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

Dissertação de Mestrado

Classificação, Quantificação e Dinâmica do Emaranhamento

Analine Pinto Valeriano Bandeira

Campina Grande – PB

Março - 2012

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

Classificação, Quantificação e Dinâmica do Emaranhamento

Analine Pinto Valeriano Bandeira

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

Área de Concentração: Física da Matéria Condensada
Linha de pesquisa: Informação Quântica.

Aércio F. Lima
Orientador

Campina Grande – PB, Paraíba, Brasil

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG

B214c Bandeira, Analine Pinto Valeriano.
Classificação, quantificação e dinâmica do Emaranhamento / Analine Pinto Valeriano Bandeira. – Campina Grande, 2013.
79 f. : il. color.

Dissertação (Mestrado em Física) – Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, 2013.

"Orientação: Prof. Dr. Aércio Ferreira de Lima".
Referências.

1. Teoria Quântica. 2. Critérios de Separabilidade. 3. Quantificação 4. Dinâmica. 5. Emaranhamento. I. Lima, Aércio Ferreira de. II. Título.

CDU 530.145(043)

Agradecimentos

Foram dois anos longe de casa, da filha, do esposo, da família. Durante estes dois anos, meu esposo e minha filha ficaram aos cuidados de meus pais na minha cidade, enquanto eu fiquei aos cuidados de meu sogro e minha sogra. Foi literalmente um troca de famílias. Os únicos dias em que eu poderia matar as saudades, eram regados ainda com muita força de vontade para enfrentar um total 600 km de distância, todos os finais de semana. Aprender a lidar com a distância não foi fácil tendo que dividir a semana em duas metades: uma para a família e outra para os estudos, assim também como a própria conclusão do curso não foi.

Como cristã, agradeço primeiramente a Deus que fez surgir todas as oportunidades cabíveis para que eu pudesse iniciar e concluir este mestrado. Como sempre, Ele nunca me deixou na mão.

Agradeço ao meu esposo Gilkerson Bandeira, por ter sido tão compreensivo diante da minha decisão de passar este tempo "fora", pela sua sabedoria que sempre me guia através de seus conselhos para a vida, sua paciência em ter sido pai e mãe com excelência por estes dois anos, pelo seu caráter e hombridade e principalmente pelo seu respeito e amor que estes dois anos me mostraram que não mudou em nada. Agradeço à minha filha Vívian Bandeira que me incentivava a cada abraço e beijo recebido e até mesmo com os próprios erros, o que me encorajava sempre a terminar o mais rápido possível pois via o quanto ela precisa de mim.

Agradeço ao meu orientador que diante de tantos elogios para aqui citar, posso resumidamente dizer que ele é um exemplo de pessoa e profissional a ser seguido.

Agradeço aos meus pais por nos acolherem em sua casa em Sousa, à minha mãe em especial por cuidar de minha filha durante este tempo e ao meu sogro e minha sogra por me acolherem como filha em sua casa durante todo o mestrado em Campina Grande, aos colegas de estudo, professores e funcionários pelas horas de conversas descontraídas ao pé da porta do departamento e na cantina, à Dona Dalva da cantina, que recarrega nossas energias com seu cuzcuz com ovo no almoço e seu cafezinho excencial pra mandar nosso sono embora e à todos aqueles que de alguma forma me deram alguma palavra de incentivo.

Obrigada a todos!

Resumo

A Computação e Informação Quânticas (CQ e IQ) têm sido campo de intensos estudos nas últimas décadas. Uma propriedade de extrema utilidade nesta área é o emaranhamento de partículas, cujas discussões teóricas tiveram início em 1935 a partir de um artigo publicado por Einstein, Podolski e Rosen [1]. Essa propriedade surge como uma conseqüência da teoria quântica e assegura que partículas mesmo separadas espacialmente de forma não causal, carregam em sua natureza a propriedade do todo. Numa linguagem mais coloquial, a totalidade do estado representativo das partículas não pode ser construída das suas partes, individualmente. Além dos aspectos puramente acadêmicos, a classificação e a quantificação do emaranhamento são indispensáveis para sua utilização na proposta de utilização tecnológica. Neste trabalho fizemos um estudo sobre alguns dos mais utilizados critérios de separabilidade para a detecção do emaranhamento e de alguns quantificadores desta propriedade tanto para estados bipartites, como para os casos multipartites. Além disso, a dinâmica do emaranhamento em estados GHZ e W nos canais quânticos de atenuação de fase, depolarização e amortecimento de amplitude generalizado foi estudada através de uma adaptação explícita do critério de separabilidade PPT para estados multipartites e com o uso medida de Schmidt. No caso dos estados GHZ, confirmamos os resultados encontrados em [2].

Palavras-chave: critérios de separabilidade, quantificação, dinâmica quântica, emaranhamento.

Abstract

The Quantum Computation and Quantum Information (QC and QI) have been the field of intense study in recent decades. An extremely useful property in this area is the entanglement of particles, whose theoretical discussions began in 1935 from an article published byEinstein, Podolsky, and Rosen [1]. This property arises as a consequence of the quantum theory and ensures that particles even spatially separated in a non-causal arrangement, take in its nature the property of the whole. In a more colloquial language, the entire state representative of the particles can not be constructed from their parts, individually. Beyond the purely academic aspects, the classification and the quantification of entanglement are essential in the proposed of the using of technology. In this work we have made a study of some of the most separability criteria used to detect the entanglement of some quantifiers of this property for both states bipartite, and for multipartite cases. Moreover, the dynamics of entanglement in W and GHZ states in quantum channels, phase damping, depolarization and generalized amplitude damping, it was studied by adapting explicit PPT separability criterion for multipartite states and using Schmidt measure. For GHZ states, we confirm the results found in [2].

Keywords: separability criteria, quantification, entanglement quantum dynamic

Sumário

Lista de Figuras

Lista de Símbolos

$\mathbb{C}$ Conjunto dos números complexos

$\mathbb{Z}$ Conjunto dos números inteiros

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

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

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

$\perp$ Ortogonalidade entre vetores

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

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

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

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

$\mathcal{H}$ Espaço de Hilbert

i Unidade imaginária, $\sqrt{-1}$

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

$\ominus$ Subtração módulo dois, e.g., $a \ominus b \equiv a - b \ (mod\ 2)$

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

$\ominus$ Subtração módulo dimensional, e.g., $a \ominus b \equiv a - b \ (mod\ d)$

d Representa a dimensão.

CAPÍTULO 1

Preliminares

1.1 O que é emaranhamento?

Desde a publicação do famoso artigo escrito por Einstein, Podolski e Rosen em 1935 [1], o emaranhamento vem sendo incessantemente estudado como recurso para o desenvolvimento das tecnologias quânticas emergentes como repetidores quânticos, processamento da informação quântica, dentre outras. Mais explicitamente, tarefas básicas como a codificação superdensa, teletransporte e a criptografia quântica fazem uso direto desta propriedade.

Mas o que é emaranhamento? Podemos da forma mais simples possível, defini-lo como sendo uma forte correlação entre partículas ou como Einstein descreveu, uma "ação fantasmagórica à distância". Esta descrição feita por ele foi fundamentada no fato de que partículas com esta característica conseguiam de alguma forma "comunicar-se"(aparentemente sem relação causal) de maneira que a medida de suas propriedades revelavam resultados coordenados entre si.

Como exemplo de partículas quânticas que podem apresentar esta propriedade, temos os fótons. Para gerá-los com emaranhamento podemos utilizar um cristal não-linear e um feixe de laser atenuado até a passagem de uma única partícula de luz. Ao passar pelo cristal teremos dois feixes resultantes emaranhados que podem ser chamados de fótons gêmeos. Uma boa forma de entender o emaranhamento é pensarmos como [5] onde o autor faz uma analogia destas partículas com pares de meias. Um par de meias possui a mesma cor e elas são feitas do mesmo material, por exemplo, um par de meias brancas de algodão ou meias brancas de lã. Se acontecer de, por uma breve distração, alguém calçar uma meia branca de lã em um pé e uma branca de algodão no outro, não importa onde esta pessoa esteja, no trabalho ou em outra cidade, ao observar as meias calçadas esta pessoa perceberá que cada uma é feita de um material diferente e saberá que seu respectivo par, onde quer que esteja, com certeza possui a mesma propriedade que a observada (cor branca e material de lã ou algodão - esta é uma analogia para uma correlação perfeita, podemos também ter pares perfeitamente anticorrelacionados). Com partículas quânticas emaranhadas temos algo semelhante, é o caso dos fótons gêmeos citados

anteriormente. Estas duas partículas estão fortemente correlacionadas de maneira que realizada uma medida em uma das propriedades de um dos fótons, teremos certeza sobre a informação da mesma propriedade da outra partícula. Esta é a característica do emaranhamento: partículas distantes uma da outra que revelam este princípio de não-localidade e são criadas de uma forma que todas as suas propriedades ficam armazenadas somente nas características globais do par, ao invés de cada partícula individual. Este foi um aspecto não-clássico reconhecido também em 1935

> *Então dispomos das provisões (até o emaranhamento estar resolvido por uma observação verdadeira) de apenas uma descrição comum dos dois (estados) no espaço de maior dimensão. Esta é a razão para que o conhecimento dos sistemas individuais possa declinar ao mais escasso, ou até mesmo a zero, enquanto que o do sistema total permanece sempre máximo. O melhor conhecimento possível do total não implica o melhor possível das partes - e isto é o que continua a nos assustar."*
>
> *Schrödinger,* 1935
>
> —"

Tendo em vista esta incrível propriedade de correlação à distância, vários experimentos envolvendo fótons foram sendo desenvolvidos a longas distâncias com o intuito de investigar sua aplicação nas áreas de telecomunicação e processamento de dados. Atualmente a maior distância já conseguida em sistemas envolvendo troca de informações através de fibra óptica é de 144 km, em experimento realizado entre duas ilhas na Espanha [6, 7].

O emaranhamento não aparece apenas em fótons, mas sim em qualquer sistema quântico no qual se possa estabelecer esta correlação não clássica. Hoje em dia os físicos estudam cada vez mais a implementação, o bom uso e melhoria desse recurso como é o caso de [8] onde os autores conseguem criar emaranhamento entre um conjunto de elétrons e spins nucleares e [9] onde é criado emaranhamento entre três feixes de lasers contínuos cada um numa faixa de comprimento de onda diferente. Neste último, temos a possibilidade de transmissão de informação em uma rede quântica formada por meios de transmissão com comprimento de onda na faixa do visível e na faixa do infravermelho onde são utilizadas fibras ópticas. Já recentemente, em dezembro de 2011 Philip Ball publicou um artigo na Nature [10] falando sobre um experimento realizado com sucesso para emaranhar as vibrações atômicas - fônons - em dois diamantes. Segundo o autor do experimento, os diamantes formariam uma base tecnológica poderosa para a prática do prcessamento de informação quântica.

Dentre tantos sistemas físicos possíveis para que ocorra a presença de emaranhamento, podemos destacar a possibilidade de ocorrência de emaranhamento feita por Briegel e Popescu [11] em seu artigo entitulado "*Entanglement and intra-molecular cooling in biological systems?*

- *A quantum thermodynamic perspective*". Em tal conjectura, os autores levam em conta que sistemas biológicos são sistemas quânticos orientados abertos cujos estados mais estáveis estão longe do equilíbrio termodinâmico. Este fato, segundo eles, possui implicações importantes na presença de emaranhamento. Tais sistemas realizam correção de erros: a decoerência introduz ruído dentro do sistema aumentando sua entropia. Por outro lado, por definição, eles possuem acesso a uma fonte de energia livre podendo usá-la para livrar-se dos erros.

Portanto, vemos que torna-se cada vez mais comum o uso desta propriedade em sistemas físicos. Muitos esforços têm sido feitos pela comunidade científica no intuito de identificar tais sistemas. Por exemplo, especulações como as feitas por Briegel e Popescu em sistemas biológicos vêm sendo realizadas desde sua primeira versão enviada para o ArXiv, tais como investigações em cenários biológicos específicos como a fotossíntese [12].

1.2 Contexto Histórico

Em 1935 Einstein, Podolsky e Rosen publicaram o famoso artigo [1] o qual afirmava que certos aspectos da mecânica quântica a tornavam uma teoria incompleta implicando a existência de variáveis ocultas que deviam ser implementadas no formalismo quântico. O trabalho considerava um sistema de duas partículas quânticas correlacionadas de tal forma que a medição direta em uma delas constituia uma medição indireta na outra. No entanto, EPR introduziram uma hipótese de realismo local que dizia que a escolha sobre qual observável medir em uma destas partículas não poderia afetar instantaneamente a outra onde quer que elas estivessem. Segundo os autores, a condição suficiente para que uma dada propriedade física seja um elemento de realidade seria a possibilidade de se prever com certeza o valor daquela propriedade imediatamente antes de uma medida.

> *Se, sem de modo algum perturbar um sistema, pudermos prever com certeza (ou seja, com probabilidade igual à unidade) o valor de uma quantidade física, então existe um elemento de realidade física correspondente a essa quantidade física."*
>
> *Einstein, Podolsky e Rosen*
>
> __"

Na verdade, o que EPR queriam mostrar é que na MQ existiam elementos da realidade (variáveis ocultas) que não tinham contrapartida na teoria em conjunto com o princípio da localidade, princípo este que afirma que elementos da realidade concernentes a um sistema não poderiam ser afetados por medições realizadas à distância em outro sistema. Em resposta, Bohr no mesmo ano publicou um artigo [13] afirmando que estados com este tipo de propriedade estavam de acordo com o formalismo da mecânica quântica a qual rejeita a noção de localidade.

Introduzida a Teoria de Variáveis Ocultas (TVO) na MQ, foram inciados vários estudos na tentativa de mostrar que ela era realmente uma teoria incompleta. O irlandês John S. Bell em 1966 publicou um artigo (tipo resenha) sobre diferentes provas de impossibilidade de TVOs [14] na mecânica quântica baseadas em certas desigualdades as quais foram sendo aprimoradas para verificação experimental da existência de estados emaranhados. Elas ficaram conhecidas como desigualdades de Bell[1] e são consideradas a primeira forma de caracterização de emaranhamento. Na década de 70 os experimentos foram sendo aprimorados cada vez mais em diversas áreas tornado os efeitos quânticos mais visíveis. Tendo em vista o grande impacto da descoberta do emaranhamento na comunidade científica, viu-se a possibilidade de aplicação de estados com estas correlações à distância na troca de informações. A partir de então surgiu a Computação e a Informação Quânticas, uma aplicação formidável da MQ. Na IQ temos a identificação e o estudo de recursos quânticos que podem ser utilizados para a transmissão de informação, já a CQ é a aplicação direta destes recursos. Veremos a seguir algumas aplicações do emaranhamento na Informação Quântica.

1.3 Qbits - os bits quânticos

Para que possamos trabalhar com o emaranhamento devemos primeiramente introduzir sua unidade fundamental. Na computação clássica, temos como unidade fundamental o bit que é representado por 0 ou 1, onde o 0 pode representar, por exemplo, a ausência de corrente e consequentemente o 1 a presença de corrente. Analogamente, na computação quântica os dois possíveis estados do bit quântico ou qbit são representados com a notação de Dirac por $|0\rangle$ ou $|1\rangle$ que correspondem aos estados clássicos 0 e 1 respectivamente. A diferença entre bits e qbits é que os qbits podem estar em diferentes estados de $|0\rangle$ ou $|1\rangle$ podendo ainda formarem combinações lineares de estados, chamadas superposições

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.1}$$

onde α e β são números complexos $|\alpha|^2 + |\beta|^2 = 1$ e $|0\rangle$, $|1\rangle$ representam por convenção o estado fundamental e excitado respectivamente, que podem ser representados pelos vetores

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.2}$$

O conjunto $\{|0\rangle, |1\rangle\}$, forma uma base bidimensional no espaço de Hilbert de um qbit e é chamada base computacional. Eles são objetos matemáticos com certas propriedades específicas que podem ser implementados como objetos físicos reais. Exemplos de sua implementação são experimentos que levam em conta sistemas como o alinhamento de um spin nuclear em um

[1] as desigualdades de Bell não serão abordadas no nosso trabalho. Para um estudo rápido sobre elas e suas variações ver referências [4, 15, 16], dentre várias

campo magnético uniforme, as duas polarizações diferentes de um fóton ou os dois estados de um elétron orbitando ao redor de um átomo.

A representação genérica de um qbit descrita pela equação 1.1 pode ser generalizada através de uma parametrização em termos dos ângulos θ e ϕ

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \tag{1.3}$$

a qual nos leva a uma visualização geométrica do qbit como um ponto sobre a superfície de uma esfera de raio unitário, a esfera de Bloch.

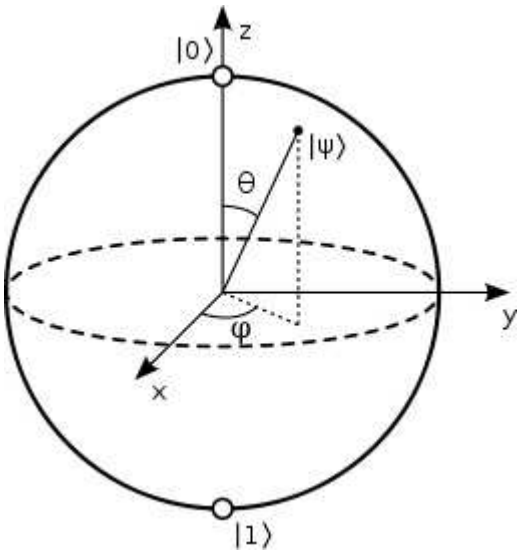

Figura 1.1 Representação geométrica de um único qbit através da esfera de Bloch. Note os pontos correspondentes aos estados $|0\rangle$ e $|1\rangle$.

Os pontos mais importantes da esfera são representados na tabela abaixo adaptada de [17]

θ	ϕ	$\|\psi\rangle$	posição
0	$-$	$\|0\rangle$	polo norte da esfera de Bloch
π	$-$	$\|1\rangle$	polo sul da esfera de Bloch
$\pi/2$	0 ou π	$(\|0\rangle \pm \|1\rangle)/\sqrt{2}$	linha do equador, exatamente no eixo x
$\pi/2$	$\pi/2$ ou $-\pi/2$	$(\|0\rangle \pm i\|1\rangle)/\sqrt{2}$	linha do equador, exatamente no eixo y

Tabela 1.1 Tabela expositiva dos principais pontos da esfera de Bloch. Cada ponto da esfera pode ser levado a outro através de operações quânticas realizadas sobre um único qbit, as quais podem ser representadas por portas quânticas

Na figura 1.1, cada ponto representado na esfera de Bloch pode ser levado a outro através de operações quânticas realizadas em um´único qbit. Estas operações são representadas por portas quânticas as quais algumas estão contidas no apêndice A.6. Como exemplo, o ponto da esfera que representa o qbit no estado $|0\rangle$ pode ser levado a um qbit numa superposição

de estados $H|0\rangle = |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, através da aplicação da porta Hadamard (H), assim como o mesmo estado $|0\rangle$ pode ser levado ao estado $X|0\rangle = |1\rangle$ aplicando-se a porta NOT, representada pela matriz de Pauli σ_x ou X.

1.4 Postulados da mecânica quântica

Numa linguagem matemática, podemos associar à Mecânica Quântica um conjunto de regras matemáticas a partir das quais as teorias físicas são construídas. Aplicando essas regras, é possível calcular propriedades de sistemas físicos observáveis a qualquer instante do tempo, desde que o Hamiltoniano seja conhecido. A teoria da MQ é baseada em quatro postulados os quais são listados a seguir [4, 17].

1. Postulado I - A qualquer sistema físico isolado, existe associado um espaço vetorial complexo equipado com produto interno, um espaço de Hilbert, conhecido como espaço de estados do sistema. O sistema é completamente descrito pelo seu vetor de espaço, um vetor unitário no espaço de estados.

2. Postulado II - A evolução de um sistema quântico fechado com o tempo é descrita por transformações unitárias do tipo

$$|\psi(t - t_0)\rangle = U(t - t_0)\,|\psi(t_0)\rangle \tag{1.4}$$

   onde $U^\dagger U = I$, com I o operador identidade. No caso em que o Hamiltoniano não depende de t, o operador de evolução unitária é dado por

$$U(t - t_0) = exp[-\frac{i}{\hbar}\mathcal{H}(t - t_0)] \tag{1.5}$$

   Fisicamente, transformações unitárias representam processos que são reversíveis no tempo. De fato, a aplicação do operador $U^\dagger$ em ambos os lados da equação (1.4) fará com que o sistema retorne ao seu estado quântico inicial $|\psi(t_0)\rangle$. Uma propriedade importante das transformações unitárias é a conservação do produto escalar $\langle\psi(t_0)|\,U^\dagger U\,|\psi(t_0)\rangle = \langle\psi(t_0)|\,\psi(t_0)\rangle = \langle\psi(t - t_0)|\,\psi(t - t_0)\rangle$.

3. Postulado III - Medidas na MQ são representadas por conjuntos de operadores chamados operadores de medidas $\{M_m\}$, onde o índice m refere-se a um dos possíveis resultados. A probabilidade $p(m)$ de um determinado valor ser encontrado numa medida é o valor esperado do operador de medida correspondente

$$p(m) = \langle\psi|\,M_m^\dagger M_m\,|\psi\rangle \tag{1.6}$$

O estado quântico do sistema após a medida será

$$|\psi\rangle = \frac{M_m}{\sqrt{p(m)}} |\psi\rangle \tag{1.7}$$

A normalização das probabilidades $\sum_m p(m) = 1$ somada à hipótese $\langle\psi|\,\psi\rangle = 1$ e equação 1.6 implica na relação de completitude

$$\sum_m M_m^\dagger M_m = I \tag{1.8}$$

4. Postulado IV - O espaço de estados de um sistema físico composto é o produto tensorial dos espaços dos sistemas físicos individuais. Se os sistemas forem numerados de 1 até n, e o sistema i for preparado no estado $|\psi_i\rangle$ com $i = 1, ..., n$, decorre que o sistema composto será $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.

1.5 Matriz densidade

Nós introduzimos uma formulação da mecânica quântica em termos de vetores de estados. Alternativamente, podemos usar uma ferramenta chamada operador densidade ou matriz densidade que é matematicamente equivalente à abordagem feita através de vetores de estado, porém mais conveniente em alguns cenários encontrados na MQ.

O operador densidade é convenientemente utilizado para descrever sistemas cujo estado não é completamente conhecido, mas apenas um conjunto de possíveis estados $\{|\psi_i\rangle\}$ com probabilidades p_i, sendo o conjunto $\{p_i, |\psi_i\rangle\}$ chamado de *ensemble de estados quânticos* e a matriz densidade representativa do sistema definida como

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \tag{1.9}$$

onde $p_i > 0$ e $\sum_i p_i = 1$. Este operador possui algumas propriedades intrínsecas muito importantes.

Definição 1.1. *Um operador ρ é considerado operador densidade do ensemble de estados $\{p_i, |\psi_i\rangle\}$ se e somente se satisfizer as seguintes condições:*

1. *Condição sobre o traço. O traço de ρ deve ser igual 1.*

2. *Condição de positividade. ρ deve ser positivo.*

O traço de uma matriz A é definido como a soma dos elementos de sua diagonal $tr(A) \equiv \sum_i \langle i|\, A\, |i\rangle = \sum_i A_{ii}$ e um operador é dito positivo se e somente se todos os seus autovelores forem não-negativos A.3.

O teorema acima permite a caracterização de operadores densidade de forma intríseca, podendo-se defini-los como um operador positivo de traço igual a 1. Todos os postulados da MQ listados na seção anterior podem ser reformulados com a utilização do formalismo da matriz densidade, no entanto, ambos os formalismos, tanto do operador densidade como de vetor do estado, levam ao mesmo resultado [4].

- Postulado I - Associado a qualquer sistema físico existe um espaço vetorial complexo com produto interno (ou seja, um espaço de Hilbert) conhecido como espaço de estados dos sistema. O sistema é completamente descrito pelo seu operador densidade, que é um operador positivo com traço 1 atuando no espaço de estados. Se o sistema está no estado ρ_i com probabilidade p_i, o seu operador densidade será $\sum_i p_i \rho_i$.

- Postulado II - A evolução de um sistema quântico fechado é descrita por transformações unitárias. Isto é, o estado ρ do sistema em um instante t_1 está relacionado ao estado ρ' em um instante t_2 por um operador unitário U que depende somente de t_1 e t_2,

$$\rho' = U\rho U^\dagger \tag{1.10}$$

- Postulado III - Medidas quânticas são descritas por uma coleção de operadores de medidas $\{M_m\}$. Esses operadores atuam sobre o espaço de estados do sistema sendo medido. O índice m refere-se a um resultado possível da medida. Se o estado do sistema imediatamente antes da medida for ρ, a probabilidade de o resultado m ocorrer será

$$p(m) = tr(M_m^\dagger M_m \rho) \tag{1.11}$$

  e o estado do sistema logo após a medida será

$$\frac{M_m \rho M_m^\dagger}{tr(M_m M_m^\dagger \rho)} \tag{1.12}$$

  onde os operadores de medida satisfazem a relação de completitude

$$\sum_m M_m^\dagger M_m = I \tag{1.13}$$

- Postulado IV - O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados das suas componentes. Além disso, se tivermos sistemas numerados de 1 até n, e o i-ésimo sistema for preparado em ρ_i, o estado do sistema composto será $\rho_1 \otimes \rho_2 \otimes ... \otimes \rho_n$.

Na seção 1.1 descrevemos a representação geométrica de estados puros na esfera de Bloch. No caso de estados mistos, tal descrição também possui uma generalização a qual apa-

rece como um exercício em [4]. Um estado misturado ρ arbitrário de um qbit pode ser escrito em termos das matrizes de Pauli $\sigma_x, \sigma_y, \sigma_z$ e da matriz identidade I

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2} \tag{1.14}$$

onde $\vec{\sigma} = \sigma_x \hat{i} + \sigma_y \hat{j} + \sigma_z \hat{k}$ é um vetor cujas componentes são as matrizes de Pauli e $\vec{r}$ é um vetor real em três dimensões, tal que $||\vec{r}|| \leq 1$ é chamado de vetor de Bloch para o estado ρ. Note que para $\rho = I/2$, $\vec{r} = 0$, ou seja, ele é um ponto no centro da esfera e o estado encontra-se maximamente misturado. Estados puros possuem sua representação geométrica na *superfície* da esfera de Bloch onde o vetor $||\vec{r}|| = 1$, portanto para qualquer $\vec{r}$ onde $||\vec{r}|| < 1$ teremos na esfera de Bloch uma representação de um único qbit num estado misturado. No capítulo 3 apresentaremos alguns canais quânticos utilizados na dinâmica do emaranhamento, onde a atuação em um único qbit pode ser facilmente visualizada e melhor compreendida através da representação geométrica na esfera de Bloch.

