas possibilidades:

(1) $m = 1$:

Neste caso, não há sucesso direto na transmissão. Bob precisará aplicar as técnicas de correção vistas no capítulo 5. O resultado será

$$P_{corr} = P_{suc}^{total} = 4 \times \frac{n^2}{2(1+n^2)} = \frac{2n^2}{1+n^2}. \quad (6.25)$$

(2) $m = n$ (*matching*):

Para as medidas de $|A_m^-\rangle$ e $|J_m^+\rangle$ haverá êxito na transmissão. A probabilidade será de

$$P_{suc} = 4 \times \frac{n^2}{2(1+n^2)^2} = \frac{2n^2}{(1+n^2)^2}. \quad (6.26)$$

Os estados restantes associados a $|A_m^+\rangle$ e $|J_m^-\rangle$ são da forma $\alpha|00\rangle_{56} + n^2\delta'|11\rangle_{56}$ e

$n^2\alpha|11\rangle_{56} - \delta'|00\rangle_{56}$ e podem ser corrigidos. O resultado será

$$P_{corr} = 4 \times \frac{n^2}{2(1+n^2)^2} = \frac{2n^4}{(1+n^2)^2}, \quad (6.27)$$

e, logo, a probabilidade total de sucesso quando houver *matching* também será de

$$P_{suc}^{total} = \frac{2n^2}{1+n^2}. \quad (6.28)$$

Este é mais um procedimento em que conseguimos atingir o valor da Eq. (4.11).

Para encerrar, vamos levantar outra questão: e se Alice medisse o sistema de uma forma diferente? Em outras palavras, o que aconteceria se permutássemos os índices na ordem $|134256\rangle$? Se isso ocorresse, o resultado final não seria alterado. Todos os testes foram realizados com diferentes ordenamentos dos índices, e os cálculos ao fim do processo foram os mesmos. Apenas os estados associados às medidas que aparecem na estrutura final são diferentes. Abaixo mostramos o estado final para o ordenamento $|134256\rangle$.

$$\begin{aligned} &= \left[\frac{\sqrt{(\alpha')^2 + (mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |A_m^+\rangle \left(\frac{\alpha'|00\rangle_{56} + mn\delta'|11\rangle_{56}}{\sqrt{(\alpha')^2 + (mn\delta')^2}} \right) + \left[\frac{\sqrt{(m\alpha')^2 + (-n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |A_m^-\rangle \left(\frac{m\alpha'|00\rangle_{56} - n\delta'|11\rangle_{56}}{\sqrt{(m\alpha')^2 + (-n\delta')^2}} \right) \\ &+ \left[\frac{\sqrt{(n\alpha')^2 + (m\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |J_m^+\rangle \left(\frac{n\alpha'|00\rangle_{56} + m\delta'|11\rangle_{56}}{\sqrt{(n\alpha')^2 + (m\delta')^2}} \right) + \left[\frac{\sqrt{(mn\alpha')^2 + (-\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |J_m^-\rangle \left(\frac{mn\alpha'|00\rangle_{56} - \delta'|11\rangle_{56}}{\sqrt{(mn\alpha')^2 + (-\delta')^2}} \right) \\ &+ \left[\frac{\sqrt{(m\beta')^2 + (-n\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |B_m^+\rangle \left(\frac{m\beta'|00\rangle_{56} - n\gamma'|11\rangle_{56}}{\sqrt{(m\beta')^2 + (-n\gamma')^2}} \right) + \left[\frac{\sqrt{(-\beta')^2 + (mn\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |B_m^-\rangle \left(\frac{-\beta'|00\rangle_{56} + mn\gamma'|11\rangle_{56}}{\sqrt{(-\beta')^2 + (mn\gamma')^2}} \right) \\ &+ \left[\frac{\sqrt{(mn\beta')^2 + (-\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |K_m^+\rangle \left(\frac{mn\beta'|00\rangle_{56} - \gamma'|11\rangle_{56}}{\sqrt{(mn\beta')^2 + (-\gamma')^2}} \right) + \left[\frac{\sqrt{(-n\beta')^2 + (m\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |K_m^-\rangle \left(\frac{-n\beta'|00\rangle_{56} + m\gamma'|11\rangle_{56}}{\sqrt{(-n\beta')^2 + (m\gamma')^2}} \right). \end{aligned} \quad (6.29)$$

Se observar com cuidado, o leitor perceberá que os *qubits* 5 e 6 se apresentam com as mesmas formas vistas na Eq. (6.23) (com exceção da diferença de sinal em alguns casos, que pode ser corrigida via transformações unitárias).

6.3 Base Generalizada e Canal GHZ

Seguiremos com outra aplicação envolvendo estados GHZ generalizados. Se na seção 6.2 utilizamos estes estados para construir o canal e a base de medidas, agora manteremos apenas a representação para o canal, e os dois pares serão medidos separadamente em duas bases de Bell generalizadas com o mesmo grau de emaranhamento ($m_a = m_b = m$). A figura 6.3 ilustra este procedimento. O estado inicial de Alice continua sendo

$$|\phi\rangle_{1,2} = \alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}, \quad (6.30)$$

e o canal também é idêntico ao da seção anterior,

$$|A_n^+\rangle_{3,5,4,6} = \frac{|0000\rangle_{3,5,4,6} + n|1111\rangle_{3,5,4,6}}{\sqrt{1+n^2}}. \quad (6.31)$$

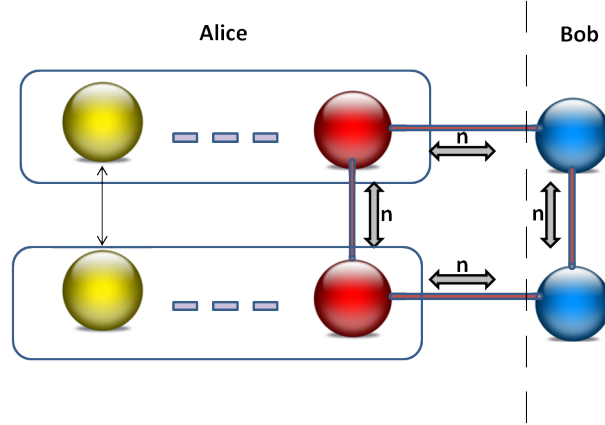


Figura 6.3: Teleporte de dois qubits utilizando um canal GHZ generalizado e medidas na base de Bell generalizada.

Por conseguinte, o estado geral também é igual ao mostrado na Eq. (6.19),

$$|\phi\rangle_{1,2}|A_n^+\rangle_{3,5,4,6} = N^2(\alpha'|00\rangle_{1,2} + \beta'|01\rangle_{1,2} + \gamma'|10\rangle_{1,2} + \delta'|11\rangle_{1,2}) \times (|0000\rangle_{3,5,4,6} + n|1111\rangle_{3,5,4,6}). \quad (6.32)$$

Como já mencionamos, as medidas de Alice serão realizadas na base de Bell generalizada, trabalhada no início deste capítulo e vista com detalhes no capítulo 4. Lembre-se de que ela é composta por

$$|\Phi_m^+\rangle = \frac{|00\rangle + m|11\rangle}{\sqrt{1+m^2}}, \quad |\Phi_m^-\rangle = \frac{m|00\rangle - |11\rangle}{\sqrt{1+m^2}}, \quad |\Psi_m^+\rangle = \frac{|01\rangle + m|10\rangle}{\sqrt{1+m^2}}, \quad |\Psi_m^-\rangle = \frac{m|01\rangle - |10\rangle}{\sqrt{1+m^2}}, \quad (6.33)$$

onde $0 < m < 1$; e, ao escrever os estados da base computacional em função dos anteriores, vimos que

$$\begin{aligned} |00\rangle &= \frac{|\Phi_m^+\rangle + m|\Phi_m^-\rangle}{\sqrt{1+m^2}}, & |01\rangle &= \frac{|\Psi_m^+\rangle + m|\Psi_m^-\rangle}{\sqrt{1+m^2}}, \\ |10\rangle &= \frac{m|\Psi_m^+\rangle - |\Psi_m^-\rangle}{\sqrt{1+m^2}}, & |11\rangle &= \frac{m|\Phi_m^+\rangle - |\Phi_m^-\rangle}{\sqrt{1+m^2}}. \end{aligned} \quad (6.34)$$

