



UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

JOÃO LUZEILTON DE OLIVEIRA

**FERRAMENTAS ALGÉBRICAS PARA O ESTUDO DO
ENTRELAÇAMENTO QUÂNTICO**

Fortaleza - Ceará

Março - 2012

UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

Ferramentas Algébricas para o Estudo do Entrelaçamento Quântico

Autor

JOÃO LUZEILTON DE OLIVEIRA

Orientador

RUBENS VIANA RAMOS

Tese submetida à Coordenação do Curso de Pós-Graduação em Engenharia de Teleinformática, da Universidade Federal do Ceará, como requisito parcial para a obtenção do grau de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado.

Fortaleza - Ceará

Março - 2012

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca de Pós-Graduação em Engenharia - BPGE

-
- O47f Oliveira, João Luzeilton de.
Ferramentas algébricas para o estudo do entrelaçamento quântico. / João Luzeilton de Oliveira – 2012.
161 f. : il. color., enc. ; 30 cm.
- Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Departamento de Engenharia de Teleinformática, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2012
Área de Concentração: Eletromagnetismo aplicado.
Orientação: Prof. Dr. Rubens Viana Ramos.
1. Teleinformática. 2. Entrelaçamento quântico. 3. Algoritmos quânticos. I. Título.

CDD 621.38

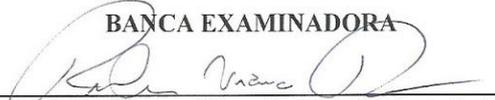
JOÃO LUZEILTON DE OLIVEIRA

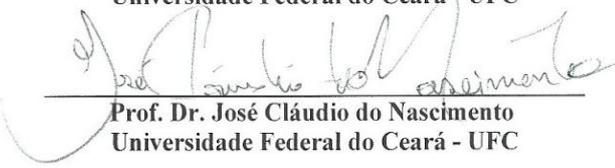
FERRAMENTAS ALGÉBRICAS PARA O ESTUDO DO ENTRELAÇAMENTO
QUÂNTICO

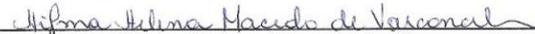
Tese submetida à Coordenação do Curso de Pós-Graduação em Engenharia de Teleinformática, da Universidade Federal do Ceará, como requisito parcial para a obtenção do grau de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado

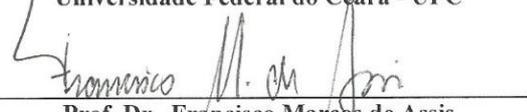
Aprovada em 02/03/2012.

BANCA EXAMINADORA


Prof. Dr. Rubens Viana Ramos (Orientador)
Universidade Federal do Ceará - UFC


Prof. Dr. José Cláudio do Nascimento
Universidade Federal do Ceará - UFC


Prof. Dr. Hilma Helena Macedo de Vasconcelos
Universidade Federal do Ceará - UFC


Prof. Dr. Francisco Marcos de Assis
Universidade Federal de Campina Grande - UFCG


Prof. Dr. Marcelo de Oliveira Terra Cunha
Universidade Federal de Minas Gerais - UFMG

DEDICATÓRIA

Aos meus pais Inácio Vieira de Oliveira (in memoriam) e Antonia Cardoso de Oliveira, à minha esposa Oralnir e aos meus filhos Luzeilton Jr., Glória Maria e Gabriel Inácio, as pessoas mais importantes da minha vida.

AGRADECIMENTOS

Este é um momento de muita alegria, momento em que se celebra uma grande conquista, depois de alguns anos de muito trabalho. Durante esse percurso, muitas inquietações surgiram. E, por isso, é hora de agradecer a todos que colaboraram de alguma maneira para que todos os obstáculos encontrados nessa trajetória fossem superados.

Inicialmente, agradeço a Deus por ter iluminado o caminho para que eu pudesse seguir e chegar ao final de mais uma grande caminhada.

Aos meus pais, pois o que hoje sou, devo à dedicação e à seriedade com que eles me educaram.

Ao professor Dr. Rubens Viana Ramos, orientador, que se tornou também um amigo, por sua dedicação, paciência e sabedoria na orientação desta tese.

Ao amigo David Sena, pela parceria ao longo desses anos de doutorado, parceria essa que me fez aprender bastante, não somente sobre entrelaçamento quântico, mas, principalmente, lições para a vida. Agora, é só dar continuidade aos trabalhos.

Aos colegas do GIQ, meu amigo Fábio Alencar (Fabão), Daniel Barbosa, João Batista, Fernando, Fátima, Socorro, Emanoela, Keuliane e Glaucionor, pelo aprendizado, pelo convívio, pelos momentos de descontração e pela companhia nas horas de almoço e traller. Também, à colega Janaína do LABVIS.

Um agradecimento especial ao também colega do GIQ, meu amigo, Paulo Vinicius, pela ajuda nos gráficos e figuras. Valeu Paulo! Muito obrigado!

Aos funcionários do DETI, Renato e Miraneide, os meus agradecimentos.

Ao meu colega de UECE e amigo, prof. Dr. Ulisses Lima Parente, pela paciência quando me ouvia nos momentos de inquietação, preocupação e satisfação quando os resultados estavam dando certo.

Ao meu sogro José Oracy Sales e ao amigo Jorge Gleisson pelo incentivo, força e compreensão nos momentos de angústia.

À minha esposa Oralnir Sales Oliveira e aos meus filhos João Luzeilton de Oliveira Jr., Glória Maria Sales Oliveira e Gabriel Inácio Sales Oliveira, motivos da minha batalha diária, por suportarem a minha ausência, mesmo estando presente fisicamente, nesses anos de doutorado.

À Universidade Estadual do Ceará, pelo apoio na realização deste trabalho.

EPÍGRAFE

“Deus nos fez perfeitos e não escolhe os capacitados, capacita os escolhidos. Fazer ou não fazer algo, só depende de nossa vontade e perseverança.”

Albert Einstein

ÍNDICE

PREÂMBULO

Lista de Figuras	xi
Lista de Tabelas	xii
Resumo	13
Abstract.....	14
Introdução.....	15

CAPÍTULOS

Capítulo 1 - Critérios de Separabilidade e Medidas de Entrelaçamento Quântico	18
1.1. Separabilidade	18
1.1.1. Critério de Separação de Peres-Horodecki.....	21
1.1.2. Critério de Horodecki.....	29
1.1.3. Critério de Separação Baseado na Imagem do Operador Densidade.....	35
1.1.4. Decomposição de Schmidt.....	46
1.2. Medidas de Entrelaçamento Quântico.....	48
1.3. Entrelaçamento Multiparte	56
1.3.1. Medida de Entrelaçamento Livre para Estados Multipartes de Qubits.....	56
1.3.2. Entrelaçamento Residual.....	60
1.4. Conclusão	65
Capítulo 2 - Os Menores Principais de Matrizes Hermitianas e a Negatividade	66
2.1. Menores Principais de Matrizes Hermitianas.....	66
2.1.1. Teorema de Sylvester.....	66
2.1.2. Critério de Peres-Horodecki segundo o Teorema de Sylvester.....	68
2.1.3. A Negatividade como Função dos Menores Principais	69
2.2. Conclusão	71
Capítulo 3 - Entrelaçamento de Estados Quânticos Tripartes e Quadripartes Puros de Qubits	73
3.1. Entrelaçamento Residual de Estados Tripartes Puros de Qubits com Tangles	73
3.1.1. Exemplos.....	75
3.1.2. Estados da Classe <i>GHZ</i>	78
3.1.3. Estados da Classe <i>W</i>	79
3.2. Entrelaçamento Residual de Estados Tripartes Puros de Qubits com Negatividade.....	80
3.2.1. Exemplos.....	81
3.3. Menores Principais de Ordem 3 de $\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}}$	82
3.4. A Negatividade para Estados Tripartes Puros de Qubits.....	84
3.4.1. A Negatividade de ρ_{XYZ}	84
3.4.2. Exemplos.....	86
3.5. A Negatividade e os Menores Principais para Estados Quadripartes Puros de Qubits ...	88
3.5.1. A Negatividade de ρ_{WXYZ}	89
3.5.2. Exemplos.....	92

3.6. Conclusão	96
Capítulo 4 - Medida de Entrelaçamento para Estados Quânticos Puros de Seis Qubits	97
4.1. Medida de Entrelaçamento para Estados Puros de Seis Qubits.....	97
4.1.1. γ_6 é uma medida de entrelaçamento.....	100
4.1.2. Exemplos.....	109
4.2. Análise da Variação do Entrelaçamento.....	111
4.3. Conclusão	115
Capítulo 5 - Um Algoritmo para Achar o Mínimo de uma Função Realizando Apenas uma Medição	116
5.1. Introdução.....	116
5.2. Revisão de Amplificação de Amplitude.....	117
5.3. Algoritmo Quântico para Achar o Mínimo de uma Função.....	118
5.4. Algoritmo Quântico para Achar o Período de uma Função Usando a BQA.....	124
5.5. Conclusão	126
Capítulo 6 - Conclusões e Trabalhos Futuros	127

APÊNDICES

Apêndice 1 - Álgebra Linear.....	130
I.1. Números Complexos.....	130
I.2. Espaços de Hilbert de Dimensão Finita (sistemas quânticos).....	130
I.2.1. Produto Interno.....	131
I.2.2. Produto Externo	132
I.3. Medidas	133
I.4. Construção do Produto Tensorial.....	134
I.4.1. Produto Tensorial	134
I.4.2. Produto Tensorial entre Matrizes	135
I.5. Matrizes Unitárias	136
I.6. Decomposição Autovalor/Autovetor	139
Apêndice 2 - Fundamentos de Informação Quântica.....	141
II.1. Fundamentos Básicos: Bits Quânticos.....	141
II.2. Portas Quânticas	145
Apêndice 3 - Algoritmo de Grover e Transformada Quântica de Fourier.....	151
III.1. Algoritmo de Grover	151
III.2. Transformada Quântica de Fourier.....	152
III.2.1. Implementação Eficiente de U_{TQF}	153

ARTIGOS

Artigos	156
---------------	-----

REFERÊNCIAS

Referências Bibliográficas.....	157
---------------------------------	-----

LISTA DE FIGURAS

Figura 3.1. Entrelaçamento do estado (3.94), medido por π_4 versus θ	93
Figura 4.1. Entrelaçamento do estado (4.62), medido por γ_6 versus θ	111
Figura 4.2. Entrelaçamentos Bipartes \mathcal{N}_{AB}^2 e \mathcal{N}_{DE}^2 do estado (4.62) versus θ	112
Figura 4.3. Grafo correspondente ao estado grafo $ G_1\rangle$	113
Figura 4.4. Grafo correspondente ao estado grafo $ G_2\rangle$	113
Figura 4.5. Entrelaçamentos de $ G_1\rangle$ versus θ	114
Figura 4.6. Entrelaçamentos de $ G_2\rangle$ versus θ	114
Figura 5.1. Circuito quântico para busca assintótica	119
Figura 5.2. Circuito quântico para encontrar o período de uma função periódica, usando a BQA.....	125
Figura 7.1. Representação geométrica de um qubit.....	142
Figura 7.2. Esfera de Bloch do qubit $ \psi\rangle$	144
Figura 7.3. Circuito para a porta CNOT Quântica	149
Figura 7.4. Circuito para geração do estado de Bell.....	149
Figura 7.5. Circuito para Transformada Quântica de Fourier	154

LISTA DE TABELAS

Tabela 5.1. Comparação entre os algoritmos quânticos BQA, LM [62] e DH [59]..... 123

RESUMO

Esta tese apresenta alguns resultados sobre dois temas importantes para a teoria da informação quântica: entrelaçamento quântico e algoritmos quânticos. Com respeito ao entrelaçamento, é estabelecida uma relação entre a negatividade e os menores principais de matrizes Hermitianas, o que permite analisar o entrelaçamento para estados de dois qubits e estados puros de três e quatro qubits, usando os menores principais. Foi proposta também uma nova medida para o cálculo do entrelaçamento de estados puros de seis qubits, usando a negatividade. Para ambos os casos, o cálculo da variação do entrelaçamento de estados parametrizados foi realizado através de fórmulas analíticas e simulações numéricas. Por fim, com relação aos algoritmos quânticos é proposto um algoritmo de busca capaz de achar o mínimo de uma função realizando apenas uma medição ao final do algoritmo. O algoritmo é descrito e um exemplo de utilização do mesmo no cálculo do período de uma função periódica é apresentado.

ABSTRACT

This thesis presents some results about two important subjects of the quantum information theory: quantum entanglement and quantum algorithms. Regarding the entanglement, a relationship between negativity and minors principals of Hermitian matrices was stablished, allowing the analysis of the entanglement of two qubits states, three and four qubits pure states, using the minors principals. It was also proposed a new measure, using negativity, for calculating the entanglement of pure states of six qubits. Finally, with respect to quantum algorithms it was proposed a quantum search algorithm able to finding the minimum of a function by performing only one measurement. The algorithm is described and an example of its usage in the calculation of the period of a periodic function is presented.

INTRODUÇÃO

O entrelaçamento é uma propriedade da física quântica que desempenha um papel importante em informação quântica [1]. Reconhecido, inicialmente, por Einstein, Podolsky, Rosen e Schrödinger [3], o entrelaçamento pode ser utilizado na realização de protocolos de comunicação, como teleportação de estados quânticos e criptografia quântica, e em algoritmos de computação. A forma básica de entendê-lo é caracterizá-lo, classificá-lo e medi-lo. Esta tarefa não é simples, pois à medida que o número de bits quânticos aumenta, tipos diferentes de entrelaçamento podem surgir e não é claro que uma medida útil para um determinado tipo de entrelaçamento seja útil para outro. Quando os estados a serem considerados são mistos, o problema fica ainda mais difícil, surgindo assim a necessidade de criar técnicas para a solução do mesmo.

Genericamente falando, o entrelaçamento identifica uma correlação marcante entre alguma propriedade observável de estados quânticos que não está sujeita a limitações de distância, sendo por isso, considerado um conceito não local. Matematicamente, tais estados não podem ser completamente decompostos na soma de produtos tensoriais de suas partes.

Todo estado quântico é plenamente representado por uma matriz Hermitiana, positiva semi-definida e de traço igual a 1, chamada matriz densidade. Ela carrega toda a informação disponível no estado quântico. Portanto, do ponto de vista estritamente matemático, estudar o entrelaçamento significa estudar as propriedades da matriz densidade que sejam úteis para a classificação e quantificação do entrelaçamento. Nesta direção, este trabalho faz uma análise da utilização dos menores principais de matrizes Hermitianas, objetivando obter informações sobre o entrelaçamento de alguns estados quânticos. Dessa forma, alguns resultados importantes foram obtidos.

- i) Para estados quânticos de dois qubits, foi obtida uma expressão para o cálculo da negatividade, envolvendo as somas dos menores principais da transposta parcial da matriz densidade do estado quântico.
- ii) Para estados puros de três qubits, uma relação entre o quadrado da negatividade de 1 qubit com um par de qubits e a soma dos menores principais de ordem 3 da transposta parcial da matriz densidade foi obtida.

- iii) Já para estados puros de quatro qubits, obteve-se também, uma relação entre o quadrado da negatividade de 1 qubit com um terno de qubits e a soma dos menores principais de ordem 3 da transposta parcial da matriz densidade.
- iv) O resultado mais expressivo, proposto nesta tese, é uma medida para o cálculo do entrelaçamento em estados puros de seis qubits, o γ_6 , via negatividade.

Os itens i), ii) e iii) juntos permitem reescrever medidas de entrelaçamento baseadas em negatividade para estados de dois a cinco qubits, como medidas baseadas nos menores principais.

Por outro lado, com o uso de algoritmos quânticos é possível resolver alguns problemas de forma mais rápida do que as suas melhores contrapartidas clássicas. O algoritmo de Grover, por exemplo, é um resultado importante em informação quântica: ele prova que propriedades da informação quântica (superposições) podem melhorar a velocidade do problema de encontrar um valor específico em uma lista desordenada com N elementos, por exemplo. A busca quântica, pelo algoritmo de Grover, realiza $O(\sqrt{N})$ operações, em média, enquanto o melhor algoritmo clássico realiza $O(N)$ operações, indicando, assim, um ganho de velocidade quadrático [55]. Além disso, importantes problemas em Matemática podem ser modelados como uma busca, como por exemplo, o problema de calcular o mínimo ou o máximo de uma função. Neste sentido, esta tese também propõe um algoritmo quântico para achar o mínimo de uma função, realizando apenas uma medição.

Assim, o presente trabalho tem como objetivos:

- i) Fornecer algumas ferramentas que, adicionadas às já existentes, auxiliam no cálculo do entrelaçamento de alguns estados quânticos;
- ii) Apresentar uma nova medida de entrelaçamento para estados puros de 6 qubits;
- iii) Apresentar um algoritmo quântico para determinar o mínimo de uma função com apenas uma medição.

O mesmo está estruturado da seguinte forma: o Capítulo 1 trata da revisão de alguns critérios de separabilidade e medidas de entrelaçamento quântico. Os Capítulos seguintes já trazem alguns resultados que deram origem ao trabalho, de modo que no Capítulo 2, os menores principais de matrizes Hermitianas e a negatividade são apresentados. Já o Capítulo 3, trata do entrelaçamento de estados tripartes e quadripartes puros de qubits, usando os menores principais de matrizes Hermitianas. No Capítulo 4, uma medida de entrelaçamento para estados puros de seis qubits, via negatividade é apresentada. Finalmente, no Capítulo 5, é

apresentado um algoritmo quântico para achar o mínimo de uma função realizando apenas uma medição.

CAPÍTULO 1

CRITÉRIOS DE SEPARABILIDADE E MEDIDAS DE ENTRELÇAMENTO QUÂNTICO

Resumo

Neste capítulo, inicialmente são dadas algumas definições e generalidades sobre estados quânticos. Em seguida são revistos alguns critérios de separabilidade para estados quânticos bipartes e a decomposição de Schmidt. Com o objetivo de esclarecer brevemente a discussão sobre entrelaçamento, algumas medidas de entrelaçamento são revistas. Por fim, alguns aspectos do entrelaçamento em sistemas quânticos multipartes também são apresentados.

1.1. Separabilidade

Dado um espaço de Hilbert \mathcal{H} (ver Apêndice 1), o estado de um sistema quântico é identificado, matematicamente, por um operador linear $\rho: \mathcal{H} \rightarrow \mathcal{H}$, que é Hermitiano, positivo e cujo traço é unitário. Isto é, ρ descreve um *estado quântico*, se

$$\rho^\dagger = \rho, \rho \geq 0, \text{Tr}(\rho) = 1. \quad (1.1)$$

O operador ρ , satisfazendo as condições acima, será chamado de *operador densidade* ou *matriz densidade* do estado quântico ρ . Além disso, ρ pode ser descrito como

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad (1.2)$$

em que $p_i > 0$ e $\sum_i p_i = 1$. Os estados ρ da forma (1.2) são chamados *estados mistos*.

Quando $p_i = 1$, para algum i , tem-se

$$\rho = |\psi_i\rangle\langle\psi_i|, \quad (1.3)$$

que é a matriz densidade do *estado puro* $|\psi_i\rangle$ (representado pelo próprio vetor de estado no espaço de Hilbert associado).

Foi visto acima, que a um sistema quântico pode ser associado um espaço de Hilbert, que é o espaço de estados do sistema. Para estados compostos, o espaço de estados é formado pelo produto tensorial dos espaços de estados dos sistemas individuais. Assim, o espaço de Hilbert associado a um sistema quântico \mathcal{S} composto pelos subsistemas $\mathcal{S}_1, \mathcal{S}_2, \dots, \mathcal{S}_n$, pode ser escrito como $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$, sendo \mathcal{H}_i o espaço de Hilbert associado ao subsistema \mathcal{S}_i , $i = 1, 2, \dots, n$.

Com base no que foi exposto acima, um estado puro $|\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$, é *totalmente separável*, se

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle, \quad (1.4)$$

em que $|\psi_i\rangle \in \mathcal{H}_i$ é o estado puro do subsistema \mathcal{S}_i , com $i = 1, 2, \dots, n$. Caso contrário, o estado é dito *entrelaçado* (não, totalmente entrelaçado; o estado $|\psi\rangle$ possui algum entrelaçamento).

Já para um estado misto $\rho \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$, diz-se que ρ é *totalmente separável*, se

$$\rho = \sum_i p_i |\psi_1^i\rangle\langle\psi_1^i| \otimes |\psi_2^i\rangle\langle\psi_2^i| \otimes \dots \otimes |\psi_n^i\rangle\langle\psi_n^i|. \quad (1.5)$$

Os estados entrelaçados, por sua vez, não podem ser escritos na forma (1.5), acima, por isso diz-se que os seus subsistemas são correlacionados.

Os estados separáveis bipartes, compostos pelos subsistemas \mathcal{S}_A e \mathcal{S}_B , por exemplo, podem ser construídos através de *operações locais (LO)* em \mathcal{S}_A e \mathcal{S}_B e comunicação clássica (*CC*) entre as partes. Surge assim, uma noção de fundamental importância no estudo do

entrelaçamento: as *operações locais e comunicação clássica* - LOCC. Assim, estados compostos da forma $\rho = \sum_{i=1}^{r \neq 1} p_i \rho_A^i \otimes \rho_B^i$, $p_i > 0$ e $\sum_i p_i = 1$, são estados que podem ser construídos por LOCC. Enquanto os estados separáveis podem ser construídos através de LOCC, o mesmo não acontece com os estados entrelaçados, pois estes contêm correlações não clássicas, as quais são chamadas correlações quânticas. Como será visto a seguir, os estados entrelaçados tem um comportamento diferente dos estados separáveis com relação a medições feitas em seus subsistemas, ou seja, os estados entrelaçados se comportam como o estado $|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, para medições feitas em seus qubits. De fato, uma medição feita no primeiro qubit de $|\varphi\rangle$ fornece $|0\rangle$ com probabilidade $\frac{1}{2}$, e $|1\rangle$, com probabilidade $\frac{1}{2}$, deixando $|\varphi\rangle$ nos estados $|\varphi'\rangle = |00\rangle$ e $|\varphi'\rangle = |11\rangle$, respectivamente. Medindo-se o segundo qubit dos estados resultantes, obtém-se com probabilidade 1, os resultados $|0\rangle$ e $|1\rangle$, respectivamente, isto é, os resultados são correlacionados.

Como visto no parágrafo acima, o entrelaçamento é uma correlação não local (aspecto físico) entre as partes individuais de um sistema quântico composto. Assim, o completo entendimento da variação do entrelaçamento quando do processamento de um estado quântico composto, seja em um computador quântico ou na propagação em um canal de comunicação, é imprescindível.

O primeiro passo para entender o comportamento do entrelaçamento é identificar quando um estado quântico composto possui entrelaçamento ou não, isto é, determinar regras (critérios) para saber se esse estado quântico é ou não entrelaçado. Feito esse estudo, surge a necessidade de quantificar o entrelaçamento, isto é, determinar o quão entrelaçado tal estado quântico é. Os estados quânticos compostos mais simples, onde há possibilidade de algum entrelaçamento ser detectado, são os estados quânticos de sistemas de dois qubits. São exatamente nesses estados onde foram concentrados os primeiros esforços na tentativa de quantificar o entrelaçamento. Por isso, a maior parte dos critérios e medidas de entrelaçamento existentes se refere a estados de sistemas de dois qubits. Como consequência dessa investigação surgiram alguns critérios e medidas de entrelaçamento para estados bipartites de dimensões arbitrárias.

Basicamente, um estado quântico puro de dois qubits, ρ , é *desentrelaçado* ou *separável*, se e somente se,

$$\rho = \rho_A \otimes \rho_B, \quad (1.6)$$

em que $\rho_A = Tr_B(\rho)$ ($\rho_B = Tr_A(\rho)$) é o traço parcial da matriz ρ em relação ao subsistema A (B). Enquanto que, um estado misto, ρ , é *desentrelaçado* ou *separável*, se

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i, \quad (1.7)$$

onde $p_i > 0$ e ρ_A^i e ρ_B^i são matrizes densidade dos subsistemas A e B , respectivamente.

Ainda, em relação a um estado puro de dois qubits, uma *condição de separabilidade* pode ser obtida. Considere o estado $|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$, com $\alpha_i \in \mathbb{C}$ e $\sum_{i=0}^3 |\alpha_i|^2 = 1$. Então, $|\psi\rangle$ é separável, se e somente se, $|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$, com $|a|^2 + |b|^2 = 1$, $|c|^2 + |d|^2 = 1$ e $a, b, c, d \in \mathbb{C}$, ou seja,

$$|\psi\rangle \text{ é separável} \Leftrightarrow \alpha_0\alpha_3 = \alpha_1\alpha_2. \quad (1.8)$$

A seguir será feito uma revisão sobre alguns critérios de separabilidade existentes na literatura.

1.1.1. Critério de Separação de Peres-Horodecki

Um critério de separação para estados em sistemas $\mathbb{C}^2 \otimes \mathbb{C}^2$ (dois qubits) e $\mathbb{C}^2 \otimes \mathbb{C}^3$ (um qubit e um qutrit) foi proposto por Peres [2] e Horodecki [3]. Peres provou uma condição necessária para a separabilidade de estados em sistemas $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$ (este critério é conhecido como condição necessária de Peres) baseada na positividade da transposta parcial da matriz densidade do estado.

A seguir será apresentada a definição de transposta parcial da matriz densidade de um estado quântico, antes de rever o critério de Peres.

Seja ρ a matriz densidade de um estado em um sistema quântico composto de dois subsistemas, A e B , com matrizes densidade dadas por $\rho_A = Tr_B(\rho)$ e $\rho_B = Tr_A(\rho)$, respectivamente. Sendo $\{|m\rangle\}$ e $\{|\mu\rangle\}$ bases ortonormais arbitrárias para A e B , nos espaços de Hilbert $\mathcal{H}_A = \mathbb{C}^M$ e $\mathcal{H}_B = \mathbb{C}^N$, respectivamente, tem-se que $\{|m\rangle \otimes |\mu\rangle\}$ é uma base ortonormal para o espaço $\mathcal{H} = \mathbb{C}^M \otimes \mathbb{C}^N$ (ver Apêndice 1). Assim, ρ pode ser escrito da seguinte forma

$$\rho = \sum_{m,\mu,n,\nu} |m\mu\rangle \langle m\mu | \rho | n\nu \rangle \langle n\nu|, \quad (1.9)$$

ou ainda,

$$\rho = \sum_{m,\mu,n,\nu} \langle m\mu | \rho | n\nu \rangle |m\mu\rangle \langle n\nu|. \quad (1.10)$$

Como $|m\mu\rangle \langle n\nu| = |m\rangle \langle n| \otimes |\mu\rangle \langle \nu|$, tem-se

$$\rho = \sum_{m,\mu,n,\nu} \langle m\mu | \rho | n\nu \rangle |m\rangle \langle n| \otimes |\mu\rangle \langle \nu|. \quad (1.11)$$

Na base $\{|m\rangle \otimes |\mu\rangle\}$, os elementos da matriz densidade ρ , são da forma

$$\rho_{m\mu,n\nu} = \langle m\mu | \rho | n\nu \rangle. \quad (1.12)$$

Segue, então, que a transposta parcial de ρ em relação ao subsistema A , indicada por ρ^{T_A} , é definida da seguinte maneira

$$\rho^{T_A} = \sum_{m,\mu,n,\nu} \langle n\mu | \rho | m\nu \rangle (|m\rangle \langle n|)^T \otimes |\mu\rangle \langle \nu|, \quad (1.13)$$

ou seja,

$$\rho^{T_A} = \sum_{m,\mu,n,\nu} \langle n\mu | \rho | m\nu \rangle |n\mu\rangle \langle m\nu|. \quad (1.14)$$

Assim, usando (1.14), os elementos da transposta parcial de ρ em relação ao subsistema A , são dados por

$$\rho_{m\mu,n\nu}^{T_A} = \rho_{n\mu,m\nu}, \quad (1.15)$$

isto é,

$$\rho_{m\mu,n\nu}^{T_A} = \langle n\mu | \rho | m\nu \rangle. \quad (1.16)$$

Em relação ao subsistema B , a transposta parcial ρ^{T_B} , é definida assim

$$\rho^{T_B} = \sum_{m,\mu,n,\nu} \langle m\nu | \rho | n\mu \rangle |m\rangle \langle n| \otimes (|\mu\rangle \langle \nu|)^T, \quad (1.17)$$

ou seja,

$$\rho^{T_B} = \sum_{m,\mu,n,\nu} \langle m\nu | \rho | n\mu \rangle |m\nu\rangle \langle n\mu|. \quad (1.18)$$

Logo, os elementos da transposta parcial de ρ em relação ao subsistema B , são dados por

$$\rho_{m\mu,n\nu}^{T_B} = \rho_{m\nu,n\mu}. \quad (1.19)$$

Para sistemas $\mathbb{C}^2 \otimes \mathbb{C}^2$, a matriz densidade do estado ρ , 4×4 , escrita na base computacional $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, é dada por

$$\rho = \begin{pmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{00,10} & \rho_{00,11} \\ \rho_{01,00} & \rho_{01,01} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{10,10} & \rho_{10,11} \\ \rho_{11,00} & \rho_{11,01} & \rho_{11,10} & \rho_{11,11} \end{pmatrix}. \quad (1.20)$$

Usando (1.12), a matriz ρ , em (1.20), pode ser reescrita como

$$\rho = \begin{pmatrix} \langle 00|\rho|00\rangle & \langle 00|\rho|01\rangle & \langle 00|\rho|10\rangle & \langle 00|\rho|11\rangle \\ \langle 01|\rho|00\rangle & \langle 01|\rho|01\rangle & \langle 01|\rho|10\rangle & \langle 01|\rho|11\rangle \\ \langle 10|\rho|00\rangle & \langle 10|\rho|01\rangle & \langle 10|\rho|10\rangle & \langle 10|\rho|11\rangle \\ \langle 11|\rho|00\rangle & \langle 11|\rho|01\rangle & \langle 11|\rho|10\rangle & \langle 11|\rho|11\rangle \end{pmatrix}. \quad (1.21)$$

Assim, de (1.15) segue que

$$\rho^{T_A} = \begin{pmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{10,00} & \rho_{10,01} \\ \rho_{01,00} & \rho_{01,01} & \rho_{11,00} & \rho_{11,01} \\ \rho_{00,10} & \rho_{00,11} & \rho_{10,10} & \rho_{10,11} \\ \rho_{01,10} & \rho_{01,11} & \rho_{11,10} & \rho_{11,11} \end{pmatrix}, \quad (1.22)$$

ou seja,

$$\rho^{T_A} = \begin{pmatrix} \langle 00|\rho|00\rangle & \langle 00|\rho|01\rangle & \langle 10|\rho|00\rangle & \langle 10|\rho|01\rangle \\ \langle 01|\rho|00\rangle & \langle 01|\rho|01\rangle & \langle 11|\rho|00\rangle & \langle 11|\rho|01\rangle \\ \langle 00|\rho|10\rangle & \langle 00|\rho|11\rangle & \langle 10|\rho|10\rangle & \langle 10|\rho|11\rangle \\ \langle 01|\rho|10\rangle & \langle 01|\rho|11\rangle & \langle 11|\rho|10\rangle & \langle 11|\rho|11\rangle \end{pmatrix}. \quad (1.23)$$

Para tornar mais claro o que foi exposto acima, considere a matriz densidade ρ formada por blocos. Para um sistema $M \times N$, já foi visto que os elementos de ρ são dados por $\rho_{m\mu,n\nu} = \langle m\mu|\rho|n\nu\rangle$, onde $\{|m\rangle\}$ e $\{|\mu\rangle\}$ são bases ortonormais para os espaços de Hilbert $\mathcal{H}_A = \mathbb{C}^M$ e $\mathcal{H}_B = \mathbb{C}^N$, respectivamente. Seja, então, a matriz do estado ρ atuando em $\mathbb{C}^M \otimes \mathbb{C}^N$, dada por

$$\rho = \begin{pmatrix} A_{11} & \cdots & A_{1M} \\ \vdots & \ddots & \vdots \\ A_{M1} & \cdots & A_{MM} \end{pmatrix}, \quad (1.24)$$

onde as matrizes A_{mn} , de ordem $N \times N$, atuam em \mathbb{C}^N . Os elementos da matriz ρ , em (1.24), são dados por

$$\{A_{mn}\}_{\mu\nu} = \rho_{m\mu, n\nu}, \quad (1.25)$$

onde $1 \leq m, n \leq M$ e $1 \leq \mu, \nu \leq N$. Dessa forma, os elementos da transposta parcial ρ^{T_B} , são definidos por

$$\{A_{mn}\}_{\mu\nu} = \rho_{m\nu, n\mu}. \quad (1.26)$$

Isto significa que ρ^{T_B} pode ser obtida de ρ , transpondo-se cada uma das matrizes A_{mn} , mantendo-se a posição que cada uma ocupa na matriz ρ , em (1.24), o que é equivalente a permutar os índices do segundo subsistema. Isto é,

$$\rho^{T_B} = \begin{pmatrix} A_{11}^T & \cdots & A_{1M}^T \\ \vdots & \ddots & \vdots \\ A_{M1}^T & \cdots & A_{MM}^T \end{pmatrix}. \quad (1.27)$$

Quando a transposta parcial é calculada em relação ao primeiro subsistema, ρ^{T_A} , os seus elementos são dados por

$$\{A_{mn}\}_{\mu\nu} = \rho_{n\mu, m\nu}. \quad (1.28)$$

Neste caso,

$$\rho^{T_A} = \begin{pmatrix} A_{11} & \cdots & A_{M1} \\ \vdots & \ddots & \vdots \\ A_{1M} & \cdots & A_{MM} \end{pmatrix}. \quad (1.29)$$

Isso significa que ρ^{T_A} pode ser obtida de ρ , permutando-se os índices do primeiro subsistema.