Operador densidade reduzido

Operadores densidade também são vastamente úteis na descrição de sistemas formados por vários subsistemas (sistemas compostos). Muitas vezes precisamos tomar informações de apenas uma parte dos subsistemas representados por uma matriz densidade ρ. Por exemplo, podemos considerar um qbit A interagindo com o ambiente B (representado por outro qbit) como um único sistema cuja matriz densidade é ρ_{AB}. Como fazer para obtermos a estatística correta para medidas realizadas em A?

A resposta a esta pergunta está no operador densidade reduzido. Ele é tão útil que se torna virtualmente indispensável na análise de sistemas quânticos compostos. No exemplo dado acima, a matriz densidade reduzida referente ao subsistema A é definida como

$$\rho^A \equiv tr_B \rho_{AB} \tag{1.15}$$

em que tr_B é uma operação conhecida como traço parcial sobre B e é definida como

$$tr_B(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|) \equiv |a_1\rangle \langle a_2| \, tr_B(|b_1\rangle \langle b_2|) \tag{1.16}$$

onde $|a_1\rangle, |a_2\rangle$ são quaisquer dois vetores do espaço de A e $|b_1\rangle, |b_2\rangle$ são quaisquer dois vetores de B. A operação do traço que aparece do lado direito da equação 1.16 é a operação usual $tr(|b_1\rangle \langle b_2|) \equiv \langle b_2 | b_1 \rangle$. Note que o *traço de uma matriz* e o *traço parcial de uma matriz* são operações completamente diferentes.

Como exemplo, podemos usar um estado de Bell $|\phi^+\rangle$ para calcular o traço sobre o subsistema B

$$\rho = \frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2} \tag{1.17}$$

$$tr_B\rho = \frac{tr_B(|00\rangle\langle 00|) + tr_B(|11\rangle\langle 00|) + tr_B(|00\rangle\langle 11|) + tr_B(|11\rangle\langle 11|)}{2} \tag{1.18}$$

$$= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \tag{1.19}$$

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{1.20}$$

$$= \frac{I}{2} \tag{1.21}$$

de onde vemos que a matriz reduzida do estado de Bell $|\phi^+\rangle$ é completamente misturada. Esta é uma característica própria de todos os estados de Bell. As equações 1.21 e 1.21 merecem destaque pois mostram explicitamente a completa aleatoriedade do estado. Por não se conhecer nada sobre o estado original da matriz 1.21, pode-se dizer que ela pode ser então representada por qualquer mistura estatísica, por isso o termo "aleatoriedade".

1.6 Aplicações do Emaranhamento

1.6.1 Teletransporte Quântico

Esta magnífica aplicação da MQ faz uso das propriedades não locais do emaranhamento para que um estado quântico possa ser teleportado de um lugar para outro sem que haja algum canal quântico de conexão entre os dois sistemas. Vamos supor que duas partes - Alice e Bob - queiram teletransportar o estado quântico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ e que os únicos recursos que eles possuam em mãos sejam um telefone (clássico) e o estado de Bell[2]

$$|\phi\rangle = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle$$

de maneira que este seja compartilhado entre os dois: o primero qbit corresponde à parte de Alice e o segundo à parte de Bob. Aqui temos uma situação complicada pois $|\psi\rangle$ é desconhecido para Alice e as leis da MQ não permitem que ela realize uma medição no estado, do contrário este colapsaria. Além do mais não há possibilidade de $|\psi\rangle$ ser clonado (A.5) mas a utilização do par EPR permite a ela que ele seja teletransportado, como veremos a seguir.

Em resumo, o que Alice precisa fazer é interagir sua parte do par EPR com o estado $|\psi\rangle$ e realizar uma medição nos dois qbits que se encontram com ela. O resultado desta medição é informado a Bob que realizará uma dentre quatro operações na sua metade para enfim recuperar $|\psi\rangle$.

Inicialmente, temos a interação entre $|\psi\rangle$ e o par EPR

[2] os estados de Bell serão formalmente apresentados no próximo capítulo.

$$\left|\psi_0^+\right\rangle = |\psi\rangle \left|\phi^+\right\rangle \tag{1.22}$$

$$= \frac{1}{\sqrt{2}} \left[\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)\right] \tag{1.23}$$

O estado 1.22 pode ser escrito em termos de uma base formada pelos estados de Bell

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.24}$$

$$\left|\phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{1.25}$$

$$\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{1.26}$$

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1.27}$$

tomando a forma

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle) \tag{1.28}$$

$$= \frac{1}{2}\Big[\left|\phi^+\right\rangle (\alpha |0\rangle + \beta |1\rangle)) + \left|\phi^-\right\rangle (\alpha |0\rangle - \beta |1\rangle)) \tag{1.29}$$

$$+ \left|\psi^+\right\rangle (\alpha |1\rangle + \beta |0\rangle)) + \left|\psi^-\right\rangle (\alpha |1\rangle - \beta |0\rangle))\Big] \tag{1.30}$$

Na representação desta base, basta que Alice realize em sua parte uma medida projetiva na própria base de Bell. Vamos supor que ao realizar a medida ela obtenha como resultado $|\psi^+\rangle$, desconhecendo ainda a parte de Bob, que neste caso é $(\alpha |1\rangle + \beta |0\rangle)$. Ela comunica ao parceiro o resultado obtido, e conhecendo o protocolo, Bob imediatamente sabe que deve realizar uma operação na sua parte para obter o estado desejado. Aplicando o operador σ_x, Bob recupera o estado desejado. As possíveis operações realizáveis por Bob para as possíveis medições realizáveis pos Alice são dadas na tabela abaixo.

Alice mede	código	Bob aplica
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	00	identidade
$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	01	σ_z
$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	10	σ_x
$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	11	σ_y

Tabela 1.2 Tabela resumindo as medições e consequentes operações quânticas realizadas por Alice e Bob respectivamente no protocolo do teletransporte.

Outra forma de se realizar o teletransporte é não escrever o estado (1.22) na base de Bell. Neste caso, podemos usar portas quânticas para realizar a tarefa. A partir de (1.22) a opereção CNOT é aplicada aos dois primeiros qbits, os quais se encontram com Alice

$$|\psi_1\rangle = CNOT\,|\psi_0\rangle \tag{1.31}$$
$$= \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)] \tag{1.32}$$

Ao fazer isso, Alice aplica a porta Hadamard ao seu primeiro qbit

$$|\psi_2\rangle = H\,|\psi_1\rangle \tag{1.33}$$
$$= \frac{1}{2}[\alpha(|0\rangle + \beta\,|1\rangle)(|00\rangle + |11\rangle) + \alpha(|0\rangle - \beta\,|1\rangle)(|10\rangle + |01\rangle)] \tag{1.34}$$

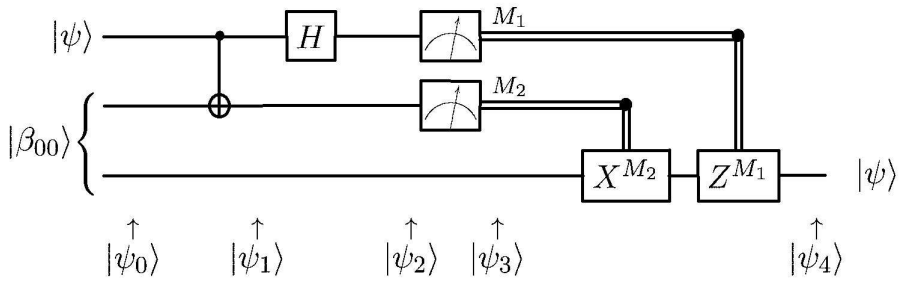

Figura 1.2 Circuito representativo do teletransporte de informação. As dua linhas de cima representam o sistema de Alice, enquanto a última, o de Bob. As linhas únicas representam os qbits, as caixas com setas dentro denotam os medidores realizando medidas e as linhas duplas que saem delas carregam bits clássicos.

Feito isto Alice realiza uma medida nos seus dois q-bits coletando informações sobre a fase e paridade e envia o resultado da sua medição para Bob através do telefone. Dependendo do resultado encontrado por Alice, Bob realizará operações de rotação sobre seu q-bit para encontrar o estado original:

$$00 \rightarrow I[\alpha\,|0\rangle + \beta\,|1\rangle] \tag{1.35}$$
$$01 \rightarrow \sigma_x[\alpha\,|1\rangle + \beta\,|0\rangle] \tag{1.36}$$
$$10 \rightarrow \sigma_z[\alpha\,|0\rangle - \beta\,|1\rangle] \tag{1.37}$$
$$11 \rightarrow \sigma_z\sigma_x[\alpha\,|1\rangle - \beta\,|0\rangle] \tag{1.38}$$

Acima, estão os bits medidos por Alice. O primeiro bit transmite à Bob informações sobre a fase e o segundo sobre a paridade do estado. Após as operações realizadas por Bob, está completo o teletransporte. Este segundo protocolo realizado através de portas quânticas em

ambos os qbits pode se visualizado na figura 1.2 a qual representa o circuito de teletransporte de um único qbit.

1.6.2 Codificação Superdensa

A codificação superdensa é um processo pelo qual dois bits de informação clássica podem ser transportados em um único qbit. Ele utiliza pares EPR para dobrar a capacidade de envio de informação entre dois meios sem no entanto contrariar o limite de Holevo [18], o qual afirma que um q-bit pode carregar no máximo um bit de informação clássica em estados ortogonais pré-definidos.

Nesta aplicação da MQ na computação, o estado de Bell é preparado e compartilhado por Alice e Bob, assim também como no teletransporte. Existem dois tipos de informação clássica em quatro sequências possíveis

$$00 \longrightarrow \frac{1}{\sqrt{2}}|00\rangle + |11\rangle \tag{1.39}$$

$$01 \longrightarrow \frac{1}{\sqrt{2}}|00\rangle - |11\rangle \tag{1.40}$$

$$10 \longrightarrow \frac{1}{\sqrt{2}}|10\rangle + |01\rangle \tag{1.41}$$

$$11 \longrightarrow \frac{1}{\sqrt{2}}|01\rangle + |10\rangle \tag{1.42}$$

$$\tag{1.43}$$

Para que Alice possa enviar informação para Bob, ela deve realizar operações na sua parte do estado, operações estas realizadas através das matrizes de Pauli $\sigma_0, \sigma_1, \sigma_2, \sigma_3$, onde σ_0 é a matriz identidade, e após isso enviar seu q-bit para Bob. Os bits de informação referem-se à fase e à paridade respectivamente, medidas no estado.

Exemplo Alice deseja enviar a Bob a sequência 10, compartilahndo o estado

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Ela deve aplicar o operador X no seu qbit, transformando o estado em

$$\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle).$$

Após a operação, Alice envia seu qbit à Bob que codifica o estado aplicando as operações CNOT e depois H, seguidas de uma medida na base computacional para descobrir a mensagem. Dessa forma, Alice enviou dois bits de informação clássica para Bob, enviando apenas um qbit de informação quântica.

1.6.3 Criptografia

A criptografia baseia-se na transmissão de dados sigilosos, sendo responsável pelo estudo de métodos matemáticos capazes de ocultar o significado de uma informação encriptando-a e tornando-a restrita às partes interessadas. Basicamente a segurança do envio de informação está no processo de fatoração de números muito grandes de maneira que quanto maior forem os números mais seguro será o código criptografado, porém o surgimento de um computador quântico derrubaria qualquer processo criptográfico clássico já existente. Classicamente falando temos dois tipos de criptografia usadas hoje em dia, a de chave pública - largamente usada (praticamente a única utilizada) - e a de chave única. Quanticamente temos duas principais que são as usadas no protocolo $BB84$ e o $E91$ onde este último faz uso de pares EPR para criptografar. Falaremos a seguir sobre cada delas. Um estudo mais detalhado pode ser encontrado em [3]

Criptografia Clássica

Protocolo de Chave Pública

No protocolo de chave pública [19] por exemplo, o interessado em realizar uma compra através da internet deve enviar para a loja suas informações pessoais, como o número do cartão de crédito, e para isso a loja deve enviar uma chave criptográfica para o mesmo que é chamada de chave pública, nome este recebido pois qualquer pessoa pode utilizar essa chave para encriptar dados. O computador do internauta por sua vez recebe a chave, criptografa as informações em termos de sequências binárias e em seguida uma operação lógica envolvendo os dados e a chave é realizada. Feito isto a informação é enviada de volta para a loja.

Mesmo qualquer pessoa podendo ter acesso à chave pública para encriptar informações, apenas a loja, a qual gerou esta chave e a enviou ao internauta, pode decodificá-la corretamente devido à existência de uma chave privada criada também pela mesma, ou seja, no processo de criação da chave pública há também a criação da chave privada de forma que esta última fica em posse apenas do seu criador (a loja no caso). Ao receber os dados encriptados, uma nova operação entre estes e a chave privada é realizada para desencriptar a informação obtendo assim os dados originais e desejados.

Protocolo de Chave Única

No caso do protocolo de chave única [19], como o próprio nome já diz, temos o uso de uma única chave tanto para encriptar como para desencriptar. A loja virtual envia para o internauta esta chave aleatória, a qual deve ser enviada de forma segura, sem espiões. O computador deste por sua vez realiza operações binárias entre os bits da chave e os bits que codificam os dados secretos (número do cartão de crédito) e envia-os de volta para a loja que utilizará a mesma chave aleatória para decodificar os dados em mãos.

A diferença entre estes dois protocolos de criptografia é que no primeiro qualquer pessoa tem acesso à chave pública gerada pela loja e uma segunda chave que só a loja possui é utilizada

para desencriptar a informação. Já no segundo protocolo temos a utilização de uma única chave a qual apenas a loja e o internauta possuem acesso, sendo incomparavelmente mais seguro que o segundo pois após uso da chave para desencriptar, ela é descartada. Porém este último protocolo se torna inviável pois a chave deve chegar ao internauta em plena segurança, problema o qual não é muito preocupante no protocolo de chave pública devido à utilização da chave privada.

Criptografia Quântica

Dentre vários protoclos de criptografia já apresentados até hoje podemos destacar dois em especial, são eles o $BB84$ e o $E91$. O primeiro destaca-se pela sua importância prática de implementação física e comercial, já o segundo é o primeiro a utilizar pares EPR para se fazer a distribuição de chaves no processo criptográfico.

BB84

O $BB84$ foi apresentado em 1984 por C. H. Bennett e G. Brassard [20] sendo o primeiro protocolo a utilizar da mecânica quântica para um dos principais fins da criptografia: a distribuição de chaves. Mesmo tendo sido o precursor desta idéia ele é utilizado em todos os sistemas bem-sucedidos de ciptografia quântica instalados até hoje, além de ser o único comercializável por empresas especializadas em transmissão de dados.

Para se fazer a distribução de uma chave criptográfica entre duas partes, Alice e Bob irão precisar de um canal quântico e um canal clássico. Este último por sua vez pode ser monitorado passivamente por um agente externo - Eva. Já a seguridade do primeiro é validada através das regras da MQ.

Utilizando um sistema de dois níveis, como a polarização de fótons, Alice e Bob escolhem duas bases A $\{|0_A\rangle, |1_A\rangle\}$ e B $\{|0_B\rangle = (1/\sqrt{2})(|0_A\rangle + |1_A\rangle), |1_B\rangle = (1/\sqrt{2})(|0_A\rangle - |1_B\rangle)\}$ compostas por estados ortogonais de polarização que serão utilizadas para transmissão e recepção dos fótons.

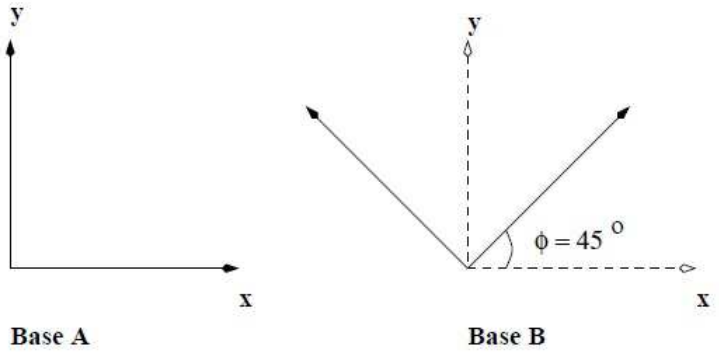

Figura 1.3 Ilustração gráfica das bases escolhidas por Alice e Bob. Na base A temos os estados ortogonais $|0_A\rangle$ e $|1_A\rangle$. A base B pode ser vista como uma rotação da base A num ângulo $\phi = 45^o$, sendo expressa como uma superposição de $|0_A\rangle$ e $|1_A\rangle$. [3]

Em seguida eles irão fazer uso do canal clássico para combinar quais estados ortogonais de quais bases irão representar os bits 0 e 1 que eles desejam enviar. Por exemplo, para a sequência 011011001011 Alice escolhe $|0_i\rangle$ para transmissão de 0 e $|1_i\rangle$ para 1 e então envia os dados na seguinte sequência de base $BABAAAAABBAB$ para os respectivos bits. Após isso, Bob escolhe a base aleatoriamente para fazer a medição e então os dois resolvem revelar publicamente quais bases foram usadas nos procedimentos de envio e medição de cada bit, mas não revelam quais bits foram enviados nem Bob revela o resultado das suas medidas. Em seguida eles consideram apenas os resultados os quais as bases utilizadas coincidiram e descartam os demais, desta forma se Eva não monitorou o envio de dados os resultados revelados por Alice e Bob devem coincidir, do contrário a probabilidade de que estes dados coincidam é praticamente nula.

A tabela abaixo extraída de [3], resume o protocolo $BB84$.

Seqüência de bits de Alice	0	1	1	0	1	1	0	0	1	0	1	1
Bases escolhidas por Alice	B	A	B	A	A	A	A	A	B	B	A	B
Fótons enviados por Alice	$\|0\rangle_B$	$\|1\rangle_A$	$\|1\rangle_B$	$\|0\rangle_A$	$\|1\rangle_A$	$\|1\rangle_A$	$\|0\rangle_A$	$\|0\rangle_A$	$\|1\rangle_B$	$\|0\rangle_B$	$\|1\rangle_A$	$\|1\rangle_B$
Bases escolhidas por Bob	A	B	B	A	A	B	B	A	B	A	B	B
Bits recebidos por Bob	1		1		1	0	0	0		1	1	1
Bob informa fótons detectados	A		B		A	B	B	A		A	B	B
Alice informa bases corretas			OK		OK			OK				OK
Informação compartilhada			1		1			0				1
Bob revela alguns bits da chave					1							
Alice confirma estes bits					OK							
Restante de bits é a chave			1					0				1

Figura 1.4 Tabela contendo resumo do protocolo criptográfico do $BB84$. As primeiras cinco linhas referem-se à transmissão quântica, as outras cinco, à discussão pública entre Alice e Bob e a última representa a chave compartilhada por eles.

Este é o conceito básico de distribução de chaves quânticas deste protocolo. Como não é objetivo deste trabalho a descrição detalhada dos mesmos, recomendamos para um estudo detalhado a leitura das referências [3, 21].

E91

Neste caso, Alice e Bob dispõem de um canal quântico que emite singletos $|\psi\rangle = \frac{1}{\sqrt{2}}|01\rangle - |10\rangle$, [3] o qual Alice recebe uma parte e Bob a outra. Vamos considerar que as partículas viajam até eles na direção z.

Para que possamos explicar como é realizada a distribuição de chave quântica (DCQ) através do protocolo $E91$ precisamos definir duas quantidades essenciais: o coeficiente de correlação de medidas de spin e S. O coeficiente de correlação de medidas de spin é dado por

$$E(a_i, b_j) = P_{00}(a_i, b_j) + P_{11}(a_i, b_j) - P_{01}(a_i, b_j) - P_{10}(a_i, b_j) \tag{1.44}$$

onde os termos P são as probabilidades de obtermos os resultados $(+1, +1), (-1, -1), (+1, -1)$, $(-1, +1)$ ao longo dos vetores unitários a_i, b_j os quais são caracterizados pelos ângulos polar $\theta_i^a(\theta_j^b)$ e azimutal $\phi_i^a(\phi_j^b)$ ilustrados na figura abaixo.

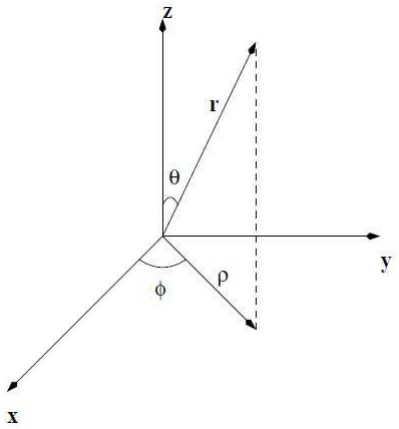

Figura 1.5 Ilustração dos ângulos polares θ e ϕ em coordenadas esféricas, com θ variando de 0 a π e ϕ variando de 0 a 2π.

Depois de realizadas as medidas, o coeficiente de correlação é facilmente calculado. Para um estado puro ele pode ser definido da forma

$$E(a_i, b_j) = \left\langle \psi^- \right| \sigma_{a_i}^A \otimes \sigma_{b_j}^B \left| \psi^- \right\rangle \tag{1.45}$$

onde $\sigma_{a_{i(j)}}^{A(B)} = a_{i(j)} \cdot \sigma^{A(B)}$ e $\sigma^{A(B)} = (\sigma_x^{A(B)}, \sigma_y^{A(B)}, \sigma_z^{A(B)})$.

A quantidade S é definida por

$$S \equiv E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3) \tag{1.46}$$

a qual para valores dos ângulos tais que $\theta_i^a = \theta_j^b = \pi/2$, $\phi_1^a = 0, \phi_2^a = \pi/4, \phi_3^a = \pi/2, \phi_1^b = \pi/4, \phi_2^b = \pi/2, \phi_3^b = 3\pi/4$ teremos

$$S = -2\sqrt{2} \tag{1.47}$$

Calculado $E(a_i, b_j)$, Alice e Bob anunciam publicamente as orientações escolhidas para as medidas e se detectaram ou não seus qbits, descartando aquelas em que eles não foram detectados. Em seguida eles separam as medidas em dois grupos

grupo 1 Grupo das medidas em que Alice e Bob usaram orientações diferentes;

grupo 2 Grupo das medidas em que ambos usaram a mesma orientação.

Então eles anunciam publicamente os resultados obtidos no grupo 1 e a partir daí a quantidade S é calculada. Se o resultado for o mesmo que o citado acima $(-2\sqrt{2})$, então eles poderão usar os dados do grupo 2 como chave criptográfica, do contrário eles terão que descartar todos os seus dados e recomeçar o protocolo.

Devemos observar que neste caso o estado utilizado foi o $|\psi^-\rangle$. A escolha da divisão em grupos é justificada pela orientação dos vetores (a_i, b_j) tendo em vista que uma possível

interferência de um agente externo (Eva) levaria o estado ao colapso o que ocasionaria um valor de S diferente, por isso neste caso todo o protocolo deve ser reiniciado.

Como vemos, o emaranhamento tem grande importância na Teoria da Informação Quântica sendo uma constante fonte de estudo. Uma das prioridades para com a qualidade do seu uso na realização das tarefas da IQ e CQ é, por exemplo, a ***resistência*** ou ***robustez*** (por quanto tempo ele dura em um sistema físico), seu ***grau*** ou a ***quantidade*** de emaranhamento (o quanto dois estados encontram-se emaranhados) e principalmente sua ***caracterização***, ou seja, se as partículas se encontram nesse estado. Visando a busca à estas respostas, foram desenvolvidos vários métodos de caracterizar e quantificar o emaranhamento. Este é o assunto do nosso próximo capítulo.

CAPÍTULO 2

Separabilidade e Quantificação

Neste capítulo serão apresentados alguns critérios de separabilidade de estados quânticos e algumas medidas de emaranhamento, tanto para sistemas bipartites como para sistemas multipartites.

2.1 Estados Bipartites

2.1.1 Separabilidade em estados puros

Vamos considerar um espaço de Hilbert bidimensional. Consideremos ainda que o primeiro subsistema descrito pelos vetores contidos em $\mathcal{H}_\mathcal{A}$ de dimensão d_A pertença à física Alice, enquanto que o segundo subsistema descrito pelos vetores contidos em $\mathcal{H}_\mathcal{B}$ de dimensão d_B pertença ao físico Bob. O estado total do sistema será descrito pelo produto tensorial dos dois espaços $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$, portanto, qualquer vetor contido em $\mathcal{H}$ poderá ser escrito como

$$|\psi\rangle = \sum_{i,j=1}^{d_A,d_B} c_{i,j} |a_i\rangle \otimes |b_j\rangle \tag{2.1}$$

com uma matriz complexa de dimensão $d_A \otimes d_B$. Para simplificar a notação, a partir de agora omitiremos o sinal de produto tensorial: $|a\rangle \otimes |b\rangle \equiv |a\rangle |b\rangle \equiv |ab\rangle$. Podemos agora definir separabilidade para um estado puro.

Definição 2.1. *Um estado puro $|\psi\rangle \in \mathcal{H}$ é chamado de* ***estado produto ou separável*** *se pudermos achar estados tais que $|\phi_A\rangle \in \mathcal{H}_\mathcal{A}$ e $|\phi_B\rangle \in \mathcal{H}_\mathcal{B}$ tal que*

$$|\psi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle \tag{2.2}$$

Do ponto de vista físico, esta definição nos diz que o estado acima encontra-se classicamente correlacionado. Em outras palavras Alice e Bob prepararam seus estados localmente de

forma independente entre si. Neste tipo de estado, a medição de um observável no estado do subsistema A não terá qualquer tipo de efeito sobre uma medição qualquer em B.

Antes de introduzirmos os critérios de separabilidade e quantificação do emaranhamento para estados bi-multipartites, devemos introduzir o conceito de operaçoes locais.

2.1.2 Operações locais estocáticas com comunicação clássica

Quando se trata de estados quânticos bipartites e até mesmo multipartites, as únicas operações que cada um pode realizar em seus respectivos subsistemas são as operações unitárias locais LU. Neste tipo de operações, cada parte - Alice, Bob, Eva... - realiza operações sem interagirem seus subsistemas estando espacialmente separados. No entanto, existe a necessidade de haver uma interação entre as partes com sistemas auxiliares locais além da realização de medidas nos subsistemas.