Retornando à expressão para o estado geral, vamos reescrevê-la com os índi-

ces ordenados em $|132456\rangle$ que havíamos escolhido na seção anterior. Assim, $|\phi\rangle_{1,2}|A_n^+\rangle_{3,5,4,6} =$

$$\begin{aligned}
&= N(\alpha|000000\rangle_{1,3,2,4,5,6} + n\alpha|001111\rangle_{1,3,2,4,5,6}) \\
&+ N(\beta|010000\rangle_{1,3,2,4,5,6} + n\beta|011111\rangle_{1,3,2,4,5,6}) \\
&+ N(\gamma|100000\rangle_{1,3,2,4,5,6} + n\gamma|101111\rangle_{1,3,2,4,5,6}) \\
&+ N(\delta|110000\rangle_{1,3,2,4,5,6} + n\delta|111111\rangle_{1,3,2,4,5,6}).
\end{aligned} \tag{6.35}$$

Agora, precisamos saber como substituir na expressão acima os quatro *qubits* iniciais (1, 3, 2, 4) pelo produto dos estados associados às possíveis medidas sobre os pares 1, 3 e 2, 4. Isto equivale a retornar à Eq. (6.6) e calcular todos os termos com $m_a = m_b = m$, cujo resultado é

$$\begin{aligned}
|0000\rangle &= M^2(|\Phi_m^+\rangle|\Phi_m^+\rangle + m|\Phi_m^+\rangle|\Phi_m^-\rangle + m|\Phi_m^-\rangle|\Phi_m^+\rangle + m^2|\Phi_m^-\rangle|\Phi_m^-\rangle), \\
|0001\rangle &= M^2(|\Phi_m^+\rangle|\Psi_m^+\rangle + m|\Phi_m^+\rangle|\Psi_m^-\rangle + m|\Phi_m^-\rangle|\Psi_m^+\rangle + m^2|\Phi_m^-\rangle|\Psi_m^-\rangle), \\
|0010\rangle &= M^2(m|\Phi_m^+\rangle|\Psi_m^+\rangle - |\Phi_m^+\rangle|\Psi_m^-\rangle + m^2|\Phi_m^-\rangle|\Psi_m^+\rangle - m|\Phi_m^-\rangle|\Psi_m^-\rangle), \\
|0011\rangle &= M^2(m|\Phi_m^+\rangle|\Phi_m^+\rangle - |\Phi_m^+\rangle|\Phi_m^-\rangle + m^2|\Phi_m^-\rangle|\Phi_m^+\rangle - m|\Phi_m^-\rangle|\Phi_m^-\rangle), \\
|0100\rangle &= M^2(|\Psi_m^+\rangle|\Phi_m^+\rangle + m|\Psi_m^+\rangle|\Phi_m^-\rangle + m|\Psi_m^-\rangle|\Phi_m^+\rangle + m^2|\Psi_m^-\rangle|\Phi_m^-\rangle), \\
|0101\rangle &= M^2(|\Psi_m^+\rangle|\Psi_m^+\rangle + m|\Psi_m^+\rangle|\Psi_m^-\rangle + m|\Psi_m^-\rangle|\Psi_m^+\rangle + m^2|\Psi_m^-\rangle|\Psi_m^-\rangle), \\
|0110\rangle &= M^2(m|\Psi_m^+\rangle|\Psi_m^+\rangle - |\Psi_m^+\rangle|\Psi_m^-\rangle + m^2|\Psi_m^-\rangle|\Psi_m^+\rangle - m|\Psi_m^-\rangle|\Psi_m^-\rangle), \\
|0111\rangle &= M^2(m|\Psi_m^+\rangle|\Phi_m^+\rangle - |\Psi_m^+\rangle|\Phi_m^-\rangle + m^2|\Psi_m^-\rangle|\Phi_m^+\rangle - m|\Psi_m^-\rangle|\Phi_m^-\rangle), \\
|1000\rangle &= M^2(m|\Psi_m^+\rangle|\Phi_m^+\rangle + m^2|\Psi_m^+\rangle|\Phi_m^-\rangle - |\Psi_m^-\rangle|\Phi_m^+\rangle - m|\Psi_m^-\rangle|\Phi_m^-\rangle), \\
|1001\rangle &= M^2(m|\Psi_m^+\rangle|\Psi_m^+\rangle + m^2|\Psi_m^+\rangle|\Psi_m^-\rangle - |\Psi_m^-\rangle|\Psi_m^+\rangle - m|\Psi_m^-\rangle|\Psi_m^-\rangle), \\
|1010\rangle &= M^2(m^2|\Psi_m^+\rangle|\Psi_m^+\rangle - m|\Psi_m^+\rangle|\Psi_m^-\rangle - m|\Psi_m^-\rangle|\Psi_m^+\rangle + |\Psi_m^-\rangle|\Psi_m^-\rangle), \\
|1011\rangle &= M^2(m^2|\Psi_m^+\rangle|\Phi_m^+\rangle - m|\Psi_m^+\rangle|\Phi_m^-\rangle - m|\Psi_m^-\rangle|\Phi_m^+\rangle + |\Psi_m^-\rangle|\Phi_m^-\rangle), \\
|1100\rangle &= M^2(m|\Phi_m^+\rangle|\Phi_m^+\rangle + m^2|\Phi_m^+\rangle|\Phi_m^-\rangle - |\Phi_m^-\rangle|\Phi_m^+\rangle - m|\Phi_m^-\rangle|\Phi_m^-\rangle), \\
|1101\rangle &= M^2(m|\Phi_m^+\rangle|\Psi_m^+\rangle + m^2|\Phi_m^+\rangle|\Psi_m^-\rangle - |\Phi_m^-\rangle|\Psi_m^+\rangle - m|\Phi_m^-\rangle|\Psi_m^-\rangle), \\
|1110\rangle &= M^2(m^2|\Phi_m^+\rangle|\Psi_m^+\rangle - m|\Phi_m^+\rangle|\Psi_m^-\rangle - m|\Phi_m^-\rangle|\Psi_m^+\rangle + |\Phi_m^-\rangle|\Psi_m^-\rangle), \\
|1111\rangle &= M^2(m^2|\Phi_m^+\rangle|\Phi_m^+\rangle - m|\Phi_m^+\rangle|\Phi_m^-\rangle - m|\Phi_m^-\rangle|\Phi_m^+\rangle + |\Phi_m^-\rangle|\Phi_m^-\rangle).
\end{aligned} \tag{6.36}$$

Substituindo estas combinações na expressão para o estado geral, teremos $|\phi\rangle_{1,2}|A_n^+\rangle_{3,5,4,6}$ igual a

$$\begin{aligned}
&M^2N\alpha(|\Phi_m^+\rangle|\Phi_m^+\rangle + m|\Phi_m^+\rangle|\Phi_m^-\rangle + m|\Phi_m^-\rangle|\Phi_m^+\rangle + m^2|\Phi_m^-\rangle|\Phi_m^-\rangle)|00\rangle_{56} \\
&+ M^2Nn\alpha(|\Psi_m^+\rangle|\Psi_m^+\rangle + m|\Psi_m^+\rangle|\Psi_m^-\rangle + m|\Psi_m^-\rangle|\Psi_m^+\rangle + m^2|\Psi_m^-\rangle|\Psi_m^-\rangle)|11\rangle_{56}
\end{aligned}$$