Considere, por exemplo, um estado em $\mathbb{C}^2 \otimes \mathbb{C}^2$, com matriz densidade ρ , definida em (1.20),

$$\rho = \begin{pmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{00,10} & \rho_{00,11} \\ \rho_{01,00} & \rho_{01,01} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{10,10} & \rho_{10,11} \\ \rho_{11,00} & \rho_{11,01} & \rho_{11,10} & \rho_{11,11} \end{pmatrix} = \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix}, \quad (1.30)$$

sendo

$$A_{00} = \begin{pmatrix} \rho_{00,00} & \rho_{00,01} \\ \rho_{01,00} & \rho_{01,01} \end{pmatrix}, \quad A_{01} = \begin{pmatrix} \rho_{00,10} & \rho_{00,11} \\ \rho_{01,10} & \rho_{01,11} \end{pmatrix}, \quad A_{10} = \begin{pmatrix} \rho_{10,00} & \rho_{10,01} \\ \rho_{11,00} & \rho_{11,01} \end{pmatrix} \text{ e } A_{11} = \begin{pmatrix} \rho_{10,10} & \rho_{10,11} \\ \rho_{11,10} & \rho_{11,11} \end{pmatrix}.$$

Assim,

$$\rho^{T_B} = \begin{pmatrix} \rho_{00,00} & \rho_{01,00} & \rho_{00,10} & \rho_{01,10} \\ \rho_{00,01} & \rho_{01,01} & \rho_{00,11} & \rho_{01,11} \\ \rho_{10,00} & \rho_{11,00} & \rho_{10,10} & \rho_{11,10} \\ \rho_{10,01} & \rho_{11,01} & \rho_{10,11} & \rho_{11,11} \end{pmatrix} = \begin{pmatrix} A_{00}^T & A_{01}^T \\ A_{10}^T & A_{11}^T \end{pmatrix}, \quad (1.31)$$

$$\rho^{T_A} = \begin{pmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{10,00} & \rho_{10,01} \\ \rho_{01,00} & \rho_{01,01} & \rho_{11,00} & \rho_{11,01} \\ \rho_{00,10} & \rho_{00,11} & \rho_{10,10} & \rho_{10,11} \\ \rho_{01,10} & \rho_{01,11} & \rho_{11,10} & \rho_{11,11} \end{pmatrix} = \begin{pmatrix} A_{00} & A_{10} \\ A_{01} & A_{11} \end{pmatrix}. \quad (1.32)$$

Agora, o critério de Peres:

“Se ρ é um estado separável em $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$, então a transposta parcial da matriz densidade, ρ^{T_A} , não tem autovalores negativos; caso contrário, o estado é entrelaçado.”

Suponha que ρ é separável, ou seja, $\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i$. Por (1.12), tem-se que $\rho_{m\mu,n\nu} = \langle m \otimes \mu | \sum_i p_i \rho_A^i \otimes \rho_B^i | n \otimes \nu \rangle$, ou seja, $\rho_{m\mu,n\nu} = \sum_i p_i \langle m | \rho_A^i | n \rangle \langle \mu | \rho_B^i | \nu \rangle$. Portanto, os elementos da matriz ρ podem ser escritos como

$$\rho_{m\mu,n\nu} = \sum_i p_i (\rho_A^i)_{mn} (\rho_B^i)_{\mu\nu}, \quad (1.33)$$

onde $(\rho_A^i)_{mn} = \langle m | \rho_A^i | n \rangle$ e $(\rho_B^i)_{\mu\nu} = \langle \mu | \rho_B^i | \nu \rangle$. Neste caso, usando a Eq. (1.15), ρ^{T_A} pode ser escrita assim

$$\rho^{T_A} = \sum_i p_i (\rho_A^i)^T \otimes \rho_B^i. \quad (1.34)$$

Como ρ_A^i é uma matriz densidade, tem-se $(\rho_A^i)^\dagger = \rho_A^i$, $\rho_A^i \geq 0$ e $Tr(\rho_A^i) = 1$. Daí, $(\rho_A^i)^T \geq 0$, $Tr(\rho_A^i)^T = 1$ (as diagonais de ρ_A^i e $(\rho_A^i)^T$ são iguais) e $((\rho_A^i)^T)^\dagger = (\rho_A^i)^T$, ou seja, $(\rho_A^i)^T$ é uma matriz densidade. Portanto, ρ^{T_A} é também uma matriz densidade de um estado quântico e, como tal, não pode ter autovalores negativos.

Observe-se, ainda, que os autovalores de ρ^{T_A} e ρ são invariantes mediante transformações unitárias locais feitas em ρ . De fato, as operações unitárias U_A e U_B , aplicadas aos estados dos subsistemas A e B , respectivamente, transformam o estado ρ no estado

$$\rho' = (U_A \otimes U_B) \rho (U_A \otimes U_B)^\dagger. \quad (1.35)$$

Como, $\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i$, tem-se

$$\rho' = (U_A \otimes U_B) \left(\sum_i p_i \rho_A^i \otimes \rho_B^i \right) (U_A \otimes U_B)^\dagger, \quad (1.36)$$

ou seja,

$$\rho' = \sum_i p_i U_A \rho_A^i (U_A)^\dagger \otimes U_B \rho_B^i (U_B)^\dagger. \quad (1.37)$$

Segue-se daí, que

$$(\rho')^{T_A} = \sum_i p_i \left(U_A \rho_A^i (U_A)^\dagger \right)^T \otimes U_B \rho_B^i (U_B)^\dagger, \quad (1.38)$$

ou seja,

$$(\rho')^{T_A} = \sum_i p_i \left((U_A)^\dagger \right)^T (\rho_A^i)^T (U_A)^T \otimes U_B \rho_B^i (U_B)^\dagger. \quad (1.39)$$

Como $U^\dagger = (U^T)^*$, tem-se:

$$(\rho')^{T_A} = \sum_i p_i (U_A)^* (\rho_A^i)^T \left((U_A)^* \right)^\dagger \otimes U_B \rho_B^i (U_B)^\dagger, \quad (1.40)$$

ou ainda,

$$(\rho')^{T_A} = \left((U_A)^* \otimes \left((U_A)^* \right)^\dagger \right) \sum_i p_i (\rho_A^i)^T \otimes \rho_B^i (U_B \otimes (U_B)^\dagger). \quad (1.41)$$

Fazendo $U^* = \bar{U}$, tem-se:

$$(\rho')^{T_A} = (\bar{U}_A \otimes U_B) \rho^{T_A} (\bar{U}_A \otimes U_B)^\dagger. \quad (1.42)$$

Mostrou-se acima que se ρ sofre uma transformação unitária local, então ρ^{T_A} também sofrerá. Note que ρ foi afetado pelas transformações U_A e U_B , enquanto ρ^{T_A} foi afetado pelas transformações $\bar{U}_A = U_A^*$ (unitária) e U_B e, portanto, os autovalores de ρ^{T_A} são invariantes mediante transformações unitárias locais. Assim, é possível aplicar o critério da transposta parcial em qualquer representação da matriz densidade ρ , não importa a base em que ρ está escrita, pois, embora, a matriz ρ^{T_A} dependa das bases usadas, seus autovalores, não.

Como foi visto, Peres fornece apenas uma condição necessária para a separabilidade de estados em sistemas $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$. A seguir, será visto como os Horodecki, usando a teoria de mapas positivos, forneceram também uma condição de separabilidade para estados em sistemas $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$, mostrando que a transposta parcial é uma condição necessária e suficiente para a separabilidade. Para outras dimensões, o uso da transposta parcial é apenas uma condição necessária.

1.1.2. Critério de Horodecki

Peres conjecturou que a condição necessária fornecida acima seria também suficiente. Mas coube aos Horodecki, usando a teoria de mapas positivos, mostrarem em que condição, o que Peres conjecturou era válido. Com isso, os Horodecki estabeleceram um critério de separação para estados em sistemas $\mathbb{C}^M \otimes \mathbb{C}^N$, via mapas positivos. Foi então que, usando a positividade da transposta parcial, que é um mapa positivo, mostraram que o critério (condição necessária e suficiente) vale apenas para estados em sistemas $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$. Para os sistemas $\mathbb{C}^M \otimes \mathbb{C}^N$, $M > 2$ e $N \geq 3$, eles mostraram que a positividade da transposta parcial é apenas uma condição necessária.

Como o critério de Horodecki é baseado em mapas positivos, algumas definições de tais mapas são necessárias. Seja \mathcal{A}_i o conjunto dos operadores lineares atuando no espaço de Hilbert \mathcal{H}_i , $i=1,2$. \mathcal{A}_i é um espaço de Hilbert (espaço de Hilbert-Schmidt) com produto escalar definido por $\langle A, B \rangle = \text{Tr}(B^\dagger A)$. Denotando por $\mathcal{L}(\mathcal{A}_1, \mathcal{A}_2)$ o espaço dos mapas lineares de \mathcal{A}_1 em \mathcal{A}_2 , diz-se que um mapa $\Lambda \in \mathcal{L}(\mathcal{A}_1, \mathcal{A}_2)$ é *positivo* se $\Lambda(\rho) \geq 0$, para todo $\rho \geq 0$ em \mathcal{A}_1 . Um mapa $\Lambda \in \mathcal{L}(\mathcal{A}_1, \mathcal{A}_2)$ é completamente positivo se a aplicação $\Lambda \otimes I_n$ de

$\mathcal{A}_1 \otimes \mathcal{M}_n$ em $\mathcal{A}_1 \otimes \mathcal{M}_n$ é positiva para todo $n \in \mathbb{N}$, em que \mathcal{M}_n representa o conjunto das matrizes complexas $n \times n$ e I_n o mapa identidade. O produto tensorial de um mapa completamente positivo pelo mapa identidade é um mapa positivo, isto é, $\rho \geq 0 \Rightarrow (\Lambda \otimes I_n)(\rho) \geq 0$, para todo $n \in \mathbb{N}$ e Λ um mapa positivo. Existem mapas positivos que não possuem essa propriedade, ou seja, não é verdade que os mapas positivos preservam a positividade de um operador: $(\Lambda \otimes I)(\rho) \not\geq 0$, quando $\rho \geq 0$. Este fato é importante para o problema da inseparabilidade quântica, pois, para estados produtos, o produto tensorial de um mapa positivo pelo mapa identidade é também um mapa positivo, ou seja, se $\rho \geq 0$, então $(\Lambda \otimes I_n)(\rho \otimes \tilde{\rho}) = \Lambda(\rho) \otimes \tilde{\rho} \geq 0$. E, pelo teorema seguinte, isto vale para estados separáveis.

A. Teorema (Horodecki)

“Seja ρ um operador densidade que atua no espaço de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Então, ρ é separável, se e somente se, para qualquer mapa positivo $\Lambda: \mathcal{A}_1 \rightarrow \mathcal{A}_2$, o operador $I \otimes \Lambda(\rho)$ é positivo.”

E assim, quando ρ não é separável, tem-se que $(\Lambda \otimes I)(\rho) \not\geq 0$, onde Λ é um mapa positivo. Assim, os estados inseparáveis podem ser reconhecidos através dos mapas positivos. Existem mapas positivos que não podem ser usados para verificar a inseparabilidade. Quais são, então, os mapas positivos que podem ser usados para a caracterização de um estado inseparável? Os Horodecki já sabiam que para os sistemas $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$, apenas a transposta parcial era o tal mapa. É o que mostra o próximo teorema.

B. Teorema (Critério de Horodecki)

“Um estado ρ atuando em $\mathbb{C}^2 \otimes \mathbb{C}^2$ ou $\mathbb{C}^2 \otimes \mathbb{C}^3$ é separável, se e somente se, sua transposta parcial é um operador positivo.”

A transposta parcial ρ^{T_B} , é dada por $\rho^{T_B} = (I \otimes T)\rho$, em que T é o mapa transposição [5]. Assim, sempre que $\rho^{T_B} \not\geq 0$, o estado ρ é entrelaçado, sendo que $\rho^{T_B} \geq 0$

não garante a separabilidade. Apenas nos casos $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$, $\rho^{T_B} \geq 0$ é condição necessária e suficiente para a separabilidade.

Aqui, é importante observar [4] que qualquer mapa positivo $\Lambda: \mathcal{A}_1 \rightarrow \mathcal{A}_2$, com ρ atuando em $\mathbb{C}^2 \otimes \mathbb{C}^2$ ou $\mathbb{C}^2 \otimes \mathbb{C}^3$, é da forma

$$\Lambda = \Lambda_1^{CP} + \Lambda_2^{CP} \mathcal{T}, \quad (1.43)$$

onde Λ_i^{CP} é um mapa completamente positivo e \mathcal{T} é o mapa transposição.

Agora, com o objetivo de entender o critério que foi estabelecido acima, alguns exemplos serão considerados.

A. Inicialmente, considere o estado [3],

$$\rho = p |\psi_1\rangle\langle\psi_1| + (1-p) |\psi_2\rangle\langle\psi_2|, \quad (1.44)$$

em que $0 \leq p \leq 1$, $|\psi_1\rangle = a|00\rangle + b|11\rangle$ e $|\psi_2\rangle = a|01\rangle + b|10\rangle$, com $a, b > 0$ e $a^2 + b^2 = 1$. As representações matriciais de ρ e ρ^{T_B} são dadas, respectivamente, por

$$\rho = \begin{pmatrix} pa^2 & 0 & 0 & pab \\ 0 & (1-p)a^2 & (1-p)ab & 0 \\ 0 & (1-p)ab & (1-p)b^2 & 0 \\ pab & 0 & 0 & pb^2 \end{pmatrix}, \quad (1.45)$$

$$\rho^{T_B} = \begin{pmatrix} pa^2 & 0 & 0 & (1-p)ab \\ 0 & (1-p)a^2 & pab & 0 \\ 0 & pab & (1-p)b^2 & 0 \\ (1-p)ab & 0 & 0 & pb^2 \end{pmatrix}. \quad (1.46)$$

E, assim, $P(\lambda) = \lambda^4 - \lambda^3 + p(1-p)\lambda^2 + (1-2p)^2 a^2 b^2 \lambda - (1-2p)^2 a^4 b^4$ é o polinômio característico de ρ^{T_B} , e seus autovalores são $\lambda_{1,2} = \frac{(1-p) \pm \sqrt{(1-p)^2 - 4(1-2p)a^2 b^2}}{2}$ e

$\lambda_{3,4} = \frac{p \pm \sqrt{p^2 + 4(1-2p)a^2 b^2}}{2}$. Observe, agora, as seguintes situações:

$$(i) \quad ab \neq 0, p > \frac{1}{2} \Rightarrow \lambda_1 > 0, \lambda_2 < 0$$

$$(ii) \quad ab \neq 0, p < \frac{1}{2} \Rightarrow \lambda_3 > 0, \lambda_4 < 0$$

Portanto, para $ab \neq 0$ e $p \neq \frac{1}{2}$, ρ é inseparável. E, finalmente, para $p = \frac{1}{2}$, tem-se $\rho^{T_B} = \rho \geq 0$ e, pelo Teorema B, Seção 1.1.2, ρ é separável.

B. Considere, agora, o estado de Peres-Horodecki [3],

$$\rho = p|\psi_-\rangle\langle\psi_-| + (1-p)|00\rangle\langle 00|, \quad (1.47)$$

com $0 \leq p \leq 1$ e $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Assim, as representações da matriz densidade do estado e de sua transposta parcial são dadas, respectivamente, por

$$\rho = \begin{pmatrix} 1-p & 0 & 0 & 0 \\ 0 & p/2 & -p/2 & 0 \\ 0 & -p/2 & p/2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (1.48)$$

$$\rho^{T_B} = \begin{pmatrix} 1-p & 0 & 0 & -p/2 \\ 0 & p/2 & 0 & 0 \\ 0 & 0 & p/2 & 0 \\ -p/2 & 0 & 0 & 0 \end{pmatrix}. \quad (1.49)$$

Portanto, os autovalores de ρ^{T_B} são $\lambda_{1,2} = \frac{p}{2} > 0$, $\lambda_3 = \frac{(1-p) + \sqrt{(1-p)^2 + p^2}}{2} > 0$ e $\lambda_4 = \frac{(1-p) - \sqrt{(1-p)^2 + p^2}}{2} < 0$, pois, $1-p < \sqrt{(1-p)^2 + p^2}$, $\forall p$, $0 < p \leq 1$. Assim, ρ é entrelaçado. E, se $p=0$, ρ é separável.

C. Considere o estado de Werner [2],

$$\rho = p|\psi_{-}\rangle\langle\psi_{-}| + (1-p)\frac{I}{4}, \quad (1.50)$$

em que, $|\psi_{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ e I é a matriz identidade de elementos $\delta_{mn}\delta_{\mu\nu}$. Assim, ρ e ρ^{T_A} são dadas, respectivamente, por

$$\rho = \begin{pmatrix} \frac{1-p}{4} & 0 & 0 & 0 \\ 0 & \frac{1+p}{4} & -\frac{p}{2} & 0 \\ 0 & -\frac{p}{2} & \frac{1+p}{4} & 0 \\ 0 & 0 & 0 & \frac{1-p}{4} \end{pmatrix}, \quad (1.51)$$

$$\rho^{T_A} = \begin{pmatrix} \frac{1-p}{4} & 0 & 0 & -\frac{p}{2} \\ 0 & \frac{1+p}{4} & 0 & 0 \\ 0 & 0 & \frac{1+p}{4} & 0 \\ -\frac{p}{2} & 0 & 0 & \frac{1-p}{4} \end{pmatrix}. \quad (1.52)$$

Os autovalores de ρ^{T_A} são $\lambda_{1,2,3} = \frac{1+p}{4} > 0$ e $\lambda_4 = \frac{1-3p}{4}$. Se $0 \leq p \leq \frac{1}{3}$, então todos os autovalores de ρ^{T_A} são não negativos, e assim, pelo critério de Horodecki, ρ é separável. E, se $\frac{1}{3} < p \leq 1$, então $\frac{1-3p}{4} < 0$, ou seja, ρ é entrelaçado.

D. Por fim, considere o estado de Gisin [2],

$$\rho = p|\psi\rangle\langle\psi| + (1-p)\left(\frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2}\right), \quad (1.53)$$

onde $0 \leq p \leq 1$ e $|\psi\rangle = a|01\rangle + b|10\rangle$, com $a, b \in \mathbb{R}$ e $a^2 + b^2 = 1$. Assim, as representações matriciais de ρ e ρ^{T_A} são dadas, respectivamente, por

$$\rho = \begin{pmatrix} \frac{1-p}{2} & 0 & 0 & 0 \\ 0 & pa^2 & pab & 0 \\ 0 & pab & pb^2 & 0 \\ 0 & 0 & 0 & \frac{1-p}{2} \end{pmatrix}, \quad (1.54)$$

$$\rho^{T_A} = \begin{pmatrix} \frac{1-p}{2} & 0 & 0 & pab \\ 0 & pa^2 & 0 & 0 \\ 0 & 0 & pb^2 & 0 \\ pab & 0 & 0 & \frac{1-p}{2} \end{pmatrix}. \quad (1.55)$$

Os autovalores de ρ^{T_A} são $\lambda_1 = pa^2$, $\lambda_2 = pb^2$, $\lambda_3 = \frac{1-(1+2|ab|)p}{2}$ e $\lambda_4 = \frac{1-(1-2|ab|)p}{2}$.

Assim, para $p > (1+2|ab|)^{-1}$, tem-se $\rho^{T_A} \not\geq 0$, ou seja, um dos autovalores é negativo e, portanto, ρ é entrelaçado. Se $p=1$, então ρ é entrelaçado se $ab < 0$, e separável se $ab \geq 0$. E, se $p=0$, então ρ é separável.

O critério de Peres-Horodecki usa a transposta parcial da matriz densidade para dizer se um estado nos sistemas $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$ é ou não entrelaçado. Entretanto, para sistemas de dimensões diferentes, a condição da transposta parcial da matriz densidade é apenas necessária. No entanto, é possível obter estados inseparáveis com transposta parcial positiva. É o que estabelece o critério que será estudado na próxima subseção.

1.1.3. Critério de Separação Baseado na Imagem do Operador Densidade

Outro critério de separação, agora baseado na análise da imagem do operador densidade do estado, através da decomposição de estados separáveis em produto tensorial de estados puros, é apresentado. Em seguida serão mostrados exemplos de estados inseparáveis com transposta parcial positiva, construídos a partir desse critério. Antes de enunciá-lo, algumas definições e teoremas serão apresentados.

Seja ρ um estado separável em um espaço de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, $\dim \mathcal{H} = m < \infty$ e $\mathcal{I} = \{(i, k); 1 \leq i, k \leq m\}$, com $n(\mathcal{I}) \leq m^2$. Então existem $n(\mathcal{I})$ produtos de projetores $\mathcal{P}_{\psi_i} \otimes \mathcal{Q}_{\phi_k}$ e probabilidades p_{ik} tais que

$$\rho = \sum_{(i,k) \in \mathcal{I}} p_{ik} \mathcal{P}_{\psi_i} \otimes \mathcal{Q}_{\phi_k}. \quad (1.56)$$

Isto significa que qualquer estado separável em um espaço de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ de dimensão finita m , pode ser escrito como uma combinação convexa de um número finito $n(\mathcal{I})$ de produtos de estados puros, com $n(\mathcal{I}) \leq m^2$.

Agora, o critério de separabilidade baseado na imagem do operador densidade, apresentado em [7], é o seguinte:

A. Critério de Separabilidade

Seja ρ um estado em um espaço de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, $\dim \mathcal{H} = m < \infty$. Se ρ é separável, então existe um conjunto de vetores do tipo $\{|\psi_i\rangle \otimes |\phi_k\rangle\}$ e probabilidades p_{ik} , com $(i, k) \in \mathcal{I}$ e $n(\mathcal{I}) \leq m^2$, tais que:

- (i) O ensemble $\{|\psi_i\rangle \otimes |\phi_k\rangle, p_{ik}\}$ ($\{|\psi_i\rangle \otimes |\phi_k^*\rangle, p_{ik}\}$) corresponde à matriz ρ (ρ^{T_B});
- (ii) Os vetores $|\psi_i\rangle \otimes |\phi_k\rangle$ ($|\psi_i\rangle \otimes |\phi_k^*\rangle$) geram a $\text{Im}(\rho)$ ($\text{Im}(\rho^{T_B})$). Em particular, qualquer um dos vetores $|\psi_i\rangle \otimes |\phi_k\rangle \in \text{Im}(\rho)$ ($|\psi_i\rangle \otimes |\phi_k^*\rangle \in \text{Im}(\rho^{T_B})$).

Isto significa que $\text{Im}(\rho)$ é o subespaço de \mathcal{H} gerado pelos autovetores de ρ , cujos autovalores associados são não nulos, ou seja, $\text{Im}(\rho) = \{|\psi\rangle \in \mathcal{H}; \rho|\phi\rangle = |\psi\rangle, \exists |\phi\rangle \in \mathcal{H}\}$.

Todo estado separável ρ pode ser escrito na forma (1.56), ou seja,

$$\rho = \sum_{(i,k) \in I} p_{ik} |\psi_i\rangle \langle \psi_i| \otimes |\phi_k\rangle \langle \phi_k| = \sum_{(i,k) \in I} p_{ik} |\psi_i \otimes \phi_k\rangle \langle \psi_i \otimes \phi_k|, \quad (1.57)$$

usando somente $n(\mathcal{I}) \leq m^2$ produtos de estados puros $\mathcal{P}_{\psi_i} \otimes \mathcal{Q}_{\phi_k}$.

Agora, para a transposta parcial, como $\mathcal{Q}_{\phi_k}^T = \mathcal{Q}_{\phi_k}^* = (|\phi_k\rangle \langle \phi_k|)^* = |\phi_k^*\rangle \langle \phi_k^*| = \mathcal{Q}_{\phi_k^*}$, tem-se

$$\rho^{T_B} = \sum_{(i,k) \in I} p_{ik} \mathcal{P}_{\psi_i} \otimes \mathcal{Q}_{\phi_k^*}, \text{ ou seja,}$$

$$\rho^{T_B} = \sum_{(i,k) \in I} p_{ik} |\psi_i \otimes \phi_k^*\rangle \langle \psi_i \otimes \phi_k^*|. \quad (1.58)$$

Por (ii), qualquer vetor $|\psi\rangle \in \text{Im}(\rho)$ ($|\psi\rangle \in \text{Im}(\rho^{T_B})$) é uma combinação linear dos vetores pertencentes ao conjunto $\{|\psi_i\rangle \otimes |\phi_k\rangle\}$ ($\{|\psi_i\rangle \otimes |\phi_k^*\rangle\}$).

Para calcular o conjugado complexo, $|\varphi^{*2}\rangle$, de $|\varphi\rangle$, procede-se como no exemplo. Se o vetor $|\varphi\rangle$, na base $\{|0\rangle, |1\rangle\}$ de \mathbb{C}^2 , é escrito como $|\varphi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$, então,

$$\begin{aligned} |\varphi^{*2}\rangle &= ((\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle))^* \\ &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)^* \\ &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma^*|0\rangle + \delta^*|1\rangle). \end{aligned} \quad (1.59)$$

O critério apresentado em **A**, Seção 1.1.3, é apenas uma condição necessária para a separabilidade. A seguir dois exemplos de estados inseparáveis com transposta parcial positiva são apresentados [7].