Vamos considerar um estado bipartite o qual é compartilhado por Alice e Bob que realizam medidas em cada uma de suas partes. Para que suas medidas sejam úteis, é necessário a existência de comunicação clássica entre eles fazendo com que os resultados das medidas sejam passados um para o outro. Este conjunto de operações que servem como um suporte para Alice e Bob no campo da informação e computação quânticas podem ser divididas em dois tipos

LOCC - operações locais com comunicação clássica as quais possuem probabilidade de sucesso 1, de muita importância para os estados emaranhados bipartites. Nestas operações, apenas com a utilização de medidas podemos realizar operações que possuem probabilidade de sucesso 1.

SLOCC - operações estocásticas com comunicação clássica, as quais possuem uma probabilidade de sucesso p, onde $0 < p \leq 1$. Estas são muito úteis quando estamos lidando com estados com mais de duas partes, os multipartites.

Um exemplo de operações LOCC é o exercício apresentado no Chuang e Nielsen [4]. Alice e Bob compartilham o estado

$$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

e querem transformá-lo no estado

$$|\phi_1\rangle = cos\theta\,|00\rangle + sen\theta\,|11\rangle$$

onde $0 \leq \theta \leq \pi/4$. Um dos protocolos para realização desta operação seria a preparação de ϕ_1 por Alice utilizando dois qbits auxiliares e teletransportando um dos qbits para Bob. No entanto, esta tarefa pode ser feita através do uso de operadores quânticos que nos oferecem resultados

mais gerais. Alice utiliza um sistema auxiliar para aplicar os seguintes operadores quânticos no seu qbit

$$M_1 = \begin{bmatrix} cos\theta & 0 \\ 0 & sen\theta \end{bmatrix}; \; M_2 = \begin{bmatrix} sen\theta & 0 \\ 0 & cos\theta \end{bmatrix}$$

A operação no sistema composto pode ser descrita por

$$\rho = M_1 \otimes I_b \left|\phi^+\right\rangle \left\langle\phi^+\right| M_1^\dagger \otimes I_b + M_2 \otimes I_b \left|\phi^+\right\rangle \left\langle\phi^+\right| M_2^\dagger \otimes I_b$$

onde I_b é o operador identidade. Ao final, Alice realiza uma medida no sistema auxiliar para saber qual das operações ocorreu, M_1 ou M_2. Se ocorreu M_1, ela irá obter

$$M_1 \left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(cos\theta \left|00\right\rangle + sen\theta \left|11\right\rangle) = \frac{1}{\sqrt{2}} \left|\phi_1\right\rangle$$

e comunica a Bob o resultado M_1 obtido mostrando que o estado foi transformado corretamente. Caso Alice obtenha M_2, teremos

$$M_2 \left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(sen\theta \left|00\right\rangle + cos\theta \left|11\right\rangle) = \frac{1}{\sqrt{2}} \left|\phi_2\right\rangle$$

assim como no caso anterior, Alice comunica o resultado à Bob sem sucesso (a priori) na transformação do estado. No entanto eles ainda podem obter $|\phi_1\rangle$ corrigindo a falha do resultado. Eles podem utilizar uma opereção local unitária para transformar $|\phi_2\rangle$ em $|\phi_1\rangle$, basta Alice aplicar σ_x no seu qbit e dizer a Bob para realizar a mesma operação na sua parte, obtendo como resultado final $|\phi_1\rangle$ [1].

2.1.3 Decomposição de Schmidt

Basicamente a decomposição de Schmidt é tida como a única forma de se caracterizar o emaranhamento bipartite de um estado puro.

Teorema 2.1. *Seja $|\psi\rangle$ um estado puro de um sistema AB. Logo, existem estados ortonormais $|i_A\rangle$ de A e $|i_B\rangle$ de B tais que [4]*

$$\psi = \sum_i \lambda_i \left|i_A\right\rangle \left|i_B\right\rangle \tag{2.3}$$

em que λ_i são números reais não-negativos satisfazendo $\sum_i \lambda_i^2 = 1$ e são conhecidos como coeficientes de Schmidt.

De acordo com a definição acima, se tomarmos a matriz densidade do estado $|\psi\rangle$ teremos que $\rho^A = \sum_i \lambda_i^2 \left|i_A\right\rangle \left\langle i_A\right|$ e $\rho^B = \sum_i \lambda_i^2 \left|i_B\right\rangle \left\langle i_B\right|$ serão as matrizes reduzidas dos subsistemas A e B respectivamente. Muitas propriedades quânticas do sistema ficam completamente descritas

[1] estados com os mesmos coeficientes de Schmidt podem ser relacionados por uma operação unitária local, que é o caso de $|\phi_1\rangle$ e $|\phi_2\rangle$

através dos autovalores do operador matriz densidade reduzida do estado, de forma que para um sistema composto de um estado puro essas propriedades serão as mesmas, pois possuem os mesmos autovalores, para ambos os subsistemas. De uma forma geral o número de Schmidt $Sch\,|\psi\rangle$ determinará se o estado é emaranhado ou não e ele nos é dado pelo número de autovalores não nulos das matrizes densidade reduzidas. Para estados separáveis esta quantidade é igual a um (apenas um autovalor não nulo).

Como exemplo comentemos sobre os estados $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ e $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$. O primeiro estado (estado de Bell) é conhecidamente emaranhado. Calculando suas matrizes densidades reduzidas e encontrando seus autovalores veremos que ele possui dois coeficiente de Schmidt (autovalor $1/2$ com multiplicidade dois). Seguindo o mesmo procedimento para o segundo estado encontramos apenas um autovalor não-nulo, o que nos diz que temos um estado separável. Obviamente podemos ver que $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Em sistemas bipartites tais que $\{|0_A\rangle, |1_A\rangle\} \in \mathcal{H}_\mathcal{A}$ e $\{|0_B\rangle, |1_B\rangle\} \in \mathcal{H}_\mathcal{B}$, os estados de Bell são considerados de emaranhamento máximo e constituem ao todo quatro pares de qbits a saber

$$\left|\phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.4}$$

$$\left|\phi^-\right\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.5}$$

$$\left|\psi^+\right\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{2.6}$$

$$\left|\psi^-\right\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.7}$$

$$\tag{2.8}$$

os quais aparecem no capítulo anterior, porém sem a nomenclatura usual de estados de Bell.

2.2 Estados Mistos Bipartites

Como visto na secção anterior a classificação se um estado puro bipartite é separável ou não é obtida diretamente através da decomposição de Schmidt, ou através do número de Schmidt ($Sch(|\psi\rangle)$). No caso em que o estado bipartite não é puro, já não podemos aplicar o critério introduzido anteriormente o que nos obriga ir em busca de outra forma de detectarmos o emaranhamento em estados mistos, no entanto para tais situações o critério de separabilidade não é tão imediato. Sistemas compostos com dimensão $\mathcal{C}^2 \otimes \mathcal{C}^4$ ainda não possuem um critério operacional e universal que possibilite testar sua separabilidade, todavia existem vários critérios criados para alguns tipos de estados específicos, de baixas dimensões, na faixa de $(\mathcal{C}^2 \otimes \mathcal{C}^{2,3})$.

Nesta seção definiremos o que é um estado misto separável e faremos um resumo dos principais critérios de separabilidade, operacionais e não-operacionais, para estados bipartites de baixas dimensões.

Considere a seguinte preparação de um sistema bipartite. Vamos supor que Alice consegue preparar o estado $|e_i\rangle$ com probabilidade p_i e comunica através de um canal clássico o resultado de sua preparação a Bob. Bob por sua vez, prepara o estado $|f_i\rangle$ obtendo-se assim o estado conjunto

$$\rho_{AB} = \sum_{i=1}^{M} p_i \, |e_i\rangle \langle e_i| \otimes |f_i\rangle \langle f_i| \tag{2.9}$$

Este estado (2.9) é o mais geral estado bipartite que Alice e Bob conseguem preparar usando operações locais e comunicação clássica.

Definição 2.2. *(Estados bipartites, mistos separáveis e emaranhados) Um estado misto é separável se e somente se pode ser escrito como uma combinação convexa de projetores de estados produzidos localmente, como em (*2.9*).* Caso contrário ele será emaranhado.

Esta definição leva em conta a forma como foi produzido o estado. Um estado pode ser considerado separável se puder ser escrito como uma soma convexa dos produtos dos subsistemas pertencentes a Alice e a Bob.

Uma função $f(\varrho)$ é dita convexa se $f[p\varrho_1 + (1-p)\varrho_2] \leq pf(\varrho_1) + (1-p)f(\varrho_2)$. Deve-se observar que o conjunto dos estados separáveis é um conjunto convexo, o que nos diz diretamente que uma combinação convexa de estados separáveis é novamente um estado separável.

É importante deixar claro que estados emaranhados não podem ser criados apenas por operações locais e comunicação clássica. No caso acima citado, Alice e Bob compartilham entre si um estado não correlacionado ou classicamente correlacionado, ou mais geralmente chamado de estado produto. Isso significa que o emaranhamento só será estabelecido se as partes anteriormente separadas, sofrerem a atuação de um operador unitário e não-local.

Tendo em vista a importância prática dos estados emaranhados, a questão fundamental é como conseguir distinguir sistemas classicamente correlacionados dos que possuem emaranhamento. Vários critérios capazes de identificar esta correlação quântica foram e ainda são desenvolvidos, mas existe ainda a problemática de que nenhuma solução geral para o problema da separabilidade foi encontrada devido a não-operacionalidade das soluções (critérios), ou até mesmo pela limitação dimensional da atuação do mesmo.

2.2.1 Critério de Peres

No ano de 1996, Asher Peres publicou um dos mais importantes critérios de separabilidade desenvolvidos até hoje, o PPT (Positive Parcial Transposition). Aplicável a matrizes

densidade compostas de apenas dois subsistemas, ele é considerado uma condição necessária e suficiente para separabilidade. Além de identificar todos os estados emaranhados com dimensões 2×2 e 2×3, o critério de Peres destaca-se também pela sua operacionalidade, itilizando-se apenas de álgebra linear básica.

Definição 2.3. *Dada a matriz densidade de um estado quântico composto por dois subsistemas*

$$\rho = \sum_{i,j}^{N}\sum_{k,l}^{M} |i\rangle\langle k| \otimes |j\rangle\langle l| = \sum_{i,j}^{N}\sum_{k,l}^{M} |ij\rangle\langle kl| \tag{2.10}$$

podemos definir a transposição parcial de ρ com relação a A como sendo

$$\rho^{T_A} = \sum_{j,i}^{N}\sum_{k,l}^{M} |k\rangle\langle j| \otimes |i\rangle\langle l| = \sum_{j,i}^{N}\sum_{k,l}^{M} |kj\rangle\langle il| \tag{2.11}$$

Se a matriz parcialmente transposta do estado possuir autovalores positivos, teremos um estado separável, e este é chamado um estado PPT [2].

Vamos ilustrar o PPT com um exemplo clássico utilizado por Peres, o estado de Werner

$$\rho_{ij,kl} = xS_{ij,kl} + (1-x)\delta_{ik}\delta_{jl}/4 \tag{2.12}$$

onde x varia no intervalo $0 \leq x \leq 1$, os índices i, j referem-se às linhas e k, l às colunas do primeiro e segundo subsistemas respesctivamente [3].

Este estado é a soma de uma fração x do estado singleto maximamente emaranhado $|\psi^-\rangle$, cuja matriz densidade é representada por $S_{ij,kl} = |\psi^-\rangle\langle\psi^-|$, e uma fração $(1-x)$ do estado separável $I/4$, onde a matriz identidade é representada pelos deltas de Kronecker $\delta_{ik}\delta_{jl}$. A matriz do sistema será

$$\rho_{ij,kl} = \begin{bmatrix} (1-x)/4 & 0 & 0 & 0 \\ 0 & (1+x)/4 & -x/4 & 0 \\ 0 & -x/4 & (1+x)/4 & 0 \\ 0 & 0 & 0 & (1-x)/4 \end{bmatrix} \tag{2.13}$$

Realizando a troca dos índices, ou seja, calculando a transposição parcial da matriz, teremos

[2] do inglês Positive Partial Transposition

[3] esta representação é apenas uma outra variação da representação matricial em termos de bra-ket's utilizada na equação 2.10

$$\rho_{kj,il} = \begin{bmatrix} (1-x)/4 & 0 & 0 & -x/4 \\ 0 & (1+x)/4 & 0 & 0 \\ 0 & 0 & (1+x)/4 & 0 \\ -x/4 & 0 & 0 & (1-x)/4 \end{bmatrix} \tag{2.14}$$

Como autovalores da matriz 2.14 temos os seguintes resultados: $(1-x)/4$ de multiplicidade 3 e um autovalor $(1-3x)/4$. Os três primeiros autovalores $(1-x)/4$ são sempre positivos, tendo em vista que o valor máximo de x é 1 e mínimo é 0. No entanto, $(1-3x)/4$ pode assumir valores negativos se $1/3 < x \leq 1$ sendo um estado emaranhado neste caso e separável quando $0 \leq x \leq 1/3$.

A transposição parcial em estados separáveis atua como uma operação local levando a matriz densidade total do sistema a outra. Para um estado emaranhado, a matriz parcialmente transposta posuirá autovalores negativos não podendo representar um estado físico e dizemos que o estado é NPT [4].

O PPT é o mais simples critério de separabilidade operacional já desenvolvido até hoje e é considerado necessário e suficiente para a detectar estados emaranhados constituídos por duas partes. No caso das dimensões 2×2, 2×3, o seu uso nos dá uma caracterização completa da separabilidade, no entanto foi provado em [22] que para estados bipartites de dimensões acima de 2×3 o PPT não se constitui um bom caracterizador de emaranhamento devido à sua aplicação não conseguir detectar tal propriedade em alguns estados com tais dimensões. Tais estados cuja detecção é falha são classificados como "*bound entanglement*"ou de *emaranhamento preso*.

Emaranhamento Preso

Suponha que A e B sejam usuários distantes compartilhando n cópias idênticas de um estado ρ_{AB} contendo emaranhamento com ruído[5]. Operações locais LOOC (operações locais com comunicação clássica), que denotaremos por $\mathcal{E}$, são aplicadas a este estado através de algum protocolo para que a partir de ρ_{AB} obtenha-se um número m (menor que n) de cópias do sistema em um estado o mais próximo possível de um estado puro (maximamente) emaranhado. O protocolo ótimo, chamado de purificação ou destilação do emaranhamento, é aquele que maximiza no limite assintótico de n grande o quociente $\frac{m}{n}$ o qual por sua vez é chamado de emaranhamento destilável E_D:

$$E_D(\rho_{AB}) \equiv \sup_{\mathcal{E}} \lim_{n\to\infty} \frac{m}{n} \tag{2.15}$$

[4] do inglês Negative Partial Transposition

[5] estados mistos são usados para a representação de ruído em estados puros já que, experimentalmente falando, é muito difícil a produção de estados puros em laboratório devido à decoerência, imperfeições operacionais, dentre outros fatores.

O protocolo de destilação foi incialmente desenvolvido por Bennet *et. al.* [23] com o objetivo principal de lidar com o ruído em estados quânticos emaranhados para poder aproveitar ao máximo as vantagens que o emaranhamento em estados puros oferecem.

Definição 2.4. *Estados mistos os quais o protocolo de destilação não pode ser aplicado de forma que não seja possível a extração de estados emaranhados os mais puros possíveis do sistema descrito por ρ_{AB} são aqueles cujo emaranhamento é preso.*

O PPT está diretamente relacionado a estados com esta característica, pois todo estado PPT com dimensões acima de 2×3 é de fato um estado não destilável [24], ou seja, a falha do Critério de Peres nestas dimensões (estados emaranhados cuja transposição parcial é positiva) é indicadora de emaranhamento preso.

Um exemplo de emaranhamento preso é o estado, introduzido em [25] mostrando justamente a falha da aplicação do critério de Peres. O estado foi construído como segue. Considere o espaço de Hilbert $\mathcal{C}^3 \otimes \mathcal{C}^3$. Seja $P_\phi \equiv |\phi\rangle \langle\phi|$ um projetor e $|e_i\rangle$, com $i = 1, 2, 3$, uma base no espaço $\mathcal{C}^3$. Podemos definir o projetor

$$Q \equiv I \otimes I - \big(\sum_i P_{e_i} \otimes P_{e_i} + P_{e_3} \otimes P_{e_3}\big) \tag{2.16}$$

os vetores,

$$\Psi \equiv \frac{1}{\sqrt{3}}(e_1 \otimes e_1 + e_2 \otimes e_2 + e_3 \otimes e_3) \tag{2.17}$$

$$\Phi_a \equiv e_3 \otimes \big(\sqrt{\frac{1+a}{2}}e_1 + \sqrt{\frac{1-a}{2}}e_3\big),\ com\ 0 \leq a \leq 1. \tag{2.18}$$

e o estado inseparável

$$\rho_{insep} \equiv \frac{3}{8}P_\psi + \frac{1}{8}Q \tag{2.19}$$

A inseparabilidade do estado (2.19) é proveniente do estado altamente emaranhado P_Ψ, enquanto que o estado P_{Φ_a} é evidentemente separável. Através dos vetores e estados acima, podemos ainda definir um outro estado

$$\rho_a = \frac{8a}{8a+1}\rho_{insep} + \frac{1}{8a+1}P_{\Psi_a} \tag{2.20}$$

cuja matriz densidade possui a forma

$$\rho_a = \frac{1}{8a+1}\begin{bmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2}+\frac{a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & 0 & a & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1}{2}+\frac{a}{2} \end{bmatrix} \tag{2.21}$$

A aplicação do PPT na matriz (2.21) nos leva a um falso resultado, indicando que (2.20) seria provavelmente um estado separável, sendo no entanto emaranhado como é provado em [25]. Por isto este estado é considerado um *bound entanglement*, ou um estado de emaranhamento preso.

PPT como um mapa não-completamente positivo

A atuação do Critério de Peres é baseada na aplicação de mapeamentos não-completamente positivos (não CP) os quais testam a negatividade do operador no qual está sendo atuado. Um mapa $\mathcal{E}$ é considerado completamente positivo se $\forall\rho \in \mathcal{B}(\mathcal{H}_B), \rho \geq 0 \Rightarrow \mathcal{E}(\rho) \geq 0$ [26]. Em palavras, para um operador ρ pertencente ao espaço de operadores $\mathcal{B}(\mathcal{H}_B)$ no espaço de Hilbert, a atuação do mapa $\mathcal{E}$ leva (mapeia) ρ em um operador ainda positivo pertencente ao mesmo espaço. No caso de dois subsistemas, se considerarmos um mapa composto de um produto tensorial no qual temos um mapa positivo atuando no primeiro subsistema e a identidade no segundo, muitas propriedades do sistema total podem ser obtidas.

Um mapa completamente positivo atuando em um estado qualquer, seja ele separável ou emaranhado, jamais identificará emaranhamento por preservar a positividade da matriz densidade em questão. Portanto, os responsáveis pela identificação do emaranhamento no PPT são os mapas *não completamente positivos* que preservam a positividade apenas das matrizes de estados separáveis. Um exemplo de um operador não CP é a transposição

$$[I_A \otimes T_B](\rho_{AB}) = \rho^{T_B} \tag{2.22}$$

onde I_A é o operador identidade e T_B é o operador de transposição atuando no segundo subsistema. É evidente que I_A é positivo, T_B também é positivo (P) mas não completamente positivo (CP) pois no caso de 2.22 nem todo estado $\rho^{T_B} \geq 0$, então o uso de um mapa não (CP) é usado por Peres para se fazer a detecção do emaranhamento.

No nosso trabalho, faremos uso constante do PPT inclusive nos estados multipartites onde para tais introduziremos o seu uso mais adiante. A seguir falaremos brevemente de alguns critérios de separabilidade sem entrar em detalhes pois seu uso não será objetivo deste trabalho.

2.2.2 Outros critérios

Critério do Realinhamento

Existe ainda uma forte classe de critérios baseados na contração linear de estados produtos. Eles derivam de um novo critério desenvolvido por Rudolph [27] e Chen [28] chamado *critério da norma cruzada* ou *critério do realinhamento de matrizes (CCNR)*[6] o qual é operacional e independente do PPT. Em termos de elementos de matriz, ele pode ser definido como [15]

Teorema 2.2. *Se o estado ρ é separável, então a matriz $\mathcal{R}(\rho)$, onde $\mathcal{R}$ é um maepamento contrativo, com elementos*

$$\langle i| \langle j| \mathcal{R}(\rho_{AB}) |k\rangle |l\rangle \equiv \langle i| \langle k| \rho |l\rangle |j\rangle \tag{2.23}$$

possui norma do traço[7] *menor que um.*

$$||\mathcal{R}(\rho_{AB})|| \leq 1 \tag{2.24}$$

Isto pode ser formalmente generalizado como segue

Teorema 2.3. *Seja $\mathcal{R}$ um mapa contrativo, ou de contração. Se $\mathcal{R}$ satisfaz*

$$||\mathcal{R}(|\phi_A\rangle \langle\phi_A| \otimes |\phi_B\rangle \langle\phi_B|)|| \leq 1 \tag{2.25}$$

para todo estado produto puro $|\phi_A\rangle \langle\phi_A| \otimes |\phi_B\rangle \langle\phi_B|$, então para qualquer separável ρ_{AB} temos $||\mathcal{R}(\rho_{AB})|| \leq 1$.

O mapa de realinhamento de matrizes $\mathcal{R}$ o qual permuta os elementos da matriz só satisfaz a contração acima em estados produtos. Achar contrações interessantes deste tipo que não são equivalentes ao realinhamento é ainda um problema aberto. Notavelmente, o realinhamento encontra alguns emaranhamentos PPT [27, 28].

Um exemplo explícito da atuação de $\mathcal{R}$ numa matriz densidade que representa um estado bipartite geral é dado a seguir:

$$\rho = \left[\begin{array}{cc|cc} \rho_{11} & \rho_{12} & \rho_{13} & \rho_{14} \\ \rho_{21} & \rho_{22} & \rho_{23} & \rho_{24} \\ \hline \rho_{31} & \rho_{32} & \rho_{33} & \rho_{34} \\ \rho_{41} & \rho_{42} & \rho_{43} & \rho_{44} \end{array}\right] \rightarrow \mathcal{R}(\rho) = \left[\begin{array}{cccc} \rho_{11} & \rho_{21} & \rho_{12} & \rho_{22} \\ \hline \rho_{13} & \rho_{23} & \rho_{14} & \rho_{24} \\ \hline \rho_{31} & \rho_{41} & \rho_{32} & \rho_{42} \\ \hline \rho_{33} & \rho_{43} & \rho_{34} & \rho_{44} \end{array}\right]$$

De fato, o critério CCNR permite provar que existe emaranhamento em muitos estados em que o PPT falha. Combinado com sua simplicidade, ele se torna uma ferramenta útil na análise do emaranhamento, no entanto, também não detecta emaranhamento em todos os estados bipartites. Contudo, podemos visualizá-lo como uma complementação para o critério de Peres.

[6] do inglês computable cross norm or realigment criterion

[7] a norma do traço de uma matriz é dada por $||X|| = Tr\sqrt{(XX^{\dagger})}$

Na seção anterior vimos em resumo que se tivermos um operador (mapa) positivo ou não completamente positivo atuando em um estado produto, este será levado a um outro estado produto. No caso de um estado emaranhado, um operador positivo conserva a positividade da matriz densidade levando-a de uma matriz densidade à outra, não detectando o emaranhamento, portanto no critério de Peres, temos como fator primordial a aplicação de operadores não-completamente positivos para a detecção do emaranhamento.

O ponto essencial do realinhamentó é o uso de certos tipos específicos de mapas lineares $\mathcal{L}$, atuando em ambos os subsistemas, que diminuem a norma do traço de estados produto [29]

$$||\mathcal{L}(\sigma_A \otimes \sigma_B)|| \leq 1$$

assim, para estados separáveis teremos $||\mathcal{L}(\rho_{AB}^{sep})|| \leq 1$. Portanto, qualquer mapa linear que não aumente a norma dos estados produtos, constitue uma condição necessária para separabilidade. Para algum estado, pode ocorrer que $||\mathcal{L}(\rho_{AB})|| > 1$, indicando emaranhamento.

Para fazer uma analogia com os mapas não-completamente positivos, vamos considerar $\mathcal{L}$ atuando apenas em um subespaço. Se $\mathcal{L}$ é uma contração da norma do traço, ou seja, se ele não aumenta a norma do traço, então teremos em estados produtos

$$||(I \otimes \mathcal{L})(\sigma_A \otimes \sigma_B)|| = ||\sigma_A||||\mathcal{L}(\sigma_B)|| \leq 1$$

Portanto, no estudo do emaranhamento através realinhamento, ao invés de mapas positivos, nós temos contrações e ao invés da positividade checa-se a norma do traço. Deve-se fazer a seguinte observação: se o mapa $I \otimes \mathcal{L}$ é por si só uma contração, todos os estados obedecerão ao critério. No entanto, os mapas relevantes não são os mapas de contração apenas, mas sim os de *não contração completa*. Um exemplo deste tipo de mapa é a transposição parcial que além de ser de contração não completa, é também não completamente positivo. Uma discussão deste tipo de mapa no contexto geral de álgebra matricial pode ser vista em [30].

Podemos usar como exemplo do realinhamento, o estado de Werner (2.12) apresentado na seção anterior. Sua matriz densidade realinhada toma a forma

$$\tilde{\rho} = \begin{bmatrix} \frac{1-x}{4} & 0 & 0 & \frac{1+x}{4} \\ 0 & \frac{-x}{4} & 0 & 0 \\ 0 & 0 & \frac{-x}{4} & 0 \\ \frac{1+x}{4} & 0 & 0 & \frac{1-x}{4} \end{bmatrix} \tag{2.26}$$

A norma do traço pode ser facilmente calculada, [8] e nos dá como resultado $||\tilde{\rho}|| = 1/2 + x$.

[8] enquanto Rudolph define o realinhamento como a norma do traço em [27], Chen *et al* em [28] faz a definição do relinhamento em termos da soma dos valores singulares da matriz realinhada. Os dois procedimentos matemáticos podem ser ditos equivalentes.