$$\begin{aligned}
& +M^2N\beta(m|\Phi_m^+\rangle|\Psi_m^+\rangle - |\Phi_m^+\rangle|\Psi_m^-\rangle + m^2|\Phi_m^-\rangle|\Psi_m^+\rangle - m|\Phi_m^-\rangle|\Psi_m^-\rangle)|00\rangle_{56} \\
& +M^2Nn\beta(m|\Psi_m^+\rangle|\Phi_m^+\rangle - |\Psi_m^+\rangle|\Phi_m^-\rangle + m^2|\Psi_m^-\rangle|\Phi_m^+\rangle - m|\Psi_m^-\rangle|\Phi_m^-\rangle)|11\rangle_{56} \\
& +M^2N\gamma(m|\Psi_m^+\rangle|\Phi_m^+\rangle + m^2|\Psi_m^+\rangle|\Phi_m^-\rangle - |\Psi_m^-\rangle|\Phi_m^+\rangle - m|\Psi_m^-\rangle|\Phi_m^-\rangle)|00\rangle_{56} \\
& +M^2Nn\gamma(m|\Phi_m^+\rangle|\Psi_m^+\rangle + m^2|\Phi_m^+\rangle|\Psi_m^-\rangle - |\Phi_m^-\rangle|\Psi_m^+\rangle - m|\Phi_m^-\rangle|\Psi_m^-\rangle)|11\rangle_{56} \\
& +M^2N\delta(m^2|\Psi_m^+\rangle|\Psi_m^+\rangle - m|\Psi_m^+\rangle|\Psi_m^-\rangle - m|\Psi_m^-\rangle|\Psi_m^+\rangle + |\Psi_m^-\rangle|\Psi_m^-\rangle)|00\rangle_{56} \\
& +M^2Nn\delta(m^2|\Phi_m^+\rangle|\Phi_m^+\rangle - m|\Phi_m^+\rangle|\Phi_m^-\rangle - m|\Phi_m^-\rangle|\Phi_m^+\rangle + |\Phi_m^-\rangle|\Phi_m^-\rangle)|11\rangle_{56};
\end{aligned} \tag{6.37}$$

e, finalmente, $|\phi\rangle_{1,2}|A_n^+\rangle_{3,5,4,6} =$

$$\begin{aligned}
& = \left[\frac{\sqrt{(\alpha')^2+(m^2n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^+\rangle|\Phi_m^+\rangle \left(\frac{\alpha'|00\rangle_{56}+m^2n\delta'|11\rangle_{56}}{\sqrt{(\alpha')^2+(m^2n\delta')^2}} \right) + \left[\frac{\sqrt{(m\alpha')^2+(-mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^+\rangle|\Phi_m^-\rangle \left(\frac{m\alpha'|00\rangle_{56}-mn\delta'|11\rangle_{56}}{\sqrt{(m\alpha')^2+(-mn\delta')^2}} \right) \\
& + \left[\frac{\sqrt{(m\alpha')^2+(-mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^-\rangle|\Phi_m^+\rangle \left(\frac{m\alpha'|00\rangle_{56}-mn\delta'|11\rangle_{56}}{\sqrt{(m\alpha')^2+(-mn\delta')^2}} \right) + \left[\frac{\sqrt{(m^2\alpha')^2+(n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^-\rangle|\Phi_m^-\rangle \left(\frac{m^2\alpha'|00\rangle_{56}+n\delta'|11\rangle_{56}}{\sqrt{(m^2\alpha')^2+(n\delta')^2}} \right) \\
& + \left[\frac{\sqrt{(n\alpha')^2+(m^2\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^+\rangle|\Psi_m^+\rangle \left(\frac{n\alpha'|11\rangle_{56}+m^2\delta'|00\rangle_{56}}{\sqrt{(n\alpha')^2+(m^2\delta')^2}} \right) + \left[\frac{\sqrt{(mn\alpha')^2+(-m\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^+\rangle|\Psi_m^-\rangle \left(\frac{mn\alpha'|11\rangle_{56}-m\delta'|00\rangle_{56}}{\sqrt{(mn\alpha')^2+(-m\delta')^2}} \right) \\
& + \left[\frac{\sqrt{(mn\alpha')^2+(-m\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^-\rangle|\Psi_m^+\rangle \left(\frac{mn\alpha'|11\rangle_{56}-m\delta'|00\rangle_{56}}{\sqrt{(mn\alpha')^2+(-m\delta')^2}} \right) + \left[\frac{\sqrt{(m^2n\alpha')^2+(\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^-\rangle|\Psi_m^-\rangle \left(\frac{m^2n\alpha'|11\rangle_{56}+\delta'|00\rangle_{56}}{\sqrt{(m^2n\alpha')^2+(\delta')^2}} \right) \\
& + \left[\frac{\sqrt{(m\beta')^2+(mn\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^+\rangle|\Psi_m^+\rangle \left(\frac{m\beta'|00\rangle_{56}+mn\gamma'|11\rangle_{56}}{\sqrt{(m\beta')^2+(mn\gamma')^2}} \right) + \left[\frac{\sqrt{(-\beta')^2+(m^2n\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^+\rangle|\Psi_m^-\rangle \left(\frac{-\beta'|00\rangle_{56}+m^2n\gamma'|11\rangle_{56}}{\sqrt{(-\beta')^2+(m^2n\gamma')^2}} \right) \\
& + \left[\frac{\sqrt{(m^2\beta')^2+(-n\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^-\rangle|\Psi_m^+\rangle \left(\frac{m^2\beta'|00\rangle_{56}-n\gamma'|11\rangle_{56}}{\sqrt{(m^2\beta')^2+(-n\gamma')^2}} \right) + \left[\frac{\sqrt{(-m\beta')^2+(-mn\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^-\rangle|\Psi_m^-\rangle \left(\frac{-m\beta'|00\rangle_{56}-mn\gamma'|11\rangle_{56}}{\sqrt{(-m\beta')^2+(-mn\gamma')^2}} \right) \\
& + \left[\frac{\sqrt{(mn\beta')^2+(m\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^+\rangle|\Phi_m^+\rangle \left(\frac{mn\beta'|11\rangle_{56}+m\gamma'|00\rangle_{56}}{\sqrt{(mn\beta')^2+(m\gamma')^2}} \right) + \left[\frac{\sqrt{(-n\beta')^2+(m^2\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^+\rangle|\Phi_m^-\rangle \left(\frac{-n\beta'|11\rangle_{56}+m^2\gamma'|00\rangle_{56}}{\sqrt{(-n\beta')^2+(m^2\gamma')^2}} \right) \\
& + \left[\frac{\sqrt{(m^2n\beta')^2+(-\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^-\rangle|\Phi_m^+\rangle \left(\frac{m^2n\beta'|11\rangle_{56}-\gamma'|00\rangle_{56}}{\sqrt{(m^2n\beta')^2+(-\gamma')^2}} \right) + \left[\frac{\sqrt{(-mn\beta')^2+(-m\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^-\rangle|\Phi_m^-\rangle \left(\frac{-mn\beta'|11\rangle_{56}-m\gamma'|00\rangle_{56}}{\sqrt{(-mn\beta')^2+(-m\gamma')^2}} \right).
\end{aligned} \tag{6.38}$$

A mesma análise discutida no fim da seção anterior aplica-se aqui. Novamente, vamos considerar que o estado inicial seja da forma $\alpha|00\rangle_{1,2} + \beta|11\rangle_{1,2}$, com $\alpha = \alpha', \beta = \delta'$ e $\beta' = \gamma' = 0$. Sendo assim, o estado geral é reduzido a

$$\begin{aligned}
& = \left[\frac{\sqrt{(\alpha')^2+(m^2n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^+\rangle|\Phi_m^+\rangle \left(\frac{\alpha'|00\rangle_{56}+m^2n\delta'|11\rangle_{56}}{\sqrt{(\alpha')^2+(m^2n\delta')^2}} \right) + \left[\frac{\sqrt{(m\alpha')^2+(-mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^+\rangle|\Phi_m^-\rangle \left(\frac{m\alpha'|00\rangle_{56}-mn\delta'|11\rangle_{56}}{\sqrt{(m\alpha')^2+(-mn\delta')^2}} \right) \\
& + \left[\frac{\sqrt{(m\alpha')^2+(-mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^-\rangle|\Phi_m^+\rangle \left(\frac{m\alpha'|00\rangle_{56}-mn\delta'|11\rangle_{56}}{\sqrt{(m\alpha')^2+(-mn\delta')^2}} \right) + \left[\frac{\sqrt{(m^2\alpha')^2+(n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Phi_m^-\rangle|\Phi_m^-\rangle \left(\frac{m^2\alpha'|00\rangle_{56}+n\delta'|11\rangle_{56}}{\sqrt{(m^2\alpha')^2+(n\delta')^2}} \right) \\
& + \left[\frac{\sqrt{(n\alpha')^2+(m^2\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^+\rangle|\Psi_m^+\rangle \left(\frac{n\alpha'|11\rangle_{56}+m^2\delta'|00\rangle_{56}}{\sqrt{(n\alpha')^2+(m^2\delta')^2}} \right) + \left[\frac{\sqrt{(mn\alpha')^2+(-m\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^+\rangle|\Psi_m^-\rangle \left(\frac{mn\alpha'|11\rangle_{56}-m\delta'|00\rangle_{56}}{\sqrt{(mn\alpha')^2+(-m\delta')^2}} \right) \\
& + \left[\frac{\sqrt{(mn\alpha')^2+(-m\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^-\rangle|\Psi_m^+\rangle \left(\frac{mn\alpha'|11\rangle_{56}-m\delta'|00\rangle_{56}}{\sqrt{(mn\alpha')^2+(-m\delta')^2}} \right) + \left[\frac{\sqrt{(m^2n\alpha')^2+(\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |\Psi_m^-\rangle|\Psi_m^-\rangle \left(\frac{m^2n\alpha'|11\rangle_{56}+\delta'|00\rangle_{56}}{\sqrt{(m^2n\alpha')^2+(\delta')^2}} \right).
\end{aligned} \tag{6.39}$$