A. Sistemas $\mathbb{C}^3 \otimes \mathbb{C}^3$

Considere o espaço de Hilbert $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^3$. Sejam $\mathcal{P}_\phi = |\phi\rangle\langle\phi|$ e $\{e_i\}$ uma base de \mathbb{C}^3 , onde $i = 1, 2, 3$. Defina, então, o projetor

$$\mathcal{Q} = I \otimes I - \left(\sum_{i=1}^3 (\mathcal{P}_{e_i} \otimes \mathcal{P}_{e_i}) + \mathcal{P}_{e_3} \otimes \mathcal{P}_{e_1} \right) \quad (1.60)$$

e os vetores

$$\Psi = \frac{1}{\sqrt{3}} (e_1 \otimes e_1 + e_2 \otimes e_2 + e_3 \otimes e_3), \quad (1.61)$$

$$\Phi_a = e_3 \otimes \left(\sqrt{\frac{1+a}{2}} e_1 + \sqrt{\frac{1-a}{2}} e_3 \right), \quad 0 \leq a \leq 1. \quad (1.62)$$

Os autovalores de $\mathcal{P}_\Psi^{T_B}$ são $\lambda_{1,2,3,4} = 0$, $\lambda_{5,6,7,8} = \frac{1}{3}$ e $\lambda_9 = -\frac{1}{3} < 0$, e assim, \mathcal{P}_Ψ é um estado puro entrelaçado. Combinando os estados $\mathcal{P}_\Psi = |\Psi\rangle\langle\Psi|$ e \mathcal{Q} , define-se o estado

$$\rho_{insep} = \frac{3}{8} \mathcal{P}_\Psi + \frac{1}{8} \mathcal{Q}, \quad (1.63)$$

cuja transposta parcial, $\rho_{insep}^{T_B}$ possui um autovalor $\lambda = \frac{1-\sqrt{5}}{2} < 0$. Logo, $\rho_{insep}^{T_B} \not\geq 0$, ou seja,

ρ_{insep} é inseparável. Considere, agora, o estado

$$\rho_a = \frac{8a}{8a+1} \rho_{insep} + \frac{1}{8a+1} \mathcal{P}_{\Phi_a}, \quad a > 0, \quad (1.64)$$

resultado da mistura dos estados ρ_{insep} e \mathcal{P}_{Φ_a} , em que $\mathcal{P}_{\Phi_a} = |\Phi_a\rangle\langle\Phi_a|$ é separável. Observe que

$$\mathcal{P}_{\hat{\phi}_a} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \frac{1+a}{2} & 0 & \sqrt{\frac{1-a^2}{2}} \\ 0 & 0 & 0 \\ \sqrt{\frac{1-a^2}{2}} & 0 & \frac{1-a}{2} \end{pmatrix}. \quad (1.65)$$

O estado em (1.64), como será visto a seguir, é inseparável, embora sua transposta parcial seja positiva. As representações matriciais de ρ_a e $\rho_a^{T_B}$ são dadas, respectivamente, por

$$\rho_a = \frac{1}{8a+1} \begin{pmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2}(a+2) & 0 & \frac{1}{2}\sqrt{1-a^2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & \frac{1}{2}\sqrt{1-a^2} & 0 & \frac{1}{2}(a+2) \end{pmatrix}, \quad (1.66)$$

$$\rho_a^{T_a} = \frac{1}{8a+1} \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & a & 0 & 0 \\ 0 & a & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & a & 0 \\ 0 & 0 & a & 0 & 0 & 0 & \frac{1}{2}(a+2) & 0 & \frac{1}{2}\sqrt{1-a^2} \\ 0 & 0 & 0 & 0 & 0 & a & 0 & a & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2}\sqrt{1-a^2} & 0 & \frac{1}{2}(a+2) \end{pmatrix}. \quad (1.67)$$

A matriz $\rho_a^{T_B}$ possui os seguintes autovalores $\lambda_{1,2,3} = 0$, $\lambda_{4,5} = \frac{2a}{8a+1} > 0$, $\lambda_{6,7} = \frac{a}{8a+1} > 0$, $\lambda_8 = \frac{1+2a+\sqrt{1-2a+2a^2}}{2(8a+1)} > 0$ e $\lambda_9 = \frac{1+2a-\sqrt{1-2a+2a^2}}{2(8a+1)} > 0$, pois $(1-a)^2 + a^2 \geq 0$ e $1+2a > \sqrt{1-2a+2a^2}$ e, portanto, $\rho_a^{T_B} \geq 0$. Será verificada, agora, a inseparabilidade de ρ_a , fazendo-se uma análise da $\text{Im}(\rho_a)$. Deseja-se, então, determinar todos os vetores produtos que pertencem a $\text{Im}(\rho_a^{T_B})$, com $a \neq 0,1$. Para isto, suponha que $u \in \text{Im}(\rho_a^{T_B})$, com $u = (x_1 \ x_2 \ x_3 \ x_4 \ x_5 \ x_6 \ x_7 \ x_8 \ x_9)^T$. Assim, existe um vetor $u' \in \mathbb{C}^3 \otimes \mathbb{C}^3$, de modo que $\rho_a^{T_B} u' = u$. Sendo $u' = (y_1 \ y_2 \ y_3 \ y_4 \ y_5 \ y_6 \ y_7 \ y_8 \ y_9)^T$, tem-se

$$u = (A, B, C; B, D, E; C + F, E, xF), \quad (1.68)$$

em que

$$A = x_1 = \frac{a}{8a+1} y_1, \quad B = x_2 = x_4 = \frac{a}{8a+1} (y_2 + y_4), \quad C = x_3 = \frac{a}{8a+1} (y_3 + y_7), \quad D = x_5 = \frac{a}{8a+1} y_5, \\ E = x_6 = \frac{a}{8a+1} (y_6 + y_8) \quad \text{e} \quad xF = \frac{1}{8a+1} \left(\frac{\sqrt{1-a^2}}{2} y_7 + \frac{1+a}{2} y_9 \right), \quad \text{com} \quad A, B, C, D, E, F \in \mathbb{C} \quad \text{e} \\ x = \sqrt{\frac{1+a}{1-a}}, \quad a \neq 0,1.$$

Por outro lado, $u \in \mathbb{C}^3 \otimes \mathbb{C}^3$ deve ser da forma

$$u_{\text{prod}} = (r, s, t) \otimes (\tilde{A}, \tilde{B}, \tilde{C}) = \left(r(\tilde{A}, \tilde{B}, \tilde{C}); s(\tilde{A}, \tilde{B}, \tilde{C}); t(\tilde{A}, \tilde{B}, \tilde{C}) \right), \quad (1.69)$$

$$r, s, t, \tilde{A}, \tilde{B}, \tilde{C} \in \mathbb{C}.$$

Os casos possíveis para r e s , são:

$$(i) \quad rs \neq 0$$

Neste caso, $r \neq 0$ e $s \neq 0$. O problema não perde a generalidade se $r = 1$, $\tilde{A} = A$, $\tilde{B} = B$ e $\tilde{C} = C$. Assim,

$$u_{prod} = (A, B, C; sA, sB, sC; tA, tB, tC). \quad (1.70)$$

Resulta da comparação entre (1.70) e (1.68), as seguintes equações: $B = sA$, $E = sC$, $C + F = tA$, $E = tB$ e $xF = tC$. De $B = sA$ e $E = tB$, vem $E = stA$, e como $E = sC$, tem-se $C = tA$, com $A \neq 0$, caso contrário, $u_{prod} \equiv 0$. De $C + F = tA$ e $C = tA$, vem $F = 0$. Finalmente, de $xF = tC$ e $C = tA$, segue $xF = t^2A$, ou seja, $t^2A = 0$. Como $A \neq 0$, tem-se $t = 0$, resultando $C = 0$. Assim, os estados u_{prod} têm a seguinte forma:

$$u_1 = (1, s, 0) \otimes (A, sA, 0) \Rightarrow u_1 = A(1, s, 0) \otimes (1, s, 0), A, s \in \mathbb{C}. \quad (1.71)$$

(ii) $r = 0$

Neste caso,

$$u_{prod} = (0, 0, 0; s(\tilde{A}, \tilde{B}, \tilde{C}); t(\tilde{A}, \tilde{B}, \tilde{C})), s, t, \tilde{A}, \tilde{B}, \tilde{C} \in \mathbb{C}, \quad (1.72)$$

ou seja,

$$u_{prod} = (0, 0, 0; 0, D, E; F, E, xF), D, E, F \in \mathbb{C}, \quad (1.73)$$

devido à forma (1.68). Se $s = 0$, então $D = E = 0$. Logo,

$$u_{prod} = (0, 0, 0; 0, 0, 0; F, 0, xF), \quad (1.74)$$

e assim, u_{prod} tem a forma:

$$u_2 = (0, 0, 1) \otimes (F, 0, xF) \Rightarrow u_2 = F(0, 0, 1) \otimes (1, 0, x), F \in \mathbb{C}. \quad (1.75)$$

Se $s \neq 0$, colocando $s = 1$, resulta:

$$u_{prod} = (0, 0, 0; \tilde{A}, \tilde{B}, \tilde{C}; t\tilde{A}, t\tilde{B}, t\tilde{C}), s, t, \tilde{A}, \tilde{B}, \tilde{C} \in \mathbb{C}. \quad (1.76)$$

Para $t = 0$, tem-se por (1.73), $u_{prod} = (0, 0, 0; 0, D, 0; 0, 0, 0)$, e assim,

$$u_3 = (0, 1, 0) \otimes (0, D, 0) \Rightarrow u_3 = D(0, 1, 0) \otimes (0, 1, 0), D \in \mathbb{C}. \quad (1.77)$$

Suponha, agora, $t \neq 0$. Da comparação entre as Eqs. (1.78) e (1.79), a seguir

$$u_{prod} = (0, 0, 0; s(\tilde{A}, \tilde{B}, \tilde{C}); t(\tilde{A}, \tilde{B}, \tilde{C})), s, t, \tilde{A}, \tilde{B}, \tilde{C} \in \mathbb{C}, \quad (1.78)$$

$$u_{prod} = (0, 0, 0; 0, D, E; F, E, xF), D, E, F \in \mathbb{C}, \quad (1.79)$$

resulta $\tilde{B} = D$, $\tilde{C} = E$, $F = t\tilde{A}$, $E = t\tilde{B}$ e $xF = t\tilde{C}$. De $\tilde{B} = D$ e $E = t\tilde{B}$, vem $E = tD$; de $\tilde{C} = E$ e $xF = t\tilde{C}$, vem, $xF = tE$, e como $\tilde{A} = 0$ e $F = t\tilde{A}$, tem-se $F = 0$. Como $xF = tE$, $F = 0$ e $t \neq 0$, tem-se $E = 0$; logo, de $E = tD$, segue que $D = 0$. Portanto, $u_{prod} = 0$.

(iii) $r \neq 0$ e $s = 0$

Como no caso (i), pondo $r = 1$, $\tilde{A} = A$, $\tilde{B} = B$ e $\tilde{C} = C$, tem-se:

$$u_{prod} = (A, B, C; 0, 0, 0; tA, tB, tC). \quad (1.80)$$

Comparando (1.80) com (1.68), resulta: $B = D = E = 0$, $tA = C + F$, $tB = E = 0$, $tC = xF$. Daí,

$$u_{prod} = (A, 0, C; 0, 0, 0; C + F, 0, xF). \quad (1.81)$$

Se $t = 0$, então $C + F = 0$ e $xF = 0$. Daí, $F = C = 0$. Assim,

$$u_4 = (1, 0, 0) \otimes (A, 0, 0) \Rightarrow u_4 = A(1, 0, 0) \otimes (1, 0, 0), A \in \mathbb{C}. \quad (1.82)$$

E, para $t \neq 0$, $tA = C + F$ e $xF = tC$. Daí, $A = (x^{-1} + t^{-1})C$. Assim,

$$u_5 = (1, 0, t) \otimes \left((x^{-1} + t^{-1})C, 0, C \right) \Rightarrow u_5 = C(1, 0, t) \otimes (x^{-1} + t^{-1}, 0, 1), t, C \in \mathbb{C}, t \neq 0. \quad (1.83)$$

Os conjugados complexos parciais dos vetores u_i , $i = 1, 2, 3, 4, 5$, são:

$$u_1^{*2} = A(1, s, 0) \otimes (1, s^*, 0), A, s \in \mathbb{C}, s \neq 0, . \quad (1.84)$$

$$u_2^{*2} = F(0, 0, 1) \otimes (1, 0, x), F \in \mathbb{C}, \quad (1.85)$$

$$u_3^{*2} = D(0, 1, 0) \otimes (0, 1, 0), D \in \mathbb{C}, \quad (1.86)$$

$$u_4^{*2} = A(1, 0, 0) \otimes (1, 0, 0), A \in \mathbb{C}, \quad (1.87)$$

$$u_5^{*2} = C(1, 0, t) \otimes \left((t^*)^{-1} + x^{-1}, 0, 1 \right), C, t \in \mathbb{C}, t \neq 0. \quad (1.88)$$

Os vetores u_i^{*2} , acima, não podem gerar $\text{Im}(\rho_a)$, pois são ortogonais ao vetor

$$\tilde{u} = (0, 0, 1) \otimes (0, 1, 0) \in \text{Im}(\rho_a) \quad (1.89)$$

e, portanto, $u_i^{*2} \notin \text{Im}(\rho_a^{T_B})$. Isto significa dizer que $\rho_a^{T_B}$ não satisfaz a segunda condição do critério **A**, Seção 1.1.3, para $a \neq 0, 1$, e assim, ρ_a é inseparável.

B. Sistemas $\mathbb{C}^2 \otimes \mathbb{C}^4$

Sejam os vetores

$$\psi_i = \frac{1}{\sqrt{2}}(e_1 \otimes e_i + e_2 \otimes e_{i+1}), i = 1, 2, 3, \quad (1.90)$$

$$\phi_b = e_2 \otimes \left(\sqrt{\frac{1+b}{2}}e_1 + \sqrt{\frac{1-b}{2}}e_3 \right), 0 \leq b \leq 1. \quad (1.91)$$

O estado definido por

$$\sigma_{insep} = \frac{2}{7} \sum_{i=1}^3 \mathcal{P}_{\psi_i} + \frac{1}{7} \mathcal{P}_{e_1 \otimes e_4} \quad (1.92)$$

possui um autovalor $\lambda = \frac{1-\sqrt{5}}{2} < 0$, ou seja, $\sigma_{insep}^{T_b} \not\geq 0$. Portanto, σ_{insep} é inseparável.

Considere agora os estados da forma

$$\sigma_b = \frac{7b}{7b+1} \sigma_{insep} + \frac{1}{7b+1} \mathcal{P}_{\phi_b}. \quad (1.93)$$

Assim, as matrizes de σ_b e $\sigma_b^{T_b}$ são dadas, respectivamente, por

$$\sigma_b = \frac{1}{7b+1} \begin{pmatrix} b & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2}(1+b) & 0 & 0 & \frac{1}{2}\sqrt{1-b^2} \\ b & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & b & 0 & \frac{1}{2}\sqrt{1-b^2} & 0 & 0 & \frac{1}{2}(1+b) \end{pmatrix}, \quad (1.94)$$

$$\sigma_b^{T_b} = \frac{1}{7b+1} \begin{pmatrix} b & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & b & 0 & 0 & 0 \\ 0 & 0 & b & 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & b & 0 \\ 0 & b & 0 & 0 & \frac{1}{2}(1+b) & 0 & 0 & \frac{1}{2}\sqrt{1-b^2} \\ 0 & 0 & b & 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2}\sqrt{1-b^2} & 0 & 0 & \frac{1}{2}(1+b) \end{pmatrix}. \quad (1.95)$$

Calculando-se os autovalores de $\sigma_b^{T_B}$, obtém-se $\lambda_{1,2,3} = 0$, $\lambda_{4,5} = \frac{2b}{7b+1} > 0$, $\lambda_6 = \frac{b}{7b+1} > 0$,
 $\lambda_7 = \frac{1+2b+\sqrt{(1-b)^2+b^2}}{2(7b+1)} > 0$ e $\lambda_8 = \frac{1+2b-\sqrt{(1-b)^2+b^2}}{2(7b+1)} > 0$, pois $(1-b)^2+b^2 \geq 0$ e
 $1+2b > \sqrt{(1-b)^2+b^2}$, e assim, $\sigma_b^{T_B} \geq 0$. Para determinar todos os vetores produtos
 pertencentes a $\text{Im}(\sigma_b)$, seja $v \in \text{Im}(\sigma_b)$. Então existe $v' \in \mathbb{C}^2 \otimes \mathbb{C}^4$ tal que $\sigma_b v' = v$, e daí
 segue que

$$v = (A, B, C, D; E, A, B, C + yE), \quad (1.96)$$

com $A, B, C, D, E \in \mathbb{C}$ e $y = \sqrt{\frac{1-b}{1+b}} \neq 0, 1$. Por outro lado, se $v \in \mathbb{C}^2 \otimes \mathbb{C}^4$, então

$$v_{prod} = (r, s) \otimes (\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D}) = (r(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D}); s(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})), r, s, \tilde{A}, \tilde{B}, \tilde{C}, \tilde{D} \in \mathbb{C}. \quad (1.97)$$

Analisando os valores de r e s , os casos a serem considerados são os seguintes:

- (i) $r \neq 0$ e $s \neq 0$

Como no Exemplo **A**, caso (i), pode-se supor sem perda de generalidade que $r=1$,
 $\tilde{A} = A, \tilde{B} = B, \tilde{C} = C, \tilde{D} = D$. Assim,

$$v_{prod} = (A, B, C, D; sA, sB, sC, sD). \quad (1.98)$$

Comparando (1.98) e (1.96), tem-se $E = sA$, $A = sB$, $B = sC$ e $C + yE = sD$. De $E = sA$ e
 $A = sB$, vem $E = s^2B$. Como $B = sC$, segue que $E = s^3C$. Substituindo $E = s^3C$ em
 $C + yE = sD$, vem $D = s^{-1}(1 + ys^3)C$. E, de $B = sC$ em $A = sB$, vem $A = s^2C$. Assim,

$$v_1 = (1, s) \otimes (s^2C, sC, C, s^{-1}(1 + ys^3)C) = C(1, s) \otimes (s^2, s, 1, s^{-1}(1 + ys^3)), C, s \in \mathbb{C}, s \neq 0. \quad (1.99)$$

- (ii) $r = 0$ e $s \neq 0$

Neste caso, $v_{prod} = (0, 0, 0, 0; E, 0, 0, yE)$, por (1.96). Assim,

$$v_2 = (0, 1) \otimes (E, 0, 0, yE) = E(0, 1) \otimes (1, 0, 0, y), E \in \mathbb{C}. \quad (1.100)$$

(iii) $r \neq 0$ e $s = 0$

Supondo $r = 1$, tem-se $v_{prod} = (A, B, C, D; 0, 0, 0, 0) = (0, 0, C, D; E, 0, 0, C + yE)$. Daí, $E = 0$ e $C + yE = 0$; assim, $C = 0$. Portanto, $v_{prod} = (0, 0, 0, D; 0, 0, 0, 0)$, ou seja,

$$v_3 = (1, 0) \otimes (0, 0, 0, D) = D(1, 0) \otimes (0, 0, 0, 1), D \in \mathbb{C}. \quad (1.101)$$

Os conjugados complexos parciais de $v_i \in \text{Im}(\sigma_b)$, são:

$$v_1^{*2} = C(1, s) \otimes \left((s^*)^2, s^*, 1, (s^*)^{-1} (1 + y(s^*)^3) \right), C, s \in \mathbb{C}, s \neq 0, \quad (1.102)$$

$$v_2^{*2} = E(0, 1) \otimes (1, 0, 0, y), E \in \mathbb{C}, \quad (1.103)$$

$$v_3^{*2} = D(1, 0) \otimes (0, 0, 0, 1), D \in \mathbb{C}. \quad (1.104)$$

Por outro lado, se $w \in \text{Im}(\sigma_b^{T_B})$, então

$$w = (A', B', C', D'; B' + yE', C', D', E'), \quad (1.105)$$

com $A', B', C', D', E' \in \mathbb{C}$ e $y = \sqrt{\frac{1-b}{1+b}} \neq 0, 1$.

O problema, agora, é saber quando $v_i^{*2} \in \text{Im}(\sigma_b^{T_B})$, isto é, quando eles podem ser colocados sob a forma (1.105). Para o vetor v_1^{*2} , suponha $v_1^{*2} \neq 0$ ($C \neq 0$). Então, v_1^{*2} é da forma (1.105), se $C' = C$, $C' = C s s^*$, $B' = s^*$, $B' + yE' = C s (s^*)^2$, $E' = C s (s^*)^{-1} (y + (s^*)^3)$,

$D' = (s^*)^{-1} \left(y + (s^*)^3 \right)$ e $D' = Cs$. De $C' = C$ e $C' = C s s^*$, vem $s s^* = 1$. Tomando-se as equações $B' = s^*$, $E' = C s (s^*)^{-1} \left(y + (s^*)^3 \right)$ e $B' + y E' = C s (s^*)^2$, e as duas equações que envolvem D' , combinando as equações resultantes e usando $s s^* = 1$, obtém-se $y s^2 = 0$. Como, $s \neq 0$, segue que $y = 0$, e isso contradiz o fato de ser $y \neq 0$. Já o vetor v_2^{*2} é da forma (1.105) se $y E' = E$ e $y E = E'$. Daí, $E = 0$, e assim $v_2^{*2} \equiv 0$. Agora, o vetor v_3^{*2} é da forma (1.105) se $D = 0$ e, então $v_3^{*2} \equiv 0$. Portanto, nenhum dos vetores v_i^{*2} pertence ao $\text{Im}(\sigma_b^{T_B})$. Assim, σ_b não satisfaz a condição (ii) do critério **A**, Seção 1.1.3, sendo, portanto, um estado inseparável.

Os exemplos acima fornecem estados inseparáveis com transposta parcial positiva. Na linguagem dos mapas positivos, sendo ρ_a e σ_b estados inseparáveis devem existir mapas positivos $\Lambda_A : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ e $\Lambda_B : \mathbb{C}^2 \rightarrow \mathbb{C}^4$, tais que $(I \otimes \Lambda_A)(\rho_A) \not\geq 0$ e $(I \otimes \Lambda_B)(\sigma_B) \not\geq 0$, isto é, cada um deles possui um autovalor negativo. De acordo com os Horodecki, os mapas Λ_A e Λ_B não podem ser da forma $\Lambda = \Lambda_1^{CP} + \Lambda_2^{CP} T$, onde Λ_i^{CP} é um mapa completamente positivo e T é o mapa transposição.

A seguir será visto a decomposição de Schmidt e como essa decomposição pode ser considerada um critério de separabilidade.

1.1.4. Decomposição de Schmidt

A decomposição de Schmidt tem um papel fundamental no estudo do entrelaçamento de estados bipartes puros, sendo considerada um critério de separabilidade para tais estados.

Seja $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ um estado puro de um sistema biparte. Então, existem bases ortonormais $\{|\psi_A^i\rangle\}$ e $\{|\psi_B^i\rangle\}$ para \mathcal{H}_A e \mathcal{H}_B , respectivamente, tais que

$$|\psi\rangle = \sum_{i=1}^n \lambda_i |\psi_A^i\rangle |\psi_B^i\rangle, \quad (1.106)$$

onde $n \leq \min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}$ e $\sum_i \lambda_i^2 = 1$, com $\lambda_i > 0$. Quando um estado puro $|\psi\rangle$ está escrito na forma (1.106), diz-se que esta é a decomposição de Schmidt para $|\psi\rangle$, e que os coeficientes λ_i são chamados coeficientes de Schmidt e as bases $\{|\psi_A^i\rangle\}$ e $\{|\psi_B^i\rangle\}$, chamadas bases de Schmidt. A quantidade de λ_i 's necessários para decompor $|\psi\rangle$, é chamada número de Schmidt.

Como exemplo, considere o estado [10]:

$$|\psi\rangle = \frac{1+\sqrt{6}}{2\sqrt{6}}|00\rangle + \frac{1-\sqrt{6}}{2\sqrt{6}}|01\rangle + \frac{\sqrt{2}-\sqrt{3}}{2\sqrt{6}}|10\rangle + \frac{\sqrt{2}+\sqrt{3}}{2\sqrt{6}}|11\rangle. \quad (1.107)$$

Assim, a decomposição de Schmidt para o estado $|\psi\rangle$, é:

$$|\psi\rangle = \lambda_1 |\psi_A^1\rangle |\psi_B^1\rangle + \lambda_2 |\psi_A^2\rangle |\psi_B^2\rangle, \quad (1.108)$$

em que

$$\left\{ |\psi_A^1\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle, |\psi_A^2\rangle = \frac{\sqrt{2}}{\sqrt{3}}|0\rangle - \frac{1}{\sqrt{3}}|1\rangle \right\}, \quad (1.109)$$

$$\left\{ |\psi_B^1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, |\psi_B^2\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right\}, \quad (1.110)$$

são as bases de Schmidt e $\lambda_1 = \frac{1}{2}$, $\lambda_2 = \frac{\sqrt{3}}{2}$ são os coeficientes de Schmidt para o estado $|\psi\rangle$.

Nesse caso, o número de Schmidt de $|\psi\rangle$ é igual a 2.

Para verificar a relação entre a decomposição de Schmidt e o entrelaçamento, considere um estado puro de dois qubits $|\psi\rangle$, que segundo (1.106), pode ser escrito como

$$|\psi\rangle = \lambda_1 |i_1\rangle |j_1\rangle + \lambda_2 |i_2\rangle |j_2\rangle, \quad (1.111)$$

$\lambda_1, \lambda_2 > 0$ e $\lambda_1^2 + \lambda_2^2 = 1$.

Seja $U = U_A \otimes U_B$ uma transformação unitária local, onde $U_A = |0\rangle\langle i_1| + |1\rangle\langle i_2|$ e $U_B = |1\rangle\langle j_1| + |0\rangle\langle j_2|$. Aplicando U em $|\psi\rangle$, tem-se $|\psi'\rangle = U|\psi\rangle = \lambda_1|01\rangle + \lambda_2|10\rangle$. Como as transformações unitárias locais preservam o grau de entrelaçamento de um sistema quântico, todo estado entrelaçado de dois qubits possui dois coeficientes de Schmidt não nulos. Se um dos coeficientes fosse igual a zero, então o estado seria separável. Isto mostra que a decomposição de Schmidt pode ser considerada como um critério de separabilidade para estados bipartes puros. Observe, neste exemplo, que o número de Schmidt é preservado por transformações LU . Observa-se, ainda, que para descrever $|\psi\rangle$, em geral, seriam necessários $\dim \mathcal{H}_1 \times \dim \mathcal{H}_2$ coeficientes λ_{ij} . A decomposição de Schmidt reduz esta quantidade para no máximo, $\min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}$. Se o número de Schmidt é igual a 1, então o estado é separável. Se a quantidade de λ_i 's é maior ou igual a 2, o estado é entrelaçado.

1.2. Medidas de Entrelaçamento Quântico

Até aqui, a preocupação foi determinar se um estado quântico possui ou não entrelaçamento, ou seja, definir critérios para decidir sobre a existência de entrelaçamento em um dado estado quântico. Mas, isso não é tudo, mais importante do que apenas determinar se um estado quântico possui ou não entrelaçamento é saber quanto entrelaçamento ele possui, isto é, medir (quantificar) o seu entrelaçamento. Obviamente toda medida de entrelaçamento exprime também uma condição de separação. Uma boa medida de entrelaçamento E , para um estado quântico ρ , deve obedecer a alguns requisitos [12]:

a) Não negativa

$$E(\rho) \geq 0, \forall \rho; E(\rho) = 0 \Leftrightarrow \rho \text{ é desentrelaçado.} \quad (1.112)$$

b) Invariante mediante operações unitárias locais

Se U_A, U_B, \dots, U_N são operações unitárias locais atuando em ρ , então

$$E(\rho) = E\left[(U_A \otimes U_B \otimes \dots \otimes U_N) \rho (U_A \otimes U_B \otimes \dots \otimes U_N)^\dagger\right]. \quad (1.113)$$

c) Monotonicidade sob LOCC

O entrelaçamento do estado ρ não pode ser aumentado através de operações quânticas locais e comunicações clássicas. Isto significa que se for realizada uma operação em qualquer um dos subsistemas de ρ , resultando em um estado total σ_i , com probabilidade p_i , então o entrelaçamento do novo estado não pode crescer em média, ou seja,

$$\sum_i p_i E(\sigma_i) \leq E(\rho), \quad (1.114)$$

com $p_i > 0$ e $\sum_i p_i = 1$.

d) Convexidade

O entrelaçamento do estado ρ é decrescente mediante combinações convexas, isto é,

$$E\left[\sum_i p_i \sigma_i\right] \leq \sum_i p_i E(\sigma_i), \quad (1.115)$$

onde $p_i > 0$ e $\sum_i p_i = 1$.

Satisfazendo a), b), c) e d), existem boas medidas de entrelaçamento para estados bipartes puros e mistos. Quando o estado biparte é puro, denotado por $|\psi\rangle$, tendo matriz densidade $\rho = |\psi\rangle\langle\psi|$, o entrelaçamento pode ser quantificado pela entropia de von Neumann de uma das partes individuais do sistema. Sendo A e B as partes individuais do sistema, tem-se

$$E(\rho) = S(\rho_X), \quad (1.116)$$

em que $S(\rho_X) = -\text{Tr}(\rho_X \log \rho_X)$ e ρ_X é a matriz densidade reduzida do sistema X ,

$X \in \{A, B\}$. A decomposição de Schmidt para $|\psi\rangle$ é dada por $|\psi\rangle = \sum_{i=1}^n \alpha_i |\psi_A^i\rangle |\psi_B^i\rangle$, em que

$\{|\psi_A^i\rangle\}$ e $\{|\psi_B^i\rangle\}$ são bases ortonormais para os subsistemas A e B , respectivamente, e $\sum_i \alpha_i^2 = 1$, $\alpha_i > 0$. Daí,

$$E(|\psi\rangle\langle\psi|) = -\sum_{i=1}^n \alpha_i^2 \log_2 \alpha_i^2. \quad (1.117)$$

Esta quantidade é a *Entropia de von Neumann* da matriz densidade associada a cada um dos subsistemas e os valores de α_i^2 são os autovalores não nulos de cada uma dessas duas matrizes densidade. Por exemplo, se $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ (maximamente entrelaçado), então $E(|\psi_-\rangle\langle\psi_-|) = 1$, enquanto, $E(|\psi\rangle\langle\psi|) = 0$, se $|\psi\rangle$ for separável.

Quando o estado de um sistema quântico composto é misto, a tarefa de medir o entrelaçamento é mais complexa. Foram propostas medidas na tentativa de quantificar o entrelaçamento: *entrelaçamento de formação*, E_F , o *entrelaçamento destilável*, E_D [14], e o *custo de entrelaçamento*, E_C , que é definido de maneira dual ao entrelaçamento destilável [15]. A primeira, E_F , como o próprio nome sugere, diz como construir estados quânticos, e é definida como segue. Considere todas as decomposições possíveis de ρ em estados puros, isto é, todos os “ensembles” de estados $|\psi_i\rangle$, com probabilidade p_i , tais que $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Para cada estado puro $|\psi_i\rangle$, o entrelaçamento E , é definido como a entropia de um dos seus dois subsistemas, $E(|\psi_i\rangle) = S(|\psi_i\rangle)$. Assim, o *Entrelaçamento de Formação* de ρ é definido como o entrelaçamento médio dos estados puros da decomposição, minimizado sobre todas as decomposições de ρ :

$$E_F(\rho) = \inf_{\{(p_i, |\psi_i\rangle)\}} \sum_i p_i E(|\psi_i\rangle), \quad (1.118)$$

sendo que os estados puros $|\psi_i\rangle$ em (1.118) não são necessariamente ortogonais.

Para determinar o *custo de entrelaçamento*, E_C , é necessário determinar o número de pares *EPR* que devem ser compartilhados entre duas partes A e B , para produzir um estado ρ ,

de dois subsistemas, A e B , através de $LOCC$. Definindo o entrelaçamento de um par EPR como 1-*ebit*, tem-se que o custo de produção de ρ é dado em *ebits*. Suponha, então, que exista um protocolo \mathcal{P} que, através de $LOCC$, leva m pares EPR em n pares do estado ρ . Tem-se que $E(\rho) = \frac{m}{n}$ *ebits*, sendo $n \rightarrow \infty$ (regime assintótico). O *custo de entrelaçamento*, E_C , é definido, portanto, como

$$E_C(\rho) = \inf_{\mathcal{P}_{LOCC}} \lim_{n \rightarrow \infty} \frac{m}{n}. \quad (1.119)$$

Já para determinar o *entrelaçamento destilável* de ρ , é preciso saber quantos pares EPR podem ser extraídos (destilados) de n pares de um estado ρ , também no regime assintótico, através de um protocolo \mathcal{P} que usa somente $LOCC$. Sendo assim, o entrelaçamento que pode ser destilado de ρ , é

$$E_D(\rho) = \sup_{\mathcal{P}_{LOCC}} \lim_{m \rightarrow \infty} \frac{n}{m}, \quad (1.120)$$

desde que m pares possam ser obtidos por $LOCC$.