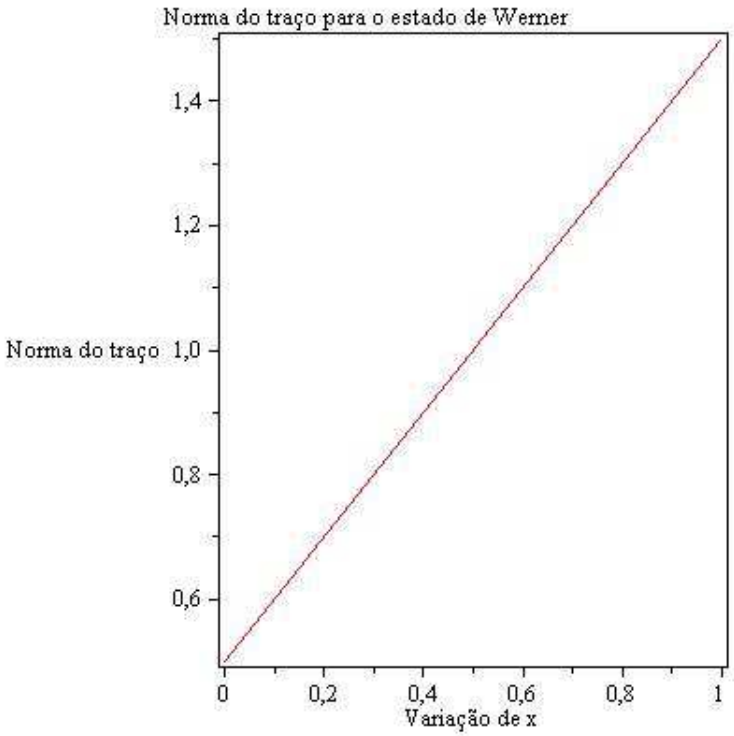

Figura 2.1 Caracterização do emaranhamento do estado de Werner bipartite através do realinhamento.

Neste caso, o estado será separável para valores de $0 \leq x \leq 1/2$. Note que o intervalo de separabilidade deste estado no realinhamento é maior que o encontrado pelo de Peres.

Figura 2.2 Comparação entre o inetervalo de separabilidade encontrado pelo PPT (linha de baixo) e pelo realinhamento (linha de cima). Nota-se que o PPT nos dá um intervalo de separabilidade menor.

Mesmo com essa grande diferença no intervalo, para o caso bipartite em baixas dimensões, o PPT é ainda considerado um critério necessário e suficiente de separabilidade apenas em dimensões mais baixas $(2 \otimes 2)$ e $2 \otimes 3$ [31].

Critério da Permutação ou GPT(Generalized Partial Transposition)

O critério da Permutação é uma generalização do critério de Peres e do Realinhamento ao mesmo tempo (CCNR) o qual usa como base contrações lineares e permutações. Dada uma matriz densidade

$$\rho = \sum_{ij,kl} \rho_{ijkl} \left|i\right\rangle \left\langle j\right| \otimes \left|k\right\rangle \left\langle l\right| \tag{2.27}$$

expandida no produto das bases, toda a informação do estado está contida nos coeficientes ρ_{ijkl}. Para estados puros normalizados teremos que a norma do traço será $||\rho_{ijkl}|| = 1$, onde ρ_{ijkl} é considerada como uma matriz $d_A^2 \times d_B^2$. Para estados produtos, ou seja, separáveis, qualquer permutação $\pi(ijkl)$ dos índices i, j, k, l nos levará a um tensor também com $||\rho_{ijkl}|| = 1$.

Verifica-se ainda que, no caso bipartite, apenas duas permutações produzem critérios de separabilidade independentes, resultando nas condições

$$||\rho_{\textbf{(ijlk)}}|| \leq 1 \tag{2.28}$$

$$||\rho_{\textbf{(ikjl)}}|| \leq 1 \tag{2.29}$$

onde a primeira equação refere-se à permutação realizada pelo no PPT e a segunda ao realinhamento. Portanto podemos ver que este critério, como dito antes, nada mais é que uma forma de generalizar estes dois critérios num único formalismo.

Apesar de o critério da permutação ter sido introduzido nesta seção, que trata de estados bipartites, sua aplicação é estendida para estados multipartites.

Emaranhamento testemunha (Entanglement witness)

Existe ainda uma outra forma de detecção do emaranhamento bem conhecida no entanto não operacional. Os critérios citados anteriormente são baseados em operações aplicadas diretamente à matriz densidade ρ do estado, implicando que ρ deve ser previamente conhecida, entretanto existe um critério necessário e suficiente para a detecção do emaranhamento em termos de medidas diretas de observáveis o qual é chamado de *emaranhamento testemunha*.

Definição 2.5. *Um observável $\mathcal{W}$ é chamado um emaranhamento testemunha se*

- $Tr(\mathcal{W}\rho) \geq 0$ *para todos os estados ρ separáveis,*
- $Tr(\mathcal{W}\rho) < 0$ *para ao menos um estado emaranhado*

Segue-se que para uma medida $Tr(\rho\mathcal{W}) < 0$ sabemos com certeza que o estado é emaranhado. Note a semelhança entre o PPT e o emaranhamento testemunha: os dois baseiam-se de certa forma no estudo da positividade da matriz densidade após realizada alguma operação na mesma. O fato deste critério basear-se em medidas diretas de quantidades faz dele uma ferramenta muito útil para a análise experimental do emaranhamento, sendo um dos principais métodos para sua detecção.

Teorema 2.4. *Para cada estado emaranhado ρ existe um emaranhamento testemunha que detecta seu emaranhamento.*

Embora este teorema afirme que qualquer estado emaranhado pode, em princípio, ser detectado pelo operador testemunha, o principal obstáculo é a própria construção deste operador, o que não é um problema trivial tendo em vista que a solução dele seria também a solução para o problema de separabilidade.

O emaranhamento testemunha possui uma representação geométrica. O conjunto de estados em que $Tr((W)\rho) = 0$ está contido em um hiperplano no conjunto de todos os estados, cortando-o em duas partes. Na parte com $Tr((W)\rho) > 0$ encontra-se o conjunto de todos os estados separáveis, a outra parte a qual $Tr((W)\rho) < 0$ é o conjunto dos estados detectados por (W), como se vê na figura 2.3 [16].

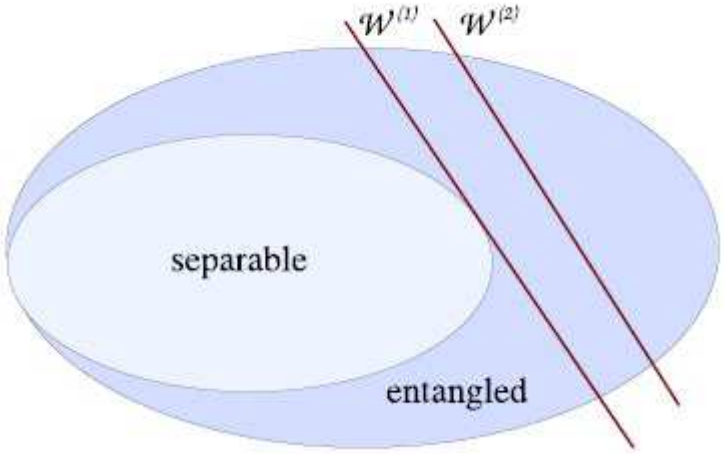

Figura 2.3 Representação geométrica dos estados detectados por (W). As linhas (W_1) e (W_2) representam os hiperplanos em que $Tr((W)\rho) = 0$. Aqui temos a representação de dois witness onde (W_1) detecção melhor que (W_2).

Como construir o operador testemunha num caso bipartite? Vamos aqui exemplificar fazendo uso de um estado ρ_e que possui transposição parcial negativa. Isto quer dizer que ele possui um autovalor negativo correspondente a um certo autovetor $|\eta\rangle$. O operador $\mathcal{W}$ possui então a forma [16]:

$$\mathcal{W} = |\eta\rangle \langle\eta|^{T_A} \tag{2.30}$$

sendo 2.30 a testemunha do emaranhamento contida em ρ_e. Se ρ_e é emaranhado e detectável por algum mapa não completamente positivo Λ, então $I \otimes \Lambda$ também possui autovalor negativo para o autovetor $|\eta\rangle$.

Note que a construção do operador testemunha $\mathcal{W}$ para o caso do critério de Peres foi fácil e que ele é formado por um autovetor da matriz densidade parcialmente transposta. Isto explicita a dificuldade do uso deste critério devido à sua forte dependência com a forma de cada estado. Vale ressaltar que para cada caso de violação de outros critérios de separabilidade o operador testemunha possui uma construção[9].

[9]note também a dependência da construção do operador $\mathcal{W}$ com a violação de um critério qualquer

Uma aplicação importante do emaranhamento testemunha em experimentos foi no problema do emaranhamento macroscópico à temperatura finita [32]. O seu uso possibilitou a identificação de um limiar de temperatura para a existência do emaranhamento. A primeira análise explícita do emaranhamento em estados térmicos foi feita em por Nielsen. Uma observação fundamental é que a teoria do emaranhamento testemunha pode ser explorada para detectar o emaranhamento em estados térmicos em geral, incluindo os casos multipartites. Como já dito anteriormente, o uso deste critério não é do nosso interesse aqui portanto nos absteremos de entrar em mais detalhes. Para uma análise resumida e ao mesmo tempo mais abrangente que a aqui apresentada, recomendamos a leitura de [15], [16].

2.3 Estados multipartites

Estados Puros

Para o caso de estados multipartite, devemos considerar dois tipos de separabilidade: a total e a parcial.

Teorema 2.5. *Seja um estado quântico $|\psi\rangle \subset \mathcal{H}_{1,\ldots,N} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_N$. Se $|\psi\rangle$ for completamente separável, pode ser escrito na forma*

$$|\psi\rangle_N = |\phi_1\rangle \otimes \ldots \otimes |\phi_N\rangle \tag{2.31}$$

No caso de um estado parcialmente separável, a análise é feita tomando uma bipartição $k, N-k$.

Teorema 2.6. *Dado o estado multipartite $|\psi\rangle \subset \mathcal{H}_{1,\ldots,N}$, ele pode ser considerado biseparável numa bipartição qualquer $k, N-k$ se puder ser escrito na forma*

$$|\psi\rangle_N = |\phi_k\rangle \otimes |\phi_{N-k}\rangle \tag{2.32}$$

podendo estar emaranhado para qualquer outra bipartição.

A partir de então, para um critério ser aplicado a este tipo de estado para testar sua biseparabilidade, deve-se tratar o grupo de qbits representado pela bipartição k como uma parte (A) e a outra bipartição $N-k$ como a outra parte (B,) resumindo todas as operações - ou mapeamentos - de tal critério a apenas estes dois grupos.

Teorema 2.7. *Um estado puro pode ser chamado genuinamente emaranhado se não possuir nenhuma bipartição.*

Um exemplo de estados completamente emaranhados são os estados GHZ e W os quais falaremos brevemente a seguir.

Estados GHZ e W

Estados GHZ

No espaço de Hilbert 2^N dimensional existem 2^N estados GHZ independentes tendo a forma

$$|GHZ\rangle^n = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}) \tag{2.33}$$

Estes estados foram introduzidos por Daniel M. Greenberger, Michael A. Horne e Anton Zeilinger, com o objetivo de provar o Teorema de Bell [33], desde então vêm sendo intensivamente estudados devido à sua vasta aplicabilidade incluindo protocolos criptográficos [34, 35], computação quântica [36], compartilhamento secreto quântico [37], teletransporte [38], metrologia quântica e espectroscopia aprimorada de emaranhamento [39, 40].

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

$$Tr_k\Big(|GHZ\rangle^n \langle GHZ| \Big) = I_{n\backslash k} \tag{2.34}$$

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

Por exemplo, considere um estado GHZ de 3 qbits. Quando se faz o traço sobre um dos três sistemas, obtém-se

$$Tr_3\Big[\Big(|000\rangle + |111\rangle \Big)\Big(\langle 000| + \langle 111| \Big)\Big] = |00\rangle \langle 00| + |11\rangle \langle 11| \tag{2.35}$$

que é um estado misturado não emaranhado. Este estado obtido em (2.35) certamente tem correlações de duas partículas (qbits), mas essas são de natureza clássica.

Estados GHZ podem ser chamados de maximamente emaranhados no sentido multipartite. Definindo-se a decomposição de Schmidt generalizada com sendo [10]

$$|\psi_{A_1 \ldots A_n}\rangle = \sum_{i=1}^{min\{d_{A_1},\ldots,d_{A_n}\}} a_i \left|e^i_{A_1}\right\rangle \otimes \ldots \otimes \left|e^i_{A_n}\right\rangle \tag{2.36}$$

para um estado $|\psi_{A_1 \ldots A_n}\rangle$ de n-partículas, pode-se facilmente verificar que os estados GHZ admitem decomposição de Schmidt generalizada.

Em geral, um estado admite decomposição de Schmidt se, realizando o traço em qualquer subsistema, o resto do sistema está em um estado completamente separável. Isto é realmente verdade para os estados GHZ.

[10] um estudo detalhado da generalização da decomposição de Schmidt pode ser encontrado em [41–46].

Estados W

Os estados W por sua vez podem ser escritos na forma geral

$$|W_N\rangle = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} \left|2^j\right\rangle \tag{2.37}$$

na base binária. Por exemplo, para $N = 3, 4, ...$ teremos

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{3}}(\left|2^1\right\rangle + \left|2^2\right\rangle + \left|2^3\right\rangle) = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \qquad (2.38) \\ |\psi_4\rangle &= \frac{1}{\sqrt{4}}(\left|2^1\right\rangle + \left|2^2\right\rangle + \left|2^3\right\rangle + \left|2^4\right\rangle) \\ &= \frac{1}{\sqrt{4}}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle) \qquad (2.39) \end{aligned}$$

De acordo com a classificação de estados dada por meio de operações locais estocásticas assistida por comunicação clássica (stochastic local operations assisted by classical communication - SLOCC, em inglês), existem de fato somente duas classes de estados de três qbits que são verdadeiramente emaranhamentos tripartite, que correspondem aos estados GHZ e aos chamados estados W, respectivamente [47]. Além disso nenhum dos dois tipos de estados pode ser transformado no outro através de tais operações, sendo assim, W e GHZ representam dois tipos totalmente diferentes de estados emaranhados.

Os estados GHZ são a superposição de dois estados maximamente distintos. Foi mostrado que eles levam a uma violação máxima do realismo local [48, 49] sendo os únicos estados que conduzem a uma violação máxima das desigualdades de Bell [50]. Por esta razão, eles podem ser considerados os estados multipartites com máximo emaranhamento.

Ao contrário do estado $|GHZ_3\rangle$, realizado um traço parcial em um dos qbits em $|W_3\rangle$, os outros dois qbits continuam emaranhados, mostrando uma robustez maior diante de perda de partículas, não admitindo decomposição de Schmidt generalizada [51]. De fato, os estados W são aqueles que possuem o máximo possível de emaranhamento bipartite em estados reduzidos de dois qbits [52, 53]. Um fato interessante é que o estado $|W_3\rangle$ é um caso especial dos estados Dicke[11] [54] os quais foram investigados no estudo de emissão de luz de nuvens de átomos em 1954.

2.3.1 Estados mistos

Da mesma forma que para estados bipartites, os estados multipartites mistos são descritos por uma mistura estatística de estados puros via uma combinação convexa. Um estado misto

[11] os estados de Dicke são em geral, autoestados simultâneos dos operadores momento angular J_z e J^2

é completamente separável ρ^{cs} se puder ser escrito como uma combinação convexa de estados puros completamente separáveis $|\phi_i\rangle$, com um peso estatístico p_i

$$\rho^{cs} = \sum_i |\phi_i^{cs}\rangle \langle\phi_i^{cs}| \tag{2.40}$$

Esta mesma linha de raciocínio é válida para a definição de estados mistos não completamente separáveis e completamente emaranhados: Um estado quântico misto ρ^{bs} é chamado não completamente separável (separável com respeito a apenas alguma(s) bipartição(ões) $(k, N-k)$ se puder ser escrito como uma combinação convexa de estados puros associados a probabilidades p_i, sendo biseparáveis com respeito à(s) mesma(s) bipartição(s)

$$\rho^{bs} = \sum_i p_i \left|\phi_i^{bs}\right\rangle \left\langle\phi_i^{bs}\right| \tag{2.41}$$

Da mesma forma, estados mistos completamente emaranhados são escritos como uma combinação convexa de estados puros completamente emaranhados com respeito a qualquer bipartição $k, N-k$. Novamente, existem duas importantes classes de estados mistos completamente emaranhados, a primeira na qual é formada por uma mistura estatística de estados W e a segunda por estados GHZ, de onde podem ser destilados em um ou noutro, respectivamente.

2.3.2 PPT adaptado

Na seção 2.2 dissemos que uma solução geral para o estudo do emaranhamento de estados compostos por duas partes era ainda uma questão aberta. No caso de estados compostos por três ou mais qbits este problema é ainda maior devido ao próprio número de partículas do sistema, todavia um dos recursos que podem facilitar tal tarefa é o uso de suas bipartições para estudar sua separabilidade parcial. Podemos tomar um exemplo já citado aqui, que é o $|GHZ_3\rangle$. Sabe-se que este estado possui emaranhamento total e parcial, sendo classificado como maximamente emaranhado

$$|GHZ_3\rangle = \frac{1}{\sqrt{2}} |000\rangle + |111\rangle \tag{2.42}$$

Tomando sua matriz densidade e uma bipartição da forma $k = 1, N-k = 2$, podemos tratar o estado como se fosse bipartite e aplicar o PPT. Transpondo qualquer uma das partes em questão, a matriz ρ_{GHZ_3} do estado toma a forma

$$\rho_{GHZ_3}^{T^{BC}} = |000\rangle \langle 000| + |011\rangle \langle 100| + |100\rangle \langle 011| + |111\rangle \langle 111| \tag{2.43}$$

a qual possui um autovalor negativo $\frac{-1}{2}$ indicando emaranhamento entre essa duas partes. O mesmo procedimento feito para qualquer que seja a bipartição $AB|C, AC|B$, encontrará ao menos um autovalor negativo que indicará o emaranhamento entre as partes e portanto o com-

pleto emaranhamento do estado $|GHZ_3\rangle$ em questão. O PPT adaptado aos estados multipartites pode também ser aplicado ao estado $|W_3\rangle$ obtendo a matriz parcialmente transposta

$$\begin{aligned}\rho_{W_3}^{T^{BC}} &= |100\rangle\langle 100| + |110\rangle\langle 000| + |101\rangle\langle 000| + |000\rangle\langle 110| \\ &+ |010\rangle\langle 010| + |001\rangle\langle 010| + |000\rangle\langle 101| + |010\rangle\langle 001| + |001\rangle\langle 001|\end{aligned} \tag{2.44}$$

a qual possui um autovalor negativo $\frac{-\sqrt{2}}{3}$. Da mesma forma obteremos ao menos um autovalor negativo para o estudo da separabilidade em qualquer de suas bipartições.

Tomamos outros estados puros utilizados em [55] e aplicamos o PPT para estudar sua atuação em cada um

estado	autovalor negativo	classificação PPT
$W = \frac{1}{2}\|0001\rangle + \|0010\rangle + \|0100\rangle + \|1000\rangle$		
AB|CD	$\frac{-1}{2}$	estado emaranhado
ABC|D	$\frac{-\sqrt{3}}{4}$	estado emaranhado
$\|\phi^+\phi^+\rangle$		
AB|CD	nenhum	estado separável
ABC|D	-1	estado emaranhado

O estado $|\phi^+\phi^+\rangle$ é formado pelo produto tensorial entre dois estados de Bell $|\phi^+\rangle$ explicitados em 2.4. Este exemplo é interessante pois mostra que tratando-os individualmente (na bipartição $AB|CD$) vemos que eles não possuem qualquer tipo de correlação quântica, no entanto se estudarmos qualquer outro tipo de bipartição, ($A|BCD$, $ABC|D$, $AC|BD$) por exemplo, encontraremos emaranhamento entre as partes.

O PPT para caso multipartite pode também ser visto como uma condição da norma do traço, como foi introduzido anteriormente. A matriz densidade escrita como um produto das bases

$$\rho = \sum_{i_1,j_1,\ldots,i_N,j_N} p_{i_1,j_1,\ldots,i_N,j_N} |i_1\rangle\langle j_1| \otimes \ldots \otimes |i_N\rangle\langle j_N| \tag{2.45}$$

será separável se

$$||\rho_{\pi(i_1,j_1,\ldots,i_N,j_N)}|| \leq 1 \tag{2.46}$$

onde π é uma permutação arbitrária dos índices. Como já vimos, para o caso bipartite existe apenas duas permutações não equivalentes as quais correspondem ao PPT e Realinhamento respectivamente.

Existem ainda vários outros critérios para estados multipartites já desenvolvidos e ainda em desenvolvimento os quais não são interessantes para nosso estudo. Para conhecimento, recomendamos a leitura de (dentre vários) [15, 16, 56–58], onde os dois primeiros são artigos de revisão e os três últimos são novos critérios desenvolvidos mais recentemente.

2.4 Quantificação

Se a tarefa de identificar o emaranhamento já é de certa forma difícil por possuir vários fatores que comprometem o objetivo, tais como a dimensão do estado, podemos dizer que quantificá-lo é um pouco mais exaustivo. Entretanto, nos últimos anos tem sido feito um esforço muito grande em busca de bom quantificadores do emaranhamento de onde o qual sugiram algumas medidas simples e ao mesmo tempo operacionais tais como a medida de Schmidt e a Negatividade que serão tratadas nesta seção.

2.4.1 Propriedades gerais

As medidas de emaranhamento devem quantificar a quantidade de emaranhamento presente nos estados, e para tal, qualquer método desenvolvido deve obedecer certas propriedades que serão citadas abaixo. No entanto, deve-se ressaltar que nem todas as propiedades listadas a seguir são satisfeitas por alguns quantificadores.

1. Qualquer medida $E(\rho)$ de emaranhamento deve ser zero para um estado separável;

2. *Invariância diante transformações unitárias* Uma medida de emaranhamento $E(\rho)$ deve ser invariante diante de uma mudança de base local, o que implica que ela também deve ser invariante diante de transformações unitárias locais

$$E(\rho) = E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger) \tag{2.47}$$

3. *Monotonicidade.* $E(\rho)$ não deve aumentar diante de LOCCs ou seja, ele é monotônico diante de operações locais assistidas por comunicação clássica. Se Λ^{LOCC} é um mapa positivo que pode ser implementado através de LOCC, então

$$E[\Lambda^{LOCC}(\rho)] \leq E(\rho) \tag{2.48}$$

Podemos ainda tratar desta propriedade com respeito ao valor médio. Se uma transformação LOCC mapeia ρ em estados ρ_k, com probabilidades p_k, então $E(\rho)$ não deve aumentar o valor médio diante de operações locais

$$\sum_k E(\rho_k) \leq E(\rho) \tag{2.49}$$

4. *Convexidade.* Uma propriedade satisfeita pela maioria dos quantificadores é que a medida de emaranhamento seja convexa ou seja, que o emaranhamento diminua seu valor diante de dois ou mais estados e estados mistos

$$E(\sum_k p_k \rho_k) \leq \sum_k p_k E(\rho_k) \tag{2.50}$$

Esta inequação expressa o fato de que se temos um conjunto de estados ρ_k e perdemos informação uma única instância de ρ_k, então o emaranhamento diminui.

5. *Aditividade*. Outra questão surge se tivermos mais de duas cópias do estado em questão. Se Alice e Bob compartilham n cópias do mesmo estado ρ, é razoável exigir aditividade.

$$E(\rho^{\otimes n}) = nE(\rho) \tag{2.51}$$

Para diferentes estados a aditividade completa é requisitada. Suponha que Alice e Bob compartilham os estado ρ_1 e ρ_2 respectivamente, então

$$E(\rho_1 \otimes \rho_2) = E(\rho_1) + E(\rho_2) \tag{2.52}$$

2.4.2 Medida de Schmidt

J. Eisert e H. J. Briegel introduziram esta funcional medida em 2001 baseada no rank de Schmidt de um estado puro bipartite[12] [55].

Teorema 2.8. *Considere um sistema quântico N-partite $A_1, \ldots, A_N$ o qual suporta subsistemas de dimensão $d_1, \ldots, d_N$. O espaço de estados do sistema composto é dado por $\mathcal{S}(\mathcal{H})$, onde $\mathcal{H} = \mathcal{C}^{d_1} \otimes \ldots \otimes \mathcal{C}^{d_N}$. Qualquer $|\psi\rangle \in \mathcal{H}$ é escrito na forma*

$$|\psi\rangle = \sum_{i=1}^{R} \alpha_i \left|\psi^i_{A_1}\right\rangle \otimes \ldots \otimes \left|\psi^i_{A_N}\right\rangle \tag{2.53}$$

onde $\alpha_i \in \mathcal{C}$, $i = 1, \ldots, R$. Seja r o número mínimo de termos produtos R numa decomposição de ψ. A medida de Schmidt é definida como

$$P(|\psi\rangle \langle\psi|) = \log_2 r \tag{2.54}$$

No caso bipartite, o número mínimo de termos produtos r é dado pelo rank de Schmidt do estado. Esta medida pode ser vista como uma generalização do rank de Schmidt para sistemas multipartites, o qual também pode ser aplicado a estados mistos.

[12] como vimos na primeira seção deste capítulo, a classificação da separabilidade de um estado puro é dada pelo número de coeficientes de Schmidt, o qual é também chamado de rank de Schmidt.

Uma vez que P é definido para estados puros, sua definição pode ser naturalmente extendida para estados mistos.

Teorema 2.9. *Dado um estado quântico representado pela matriz densidade $\rho \in \mathcal{S}(\mathcal{H})$, a medida de Schmidt é dada por*

$$P(\rho) = min \sum_i \lambda_i P(|\psi_i\rangle \langle\psi_i|) \tag{2.55}$$

onde o mínimo é tomado com relação à todas as possíveis combinações convexas da forma $\rho = \sum_i \lambda_i |\psi_i\rangle \langle\psi_i|$ em termos dos estados puros $|\psi_1\rangle \langle\psi_1|, |\psi_2\rangle \langle\psi_2|, \ldots, |\psi_i\rangle \langle\psi_i|$ com $0 \leq \lambda_i \leq 1$ para todo i.

Todas as propriedades citadas das medidas de emaranhamento são satisfeitas pela medida de Schmidt (MS) [55, 59].

A quantificação do emaranhamento feita pela MS leva em conta tanto o emaranhamento geral do sistema quanto o parcial ou seja, com relação às partições[13] as quais o autor [55] chama de k-splits. Neles, há a junção de dois ou mais qbits sendo considerados como apenas uma parte, por exemplo, num estado com k-split do tipo AB(CDE) temos três partes: A, B e (CDE).