Para determinar a probabilidade final, realizamos cálculos para $m = 1$, $m = n$ e $m = n^2$. Os resultados foram

(1) $m = 1$:

Não há sucesso direto na transmissão, e, após aplicação das técnicas de correção vistas no capítulo 5, chegamos ao valor de

$$P_{corr} = P_{suc}^{total} = 8 \times \frac{n^2}{4(1+n^2)} = \frac{2n^2}{1+n^2}. \quad (6.40)$$

(2) $m = n$:

Não há sucesso direto, e o valor final encontrado após as correções foi de

$$P_{corr} = P_{suc}^{total} = \frac{2n^6 + 6n^4}{(1+n^2)^3}, \quad (6.41)$$

que é menor do que $2n^2/1+n^2$.

(3) $m = n^2$:

Sucesso direto para as medidas de $|\Phi_m^-\rangle|\Phi_m^-\rangle$ e $|\Psi_m^+\rangle|\Psi_m^+\rangle$, com probabilidade igual a

$$P_{suc} = 2 \times \frac{n^2}{(1+m^2)^2(1+n^2)} = \frac{2n^2}{(1+n)^2(1+n^2)}. \quad (6.42)$$

A correção dos estados restantes gera o valor de

$$P_{corr} = \frac{2n^4 + 4n^3}{(1+n)^2(1+n^2)}, \quad (6.43)$$

que, somado a P_{suc} , gera uma probabilidade total de sucesso igual a

$$P_{suc}^{total} = \frac{2n^2}{(1+n)^2(1+n^2)} + \frac{2n^4 + 4n^3}{(1+n)^2(1+n^2)} = \frac{2n^2}{1+n^2}. \quad (6.44)$$

Assim, mostramos mais um método em que conseguimos atingir o resultado da Eq. (4.11), desta vez para os valores de $m = 1$ e $m = n^2$ nas duas bases de medidas. Embora não tenhamos explicitado os cálculos, a permutação dos índices na estrutura do estado geral também não afeta P_{suc}^{total} .

6.4 Base GHZ e Canais Paralelos

Nas seções precedentes, vimos combinações entre dois tipos de estados - os de Bell generalizados e os GHZ - e mostramos como associá-los com a base de medidas e os canais. Em 6.1, estes últimos foram representados apenas pelo primeiro tipo, e, na seção seguinte, utilizamos os estados GHZ para representar tanto o canal como a base de medidas. Em 6.3 combinamos o primeiro tipo (base de medidas) com o segundo (canal) e apresentamos um novo protocolo. Agora, encerraremos o capítulo com a última combinação possível para os estados discutidos. Não entraremos em detalhes, pois não há

conceitos novos relacionados ao canal e à base de medidas e tampouco resultados inéditos, mas, mesmo assim, comentaremos esta alternativa para mostrar uma nova maneira de obter $P_{suc}^{total} = 2n^2/(1+n^2)$. Com isso, cobrimos todos os procedimentos possíveis que associam estados GHZ e base de Bell generalizadas utilizados para o teleporte de dois *qubits*. A figura 6.4 mostra como funcionará o protocolo. Agora, temos à nossa disposição

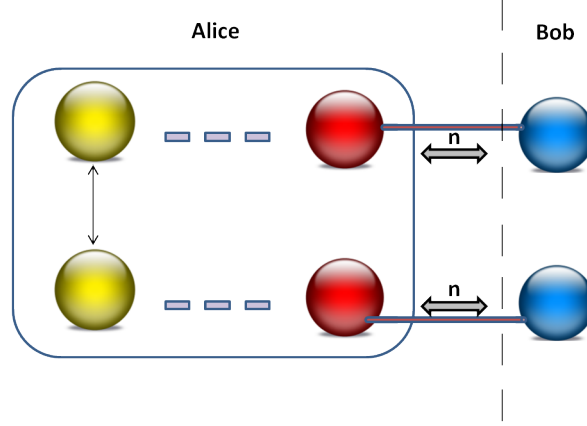


Figura 6.4: Teleporte de dois qubits utilizando canais paralelos e medidas na base GHZ generalizada.

dois canais paralelos simples e realizaremos as medidas na base GHZ generalizada de quatro *qubits*, como vimos na Eq. (6.18). Inicialmente, o estado geral do sistema será idêntico ao da Eq. (6.45),

$$|\phi\rangle_1 |\Phi_n^+\rangle_{3,5} |\Phi_n^+\rangle_{4,6} = N^2 (\alpha' |00\rangle_{1,2} + \beta' |01\rangle_{1,2} + \gamma' |10\rangle_{1,2} + \delta' |11\rangle_{1,2}) \times (|0000\rangle_{3,5,4,6} + n|0011\rangle_{3,5,4,6} + n|1100\rangle_{3,5,4,6} + n^2|1111\rangle_{3,5,4,6}). \quad (6.45)$$

Após a troca de índices para a ordem $|132456\rangle$ e substituição dos quatro primeiros *qubits* pela combinação dos estados GHZ associados à base de medidas, o estado geral se apresentará como $|\phi\rangle_1 |\Phi_n^+\rangle_{3,5} |\Phi_n^+\rangle_{4,6} =$

$$\begin{aligned} &= \left[\frac{\sqrt{(\alpha')^2 + (mn^2\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |A_m^+\rangle \left(\frac{\alpha' |00\rangle_{56} + mn^2\delta' |11\rangle_{56}}{\sqrt{(\alpha')^2 + (mn^2\delta')^2}} \right) + \left[\frac{\sqrt{(m\alpha')^2 + (-n^2\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |A_m^-\rangle \left(\frac{m\alpha' |00\rangle_{56} - n^2\delta' |11\rangle_{56}}{\sqrt{(m\alpha')^2 + (-n^2\delta')^2}} \right) \\ &+ \left[\frac{\sqrt{(mn\alpha')^2 + (n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |B_m^+\rangle \left(\frac{mn\alpha' |01\rangle_{56} + n\delta' |10\rangle_{56}}{\sqrt{(mn\alpha')^2 + (n\delta')^2}} \right) + \left[\frac{\sqrt{(-n\alpha')^2 + (mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |B_m^-\rangle \left(\frac{-n\alpha' |01\rangle_{56} + mn\delta' |10\rangle_{56}}{\sqrt{(-n\alpha')^2 + (mn\delta')^2}} \right) \\ &+ \left[\frac{\sqrt{(\beta')^2 + (mn^2\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |C_m^+\rangle \left(\frac{\beta' |00\rangle_{56} + mn^2\gamma' |10\rangle_{56}}{\sqrt{(\beta')^2 + (mn^2\gamma')^2}} \right) + \left[\frac{\sqrt{(m\beta')^2 + (-n^2\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |C_m^-\rangle \left(\frac{m\beta' |00\rangle_{56} - n^2\gamma' |10\rangle_{56}}{\sqrt{(m\beta')^2 + (-n^2\gamma')^2}} \right) \\ &+ \left[\frac{\sqrt{(mn\beta')^2 + (n\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |D_m^+\rangle \left(\frac{mn\beta' |01\rangle_{56} + n\gamma' |10\rangle_{56}}{\sqrt{(mn\beta')^2 + (n\gamma')^2}} \right) + \left[\frac{\sqrt{(-n\beta')^2 + (mn\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |D_m^-\rangle \left(\frac{-n\beta' |01\rangle_{56} + mn\gamma' |10\rangle_{56}}{\sqrt{(-n\beta')^2 + (mn\gamma')^2}} \right) \\ &+ \left[\frac{\sqrt{(n\alpha')^2 + (mn\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |E_m^+\rangle \left(\frac{n\alpha' |10\rangle_{56} + mn\delta' |01\rangle_{56}}{\sqrt{(n\alpha')^2 + (mn\delta')^2}} \right) + \left[\frac{\sqrt{(mn\alpha')^2 + (-n\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |E_m^-\rangle \left(\frac{mn\alpha' |10\rangle_{56} - n\delta' |01\rangle_{56}}{\sqrt{(mn\alpha')^2 + (-n\delta')^2}} \right) \\ &+ \left[\frac{\sqrt{(mn^2\alpha')^2 + (\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |F_m^+\rangle \left(\frac{mn^2\alpha' |11\rangle_{56} + \delta' |00\rangle_{56}}{\sqrt{(mn^2\alpha')^2 + (\delta')^2}} \right) + \left[\frac{\sqrt{(-n^2\alpha')^2 + (m\delta')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |F_m^-\rangle \left(\frac{-n^2\alpha' |11\rangle_{56} + m\delta' |00\rangle_{56}}{\sqrt{(-n^2\alpha')^2 + (m\delta')^2}} \right) \\ &+ \left[\frac{\sqrt{(n\beta')^2 + (mn\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |J_m^+\rangle \left(\frac{n\beta' |10\rangle_{56} + mn\gamma' |01\rangle_{56}}{\sqrt{(n\beta')^2 + (mn\gamma')^2}} \right) + \left[\frac{\sqrt{(mn\beta')^2 + (-n\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |J_m^-\rangle \left(\frac{mn\beta' |10\rangle_{56} - n\gamma' |01\rangle_{56}}{\sqrt{(mn\beta')^2 + (-n\gamma')^2}} \right) \end{aligned}$$