Para o cálculo do *entrelaçamento de formação* de um sistema biparte de dois qubits, existe uma fórmula analítica relacionada com outra quantidade, chamada de *concorrência*.

Considere, por exemplo, $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, um estado biparte puro de qubits, com $a, b, c, d > 0$ e $a^2 + b^2 + c^2 + d^2 = 1$. Usando a decomposição de Schmidt, $|\psi\rangle$ pode ser escrito como $|\psi\rangle = \alpha_1|01\rangle + \alpha_2|10\rangle$, $\alpha_1, \alpha_2 > 0$, $\alpha_1^2 + \alpha_2^2 = 1$ e $\alpha_1 \geq \alpha_2$. Assim, por (1.116),

$$E(|\psi\rangle\langle\psi|) = -\alpha_1^2 \log_2 \alpha_1^2 - (1 - \alpha_1^2) \log_2 (1 - \alpha_1^2). \quad (1.121)$$

Será mostrado a seguir que $E(|\psi\rangle\langle\psi|)$ pode ser escrito como uma função da *concorrência* que, neste caso, é definida por

$$\mathcal{C}(\psi) = |\langle \psi | \tilde{\psi} \rangle|, \quad (1.122)$$

na qual $|\tilde{\psi}\rangle = \sigma_y \otimes \sigma_y |\psi^*\rangle$ é a transformação “spin-flip”, $|\psi^*\rangle = \alpha_1^* |01\rangle + \alpha_2^* |10\rangle$ é o complexo conjugado de $|\psi\rangle$ na base canônica $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ e $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. Assim,

$$\mathcal{C}(\psi) = 2\alpha_1\alpha_2. \quad (1.123)$$

Considere, agora, uma função E definida por

$$E(\psi) = \mathcal{E}(\mathcal{C}(\psi)), \quad (1.124)$$

$$\mathcal{E}(\mathcal{C}) = h\left(\frac{1 + \sqrt{1 - \mathcal{C}^2}}{2}\right), \quad (1.125)$$

$$h(x) = -x \log_2 x - (1-x) \log_2 (1-x). \quad (1.126)$$

De fato, substituindo o valor de \mathcal{C} em (1.125), tem-se $\mathcal{E}(\mathcal{C}) = h\left(\frac{1 + \sqrt{1 - \mathcal{C}^2}}{2}\right) = h(\alpha_1^2)$. Mas, por (1.126), $h(\alpha_1^2) = -\alpha_1^2 \log_2 \alpha_1^2 - (1 - \alpha_1^2) \log_2 (1 - \alpha_1^2)$, ou seja, $\mathcal{E}(\mathcal{C}(\psi)) = E(|\psi\rangle\langle\psi|)$, por (1.117). Assim, $E(\psi) = \mathcal{E}(\mathcal{C}(\psi))$ e, portanto, E é uma função monotonicamente crescente de \mathcal{C} , para $0 \leq \mathcal{C} \leq 1$.

A seguir uma expressão analítica que permite determinar a *concorrência* do estado $|\psi\rangle$, quando $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, com $a, b, c, d > 0$ e $a^2 + b^2 + c^2 + d^2 = 1$. Usando (1.122), obtem-se:

$$\mathcal{C}(\psi) = 2|ad - bc|. \quad (1.127)$$

De (1.8), segue que o estado $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ é separável, se e somente se, $ad = bc$. Neste caso, $\mathcal{C}(\psi) = 0$, e assim, $E(\psi) = 0$. Para $ad \neq bc$, tem-se $E(\psi) > 0$.

Para estados mistos bipartes de qubits, o entrelaçamento de formação pode ser calculado analiticamente através do uso da equação de Wootters [17],

$$E(\rho) = \mathcal{E}(\mathcal{C}(\rho)), \quad (1.128)$$

com $\mathcal{C}(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$, onde $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$ são os autovalores da matriz Hermitiana $R = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$ ou, equivalentemente, $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$ são as raízes quadradas dos autovalores da matriz não Hermitiana $\rho\tilde{\rho}$. Aqui, $\tilde{\rho}$ é o estado definido por $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$ e ρ^* é o complexo conjugado do estado ρ na base canônica $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Por [14], qualquer outra medida E , satisfazendo a), b), c), d), que é baseada em entropia deve satisfazer $E_D(\rho) \leq E(\rho) \leq E_F(\rho)$. Entre estas, uma das mais diretas e utilizadas é a entropia relativa do entrelaçamento, que foi introduzida por Vedral e Plenio [18] e, de forma simplificada, pode ser descrita da seguinte maneira:

“O entrelaçamento de um estado quântico ρ pode ser dado pela mínima distância entre o mesmo e um estado desentrelaçado, ou seja,

$$E(\rho) = \min_{\sigma \in \mathcal{D}} d(\rho \parallel \sigma), \quad (1.129)$$

onde \mathcal{D} é o conjunto de todos os possíveis estados desentrelaçados.”

Para a distância d , não necessariamente usa-se uma métrica, pode-se usar a entropia relativa quântica, dada por

$$d(\rho \parallel \sigma) \equiv S(\rho \parallel \sigma) = \text{Tr}(\rho \ln \rho - \rho \ln \sigma). \quad (1.130)$$

A mínima distância, dada por (1.129), pode ser obtida numericamente. Outras medidas de distância têm sido testadas, como a métrica de Bures e a norma de Hilbert-Schmidt (ou norma de Frobenius) que são dadas, respectivamente, por [18]

$$d_B(\rho\|\sigma) = 2 - 2\text{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}} = 2 - 2F(\rho, \sigma), \quad (1.131)$$

$$d_{HS}(\rho\|\sigma) = \sqrt{\text{Tr}(\rho - \sigma)^2}. \quad (1.132)$$

Uma vez que se precisa calcular (1.129) e (1.130), dentre todos os possíveis estados desentrelaçados, torna-se necessária a fórmula geral dos estados bipartes de qubits desentrelaçados [19]. Para tais estados essa fórmula é dada por

$$\rho = \sum_{i=1}^{16} p_i (\rho_A^i \otimes \rho_B^i), \quad (1.133)$$

com $\sum_i p_i = 1$ e $\rho_{A,B}^i$ estados puros da forma

$$\rho_A^i = \begin{pmatrix} \cos^2(\theta_i) & \cos(\theta_i)\sin(\theta_i)\exp(i\xi_i) \\ \cos(\theta_i)\sin(\theta_i)\exp(-i\xi_i) & \sin^2(\theta_i) \end{pmatrix} \quad (1.134)$$

$$\rho_B^i = \begin{pmatrix} \cos^2(\varphi_i) & \cos(\varphi_i)\sin(\varphi_i)\exp(i\phi_i) \\ \cos(\varphi_i)\sin(\varphi_i)\exp(-i\phi_i) & \sin^2(\varphi_i) \end{pmatrix}. \quad (1.135)$$

A última medida a ser aqui considerada é a *Negatividade*. O critério de Peres-Horodecki é uma condição binária: *a transposta parcial da matriz densidade tem ou não algum autovalor negativo?* Uma versão quantitativa deste critério foi proposta por Vidal e Werner através do uso de uma nova quantidade baseada na norma traço da transposta parcial, chamada *Negatividade* [20]:

$$\mathcal{N}(\rho) \equiv \frac{\|\rho^{T_A}\|_1 - 1}{2}, \quad (1.136)$$

em que $\|\rho^{T_A}\|_1 = \text{Tr}\sqrt{(\rho^{T_A})^\dagger \rho^{T_A}}$ é a soma dos valores absolutos dos autovalores de ρ^{T_A} . Basicamente, a negatividade mede o grau em que a matriz ρ^{T_A} falha em ser positiva semidefinida, pois $\mathcal{N}(\rho)$ é o valor absoluto da soma dos autovalores negativos de ρ^{T_A} . A negatividade não é baseada em destilação e diluição assintótica de estados entrelaçados puros, como E_F , E_D e a entropia relativa do entrelaçamento. Devido a este fato, a negatividade não se reduz à entropia parcial de von Neumann quando aplicada a estados puros, o que ocorre com as outras medidas citadas. Além disso, um ponto interessante é o fato de que a negatividade e o entrelaçamento de formação, por exemplo, não preservam a mesma ordenação, isto é, se ρ_1 e ρ_2 são dois estados quânticos, então $E_F(\rho_1) > E_F(\rho_2)$ não necessariamente implica em $\mathcal{N}(\rho_1) > \mathcal{N}(\rho_2)$. Se para duas medidas de entrelaçamento, E_1 e E_2 , ocorrer

$$E_1(\rho_1) > E_1(\rho_2) \Leftrightarrow E_2(\rho_1) > E_2(\rho_2), \quad (1.137)$$

para quaisquer operadores densidade ρ_1 e ρ_2 , diz-se que E_1 e E_2 preservam a mesma ordenação de operadores densidade.

Como exemplo, considere $\rho_1 = |\psi\rangle\langle\psi|$, onde $|\psi\rangle$ é um estado puro de dois qubits, cuja decomposição de Schmidt é dada por $|\psi\rangle = \alpha_1|00\rangle + \alpha_2|11\rangle$, com $\alpha_1, \alpha_2 > 0$. Neste caso, $E_F(\rho_1) = S(\rho_1)$ e $\mathcal{N}(\rho_1) = \alpha_1\alpha_2 = \alpha_1\sqrt{1-\alpha_1^2}$, que decrescem monotonicamente com α_1 . Logo, para estados puros, (1.137) é satisfeita. Tem-se, também, que $\mathcal{C}(|\psi\rangle\langle\psi|) = 2\alpha_1\sqrt{1-\alpha_1^2}$. Assim, para estados puros arbitrários $\rho = |\psi\rangle\langle\psi|$, $\mathcal{C}(\rho) = 2\mathcal{N}(\rho)$. Considere agora o estado de Werner [21], $\rho_F = \frac{4F-1}{3}|\psi^-\rangle\langle\psi^-| + \frac{1-F}{3}I$, onde $\frac{1}{4} \leq F \leq 1$ e $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Então, $\mathcal{C}(\rho_F) = 2F - 1$, para $F \geq \frac{1}{2}$ (caso contrário, ρ_F é separável), enquanto $E_F(\rho_F) = -\mu \log_2 \mu - (1-\mu) \log_2 (1-\mu)$, $\mu = \frac{1}{2} + \sqrt{F(1-F)}$. A negatividade de ρ_F é dada

por $\mathcal{N}(\rho_F) = F - \frac{1}{2}$, e assim, a equação $\mathcal{C}(\rho) = 2\mathcal{N}(\rho)$, também, é válida para os estados de Werner. Como essas decrescem monotonicamente com F , (1.137) é satisfeita.

Agora, se, por exemplo, ρ_1 é puro e ρ_2 é o estado de Werner, (1.137) pode não ser satisfeita. Como \mathcal{E} é uma função monotonicamente crescente de \mathcal{C} , tem-se $\mathcal{C}(\rho_1) > \mathcal{C}(\rho_2) \wedge \mathcal{N}(\rho_1) > \mathcal{N}(\rho_2)$, que não pode ser satisfeita para todo F .

Na seção seguinte, algumas medidas de entrelaçamento em sistemas multipartes serão apresentadas.

1.3. Entrelaçamento Multiparte

Nesta seção serão apresentadas duas medidas de entrelaçamento para sistemas multipartes: o entrelaçamento livre e o entrelaçamento residual.

1.3.1. Entrelaçamento Livre para Estados Quânticos Multipartes Puros

Será visto a seguir que um estado em um sistema multiparte puro pode ser escrito como um estado em um sistema biparte. Em sistemas bipartes algumas medidas de entrelaçamento já são conhecidas. Sendo assim, uma medida de entrelaçamento multiparte, pode ser obtida de uma medida de entrelaçamento biparte correspondente a cada agrupamento biparte.

Sejam A_1, A_2, \dots, A_n os subsistemas de um sistema de n partes de qubits. Como foi visto na Seção 1.1, um estado $|\psi\rangle$ em um sistema de n partes, é completamente separável se ele pode ser escrito sob a forma $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$, na qual $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle$ são os estados dos subsistemas A_1, A_2, \dots, A_n , respectivamente. Já um estado misto, ρ , de n partes é completamente separável, se $\rho = \sum_i p_i |\psi_1^i\rangle\langle\psi_1^i| \otimes \dots \otimes |\psi_n^i\rangle\langle\psi_n^i|$, onde $\sum_i p_i = 1$, $p_i > 0$ e $|\psi_j^i\rangle\langle\psi_j^i|$ são as matrizes densidade dos estados puros dos subsistemas de ρ , $j = 1, 2, \dots, n$. Para que estas definições sejam operacionais, será feita uma classificação dos estados multipartes, a partir de uma classificação para estados tripartes, que se encontra em [23]. Os estados tripartes, conforme eles sejam separáveis ou não, em relação aos seus qubits, podem ser escritos em uma das formas:

$$\rho = \sum_i p_i |\psi_1^i\rangle\langle\psi_1^i| \otimes |\psi_2^i\rangle\langle\psi_2^i| \otimes |\psi_3^i\rangle\langle\psi_3^i|, \quad (1.138)$$

$$\rho = \sum_i p_i |\psi_1^i\rangle\langle\psi_1^i| \otimes |\psi_{23}^i\rangle\langle\psi_{23}^i|, \quad (1.139)$$

$$\rho = \sum_i p_i |\psi_2^i\rangle\langle\psi_2^i| \otimes |\psi_{13}^i\rangle\langle\psi_{13}^i|, \quad (1.140)$$

$$\rho = \sum_i p_i |\psi_3^i\rangle\langle\psi_3^i| \otimes |\psi_{12}^i\rangle\langle\psi_{12}^i|, \quad (1.141)$$

sendo $|\psi_1^i\rangle$, $|\psi_2^i\rangle$ e $|\psi_3^i\rangle$ estados dos subsistemas 1, 2 e 3, respectivamente, e $|\psi_{12}^i\rangle$, $|\psi_{23}^i\rangle$ e $|\psi_{13}^i\rangle$ são estados de dois subsistemas juntos. Para os estados acima, tem-se as seguintes classes disjuntas:

1. Nesta classe, os estados não podem ser escritos em nenhuma das formas acima, isto é, são *estados completamente inseparáveis*;
2. (1-qubit separável) Esta classe é formada pelos estados biseparáveis com relação ao qubit A, ou seja, são os estados separáveis em relação ao primeiro qubit, porém não separável com relação aos outros dois. São, portanto, estados que podem ser escritos na forma (1.139), mas não podem ser escritos nas formas (1.140) ou (1.141).
3. (2-qubits separáveis) São os estados biseparáveis com relação aos qubits A e B, ou seja, são os estados separáveis em relação ao primeiro e segundo qubits, porém não separável com relação ao terceiro. São, portanto, os estados que podem ser escritos nas formas (1.139) e (1.140), porém não na forma (1.141).
4. (3-qubits separáveis) São os estados que podem ser escritos como (1.139), (1.140) e (1.141), porém não como (1.138).
5. (Estados completamente separáveis). São os estados que podem ser escritos na forma (1.138).

Para efeito de *entrelaçamento livre* (que é uma espécie de entrelaçamento em sistemas multipartes), não serão considerados estados que pertencem à classe 4, na classificação acima.

Nesse caso, só serão considerados estados multipartes que se reduzem a estados bipartes de dimensões arbitrárias, isto é, no agrupamento biparte resultante, o primeiro e segundo subsistemas devem ter dimensões maiores do que 2. Para isto, considere um estado $|\psi\rangle$, puro de n partes, em $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$. Se $\dim \mathcal{H}_i = d_i$, então $\dim \mathcal{H} = \prod_{i=1}^n d_i$. Portanto, um estado multiparte, tendo a dimensão de cada um dos subsistemas fixada, pode ser escrito como um estado mais simples em que cada subsistema do novo estado tem dimensão maior do que a dimensão dos subsistemas do estado original. Assim, se um estado puro de n partes, $|\psi\rangle$, em \mathcal{H} , é tal que $\dim \mathcal{H} = s$, então, usando a decomposição generalizada de Schmidt [25], escreve-se

$$|\psi\rangle_{A_1 A_2 A_3 \dots A_n} = \sum_i \sqrt{\lambda_i} |\psi_i^1\rangle \otimes |\psi_i^2\rangle, \quad (1.142)$$

onde $\{|\psi_A^i\rangle\}$ e $\{|\psi_B^i\rangle\}$ são bases dos espaços de Hilbert \mathcal{H}_A e \mathcal{H}_B , respectivamente, $\dim \mathcal{H}_A = n_1$, $\dim \mathcal{H}_B = n_2$ e $n_1 n_2 = s$. Logo, um estado puro, $|\psi\rangle$, de n partes pode sempre ser escrito na forma de um estado biparte, que corresponde ao agrupamento biparte do sistema de n partes, e $\{|\psi_A^i\rangle\}$ e $\{|\psi_B^i\rangle\}$ correspondem a cada grupo, respectivamente. De maneira análoga, um estado misto, $\rho = \sum_i p_i |\psi_{A_1 A_2 A_3 \dots A_n}^i\rangle \langle \psi_{A_1 A_2 A_3 \dots A_n}^i|$, de n partes, pode ser escrito da mesma forma, pois cada estado $|\psi_{A_1 A_2 A_3 \dots A_n}^i\rangle$ é um estado puro de todos os subsistemas de ρ . Como foi feito para os sistemas de três qubits e considerando agrupamentos bipartes de um sistema de n partes, têm-se as três classes seguintes:

$$\rho = \sum_i p_i |\psi_1^i\rangle \langle \psi_1^i| \otimes \dots \otimes |\psi_n^i\rangle \langle \psi_n^i| \quad (1.143)$$

$$\rho = \sum_i p_i |\psi_{\Sigma_j}^i\rangle \langle \psi_{\Sigma_j}^i| \otimes |\psi_{\Sigma - \Sigma_j}^i\rangle \langle \psi_{\Sigma - \Sigma_j}^i|, \quad (1.144)$$

$$\rho = \sum_i p_i |\psi_{A_1 A_2 A_3 \dots A_n}^i\rangle \langle \psi_{A_1 A_2 A_3 \dots A_n}^i|, \quad (1.145)$$

onde $\Sigma_j = X$, (i.e., Σ_j é qualquer um dos subsistemas $A_1, A_2, A_3, \dots, A_n$), $\{|\psi_{\Sigma_j}^i\rangle\}$ uma base para os estados dos subsistemas Σ_j , $\{|\psi_{\Sigma-\Sigma_j}^i\rangle\}$ uma base para os estados dos subsistemas restantes e $|\psi_{A_1 A_2 A_3 \dots A_n}^i\rangle$ representa os estados completamente inseparáveis de todos os n subsistemas. Para ficar claro como serão feitos os agrupamentos bipartes, note que se, por exemplo, o Σ_j representasse apenas um dos n subsistemas, ou seja, se o primeiro subsistema tivesse apenas uma parte, existiriam $\binom{n}{1} = n$ maneiras de escolher uma das n partes, ou seja, os n subsistemas de ρ podem ser divididos em dois grandes subsistemas, ρ_{Σ_j} e $\rho_{\Sigma-\Sigma_j}$, onde o primeiro inclui um dos n subsistemas ($\Sigma_j = A_1$, por exemplo) e o outro inclui os $n-1$ subsistemas restantes. Isto significa que

$$\rho = \sum_i p_i \rho_{\Sigma_j}^i \otimes \rho_{\Sigma-\Sigma_j}^i \quad (1.146)$$

é válida para $\Sigma_j = A_1$, ou seja, existem $\binom{n}{1} = n$ maneiras de formar o agrupamento biparte. Neste caso, o estado ρ é semiseparável. Entretanto, se não existir $\Sigma_j = X$ tal que (1.146) seja satisfeita, isto não necessariamente implica que ρ seja completamente inseparável. Por exemplo, para o estado de 4 qubits, $|\psi\rangle = |\psi^+\rangle \otimes |\psi^+\rangle$, $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, tem-se $|\psi\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$, que não é possível escrever como um produto, onde o estado do primeiro fator tenha apenas 1 qubit e, no entanto, ele não é completamente inseparável. O estado ρ pode ser incompletamente separável. Até aqui, o Σ_j denotou apenas um subsistema. Agora, para verificar a completa inseparabilidade do estado de n partes, melhora-se a condição acima, isto é, considera-se que o Σ_j possa denotar não mais apenas um dos n subsistemas e, sim, $\Sigma_j = A_1, A_2, \dots, A_{\lfloor n/2 \rfloor}$, onde o número de partes do primeiro estado em todos os possíveis agrupamentos bipartes, é $\lfloor \frac{n}{2} \rfloor = \frac{n}{2}$, se n é par, e $\lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$, se n é ímpar. Desta forma, uma condição de separabilidade mais forte que a dada em (1.146), é:

“O sistema de n partes ρ , o qual pode ser dividido em dois subsistemas, ρ_{Σ_j} e $\rho_{\Sigma-\Sigma_j}$, de

$\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{i}$ maneiras diferentes, é:

- (i) Semiseparável, se e somente se, (1.146) é satisfeita para todo Σ_j , $\Sigma_j \in \{A_1, A_2, \dots, A_{\lfloor n/2 \rfloor}\}$;
- (ii) Completamente inseparável, se somente se, não existir Σ_j , $\Sigma_j \in \{A_1, A_2, \dots, A_{\lfloor n/2 \rfloor}\}$, tal que (1.146) seja satisfeita.”

Usando a definição acima, a medida de entrelaçamento multipartes \bar{E} , proposta em [25], é dada por

$$\bar{E} = \sum_{j=1}^M \frac{1}{M} E_j, \quad (1.147)$$

sendo E_j o entrelaçamento biparte do j -ésimo agrupamento biparte e $M = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{i}$. Se o estado multiparte é puro (misto), então os estados bipartes, obtidos pelos agrupamentos bipartes correspondentes ao estado multiparte, são puros (mistos). Esta medida, para estados puros de dimensões arbitrárias, pode ser, por exemplo, a entropia reduzida de von Neumann, a concorrência, ou ainda, a negatividade.

1.3.2. Entrelaçamento Residual

Seja $\rho_{A_1 A_2 A_3 \dots A_n}$ a matriz densidade de um sistema de n partes, $A_1 A_2 A_3 \dots A_n$, com dimensões dos subsistemas A_i arbitrárias, ou seja, $\rho_{A_1 A_2 A_3 \dots A_n}$ é um estado em um espaço de Hilbert $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$, em que os \mathcal{H}_i têm dimensões finitas. Para estudar o *entrelaçamento residual* em tais sistemas, consideram-se os mesmos como se fossem estados tripartes do tipo $A_1 A_2 (A_3 \dots A_n)$, onde $A_3 \dots A_n$ é considerado como um único subsistema.

Para estados de n partes de qubits, vale a desigualdade generalizada de Coffman-Kundu-Wootters [28],

$$\tau(\rho_{A_1 A_2}) + \tau(\rho_{A_1 A_3}) + \dots + \tau(\rho_{A_1 A_n}) \leq \tau(\rho_{A_1(A_2 A_3 \dots A_n)}), \quad (1.148)$$

onde $\tau(\rho_{A_1(A_2 A_3 \dots A_n)})$ é o *tangle* que mede o entrelaçamento da bipartição $A_1 : A_2 A_3 \dots A_n$. No Capítulo 3 será visto a desigualdade CKW, $\mathcal{C}_{AB}^2(\rho) + \mathcal{C}_{AC}^2(\rho) \leq \mathcal{C}_{A(BC)}^2(\rho)$, para sistemas tripartes de qubits.

Para estados tripartes ρ , de dimensões arbitrárias, com subsistemas A , B e C , a desigualdade CKW, também é válida [26]

$$\mathcal{C}_{AB}^2(\rho) + \mathcal{C}_{AC}^2(\rho) \leq \mathcal{C}_{A(BC)}^2(\rho). \quad (1.149)$$

Para um estado misto ρ , biparte de dimensão arbitrária, a *concorrência* é dada por [29]

$$\mathcal{C}(\rho) = \inf_{\{p_i, |\psi_i\rangle\}} \sum_i p_i \mathcal{C}(|\psi_i\rangle), \quad (1.150)$$

para todos os ensembles $\{|\psi_i\rangle, p_i\}$ tais que $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, onde $p_i \geq 0$ e $\sum_i p_i = 1$. Se $|\psi\rangle$ é um produto de estados puros, então $\mathcal{C}(\rho) = 0$. Logo, ρ é separável, se e somente se, $\mathcal{C}(\rho) = 0$. Assim, ρ pode ser representada como uma combinação convexa do produto de estados como $\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B$, onde ρ_i^A e ρ_i^B são as matrizes densidade dos subsistemas A e B , respectivamente. Observe-se que em (1.149) o qubit A foi tomado como foco, sendo que a desigualdade continua verdadeira, independente da escolha do foco. Portanto, as outras desigualdades análogas, são:

$$\mathcal{C}_{BA}^2(\rho) + \mathcal{C}_{BC}^2(\rho) \leq \mathcal{C}_{B(AC)}^2(\rho), \quad (1.151)$$

$$\mathcal{C}_{CA}^2(\rho) + \mathcal{C}_{CB}^2(\rho) \leq \mathcal{C}_{C(AB)}^2(\rho). \quad (1.152)$$

Para cada uma dessas desigualdades se introduz uma quantidade τ correspondente a cada foco possível. Neste caso, obtêm-se as seguintes igualdades:

$$\tau_{A(BC)} + \mathcal{C}_{AB}^2(\rho) + \mathcal{C}_{AC}^2(\rho) = \mathcal{C}_{A(BC)}^2(\rho), \quad (1.153)$$

$$\tau_{B(AC)} + \mathcal{C}_{BA}^2(\rho) + \mathcal{C}_{BC}^2(\rho) = \mathcal{C}_{B(AC)}^2(\rho), \quad (1.154)$$

$$\tau_{C(AB)} + \mathcal{C}_{CA}^2(\rho) + \mathcal{C}_{CB}^2(\rho) = \mathcal{C}_{C(AB)}^2(\rho). \quad (1.155)$$

Em [26], $\tau_{A(BC)}$ representa uma propriedade global de 3 qubits que é usada para medir o entrelaçamento residual em um estado puro de 3 qubits de um sistema triparte. Aqui, já não é fácil dizer se $\tau_{A(BC)}$, $\tau_{B(AC)}$ e $\tau_{C(AB)}$ são iguais ou não, pois, τ_α , onde α corresponde a cada foco em $A(BC)$, $B(AC)$, $C(AB)$, inclui uma quantidade comum que representa uma espécie de propriedade global, independente das permutações dos qubits e que pode ser usada para medir o *entrelaçamento residual*. Não importando se os τ_α 's são iguais ou não, define-se o mínimo de τ_α como o *entrelaçamento residual*.

Agora será calculado o entrelaçamento residual em um estado $A_1A_2A_3\dots A_n$ de n partes de dimensões arbitrárias. Considere que o estado dado pode ser escrito como um estado triparte da forma $A_1A_2(A_3\dots A_n)$, onde $A_3\dots A_n$ é considerado como um único subsistema, ou seja, o estado original possui, agora, três partes: A_1 , A_2 e $A_3\dots A_n$. Aplicando a desigualdade CKW, para estados tripartes de dimensões arbitrárias, ao estado $A_1A_2(A_3\dots A_n)$, tem-se

$$\mathcal{C}_{A_1A_2}^2(\rho) + \mathcal{C}_{A_1(A_3A_4A_5\dots A_n)}^2(\rho) \leq \mathcal{C}_{A_1(A_2A_3A_4\dots A_n)}^2(\rho). \quad (1.156)$$

Considere, agora, o estado $A_1(A_3A_4A_5\dots A_n)$ em $\mathcal{C}_{A_1(A_3A_4A_5\dots A_n)}^2$, na desigualdade (1.156). Escreva o mesmo como um estado triparte da forma $A_1A_3(A_4A_5\dots A_n)$. Aplicando a desigualdade CKW, tem-se

$$\mathcal{C}_{A_1 A_3}^2(\rho) + \mathcal{C}_{A_1(A_4 A_5 \dots A_n)}^2(\rho) \leq \mathcal{C}_{A_1(A_3 A_4 A_5 \dots A_n)}^2(\rho). \quad (1.157)$$

De maneira análoga, para o estado $A_1(A_4 A_5 \dots A_n)$ em $\mathcal{C}_{A_1(A_4 A_5 \dots A_n)}^2$, na desigualdade (1.157), obtem-se

$$\mathcal{C}_{A_1 A_4}^2(\rho) + \mathcal{C}_{A_1(A_5 \dots A_n)}^2(\rho) \leq \mathcal{C}_{A_1(A_4 A_5 \dots A_n)}^2(\rho). \quad (1.158)$$

Continuando este processo, que é finito, chega-se à desigualdade de ordem $n-2$:

$$\mathcal{C}_{A_1 A_{n-1}}^2(\rho) + \mathcal{C}_{A_1 A_n}^2(\rho) \leq \mathcal{C}_{A_1(A_{n-1} A_n)}^2(\rho). \quad (1.159)$$

Somando, membro a membro, as $n-2$ desigualdades acima, obtém-se

$$\mathcal{C}_{A_1 A_2}^2(\rho) + \mathcal{C}_{A_1 A_3}^2(\rho) + \dots + \mathcal{C}_{A_1 A_n}^2(\rho) \leq \mathcal{C}_{A_1(A_2 A_3 A_4 \dots A_n)}^2(\rho). \quad (1.160)$$

De maneira análoga à construção feita na seção anterior, obtém-se

$$\tau_{A_1(A_2 A_3 \dots A_n)} + \mathcal{C}_{A_1 A_2}^2(\rho) + \mathcal{C}_{A_1 A_3}^2(\rho) + \dots + \mathcal{C}_{A_1 A_n}^2(\rho) = \mathcal{C}_{A_1(A_2 A_3 A_4 \dots A_n)}^2(\rho). \quad (1.161)$$

Observe-se que para chegar a (1.160) e (1.161), tomou-se como foco o subsistema A_1 . Se o foco é mudado, obtem-se as outras $n-1$ desigualdades restantes, análogas a (1.160), e as outras $n-1$ igualdades restantes, análogas a (1.161), correspondentes a cada foco, pois existem n desigualdades e n equações, análogas, correspondentes a cada foco. Até agora, o foco foi tomado como sendo apenas um dos subsistemas. É importante observar que $A_1 A_2$, $A_1 A_2 A_3, \dots$, considerados como se fossem um único subsistema, também podem ser usados como focos. Desta forma, cada foco pode ser representado por no máximo $\left\lceil \frac{n}{2} \right\rceil$ subsistemas,

e assim, existem $M = \sum_{i=1}^{\lceil n/2 \rceil} \binom{n}{i}$ desigualdades análogas à (1.160), considerando o foco como uma seqüência de subsistemas, onde cada seqüência é considerada como se fosse um único

subsistema, podendo ser formada por 1 subsistema, 2 subsistemas, e assim por diante, até no máximo $\left\lceil \frac{n}{2} \right\rceil$ subsistemas.