Estados Puros

A aplicação da medida de Schmidt em estados puros é praticamente direta, principalmente no que se refere aos estados W e GHZ os quais já estão com o número de produtos termos o mais reduzidos possível. Abaixo temos uma tabela com alguns estados (alguns deles usados para exemplificar o critério de Peres aplicado a estados multipartites) e o valor de suas respectivas medidas.

	GHZ	W	$\|\phi_4\rangle$	$\|\phi^+\rangle \|\phi^+\rangle$
ABCD	$\log_2 2 = 1$	$\log_2 4 = 2$	$\log_2 4 = 2$	$\log_2 4 = 2$
(AB)CD	1	$\log_2 3$	1	1
(AB)(CD)	1	1	1	0
(AC)(BD)	1	1	2	2
(ABC)D	1	1	1	1

Tabela 2.1 Valores da medida de Schmidt definida por $P(|\psi\rangle \langle\psi|) = \log_2 r$ para os estados $|GHZ_4\rangle$, $|W_4\rangle$, $|\phi_4\rangle = (|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)/2$ e o produto de dois estados maximamente emaranhados $|\phi^+\rangle |\phi^+\rangle$. Tabela extraída de [55]

Na tabela 2.4.2 os estados dados são $|GHZ_4\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$, $|W_4\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$, $|\phi_4\rangle = (|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)/2$ e $|\phi^+\rangle |\phi^+\rangle = \frac{1}{2}(|00\rangle + |11\rangle) \otimes (|00\rangle + |11\rangle)$. Em alguns casos o valor de P associado a alguns splits são

[13] não confundir com bipartições

obtidos a partir da simetria permutacional do estado, o estado W_4 é um exemplo desse tipo de simetria, uma vez que ele pode ser escrito na forma

$$|W\rangle = \frac{1}{2}|00\rangle_{A'}(|01\rangle + |10\rangle)_{B'} + (|01\rangle + |10\rangle)_{A'}|00\rangle_{B'}$$

onde A' e B' correspondem às partes AB e CD respectivamente. Podemos ver que a parte A' e B' são permutáveis na superposição descrita acima.

Estados Mistos

Nos estados mistos a aplicação de P é um pouco diferente pois estão presentes as correlações clássicas e quânticas, portanto, uma minimização sobre a decomposição do estado deve ser feita. Vejamos: se $\rho = \sum \eta_i |\psi_i\rangle \langle\psi_i|$ é qualquer decomposição não necessariamente ótima do estado $\rho \in \mathcal{S}(\mathcal{H})$, então $\sum_i \eta_i P(|\psi_i\rangle \langle\psi_i|)$ é um limite superior de P .Vamos considerar o exemplo do estado de Werner

$$\rho_W(\lambda) = \lambda \left|\psi^-\right\rangle \left\langle\psi^-\right| + (1-\lambda)\frac{I}{4} \tag{2.56}$$

com $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ e $0 \leq \lambda \leq 1$. Como todo estado puro alcançado por $\rho_W(\lambda)$ tem medida de Schmidt entre 0 e 1, em qualquer decomposição $\rho_W(\lambda) = \sum_i \eta_i |\psi_i\rangle \langle\psi_i|$ temos que identificar os termos com medida de Schmidt 0 e 1. Em decorrência disso, a MS pode ser definida também por

$$P(\rho_W(\lambda)) = 1 - s \tag{2.57}$$

onde s é o peso da separabilidade do estado que pode ser maximamente extraído de $\rho_W(\lambda)$ mantendo a semipositividade do estado. Para o estado 2.56 teremos

$$P(\rho_W(\lambda)) = \begin{cases} \frac{3}{2}\lambda - \frac{1}{2} & inseparvel\ para \quad 1/3 < \lambda \leq 1 \\ 0 & separvel\ para \quad 0 \leq \lambda \leq 1/3 \end{cases} \tag{2.58}$$

Resumidamente, P é dado pelo peso da inseparabilidade. Deve-se observar ainda que a medida de Schmidt no intervalo de qualquer estado $\in \mathcal{S}(\mathcal{C}^2 \otimes \mathcal{C}^2)$ é menor ou igual a 2, válido para qualquer estado. No caso da equação definida em (2.57), o máximo do emaranhamento ocorre para $P(\rho) = 1$ onde o peso s é zero. Note que o peso s da separabilidade é obtido através do estudo da separabilidade do estado pelos autovalores, tendo em vista que o estado (2.56) estudado em [60] é separável para valores de x contidos no intervalo $0 < x < 1/3$.

2.4.3 Negatividade

Em 2002, G. Vidal e R. F. Werner introduziram um outro quantificador do emaranhamento: a negatividade [61]. Ele é baseado na norma do traço da transposição parcial ρ^{T_A} de um estado misto bipartite qualquer, sendo de operacionalidade bastante simples utilizando-se

apenas de álgebra linear básica. A negatividade pode ser considerada a versão quantitativa do Critério de Peres, medindo o grau do quanto ρ^{T_A} falha em ser positiva. A expressão geral para a negatividade faz uso da norma do traço para quantificação

$$\mathcal{N}(\rho) \equiv \frac{||\rho^{T_A}|| - 1}{2} \tag{2.59}$$

onde $||\rho^{T_A}||$ é a soma dos módulos dos autovalores de ρ^{T_A}, sendo nula $\mathcal{N}(\rho) = 0$ no caso de um estado separável. Além de poder ser expressa como o módulo da soma só dos autovalores negativos, $\mathcal{N}$ pode ainda ser apresentada na forma logaritmica

$$E_{\mathcal{N}(\rho)} \equiv \log_2 ||\rho^{T_A}|| \tag{2.60}$$

Ambas as equações (2.59) e (2.60), são monotônicas diante de operações LOCC além de quantidades aditivas. Na equação (2.59) vemos claramente que para um estado separável, a transposição parcial conserva a sua semi-positividade fazendo com que ρ^{T_A} continue a representar uma matriz densidade o que implica em $||\rho^{T_A}|| = 1 \Rightarrow \mathcal{N}(\rho) = 0$.

Como exemplo, vamos usar novamente o estado de Werner (2.56), o qual possui apenas um possível autovalor negativo $\frac{1-3x}{4}$. $\mathcal{N}$ será

$$\mathcal{N} = \frac{1 - 3x}{4} \tag{2.61}$$

onde a quantidade de emaranhamento (em valor absoluto) irá variar de acordo com x. Na apresentação do critério de Peres, vimos que este estado será emaranhado no intervalo $1/3 < x < 1$. No gráfico abaixo, plotamos a quantidade de emaranhamento neste estado em função da variável x. Por definição, $\mathcal{N} = 0$ para estados separáveis. Note que a partir de $x = 1/3 \approx 0,33$ seu emaranhamento aumenta além de que o intervalo de separabilidade do estado é bem pequeno comparado com o de emaranhamento.

Negatividade em estados multipartites

Até agora,por simplicidade, introduzimos o uso da negatividade em casos bipartites, no entanto, utilizando o conceito de bipartições [61], podemos estender o uso de $\mathcal{N}$ para estados multipartites, classificando as propriedades do emaranhamento ao olhar para os diferentes splits do sistema, como feito na medida de Schmidt. No caso de um estado tripartite, podemos estudar o caso $A|BC$ e calcular a soma dos seus autovalores negativos. Isto é automaticamente um emaranhamento monotônico, tendo em vista que $\mathcal{N}_{A|BC}$ é uma função monotônica do estado bipartite $A|BC$ diante de LOCC.

As propriedades do emaranhamento de uma matriz reduzida também são consideradas. Em um estado emaranhado tripartite, realizando um traço em qualquer uma das partes, a matriz densidade reduzida pode ainda obter vestígios do emaranhamento original e a negatividade pode ser usada para quantificá-lo.

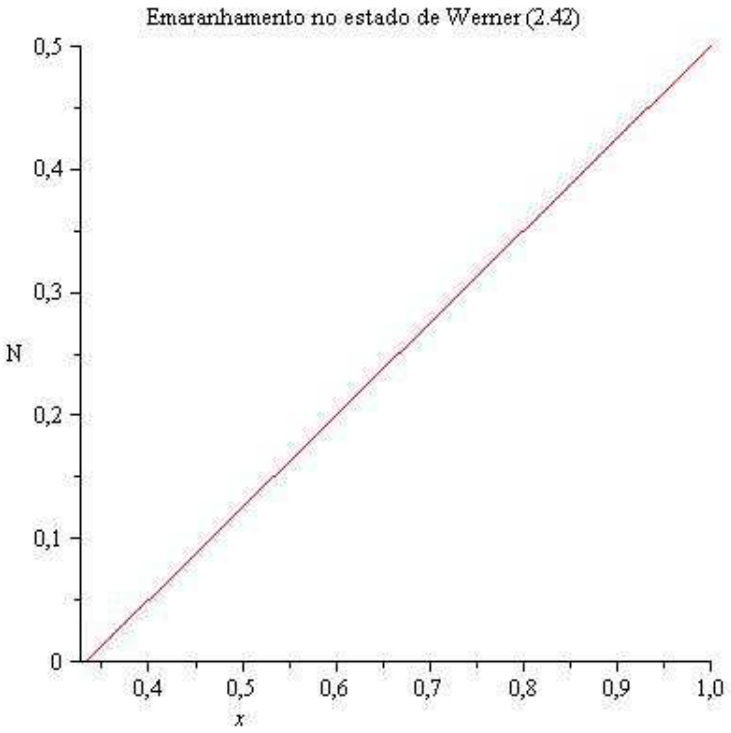

Figura 2.4 Quantificação do emaranhamento do estado de Werner bipartite através da negatividade. $\mathcal{N}$ varia em função x que pode assumir qualquer valor no intervalo $0 \leq x \leq 1$. Note que o máximo da negatividade $N = 0.5$ ocorre quando $x = 1$. Por definição, $\mathcal{N} = 0$ para estados separáveis.

CAPÍTULO 3

Dinâmica do emaranhamento

Neste capítulo, iremos mostrar a evolução do emaranhamento de estados GHZ e W com respeito à amplitude, fase e polarização. Este estudo é baseado no trabalho desenvolvido por L.Aolita [2], no entanto a quantificação do emaranhamento após a passagem dos estados pelos canais será avaliada via outro quantificador que não a negatividade.

No mundo real, não existem sistemas perfeitamente fechados, com excessão do universo como um todo. Os sistemas reais sofrem interações indesejadas com o meio externo aparecendo como ruído nos sistemas de processamento de informação quântica. Para que sistemas úteis possam ser construídos, torna-se necessária a compreensão e o controle do processo de ruído.

Como exemplo de sistema físico [4], temos um pêndulo o qual interage fracamente com o meio externo, principalmente por meio do atrito. No entanto, para que sua dinâmica seja completamente descrita e explicarmos porque depois de um certo tempo ele pára de oscilar, devemos levar em conta os efeitos de atenuação devido ao ar e as imperfeições de seu mecanismo de suspensão. De forma semelhante, um sistema quântico não pode ser perfeitamente fechado, principalmente quando se trata de computadores quânticos que precisam ser programados cuidadosamente por um sistema externo para realizar as operações desejadas.

Devemos inicialmente introduzir uma breve noção de operador-soma, formalismo necessário nas operações quânticas para descrição de sistemas abertos.

3.1 Representação de operador-soma

Operações quânticas podem ser representadas de uma forma elegante através da representação de operador-soma. Seja $|e_k\rangle$ uma base ortonormal do espaço de estados do ambiente com número de dimensão finita, e $\rho_{amb} = |e_0\rangle \langle e_0|$ seu estado inicial. O mapeamento $\mathcal{E}$, que representa a operação quântica de evolução do estado, pode ser descrito como

$$\begin{aligned}\mathcal{E}(\rho) &= \sum_k \langle e_k| U[\rho \otimes |e_0\rangle \langle e_0|]U^\dagger |e_k\rangle \\ &= \sum_k E_k \rho E_k^\dagger\end{aligned} \tag{3.1}$$

em que $E_k \equiv \langle e_k| U |e_0\rangle$ é um operador sobre o espaço de estados do sistema principal. A equação é conhecida como a representação de operador soma do mapeamento $\mathcal{E}$. Os operadores $\{E_k\}$ são chamados de elementos de operação da operação quântica $\mathcal{E}$ e satisfazem a relação de completitude $\sum_k E_k^\dagger E_k = I$.

Além de uma descrição geral da dinâmica de sistemas quânticos, a representação do operador-soma nos dá uma liberdade com respeito ao uso desses operadores para representar algum tipo de operação, de forma que os elementos que aparecem na representação de operador-soma não são únicos.

Teorema 3.1. ***Liberdade unitária na representação de operador-soma****. Sejam $\{E_1, ..., E_m\}$ e $\{F_1, ..., F_m\}$ elementos de operação que originam as operações quânticas $\mathcal{E}$ e $\mathcal{F}$, respectivamente.Adicionando operadores nulos na lista dos elemntos de operação menor, pode-se assegurar que $m = n$. Portanto, $\mathcal{E} = \mathcal{F}$ se e somente se existirem números complexos u_{ij} tais que $E_i = \sum_j u_{ij} F_{ij}$, e u_{ij} sejam os elementos de uma matriz unitária m por m.*

Tomemos como exemplo os elementos de operação [62]

$$E_0 = \sqrt{1-p} I;\ E_1 = \sqrt{p}\frac{1}{2}(I + \sigma_z);\ e\ E_3 = \sqrt{p}\frac{1}{2}(I - \sigma_z) \tag{3.2}$$

como veremos mais adiante, estes elementos representam a operação do canal de atenuação de fase. A aplicação de (3.2) a um estado qualquer ρ, faz a equação (3.1) tomar a forma

$$\begin{aligned}\mathcal{E}(\rho) &= (1-p)I\rho I + \frac{p}{4}(1+\sigma_z)\rho(1+\sigma_z) + \frac{p}{4}(1-\sigma_z)\rho(1-\sigma_z) \\ &\quad (1-p)\rho + \frac{p}{4}(2\rho + 2\sigma_z\rho\sigma_z) \\ &\quad (1-p)\rho + \frac{p}{2}[\rho + (|0\rangle\langle 0| - |1\rangle\langle 1|)\rho(|0\rangle\langle 0| - |1\rangle\langle 1|)] \\ &\quad (1-p)\rho + \frac{p}{2}[P_0\rho P_0 + P_1\rho P_1 - P_0\rho P_1 - P_1\rho P_0] \\ &\quad (1-p)I\rho I + \frac{p}{2}[P_0\rho P_0 + P_1\rho P_1 - P_0\rho P_1 - P_1\rho P_0] \\ &\quad (1-p)(|0\rangle\langle 0| - |1\rangle\langle 1|)\rho(|0\rangle\langle 0| - |1\rangle\langle 1|) + \frac{p}{2}[P_0\rho P_0 + P_1\rho P_1 - P_0\rho P_1 - P_1\rho P_0] \\ &\quad (1-p)\rho + p(P_0\rho P_0 + P_1\rho P_1)\end{aligned} \tag{3.3}$$

onde $P_0 = |0\rangle\langle 0|$ e $P_1 = |1\rangle|1\rangle$. A equação (3.2) e (3.3) são equivalentes.

Esta representação é importante porque nos fornece uma forma intrínseca de caracterizarmos a dinâmica do sistema principal, nos permitindo descrevê-la sem a necessidade de considerarmos explicitamente as propriedades do ambiente de maneira que tudo o que é preciso está nos operadores E_k que atuam somente no sistema principal simplificando bastante os cálculos e levando a um entendimento teórico maior.

Descreveremos a seguir alguns exemplos concretos de ruído quântico e operações quânticas, o que é, ou qual a importância de cada um dessas canais escolhidos. São eles: a despolarização, a atenuação da amplitude generalizada e a defasagem.

3.2 Canais Quânticos

Despolarização - D

O canal de despolarização representa um ruído quântico no qual o estado inicial possui uma probabilidade p de ser despolarizado ou se tornar completamente misturado e uma probabilidade $(1-p)$ de permanecer polarizado, sendo o estado final representado por

$$\mathcal{E}_i\rho_{0_i}^D = (1-p)\rho_0 + p\frac{I}{2} \tag{3.4}$$

No formalismo de Kraus, este canal possui duas parametrizações (Teo 3.1) as quais são expressas através das matrizes de Pauli. Aqui iremos apresentar apenas a parametrização que foi utilizada na obtenção dos resultados

$$\mathcal{E}_i^D\rho_{0_i} = (1-\frac{3p}{4})\rho_{0_i} + \frac{p}{4}(X\rho_{0_i}X + Y\rho_{0_i}Y + Z\rho_{0_i}Z) \tag{3.5}$$

É interessante ver o que ocorre com cada qbit diante da operação de cada canal e isto pode ser entendido da melhor forma se tomarmos uma visão geométrica de um único qbit (esfera de Bloch) [4] antes e depois da operação quântica. O canal de despolarização faz com que o módulo do vetor de Bloch diminua, o que implica na diminuição do raio da esfera causando sua contração uniforme, levando um estado inicialmente puro (superfície da esfera de Bloch) a um estado misturado (interior da esfera de Bloch), como pode ser visto na figura 3.2.

Atenuação de fase - PD [1]

Este canal descreve um processo inteiramente quântico no qual a perda de informação acontece sem a perda de energia. Durante a evolução, o valor esperado dos elementos de fora da diagonal da matriz densidade decaem a zero com o tempo implicando na perda de coerência do estado. Um exemplo explícito seria o espalhamento aleatório de um fóton à medida que este viaja numa guia de onda, ou a perturbação dos estados eletrônicos de um átomo através da interação com cargas elétricas distantes [4]. Sua atuação no estado é dada, na representação de operador soma [62]

[1] Phase Damping

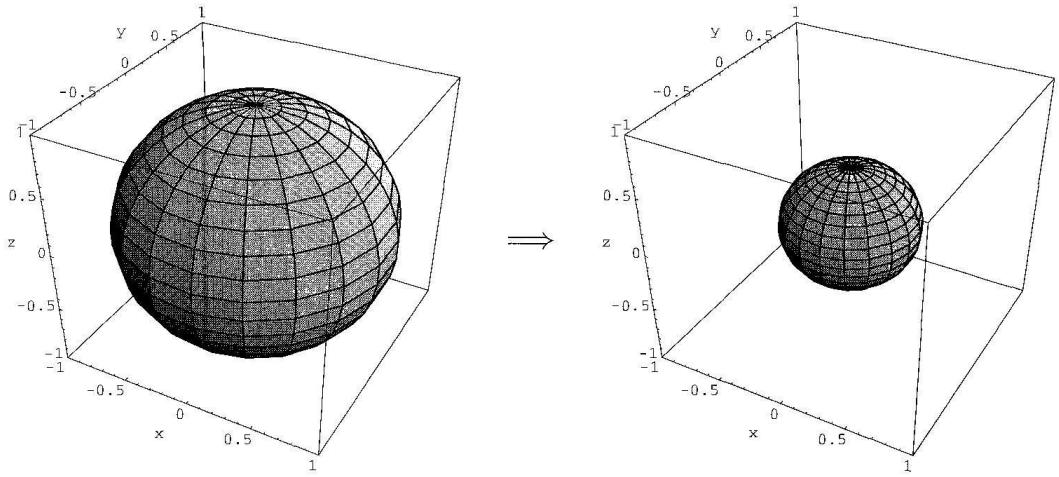

Figura 3.1 Esfera de Bloch representando um único qbit após a atuação do canal de despolarização. O módulo do vetor de Bloch (raio) diminui causando uma contração uniforme da esfera, conforme [4]

$$\mathcal{E}_i^{PD}\rho_{0_i} = E_0\rho_{0_i}E_0^\dagger + E_1\rho_{0_i}E_1^\dagger + E_2\rho_{0_i}E_2^\dagger \tag{3.6}$$

onde $E_0 = \sqrt{1-p}I$, $E_1 = \sqrt{p}\frac{1}{2}(I+\sigma_z)$ e $E_2 = \sqrt{p}\frac{1}{2}(I-\sigma_z)$. A equação (**??**) pode também ser reescrita na forma

$$\mathcal{E}_i^{PD}\rho_{0_i} = (1-p)\rho_{0_i} + p(|0\rangle\langle 0|\rho_{0_i}|0\rangle\langle 0| + |1\rangle\langle 1|\rho_{0_i}|1\rangle\langle 1|) \tag{3.7}$$

onde a perda de coerência ocorre com probabilidade p.

Na representação da esfera de Bloch, os estados sobre o eixo $\hat{z}$ permanecem inalterados, enquanto que aqueles contidos no plano $\hat{x}\hat{y}$ são contraídos uniformemente como pode ser visto no gráfico 3.2.

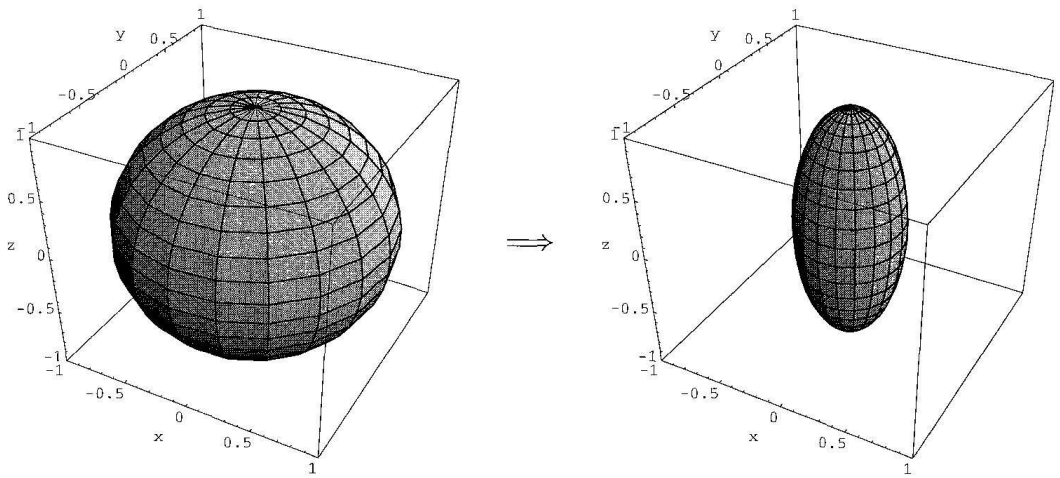

Figura 3.2 Esfera de Bloch representando um único qbit após a atuação do canal de atenuação de fase. Os estados sobre o eixo $\hat{z}$ permanecem inalterados, enquanto que aqueles contidos no plano $\hat{x}\hat{y}$ são contraídos uniformemente.

Atenuação da amplitude generalizada - GAD [2]

Operações quânticas nas quais há perda de energia em sistemas quânticos podem ser descritas pelo canal GAD. Como exemplo de tais sitemas temos um átomo emitindo um fóton espontaneamente ou um fóton em um interferômetro (cavidade) quando sujeito a espalhamento e atenuação. O canal GAD se constitui uma generalização para temperaturas finitas no caso puramente dissipativo - canal de atenuação de amplitude. A atenuação de amplitude generalizada decreve o processo de relaxação "T_1"devido ao acoplamento de spins à rede em torno, um sistema muito maior que se encontra a uma temperatura bem mais elevada do que a temperatura de spins, caso relevante para a computação quântica por NMR.

Segundo a representação de Kraus teremos

$$\mathcal{E}_i^{GAD}\rho_{0_i} = E_0\rho_{0_i}E_0^\dagger + E_1\rho_{0_i}E_1^\dagger + E_2\rho_{0_i}E_2^\dagger + E_3\rho_{0_i}E_3^\dagger \tag{3.8}$$

Num banho térmico à temperatura arbitrária, os operadores-soma possuem a forma

$$E_0 \equiv \sqrt{\frac{\overline{n}+1}{2\overline{n}+1}}(|0\rangle\langle 0| + \sqrt{1-p}\,|1\rangle\langle 1|) \tag{3.9}$$

$$E_1 \equiv \sqrt{\frac{\overline{n}+1}{2\overline{n}+1}}p\,|0\rangle\langle 1| \tag{3.10}$$

$$E_2 \equiv \sqrt{\frac{\overline{n}}{2\overline{n}+1}}(\sqrt{1-p}\,|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{3.11}$$

$$E_3 \equiv \sqrt{\frac{\overline{n}}{2\overline{n}+1}}p\,|1\rangle\langle 0| \tag{3.12}$$

Aqui, $\overline{n}$ é o número médio de excitações no banho, $p \equiv p(t) \equiv 1 - e^{-(1/2)\gamma(2(\overline{n})+1)t}$ é a probabilidade do qbit trocar um quantum com o banho no tempo t, e γ é a taxa de dissipação à temperatura zero.

De forma geral, o canal de atenuação da amplitude pode ser visualizada como um fluxo sobre a esfera de Bloch que leva todos os pontos sobre a esfera em direção ao ponto fixo no polo norte que representa o estado $|0\rangle$ [4] como pode ser visualizado na figura 3.3.

É importante ressaltar que a probabilidade p é uma parametrização do tempo, onde $p = 0$ para $t = 0$, estado inicial completamente emaranhado e $p = 1$ refere-se ao caso em que $t \to \infty$, que é o limite assintótico.