$$+ \left[\frac{\sqrt{(mn^2\beta')^2 + (\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |K_m^+\rangle \left(\frac{mn^2\beta' |11\rangle_{56} + \gamma' |00\rangle_{56}}{\sqrt{(mn^2\beta')^2 + (\gamma')^2}} \right) + \left[\frac{\sqrt{(-n^2\beta')^2 + (m\gamma')^2}}{\sqrt{(1+m^2)(1+n^2)}} \right] |K_m^-\rangle \left(\frac{-n^2\beta' |11\rangle_{56} + m\gamma' |00\rangle_{56}}{\sqrt{(-n^2\beta')^2 + (m\gamma')^2}} \right). \quad (6.46)$$

Ao definir o estado inicial como $\alpha|00\rangle + \beta|11\rangle$ e realizar cálculos para $m = 1$, $m = n$ e $m = n^2$, obtivemos resultados idênticos ao da seção 6.3. Assim como na Eq. (6.11) existem casos em que o teleporte ocorre com sucesso sem que Alice e Bob precisem conhecer o grau de emaranhamento dos canais se estes valores forem idênticos em ambos. Estes casos aparecem quando $m = 1$ e Alice obtém como resultado de sua medida qualquer um dos seguintes estados

$$|B_m^+\rangle, |B_m^-\rangle, |D_m^+\rangle, |D_m^-\rangle, |E_m^+\rangle, |E_m^-\rangle, |J_m^+\rangle \text{ ou } |J_m^-\rangle. \quad (6.47)$$

Com isso, finalizamos o capítulo com mais um método que funciona para o teleporte de dois *qubits* e atinge o valor de $P_{suc}^{total} = 2n^2/(1 + n^2)$. Em comum, todos os protocolos vistos até o momento alcançam esta probabilidade para alguma escolha particular de valores para os parâmetros da base de medidas e do canal, e, em especial, os que apresentamos neste capítulo permitem o envio tanto de um como de dois *qubits*. Em Vidal, 1999, foi previsto que o máximo valor associado à transmissão de informação quântica utilizando dois canais paralelos seria de $P_{suc}^{total} = 4n^2/(1 + n^2)^2$, através de técnicas que envolviam destilação. Até o presente momento, não há notícia de nenhum método que tenha alcançado este resultado.

Capítulo 7

Conclusões

Neste trabalho, priorizamos a reformulação de procedimentos conhecidos e a idealização de novos protocolos de teletransporte, visando sempre superar ou igualar a eficiência de métodos que já operam em dispositivos práticos e de outros que ainda não foram implementados no mercado. Para isso, direcionamos nosso foco para a análise do grau de emaranhamento (*entanglement*) dos estados envolvidos nestes procedimentos, visando obter resultados cada vez melhores para a probabilidade de sucesso no envio de informação quântica dos métodos propostos.

No capítulo 3 discutimos o artigo que introduziu o primeiro protocolo de teleporte de informação quântica usando estados emaranhados (Bennett et al. (1993)). Apresentamos os recursos necessários para a viabilização deste método, como o canal quântico formado por um par emaranhado, o canal clássico utilizado no final do procedimento e o uso de uma base (neste caso, a base de Bell) com estados diferentes daqueles associados aos *qubits* do canal, para os quais foram escolhidos os autoestados $|0\rangle$ e $|1\rangle$ do operador σ_z . Vimos a sequência de passos que Alice e Bob devem seguir desde a medida do primeiro par de *qubits* até os ajustes finais de Bob sobre uma das possíveis formas que seu estado poderia assumir. Mostramos como estes estados poderiam ser corrigidos pelos operadores de Pauli quando diferiam do estado original de Alice e discutimos questões envolvendo relatividade restrita de Einstein e a transmissão de informação útil pelo teleporte. Vimos a estrutura do estado geral do sistema e do operador densidade antes e após as medidas e mostramos como calcular a probabilidade de sucesso para cada resultado da medida de Alice. Com isso, provamos que o teleporte ocorre com probabilidade um mantendo a fidelidade de todos os estados após o término do processo.

No capítulo 4 introduzimos o conceito de estados parcialmente emaranhados apresentando pares de *qubits* que possuem um determinado grau de emaranhamento associado menor do que um. Simulamos o procedimento de teleporte utilizando estados com esta estrutura em detrimento dos estados da base de Bell e do canal maximamente emaranhado analisados no capítulo 3, e, desta forma, aproximamos o protocolo original para um cenário mais real, visto que na prática os estados maximamente emaranhados

costumam ser instáveis. Ao efetuar estas substituições, constatamos a impossibilidade de atingir probabilidade um ao final do processo, motivo pelo qual classificamos os protocolos com estas características de teleportes probabilísticos. Assim, mostramos neste capítulo três maneiras diferentes de obter estados com fidelidade um, cada uma com métodos e probabilidades únicas. Na primeira (Li et al. (2000)), vimos que os estados imperfeitos poderiam ser corrigidos através de um operador específico, ao qual nos referimos como técnica de evolução unitária. Vimos também que este método atingia a maior eficiência possível para teleportes probabilísticos que operam com transmissão serial de informação (Vidal (1999)). Na segunda (Agrawal and Pati (2002)), constatamos que o ajuste correto do grau de emaranhamento da base de medidas e do canal permitia que o teleporte ocorresse sem a necessidade do uso da técnica de evolução unitária, porém com uma probabilidade inferior. No último (Rigolin (2009)), mostramos que Bob poderia acoplar ao canal que compartilhava com Alice outros canais em série mantidos sob seu domínio. Assim, uma vez que soubesse o resultado da medida de Alice e conhecesse os cálculos necessários caso quisesse teleportar seu *qubit*, independente da estrutura deste último, Bob poderia teleportá-lo e medir os respectivos resultados de cada teleporte quantas vezes fossem necessárias até que obtivesse um estado com fidelidade um. A eficiência deste método está intimamente relacionada à escolha do grau de emaranhamento de cada canal, e, após discutir diferentes cenários, mostramos dentre todos os possíveis aquele que seria o mais eficiente e gerava o segundo melhor resultado neste capítulo para a probabilidade total de sucesso.