Seja τ_α (α pertencente ao conjunto de todos os focos possíveis) uma quantidade cujo valor mínimo será usado como o *entrelaçamento residual*, correspondente a cada foco, análogo ao caso dos sistemas tripartes. Então, existem M τ_α 's, independentes da escolha do foco (ou permutações). Como o *entrelaçamento residual* pode ser escrito de uma maneira geral, considerando o caso triparte, de forma mais rigorosa, tem-se a seguinte definição:

“O *entrelaçamento residual* $\tau_{A_1 A_2 A_3 \dots A_n}$ de um sistema de n partes $\rho_{A_1 A_2 A_3 \dots A_n}$ é definido por [26]

$$\tau_{A_1 A_2 A_3 \dots A_n} = \min \{ \tau_\alpha \mid \alpha = 1, 2, \dots, M \}, \quad (1.162)$$

onde α corresponde a todos os focos possíveis.”

A seguir, alguns exemplos que são apresentados em [26].

A. Como primeiro exemplo, considere $|\psi\rangle = \frac{1}{\sqrt{2}} \left(\underbrace{|00\dots 0\rangle}_{n \text{ qubits}} + \underbrace{|11\dots 1\rangle}_{n \text{ qubits}} \right)$ o estado *GHZ*

generalizado para n qubits. Como $\rho = |\psi\rangle\langle\psi|$, tem-se

$$\rho_{A_i} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \quad \rho_{A_i A_j} = \text{Tr}_{A_3 \dots A_n} (\rho) = \frac{1}{2} (|00\rangle\langle 00| + |11\rangle\langle 11|) = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}$$

e $\rho_{A_1 A_3} = \rho_{A_1 A_4} = \dots = \rho_{A_1 A_n} = \rho_{A_1 A_2}$. Como $\tilde{\rho} = (\sigma_y \otimes \sigma_y) \rho^* (\sigma_y \otimes \sigma_y)$, tem-se:

$$\tilde{\rho}_{A_1 A_3} = \tilde{\rho}_{A_1 A_4} = \dots = \tilde{\rho}_{A_1 A_n} = \tilde{\rho}_{A_1 A_2} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Daí,

$$\rho_{A_1 A_3} \tilde{\rho}_{A_1 A_3} = \rho_{A_1 A_4} \tilde{\rho}_{A_1 A_4} = \dots = \rho_{A_1 A_n} \tilde{\rho}_{A_1 A_n} = \rho_{A_1 A_2} \tilde{\rho}_{A_1 A_2} = \begin{pmatrix} 1/4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/4 \end{pmatrix}.$$

Portanto, $\mathcal{C}_{A_1 A_2}^2(\rho) = \dots = \mathcal{C}_{A_1 A_n}^2(\rho) = 0$ e $\mathcal{C}_{A_1(A_2 A_3 \dots A_n)}^2(\rho) = 1$, e assim, $\tau_{A_1 A_2 A_3 \dots A_n} = 1$.

B. O estado $|\psi\rangle = \alpha_1 |10\dots 0\rangle + \alpha_2 |01\dots 0\rangle + \alpha_3 |001\dots 0\rangle + \dots + \alpha_n |0000\dots 1\rangle$ de n qubits, que é um caso particular dos estados de n partes estudados aqui. Como $\mathcal{C}_{12}^2 + \mathcal{C}_{13}^2 + \dots + \mathcal{C}_{1n}^2 = \mathcal{C}_{1(2\dots n)}^2$, tem-se $\tau_{123\dots n} = 0$.

C. Seja $\rho = \sum_i \rho_1^i \otimes \rho_2^i$, um sistema de n partes em que ρ_1 corresponde a n_1 partes e ρ_2 corresponde a n_2 partes. Se as partes correspondentes a ρ_1 , por exemplo, são tomadas como foco, tem-se $\mathcal{C}_{n_1 n_2}^2(\rho) = 0$ (o mesmo ocorre se as partes de ρ_2 são tomadas como foco). Como $\tau \geq 0$ é o mínimo de todos os τ_α 's, então $\tau = 0$, neste caso.

1.4. Conclusão

Neste capítulo foi feita uma revisão de alguns critérios de separabilidade baseado na análise dos autovalores da transposta parcial da matriz densidade. Algumas medidas de entrelaçamento para estados bipartes, tripartes puros e multipartes puros, também foram apresentadas.

No capítulo 2, a seguir, mostra-se como calcular a negatividade de um estado quântico biparte a partir dos menores principais de matrizes Hermitianas.

CAPÍTULO 2

OS MENORES PRINCIPAIS DE MATRIZES HERMITIANAS E A NEGATIVIDADE

Resumo

Este capítulo tem como objetivo mostrar o cálculo da negatividade de estados quânticos bipartes de qubits a partir dos menores principais de matrizes Hermitianas.

2.1. Menores Principais de Matrizes Hermitianas

Uma matriz Hermitiana é positiva semidefinida, se todos os seus autovalores são não negativos. Mas, outro critério baseado na positividade semidefinida de uma matriz Hermitiana está relacionado aos seus menores principais. É o teorema de Sylvester [30].

2.1.1. Teorema de Sylvester

“Uma matriz Hermitiana ρ é positiva semidefinida se todos os seus menores principais são não negativos.”

Na verdade, para verificar a positividade semidefinida de uma matriz Hermitiana, é suficiente testar apenas os menores principais líderes.

Sendo A uma matriz $n \times n$, uma submatriz principal $k \times k$, $1 \leq k \leq n$, de A , é uma matriz que pode ser obtida de A , eliminando-se $n - k$ linhas e $n - k$ colunas. Em outras palavras, uma submatriz principal de A , é uma matriz cuja diagonal está contida na diagonal de A . Assim, um menor principal de ordem $k \times k$, de A , é o determinante de uma submatriz

principal $k \times k$. Seja M_j^k o j -ésimo menor principal de ordem k , com $1 \leq l \leq m$,

$m = \binom{n}{k} = \frac{n!}{k!(n-k)!}$. Isto significa que para matrizes $n \times n$, existem m menores principais

de ordem k , e o número total de menores principais é igual a $2^n - 1$. Desta forma, o polinômio característico da matriz A , é dado por

$$P(\lambda) = \lambda^n - S_1 \lambda^{n-1} + S_2 \lambda^{n-2} - S_3 \lambda^{n-3} + \dots + (-1)^k S_k \lambda^{n-k} + \dots + (-1)^n S_n, \quad (2.1)$$

onde $S_i = \sum_{j=1}^m M_j^i$ é a soma dos menores principais de ordem i , $1 \leq i \leq n$, de A . Já os menores

principais líderes de A , são os determinantes das submatrizes de A obtidas eliminando-se as últimas k colunas e as últimas k linhas, para $k = n-1, n-2, \dots, 0$.

Para uma matriz Hermitiana $\rho = (\rho_{ij})_{4 \times 4}$, $1 \leq i, j \leq 4$, os menores principais são:

Ordem 1:

$$M_1^1 = \rho_{11}, M_2^1 = \rho_{22}, M_3^1 = \rho_{33}, M_4^1 = \rho_{44}. \quad (2.2)$$

Ordem 2:

$$M_1^2 = \begin{vmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{vmatrix}, M_2^2 = \begin{vmatrix} \rho_{11} & \rho_{13} \\ \rho_{31} & \rho_{33} \end{vmatrix}, M_3^2 = \begin{vmatrix} \rho_{11} & \rho_{14} \\ \rho_{41} & \rho_{44} \end{vmatrix}, M_4^2 = \begin{vmatrix} \rho_{22} & \rho_{23} \\ \rho_{32} & \rho_{33} \end{vmatrix}, M_5^2 = \begin{vmatrix} \rho_{22} & \rho_{24} \\ \rho_{42} & \rho_{44} \end{vmatrix}, M_6^2 = \begin{vmatrix} \rho_{33} & \rho_{34} \\ \rho_{43} & \rho_{44} \end{vmatrix}. \quad (2.3)$$

Ordem 3:

$$M_1^3 = \begin{vmatrix} \rho_{11} & \rho_{12} & \rho_{13} \\ \rho_{21} & \rho_{22} & \rho_{23} \\ \rho_{31} & \rho_{32} & \rho_{33} \end{vmatrix}, M_2^3 = \begin{vmatrix} \rho_{11} & \rho_{13} & \rho_{14} \\ \rho_{31} & \rho_{33} & \rho_{34} \\ \rho_{41} & \rho_{43} & \rho_{44} \end{vmatrix}, M_3^3 = \begin{vmatrix} \rho_{11} & \rho_{13} & \rho_{14} \\ \rho_{31} & \rho_{33} & \rho_{34} \\ \rho_{41} & \rho_{43} & \rho_{44} \end{vmatrix}, M_4^3 = \begin{vmatrix} \rho_{22} & \rho_{23} & \rho_{24} \\ \rho_{32} & \rho_{33} & \rho_{34} \\ \rho_{42} & \rho_{43} & \rho_{44} \end{vmatrix}. \quad (2.4)$$

Ordem 4:

$$M_1^4 = \det(\rho). \quad (2.5)$$

Os menores principais líderes de $\rho = (\rho_{ij})_{4 \times 4}$ são:

$$\rho_{11}, \begin{vmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{vmatrix}, \begin{vmatrix} \rho_{11} & \rho_{12} & \rho_{13} \\ \rho_{21} & \rho_{22} & \rho_{23} \\ \rho_{31} & \rho_{32} & \rho_{33} \end{vmatrix}, \det(\rho). \quad (2.6)$$

Já foi visto acima, que a positividade semidefinida de uma matriz Hermitiana pode ser verificada usando-se o teorema de Sylvester. Veja, agora, o resultado da comparação do critério de separabilidade de Peres-Horodecki e o teorema de Sylvester.

2.1.2. Critério de Peres-Horodecki segundo o Teorema de Sylvester

“Se a transposta parcial da matriz densidade de um estado em $\mathbb{C}^2 \otimes \mathbb{C}^2$ e $\mathbb{C}^2 \otimes \mathbb{C}^3$ não tem menores principais negativos, então o estado é separável; caso contrário, o estado é entrelaçado.”

Neste caso, a fim de verificar a separabilidade dos estados bipartes, ao invés de calcular as raízes do polinômio característico da transposta parcial da matriz densidade, e checar se alguma delas é negativa, calculam-se os menores principais líderes da transposta parcial e verifica se um deles é negativo. Entretanto, diferentemente da ideia de negatividade, o valor absoluto da soma dos menores principais negativos não é uma medida de entrelaçamento.

Com o objetivo de estabelecer uma medida de entrelaçamento para sistemas de dois qubits, usando os menores principais, considere o polinômio em (2.1), com $n = 4$:

$$P(\lambda) = \lambda^4 - S_1\lambda^3 + S_2\lambda^2 - S_3\lambda + S_4. \quad (2.7)$$

O polinômio em (2.7) tem quatro raízes e, se o estado quântico ρ é entrelaçado, então uma delas é negativa. O valor absoluto dessa raiz é a negatividade dada em (1.136). Assim, a negatividade pode ser estabelecida como

$$\mathcal{N}(\rho) = -\min\{0, \lambda_{\min}\}, \quad (2.8)$$

em que λ_{\min} a raiz mínima de (2.7).

A seguir será apresentado o principal resultado do capítulo: uma relação entre a negatividade e os menores principais de uma matriz Hermitiana.

2.1.3. A Negatividade como Função dos Menores Principais

Seja ρ a matriz densidade de um estado quântico de um sistema biparte de dois qubits, cujo polinômio característico da transposta parcial de ρ é dado pela Eq. (2.7). Como a equação $\lambda^4 - S_1\lambda^3 + S_2\lambda^2 - S_3\lambda + S_4 = 0$ possui uma única raiz negativa, a saber

$$-\frac{1}{4}\left(-S_1 + \sqrt{S_1^2 - 4S_2 + 4y}\right) - \frac{1}{2}\sqrt{\frac{1}{4}\left(-S_1 + \sqrt{S_1^2 - 4S_2 + 4y}\right)^2 - 2\left(y - \sqrt{y^2 - 4S_4}\right)}, \quad (2.9)$$

tem-se que a negatividade como função dos menores principais da transposta parcial de ρ , é dada por

$$\mathcal{N}(\rho) = \frac{1}{2}\left(-S_1 + \sqrt{S_1^2 - 4S_2 + 4y}\right) + \sqrt{\frac{1}{4}\left(-S_1 + \sqrt{S_1^2 - 4S_2 + 4y}\right)^2 - 2\left(y - \sqrt{y^2 - 4S_4}\right)}, \quad (2.10)$$

em que

$$y = 2\sqrt{-Q} \cos\left(\frac{\theta}{3}\right) + \frac{S_2}{3}, \quad (2.11)$$

$$\theta = \cos^{-1}\left(\frac{R}{\sqrt{-Q^3}}\right), \quad (2.12)$$

$$Q = \frac{3(S_1S_3 - 4S_4) - S_2^2}{9}, \quad (2.13)$$

$$R = \frac{-9S_2(S_1S_3 - 4S_4) - 27(4S_2S_4 - S_3^2 - S_1^2S_4) + 2S_2^3}{54}. \quad (2.14)$$

Veja, agora, como ficam os Exemplos **A**, **B** e **C**, da Seção 1.1.2, Cap. 1, usando-se os menores principais.

A. Considere o estado

$$\rho = \frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2|, \quad (2.15)$$

em que $0 \leq p \leq 1$, $|\psi_1\rangle = a|00\rangle + b|11\rangle$ e $|\psi_2\rangle = a|01\rangle + b|10\rangle$, com $a, b > 0$ e $a^2 + b^2 = 1$. O polinômio característico de ρ^{T_B} é dado por

$$P(\lambda) = \lambda^4 - \lambda^3 + \frac{1}{4}\lambda^2. \quad (2.16)$$

Assim, $S_1 = 1$, $S_2 = \frac{1}{4}$, $S_3 = S_4 = 0$ e, daí $Q = -\frac{1}{144}$, $R = \frac{1}{64 \times 27}$, $\theta = 0$ e $y = \frac{1}{4}$.

Substituindo esses valores nas Eqs. (2.10) - (2.14), obtem-se $\mathcal{N}(\rho) = 0$.

B. Estado de Peres-Horodecki

Considere o estado

$$\rho = p|\psi_-\rangle\langle\psi_-| + (1-p)|00\rangle\langle 00|, \quad (2.17)$$

em que $0 \leq p \leq 1$ e $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. O polinômio característico de ρ^{T_B} é dado por

$$P(\lambda) = \lambda^4 - \lambda^3 + p(1-p)\lambda^2 - (1-2p)\frac{p^2}{4}\lambda - \frac{p^4}{16}. \quad (2.18)$$

Assim, $S_1 = 1$, $S_2 = p(1-p)$, $S_3 = (1-2p)\frac{p^2}{4}$ e $S_4 = -\frac{p^4}{16} = M_1^4 < 0$. Substituindo-se esses valores nas Eqs. (2.10) - (2.14), obtém-se $Q = -\frac{p^2(1-p)^2}{4 \times 9}$, $R = -\frac{p^3(1-p)^3}{4 \times 54}$, $\theta = \pi$ e $y = \frac{p(1-p)}{2}$. Portanto, $\mathcal{N}(\rho) = p - 1 + \sqrt{1 - 2p + 2p^2}$, com $0 \leq (p-1) + \sqrt{1 - 2p + 2p^2} \leq 1$.

C. Estado de Werner

Por fim, considere o estado

$$\rho = p|\psi_-\rangle\langle\psi_-| + (1-p)\frac{I}{4}, \quad (2.19)$$

em que $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ e I é a matriz identidade de elementos $\delta_{mn}\delta_{\mu\nu}$. O polinômio característico de ρ^{T_A} é

$$P(\lambda) = \lambda^4 - \lambda^3 + \frac{3}{8}(1-p^2)\lambda^2 - (1-2p)\left(\frac{1+p}{4}\right)^2\lambda + \frac{1-3p}{4}\left(\frac{1+p}{4}\right)^3. \quad (2.20)$$

Logo, $S_1 = 1$, $S_2 = \frac{3}{8}(1-p^2)$, $S_3 = (1-2p)\left(\frac{1+p}{4}\right)^2$ e $S_4 = \frac{1-3p}{4}\left(\frac{1+p}{4}\right)^3$, $\forall p$, $0 \leq p \leq 1$.

Daí, $Q = 0$ e $y = \frac{1-p^2}{8}$. Portanto, usando as Eqs. (2.10) - (2.14), obtém-se $\mathcal{N}(\rho) = \frac{3p-1}{2}$,

com $\frac{1}{3} < p \leq 1$. Se $0 \leq p \leq \frac{1}{3}$, então o estado ρ é separável, ou seja, $\mathcal{N}(\rho) = 0$.

2.2. Conclusão

Após a comparação do teorema de Sylvester e o critério de Peres-Horodecki, mostrou-se como calcular a negatividade de um estado biparte de dois qubits em função dos menores principais. A vantagem deste método, que utiliza o teorema de Sylvester, é que ao invés de calcular os autovalores da transposta parcial da matriz densidade, aqui se calculam os S_i , em (2.7), que são as somas dos menores principais de ordem 1, 2, 3 e 4 do polinômio

característico da transposta parcial da matriz densidade, sem necessariamente ter que calcular esses menores.

CAPÍTULO 3

ENTRELAÇAMENTO DE ESTADOS QUÂNTICOS TRIPARTES E QUADRIPTES PUROS DE QUBITS

Resumo

Neste capítulo, após uma revisão sobre o entrelaçamento residual em estados tripartes e quadripartes puros de qubits, π_3 e π_4 , respectivamente, mostra-se como este entrelaçamento pode ser medido pela negatividade, usando-se os menores principais. Especificamente, o resultado principal deste capítulo, mostra uma relação entre $\mathcal{N}_{X_l(X_1 \dots X_{l-1} X_{l+1} \dots X_n)}^2$ e $S_3\left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}}\right)$, para os casos $n = 3$ e $n = 4$, nas Seções 3.3 e 3.4.

3.1. Entrelaçamento Residual de Estados Tripartes Puros de Qubits com Tangles

Seja $|\psi\rangle$ um estado puro de três qubits, A , B e C e sejam $|\psi_1\rangle$, $|\psi_2\rangle$ e $|\psi_3\rangle$ estados dos subsistemas A , B e C , respectivamente. Segundo [24], $|\psi\rangle$ pode ser escrito como um dos estados pertencentes às seguintes classes inequivalentes:

1. A classe formada pelos estados $|\psi\rangle$ desentrelaçados (estados tripartes separáveis), isto é, $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle$;
2. A - BC dos estados bipartes separáveis, se $|\psi\rangle = |\psi_1\rangle \otimes |\psi_{23}\rangle$;
3. B - AC dos estados bipartes separáveis, se $|\psi\rangle = |\psi_2\rangle \otimes |\psi_{13}\rangle$;
4. C - AB dos estados bipartes separáveis, se $|\psi\rangle = |\psi_{12}\rangle \otimes |\psi_3\rangle$;

5. Estados da classe *GHZ*, com entrelaçamento genuíno triparte, da forma $|\psi\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\theta}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle$;
6. Estados da classe *W*, com entrelaçamento genuíno triparte, da forma $|\psi\rangle = \lambda_0|000\rangle + \lambda_1|001\rangle + \lambda_2|010\rangle + \lambda_3|100\rangle$.

Para quantificar o entrelaçamento existente nos estados pertencentes às classes acima, usam-se os *tangles*, representados por τ_{XY} , $\tau_{X(YZ)}$, $X, Y, Z \in \{A, B, C\}$, e τ_{ABC} ou τ_3 . Antes de calcular essas medidas, que estão relacionadas com a *concorrência*, dados os qubits *A*, *B* e *C*, como é a relação entre o entrelaçamento de *A* com *B* e o entrelaçamento de *A* com *C*? Já foi visto na Seção 1.3 que para um sistema com dois qubits, *A* e *B*, a *concorrência* é dada por $C_{AB} = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$, na qual $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$ são as raízes quadradas dos autovalores não nulos da matriz não Hermitiana $\rho_{AB}\tilde{\rho}_{AB}$. No caso do estado *AB* ser um estado puro, tem-se que $C_{AB} = 2\sqrt{\det \rho_A}$, onde $\rho_A = Tr_B(\rho_{AB})$.

Um estado puro em $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ (i.e., um estado triparte puro de três qubits), é representado por

$$|\psi\rangle = \sum_{i,j,k=0}^1 \alpha_{ijk} |ijk\rangle, \quad (3.1)$$

no qual $\alpha_{ijk} \in \mathbb{C}$, $i, j, k \in \mathbb{Z}_2$, tais que $\sum_{i,j,k=0}^1 |\alpha_{ijk}|^2 = 1$. A matriz densidade ρ associada ao estado $|\psi\rangle$ é $\rho = |\psi\rangle\langle\psi|$,

$$\rho = \sum_{i,j,k,i',j',k'=0}^1 \alpha_{ijk} \alpha_{i'j'k'}^* |ijk\rangle\langle i'j'k'|. \quad (3.2)$$

A fim de tornar a notação mais simples, o estado $|\psi\rangle$, em (3.1), pode ser escrito na forma:

$$|\psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle, \quad (3.3)$$

sendo $\alpha_i \in \mathbb{C}$, $i \in \mathbb{Z}$, $0 \leq i \leq 7$, tais que $\sum_{i=0}^7 |\alpha_i|^2 = 1$.

Segundo a referência [31], existe uma relação entre o entrelaçamento do qubit A com o qubit B e do entrelaçamento de A com o qubit C , conhecida como desigualdade CKW, dada por

$$C_{AB}^2 + C_{AC}^2 \leq C_{A(BC)}^2, \quad (3.4)$$

sendo

$$C_{AB}^2 = \text{Tr}(\rho_{AB} \tilde{\rho}_{AB}) - 2\lambda_1^{AB} \lambda_2^{AB}, \quad (3.5)$$

$$C_{AC}^2 = \text{Tr}(\rho_{AC} \tilde{\rho}_{AC}) - 2\lambda_1^{AC} \lambda_2^{AC}, \quad (3.6)$$

em que λ_i^{AB} e λ_i^{AC} , $i=1,2$, são as raízes quadradas dos dois autovalores não nulos de $\rho_{AB} \tilde{\rho}_{AB}$ e $\rho_{AC} \tilde{\rho}_{AC}$, respectivamente, $\rho_{AB} = \text{Tr}_C(\rho_{ABC})$ e $\rho_{AC} = \text{Tr}_B(\rho_{ABC})$ são estados mistos, e

$$C_{A(BC)}^2 = 4 \det \rho_A. \quad (3.7)$$

3.1.1. Exemplos

Considere o seguinte estado puro de três qubits, em que cada qubit corresponde, respectivamente, a cada um dos subsistemas A , B e C ,

$$|\psi\rangle = \alpha|100\rangle + \beta|010\rangle + \gamma|001\rangle. \quad (3.8)$$

Usando as Eqs. (3.5) - (3.7), encontra-se $C_{AB} = 2|\alpha\beta|$, $C_{AC} = 2|\alpha\gamma|$ e $C_{A(BC)} = 2|\alpha|\sqrt{|\beta|^2 + |\gamma|^2}$. Substituindo esses valores em (3.4), obtém-se $C_{AB}^2 + C_{AC}^2 = C_{A(BC)}^2$. Este exemplo mostra que para o estado (3.8), a desigualdade CKW torna-se uma igualdade.

Existem estados para os quais a desigualdade CKW é estrita. Por exemplo, para o estado $|\phi\rangle = \alpha|010\rangle + \beta|101\rangle$, tem-se $\mathcal{C}_{AB} = \mathcal{C}_{AC} = 0$ e $\mathcal{C}_{A(BC)} = 2|\alpha\beta|$. Substituindo-se esses valores em (3.4), encontra-se $\mathcal{C}_{AB}^2 + \mathcal{C}_{AC}^2 < \mathcal{C}_{A(BC)}^2$.

Dos exemplos acima, conclui-se que é de grande importância estudar a diferença $\mathcal{C}_{A(BC)}^2 - \mathcal{C}_{AB}^2 - \mathcal{C}_{AC}^2$, pois é nela que se encontra uma maneira de verificar que o entrelaçamento entre A e BC pode não ocorrer pelo entrelaçamento entre A e B e o entrelaçamento entre A e C , separadamente. Esta diferença, chamada de *entrelaçamento residual*, é dada por

$$\mathcal{C}_{A(BC)}^2 - \mathcal{C}_{AB}^2 - \mathcal{C}_{AC}^2 = 4|d_1 - 2d_2 + 4d_3|, \quad (3.9)$$

onde

$$d_1 = \alpha_0^2\alpha_7^2 + \alpha_1^2\alpha_6^2 + \alpha_2^2\alpha_5^2 + \alpha_3^2\alpha_4^2, \quad (3.10)$$

$$d_2 = \alpha_0\alpha_7\alpha_3\alpha_4 + \alpha_0\alpha_7\alpha_5\alpha_2 + \alpha_0\alpha_7\alpha_6\alpha_1 + \alpha_3\alpha_4\alpha_5\alpha_2 + \alpha_3\alpha_4\alpha_6\alpha_1 + \alpha_5\alpha_2\alpha_6\alpha_1, \quad (3.11)$$

$$d_3 = \alpha_0\alpha_6\alpha_5\alpha_3 + \alpha_7\alpha_1\alpha_2\alpha_4. \quad (3.12)$$

Observe que a diferença acima independe do qubit escolhido como foco. Por exemplo, nessa disposição o qubit A foi tomado como foco, como pode ser observado na Eq. (3.9). Se os qubits focos forem B e C tem-se, respectivamente,

$$\mathcal{C}_{B(CA)}^2 - \mathcal{C}_{BC}^2 - \mathcal{C}_{BA}^2 = 4|d_1 - 2d_2 + 4d_3|, \quad (3.13)$$

$$\mathcal{C}_{C(AB)}^2 - \mathcal{C}_{CA}^2 - \mathcal{C}_{CB}^2 = 4|d_1 - 2d_2 + 4d_3|. \quad (3.14)$$

Assim, o entrelaçamento residual medido com *concorrências* representa uma propriedade coletiva de três qubits que é invariante mediante permutações desses qubits. Ele mede essencialmente o entrelaçamento em estados com três qubits. Representando essa quantidade por τ_{ABC} , tem-se

$$\tau_{ABC} = C_{A(BC)}^2 - C_{AB}^2 - C_{AC}^2. \quad (3.15)$$

Isto significa que o entrelaçamento do qubit A com o par BC se manifesta de três maneiras: o entrelaçamento de A com B , o entrelaçamento de A com C e um entrelaçamento em três vias. E, essas três maneiras devem compartilhar o entrelaçamento total [31]. Por exemplo, para o estado GHZ , $|\varphi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $C_{AB} = C_{AC} = 0$ e $C_{A(BC)} = 1$. Logo, $\tau_{ABC} = 1$.

Para medir o entrelaçamento entre os qubits X e Y , usa-se o *tangle* τ_{XY} , que é definido por

$$\tau_{XY} = C_{XY}^2, \quad (3.16)$$

onde $C_{XY}^2 = \text{Tr}(\rho_{XY} \tilde{\rho}_{XY}) - 2\lambda_1^{XY} \lambda_2^{XY}$, $X, Y \in \{A, B, C\}$ e λ_i^{XY} , são as raízes quadradas dos dois autovalores não nulos de $\rho_{XY} \tilde{\rho}_{XY}$, $i = 1, 2$, de acordo com as Eqs. (3.5) e (3.6) [31].

O entrelaçamento do estado $X(YZ)$ pode ser calculado usando-se $\tau_{X(YZ)}$, definido por $\tau_{X(YZ)} = C_{X(YZ)}^2$, ou seja,

$$\tau_{X(YZ)} = 4 \det \rho_X, \quad (3.17)$$

sendo $\rho_X = \text{Tr}_{YZ}(\rho_{XYZ})$ a matriz densidade associada ao qubit X , onde $X, Y, Z \in \{A, B, C\}$ [31].

Agora, de $C_{XY}^2 + C_{XZ}^2 \leq C_{X(YZ)}^2$, $\tau_{XY} = C_{XY}^2$, e $\tau_{X(YZ)} = C_{X(YZ)}^2$, $X, Y, Z \in \{A, B, C\}$, segue que

$$\tau_{AB} + \tau_{AC} \leq \tau_{A(BC)}, \quad (3.18)$$

isto é, a soma do entrelaçamento de A com B e do entrelaçamento de A com C é, no máximo, o entrelaçamento entre A e o par BC . Se ocorrer $\tau_{AB} + \tau_{AC} = \tau_{A(BC)}$, define-se a classe dos estados tripartes maximamente entrelaçados aos pares; e, se ocorrer $\tau_{AB} + \tau_{AC} < \tau_{A(BC)}$, tem-se

o entrelaçamento residual (entrelaçamento em três vias), que é medido pelo *tangle* τ_{ABC} , ou seja,

$$\tau_{ABC} = \tau_{A(BC)} - \tau_{AB} - \tau_{AC} = \tau_{B(AC)} - \tau_{AB} - \tau_{BC} = \tau_{C(AB)} - \tau_{AC} - \tau_{BC}. \quad (3.19)$$

Quando os qubits A , B e C , em (3.18), estão em um estado maximamente entrelaçado, tem-se $\tau_{AB} = 1$, $\tau_{AC} = 0$ e, portanto, $\tau_{A(BC)} = 1$, transformando (3.18) numa igualdade. E, assim, A e B atingem seu entrelaçamento máximo, não compartilhando qualquer correlação quântica com C . Este resultado é conhecido como *monogamia de entrelaçamento* [32].

As duas próximas subseções são dedicadas à verificação dessas relações para estados das classes GHZ e W .