3.3 Dinâmica do emaranhamento

Para cada canal, teremos um operador de evoluçaõ $\mathcal{E}_i$ o qual deverá ser aplicado em cada i-ésimo qbit correspondente, de forma que o estado final será dado pela simples operação

[2] Generalized Amplitude Damping

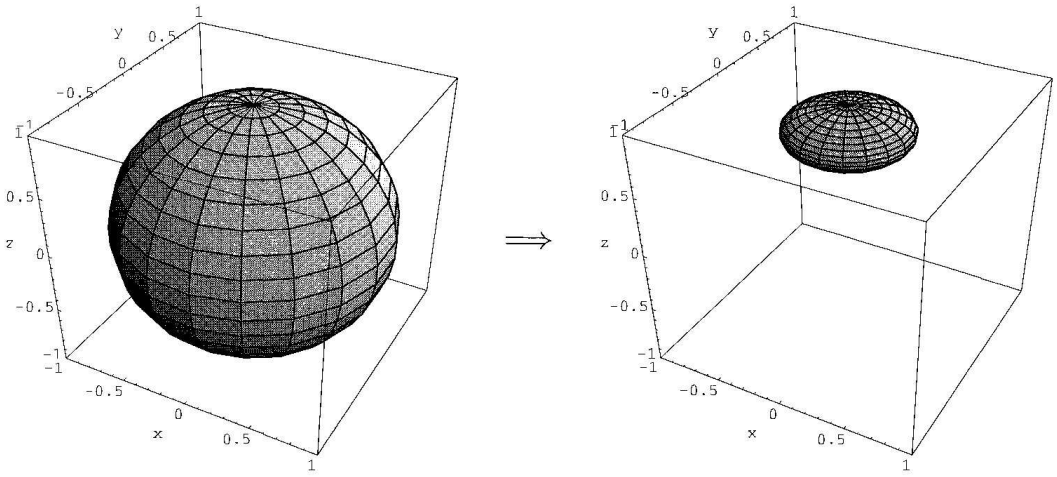

Figura 3.3 Representação de um qbit na esfera de Bloch após a atuação do canal de atenuação de amplitude. Note que após passagem pelo canal, ocorre um fluxo de todos os pontos da esfera em direção à seu pólo norte.

$$\rho = \mathcal{E}_i \ldots \mathcal{E}_1 \mathcal{E}_0 \rho_0 \tag{3.13}$$

Nesta seção mostraremos a dinâmica do GHZ nestes modelos de decoerência. Por simplicidade, inicialmente utilizaremos apenas dois qbits como exemplo [3], no entanto a dinâmica para $N = 2$ pode ser estendida para N qualquer. Após a passagem pelo canal, aplicaremos o PPT à matriz resultante (no caso $N > 2$ teremos bipartições) e extrairemos seus autovalores para uma breve análise, em seguida iremos quantificar o emaranhamento através da medida de Schmidt, pue para o nosso caso é dada pelo peso da separabilidade [55], mesma definição utilizada na quantificação do estado de Werner.

Consideremos o estado inicial dado por

$$|\phi\rangle = \alpha\,|00\rangle + \beta\,|11\rangle \tag{3.14}$$

cuja matriz densidade é

$$\rho = |\alpha|^2\,|00\rangle\langle 00| + \alpha\beta^*\,|00\rangle\langle 11| + \alpha^*\beta\,|11\rangle\langle 00| + |\beta|^2\,|11\rangle\langle 11| \tag{3.15}$$

3.3.1 Canal de depolarização

Para o canal de depolarização, a equação 3.13 terá a forma

[3] no caso de dois qbits teremos os estados de Bell

$$\begin{aligned}\mathcal{E}_i\rho_{0_i} &= (1-\frac{3p}{4})\rho_{0_i}+\frac{p}{4}(X\rho_{0_i}X+Y\rho_{0_i}Y+Z\rho_{0_i}Z) \\ &= (1-\frac{3p}{4})\rho_{0_i}+\frac{p}{4}\big[\big(|0\rangle\langle 1|+|1\rangle\langle 0|\big)\rho_{0_i}\big(|0\rangle\langle 1|-|1\rangle\langle 0|\big)+ \\ &\quad \big(|0\rangle\langle 1|-i\,|1\rangle\langle 0|\big)\rho_{0_i}\big(|0\rangle\langle 1|-i\,|1\rangle\langle 0|\big)+\big(|0\rangle\langle 0|-|1\rangle\langle 1|\big)\rho_{0_i}\big(|0\rangle\langle 0|-|1\rangle\langle 1|\big)\big]\end{aligned} \tag{3.16}$$

Conhecendo a aplicação das matrizes de Pauli em cada bit quântico ($X|0\rangle=|1\rangle, X|1\rangle=|0\rangle;\ Y|0\rangle=i|0\rangle, Y|1\rangle=-i|1\rangle;\ Z|0\rangle=|0\rangle, Z|1\rangle=-|1\rangle$), esta operação pode ser facilmente calculada. O resultado da atuação do canal no primeiro qbit é

$$\begin{aligned}\rho &= (1-\frac{p}{2})|\alpha|^2|00\rangle\langle 00|+(1-\frac{p}{2})|\beta|^2|11\rangle\langle 11|+ \\ &\quad (1-p)\alpha\beta^*|00\rangle\langle 11|+(1-p)\alpha^*\beta|11\rangle\langle 00|+\frac{p}{2}\big[|\beta|^2|01\rangle\langle 01|+ \\ &\quad |\alpha|^2|10\rangle\langle 10|\big]\end{aligned} \tag{3.17}$$

tomando (3.17) e aplicando (3.5) ao segundo qbit, encontra-se

$$\begin{aligned}\rho &= (1-\frac{p}{2})^2|\alpha|^2+(\frac{p}{2})^2|\beta|^2|00\rangle\langle 00|+(\frac{p}{2})^2|\alpha|^2+(1-\frac{p}{2})^2|\beta|^2|11\rangle\langle 11|+ \\ &\quad \alpha\beta^*(1-p)^2|00\rangle\langle 11|+\alpha\beta^*(1-p)^2|11\rangle\langle 00|+\frac{p}{2}(1-\frac{p}{2})|\alpha|^2+\frac{p}{2}(1-\frac{p}{2})|\beta|^2|01\rangle\langle 01|+ \\ &\quad \frac{p}{2}(1-\frac{p}{2})|\alpha|^2+\frac{p}{2}(1-\frac{p}{2})|\beta|^2|10\rangle\langle 10|\end{aligned} \tag{3.18}$$

(3.19)

os termos de coerência são multiplicados por $(1-p)^2$ e os termos da diagonal podem ser escritos como $\lambda_k=|\alpha|^2(1-\frac{p}{2})^{2-k}(\frac{p}{2})^k+|\beta|^2(1-\frac{p}{2})^{2-k}(\frac{p}{2})^k$, com $k=0,1,2$. A forma matricial de 3.18 em termos dos coeficientes λ é

$$\begin{bmatrix}\lambda_0 & 0 & 0 & c\\ 0 & \lambda_1 & 0 & 0\\ 0 & 0 & \lambda_1 & 0\\ c^* & 0 & 0 & \lambda_2\end{bmatrix} \tag{3.20}$$

com $c=\alpha\beta^*(1-p)^2$.

Tomando N qbits e aplicando (3.16), veremos que todos os termos da diagonal podem ser escritos na forma geral $\lambda_k=|\alpha|^2(1-\frac{p}{2})^{N-k}(\frac{p}{2})^k+|\beta|^2(1-\frac{p}{2})^{N-k}(\frac{p}{2})^k$. A passagem do estado pelo canal levará a matriz antes composta apenas por dois elementos na diagonal e dois

na antidiagonal a uma matriz ainda com dois elementos na antidiagonal e diagonal completamente preenchida. Tendo em mãos a forma geral dos λ_k e da matriz densidade do estado após a passagem pelo canal, podemos escrever a matriz do estado evoluído para qualquer N, por exemplo, $N = 3$:

$$\begin{bmatrix} \lambda_0 & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 & 0 \\ c^* & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 \end{bmatrix} \tag{3.21}$$

onde há repetição de alguns termos na diagonal da matriz ocorrendo $\begin{pmatrix} N \\ k \end{pmatrix}$ vezes para cada um deles. Um estado GHZ com N qbits evoluído será descrito pela matriz

$$\begin{bmatrix} \lambda_0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & c \\ \vdots & \lambda_1 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \lambda_k & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \lambda_{N-k} & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \lambda_{N-1} & 0 \\ c^* & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0\lambda_N \end{bmatrix} \tag{3.22}$$

com $c = \alpha\beta(1-p)^N$

Esta forma geral é válida tanto para o canal de depolarização, quanto para os canais de atenuação de fase e o de atenuação de amplitude generalizada. Nosso objetivo é estudar o emaranhamento após a dinâmica do estado, e para tanto devemos fazer uso da matriz 3.22 para

quantifica-lo através da medida de Schmidt. Não é viável usar a definição 2.54 para quantificação, pois trata-se de um estado misto, usaremos aqui a equação 2.57 $P = 1 - s$ onde s é o peso da separabilidade que por sua vez é estimado fazendo uso do PPT.

Consideremos a matriz densidade 3.21 referente ao estado final da dinâmica do GHZ com $N = 3$, cujos autovalores são $\lambda_1, \lambda_2, \frac{1}{2}(\lambda_0 + \lambda_3 + \sqrt{\Delta}), \frac{1}{2}(\lambda_0 + \lambda_3 - \sqrt{\Delta})$ com $\Delta = (\lambda_0 - \lambda_3)^2 + 4|c|^2$. Consideremos também duas possíveis bipartições: $A|BC$ com $k = 1$ e $AB|C$ com $k = 2$. Para o caso da bipartição $A|BC$ a matriz parcialmente transposta é dada por

$$\rho^{T_{BC}} \begin{bmatrix} \lambda_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_1 & c & 0 & 0 & 0 \\ 0 & 0 & 0 & c^* & \lambda_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3 \end{bmatrix} \tag{3.23}$$

cujos autovalores são $\lambda_0, \lambda_1, \lambda_2, \lambda_3, \frac{1}{2}(\lambda_1 + \lambda_2 + \sqrt{\Delta}), \frac{1}{2}(\lambda_1 + \lambda_2 - \sqrt{\Delta})$. Como a matriz densidade é um operador positivo, todos os λ_i são positivos, isto quer dizer que na nossa análise da positividade da matriz parcialmente transposta numa bipartição qualquer, apenas os autovalores envolvendo o termo Δ nos interessa, os quais seriam os mesmos obtidos numa matriz de dimensão 2×2, formada pelos elementos de coerência e aqueles que estiverem contidos em sua linha:

$$\begin{bmatrix} \lambda_k & c \\ c^* & \lambda_{N-k} \end{bmatrix} \tag{3.24}$$

onde no nosso exemplo $\lambda_k = \lambda_1$ e $\lambda_{N-k} = \lambda_2$.

Esta observação feita para um GHZ composto por 3 qbits é válida para N qualquer. A decomposição da matriz densidade (3.22) em uma soma de uma matriz diagonal positiva com uma matriz de posto 4 feita em [2] é justificada a partir deste raciocínio: ao aplicarmos o PPT biparticionado em 3.22 os elementos de coerência são transpostos para outra linha contendo um certo λ_i. A matriz de posto 4 será formada justamente pelos elementos das linhas em que os elementos de coerência aparecem após a transposição parcial, e pelos elementos λ_0, λ_N, sendo usada como recurso para que o critério de Peres consiga identificar o emaranhamento, já que ela representa um operador densidade de dois qbits e nesta dimensão não existem os chamados *bound entanglement* [63].

No nosso estudo usamos diretamente a matriz 3.24. Para N qualquer, os autovalores a serem analizados serão dados por

$$\frac{1}{2}(\lambda_k + \lambda_{N-k} + \sqrt{\Delta}),\ \frac{1}{2}(\lambda_k + \lambda_{N-k} - \sqrt{\Delta}) \tag{3.25}$$

onde Δ possui a forma

$$\Delta = (\lambda_k - \lambda_{N-k})^2 + 4|c|^2 \tag{3.26}$$

Da equação (3.25) vemos claramente que a matriz positiva semidefinida (3.22) será uma matriz densidade quando $\Delta \leq (\lambda_k + \lambda_{N-k})^2$ e consequentemente, a condição para que tenhamos um estado emaranhado é que os valores de Δ sejam maiores que este. Da definição 2.57, podemos escrever a medida de Schmidt na forma

$$P(\lambda(p)) = \Delta - \eta \tag{3.27}$$

onde Δ são todos os valores que os autovalores de ρ podem assumir para que a matriz seja separável ou emaranhada e $\eta = (\lambda_k + \lambda_{N-k})^2$ é o valor máximo que os autovalores de ρ devem assumir para que tenhamos uma matriz densidade. Ao calcularmos $\Delta - \eta$, estamos tomando todos os possíveis valores para os quais ρ seja separável ou inseparável e subtraindo apenas aqueles os quais a torna separável, desta forma podemos obter um comportamento isolado do emaranhamento com a variação do parâmetro em questão, p. (3.27) pode ser escrita explicitamente neste caso como

$$\begin{aligned} P(\lambda(p)) &= (\lambda_k - \lambda_{N-k})^2 + 4|c|^2 - (\lambda_k + \lambda_{N-k})^2 \\ &= 4\{|\alpha\beta|^2(1-p)^{2N} - [1-(1-p)^2]^N\} \end{aligned} \tag{3.28}$$

Deve-se ressaltar que os valores de Δ e η não serão sempre os mesmos, podendo tomar uma forma diferente para cada tipo de estado[4].

A equação 3.27 depende da quantidade p a qual é uma parametrização do tempo, onde $p = 0$ corresponde ao estado incial em $t = 0$ e $p = 1$ quando $t \to \infty$. A probabilidade do estado ser separável associada às bipartições mais balanceadas, no caso de N par $(k = N/2)$ é obtida tomando $P(\lambda(p)) = 0$, o que nos dá

$$p = 1 - \frac{1}{\sqrt{1 + 4|\alpha\beta|^{2/N}}} \tag{3.29}$$

Na figura 3.3.1 estima-se a quantidade do emaranhamento em termos da probabilidade p e observa-se o comportamento para cada caso em que $N = 4, 40, 400$. Nota-se que quanto maior o número de qbits, mais rápido o estado se tornará separável. Este resultado é esperado devido ao maior número de partículas gerarem uma maior interação mútua.

[4]isso é justificado devido ao fato de que a construção de Δ e η é feita através de uma análise dos autovalores da matriz parcialmente transposta a ser estudada

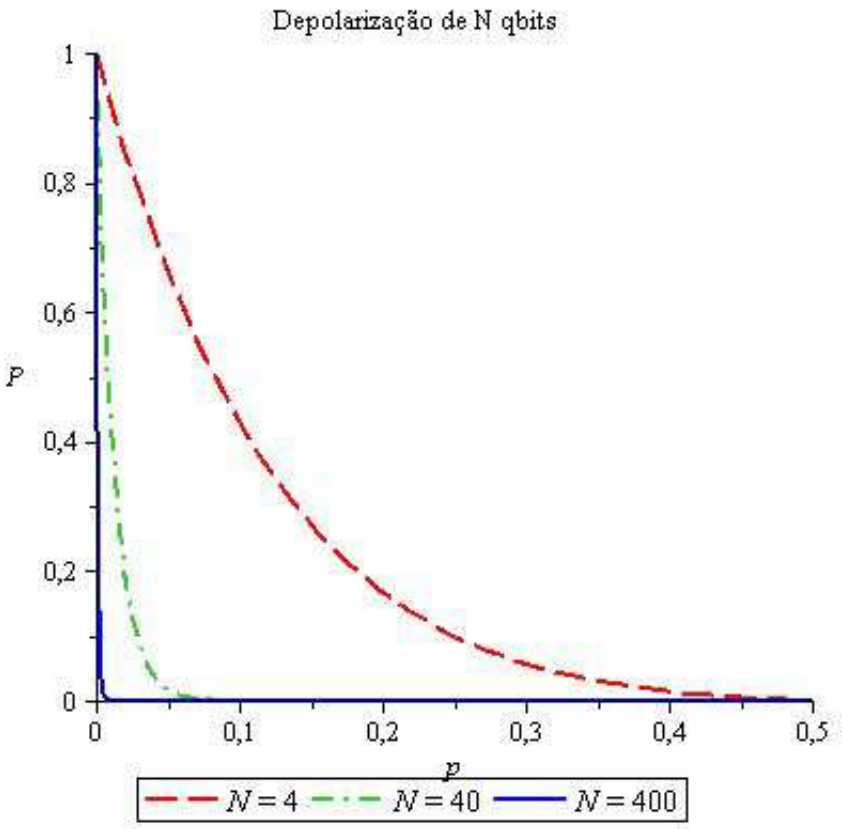

Figura 3.4 Gráfico de $P(\rho(\lambda)$ versus p mostrando a evolução do estado GHZ com $N = 4, N = 40, N = 400$ qbits, após a passagem pelo canal de despolarização.

Em contrapartida, para uma dada bipartição, a equação (3.29) nos mostra que quanto maior o número N de qbits, maior será o tempo para que o estado se torne separável, isto pode ser visto substituindo os valores de N em (3.29), de maneira que $p(N = 4) \approx 0,540$, $p(N = 40) \approx 0,546$ e $p(N = 400) \approx 0,552$, no caso $N \to \infty$ teremos $p \approx 0,553 \approx 0,55$. No entanto, vemos no gráfico 3.3.1 que quanto maior o número de qbits maior será o tempo para que ocorra a morte súbita do emaranhamento [64, 65]. Ao mesmo tempo em que há uma queda brusca no emaranhamento diretamente proporcional a N verificada no gráfico , há também uma certa resistência à separabilidade cuja dependência em N é inversamente proporcional. No entanto, como descrito em [2], o que importa na prática não é que o emaranhamento não desaparaça, e sim que uma parcela significativa do emaranhamento inicial perdure, o que não é observado neste caso.

3.3.2 Canal de atenuação de amplitude generalizada

A aplicação de 3.8 ao estado descrito pela matriz densidade 3.15 o levará ao estado

$$\rho^{GAD} = \lambda_0 |00\rangle \langle 00| + \lambda_1 |01\rangle \langle 01| + \lambda_1 |10\rangle \langle 10| + \lambda_2 |11\rangle \langle 11| + \alpha\beta^*(1-p) |00\rangle \langle 11| + \alpha^*\beta(1-p) |11\rangle \langle 00| \tag{3.30}$$

onde vemos novamente que a matriz evoluída possui a diagonal completamente preechida com os termos multiplicados pelos coeficientes λ_k. Para N qualquer estes coeficientes terão a forma

$$\lambda_k = |\alpha|^2 x^{N-k} y^k + |\beta|^2 w^{N-k} z^k \tag{3.31}$$

com $0 \leq x \equiv \frac{-p\overline{n}}{2\overline{n}+1} + 1, y \equiv \frac{p\overline{n}}{2\overline{n}+1}, w \equiv \frac{p(\overline{n}+1}{)} 2\overline{n} + 1, z \equiv \frac{-p(\overline{n}+1)}{2\overline{n}+1} + 1 \leq 1$. Já os termos de coerência passam a ser multiplicados pelo fator $c = \alpha\beta(1-p)^{N/2}$

Após a evolução de ρ_0, podemos tomar a matriz densidade evoluída e realizar os mesmos procedimentos utilizados no canal de depolarização, desta forma, após a transposição parcial do estado biparticionado os autovalores para qualquer bipartição serão dados por [5]

$$\frac{1}{2}(\lambda_k + \lambda_{N-k}) + \sqrt{\Delta},\ \frac{1}{2}(\lambda_k + \lambda_{N-k}) - \sqrt{\Delta} \tag{3.32}$$

Novamente, a positividade da matriz resume-se aos possíveis valores que $\Delta = (\lambda_k - \lambda_{N-k})^2 + 4|c|^2$ pode assumir. Assim como no caso anterior ela torna-se negativa quando $\Delta > (\lambda_k + \lambda_{N-k})^2$, isso faz com que a medida de Schmidt para o canal GAD possua praticamente a mesma forma da do canal de defasagem 3.27, onde $\eta = (\lambda_k + \lambda_{N-k})^2$.

Podemos tomar o caso particular em que $\overline{n} = 0$, no limite em que a temperatura tende a zero

$$\begin{aligned} P(\lambda(p)) &= \Delta - \eta & (3.33)\\ &= (\lambda_k - \lambda_{N-k})^2 + 4|c|^2 - (\lambda_k + \lambda_{N-k})^2 & (3.34)\\ &= 4\big[(1-p)^N(|\alpha\beta|^2 - |\beta|^4 p^N) & (3.35) \end{aligned}$$

Tomando ainda $\alpha = \beta = \frac{1}{\sqrt{2}}$, temos

$$P(\lambda(p)) = (1-p)^N(1-p^N) \tag{3.36}$$

Como podemos ver na figura 3.5, a evolução do estado nos dois canais possui comportamento parecido. Este fato é justificável devido à semelhança da matriz densidade do estado após a passagem por cada canal[6]

A probabilidade crítica de desaparecimento do emaranhamento $P(\lambda(p)) = 0$ é dada por

$$p_c^{AD} = min\{1, |\frac{\alpha}{\beta}|^{2/N}\} \tag{3.37}$$

Mesmo resultado obtido em [2].

[5] apenas os que nos interessam para o estudo da positividade da matriz

[6] Nos dois casos a matriz passa a ter todos os elementos da diagonal não nulos e multiplicados pelos coeficientes λ_k além dos dois únicos elementos de coerência serem multiplicados por $(1-p)$ elevado a uma potência de N.

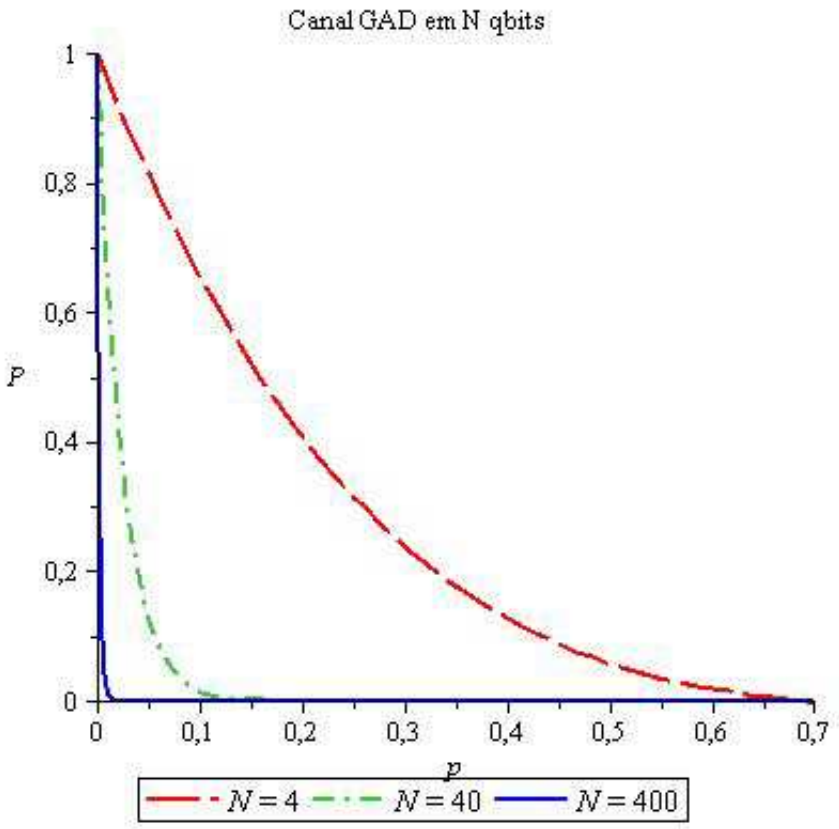

Figura 3.5 Gráfico de $P(\rho(\lambda)$ versus p mostrando a evolução do estado GHZ com $N = 4, N = 40, N = 400$ qbits, após a passagem pelo canal GAD.

3.3.3 Canal de atenuação de fase

Aplicando a definição 3.7 em 3.15, teremos o estado final dado por

$$\rho^{PD} = |\alpha|^2 |00\rangle \langle 00| + |\beta|^2 |11\rangle \langle 11| + \alpha\beta^*(1-p)^2 |00\rangle \langle 11| + \alpha^*\beta(1-p)^2 |11\rangle \langle 00| \quad (3.38)$$

Neste caso vemos que os termos da diagonal não sofrem qualquer alteração, o que nos mostra que os coeficientes $\lambda_k = 0$ para qualquer elemento diagonal da matriz, com exceção do primeiro e último elementos onde $\lambda_0, \lambda_N \neq 0$. Os autovalores da matriz parcialmente transposta para qualquer bipartição serão $|\alpha|^2, |\beta|^2, -|\alpha\beta|(1-p)^N, |\alpha\beta|(1-p)^N$. Neste caso, a matriz será separável apenas para valores de $p = 1$, que é exatamente o caso assintótico, portanto a quantificação do emaranhamento será dada pelo próprio autovalor dependente de p.

$$P(p) = |\alpha\beta|(1-p)^N \quad (3.39)$$

Não podemos, como feito nos outros canais, estimar o comportamento do emaranhamento com o tempo (calcular a probabilidade crítica) utilizando diretamente a equação 3.27 com $\eta = 1$ (valor ótimo para o estado ser separável) pois assim estaríamos dizendo que

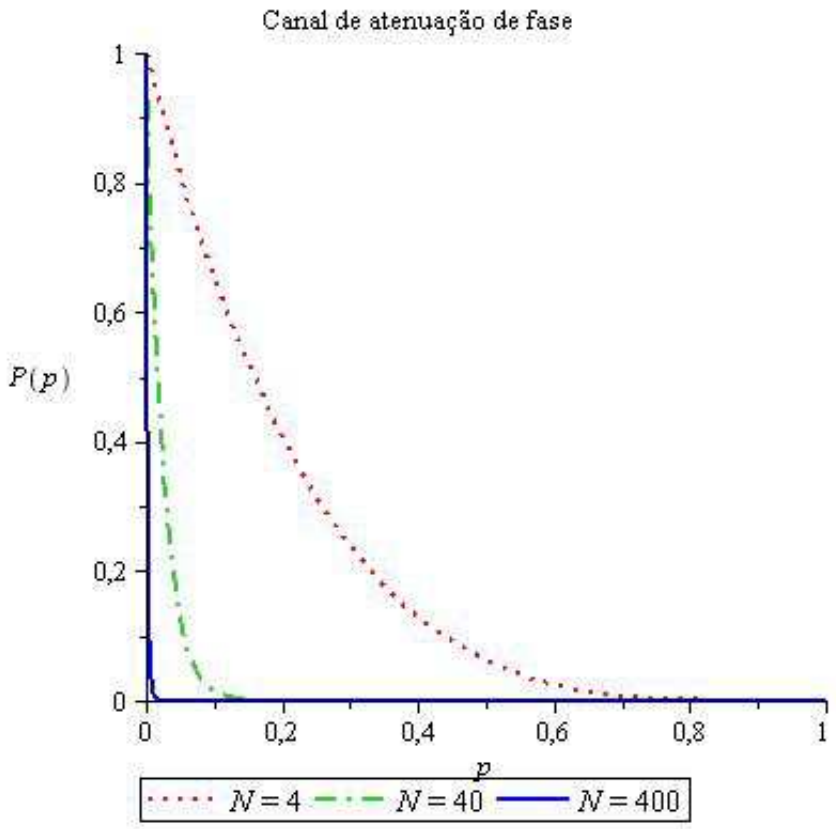

Figura 3.6 Gráfico de $P(\rho(\lambda)$ versus p mostrando a evolução no estado GHZ para $N = 4, 40, 400$ qbits após a passagem pelo canal de defasagem.