No capítulo 5 apresentamos os primeiros modelos propostos por esta dissertação. Mantivemos o foco em teleportes de um *qubit* e construímos novos protocolos ao introduzir diferentes possibilidades para a estrutura dos estados parcialmente emaranhados e mesclar algumas das técnicas vistas no capítulo 4. No primeiro modelo, adaptamos a técnica de evolução unitária ao teleporte múltiplo. Repetimos os procedimentos de teleportar um *qubit* através de canais associados em série e analisamos os resultados para as primeiras etapas. Assim, para uma determinada etapa q , corrigimos todos os estados imperfeitos com a técnica de evolução unitária e comparamos os resultados com o caso em que estes estados seriam teleportados à etapa seguinte. Descobrimos que este método supera o teleporte múltiplo de Rigolin (2009) e provamos que atinge a mesma eficiência de Li et al. (2000) e Vidal (1999), independentemente do número de teleportes realizados. Mais ainda, provamos que para um elevado número de etapas a probabilidade total de sucesso associada ao protocolo de teleporte múltiplo aproxima-se deste mesmo resultado. Concluímos então que não haveria vantagem em realizar sucessivos teleportes para corrigir os estados imperfeitos em uma determinada etapa, visto que um único teleporte seguido de correções gerava a mesma probabilidade total de sucesso. No segundo modelo, aproveitamos o conceito de teleporte múltiplo com evolução unitária para construir um procedimento em que Alice e Bob não teriam acesso a nenhum dos canais intermediários.

Assim, o teleporte do estado inicial de Alice era efetuado repetidamente e de maneira independente até que afetasse o *qubit* final em posse de Bob, o qual, em seguida, aplicava a técnica de correção unitária. Encontramos para a probabilidade total de sucesso o mesmo resultado de [Perseguers et al. \(2008\)](#), e que até o momento era o considerado não só o melhor resultado para procedimentos deste tipo (em que Alice e Bob não controlam o que ocorre durante o teleporte) como também não possuía uma alternativa viável. Assim, provamos que nosso modelo pode ser utilizado para substituir a técnica de destilação proposta por [Perseguers et al. \(2008\)](#). No terceiro e último modelo introduzimos o estado *GHZ* sobre o qual realizamos algumas adaptações para construir estados parcialmente emaranhados. Mostramos um método que demanda dois canais paralelos e apenas uma medida para que a informação de Alice seja transmitida a Bob. Porém, embora Alice possua somente um *qubit*, Bob dispõe de um par, e, desta forma, é preciso que algum dos *qubits* deste par seja medido para que o outro assuma a forma do estado original de Alice. Em um primeiro momento, mostramos como satisfazer a esta condição e que a eficiência ao fim do processo era a mesma de [Agrawal and Pati \(2002\)](#). Depois, ao prosseguir com os cálculos corrigindo os estados imperfeitos com a técnica de evolução unitária, atingimos novamente os resultados de [Li et al. \(2000\)](#) e [Vidal \(1999\)](#).

No capítulo 6 apresentamos os modelos finais propostos neste trabalho. Ao todo, foram quatro modelos distintos cujos objetivos eram a transmissão de um par de *qubits*, que poderia ser refinado a somente um *qubit* dependendo dos objetivos de emissor e receptor. No primeiro modelo, Alice e Bob compartilhavam dois canais paralelos e era necessário que a primeira efetuasse duas medidas distintas sobre os pares aos quais possuía acesso. Vimos que se o estado original fosse formado pela combinação dos quatro estados de base para sistemas de dois *qubits*, o teleporte só poderia ocorrer com sucesso para condições rigorosamente específicas ($m_a = m_b = n$). Fomos então forçados a reduzir o estado original a uma combinação de apenas dois estados de base, e, com isso, atingimos o resultado de [Agrawal and Pati \(2002\)](#). Ao aplicar a técnica de evolução unitária, obtivemos novamente a eficiência encontrada em [Li et al. \(2000\)](#) e [Vidal \(1999\)](#). No segundo modelo, o canal e a base de medidas de Alice foram expressos por estados *GHZ*. As probabilidades associadas aos casos tanto de sucesso direto como após a correção via evolução unitária foram iguais às do primeiro modelo, e mais uma vez fomos obrigados a reduzir o estado original a uma combinação de apenas dois estados de base. No terceiro modelo, mantivemos o canal *GHZ* e retornamos às medidas na base generalizada, e no quarto modelo invertemos esta relação ao utilizar dois canais paralelos e a base de medidas com estados *GHZ*. Nestes dois últimos, também atingimos a probabilidade total de sucesso máxima alcançada pelos modelos anteriores. Por fim, mostramos que o primeiro e o quarto modelo permitem que o estado original seja enviado sem que Alice e Bob conheçam o grau de emaranhamento dos canais paralelos, bastando apenas que os valores sejam idênticos em ambos.

Desta forma, concluímos a dissertação ressaltando os métodos que propu-

semos para teleporte de estados quânticos. Se por um lado não superamos a eficiência de nenhum protocolo conhecido, em contrapartida atingimos as máximas eficiências permitidas para os procedimentos analisados. Com isso, alguns dos protocolos que apresentamos podem vir a ser implementados em dispositivos reais. Dentre os planos de trabalho futuro estamos considerando a análise de métodos de teleporte cujos canais sejam descritos por estados mistos.

Apêndice A

Probabilidade Máxima Associada ao Teleporte Múltiplo em Série

Demonstraremos a seguir que a expressão $2n^2/(1+n^2)$ fornece o valor máximo para a probabilidade associada ao teleporte múltiplo em série discutido nas seções 4.3 e 5.1.

Demonstração

- 1) Para um estado cuja estrutura seja $|\Psi\rangle|0\rangle_{aux} = (\alpha|0\rangle + T\beta|1\rangle)|0\rangle_{aux}$ ou $|\Psi\rangle|0\rangle_{aux} = (T\alpha|0\rangle + \beta|1\rangle)|0\rangle_{aux}$, sendo T um número complexo qualquer, a aplicação da correção via evolução unitária pela matriz U_T gera um estado final do tipo

$$U_T(|\Psi\rangle|0\rangle_{aux}) = T(\alpha|0\rangle + \beta|1\rangle)|0\rangle_{aux} + (\dots)|1\rangle_{aux}. \quad (\text{A.1})$$

onde o coeficiente (...) associado ao *qubit* $|1\rangle_{aux}$ não preserva nenhuma informação relativa ao estado original $\alpha|0\rangle + \beta|1\rangle$.

- 2) Se um estado $\alpha|0\rangle + \beta|1\rangle$ for teleportado através de um canal do tipo "n", a configuração seguinte do sistema será

$$\begin{aligned} & \frac{1}{\sqrt{1+n^2}}|\Phi^+\rangle[\alpha|0\rangle + n\beta|1\rangle] + \frac{1}{\sqrt{1+n^2}}|\Phi^-\rangle[\alpha|0\rangle + n\beta|1\rangle] + \\ & + \frac{1}{\sqrt{1+n^2}}|\Psi^+\rangle[n\alpha|0\rangle + \beta|1\rangle] + \frac{1}{\sqrt{1+n^2}}|\Psi^-\rangle[n\alpha|0\rangle + \beta|1\rangle]. \end{aligned} \quad (\text{A.2})$$

Repare que as medidas associadas aos estados $|\Phi^+\rangle$ e $|\Phi^-\rangle$ "introduzem" no coeficiente β um fator multiplicativo n , mantendo α intacto. Para os estados $|\Psi^+\rangle$ e $|\Psi^-\rangle$ o papel se inverte: β permanece inalterado, enquanto α cede lugar a $n\alpha$.

- 3) Podemos estender os resultados para saber a configuração do sistema após o teleporte de $\alpha|0\rangle + T\beta|1\rangle$ ou $T\alpha|0\rangle + \beta|1\rangle$: basta reescrever a equação anterior, substituindo β por $T\beta$ no primeiro caso e α por $T\alpha$ no segundo. Se teleportarmos o estado $|\Psi\rangle = \alpha|0\rangle + T\beta|1\rangle$ utilizando um canal com grau " T " de emaranhamento, teremos, na etapa seguinte

$$\begin{aligned} & \frac{1}{\sqrt{1+T^2}}|\Phi^+\rangle[\alpha|0\rangle + T^2\beta|1\rangle] + \frac{1}{\sqrt{1+T^2}}|\Phi^-\rangle[\alpha|0\rangle + T^2\beta|1\rangle] + \\ & + \frac{1}{\sqrt{1+T^2}}|\Psi^+\rangle[T(\alpha|0\rangle + \beta|1\rangle)] + \frac{1}{\sqrt{1+T^2}}|\Psi^-\rangle[T(\alpha|0\rangle + \beta|1\rangle)]. \end{aligned} \quad (\text{A.3})$$

Por outro lado, se teleportarmos o estado $|\Psi\rangle = T\alpha|0\rangle + \beta|1\rangle$ e utilizarmos um canal semelhante, o estado geral do sistema será

$$\begin{aligned} & \frac{1}{\sqrt{1+T^2}}|\Phi^+\rangle[T(\alpha|0\rangle + \beta|1\rangle)] + \frac{1}{\sqrt{1+T^2}}|\Phi^-\rangle[T(\alpha|0\rangle + \beta|1\rangle)] + \\ & + \frac{1}{\sqrt{1+T^2}}|\Psi^+\rangle[T^2\alpha|0\rangle + \beta|1\rangle] + \frac{1}{\sqrt{1+T^2}}|\Psi^-\rangle[T^2\alpha|0\rangle + \beta|1\rangle]. \end{aligned} \quad (\text{A.4})$$

Assim, para cada um dos casos, duas das quatro medidas fornecem o *qubit* em sua estrutura original. Como o coeficiente T é arbitrário, esta análise serve para qualquer etapa q na seqüência de teleportes, e, dessa forma, para 50% dos casos é possível encontrar o estado original enviado no início do protocolo (não confundir com a probabilidade específica associada à obtenção do mesmo estado como resultado da medida do sistema; ou seja, o módulo quadrático de seu coeficiente).