3.1.2. Estados da Classe GHZ

Considere os estados tripartes de qubits pertencentes à classe GHZ [34],

$$|\psi\rangle = \lambda_0 |000\rangle + \lambda_1 e^{i\theta} |100\rangle + \lambda_2 |101\rangle + \lambda_3 |110\rangle + \lambda_4 |111\rangle, \quad (3.20)$$

com $\lambda_i \geq 0$, $\sum_{i=0}^4 \lambda_i^2 = 1$ e $0 \leq \theta \leq \pi$. Usando-se as Eqs. (3.16) e (3.17), obtêm-se as seguintes relações

$$\tau_{AB} = 4(\lambda_0 \lambda_3)^2, \quad (3.21)$$

$$\tau_{AC} = 4(\lambda_0 \lambda_2)^2, \quad (3.22)$$

$$\tau_{BC} = 4|\lambda_1 e^{i\theta} \lambda_4 - \lambda_2 \lambda_3|^2, \quad (3.23)$$

$$\tau_A = 4\lambda_0^2 (\lambda_2^2 + \lambda_3^2 + \lambda_4^2), \quad (3.24)$$

$$\tau_B = 4 \left[\lambda_0^2 (\lambda_3^2 + \lambda_4^2) + |\lambda_1 e^{i\theta} \lambda_4 - \lambda_2 \lambda_3|^2 \right], \quad (3.25)$$

$$\tau_C = 4 \left[\lambda_0^2 (\lambda_2^2 + \lambda_4^2) + |\lambda_1 e^{i\theta} \lambda_4 - \lambda_2 \lambda_3|^2 \right]. \quad (3.26)$$

Substituindo (3.21) - (3.26) em (3.19), obtém-se

$$\tau_{ABC} = 4(\lambda_0 \lambda_4)^2. \quad (3.27)$$

Assim, para os estados da classe *GHZ*, a desigualdade CKW é estrita, ou seja, $\tau_{ABC}(GHZ) > 0$.

3.1.3. Estados da Classe *W*

Para os estados triparte da classe *W*,

$$|\psi\rangle = \lambda_0 |000\rangle + \lambda_1 |001\rangle + \lambda_2 |010\rangle + \lambda_3 |100\rangle, \quad (3.28)$$

com $\lambda_i \in \mathbb{C}$ e $\sum_{i=0}^3 |\lambda_i|^2 = 1$, tem-se

$$\tau_{AB} = 4 |\lambda_2 \lambda_3|^2, \quad (3.29)$$

$$\tau_{AC} = 4 |\lambda_1 \lambda_3|^2, \quad (3.30)$$

$$\tau_{BC} = 4 |\lambda_1 \lambda_2|^2, \quad (3.31)$$

$$\tau_A = 4 |\lambda_3|^2 (|\lambda_1|^2 + |\lambda_2|^2), \quad (3.32)$$

$$\tau_B = 4 |\lambda_2|^2 (|\lambda_1|^2 + |\lambda_3|^2), \quad (3.33)$$

$$\tau_C = 4|\lambda_1|^2 \left(|\lambda_2|^2 + |\lambda_3|^2 \right). \quad (3.34)$$

Substituindo (3.29) - (3.34) em (3.19), obtém-se

$$\tau_{ABC} = 0. \quad (3.35)$$

Neste caso, a desigualdade CKW torna-se uma igualdade, ou seja, $\tau_{ABC}(W) = 0$.

3.2. Entrelaçamento Residual de Estados Tripartes Puros de Qubits com Negatividade

Pode-se medir o entrelaçamento residual em estados tripartes puros de qubits através da negatividade usando-se o π_3 ou π_{ABC} , que será definida mais adiante. Antes, é importante observar que existe uma desigualdade semelhante à desigualdade CKW, chamada desigualdade monogâmica em termos da negatividade [35]

$$\mathcal{N}_{AB}^2 + \mathcal{N}_{AC}^2 \leq \mathcal{N}_{A(BC)}^2, \quad (3.36)$$

onde $\mathcal{N}_{AB} \leq \mathcal{C}_{AB}$, $\mathcal{N}_{AC} \leq \mathcal{C}_{AC}$ e $\mathcal{N}_{A(BC)} = \mathcal{C}_{A(BC)}$. Aqui, \mathcal{N}_{AB} e \mathcal{N}_{AC} são as negatividades dos estados mistos ρ_{AB} e ρ_{AC} , respectivamente. E, se AB é um estado puro de qubits, então $\mathcal{N}_{AB} = \mathcal{C}_{AB}$.

Na desigualdade (3.36), foi considerado como foco o qubit A. Mudando-se o foco, obtêm-se as demais desigualdades monogâmicas:

$$\mathcal{N}_{BA}^2 + \mathcal{N}_{BC}^2 \leq \mathcal{N}_{B(AC)}^2, \quad (3.37)$$

$$\mathcal{N}_{CA}^2 + \mathcal{N}_{CB}^2 \leq \mathcal{N}_{C(AB)}^2. \quad (3.38)$$

Tomando-se a diferença entre o primeiro e o segundo membros em cada equação acima, define-se uma nova medida de entrelaçamento envolvendo a negatividade:

$$\pi_{ABC} = \frac{1}{3}(\pi_A + \pi_B + \pi_C), \quad (3.39)$$

$$\pi_A = \mathcal{N}_{A(BC)}^2 - \mathcal{N}_{AB}^2 - \mathcal{N}_{AC}^2, \quad (3.40)$$

$$\pi_B = \mathcal{N}_{B(AC)}^2 - \mathcal{N}_{AB}^2 - \mathcal{N}_{BC}^2, \quad (3.41)$$

$$\pi_C = \mathcal{N}_{C(AB)}^2 - \mathcal{N}_{AC}^2 - \mathcal{N}_{BC}^2, \quad (3.42)$$

em que

$$\mathcal{N}_{X(YZ)}^2 = \mathcal{C}_{X(YZ)}^2 = 2\left(1 - \text{Tr}(\rho_X^2)\right) \quad (3.43)$$

é a negatividade do sistema composto pelo subsistema simples X e o sistema biparte YZ , enquanto $\mathcal{N}_{XY} = \text{Tr}\sqrt{\rho_{XY}^{T_A}(\rho_{XY}^{T_A})^\dagger} - 1$ é a negatividade do subsistema XY , $X, Y, Z \in \{A, B, C\}$.

Em geral, $\pi_A \neq \pi_B \neq \pi_C$ (isto significa que o entrelaçamento residual correspondente aos diferentes focos varia mediante permutação dos qubits), ao passo que π_{ABC} , em (3.39), não varia mediante permutação de qubits. Em [35], mostra-se que π_{ABC} é uma medida de entrelaçamento, isto é, π_{ABC} é invariante mediante operações LU , não cresce em média com $LOCC$ e é positiva. Para os estados das classes GHZ e W , π_3 é maior do que zero, isto é, para tais estados sempre existe o entrelaçamento em três vias.

3.2.1. Exemplos

Como primeiro exemplo, considere o estado da classe W , dado na Eq. (3.28), $\lambda_i \geq 0$.

Usando a Eq. 1.136, obtém-se

$$\mathcal{N}_{AB}^2 = 4\lambda_2^2\lambda_3^2 + 2\lambda_1^4 - 2\lambda_1^2\sqrt{\lambda_1^4 + 4\lambda_2^2\lambda_3^2},$$

$$\mathcal{N}_{AC}^2 = 4\lambda_1^2\lambda_2^2 + 2\lambda_3^4 - 2\lambda_3^2\sqrt{\lambda_3^4 + 4\lambda_1^2\lambda_2^2},$$

$$\mathcal{N}_{BC}^2 = 4\lambda_1^2\lambda_3^2 + 2\lambda_2^4 - 2\lambda_2^2\sqrt{\lambda_2^4 + 4\lambda_1^2\lambda_3^2}.$$

E, por (3.43), obtém-se

$$\mathcal{N}_{A(BC)}^2 = 4\lambda_3^2(\lambda_1^2 + \lambda_2^2), \quad \mathcal{N}_{B(AC)}^2 = 4\lambda_2^2(\lambda_1^2 + \lambda_3^2) \quad \text{e} \quad \mathcal{N}_{C(AB)}^2 = 4\lambda_1^2(\lambda_2^2 + \lambda_3^2).$$

Assim, de (3.39) - (3.42), segue que

$$\pi_3 = \frac{4}{3} \left(\lambda_1^2 \sqrt{\lambda_1^4 + 4\lambda_2^2\lambda_3^2} + \lambda_2^2 \sqrt{\lambda_2^4 + 4\lambda_1^2\lambda_3^2} + \lambda_3^2 \sqrt{\lambda_3^4 + 4\lambda_1^2\lambda_2^2} - \lambda_1^4 - \lambda_2^4 - \lambda_3^4 \right) > 0. \quad (3.44)$$

Portanto, $\pi_{ABC}(W) > \tau_{ABC}(W) = 0$, e assim, o τ_{ABC} não mede o estado W , enquanto π_{ABC} mede W .

Para os estados da classe GHZ , (3.20), tem-se $\pi_{ABC}(GHZ) \geq \tau_{ABC}(GHZ) > 0$, enquanto que para os estados $|\Phi\rangle_{ABC}$ pertencentes às classes que não incluem os estados GHZ e W , ou seja, estados do tipo $A-B-C$, $A(BC)$, $B(AC)$ ou $C(AB)$, tem-se $\pi_{ABC}(\Phi) = \tau_{ABC}(\Phi) = 0$.

Nas seções 3.4 e 3.5, será calculada a negatividade para estados puros de 3 e 4 qubits, usando-se um novo recurso: os menores principais da transposta parcial da matriz densidade desses estados. Antes, será obtida uma expressão para a soma dos menores principais de ordem 3 da transposta parcial de uma matriz densidade de n qubits.

3.3. Menores Principais de Ordem 3 de $\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}}$

Para um estado puro de n qubits, o polinômio característico da matriz $\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}}$, $N \times N$, $N = 2^n$, pode ser escrito como

$$P(\lambda) = \lambda^N + \alpha_{N-1}\lambda^{N-1} + \alpha_{N-2}\lambda^{N-2} + \alpha_{N-3}\lambda^{N-3} + \dots + \alpha_{N-k}\lambda^{N-k} + \dots + \alpha_0, \quad (3.45)$$

ou ainda,

$$P(\lambda) = \lambda^N - S_1\lambda^{N-1} + S_2\lambda^{N-2} - S_3\lambda^{N-3} + \dots + (-1)^k S_k\lambda^{N-k} + \dots + (-1)^N S_N, \quad (3.46)$$

em que

$$\alpha_{N-1} = -Tr \left[\left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right) D_1 \right], D_1 = I_N, \quad (3.47)$$

$$\alpha_{N-i} = -\frac{1}{i} Tr \left[\left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right) D_i \right], \quad (3.48)$$

com

$$D_i = \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right) D_{i-1} + \alpha_{N-i+1} I_N, i \geq 2. \quad (3.49)$$

De uma comparação direta entre as Eqs. (3.45) e (3.46), resulta

$$\alpha_{N-3} = -S_3. \quad (3.50)$$

De (3.49) segue que

$$D_2 = \rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} + \alpha_{N-1} I_N, D_3 = \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right)^2 + \alpha_{N-1} \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right) + \alpha_{N-2} I_N \text{ e}$$

$$\left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right) D_3 = \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right)^3 + \alpha_{N-1} \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right)^2 + \alpha_{N-2} \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right).$$

Por (3.47), $\alpha_{N-1} = -Tr \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right) = -S_1 = -1$, logo $Tr \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right) = 1$. Como

$$Tr \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right)^2 = 1, \text{ tem-se } Tr \left(\left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right) D_3 \right) = Tr \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right)^3 - 1.$$

Assim,

$$\alpha_{N-3} = \frac{1}{3} \left(1 - Tr \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right)^3 \right). \quad (3.51)$$

Substituindo $\alpha_{N-3} = -S_3$ em (3.51), tem-se

$$S_3 = -\frac{1}{3} \left(1 - Tr \left(\rho_{X_1 \dots X_{l-1} X_l X_{l+1} \dots X_n}^{T_{X_l}} \right)^3 \right). \quad (3.52)$$

Na próxima seção, será apresentado o primeiro resultado do capítulo: a relação entre a negatividade de um estado puro de 3 qubits e a soma dos menores principais de ordem 3 da transposta parcial da matriz densidade do estado.

3.4. A Negatividade para Estados Tripartes Puros de Qubits

O estado puro triparte de qubits A, B, C , em (3.1), com os índices das amplitudes na base 10, pode ser escrito como

$$|\psi\rangle = \sum_{i=0}^7 \alpha_i |i\rangle, \quad (3.53)$$

em que $\alpha_i \in \mathbb{C}$ e $\sum_{i=0}^7 |\alpha_i|^2 = 1$. Assim, $\rho_{XYZ} = |\psi\rangle\langle\psi|$ e $\rho_{XYZ}^{T_X}$ é a transposta parcial de ρ_{XYZ} em relação ao subsistema X .

A seguir será calculada a negatividade do estado ρ_{XYZ} em termos das amplitudes do estado $|\psi\rangle$.

3.4.1. A Negatividade de ρ_{XYZ}

Determinando-se a matriz ρ_X^2 , após alguns cálculos, obtém-se o valor de $1 - \text{Tr}(\rho_X^2)$.

Como $\mathcal{N}_{X(YZ)}^2 = 2(1 - \text{Tr}(\rho_X^2))$, $X, Y, Z \in \{A, B, C\}$, tem-se

$$\mathcal{N}_{A(BC)}^2 = 4 \times \left(\begin{aligned} &|\alpha_0\alpha_5 - \alpha_1\alpha_4|^2 + |\alpha_0\alpha_6 - \alpha_2\alpha_4|^2 + |\alpha_0\alpha_7 - \alpha_3\alpha_4|^2 + \\ &+ |\alpha_1\alpha_6 - \alpha_2\alpha_5|^2 + |\alpha_1\alpha_7 - \alpha_3\alpha_5|^2 + |\alpha_2\alpha_7 - \alpha_3\alpha_6|^2 \end{aligned} \right), \quad (3.54)$$

$$\mathcal{N}_{B(AC)}^2 = 4 \times \left(\begin{aligned} &|\alpha_0\alpha_3 - \alpha_1\alpha_2|^2 + |\alpha_0\alpha_6 - \alpha_4\alpha_2|^2 + |\alpha_0\alpha_7 - \alpha_5\alpha_2|^2 + \\ &+ |\alpha_1\alpha_6 - \alpha_4\alpha_3|^2 + |\alpha_1\alpha_7 - \alpha_5\alpha_3|^2 + |\alpha_4\alpha_7 - \alpha_5\alpha_6|^2 \end{aligned} \right), \quad (3.55)$$

$$\mathcal{N}_{C(AB)}^2 = 4 \times \left(\begin{aligned} &|\alpha_0\alpha_3 - \alpha_2\alpha_1|^2 + |\alpha_0\alpha_5 - \alpha_4\alpha_1|^2 + |\alpha_0\alpha_7 - \alpha_6\alpha_1|^2 + \\ &+ |\alpha_2\alpha_5 - \alpha_4\alpha_3|^2 + |\alpha_2\alpha_7 - \alpha_6\alpha_3|^2 + |\alpha_4\alpha_7 - \alpha_6\alpha_5|^2 \end{aligned} \right). \quad (3.56)$$

As Eqs (3.54) - (3.56), com os índices das amplitudes na base 2, são escritas, respectivamente, como

$$\mathcal{N}_{A(BC)}^2 = 4 \times \left(\sum_{\substack{jk \neq j'k', j'k' \neq 00}} |\alpha_{0jk} \alpha_{1j'k'} - \alpha_{0j'k'} \alpha_{1jk}|^2 \right), \quad (3.57)$$

$$\mathcal{N}_{B(AC)}^2 = 4 \times \left(\sum_{\substack{ik \neq i'k', i'k' \neq 00}} |\alpha_{i0k} \alpha_{i'1k'} - \alpha_{i'0k'} \alpha_{i1k}|^2 \right), \quad (3.58)$$

$$\mathcal{N}_{C(AB)}^2 = 4 \times \left(\sum_{\substack{ij \neq i'j', i'j' \neq 00}} |\alpha_{ij0} \alpha_{i'j'1} - \alpha_{i'j'0} \alpha_{ij1}|^2 \right). \quad (3.59)$$

Agora, observe que o número total de menores principais de ordem 3 da matriz $\rho_{XYZ}^{T_x}$, é igual a $\binom{8}{3} = 56$, sendo que o número de menores principais de ordem 3, nulos, de $\rho_{XYZ}^{T_x}$, é igual a $2 \times \binom{4}{3} = 8$. Assim, o número de menores principais, não nulos, de $\rho_{XYZ}^{T_x}$, é igual a $\binom{8}{3} - 2 \times \binom{4}{3} = 48$. Para a matriz $\rho_{ABC}^{T_A}$, cada um desses menores pode ser escrito como

$$-|\alpha_{ijk}|^2 \times \left(\sum_{\substack{jk \neq j'k', j'k' \neq 00}} |\alpha_{0jk} \alpha_{1j'k'} - \alpha_{0j'k'} \alpha_{1jk}|^2 \right), \quad (3.60)$$

$i, j, k \in \{0,1\}$. A quantidade de somas do tipo (3.60) é igual a 8 e cada uma dessas somas possui 6 parcelas. Somando, membro a membro, essas 8 igualdades, obtém-se

$$S_3(\rho_{ABC}^{T_A}) = - \sum_{\substack{jk \neq j'k', j'k' \neq 00}} |\alpha_{0jk} \alpha_{1j'k'} - \alpha_{0j'k'} \alpha_{1jk}|^2. \quad (3.61)$$

De modo análogo, obtém-se para $S_3(\rho_{ABC}^{T_B})$ e $S_3(\rho_{ABC}^{T_C})$, as expressões:

$$S_3(\rho_{ABC}^{T_B}) = - \sum_{\overline{ik \neq i'k'}, \overline{i'k' \neq 00}} |\alpha_{i0k} \alpha_{i'1k'} - \alpha_{i'0k'} \alpha_{i1k}|^2, \quad (3.62)$$

$$S_3(\rho_{ABC}^{T_C}) = - \sum_{\overline{ij \neq i'j'}, \overline{i'j' \neq 00}} |\alpha_{ij0} \alpha_{i'j'1} - \alpha_{i'j'0} \alpha_{ij1}|^2. \quad (3.63)$$

A notação \overline{ab} , usada em (3.57) - (3.63), significa que $\overline{ab} = a \times 2^1 + b \times 2^0$.

De (3.54) - (3.56) e (3.61) - (3.63), e considerando os menores principais, se $\rho_{XYZ}^{T_X} = \sum_{ijk, i'j'k'} \alpha_{ijk} \alpha_{i'j'k'}^* |i'jk\rangle \langle ij'k'|$ é a transposta parcial da matriz densidade ρ_{XYZ} com relação ao subsistema X , então

$$\mathcal{N}_{X(YZ)}^2 = -4S_3(\rho_{XYZ}^{T_X}), \quad (3.64)$$

em que

$$S_3(\rho_{XYZ}^{T_X}) = -\frac{1}{3} \left(1 - \text{Tr}(\rho_{XYZ}^{T_X})^3 \right), \quad (3.65)$$

é a soma dos menores principais de ordem 3 da transposta parcial $\rho_{XYZ}^{T_X}$, em relação ao subsistema X , com $X, Y, Z \in \{A, B, C\}$, $X \neq Y \neq Z$.

Nos exemplos a seguir, será calculada a negatividade para os estados puros de três qubits W e GHZ , usando-se os resultados obtidos acima.

3.4.2. Exemplos

A. Inicialmente, considere estados puros tripartes pertencentes à classe W ,

$$|\psi\rangle = \lambda_0 |000\rangle + \lambda_1 |001\rangle + \lambda_2 |010\rangle + \lambda_3 |100\rangle, \quad (3.66)$$

com $\lambda_i \geq 0$ e $\sum_{i=0}^3 \lambda_i^2 = 1$. Para os estados (3.28) e $X = A$, $Y = B$ e $Z = C$ em (3.54), depois de alguns cálculos, pode-se achar:

$$\mathcal{N}_{A(BC)}^2 = 2\left(1 - \text{Tr}(\rho_A^2)\right) = 4\lambda_3^2(\lambda_1^2 + \lambda_2^2), \quad (3.67)$$

enquanto que

$$S_3(\rho_{ABC}^{T_A}) = -\lambda_3^2(\lambda_1^2 + \lambda_2^2). \quad (3.68)$$

Substituindo (3.68) em (3.67), (3.64) é obtida.

B. Agora, para os estados puros pertencentes à classe *GHZ* [31],

$$|\psi\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\theta}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle, \quad (3.69)$$

com $\sum_{i=0}^4 |\lambda_i|^2 = 1$ e $0 \leq \theta \leq \pi$. Para os estados (3.20) e $X = A$, $Y = B$ e $Z = C$ em (3.55), depois de alguns cálculos, pode-se achar

$$\mathcal{N}_{B(AC)}^2 = 2\left(1 - \text{Tr}(\rho_B^2)\right) = 4\left[\lambda_0^2(\lambda_3^2 + \lambda_4^2) + \lambda_1^2\lambda_4^2 + \lambda_2^2\lambda_3^2 - 2\lambda_1\lambda_2\lambda_3\lambda_4 \cos(\theta)\right], \quad (3.70)$$

enquanto que

$$S_3(\rho_{ABC}^{T_B}) = -\lambda_0^2(\lambda_3^2 + \lambda_4^2) - \left[\lambda_1^2\lambda_4^2 + \lambda_2^2\lambda_3^2 - 2\lambda_1\lambda_2\lambda_3\lambda_4 \cos(\theta)\right]. \quad (3.71)$$

Substituindo (3.71) em (3.70), (3.64) é obtida.

Portanto, a medida de entrelaçamento residual dada em (3.39) - (3.42), pode ser calculada usando os menores principais de acordo com (3.64), (3.65) e (2.10) - (2.14).

3.5. A Negatividade e os Menores Principais para Estados Quadripartes Puros de Qubits

Agora, os menores principais serão usados para calcular a negatividade em estados quadripartes puros de qubits.

Um estado puro quadriparte de qubits, tem a forma

$$|\psi\rangle = \sum_{i,j,k,l=0}^1 \alpha_{ijkl} |ijkl\rangle, \quad (3.72)$$

sendo que $\alpha_{ijkl} \in \mathbb{C}$ e $\sum_{i,j,k,l=0}^1 |\alpha_{ijkl}|^2 = 1$. Colocando-se os índices das amplitudes do estado em (3.72) na base 10, tem-se

$$|\psi\rangle = \alpha_0 |0000\rangle + \alpha_1 |0001\rangle + \alpha_2 |0010\rangle + \alpha_3 |0011\rangle + \alpha_4 |0100\rangle + \alpha_5 |0101\rangle + \alpha_6 |0110\rangle + \alpha_7 |0111\rangle + \alpha_8 |1000\rangle + \alpha_9 |1001\rangle + \alpha_{10} |1010\rangle + \alpha_{11} |1011\rangle + \alpha_{12} |1100\rangle + \alpha_{13} |1101\rangle + \alpha_{14} |1110\rangle + \alpha_{15} |1111\rangle, \quad (3.73)$$

em que os $\alpha_i \in \mathbb{C}$, com $i \in \mathbb{Z}$ e $0 \leq i \leq 15$, são tais que $\sum_{i=0}^{15} |\alpha_i|^2 = 1$.

O entrelaçamento em quatro vias pode ser medido usando π_4 ou π_{ABCD} , uma extensão de π_3 , definida em [36], como

$$\pi_4 = \sqrt[4]{\pi_A \pi_B \pi_C \pi_D}, \quad (3.74)$$

sendo

$$\pi_A = \mathcal{N}_{A(BCD)}^2 - \mathcal{N}_{AB}^2 - \mathcal{N}_{AC}^2 - \mathcal{N}_{AD}^2 \quad (3.75)$$

$$\pi_B = \mathcal{N}_{B(ACD)}^2 - \mathcal{N}_{AB}^2 - \mathcal{N}_{BC}^2 - \mathcal{N}_{BD}^2 \quad (3.76)$$

$$\pi_C = \mathcal{N}_{C(ABD)}^2 - \mathcal{N}_{AC}^2 - \mathcal{N}_{BC}^2 - \mathcal{N}_{CD}^2 \quad (3.77)$$

$$\pi_D = \mathcal{N}_{D(ABC)}^2 - \mathcal{N}_{AD}^2 - \mathcal{N}_{BD}^2 - \mathcal{N}_{CD}^2. \quad (3.78)$$

Como se vê, o π_3 usa a média aritmética, enquanto o π_4 usa a média geométrica. Essa mudança se deve ao fato de que a média aritmética em π_4 leva a resultados errados, ou seja, estados sem entrelaçamento em 4 vias, tem π_4 maior do que zero se for usada a média aritmética. Para mais detalhes sobre a medida de entrelaçamento π_4 , como uma extensão de π_3 , pode-se consultar as Referências [36,37].

3.5.1. A Negatividade de ρ_{WXYZ}

Determinando-se a matriz ρ_X^2 , após alguns cálculos, determina-se o valor de $1 - \text{Tr}(\rho_X^2)$. Como $\mathcal{N}_{W(XYZ)}^2 = 2(1 - \text{Tr}(\rho_W^2))$, $W, X, Y, Z \in \{A, B, C, D\}$, tem-se

$$\mathcal{N}_{A(BCD)}^2 = 4 \times \left\{ \begin{array}{l} |\alpha_0\alpha_9 - \alpha_1\alpha_8|^2 + |\alpha_0\alpha_{10} - \alpha_2\alpha_8|^2 + |\alpha_0\alpha_{11} - \alpha_3\alpha_8|^2 + |\alpha_0\alpha_{12} - \alpha_4\alpha_8|^2 + \\ + |\alpha_0\alpha_{13} - \alpha_5\alpha_8|^2 + |\alpha_0\alpha_{14} - \alpha_6\alpha_8|^2 + |\alpha_0\alpha_{15} - \alpha_7\alpha_8|^2 + |\alpha_1\alpha_{10} - \alpha_2\alpha_9|^2 + \\ + |\alpha_1\alpha_{11} - \alpha_3\alpha_9|^2 + |\alpha_1\alpha_{12} - \alpha_4\alpha_9|^2 + |\alpha_1\alpha_{13} - \alpha_5\alpha_9|^2 + |\alpha_1\alpha_{14} - \alpha_6\alpha_9|^2 + \\ + |\alpha_1\alpha_{15} - \alpha_7\alpha_9|^2 + |\alpha_2\alpha_{12} - \alpha_4\alpha_{10}|^2 + |\alpha_2\alpha_{13} - \alpha_5\alpha_{10}|^2 + |\alpha_2\alpha_{14} - \alpha_6\alpha_{10}|^2 + \\ + |\alpha_2\alpha_{15} - \alpha_7\alpha_{10}|^2 + |\alpha_3\alpha_{10} - \alpha_2\alpha_{11}|^2 + |\alpha_3\alpha_{12} - \alpha_4\alpha_{11}|^2 + |\alpha_3\alpha_{13} - \alpha_5\alpha_{11}|^2 + \\ + |\alpha_3\alpha_{14} - \alpha_6\alpha_{11}|^2 + |\alpha_7\alpha_{11} - \alpha_3\alpha_{15}|^2 + |\alpha_4\alpha_{13} - \alpha_5\alpha_{12}|^2 + |\alpha_4\alpha_{14} - \alpha_6\alpha_{12}|^2 + \\ + |\alpha_4\alpha_{15} - \alpha_7\alpha_{12}|^2 + |\alpha_5\alpha_{14} - \alpha_6\alpha_{13}|^2 + |\alpha_5\alpha_{15} - \alpha_7\alpha_{13}|^2 + |\alpha_6\alpha_{15} - \alpha_7\alpha_{14}|^2 \end{array} \right\}, \quad (3.79)$$

$$\mathcal{N}_{B(ACD)}^2 = 4 \times \left\{ \begin{array}{l} |\alpha_0\alpha_5 - \alpha_1\alpha_4|^2 + |\alpha_0\alpha_6 - \alpha_2\alpha_4|^2 + |\alpha_0\alpha_7 - \alpha_3\alpha_4|^2 + |\alpha_0\alpha_{12} - \alpha_8\alpha_4|^2 + \\ + |\alpha_0\alpha_{13} - \alpha_9\alpha_4|^2 + |\alpha_0\alpha_{14} - \alpha_{10}\alpha_4|^2 + |\alpha_0\alpha_{15} - \alpha_{11}\alpha_4|^2 + |\alpha_1\alpha_6 - \alpha_2\alpha_5|^2 + \\ + |\alpha_1\alpha_7 - \alpha_3\alpha_5|^2 + |\alpha_1\alpha_{12} - \alpha_8\alpha_5|^2 + |\alpha_1\alpha_{13} - \alpha_9\alpha_5|^2 + |\alpha_1\alpha_{14} - \alpha_{10}\alpha_5|^2 + \\ + |\alpha_1\alpha_{15} - \alpha_{11}\alpha_5|^2 + |\alpha_2\alpha_7 - \alpha_3\alpha_6|^2 + |\alpha_2\alpha_{12} - \alpha_8\alpha_6|^2 + |\alpha_2\alpha_{13} - \alpha_9\alpha_6|^2 + \\ + |\alpha_2\alpha_{14} - \alpha_{10}\alpha_6|^2 + |\alpha_2\alpha_{15} - \alpha_{11}\alpha_6|^2 + |\alpha_3\alpha_{12} - \alpha_8\alpha_7|^2 + |\alpha_3\alpha_{13} - \alpha_9\alpha_7|^2 + \\ + |\alpha_3\alpha_{14} - \alpha_{10}\alpha_7|^2 + |\alpha_3\alpha_{15} - \alpha_{11}\alpha_7|^2 + |\alpha_8\alpha_{13} - \alpha_9\alpha_{12}|^2 + |\alpha_8\alpha_{14} - \alpha_{10}\alpha_{12}|^2 + \\ + |\alpha_8\alpha_{15} - \alpha_{11}\alpha_{12}|^2 + |\alpha_9\alpha_{14} - \alpha_{10}\alpha_{13}|^2 + |\alpha_9\alpha_{15} - \alpha_{11}\alpha_{13}|^2 + |\alpha_{10}\alpha_{15} - \alpha_{11}\alpha_{14}|^2 \end{array} \right\}, \quad (3.80)$$

$$\mathcal{N}_{C(ABD)}^2 = 4 \times \left\{ \begin{array}{l} |\alpha_0\alpha_3 - \alpha_1\alpha_2|^2 + |\alpha_0\alpha_6 - \alpha_4\alpha_2|^2 + |\alpha_0\alpha_7 - \alpha_5\alpha_2|^2 + |\alpha_0\alpha_{10} - \alpha_8\alpha_2|^2 + \\ + |\alpha_0\alpha_{11} - \alpha_9\alpha_2|^2 + |\alpha_0\alpha_{14} - \alpha_{12}\alpha_2|^2 + |\alpha_0\alpha_{15} - \alpha_{13}\alpha_2|^2 + |\alpha_1\alpha_6 - \alpha_4\alpha_3|^2 + \\ + |\alpha_1\alpha_7 - \alpha_5\alpha_3|^2 + |\alpha_1\alpha_{10} - \alpha_8\alpha_3|^2 + |\alpha_1\alpha_{11} - \alpha_9\alpha_3|^2 + |\alpha_1\alpha_{14} - \alpha_{12}\alpha_3|^2 + \\ + |\alpha_1\alpha_{15} - \alpha_{13}\alpha_3|^2 + |\alpha_4\alpha_7 - \alpha_5\alpha_6|^2 + |\alpha_4\alpha_{10} - \alpha_8\alpha_6|^2 + |\alpha_4\alpha_{11} - \alpha_9\alpha_6|^2 + \\ + |\alpha_4\alpha_{14} - \alpha_{12}\alpha_6|^2 + |\alpha_4\alpha_{15} - \alpha_{13}\alpha_6|^2 + |\alpha_5\alpha_{10} - \alpha_8\alpha_7|^2 + |\alpha_5\alpha_{11} - \alpha_9\alpha_7|^2 + \\ + |\alpha_5\alpha_{14} - \alpha_{12}\alpha_7|^2 + |\alpha_5\alpha_{15} - \alpha_{13}\alpha_7|^2 + |\alpha_8\alpha_{11} - \alpha_9\alpha_{10}|^2 + |\alpha_8\alpha_{14} - \alpha_{12}\alpha_{10}|^2 + \\ + |\alpha_8\alpha_{15} - \alpha_{13}\alpha_{10}|^2 + |\alpha_9\alpha_{14} - \alpha_{12}\alpha_{11}|^2 + |\alpha_9\alpha_{15} - \alpha_{13}\alpha_{11}|^2 + |\alpha_{12}\alpha_{15} - \alpha_{13}\alpha_{14}|^2 \end{array} \right\}, \quad (3.81)$$

$$\mathcal{N}_{D(ABC)}^2 = 4 \times \left\{ \begin{array}{l} |\alpha_0\alpha_3 - \alpha_2\alpha_1|^2 + |\alpha_0\alpha_5 - \alpha_4\alpha_1|^2 + |\alpha_0\alpha_7 - \alpha_6\alpha_1|^2 + |\alpha_0\alpha_9 - \alpha_8\alpha_1|^2 + \\ + |\alpha_0\alpha_{11} - \alpha_{10}\alpha_1|^2 + |\alpha_0\alpha_{13} - \alpha_{12}\alpha_1|^2 + |\alpha_0\alpha_{15} - \alpha_{14}\alpha_1|^2 + |\alpha_2\alpha_5 - \alpha_4\alpha_3|^2 + \\ + |\alpha_2\alpha_7 - \alpha_6\alpha_3|^2 + |\alpha_2\alpha_9 - \alpha_8\alpha_3|^2 + |\alpha_2\alpha_{11} - \alpha_{10}\alpha_3|^2 + |\alpha_2\alpha_{13} - \alpha_{12}\alpha_3|^2 + \\ + |\alpha_2\alpha_{15} - \alpha_{14}\alpha_3|^2 + |\alpha_4\alpha_7 - \alpha_6\alpha_5|^2 + |\alpha_4\alpha_9 - \alpha_8\alpha_5|^2 + |\alpha_4\alpha_{11} - \alpha_{10}\alpha_5|^2 + \\ + |\alpha_4\alpha_{13} - \alpha_{12}\alpha_5|^2 + |\alpha_4\alpha_{15} - \alpha_{14}\alpha_5|^2 + |\alpha_6\alpha_9 - \alpha_8\alpha_7|^2 + |\alpha_6\alpha_{11} - \alpha_{10}\alpha_7|^2 + \\ + |\alpha_6\alpha_{13} - \alpha_{12}\alpha_7|^2 + |\alpha_6\alpha_{15} - \alpha_{14}\alpha_7|^2 + |\alpha_8\alpha_{11} - \alpha_{10}\alpha_9|^2 + |\alpha_8\alpha_{13} - \alpha_{12}\alpha_9|^2 + \\ + |\alpha_8\alpha_{15} - \alpha_{14}\alpha_9|^2 + |\alpha_{10}\alpha_{13} - \alpha_{12}\alpha_{11}|^2 + |\alpha_{10}\alpha_{15} - \alpha_{14}\alpha_{11}|^2 + |\alpha_{12}\alpha_{15} - \alpha_{14}\alpha_{13}|^2 \end{array} \right\}. \quad (3.82)$$