$\Delta = |\alpha\beta|(1-p)^N > 1$, o que não é verdade já que p, α e β só assumem valores entre 0 e 1. Nota-se que não há uma probabilidade crítica para o decaimento do emaranhamento pois quando $P(p) = 0 \rightarrow p = 1$.

Como pôde ser visto, diferentemente dos outros canais, a morte do emaranhamento acontece apenas no limite assintótico $p \rightarrow 1$ indicando que na passagem de estados GHZ por um canal de defasagem não há morte súbita (ESD). Este comportamento pode ser claramente observado se compararmos o gráfico de $P(p)$ obtido no modelo de defasagem com os obtidos nos canais anteriores onde o emaranhamento morre antes da metade do tempo ($p = 0,5$). Este comportamento é esperado devido ao canal de fase não provocar perda de energia do sistema. Como consequência direta , a perda de correlações quânticas existentes no emaranhamento é menor.

3.3.4 Estados W

Os estados W, diferentemente dos GHZ, possuem número de termos produtos à medida que N também cresce. Como exemplo podemos citar $|W_3\rangle$ e $|W_4\rangle$ explicitados em (2.38, 2.38). Decorre deste fato que sua dinâmica é um pouco, se não muito mais laboriosa que a dos GHZ.

O caso mais simples possível para exemplificar a dinâmica destes estados, seria tomar o estado W com $N = 3$.

$$|W_3\rangle = \alpha\,|001\rangle + \beta\,|010\rangle + \gamma\,|100\rangle \tag{3.40}$$

cuja matriz densidade é escrita na forma

$$\begin{aligned} |W_3\rangle\langle W_3| &= |\alpha|^2\,|001\rangle\langle 001| + |\beta|^2\,|010\rangle\langle 010| + |\gamma|^2\,|100\rangle\langle 100| \\ &= +\alpha\beta^*\,|001\rangle\langle 010| + \alpha\gamma^*\,|001\rangle\langle 100| + \beta\gamma^*\,|010\rangle\langle 100| \\ &= +\alpha^*\beta\,|010\rangle\langle 001| + \alpha^*\gamma\,|100\rangle\langle 001| + \beta^*\gamma\,|011\rangle\langle 010| \end{aligned} \tag{3.41}$$

onde α, β, γ são números complexos que podem ser escritos na forma $\frac{e^{i\alpha}}{\sqrt{3}}, \frac{e^{i\beta}}{\sqrt{3}}, \frac{e^{i\gamma}}{\sqrt{3}}$ e obedecem à relação $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$. Assim, mostraremos a seguir a passagem de $|W_3\rangle$ pelos canais de atenuação de fase, decaimento de amplitude e defasagem, respectivamente.

Atenuação de fase

A aplicação da equação (3.7) ao estado (3.40) nos três qbits nos leva a

$$\begin{aligned} \rho_W^{PD} = {} & |\alpha|^2\,|0\rangle 01\langle 001| + |\beta|^2\,|010\rangle\langle 010| + |\gamma|^2\,|100\rangle\langle 100| + \alpha^*\beta(1-p)^2\,|010\rangle\langle 00| \\ & +\alpha\beta^*(1-p)^2\,|001\rangle\langle 010| + \alpha\gamma^*(1-p)^2\,|001\rangle\langle 100| + \alpha^*\gamma(1-p)^2\,|100\rangle\langle 001| + \\ & \beta\gamma^*(1-p)^2\,|010\rangle\langle 100| + \beta^*\gamma(1-p)^2\,|100\rangle\langle 010| \end{aligned} \tag{3.42}$$

Vemos de (3.42), que os termos da diagonal não sofrem nenhuma modificação e que todos os termos de coerência são multiplicados pelo fator $(1-p)^2$. Uma observação a ser feita, é que ao contrário do GHZ, ao passar pelo canal, os W passam a ter um número maior de elementos de coerência (termos não diagonais) do que o estado inicial como visto acima.

Considerando o número de qbits, quantificar o emaranhamento em (3.42) é ainda uma tarefa fácil no caso do canal de atenuação de fase. Tomando uma bipartição qualquer e sua transposta parcial, obtemos como autovalores

$$|\gamma|^2, \frac{1}{2}(|\alpha|^2 + |\beta|^2 + \sqrt{\Delta_1}), \frac{1}{2}(|\alpha|^2 + |\beta|^2 - \sqrt{\Delta_1}), \sqrt{\Delta_2}(1-p)^2, -\sqrt{\Delta_2}(1-p)^2 \tag{3.43}$$

onde $\Delta_1 = |\alpha|^4 + 2|\alpha\beta|^2 + |\beta|^4 - 16|\alpha\beta|^2p^3 + 4|\alpha\beta|^2p^4 - 16|\alpha\beta|^2p + 24|\alpha\beta|^2p^2$ e $\Delta_2 = |\alpha\gamma|^2 + |\beta\gamma|^2$.

Vemos que a matriz parcialmente transposta possui um autovalor negativo explícito $-\sqrt{\Delta_2}(1-p)^2$ o qual por si só nos dará o peso da separabilidade do estado. Este autovalor deixará de existir (portanto deixaremos de ter um autovalor negativo) apenas quando $p = 1$, ou

seja, no limite assintótico em que $t \to \infty$. Baseado nisto, podemos afirmar na passagem do estado $|W_3\rangle$ pelo canal de atenuação de fase não há morte súbita do emaranhamento.

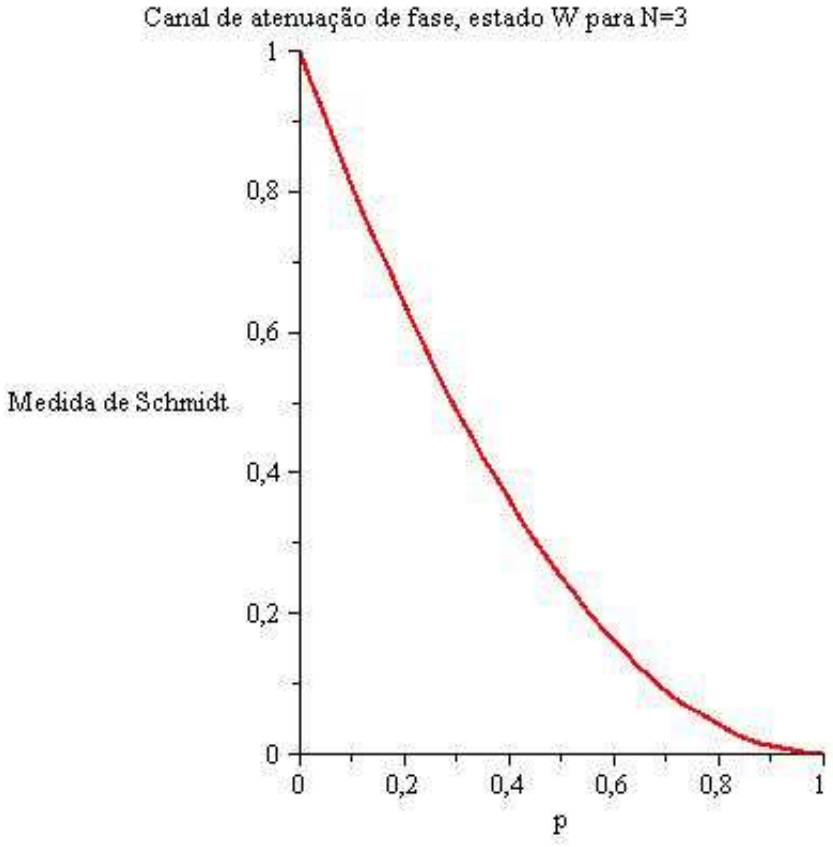

Figura 3.7 Gráfico de $P(\rho(p))$ versus p mostrando a evolução no estado W para $N = 3$ qbits após a passagem pelo canal de atenuação de fase.

O comportamento descrito acima é observado para qualquer bipartição tomada. À medida que N cresce, cresce também a dificuldade na construção da matriz do estado evoluído de W, devido justamente ao aumento do seu número de termos produtos, por exemplo, se $N = 6$ teremos 6 termos produtos em W_6, $N = 100$, 100 termos produtos, e assim sucessivamente. Isto possui uma consequência direta no aumento da dificuldade do cálculo dos autovalores como veremos a seguir, entretanto é de se esperar que o comportamento do emaranhamento, dado pela medida, não se altere após o efeito do canal. Fisicamente a atenuação na fase não altera a distribuiçao de energia do sistema e portanto, deixa intacta a interação entre seus constituintes.

Canal de atenuação de amplitude

O canal de atenuação de amplitude é dado por

$$\mathcal{E}_{AD}\rho = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger \tag{3.44}$$

onde $E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{bmatrix}$ e $E_1 = \begin{bmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{bmatrix}$.

A matriz densidade do estado evoluído, ou seja, após a aplicação do canal aos três qbits será

$$\rho = (1-p)\,|W_3\rangle\,\langle W_3| + p(|\alpha|^2 + |\beta|^2 + |\gamma|^2)\,|000\rangle\,\langle 000| \tag{3.45}$$

É fácil ver em (3.45) que quando $p = 0$ o estado está maximamente emaranhado sendo igual ao estado inicial, e se $p = 1, (t \to \infty)$, ele encontra-se separável, colapsando no estado $|000\rangle\,\langle 000|$.

Tomando uma bipartição qualquer em (3.45) e calculando seus autovalores, encontramos (autovalores não nulos)

- $|\gamma|^2(1-p)$
- $\frac{1}{2}(|\alpha|^2 + |\beta|^2 - \sqrt{\Delta_1}(1-p))$;
- $-\frac{1}{2}(|\alpha|^2 + |\beta|^2 + \sqrt{\Delta_1}(1-p))$;
- $\frac{1}{2}p(|\alpha|^2 + |\gamma|^2 + |\beta|^2 + \sqrt{\Delta_2})$;
- $\frac{1}{2}p(|\alpha|^2 + |\gamma|^2 + |\beta|^2 - \sqrt{\Delta_2})$;

onde $\Delta_1 = (|\alpha|^2 + |\beta|^{22})$ é sempre positivo e $\Delta_2 = |\gamma|^2p^2 + 6p^2|\alpha\gamma|^2 + 2p^2|\beta\gamma|^2 + p^2|\alpha|^4 + 2p^2|\alpha\beta|^2 + p^2|\beta|^4 - 8p|\alpha\gamma|^2 + 4|\alpha\gamma|^2 + (2p\beta\gamma^*)^2 + (2p\beta\gamma^*)^2 - 8p\beta^2(\gamma^*)^2$. Dentre estes autovalores não nulos, vemos que existe um negativo o qual deverá deixar de existir apenas quando $p = 1$, ou seja, quando $t \to \infty$, caso assintótico. Portanto, podemos afirmar que o canal de atenuação de amplitude, assim como o de defasagem, não induz morte súbita no estado $|W_3\rangle$.

Canal de despolarização

Aplicando o canal (3.16) à todos os bits da matriz densidade de $|W_3\rangle$, encontramos como estado final

$$
\begin{aligned}
\rho_W^D &= |000\rangle\langle 000|\,[(|\alpha|^2+|\beta|^2+|\gamma|^2)p/2(1-p/2)^2] \\
&+ |001\rangle\langle 001|\,[|\alpha|^2(1-p/2)^3+(|\beta|^2+|\gamma|^2(p/2)^2(1-p/2)] \\
&+ |010\rangle\langle 010|\,[(|\alpha|^2+|\gamma|^2)(p/2^2)(1-p/2)+|\beta|^2(1-p/2)^3] \\
&+ |011\rangle\langle 011|\,[(|\alpha|^2+|\beta|^2)(p/2)(1-p/2)^2+|\gamma|^2(p/2)^3] \\
&+ |100\rangle\langle 100|\,[(|\alpha|^2+|\beta|^2)(p/2)^2(1-p/2)+|\gamma|^2(1-p/2)^3] \\
&+ |101\rangle\langle 101|\,[(|\alpha|^2+|\gamma|^2)(p/2)(1-p/2)^2+|\beta|^2(p/2)^3] \\
&+ |110\rangle\langle 110|\,[|\alpha|^2(p/2)^2(1-p/2)+(|\beta|^2+|\gamma|^2)(p/2)(1-p/2)^2] \\
&+ |111\rangle\langle 111|\,[(|\alpha|^2+|\beta|^2+|\gamma|^2)(p/2)^2(1-p/2)] \\
&+ |011\rangle\langle 110|\,[\alpha\gamma^*(p/2)(1-p)^2]+|110\rangle\langle 011|\,[\alpha^*\gamma(p/2)(1-p)^2] \\
&+ |001\rangle\langle 010|\,[\alpha\beta^*(1-p)^2(1-p/2)]+|010\rangle\langle 001|\,[\alpha^*\beta(1-p)^2(1-p/2)] \\
&+ |001\rangle\langle 100|\,[\alpha\gamma^*(1-p)^2(1-p/2)]+|100\rangle\langle 001|\,[\alpha^*\gamma(1-p)^2(1-p/2)] \\
&+ |010\rangle\langle 100|\,[\beta\gamma^*(1-p)^2(1-p/2)]+|100\rangle\langle 010|\,[\beta^*\gamma(1-p)^2(1-p/2)] \\
&+ |101\rangle\langle 110|\,[\alpha\beta^*(p/2)(1-p)^2]+|110\rangle\langle 101|\,[\alpha^*\beta(p/2)(1-p)^2] \\
&+ |011\rangle\langle 101|\,[\beta\gamma^*(p/2)(1-p)^2]+|101\rangle\langle 011|\,[\beta^*\gamma(p/2)(1-p)^2]
\end{aligned}
\tag{3.46}
$$

Como vemos, a matriz (3.46) é bem mais "ornamentada"que qualquer caso apresentado anteriormente neste trabalho. Não foi encontrada nenhuma maneira de se escrever os elementos da diagonal numa forma geral como feito para o caso GHZ. Além do mais, ao passar pelo canal, percebe-se claramente que o número de termos de coerência é duplicado. Isto dificulta bastante o cálculo dos autovalores da matriz. Para este caso específico, $N = 3$ seus autovalores foram calculados com a utilização do Maple e foram encontrados com dificuldade[7] pelo software devido à complexidade de tais. Por este motivo eles não serão apresentados aqui, pois nem sequer caberiam em uma única página. A análise do grau do emaranhamento para tais estados neste canal poderia ser melhor realizada através de algum algoritmo que além de calcular os autovalores, realizassem sua simplificação em um software mais poderoso, o que não foi feito no nosso trabalho.

Podemos conjecturar que o emaranhamento dos estados W ao passarem pelo canal de depolarização possa ser mais robusto. Nossa suposição é baseada na característica intrínseca deste estado, apresentada no capítulo anterior, de que eles possuem uma robustez no emaranhamento maior qua a do GHZ a qual pode ser notada ao realizar um traço parcial sobre um dos subsistemas.

A dificuldade algébrica para tratar estados com N qualquer nos impossibilita de ter um resultado conclusivo com respeito à robustez do estado sob efeito desse canal. Pretendemos refinar nosso procedimento algébrico para melhor investigar este conteúdo.

[7] o tempo de computação algébrica cresce com o número de qbits, dificultando a computação do resultado

3.4 Resultados, Conclusões e Perspectivas

Neste trabalho fizemos um breve estudo de alguns critérios de separabilidade, além de quantificadores de emaranhamento com o objetivo de aplicá-los no estudo da dinâmica de alguns estados puros emaranhados.

No estudo da separabilidade foi dada uma ênfase maior aos critérios PPT e Realinhamento, o primeiro por possuir uma prática operacionalidade dando início ao desenvolvimento de uma gama de critérios que seguem a mesma linha de raciocínio como o Realinhamento. Explicitamos a adaptação e aplicação do PPT a estados multipartites, algo que não foi encontrado na literatura nos moldes aqui discutidos. Na quantificação dos estados, foram apresentados dois quantificadores, Negatividade e medida de Schmidt, este último sendo utilizado na quantificação de estados submetidos a efeito de ruídos.

O estudo de modelos de ruídos quânticos é importante para a compreensão de seus efeitos práticos em sistemas físicos. Introduzimos brevemente três canais os quais foram usados para representar a evolução dos estados quânticos GHZ através de sua passagem por cada um deles. A partir do estado evoluído, estudamos quantitativamente o comportamento do emaranhamento com o tempo, tomando o estado maximamente emaranhado em $t = 0$. Este estudo quantitativo já foi realizado em [2] com a utilização da Negatividade como meio quantificador, no nosso caso a medida de Schmidt é usada no lugar da Negatividade, confirmando os resultados obtidos por Aolita [2]. Vale salientar que o uso da medida de Schmidt requer um estudo mais minuncioso dos autovalores do sistema.

Um estudo inédito da evolução do estado W no canal de atenuação de fase e no canal de atenuação de amplitude foi realizado para o caso em que $N = 3$, denunciando a inexistência de morte súbita do emaranhamento na passagem por tais canais. Uma generalização para este caso ainda deve ser feita. Calculamos ainda a evolução deste estado na passagem pelo canal de depolarização, no entanto, sua quantificação continua uma questão aberta, assim também como no caso do canal de amortecimento de amplitude generalizado (GAD).

Dentre os modelos de decoerência estudados, vimos que tanto para os estado GHZ quanto para os W, o canal de atenuação de fase preserva o emaranhamento do sistema por mais tempo, desaparecendo apenas no limite assintótico $t \to \infty$. Deve-se ressaltar que para a transmissão de informação com uso de estados emaranhados é importante saber que o que realmente importa não é que o emaranhamento permaneça por mais tempo, e sim que uma parcela sua significativa permaneça. Tendo conhecimento deste fato, vemos que o uso de estados GHZ para tal tarefa não seria bem recomendado. Podemos especular a utilização dos estados W, no entanto uma investigação mais completa sobre eles deve ainda ser feita.

Referências Bibliográficas

[1] B. Podolsky Einstein, A. and N. Rosen. Can quantum mechanical description of physical reality be considered complete? *Phys. Rev.*, 47, 777, 1935.

[2] D. Cavalcanti A. Acín L. Davidovich L. Aolita, R. Chaves. Scaling laws for the decay of multiqubit entanglement. *Phys. Rev. Lett.*, 100, 080501:4, 2008.

[3] Rieznik A. A. Rigolin, G. Introdução à criptografia quântica. *Revista Brasileira de Ensino de Física*, 27, nº 4:517 – 526, 2005.

[4] Isaac L. Chuang Michael A. Nielsen. *Computação Quântica e Informação Quântica*. 2005.

[5] Ernesto F. Galvão. *O que é computação quântica?* Rio de Janeiro - Ciência no Bolso, 2007.

[6] T. Schmitt-Manderbach H. Weier T. Scheidl M. Lindenthal B. Blauensteiner T.Jennewein J. Perdigues P. Trojek B. Omer M.ÄFÄurst M. Meyenburg J. Rarity Z. Sodnik C. Barbieri H. Weinfurter e A. Zeilinger. R. Ursin, F. Tiefenbacher. Free-space distribution of entanglement and single photons over 144 km. *Nature Physics*, 3:481, 2007.

[7] M. FÄurst R. Ursin F. Tiefenbacher T. Scheidl J. Perdigues Z. Sodnik C. Kurtsiefer J. G. Rarity A. Zeilinger e H. Weinfurter. T. Schmitt-Manderbach, H. Weier. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, 2007.

[8] Brown M. R. Riemann H. Abrosimov N. V. Becker P. Pohl H. Thewalt M. L. W. Itoh K. M. Morton J. J. L. Simmons, S. Entenglement in a solid-state spin ensemble. *Nature*, 09696, 2011.

[9] A. S. O. Coelho. Emaranhamento tripartite no oscilador paramétrico óptico. Master's thesis, USP/IF/SBI, 2009.

[10] Philip Ball. Entangled diamods vibrate together. *Nature*, 2011.

[11] Sandu Popescu Hans J. Briegal. Entanglement and intra-molecular cooling in biological systems? - a quantum thermodynamic perspective. *Quantum Physics*, 2009.

[12] G. R. Fleming M. Sarovar M., A. Ishizaki and K. B. Whaley. Quantum entanglement in photosynthetic light harvesting complexes. *Quantum Physics*, 2010.

[13] N. Bohr. Can quantum mechanical description of physical reality be considered complete? *Phys. Rev.*, 48:696, 1935.

[14] John S. Bell. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys*, 38:447–452, 1966.

[15] Michael Horodecki Karol Horodecki Ryszard Horodecki, Pawel Horodecki. Quantum entanglement. *Rev.Mod.Phys*, 81:865–942, 2009.

[16] Otfried Gühne e Géza Tóth. Entanglement detection. *Physics Reports*, 474, 2009.

[17] Roberto S. Sarthour Jair C.C. Freitas Ivan S. oliveira, Tito J. Bonagama and Eduardo R. deAzevedo. *NMR Quantum Information Processing*. Elsevier, 2007.

[18] A. S. Holevo. Optimal quantum measurements. *Teoret. Mat. Fiz.*, 17, 3:319326, 1973.

[19] Paulo Henrique Souto Ribeiro. Criptografia quântica. *Ciência Hoje*, 47, nº 277:26–31, 2010.

[20] G. Brassard C. H. Bennett. Quantum criptografy: Public key distribution and coin tossing. In *Internationan Conference on Computers, Signal and Signal Processing,*, Bangalore, India - 1984.

[21] Charles Bennett. Quantum cryptography: Uncertainty in the service of privacy. *Science*, 257:752–753, 1992.

[22] Pawel Horodecki Michael Horodecki, Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Rev. A*, 223:1–8, 1996.

[23] S. Popescu B. Schumacher J. Smolin C. H. Bennett, G. Brassard and W. K. Wooters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 78:2031, 1996.

[24] P. Horodecki M. Horodecki and R. Horodecki. Mixed-state entanglement and distillation: Is there a bound entanglement in nature? *Phys. Rev. Lett.*, 80:5239, 1998.

[25] Pawel Horodecki. Separability criterion and inseparable mixed states with positive parcial transposition. *Phys. Lett. A*, 232:333–339, 1997.

[26] Maciej Lewenstein Anna Sanpera Aditi Sen De, Ujjwal Sen. *The separability versus entanglement problem*. Wiley - VCH Berlin, 2006.

[27] O. Rudolph. On the cross norm criterion for separability. *J. Phys. A*, 36:5825, 2003.

[28] Kai Chen and Ling-An Wu. A matrix realinment method for recognizing entanglement. *Quantum Information and Computation*, 3:10, 2003.

[29] Pawe l Horodecki Micha l Horodecki and Ryszard Horodecki. Separability of mixed quantum states: Linear contractions and permutation criteria. *Open Syst. Inf. Dyn.*, 13:103, 2006.

[30] C. J. Oxenrider and R. D. Hill. *Lin. Alg. Appl.*, 69:205, 1985.

[31] P. Horodecki M. Horodecki and R. Horodecki. Separability criterion and inseparable mixed states with positive parcial transposition. *Phys. Lett. A*, 223, 1, 1996.

[32] M. A. Nielsen. *Quantum Information Theory*. PhD thesis, The University of New Mexico, 1998.

[33] M. A. Horne D. M. Greenberger and A. Zeilinger. *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*. Kluwer, Dordrecht, 1989.

[34] K. Chen and H. K. Lo. Multipartite quantum cryptografic protocols qith noisy ghz states. *Quantum Inf. Comp.*, 7:689, 2007.

[35] M. Christandl and S. Wehner. Quantum anonymous transmissions. *Proc. of 11th ASIACRYPT, LNCS*, 3788:217, 2005.

[36] D. Gottesman and I. Chuang. Demonstraiting the viability of universal quantum computation using teleportation and single qbit operations. *Nature*, 402:390, 1999.

[37] V. Buzec M. Hillery and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829, 1999.

[38] A.-N. Zhang T. Yang H. J. Briegel Z. Zhao, Y.-A. Chen and J.-W. Pan. Experimental demonstration of the five photon entanglement and open-destination teleportation. *Nature*, 430:54, 2004.

[39] T. Schätz J. Britton J. Chiaverini W. M. Itano J. D. Jost C. Langer D. Leibfried, M. D. Barret and D. J. Wineland. Toward heisemberg-limited spectroscopy with multiparticle entangled states. *Science*, 304:1476, 2004.

[40] S. Lloyd V. Giovannetti and L. Maccone. Quantum-enhanced measurements: Beating the standart quantum limit. *Science*, 306:1330, 2004.

[41] J. Myrheim F. Verstraete and B. De Moor. Normal forms and entanglement measures for multipartite quantum states. *Phys. Rev. A*, 68:012103, 2003.

[42] A. Higuchi H. A. Cartered and A. Sudberry. Multipartite generalisation of the schmidt decomposition. *J. Math. Phys.*, 41:7932, 2000.

[43] A. Sudbery. On local invariants of pure three-qubit states. *J. Phys. Math. Gen.*, 34:643, 2001.

[44] E Jané A Acín, A Andrianov and R Tarrach. Three-qubit pure-state canonical forms. *J. Phys A: Math Gen.*, 34:6725, 2001.

[45] Julia Kempe. Multiparticle entanglement and its applications to cryptography. *Phys. Rev. A*, 60:910, 1999.

[46] Sayatnova Tamaryan Levon Tamaryan, DaeKil Park. Generalized schmidt decomposition based on injective tensor norm. *Quantum Physics*, arXiv:0809.1290v2, 2009.

[47] Dehaene J. Verstraete, F. and B. De. Moor. Normal forms and entanglement measures for multipartite quantum states. *Physical Review A*, 68: 012103, 2003.

[48] Anton Zeilinger Daniel M. Greenberger, Michael A. Horne. Going beyond bell's theorem. *Quantum Physics*, arXiv:0712.0921v1, 2007.

[49] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838, 1990.

[50] Valerio Scarani and Nicolas Gisin. Spectral decomposition of bell's operators for qubits. *J. Phys A: Math Gen.*, 34:6043, 2001.

[51] W. Dür and J. I. Cirac. Classification of multiqubit mixed states: Separability and distillability properties. *Phys. Rev. A*, 61:042314, 2000.

[52] G. Vidal W. Dür and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:062314, 2000.

[53] Vladimír Buek Masato Koashi and Nobuyuki Imoto. Entangled webs: Tight bound for symmetric sharing of entanglement. *Phys. Rev. A*, 62:050302, 2000.

[54] R. H. Dicke. Coherence in spontaneous radiation processes. *Phys. Rev.*, 93:99, 1954.

[55] Hans J. Briegel Jens Eisert. Schmidt measure as a tool for quantifying multiparticle entanglement. *Phys. Rev. A*, 64:4, 2001.