- 4) Para os estados que falharam em (3) e (4), podemos introduzir um *qubit* auxiliar $|0\rangle_{aux}$ e aplicar a correção através da matriz U_T . De acordo com a Eq. (A.1), o novo estado do sistema será

$$\frac{1}{\sqrt{1+T^2}}T^2(\alpha|0\rangle + \beta|1\rangle)|0\rangle_{aux} + (\dots)|1\rangle_{aux}. \quad (\text{A.5})$$

onde deixamos o coeficiente $\frac{1}{\sqrt{1+T^2}}$ implícito em (...). Assim, incluindo as futuras correções com U_T , o estado geral do sistema pode ser expresso em termos de

$$\begin{aligned} & \frac{1}{\sqrt{1+T^2}}T(\alpha|0\rangle + \beta|1\rangle); \text{ para dois dos quatro casos; e} \\ & \frac{1}{\sqrt{1+T^2}}T^2(\alpha|0\rangle + \beta|1\rangle)|0\rangle_{aux} + (\dots)|1\rangle_{aux}, \text{ para os dois casos restantes.} \end{aligned} \quad (\text{A.6})$$

Desse modo, após sucessivos teleportes até uma determinada etapa q , metade das possibilidades fornecerão $\alpha|0\rangle + \beta|1\rangle$. Para a metade restante, introduz-se $|0\rangle_{aux}$ e aplica-se U_T para tentar obter $(\alpha|0\rangle + \beta|1\rangle)|0\rangle_{aux}$.

- 5) Em uma etapa q qualquer, já vimos que para a metade dos casos o teleporte ocorrerá com sucesso direto. O fator multiplicativo associado a estes estados é proporcional a $n^{2^{q-2}}$; ou seja, ao grau de emaranhamento do canal, já que a escolha deste último é feita com o objetivo de "corrigir" metade dos estados em que houve falha na etapa $q - 1$. Assim, α e β são multiplicados por $n^{2^{q-2}}$. Para a outra metade, o fator será da forma $(n^{2^{q-2}}) \times (n^{2^{q-2}}) = n^{2^{q-1}}$ para um dos coeficientes, e o outro permanecerá inalterado. Os estados serão então

$$\begin{aligned} Mn^{2^{q-2}}(\alpha|0\rangle + \beta|1\rangle) &\rightarrow \text{sucesso direto;} \\ Mn^{2^{q-1}}\alpha|0\rangle + \beta|1\rangle \quad \text{ou} \quad \alpha|0\rangle + Mn^{2^{q-1}}\beta|1\rangle &\rightarrow \text{necessitam de correção;} \end{aligned} \quad (\text{A.7})$$

em que M é um fator global associado aos estados na etapa q . É possível mostrar que

$$M = \frac{1}{\sqrt{2^q}} \frac{1}{\sqrt{1+n^2}} \frac{1}{\sqrt{1+n^2}} \frac{1}{\sqrt{1+n^4}} \frac{1}{\sqrt{1+n^8}} \cdots \frac{1}{\sqrt{1+n^{2^{q-1}}}}. \quad (\text{A.8})$$

Assim, se aplicarmos U_T nos estados em que não ocorreria o teleporte direto - $Mn^{2^{q-1}}\alpha|0\rangle + \beta|1\rangle$ ou $\alpha|0\rangle + Mn^{2^{q-1}}\beta|1\rangle$ - o novo estado será

$$Mn^{2^{q-1}}(\alpha|0\rangle + \beta|1\rangle)|0\rangle_{aux} + (\dots)|1\rangle_{aux}. \quad (\text{A.9})$$

Vamos chamar a probabilidade original de sucesso de $P_{(orig)}^{(q)} = |Mn^{2^{q-2}}|^2$ e a probabilidade relacionada somente à correção de $P_{(corr)}^{(q+1)} = |Mn^{2^{q-1}}|^2$. Assim, temos que

$$\begin{aligned} \frac{P_{(corr)}^{(q+1)}}{P_{(orig)}^{(q)}} &= \frac{|Mn^{2^{q-1}}|^2}{|Mn^{2^{q-2}}|^2} = \frac{(n^{2^{q-1}})^2}{(n^{2^{q-2}})^2} \\ &= (n^{2^{q-1}-2^{q-2}})^2 = (n^{2^{q-2}})^2 = n^{2 \times 2^{q-2}} = n^{2^{q-1}}. \end{aligned} \quad (\text{A.10})$$

Logo,

$$P_{(corr)}^{(q+1)} = P_{(orig)}^{(q)} \times n^{2^{q-1}}, \quad (\text{A.11})$$

e $P_{(corr)}^{(q+1)}$ é proporcional a $P_{(orig)}^{(q)}$ pelo fator $n^{2^{q-1}}$.

- 6) A equação (3) do artigo [Rigolin, 2009](#) nos diz que

$$P_{(orig)}^{(q)} = 2n^{2^{q-1}} \times \frac{(1-n^2)}{(1+n^2)(1-n^{2^q})}. \quad (\text{A.12})$$

Podemos expandir $(1 - n^{2^q})$ no produto

$$(1 - n^{2^q}) = (1 + n^{2^{q-1}})(1 + n^{2^{q-2}})\dots(1 + n^4)(1 + n^2)(1 - n^2). \quad (\text{A.13})$$

Assim, temos que

$$\begin{aligned} P_{(orig)}^{(q)} &= 2n^{2^{q-1}} \times \frac{(1-n^2)}{(1+n^2)(1+n^{2^{q-1}})(1+n^{2^{q-2}})\dots(1+n^4)(1+n^2)(1-n^2)} \\ &= \frac{2n^{2^{q-1}}}{(1+n^{2^{q-1}})(1+n^{2^{q-2}})\dots(1+n^4)(1+n^2)^2}. \end{aligned} \quad (\text{A.14})$$

Então,

$$\begin{aligned} P_{(orig)}^{(q)} &= \frac{2n^{2^{q-1}}}{(1+n^{2^{q-1}})(1+n^{2^{q-2}})\dots(1+n^4)(1+n^2)^2}; \\ P_{(orig)}^{(q-1)} &= \frac{2n^{2^{q-2}}}{(1+n^{2^{q-2}})(1+n^{2^{q-3}})\dots(1+n^4)(1+n^2)^2}; \\ P_{(orig)}^{(q+1)} &= \frac{2n^{2^q}}{(1+n^{2^q})(1+n^{2^{q-1}})\dots(1+n^4)(1+n^2)^2}; \end{aligned} \quad (\text{A.15})$$

e, desta forma, temos que

$$P_{(orig)}^{(q+1)} = P_{(orig)}^{(q)} \times \frac{n^{2^{q-1}}}{1 + n^{2^q}}. \quad (\text{A.16})$$

Logo, $P_{(orig)}^{(q+1)}$ é proporcional a $P_{(orig)}^{(q)}$ pelo fator $n^{2^{q-1}}/(1 + n^{2^q})$.