As relações em (3.79) - (3.82), escritas na base 2, tornam-se, respectivamente:

$$\mathcal{N}_{A(BCD)}^2 = 4 \times \left(\sum_{\substack{jkl \neq j'k'l', j'k'l' \neq 000}} |\alpha_{0jkl}\alpha_{1j'k'l'} - \alpha_{0j'k'l'}\alpha_{1jkl}|^2 \right). \quad (3.83)$$

$$\mathcal{N}_{B(ACD)}^2 = 4 \times \left(\sum_{\substack{ikl \neq i'k'l', i'k'l' \neq 000}} |\alpha_{i0kl}\alpha_{i'1k'l'} - \alpha_{i'0k'l'}\alpha_{i1kl}|^2 \right), \quad (3.84)$$

$$\mathcal{N}_{C(ABD)}^2 = 4 \times \left(\sum_{\substack{ijl \neq i'j'l', i'j'l' \neq 000}} |\alpha_{ij0l}\alpha_{i'j'1l'} - \alpha_{i'j'0l'}\alpha_{ij1l}|^2 \right), \quad (3.85)$$

$$\mathcal{N}_{D(ABC)}^2 = 4 \times \left(\sum_{\substack{ijk \neq i'j'k', i'j'k' \neq 000}} |\alpha_{ijk0}\alpha_{i'j'k'1} - \alpha_{i'j'k'0}\alpha_{ijk1}|^2 \right). \quad (3.86)$$

Considerando os menores principais, se $\rho_{WXYZ}^{T_W} = \sum_{ijkl, i'j'k'l'} \alpha_{ijkl} \alpha_{i'j'k'l'}^* |i'jkl\rangle \langle ij'k'l'|$ é a transposta parcial da matriz densidade ρ_{WXYZ} com relação ao subsistema W , então o total de menores principais de $\rho_{WXYZ}^{T_W}$ é igual a $\binom{16}{3} = 560$, sendo que deste total, $2 \times \binom{8}{3} = 112$ são nulos. Assim, o número de menores principais, não nulos, de $\rho_{WXYZ}^{T_W}$, é $\binom{16}{3} - 2 \times \binom{8}{3} = 448$.

Para a matriz $\rho_{ABCD}^{T_A}$, cada menor principal é do tipo

$$-\left| \alpha_{ijkl} \right|^2 \times \sum_{\overline{ijkl \neq j'k'l'}, \overline{j'k'l' \neq 000}} \left| \alpha_{0jkl} \alpha_{1j'k'l'} - \alpha_{0j'k'l'} \alpha_{1jkl} \right|^2, \quad (3.87)$$

$i, j, k, l \in \{0, 1\}$. Cada uma das 16 somas, em (3.87), possui 28 parcelas. Somando, membro a membro, essas 16 igualdades obtêm-se

$$S_3(\rho_{ABCD}^{T_A}) = - \sum_{\overline{ijkl \neq j'k'l'}, \overline{j'k'l' \neq 000}} \left| \alpha_{0jkl} \alpha_{1j'k'l'} - \alpha_{0j'k'l'} \alpha_{1jkl} \right|^2. \quad (3.88)$$

Usando o mesmo raciocínio determinam-se as outras igualdades $S_3(\rho_{ABCD}^{T_B})$, $S_3(\rho_{ABCD}^{T_C})$ e $S_3(\rho_{ABCD}^{T_D})$:

$$S_3(\rho_{ABCD}^{T_B}) = - \sum_{\overline{ikl \neq i'k'l'}, \overline{i'k'l' \neq 000}} \left| \alpha_{i0kl} \alpha_{i'1k'l'} - \alpha_{i'0k'l'} \alpha_{i1kl} \right|^2, \quad (3.89)$$

$$S_3(\rho_{ABCD}^{T_C}) = - \sum_{\overline{ijl \neq i'j'l'}, \overline{i'j'l' \neq 000}} \left| \alpha_{ij0l} \alpha_{i'j'1l'} - \alpha_{i'j'0l'} \alpha_{ij1l} \right|^2, \quad (3.90)$$

$$S_3(\rho_{ABCD}^{T_D}) = - \sum_{\overline{ijk \neq i'j'k'}, \overline{i'j'k' \neq 000}} \left| \alpha_{ijk0} \alpha_{i'j'k'1} - \alpha_{i'j'k'0} \alpha_{ijk1} \right|^2. \quad (3.91)$$

A notação \overline{abc} , usada em (3.83) - (3.91), significa que $\overline{abc} = a \times 2^2 + b \times 2^1 + c \times 2^0$.

De (3.83) - (3.86) e (3.88) - (3.91), vem

$$\mathcal{N}_{W(XYZ)}^2 = -4\mathcal{S}_3(\rho_{WXYZ}^T), \quad (3.92)$$

em que

$$\mathcal{S}_3(\rho_{WXYZ}^T) = -\frac{1}{3} \left(1 - \text{Tr}(\rho_{WXYZ}^T)^3 \right) \quad (3.93)$$

é a soma dos menores principais de ordem 3 da transposta parcial ρ_{WXYZ}^T , em relação ao subsistema W , com $W, X, Y, Z \in \{A, B, C, D\}$, $W \neq X \neq Y \neq Z$.

Portanto, o entrelaçamento em quatro vias de estados puros quadripartes de qubits pode ser calculado usando os menores principais de acordo com (3.92), (3.93) e (2.10) - (2.14).

3.5.2. Exemplos

A. Como primeiro exemplo, considere o estado quântico $|\Psi\rangle$ dado por

$$|\Psi\rangle = \left(e^{i\theta X \otimes X} \otimes e^{i0.25\pi X \otimes X} \right) |0\rangle \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) |0\rangle, \quad (3.94)$$

$$|\Psi\rangle = \frac{1}{2} \left(\begin{aligned} &\cos(\theta)|0000\rangle - i\cos(\theta)|0011\rangle - i\cos(\theta)|0101\rangle + \cos(\theta)|0110\rangle \\ &-\sin(\theta)|1001\rangle - i\sin(\theta)|1010\rangle - i\sin(\theta)|1100\rangle - \sin(\theta)|1111\rangle \end{aligned} \right). \quad (3.95)$$

Os polinômios característicos de $\rho_{ABCD}^{T_A}$, $\rho_{ABCD}^{T_B}$, $\rho_{ABCD}^{T_C}$, $\rho_{ABCD}^{T_D}$ são:

$$\rho_{ABCD}^{T_A} \rightarrow \lambda^{16} - \lambda^{15} + (\sin(\theta)\cos(\theta))^2 \lambda^{13} - (\sin(\theta)\cos(\theta))^4 \lambda^{12}, \quad (3.96)$$

$$\rho_{ABCD}^{T_B}, \rho_{ABCD}^{T_C}, \rho_{ABCD}^{T_D} \rightarrow \lambda^{16} - \lambda^{15} + \frac{1}{4} \lambda^{13} - \frac{1}{16} \lambda^{12}. \quad (3.97)$$

Usando (3.92) em (3.94), obtém-se:

$$\mathcal{N}_{A(BCD)}^2 = 4(\sin(\theta)\cos(\theta))^2; \mathcal{N}_{B(ACD)}^2 = \mathcal{N}_{C(ABD)}^2 = \mathcal{N}_{D(ABC)}^2 = 1. \quad (3.98)$$

Observando (2.10) - (2.14), pode-se ver que $\mathcal{N} = 0$ se $S_3 = S_4 = 0$. Os polinômios característicos de ρ_{AB} , ρ_{AC} , ρ_{AD} , ρ_{BC} , ρ_{BD} , ρ_{CD} são iguais a $\lambda^4 - \lambda^3 + \frac{1}{4}\lambda^2$. Assim,

$$\mathcal{N}_{AB}^2 = \mathcal{N}_{AC}^2 = \mathcal{N}_{AD}^2 = \mathcal{N}_{BC}^2 = \mathcal{N}_{BD}^2 = \mathcal{N}_{CD}^2 = 0. \quad (3.99)$$

Agora, substituindo (3.96) e (3.97) em (3.74) - (3.78), tem-se:

$$\pi_4 = \sqrt{2|\sin(\theta)\cos(\theta)|}. \quad (3.100)$$

Na Figura 3.1 é mostrada a morte e a ressurreição de π_4 de (3.94), quando θ varia de 0 a π (rad). O estado (3.95), com $\theta = \frac{\pi}{2}$, se reduz ao produto tensorial de um qubit com um estado de três qubits, ou seja, $|\Psi\rangle = \frac{1}{2}(|1\rangle \otimes (|001\rangle - i|010\rangle - i|100\rangle - |111\rangle))$. E, portanto, sem entrelaçamento em 4 vias.

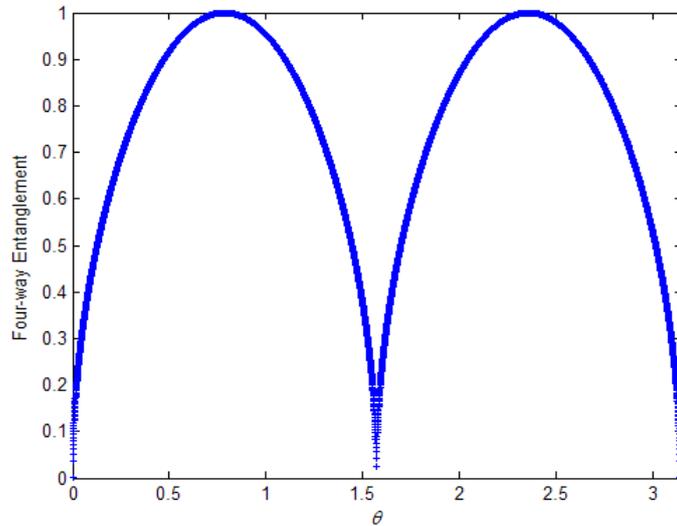


Figura 3.1. Entrelaçamento do estado (3.94) medido por π_4 versus θ .

B. Como segundo exemplo, considere o estado

$$|\Gamma\rangle = (I_2 \otimes e^{i\theta X \otimes X} \otimes I_2) \left(\frac{(|\phi^+\rangle|\phi^+\rangle + |\phi^-\rangle|\phi^-\rangle + |\psi^+\rangle|\psi^+\rangle + |\psi^-\rangle|\psi^-\rangle)_{ABCD}}{2} \right). \quad (3.101)$$

Em (3.101) tem-se $|\phi^\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$ e $|\psi^\pm\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$. Os polinômios característicos da transposta parcial dos estados bipartes reduzidos de $|\Gamma\rangle$ são:

$$\rho_{AB}^{T_A} = \rho_{AD}^{T_A} = \rho_{BC}^{T_B} = \rho_{CD}^{T_C} \rightarrow p(x) = \left(x - \frac{1}{4}\right)^4, \quad (3.102)$$

$$\rho_{AC}^{T_A} = \rho_{BD}^{T_B} \rightarrow p(x) = x^4 - x^3 + \frac{x^2}{8}(1 - \cos 4\theta) + \frac{x}{8}(1 + \cos 4\theta) - \frac{1}{32}(1 + \cos 4\theta). \quad (3.103)$$

Usando (2.10) - (2.14), obtém-se $\mathcal{N}_{AB} = \mathcal{N}_{AD} = \mathcal{N}_{BC} = \mathcal{N}_{CD} = 0$ e $\mathcal{N}_{AC} = \mathcal{N}_{BD} = |\cos 2\theta|$. Por outro lado, os polinômios característicos de $\rho_{ABCD}^{T_A}$, $\rho_{ABCD}^{T_B}$, $\rho_{ABCD}^{T_C}$ e $\rho_{ABCD}^{T_D}$ são:

$$\rho_{ABCD}^{T_A}, \rho_{ABCD}^{T_B}, \rho_{ABCD}^{T_C}, \rho_{ABCD}^{T_D} \rightarrow p(\lambda) = \lambda^{16} - \lambda^{15} + \frac{1}{4}\lambda^{13} - \frac{1}{16}\lambda^{12}, \quad (3.104)$$

e assim, usando (3.92) obtém-se $\mathcal{N}_{A(BCD)} = \mathcal{N}_{B(ACD)} = \mathcal{N}_{C(ABD)} = \mathcal{N}_{D(ABC)} = 1$. Então o entrelaçamento em quatro vias e o entrelaçamento biparte do estado (3.101), são:

$$\pi_4 = 1 - \cos^2 2\theta, \quad (3.105)$$

$$\mathcal{N}_{AC} = \mathcal{N}_{BD} = |\cos 2\theta|. \quad (3.106)$$

Observando (3.105) e (3.106), vê-se que existe uma troca entre o entrelaçamento em quatro vias e o entrelaçamento biparte. Quando um é máximo, o outro é mínimo.

C. Agora, considere o estado [38],

$$|\psi_{HS}\rangle = \frac{1}{\sqrt{6}}(|1100\rangle + |0011\rangle + \xi^2(|1010\rangle + |0101\rangle) + \xi(|1001\rangle + |0110\rangle)), \quad (3.107)$$

com $|\xi^2|=1$. Os polinômios característicos da transposta parcial dos estados bipartes reduzidos de $|\psi_{HS}\rangle$, são

$$\rho_{AB}^{T_A} = \rho_{CD}^{T_C} = \rho_{AC}^{T_A} = \rho_{BD}^{T_B} \rightarrow \frac{1}{1296}(6\lambda + 2\operatorname{Re}(\xi) - 1)(6\lambda - 2\operatorname{Re}(\xi) - 1)(6\lambda - 2)^2, \quad (3.108)$$

$$\rho_{AD}^{T_A} = \rho_{BC}^{T_B} \rightarrow \frac{1}{1296}(6\lambda + 2\operatorname{Re}(\xi^2) - 1)(6\lambda - 2\operatorname{Re}(\xi^2) - 1)(6\lambda - 2)^2. \quad (3.109)$$

Usando (2.10) - (2.14) e $\xi = a + i(1 - a^2)^{1/2}$, obtém-se:

$$\mathcal{N}_{AB} = \mathcal{N}_{CD} = \mathcal{N}_{AC} = \mathcal{N}_{BD} = \frac{1}{6} - \frac{|a|}{3}, \quad (3.110)$$

$$\mathcal{N}_{AD} = \mathcal{N}_{BC} = \frac{1}{6} - \frac{|2a^2 - 1|}{3}. \quad (3.111)$$

Por outro lado, os polinômios característicos de $\rho_{ABCD}^{T_A}$, $\rho_{ABCD}^{T_B}$, $\rho_{ABCD}^{T_C}$ e $\rho_{ABCD}^{T_D}$ são os mesmos em (3.104). Assim, usando (3.92) obtém-se $\mathcal{N}_{A(BCD)} = \mathcal{N}_{B(ACD)} = \mathcal{N}_{C(ABD)} = \mathcal{N}_{D(ABC)} = 1$. Portanto, o entrelaçamento em quatro vias do estado dado por (3.107), é

$$\pi_4 = 1 - 2 \times \left(\frac{1}{6} - \frac{|a|}{3} \right)^2 - \left(\frac{1}{6} - \frac{|2a^2 - 1|}{3} \right)^2. \quad (3.112)$$

O entrelaçamento de quatro vias é máximo se $|a| = \frac{1}{2}$; logo, $\pi_4 = 1$, se $\xi = \pm \frac{1}{2} + i \frac{\sqrt{3}}{2}$. O mesmo resultado foi obtido em [38].

3.6. Conclusão

Neste capítulo, foram mostradas relações entre a negatividade e a soma dos menores principais de ordem 3 da transposta parcial da matriz densidade, para estados tripartes e quadripartes (puros) de qubits. Ou seja, foram obtidas fórmulas para o cálculo do entrelaçamento de estados tripartes e quadripartes (puros) de qubits, usando os menores principais. Em ambos os casos, a característica relevante é a soma de todos os menores principais de ordem 3. Assim, é suficiente determinar o polinômio característico e tomar o termo S_3 .

No capítulo seguinte será apresentada uma medida de entrelaçamento para estados puros de seis qubits.

CAPÍTULO 4

MEDIDAS DE ENTRELAÇAMENTO PARA ESTADOS QUÂNTICOS PUROS DE SEIS QUBITS

Resumo

Neste capítulo propõe-se uma medida para o cálculo do entrelaçamento em um estado puro de seis qubits. Tal medida, baseada na negatividade, é usada para quantificar o entrelaçamento em alguns estados de seis qubits que são úteis no processamento da informação quântica e na análise da variação do entrelaçamento de alguns estados parametrizados de seis qubits. O entrelaçamento residual em alguns estados de seis partes também é medido usando-se a negatividade.

4.1. Medida de Entrelaçamento para Estados Puros de Seis Qubits

Um estado puro em $(\mathbb{C}^2)^{\otimes 6}$ (i.e., um estado puro de seis qubits), é representado por

$$|\psi\rangle = \sum_{i,j,k,l,m,n=0}^1 \alpha_{ijklmn} |ijklmn\rangle, \quad (4.1)$$

com $\alpha_{ijklmn} \in \mathbb{C}$ tal que $\sum_{i,j,k,l,m,n=0}^1 |\alpha_{ijklmn}|^2 = 1$. A matriz densidade ρ associada ao estado $|\psi\rangle$,

$\rho = |\psi\rangle\langle\psi|$, é dada por

$$\rho = \sum_{i,j,k,l,m,n,i',j',k',l',m',n'=0}^1 \alpha_{ijklmn} \alpha_{i'j'k'l'm'n'}^* |ijklmn\rangle \langle i'j'k'l'm'n'|. \quad (4.2)$$

No Capítulo 3, mais precisamente nas Eqs. (3.39) - (3.42) e (3.74) - (3.78), foram vistas fórmulas para o cálculo do entrelaçamento de estados puros de três e quatro qubits, respectivamente, usando a negatividade.

Uma medida de entrelaçamento para estados puros de cinco qubits, chamada de π_5 , se estende de maneira natural do π_4 , e é definida por [36,37]

$$\pi_5 = \sqrt[5]{\pi_A \pi_B \pi_C \pi_D \pi_E}, \quad (4.3)$$

sendo, por exemplo, $\pi_A = \mathcal{N}_{A(BCDE)}^2 - \mathcal{N}_{AB}^2 - \mathcal{N}_{AC}^2 - \mathcal{N}_{AD}^2 - \mathcal{N}_{AE}^2$.

Para estados puros quaisquer de seis qubits, $|\psi_{ABCDEF}\rangle$ (que, por simplificação de notação, será descrito apenas por $ABCDEF$), vale a desigualdade monogâmica [35]

$$\mathcal{N}_{AB}^2 + \mathcal{N}_{AC}^2 + \mathcal{N}_{AD}^2 + \mathcal{N}_{AE}^2 + \mathcal{N}_{AF}^2 \leq \mathcal{N}_{A(BCDEF)}^2. \quad (4.4)$$

Assim, se for possível estender naturalmente o π_3 , como foi feito para 4 e 5 qubits, para estados de seis qubits, nesse sentido, tem-se

$$\pi_6 = \sqrt[6]{\pi_A \pi_B \pi_C \pi_D \pi_E \pi_F}, \quad (4.5)$$

onde, por exemplo,

$$\pi_A = \mathcal{N}_{A(BCDEF)}^2 - \mathcal{N}_{AB}^2 - \mathcal{N}_{AC}^2 - \mathcal{N}_{AD}^2 - \mathcal{N}_{AE}^2 - \mathcal{N}_{AF}^2. \quad (4.6)$$

Mas, para estados de seis qubits, o procedimento de extensão de π_3 falha. Por exemplo, para o estado desentrelaçado

$$\begin{aligned}
 |\varphi\rangle &= \frac{1}{2}(|000\rangle + |111\rangle)(|000\rangle - |111\rangle) \\
 &= \frac{1}{2}(|000000\rangle - |000111\rangle + |111000\rangle - |111111\rangle),
 \end{aligned} \tag{4.7}$$

tem-se $\mathcal{N}_{A(BCDEF)}^2 = 1$, $\mathcal{N}_{AB}^2 = \mathcal{N}_{AC}^2 = \mathcal{N}_{AD}^2 = \mathcal{N}_{AE}^2 = \mathcal{N}_{AF}^2 = 0$, e assim, a desigualdade em (4.4)

é estrita, o que mostra que o candidato a π_6 , na Eq. (4.5), não é uma extensão natural do π_5 .

Basicamente, para um estado puro de seis qubits do tipo $|\psi_{ABCDEF}\rangle = |\varepsilon_{ABC}\rangle|\sigma_{DEF}\rangle$, tem-se

$$\mathcal{N}_{A(BCDEF)}^2 - \mathcal{N}_{AB}^2 - \mathcal{N}_{AC}^2 - \mathcal{N}_{AD}^2 - \mathcal{N}_{AE}^2 - \mathcal{N}_{AF}^2 > 0, \tag{4.8}$$

(o mesmo acontece quando qualquer outro qubit é tomado como foco) quando os estados $|\varepsilon_{ABC}\rangle$ e $|\sigma_{DEF}\rangle$ são entrelaçados em três vias: $\pi_3(|\varepsilon_{ABC}\rangle) > 0$ e $\pi_3(|\sigma_{DEF}\rangle) > 0$. Isto conduz ao resultado $\pi_6(|\varepsilon_{ABC}\rangle|\sigma_{DEF}\rangle) > 0$, quando na verdade, o resultado deveria ser $\pi_6(|\varepsilon_{ABC}\rangle|\sigma_{DEF}\rangle) = 0$. Propõe-se, portanto, uma modificação no cálculo de π_6 com o objetivo de evitar esse tipo de erro, inclusive mudando a notação para essa medida, para evitar confusão e melhorar o entendimento. Uma nova medida de entrelaçamento em seis vias, γ_6 , será introduzida e usada para quantificar o entrelaçamento de estados puros de seis qubits, úteis no processamento da informação quântica.

A fim de evitar o erro descrito anteriormente, propõe-se o seguinte conjunto de equações para medir o entrelaçamento de estados puros de seis qubits:

$$\gamma_6 = \sqrt[6]{\gamma_A \gamma_B \gamma_C \gamma_D \gamma_E \gamma_F}, \tag{4.9}$$

sendo

$$\gamma_A = \mathcal{N}_{A(BCDEF)}^2 - \mathcal{N}_{A(BC)}^2 - \mathcal{N}_{AD}^2 - \mathcal{N}_{AE}^2 - \mathcal{N}_{AF}^2, \tag{4.10}$$

$$\gamma_B = \mathcal{N}_{B(ACDEF)}^2 - \mathcal{N}_{B(AC)}^2 - \mathcal{N}_{BD}^2 - \mathcal{N}_{BE}^2 - \mathcal{N}_{BF}^2, \tag{4.11}$$

$$\gamma_C = \mathcal{N}_{C(ABDEF)}^2 - \mathcal{N}_{C(AB)}^2 - \mathcal{N}_{CD}^2 - \mathcal{N}_{CE}^2 - \mathcal{N}_{CF}^2, \quad (4.12)$$

$$\gamma_D = \mathcal{N}_{D(ABCEF)}^2 - \mathcal{N}_{D(EF)}^2 - \mathcal{N}_{AD}^2 - \mathcal{N}_{BD}^2 - \mathcal{N}_{CD}^2, \quad (4.13)$$

$$\gamma_E = \mathcal{N}_{E(ABCDF)}^2 - \mathcal{N}_{E(DF)}^2 - \mathcal{N}_{AE}^2 - \mathcal{N}_{BE}^2 - \mathcal{N}_{CE}^2, \quad (4.14)$$

$$\gamma_F = \mathcal{N}_{F(ABCDE)}^2 - \mathcal{N}_{F(DE)}^2 - \mathcal{N}_{AF}^2 - \mathcal{N}_{BF}^2 - \mathcal{N}_{CF}^2, \quad (4.15)$$

de acordo com [37].

A seguir serão verificadas as condições que fazem de γ_6 uma medida natural de entrelaçamento.

4.1.1. γ_6 é uma medida de entrelaçamento

De acordo com [18], para mostrar que γ_6 é uma medida natural de entrelaçamento para estados puros de seis qubits $|\psi\rangle_{ABCDEF}$, é preciso provar as seguintes condições:

1. $\gamma_6(|\psi\rangle) \geq 0$;
2. γ_6 é invariante mediante transformações unitárias locais (LU);
3. γ_6 não cresce em média através de LOCC.

Para provar a condição 1), é preciso mostrar que em (4.9) - (4.15), cada $\gamma_X(|\psi\rangle) \geq 0$, com $X \in \{A, B, C, D, E, F\}$. Inicialmente, prova-se que $\gamma_A(|\psi\rangle) \geq 0$. De fato, um estado $ABCDEF$ de seis qubits pode ser escrito como um estado triparte do tipo $A((BC)(DEF))$. Aplicando a desigualdade monogâmica a esse estado, tem-se:

$$\mathcal{N}_{A(BC)}^2 + \mathcal{N}_{A(DEF)}^2 \leq \mathcal{N}_{A(BCDEF)}^2. \quad (4.16)$$

O estado $A(DEF)$, em (4.16), pode ser escrito como $A(D(EF))$, um estado triparte.

Aplicando novamente a desigualdade monogâmica ao estado $A(DEF)$, obtém-se

$$\mathcal{N}_{AD}^2 + \mathcal{N}_{A(EF)}^2 \leq \mathcal{N}_{A(DEF)}^2. \quad (4.17)$$

Finalmente, para o estado $A(EF)$, em (4.17), tem-se

$$\mathcal{N}_{AE}^2 + \mathcal{N}_{AF}^2 \leq \mathcal{N}_{A(EF)}^2. \quad (4.18)$$

Somando, membro a membro, as três desigualdades acima, chega-se a

$$\mathcal{N}_{A(BC)}^2 + \mathcal{N}_{AD}^2 + \mathcal{N}_{AE}^2 + \mathcal{N}_{AF}^2 \leq \mathcal{N}_{A(BCDEF)}^2, \quad (4.19)$$

ou seja, $\gamma_A(|\psi\rangle) \geq 0$. De maneira análoga, mostra-se que $\gamma_B, \gamma_C, \gamma_D, \gamma_E, \gamma_F$ são não negativas, e como $\gamma_6 = \sqrt[6]{\gamma_A \gamma_B \gamma_C \gamma_D \gamma_E \gamma_F}$, conclui-se que $\gamma_6(|\psi\rangle) \geq 0$.