[56] Otfried Gühne and Michael Seevinck. Separability criteria for genuine multiparticle entanglement. *New Journal of Physics*, 12:9, 2010.

[57] Otfried Gühne. Entanglement criterion and full separability of multiqubit quantum states. *Physics Letters A*, 375:11, 2011.

[58] O. Tóth, G.; Gühne. Separability criteria and entanglement witnesses for symmetric quantum states. *Appl. Phys. B*, 98:617–622, 2010.

[59] Pawel Horodecki M. Horodecki, Ryszard Horodecki. Limits for entanglement measures. *Phys. Rev. Lett.*, 84:2014–2017, 2000.

[60] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, 1996.

[61] R.F. Werner G. Vidal. Computable measure of entanglement. *Phys. Rev. A*, 65, 032314:11, 2002.

[62] John Preskill. Lecture notes for physics 229: Quantum information and computation. California Institute of Technology, September, 1998.

[63] Barbara M. Terhal Pawel Horodecki, John A. Smolin and Ashish V. Thapliyal. Rank two bipartite bound entangled states do not exist. *Theoretical Computer Science*, 292:589–596, 2003.

[64] Ting Yu and J. H. Eberly. Sudden death of entanglement. *SCIENCE*, 323, 2009.

[65] M. Hor-Meyll A. Salles S. P. Walborn P. H. Souto Ribeiro M. P. Almeida, F. de Melo and L. Davidovich. Environment-induced sudden death of entanglement. *Science*, 316:579–582, 2007.

[66] Aércio Ferreira de Lima. *Notas de Aula: Uma Introdução a Computação e Informação Quânticas*. 2004.

APÊNDICE A

Alguns Tópicos em Processamento da Informação Quântica

A.1 Brackets, a notação de Dirac

Notação Bra-ket é uma notação padrão para descrever estados quânticos na teoria da mecânica quântica, principalmente devido à sua praticidade em representar as transformações e estados quânticos, como será visto adiante. O símbolo $\langle\cdot|$ é chamado de *bra* e o símbolo $|\cdot\rangle$ é chamado de *ket*. A notação $\langle\cdot|\cdot\rangle$ é então chamada de *bracket*. A notação foi criada por Paul Dirac, e por isso é também conhecida como notação de Dirac.

Além disso, a notação de Dirac para espaços vetoriais adquire um significado adicional. Um *ket* como $|x\rangle$ denota vetores em coluna e são geralmente usados para descrever estados quânticos. O *bra* $\langle x|$ denota a conjugada[1] transposta de $|x\rangle$, e é denotado por um vetor em linha.

De acordo com a notação de Dirac para espaços vetoriais, $\langle\phi|\psi\rangle$ agora denota o *produto interno* de dois vetores. Por exemplo, sejam $|0\rangle$ e $|1\rangle$ duas bases ortonormais.[2] Como $|0\rangle$ é um vetor unitário, então $\langle 0|0\rangle = 1$ e como $|0\rangle$ e $|1\rangle$ são ortonormais, então $\langle 0|1\rangle = 0$. A notação $|\phi\rangle\langle\psi|$ significa o *produto vetorial* (produto externo) dos dois vetores. Pode-se também expressar $|\phi\rangle\langle\psi|$ em forma de matrizes. Por exemplo, $|0\rangle\langle 1|$ poderia ser escrito em sua forma matricial, onde $|0\rangle = [1,0]^T$, $\langle 0| = [1,0]$, $|1\rangle = [0,1]^T$, $\langle 1| = [0,1]$, então:

$$|0\rangle\langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \tag{A.1}$$

Como visto acima, um ket $|x\rangle$ é uma maneira útil e concisa para descrever as bases (e estados como um todo) de um espaço vetorial.

[1] O complexo conjugado de um número complexo $z = a + bi$ é definido como $z^\dagger = a - bi$. A matriz conjugada da matriz A é a matriz obtida substituindo cada elemento $a_{j,k} \in A$ pelo seu complexo conjugado $a^\dagger_{j,k}$.

[2] Base ortonormal é uma base ortogonal onde os vetores da base são unitários.

A.2 Espaço de Hilbert

Para entendermos um pouco da mecânica quântica necessária para a computação quântica e informação quântica, precisamos ter uma compreensão minuciosa de alguns conceitos básicos da algebra linear. Sabemos que a Algebra Linear estuda operações lineares em espaços vetoriais, mas na Mecânica Quântica o espaço vetorial utilizado é o espaço de Hilbert $(\mathcal{H})$ ou espaço veorial complexo $\mathbb{C}^n$ e linear.

Espaços de Hilbert são uma classe especial de espaços normados. Toda a teoria destes espaços foi criada pelo matemático alemão David Hilbert por volta de 1912, onde os elementos abstratos do espaço de Hilbert são denominados de vetores. Esse espaço vetorial é dotado de um produto interno, ou seja, noções de distância e ângulos e obdece à relação de completitude, garantindo que os limites existem quando esperados, o que permite e facilita diversas definições de análise. Logo na mecânica quântica um sistema físico é descrito por um espaço de Hilbert complexo que contém os vetores de estado os quais contêm todas as informações do sistema.

Observemos algumas propriedades fundamentais que constituem o espaço de Hilbert [66], são elas:

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

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

i) se dois vetores $|f\rangle, |g\rangle \in \mathcal{H}$, então a soma $|f\rangle + |g\rangle$ também é um vetor de $\mathcal{H}$;

ii) a soma é comutativa e associativa: $|f\rangle + |g\rangle = |g\rangle + |f\rangle$ e $(|f\rangle + |g\rangle) + |h\rangle = |f\rangle + (|g\rangle + |h\rangle)$;

iii) existe em $\mathcal{H}$ um vetor chamado nulo, tal que $|f\rangle + 0 = |f\rangle \ \forall \ |f\rangle \in \mathcal{H}$;

iv) é definida também uma operação de produto por escalar sendo que α e β pertencem ao conjunto dos complexos, e $|f\rangle$ e $|g\rangle$ são elementos de $\mathcal{H}$, logo:

a) $\alpha |f\rangle \in \mathcal{H}$

b) $(\alpha\beta) |f\rangle = \alpha(\beta |f\rangle)$

c) $(\alpha + \beta) |f\rangle = \alpha |f\rangle + \beta |f\rangle$

d) $\alpha(|f\rangle + |g\rangle) = \alpha |f\rangle + \alpha |g\rangle$

e) $1 |f\rangle = |f\rangle$

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

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

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

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

iii) $(|f\rangle, \alpha |g\rangle) = \alpha(|f\rangle, |g\rangle)$ ou $\langle f | \alpha |g\rangle = \alpha \langle f | g\rangle$;

iv) $(\alpha\,|f\rangle\,,|g\rangle) = \alpha^*(|f\rangle\,,|g\rangle)$

v) $(|f\rangle\,,|f\rangle) \geq 0$, e $(|f\rangle\,,|f\rangle) = 0$ ou $\langle f|\,f\rangle \geq 0$ e $\langle f|\,f\rangle = 0$ se e somente se $|f\rangle = 0$ (vetor nulo).

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

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

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

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

$$|\psi\rangle = \sum_{i=1}^{N} \alpha_i\,|e_i\rangle \tag{A.2}$$

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

A.3 Algebra Linear

A.3.1 Operadores lineares e matrizes

Consideremos dois espaços vetoriais V e W. Um operador linear entre V e W é definido como uma aplicação $A : V \to W$, linear na sua ação

$$A\big(\sum_i a_i\,|v_i\rangle\,\big) = \sum_i a_i A\,|v_i\rangle \tag{A.3}$$

Um operador linear A definido no espaço vetorial V é um operador que atua em V levando-o para o próprio espaço V.Como exemplo de operador deste tipo para qualquer espaço, temos o operador identidade I.

As operações lineares são mais bem entendidas através da sua representação matricial. Existe uma completa equivalência entre a operação linear no espaço vetotial e a matriz que a representa neste espaço. Considere uma operaçaõ linear do tipo $A : V \to W$ entre os espaços vetoriais V e W. Suponha que $\{|v_1\rangle\,,|v_2\rangle\,,...,|v_n\rangle\}$ é uma base para V e $\{|w_1\rangle\,,|w_2\rangle\,,...,|w_n\rangle\}$ é uma base para W. Então, para j variando de $1,...,n$, existem números de A_{1j} até A_{nj} tais que

$$A|v_i\rangle = \sum_{i=1}^{n} A_{ij}|w_i\rangle \tag{A.4}$$

A matriz cujos elementos são A_{ij} é a chamada representação matricial do operador linear A. Para se determinar a representação matricial do operador linear, é necessário especificar as entradas e as saídas da operação sobre os vetores da base do espaço vetorial no qual o operador é aplicado. Por exemplo, consideremos Um operador A no espaço vetorial V, com vetores da base $|0\rangle$ e $|1\rangle$. A atuação dos vetores na base (de entrada) é dada por $A|0\rangle = |1\rangle$ e $A|1\rangle = |0\rangle$. Escolhendo a base de saída dada por $|0\rangle$ e $|1\rangle$, encontramos como representação matricial

$$A|0\rangle = 0|0\rangle + 1|1\rangle = A_{00}|0\rangle + A_{01}|1\rangle \tag{A.5}$$

$$A|1\rangle = 1|0\rangle + 0|1\rangle = A_{10}|0\rangle + A_{11}|1\rangle \tag{A.6}$$

Associando o resultado aos elementos de matriz através da equação A.4, achamos a matriz representativa para este caso

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{A.7}$$

A.3.2 Autovalores e autovetores

Um autovetor de um operador linear A em um espaço vetorial, é um vetor $|v\rangle$ tal que $A|v\rangle = v|v\rangle$, em que v é um número complexo conhecido como autovalor de A, correspondente a v. Os autovalores são encontrados a partir da solução da equação característica definida como $det|A - \lambda I| = 0$, onde det é o determinante da matriz.

A representação diagonal de um operador A em um espaço vetorial V, é uma representação do tipo $A = \sum_i \lambda_i |i\rangle\langle i|$, em que os vetores $|i\rangle$ formam um conjunto de autovetores ortogonais de A, com autovalores correspondentes λ_i. Um operador é dito diagonalizável se possuir uma representação diagonal deste tipo.

A.3.3 Operadores Hermitianos e Positivos

Operadores Hermitianos

Se A é um operador linear em um espaço de Hilbert V. Resulta que existe um único operador linear $A^\dagger$ em V, tal que para todos os vetores $|v\rangle, |w\rangle \in V$,

$$(|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle) \tag{A.8}$$

Este operador é conhecido como adjunto ou conjugado hermitiano de A. Da definição, é fácil ver que $(AB)^\dagger = B^\dagger A^\dagger$. É importatnte saber como a definição da operação adjunta se

traduz nas representações matriciais dos operadores lineares. Para isso observe que calculando o complexo conjugado de A.8 teremos

$$\begin{aligned} (|v\rangle, A|w\rangle)* &= (A^\dagger|v\rangle, |w\rangle)* = (|w\rangle, A^\dagger|v\rangle) && \text{(A.9)} \\ \langle v|A|w\rangle * &= \langle w|A^\dagger|v\rangle \end{aligned}$$

(A.10)

Definição A.1. *A operação adjunta " † " é aquivalente à trnsposição da matriz e conjugação complexa dos seus elementos.*

Como $|v\rangle$ e $|w\rangle$ são quaisquer, podemos considerálos como vetores da base ortonormal $\{|i\rangle, |j\rangle\}$ de V. Assim, A.9 determina os elementos de matriz do operador A em V,

$$A^*_{ji} = A^\dagger_{ij}$$

.

Pode-se mostrar que todo operador hermitiano possui autovalores reais e que seus autovetores são ortogonais.

Prova

A equação de autovalores é dada por $A|a\rangle = a|a\rangle$. Seu complexo conjugado é $\langle a|A^\dagger = \langle a|a*$. Multiplicando a primeira por $\langle a|$ e a segunda por $|a\rangle$ teremos

$$\begin{aligned} \langle a|A|a\rangle &= a|a\rangle\langle a| && \text{(A.11)} \\ \langle a|A^\dagger|a\rangle &= a*|a\rangle\langle a| && \text{(A.12)} \end{aligned}$$

(A.13)

Segue-se que por definição $A^\dagger = A$, portanto teremos que $a* = a$, ou seja, os autovalores serão reais. Com relação aos autovetores, teremos

$$A|a\rangle = a|a\rangle \quad \text{(A.14)}$$

$$A|a'\rangle = a'|a'\rangle \quad \text{(A.15)}$$

(A.16)

multiplicando novamente a primeira equação acima por $\langle a'|$ e a segunda por $\langle a|$, teremos

$$\langle a'| A |a\rangle = a \langle a'| a\rangle \tag{A.17}$$

$$\langle a'| A^\dagger |a\rangle = a' \langle a'| a\rangle \tag{A.18}$$

igualando as duas equações A.17 e A.18, teremos que $(a - a') \langle a'| a\rangle = 0$. Como um operador linear deve ter ao menos um auto valor não nulo, esta igualdade só será verdadeira se $\langle a'| a\rangle = 0$.

A.3.4 Operadores positivos

Operadores positivos são um subconjunto de operadores hermitianos muito importantes na discussão da teoria de medições de sistemas quânticos.

Definição A.2. *Um operador A é dito positivo, se para todo $|v\rangle$*

$$|v\rangle A |v\rangle \geq 0$$

A.3.5 Produto tensorial

O produto tensorial é uma forma de se juntar espaços vetoriais para formar espaços vetoriais maiores, sendo de excencial importância na mecânica quântica para a descrição de sistemas compostos por várias partículas.

Supanha V e W espaços vetoriais de Hilbert de dimensões m e n respectivamente. $V \otimes W$ (lê-se V tensor W) será um espaço vetorial com dimensão mn. Os elementos de $V \otimes W$ são combinações lineares de produtos tensoriais $|v\rangle \otimes |w\rangle$ dos elementos $|v\rangle$ de V e $|w\rangle$ de W. Se $|i\rangle, |j\rangle$ são bases ortonormais destes dois espaços, então $|i\rangle \otimes |j\rangle$ é uma base de $V \otimes W$. O sinal $\otimes$ pode ser omitido por simplicidade e o produto tensorial entre dois vetores pode ser expresso como $|i\rangle \otimes |j\rangle = |ij\rangle$.

O produto tensorial satisfaz as seguintes propriedades

1. Para um escalar z arbitrário, e elementos $|v\rangle$ de V e $|w\rangle$ de W,

$$z(|v\rangle \otimes |w\rangle) = (z |v\rangle) \otimes |w\rangle = |v\rangle \otimes z(|w\rangle) \tag{A.19}$$

2. Para $|v_1\rangle$ e $|v_2\rangle$ arbitrários em V e $|w\rangle$ em W,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle \tag{A.20}$$

3. Pra $|v\rangle$ arbitrário em V e $|w_1\rangle$ e $|w_2\rangle$ em W,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle \tag{A.21}$$

A representação matricial do produto de kronecker é dada a seguir. Seja A uma matriz $m \times n$, e B uma matriz $p \times q$, o produto $A \otimes B$ será

$$\begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix} \tag{A.22}$$

ou, de forma mais explícita, podemos usar como exemplo as matrizes de Pauli $X \otimes Y$

$$X \otimes Y = \begin{bmatrix} 0 \cdot Y & 1 \cdot Y \\ 1 \cdot Y & 0 \cdot Y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix} \tag{A.23}$$

A.3.6 Produto interno de Hilbert-Schmidt

A definição do produto interno de Hilbert-Schmidt aparece como um exercício em [4]. O conjunto L_V de operadores lineares em um espaço de Hilbert V é definido também um espaço vetorial, obedecendo as seguintes propriedades

1. zA é um operador linear se A é um operador linear;
2. existe um elemento nulo 0.

A função $(.,.)$ sobre $L_V \times L_V$ é definida por $(A, B) \equiv tr(A^\dagger B)$ é uma função produto interno chamado de produto interno de Hilbert-Schmidt ou traço. No caso de operadores hermitianos onde $A = A^\dagger$, teremos $(A, A) \equiv tr(A^\dagger A) = tr(A^2)$

Existe um análogo da norma de vetores para o caso de operadores, que é a norma do traço de operadores definida por

$$||A|| = tr\sqrt{(A^\dagger A)}$$

.

A.4 Matrizes e Grupos de Pauli

A discretização dos erros é um dos pontos fundamentais na teoria de códigos quânticos. O conceito por trás da discretização é que um operador de erro arbitrário com elementos complexos pode ser representado em uma base de erros. Dentre as inúmeras escolhas possíveis para a base de erros, utiliza-se com frequência a base formada pelas matrizes de Pauli $\sigma_0 = I_2$, $\sigma_x = X$, $\sigma_y = Y$ e $\sigma_z = Z$. Essas matrizes são definidas como:

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad sendo \ i = \sqrt{-1}. \tag{A.24}$$

Pode-se verificar facilmente que: $\sigma_x = i\sigma_z\sigma_y = -i\sigma_y\sigma_z$, $\sigma_y = i\sigma_x\sigma_z = -i\sigma_z\sigma_x$ e $\sigma_z = -i\sigma_x\sigma_y = i\sigma_y\sigma_x$. Dessa forma, as matrizes de Pauli, descritas acima, multiplicadas pelos fatores ± 1 e $\pm i$ formam um grupo sob multiplicação, o grupo de Pauli denotado por $\mathcal{P}_1$.

As matrizes de Pauli definidas em (A.24) representam operações unitárias que atuam sobre um único qbit. Assim como um sistema composto formado por n qbits independentes é representado pelo produto tensorial de n qbits, a base de erro para n qbits é formada por todas as combinações de n produtos tensoriais das matrizes de Pauli. De modo similar, n produtos tensoriais de matrizes de Pauli multiplicados pelos fatores ± 1 e $\pm i$ formam um grupo sob multiplicação, o grupo de Pauli $\mathcal{P}_n$.

As matrizes de Pauli dadas em (A.24) ou comutam ou anticomutam. Duas matrizes A e B comutam se $[A, B] \equiv AB - BA = 0$ e anticomutam se $\{A, B\} \equiv AB + BA = 0$. Para as matrizes de Pauli tem-se que:

- $\{\sigma_i, \sigma_j\} = 0$, sendo $i, j \in (x, y, z)$ e $i \neq j$;
- $[\sigma_i, \sigma_i] = 0$, sendo $i \in (x, y, z)$;
- $[\sigma_0, \sigma_i] = 0$, sendo $i \in (0, x, y, z)$.

A importância das relações de comutação é que duas matrizes que comutam podem ser diagonalizadas simultaneamente. As matrizes σ_0 e σ_x por exemplo, podem ser escritas na base formada pelos autovetores de σ_x $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, como: $\sigma_0 = 1/2(|+\rangle\langle+|) + 1/2(|-\rangle\langle-|)$ e $\sigma_x = 1/2(|+\rangle\langle+|) - 1/2(|-\rangle\langle-|)$.

Produtos tensoriais de n matrizes de Pauli também comutam ou anticomutam. Isto pode ser mostrado considerando o fato que para quaisquer matrizes A, B, C e D com ordens compatíveis, tem-se que $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$. Sendo assim, tem-se que $(\sigma_i^1 \otimes \sigma_i^2 \otimes \cdots \otimes \sigma_i^n) \cdot (\sigma_j^1 \otimes \sigma_j^2 \otimes \cdots \otimes \sigma_j^n) = (\sigma_i^1\sigma_j^1) \otimes (\sigma_i^2\sigma_j^2) \otimes \cdots \otimes (\sigma_i^n\sigma_j^n)$. Se um número ímpar de produtos $\sigma_i^k\sigma_j^k$ anticomuta então os dois produtos tensoriais anticomutam. Caso esse número seja par, eles comutam.

Com base no que foi exposto acima, seguem então algumas propriedades úteis do grupo de Pauli $\mathcal{P}_n$: (i) todo elemento de $\mathcal{P}_n$ se combina com $\pm I$ (mais ou menos a identidade); (ii) quaisquer dois elementos de $\mathcal{P}_n$ ou comutam ou anticomutam; (iii) todo elemento de $\mathcal{P}_n$ é unitário.

A.5 Teorema da Não Clonagem

Seria possível criar uma combinação de circuitos quânticos mais complicada que conseguisse copiar estados quânticos arbitrários? A resposta é não. É impossível clonar um estado quântico. É fácil verificar que a clonagem é impossível de ser realizada usando uma medição desse estado. Isso porque, para clonar um estado, seria necessário realizar uma medição nele. No entanto, ao realizar a medição, seria criado um qbit clone, mas o qbit original teria sido colapsado devido à medição feita. Qualquer outro método utilizado para tentar clonar qbits também seria uma tentativa fadada ao fracasso devido ao Teorema da Não Clonagem.

Teorema A.1 (Teorema da Não Clonagem)**.** *[4] Seja $|\psi\rangle$ um estado. Não existe uma transformação unitária U tal que*

$$U\,|\psi 0\rangle = |\psi\psi\rangle\,.$$

Demonstração: Suponha que exista U tal que:

$$\begin{aligned} U(|\psi 0\rangle) &= |\psi\psi\rangle\,, \\ U(|\phi 0\rangle) &= |\phi\phi\rangle\,, \end{aligned} \tag{A.25}$$

para quaisquer ψ, ϕ. U estaria representando a suposta operação de clonagem. Considere $|\varphi\rangle = (1/\sqrt{2})(|\psi\rangle + |\phi\rangle)$. Então, por linearidade:

$$\begin{aligned} U(|\varphi 0\rangle) &= \frac{1}{\sqrt{2}}\Big(U\big(\,|\psi 0\rangle\,\big) + U\big(\,|\phi 0\rangle\,\big)\Big) \\ &= \frac{1}{\sqrt{2}}\Big(\,|\psi\psi\rangle + |\phi\phi\rangle\,\Big). \end{aligned} \tag{A.26}$$

Mas se U é uma transformação de clonagem, então:

$$U(|\varphi 0\rangle) = |\varphi\varphi\rangle = \frac{1}{2}\Big(\,|\psi\psi\rangle + |\psi\phi\rangle + |\phi\psi\rangle + |\phi\phi\rangle\,\Big). \tag{A.27}$$

C.Q.D.

É importante entender que os qbits cujos estados quânticos são conhecidos são facilmente clonáveis, pois já estão colapsados em alguma base, e qualquer medição realizada não irá mudar seu estado, ou seja, é análogo a copiar (clonar) bits clássicos. O que o Teorema da Não Clonagem realmente diz é que não há como clonar qbits cujos estados quânticos sejam desconhecidos.

A.6 Portas Quânticas Elementares

Para a construção de circuitos quânticos, é necessário a contrução de portas quânticas lógicas que podem representar operações locais. Nesta seção apresentaremos algumas portas utilizadas em nosso texto, são elas o Not, o CNot e o Hadamard.

A.6.1 NOT

A porta clássica mais simples é a porta NOT, que é uma porta de um bit que nega o estado do bit de entrada: 0 vira 1 e vice-versa. A porta quântica correspondente é implementada via uma operação unitária que faz com que os estados-base mudem seus estados de acordo com a tabela-verdade do NOT clássico. O U_{not} é a operação quântica unitária que corresponde ao NOT clássico e é representada pela matriz de Pauli σ_x a qual denotaremos por X. Essa operação, aplicada a um estado, pode ser descrita como

$$\begin{aligned} X(|0\rangle) &= |1\rangle\,, \\ X(|1\rangle) &= |0\rangle\,. \end{aligned}$$

Supondo que $|0\rangle$ e $|1\rangle$ sejam definidos como os vetores $[1,0]^T$ e $[0,1]^T$, respectivamente, então a operação de NOT funciona da seguinte maneira:

$$X(|0\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle.$$

Analogamente, pode-se aplicar X para $|1\rangle$.

A.6.2 Hadamard

Uma das mais importantes portas da computação quântica, a porta Hadamard não tem uma função análoga na computação clássica. Sua matriz é dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{A.28}$$

Sua função é a seguinte

$$\begin{aligned} H\big(\,|0\rangle\,\big) &= \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big), \\ H\big(\,|1\rangle\,\big) &= \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big). \end{aligned}$$

No caso de um estado formado por mais de um qbit, a porta H é aplicada em todos os qbits do estado. Essa transformação é de grande utilidade: seja $|\psi\rangle$ um estado inicialmente configurado com todos os seus qbits em $|0\rangle$. Aplicando-se a porta H em cada qbit separadamente, então o resultado fica

$$\begin{aligned} |\psi\rangle &= H \otimes H \otimes \cdots \otimes H \, |00\cdots0\rangle \\ &= \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \\ &= \left(\frac{1}{\sqrt{2}}\right)^n \Big(\,|00\cdots0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle\,\Big) \\ &= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{i=0}^{2^n-1} |i\rangle\,. \end{aligned} \tag{A.29}$$

Em outras palavras, ao aplicar a transformação Hadamard num estado inicialmente configurado em $|00\cdots0\rangle$, consegue-se uma sobreposição de todos os valores possíveis de ser armazenados nesse estado. Além disso, com um número linear de operações (i.e, para um estado de n qbits, aplica-se a porta Hadamard n vezes), gera-se um estado que contém um número exponencial (2^n) de termos distintos, i.e., o estado contém todos os valores numéricos de tamanho n possíveis em sobreposição e com a mesma amplitude. Em contraste com o caso clássico, num estado de n bits, pode-se armazenar somente um único valor numérico em cada estado.

A.6.3 NOT-Controlado

A porta NOT-Controlado (abreviada como CNOT) tem sua representação num circuito qualquer pela Figura A.1.

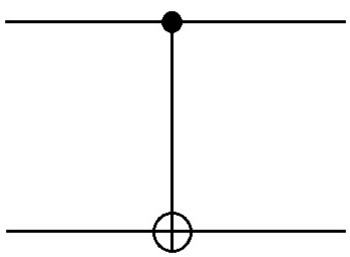

Figura A.1 Notação para a porta NOT-Controlado (CNOT).

Vamos supor que um qbit $|a\rangle$ posiciona-se na linha de cima, e um outro qbit $|b\rangle$ na de baixo. Esse diagrama nos diz que o qbit $|a\rangle$ é um sinal de controle para especificar se deve-se

ou não negar o qbit $|b\rangle$. Em outras palavras, se o qbit $|a\rangle$ estiver "ligado", o qbit $|b\rangle$ é negado. Se $|a\rangle$ estiver "desligado", $|b\rangle$ não é modificado. Essa transformação é dada pela matriz

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$