- 7) Cálculo da probabilidade total P_{suc}^{total} : a probabilidade total de sucesso de teleportes até uma determinada etapa é o resultado da soma de todas as probabilidades individuais associadas às etapas anteriores, incluindo a etapa em questão. Assim, por exemplo, para calcular P_{suc}^{total} até a etapa $q + 1$ (incluindo a correção nesta etapa), devemos efetuar a seguinte soma

$$P_{suc}^{total} = \sum_{k=2}^q P_{(orig)}^{(k)} + P_{(corr)}^{(q+1)}, \quad (\text{A.17})$$

lembrando que $P_{(orig)}^{(1)} = 0$.

Mas, utilizando a Eq. (A.11), vemos que

$$\begin{aligned} P_{(orig)}^{(q)} + P_{(corr)}^{(q+1)} &= P_{(orig)}^{(q)} \times (1 + n^{2^{q-1}}) = \frac{2n^{2^{q-1}}}{(1+n^{2^{q-2}})(1+n^{2^{q-3}})\dots(1+n^4)(1+n^2)^2} \\ &= P_{(orig)}^{(q-1)} \times (n^{2^{q-2}}). \end{aligned} \quad (\text{A.18})$$

Desse modo,

$$\begin{aligned}
 P_{suc}^{total} &= \sum_{k=2}^q P_{(orig)}^{(k)} + P_{(corr)}^{(q+1)} = \sum_{k=2}^{q-1} P_{(orig)}^{(k)} + P_{(orig)}^{(q)} + P_{(corr)}^{(q+1)} \\
 &= \sum_{k=2}^{q-1} P_{(orig)}^{(k)} + P_{(orig)}^{(q-1)} \times (n^{2^{q-2}}) = \sum_{k=2}^{q-2} P_{(orig)}^{(k)} + P_{(orig)}^{(q-1)} \times (1 + n^{2^{q-2}}).
 \end{aligned} \tag{A.19}$$

Expandindo esta soma e utilizando as expressões em (A.15), temos

$$\begin{aligned}
 \sum_{k=2}^{q-2} P_{(orig)}^{(k)} + \frac{2n^{2^{q-2}}}{(1+n^{2^{q-3}})\dots(1+n^4)(1+n^2)^2} &= \sum_{k=2}^{q-2} P_{(orig)}^{(k)} + P_{(orig)}^{(q-2)} \times (n^{2^{q-3}}) \\
 &= \sum_{k=2}^{q-3} P_{(orig)}^{(k)} + P_{(orig)}^{(q-2)} \times (1 + n^{2^{q-3}}).
 \end{aligned} \tag{A.20}$$

Note que existe uma relação de recorrência na soma acima, onde os dois últimos termos da soma de ordens k geram um múltiplo do termo de ordem $k-1$. Portanto,

$$\begin{aligned}
 P_{suc}^{total} &= \sum_{k=2}^{q-2} P_{(orig)}^{(k)} + P_{(orig)}^{(q-1)} \times (1 + n^{2^{q-2}}) = \sum_{k=2}^{q-3} P_{(orig)}^{(k)} + P_{(orig)}^{(q-2)} \times (1 + n^{2^{q-3}})\dots \\
 &= \dots \sum_{k=2}^2 P_{(orig)}^{(k)} + P_{(orig)}^{(3)} \times (1 + n^{2^2}) = P_{(orig)}^{(2)} + P_{(orig)}^{(3)} \times (1 + n^4) \\
 &= \frac{2n^2}{(1+n^2)^2} + \frac{2n^4}{(1+n^4)(1+n^2)^2} \times (1 + n^4) = \frac{2n^2}{(1+n^2)},
 \end{aligned} \tag{A.21}$$

e a soma é independente do valor de q , como queríamos demonstrar. Para completar a prova, basta lembrar que

$$P_{(corr)}^{(q+1)} = P_{(orig)}^{(q)} \times n^{2^{q-1}} > P_{(orig)}^{(q)} \times \frac{n^{2^{q-1}}}{1 + n^{2^q}} = P_{(orig)}^{(q+1)}. \tag{A.22}$$

Logo,

$$\sum_{k=2}^{q+1} P_{(orig)}^{(k)} < \sum_{k=2}^q P_{(orig)}^{(k)} + P_{(corr)}^{(q+1)} = \frac{2n^2}{(1 + n^2)}. \tag{A.23}$$

Portanto,

$$\lim_{q \rightarrow \infty} \sum_{k=2}^{q+1} P_{(orig)}^{(k)} \longrightarrow \frac{2n^2}{(1 + n^2)}, \tag{A.24}$$

e a prova está completa.

Referências Bibliográficas

- Agrawal, P. and Pati, A. K. (2002), ‘Probabilistic quantum teleportation’, *Physics Letters A* **305**, 12–17. [56](#), [69](#), [102](#), [103](#)
- Benenti, G., Casati, G. and Strini, G. (2007), *Principles of Quantum Computation And Information: Basic Tools And Special Topics*, World Scientific Publishing Co., Inc., River Edge, NJ, USA. [xi](#), [xiii](#), [5](#), [7](#), [10](#), [13](#), [17](#), [21](#), [22](#), [25](#), [32](#), [41](#), [42](#), [43](#), [44](#)
- Bennett, C. H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A. and Wootters, W. K. (1993), ‘Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels’, *Physical Review Letters* **70**, 1895–1899. [1](#), [2](#), [69](#), [101](#)
- Bennett, C. H. and Wiesner, S. J. (1992), ‘Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states’, *Physical Review Letters* **69**, 2881–2884. [2](#)
- Braunstein, S. L. and Kimble, H. J. (2000), ‘Dense coding for continuous variables’, *Physical Review A* **61**, 042302. [2](#)
- Braunstein, S. L. and van Loock, P. (2005), ‘Quantum information with continuous variables’, *Reviews of Modern Physics* **77**, 513–577. [2](#)
- Dieks, D. (1982), ‘Communication by epr devices’, *Physics Letters A* **92**(6), 271 – 272. [46](#)
- Dirk, B., K., E. A. and Anton, Z. (2000), *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, Springer. [2](#)
- Einstein, A., Podolsky, B. and Rosen, N. (1935), ‘Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?’, *Physical Review* **47**, 777–780. [2](#), [47](#)
- Ekert, A. K. (1991), ‘Quantum cryptography based on bell’s theorem’, *Physical Review Letters* **67**, 661–663. [2](#)
- Greenberger, D., Horne, M. and Zeilinger, A. (2010), *in Bell’s Theorem, Quantum Theory and Conceptions of the Universe*, Fundamental Theories of Physics Series, Springer. [75](#)

- Grover, L. K. (1996), ‘A fast quantum mechanical algorithm for database search’, *eprint arXiv:quant-ph/9605043* . 2
- Li, W.-L., Li, C.-F. and Guo, G.-C. (2000), ‘Probabilistic teleportation and entanglement matching’, *Phys. Rev. A* **61**, 034301. 53, 69, 102, 103
- Mermin, N. D. (2007), *Quantum Computer Science: An Introduction*, Cambridge University Press, New York, NY, USA. 5
- Modławska, J. and Grudka, A. (2008), ‘Nonmaximally entangled states can be better for multiple linear optical teleportation’, *Physics Review Letters* **100**, 110503. 58
- Nielsen, M. A. and Chuang, I. L. (2004), *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, MA, USA. xiii, 2, 5, 28
- Perseguers, S., Cirac, J. I., AcAn, A., Lewenstein, M. and Wehr, J. (2008), ‘Entanglement distribution in pure-state quantum networks’, *Physics Review A* **77**, 022308. 3, 73, 74, 75, 103
- Rigolin, G. (2004), Superdense coding using multipartite states, Technical Report quant-ph/0407193. 69
- Rigolin, G. (2005), ‘Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement’, *Physics Letters A* **71**, 032303. 69, 75
- Rigolin, G. (2009), ‘Unity fidelity multiple teleportation using partially entangled states’, *Advances In Atomic, Molecular, and Optical Physics* **42**, 235504. xiv, 2, 58, 61, 62, 64, 65, 68, 69, 74, 102, 107
- Shor, P. W. (1996), ‘Fault-tolerant quantum computation’, *eprint arXiv:quant-ph/9605011* . 2
- Tittel, W., Ribordy, G. and Gisin, N. (1998), ‘Quantum cryptography’, *Physics World* pp. 42–46. 2
- Vidal, G. (1999), ‘Entanglement of pure states for a single copy’, *Physics Review Letters* **83**, 1046–1049. 56, 99, 102, 103