Agora, para provar a condição 2), considere o estado puro

$$|\phi\rangle = U_A \otimes U_B \otimes U_C \otimes U_D \otimes U_E \otimes U_F |\psi\rangle \quad (4.20)$$

de seis qubits, obtido de $|\psi\rangle$ através da aplicação de transformações unitárias locais. Para mostrar que γ_6 é invariante mediante LU , é preciso mostrar que cada γ_X , $X \in \{A, B, C, D, E, F\}$, é também invariante mediante LU , ou seja, que todas as negatividades em γ_X são invariantes mediante tais operações. Inicialmente, é necessário mostrar que $\mathcal{N}_{A(BCDEF)}$ é invariante mediante LU . De fato, como a operação traço (soma dos autovalores) é invariante mediante uma transformação LU e $\mathcal{N}_{A(BCDEF)}^2(|\phi\rangle) = 2(1 - \text{Tr}(\rho_A^2(|\phi\rangle)))$, tem-se $\mathcal{N}_{A(BCDEF)}^2(|\phi\rangle) = 2(1 - \text{Tr}\{(U_A \rho_A(|\psi\rangle) U_A^\dagger)^2\})$. Daí, $\mathcal{N}_{A(BCDEF)}^2(|\phi\rangle) = 2(1 - \text{Tr}(\rho_A^2(|\psi\rangle)))$ e, portanto,

$$\mathcal{N}_{A(BCDEF)}^2(|\phi\rangle) = \mathcal{N}_{A(BCDEF)}^2(|\psi\rangle). \quad (4.21)$$

De maneira análoga, mostra-se que $\mathcal{N}_{B(ACDEF)}$, $\mathcal{N}_{C(ABDEF)}$, $\mathcal{N}_{D(ABCEF)}$, $\mathcal{N}_{E(ABCDF)}$ e $\mathcal{N}_{F(ABCDE)}$ são invariantes mediante transformações LU . A negatividade biparte proposta por Vidal e Werner é por si mesmo, uma medida de entrelaçamento, portanto, invariante mediante transformações LU , isto é, $\mathcal{N}_{AB}(\rho_{AB}) = \mathcal{N}_{AB}\left((U_A \otimes U_B)\rho_{AB}(U_A \otimes U_B)^\dagger\right)$. Tomando o estado $|\phi\rangle = U_A \otimes U_B \otimes U_C \otimes U_D \otimes U_E \otimes U_F |\psi\rangle$, tem-se $\mathcal{N}_{AB}(\rho_{AB}(|\phi\rangle)) = \mathcal{N}_{AB}(\rho_{AB}(|\psi\rangle))$, sendo $\rho_{AB}(|\phi\rangle) = \text{Tr}_{CDEF}(|\phi\rangle\langle\phi|) = (U_A \otimes U_B)\rho_{AB}(|\psi\rangle)(U_A \otimes U_B)^\dagger$. De maneira análoga, mostra-se que \mathcal{N}_{AD} , \mathcal{N}_{AE} , \mathcal{N}_{AF} , \mathcal{N}_{BD} , \mathcal{N}_{BE} , \mathcal{N}_{BF} , \mathcal{N}_{CD} , \mathcal{N}_{CE} e \mathcal{N}_{CF} são também invariantes mediante transformações LU . Finalmente, mostra-se que $\mathcal{N}_{A(BC)}(\rho_{ABC})$, é também invariante mediante LU , quando $\rho_{ABC} = \text{Tr}_{DEF}(|\phi\rangle\langle\phi|)$ é um estado misto. Um estado misto, ρ_{ABC} , é descrito da seguinte forma

$$\rho_{ABC} = \sum_i p_i \sum_{m,n,l,m',n',l'} \alpha_{mnl}^i (\alpha_{m'n'l'}^i)^* |mnl\rangle\langle m'n'l'|. \quad (4.22)$$

Seja agora o estado $\xi_{ABC} = U_A \otimes U_B \otimes U_C \rho_{ABC} U_A^\dagger \otimes U_B^\dagger \otimes U_C^\dagger$, obtido de ρ_{ABC} através de transformações locais unitárias, ou seja,

$$\xi_{ABC} = U_A \otimes U_B \otimes U_C \left(\sum_i p_i \sum_{m,n,l,m',n',l'} \alpha_{mnl}^i (\alpha_{m'n'l'}^i)^* |mnl\rangle\langle m'n'l'| \right) U_A^\dagger \otimes U_B^\dagger \otimes U_C^\dagger, \quad (4.23)$$

ou ainda,

$$\xi_{ABC} = \sum_i p_i \sum_{m,n,l,m',n',l'} \alpha_{mnl}^i (\alpha_{m'n'l'}^i)^* U_A |m\rangle\langle m'| U_A^\dagger \otimes U_B |n\rangle\langle n'| U_B^\dagger \otimes U_C |l\rangle\langle l'| U_C^\dagger. \quad (4.24)$$

Assim,

$$\xi_{ABC}^T = \sum_i p_i \sum_{m,n,l,m',n',l'} \alpha_{m'n'l'}^i (\alpha_{mnl}^i)^* (U_A |m\rangle\langle m'| U_A^\dagger)^T \otimes U_B |n\rangle\langle n'| U_B^\dagger \otimes U_C |l\rangle\langle l'| U_C^\dagger. \quad (4.25)$$

Como

$$(U_A |m\rangle\langle m'|U_A^\dagger)^T = (\langle m'|U_A^\dagger)^T (U_A |m\rangle)^T = (U_A^\dagger)^T |m'\rangle\langle m|U_A^T = U_A^* |m'\rangle\langle m|U_A^T = U_a |m'\rangle\langle m|U_a^\dagger, \quad (4.26)$$

$U_a = U_A^*$ e $U_a^\dagger = U_A^T$, tem-se

$$\xi_{ABC}^{T_A} = U_a \otimes U_B \otimes U_C \left(\sum_i p_i \sum_{m,n,l,m',n',l'} \alpha_{m'n'l}^i (\alpha_{mm'l'}^i)^* |m'n'l\rangle\langle mn'l'| \right) U_a^\dagger \otimes U_B^\dagger \otimes U_C^\dagger. \quad (4.27)$$

Portanto,

$$\mathcal{N}_{A(BC)}(\xi_{ABC}) = \mathcal{N}_{A(BC)}(\rho_{ABC}). \quad (4.28)$$

O mesmo procedimento pode ser usado para mostrar que $\mathcal{N}_{B(AC)}(\rho_{ABC})$, $\mathcal{N}_{C(AB)}(\rho_{ABC})$, $\mathcal{N}_{D(EF)}(\rho_{ABC})$, $\mathcal{N}_{E(DF)}(\rho_{ABC})$ e $\mathcal{N}_{F(DE)}(\rho_{ABC})$ são também invariantes mediante transformações unitárias locais. Desde que todas as negatividades usadas para a definição de γ_6 são invariantes mediante transformações LU , tem-se que γ_6 é também invariante mediante transformações LU .

Antes de provar a condição 3, considere o estado $|W\rangle$ de seis qubits,

$$|\psi\rangle = \alpha|100000\rangle + \beta|010000\rangle + \gamma|001000\rangle + \delta|000100\rangle + \theta|000010\rangle + \eta|000001\rangle, \quad (4.29)$$

com $0 < \alpha, \beta, \gamma, \delta, \theta, \eta < 1$ e $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 + \theta^2 + \eta^2 = 1$. Para este estado, tomando-se como foco o qubit A , tem-se

$$\mathcal{N}_{A(BCDEF)}^2 = 4\alpha^2 (\beta^2 + \gamma^2 + \delta^2 + \eta^2). \quad (4.30)$$

Os quadrados das negatividades dos estados bipartes reduzidos, AD , AE e AF , são dados, respectivamente, por

$$\mathcal{N}_{AD}^2 = 4\alpha^2\delta^2 + 2(\beta^2 + \gamma^2 + \theta^2 + \eta^2)^2 - 2(\beta^2 + \gamma^2 + \theta^2 + \eta^2)\sqrt{(\beta^2 + \gamma^2 + \theta^2 + \eta^2)^2 + 4\alpha^2\delta^2}, \quad (4.31)$$

$$\mathcal{N}_{AE}^2 = 4\alpha^2\theta^2 + 2(\beta^2 + \gamma^2 + \delta^2 + \eta^2)^2 - 2(\beta^2 + \gamma^2 + \delta^2 + \eta^2)\sqrt{(\beta^2 + \gamma^2 + \delta^2 + \eta^2)^2 + 4\alpha^2\theta^2}, \quad (4.32)$$

$$\mathcal{N}_{AF}^2 = 4\alpha^2\eta^2 + 2(\beta^2 + \gamma^2 + \delta^2 + \theta^2)^2 - 2(\beta^2 + \gamma^2 + \delta^2 + \theta^2)\sqrt{(\beta^2 + \gamma^2 + \delta^2 + \theta^2)^2 + 4\alpha^2\eta^2}. \quad (4.33)$$

E, para o estado reduzido $A(BC)$, por exemplo, tem-se

$$\mathcal{N}_{A(BC)}^2 = 4\alpha^2\beta^2 + 4\alpha^2\gamma^2 + 2(\delta^2 + \theta^2 + \eta^2)^2 - 2(\delta^2 + \theta^2 + \eta^2)\sqrt{(\delta^2 + \theta^2 + \eta^2)^2 + 4\alpha^2\beta^2 + 4\alpha^2\gamma^2}. \quad (4.34)$$

Finalmente, mostrar a condição 3), significa provar que se uma operação é realizada em uma das partes do sistema, em média o entrelaçamento do estado resultante não pode crescer. Para isto, usando um procedimento descrito em [35], considere elementos de POVMs, ou seja, operadores $A_x^\dagger A_x$ tais que $A_x^\dagger A_x \geq 0$, $(A_x^\dagger A_x)^\dagger = A_x^\dagger A_x$ e $A_1^\dagger A_1 + A_2^\dagger A_2 = I$. Pela decomposição em valores singulares, A_x pode ser escrito como $A_x = U_x D_x V$, onde U_x e V são matrizes unitárias e D_x são matrizes diagonais com entradas (a, b) e $(\sqrt{1-a^2}, \sqrt{1-b^2})$, nas quais $0 \leq a, b \leq 1$. Os operadores A_x atuarão apenas sobre um qubit, aqui o primeiro qubit de (4.1), por exemplo. Assim, aplicando A_x em (4.1), obtém-se o estado

$|\phi'_x\rangle = A_x |\psi\rangle$, cuja forma normalizada é $|\phi_x\rangle = \frac{1}{\sqrt{p_x}} |\phi'_x\rangle = \frac{1}{\sqrt{p_x}} A_x |\psi\rangle$. Assim,

$$\gamma_6(|\phi_x\rangle) = \gamma_6\left(\frac{1}{\sqrt{p_x}} \sum_{i,j,k,l,m,n=0}^1 \alpha_{ijklmn} U_x D_x V |i\rangle \otimes I |j\rangle \otimes I |k\rangle \otimes I |l\rangle \otimes I |m\rangle \otimes I |n\rangle\right), \quad (4.35)$$

com $p_x = \langle \phi'_x | \phi'_x \rangle = \langle \psi | A_x^\dagger A_x | \psi \rangle$ e $p_1 + p_2 = 1$. Mas, γ_6 é invariante mediante LU , logo,

$\gamma_6(U_x D_x V |\phi_x\rangle) = \gamma_6(D_x V |\phi_x\rangle)$, e assim,

$$\gamma_6(|\phi_x\rangle) = \gamma_6\left(\frac{1}{\sqrt{p_x}} \sum_{i,j,k,l,m,n=0}^1 \alpha_{ijklmn} D_x V |i\rangle \otimes I |j\rangle \otimes I |k\rangle \otimes I |l\rangle \otimes I |m\rangle \otimes I |n\rangle\right). \quad (4.36)$$

A média de $\gamma_6(\psi)$ é dada por

$$\langle \gamma_6(|\psi\rangle) \rangle = p_1 \gamma_6(|\phi_1\rangle) + p_2 \gamma_6(|\phi_2\rangle). \quad (4.37)$$

Usando o fato de que γ_6 é uma função quártica de seus coeficientes, como pode ser visto no estado da Eq. 4.29, tem-se

$$\gamma_6(|\phi_1\rangle) = \frac{a^2 b^2}{p_1^2} \gamma_6(|\psi\rangle), \quad (4.38)$$

$$\gamma_6(|\phi_2\rangle) = \frac{(1-a^2)^2 (1-b^2)^2}{p_2^2} \gamma_6(|\psi\rangle). \quad (4.39)$$

Agora, substituindo-se (4.38) e (4.39) em (4.37), obtém-se

$$\begin{aligned} \langle \gamma_6(|\psi\rangle) \rangle &= p_1 \gamma_6(|\phi_1\rangle) + p_2 \gamma_6(|\phi_2\rangle) \\ &= \frac{a^2 b^2}{\langle \psi | A_1^\dagger A_1 | \psi \rangle} \gamma_6(|\psi\rangle) + \frac{(1-a^2)^2 (1-b^2)^2}{\langle \psi | A_2^\dagger A_2 | \psi \rangle} \gamma_6(|\psi\rangle) \leq \gamma_6(|\psi\rangle), \end{aligned} \quad (4.40)$$

o que significa que $\gamma_6(|\psi\rangle)$ não cresce em média com *LOCC*. E, portanto, γ_6 é um monótono de entrelaçamento.

Um estado puro de seis qubits que não é completamente entrelaçado é descrito de uma das formas:

$$1. |\psi\rangle = |\psi_X\rangle \otimes |\psi_{YZWKL}\rangle.$$

Neste caso, $\gamma_6(|\psi\rangle) = 0$, pois $\mathcal{N}_{X(YZWKL)} = 0$, com $X, Y, Z, K, W, L \in \{A, B, C, D, E, F\}$, isto é,

$$\gamma_X(|\psi\rangle) = 0.$$

$$2. |\psi\rangle = |\psi_{XY}\rangle \otimes |\psi_{ZWKL}\rangle \text{ ou } |\psi\rangle = |\psi_{XYZ}\rangle \otimes |\psi_{WKL}\rangle.$$

Aqui, tem-se também $\gamma_6(|\psi\rangle) = 0$, porque $\mathcal{N}_{X(YZWKL)} = \mathcal{N}_{X(YZ)}$ e $\mathcal{N}_{XW} = \mathcal{N}_{XK} = \mathcal{N}_{XL} = 0$, e assim, $\gamma_X(|\psi\rangle) = 0$. Portanto, $\gamma_6(|\psi\rangle) = 0$, quando $|\psi\rangle$ é um estado produto.

Reciprocamente, se $\gamma_6(|\psi\rangle) = 0$, então $\gamma_X(|\psi\rangle) = 0$, para algum X , $X \in \{A, B, C, D, E, F\}$, ($\gamma_A(|\psi\rangle) = 0$, por exemplo). Neste caso, $|\psi\rangle$ não pode ser completamente entrelaçado. Da desigualdade monogâmica para estados tripartes tem-se $\mathcal{C}_{X(YZ)}^2 \geq \mathcal{C}_{XY}^2 + \mathcal{C}_{XZ}^2$, onde a igualdade ocorre, se e somente se, X não é entrelaçado com Y e/ou Z [28]. Portanto, desde que $\mathcal{N}_{X(YZ)} \leq \mathcal{C}_{X(YZ)}$ e $\mathcal{N}_{XY} \leq \mathcal{C}_{XY}$ ($\mathcal{N}_{XZ} \leq \mathcal{C}_{XZ}$) para qualquer estado misto $m \otimes n$, $m \leq n$ (a igualdade ocorre para estados puros), obtém-se $\mathcal{N}_{X(YZ)}^2 \geq \mathcal{N}_{XY}^2 + \mathcal{N}_{XZ}^2$ [35]. Agora, considerando $X = A$, $Y = BC$ e $Z = DEF$, tem-se

$$\mathcal{N}_{A(BCDEF)}^2 \geq \mathcal{N}_{A(BC)}^2 + \mathcal{N}_{A(DEF)}^2, \quad (4.41)$$

na qual a igualdade em (4.41) ocorre, se e somente se, o sistema A não é entrelaçado com os sistemas BC e/ou DEF . Em outras palavras, a igualdade em (4.41) significa a ausência de entrelaçamento genuíno em seis vias. De maneira similar e usando a generalização do entrelaçamento residual [26], obtém-se

$$\mathcal{N}_{A(DEF)}^2 \geq \mathcal{N}_{AD}^2 + \mathcal{N}_{AE}^2 + \mathcal{N}_{AF}^2 \quad (4.42)$$

De (4.41) e (4.42), segue

$$\mathcal{N}_{A(BCDEF)}^2 - \mathcal{N}_{A(BC)}^2 \geq \mathcal{N}_{A(DEF)}^2 \geq \mathcal{N}_{AD}^2 + \mathcal{N}_{AE}^2 + \mathcal{N}_{AF}^2 \quad (4.43)$$

Agora, se $\gamma_A = 0$, então

$$\mathcal{N}_{A(BCDEF)}^2 - \mathcal{N}_{A(BC)}^2 = \mathcal{N}_{AD}^2 + \mathcal{N}_{AE}^2 + \mathcal{N}_{AF}^2. \quad (4.44)$$

Comparando (4.43) e (4.44), vê-se que $\gamma_A = 0$ implica $\mathcal{N}_{A(BCDEF)}^2 - \mathcal{N}_{A(BC)}^2 = \mathcal{N}_{A(DEF)}^2$, a igualdade em (4.41). Portanto, como visto anteriormente, isto significa a ausência de entrelaçamento genuíno em seis vias para o estado $|\psi\rangle$, ou seja, $|\psi\rangle = |\psi_X\rangle \otimes |\psi_{YZWKL}\rangle$, $|\psi\rangle = |\psi_{XY}\rangle \otimes |\psi_{ZWKL}\rangle$ ou $|\psi\rangle = |\psi_{XYZ}\rangle \otimes |\psi_{WKL}\rangle$. Uma afirmação similar pode ser obtida quando outros qubits são tomados como focos. Assim, $\gamma_6 = 0$, se e somente se, o estado $|\psi\rangle_{ABCDEF}$ não tem um entrelaçamento genuíno em seis vias.

Um ponto fraco de γ_6 é o fato de que ela não é invariante com relação a algumas permutações dos subsistemas. Somente as permutações dentro dos subsistemas ABC e DEF , separadamente, não mudam o γ_6 . Por exemplo, $\gamma_6(|GHZ\rangle_3 \otimes |GHZ\rangle_3) = 0$, enquanto, $\gamma_6(I \otimes I \otimes S_w \otimes I \otimes I (|GHZ\rangle_3 \otimes |GHZ\rangle_3)) = 1$, sendo $|GHZ\rangle_3 = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, S_w e I , as portas *swap* e *identidade*, respectivamente.

A fim de resolver esse problema, deixando a medida de entrelaçamento em seis vias, invariante mediante permutações dos subsistemas, considere o estado $|\psi\rangle$ de seis qubits, A, B, C, D, E, F , em que $\rho = |\psi\rangle\langle\psi|$ é a matriz densidade desse estado. Deseja-se obter todas as bipartições de 3 qubits, $|xyz\rangle \otimes |wvt\rangle$, a partir do estado $|\psi\rangle$, permutando-se os subsistemas de $|xyz\rangle$ com os subsistemas de $|wvt\rangle$. Dessa maneira, obtêm-se as seguintes bipartições, ρ_i , de acordo com [37]:

$$\begin{aligned}
 U_{SW}^{(1)} &= ABCDEF \\
 U_{SW}^{(2)} &= (S_W^{AD}) U_{SW}^{(1)} (S_W^{AD})^\dagger = DBCAEF \\
 U_{SW}^{(3)} &= (S_W^{AE}) U_{SW}^{(2)} (S_W^{AE})^\dagger = EBCDAF \\
 U_{SW}^{(4)} &= (S_W^{AF}) U_{SW}^{(3)} (S_W^{AF})^\dagger = FBCDEA \\
 U_{SW}^{(5)} &= (S_W^{BD}) U_{SW}^{(4)} (S_W^{BD})^\dagger = ADCBEF \\
 U_{SW}^{(6)} &= (S_W^{BE}) U_{SW}^{(5)} (S_W^{BE})^\dagger = AECDBF \\
 U_{SW}^{(7)} &= (S_W^{BF}) U_{SW}^{(6)} (S_W^{BF})^\dagger = AFCDEB \\
 U_{SW}^{(8)} &= (S_W^{CD}) U_{SW}^{(7)} (S_W^{CD})^\dagger = ABDCEF \\
 U_{SW}^{(9)} &= (S_W^{CE}) U_{SW}^{(8)} (S_W^{CE})^\dagger = ABEDCF \\
 U_{SW}^{(10)} &= (S_W^{CF}) U_{SW}^{(9)} (S_W^{CF})^\dagger = ABFDEC,
 \end{aligned} \tag{4.45}$$

de modo que cada porta $U_{SW}^{(i)}$ é aplicada ao estado ρ , para obter o estado ρ_i .

As equações (4.9) - (4.15) fornecem os valores de γ_6 e γ_X , para cada um dos 10 estados em (4.45), com $X \in \{A, B, C, D, E, F\}$. Assim, para cada estado $U_{SW}^{(i)}$, tem-se

$$\gamma_6^{(i)} = \sqrt[6]{\gamma_A^{(i)} \gamma_B^{(i)} \gamma_C^{(i)} \gamma_D^{(i)} \gamma_E^{(i)} \gamma_F^{(i)}}, \quad (4.46)$$

onde

$$\gamma_A^{(i)} = \mathcal{N}_{A(BCDEF)}^2 - \mathcal{N}_{A(BC)}^2 - \mathcal{N}_{AD}^2 - \mathcal{N}_{AE}^2 - \mathcal{N}_{AF}^2, \quad (4.47)$$

$$\gamma_B^{(i)} = \mathcal{N}_{B(ACDEF)}^2 - \mathcal{N}_{B(AC)}^2 - \mathcal{N}_{BD}^2 - \mathcal{N}_{BE}^2 - \mathcal{N}_{BF}^2, \quad (4.48)$$

$$\gamma_C^{(i)} = \mathcal{N}_{C(ABDEF)}^2 - \mathcal{N}_{C(AB)}^2 - \mathcal{N}_{CD}^2 - \mathcal{N}_{CE}^2 - \mathcal{N}_{CF}^2, \quad (4.49)$$

$$\gamma_D^{(i)} = \mathcal{N}_{D(ABCEF)}^2 - \mathcal{N}_{D(EF)}^2 - \mathcal{N}_{AD}^2 - \mathcal{N}_{BD}^2 - \mathcal{N}_{CD}^2, \quad (4.50)$$

$$\gamma_E^{(i)} = \mathcal{N}_{E(ABCDF)}^2 - \mathcal{N}_{E(DF)}^2 - \mathcal{N}_{AE}^2 - \mathcal{N}_{BE}^2 - \mathcal{N}_{CE}^2, \quad (4.51)$$

$$\gamma_F^{(i)} = \mathcal{N}_{F(ABCDE)}^2 - \mathcal{N}_{F(DE)}^2 - \mathcal{N}_{AF}^2 - \mathcal{N}_{BF}^2 - \mathcal{N}_{CF}^2. \quad (4.52)$$

com $i = 1, 2, \dots, 10$.

Considere, agora, a matriz $\Pi_X = (\gamma_X^{(i)})_{6 \times 10}$, ou seja,

$$\Pi_X = \begin{pmatrix} \gamma_A^{(1)} & \gamma_A^{(2)} & \gamma_A^{(3)} & \gamma_A^{(4)} & \gamma_A^{(5)} & \gamma_A^{(6)} & \gamma_A^{(7)} & \gamma_A^{(8)} & \gamma_A^{(9)} & \gamma_A^{(10)} \\ \gamma_B^{(1)} & \gamma_B^{(2)} & \gamma_B^{(3)} & \gamma_B^{(4)} & \gamma_B^{(5)} & \gamma_B^{(6)} & \gamma_B^{(7)} & \gamma_B^{(8)} & \gamma_B^{(9)} & \gamma_B^{(10)} \\ \gamma_C^{(1)} & \gamma_C^{(2)} & \gamma_C^{(3)} & \gamma_C^{(4)} & \gamma_C^{(5)} & \gamma_C^{(6)} & \gamma_C^{(7)} & \gamma_C^{(8)} & \gamma_C^{(9)} & \gamma_C^{(10)} \\ \gamma_D^{(1)} & \gamma_D^{(2)} & \gamma_D^{(3)} & \gamma_D^{(4)} & \gamma_D^{(5)} & \gamma_D^{(6)} & \gamma_D^{(7)} & \gamma_D^{(8)} & \gamma_D^{(9)} & \gamma_D^{(10)} \\ \gamma_E^{(1)} & \gamma_E^{(2)} & \gamma_E^{(3)} & \gamma_E^{(4)} & \gamma_E^{(5)} & \gamma_E^{(6)} & \gamma_E^{(7)} & \gamma_E^{(8)} & \gamma_E^{(9)} & \gamma_E^{(10)} \\ \gamma_F^{(1)} & \gamma_F^{(2)} & \gamma_F^{(3)} & \gamma_F^{(4)} & \gamma_F^{(5)} & \gamma_F^{(6)} & \gamma_F^{(7)} & \gamma_F^{(8)} & \gamma_F^{(9)} & \gamma_F^{(10)} \end{pmatrix}, \quad (4.53)$$

em que os seus elementos são dispostos de maneira que, cada $\gamma_6^{(i)}$ é igual à média geométrica dos elementos da coluna de ordem i , e cada linha é formada pelos $\gamma_X^{(i)} = \gamma_X(U_{SW}^{(i)}(\rho_i))$ com $X \in \{A, B, C, D, E, F\}$ e $i = 1, 2, \dots, 10$. Para calcular a quantidade de entrelaçamento do estado ρ , usa-se a expressão

$$\gamma_6(\rho) = \max_i \left(\gamma_6(U_{SW}^{(i)}(\rho_i)) \right) \times \mathcal{D}, \quad (4.54)$$

em que \mathcal{D} é o critério de separabilidade dado por $\mathcal{D} = 0$, se a matriz \prod_X tem no mínimo uma linha ou coluna formada apenas por zeros, caso contrário, $\mathcal{D} = 1$. Além disso, o máximo é tomado sobre o conjunto de portas de seis qubits $U_{SW}^{(i)}$, em (4.45).

Agora, para testar essa medida, alguns exemplos são considerados.

4.1.2. Exemplos

A. Considere, inicialmente, os já conhecidos estados GHZ e W , e o estado CZG de seis qubits proposto em [41],

$$|GHZ_6\rangle = \frac{|000000\rangle + |111111\rangle}{\sqrt{2}}, \quad (4.55)$$

$$|W_6\rangle = \frac{|100000\rangle + |010000\rangle + |001000\rangle + |000100\rangle + |000010\rangle + |000001\rangle}{\sqrt{6}}. \quad (4.56)$$

$$|CZG_6\rangle = \frac{|000000\rangle + |011100\rangle + |111000\rangle + |100100\rangle + |001111\rangle + |010011\rangle + |110111\rangle + |101011\rangle}{\sqrt{8}} \quad (4.57)$$

Medindo-se o entrelaçamento dos estados (4.55) - (4.57), obtém-se $\gamma_6(|GHZ_6\rangle) = 1$, $\gamma_6(|W_6\rangle) = 0,5019$ e $\gamma_6(|CZG_6\rangle) = 1$. Usando a medida proposta em [42] obtém-se, para o mesmo conjunto de estados: $E_G^{(1)}(|GHZ_6\rangle) = 1$, $E_G^{(1)}(|W_6\rangle) \approx 0,556$ e $E_G^{(1)}(|CZG_6\rangle) = 1$.

Outros três exemplos para estados de seis qubits úteis no processamento de informação quântica são dados em [43-50].

B. Considere os estados:

$$|C_6\rangle = \frac{1}{2}(|000000\rangle + |000111\rangle + |111000\rangle - |111111\rangle), \quad (4.58)$$

$$|\psi_6\rangle = \frac{1}{\sqrt{2}} \left(\frac{|000111\rangle + |111000\rangle}{\sqrt{2}} \right) + \frac{1}{2}(|\bar{w}_3\rangle|w_3\rangle + |w_3\rangle|\bar{w}_3\rangle), \quad (4.59)$$

onde $|w_3\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ e $|\bar{w}_3\rangle = (|110\rangle + |101\rangle + |011\rangle)/\sqrt{3}$.

$$|\xi_6\rangle = \frac{1}{4} \begin{bmatrix} |000\rangle(|0\rangle|\phi^+\rangle + |1\rangle|\psi^+\rangle) + |001\rangle(|0\rangle|\psi^-\rangle - |1\rangle|\phi^-\rangle) + \\ |010\rangle(|0\rangle|\psi^+\rangle - |1\rangle|\phi^+\rangle) + |011\rangle(|0\rangle|\phi^-\rangle + |1\rangle|\psi^-\rangle) + \\ |100\rangle(-|0\rangle|\psi^-\rangle - |1\rangle|\phi^-\rangle) + |101\rangle(-|0\rangle|\phi^+\rangle + |1\rangle|\psi^+\rangle) + \\ |110\rangle(|0\rangle|\phi^-\rangle - |1\rangle|\psi^-\rangle) + |111\rangle(|0\rangle|\psi^+\rangle + |1\rangle|\phi^+\rangle) \end{bmatrix}, \quad (4.60)$$

onde $|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ e $|\psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$.

Para esses estados, tem-se $\gamma_6(|C_6\rangle) = 1$, $\gamma_6(|\psi_6\rangle) = 0,6667$ e $\gamma_6(|\xi_6\rangle) = 0,6667$.

C. Por fim, o estado

$$|\Omega_6\rangle = \frac{1}{2}(|\xi_0\rangle|\phi^+\rangle + |\xi_1\rangle|\phi^-\rangle + |\bar{\xi}_0\rangle|\psi^+\rangle + |\bar{\xi}_1\rangle|\psi^-\rangle), \quad (4.61)$$

onde $|\xi_0\rangle = (|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle)/2$, $|\xi_1\rangle = (|1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle)/2$, $X^{\otimes 4}|\xi_0\rangle = |\bar{\xi}_0\rangle$ e $X^{\otimes 4}|\xi_1\rangle = |\bar{\xi}_1\rangle$, é também maximamente entrelaçado, $\gamma_6(|\Omega_6\rangle) = 1$. Em (4.61), X é uma porta bit-flip.

Na seção seguinte será feito uma análise da Variação do Entrelaçamento, observando-se a dinâmica do entrelaçamento de alguns sistemas particulares de seis qubits.

4.2. Análise da Variação do Entrelaçamento

Inicialmente, serão considerados os seguintes estados de seis qubits:

Considere o estado:

$$|\Phi(\theta)\rangle = I \otimes \exp(i\theta X \otimes X \otimes X \otimes X) \otimes I |W_6\rangle, \quad (4.62)$$

ou

$$|\Phi(\theta)\rangle = \frac{1}{\sqrt{6}} \left(\begin{aligned} &(\cos \theta)|000000\rangle + (\cos \theta)|000001\rangle + (\cos \theta)|000010\rangle + (\cos \theta)|000100\rangle + \\ &+ (\cos \theta)|001000\rangle + (\cos \theta)|010000\rangle + i(\text{sen}\theta)|001110\rangle + i(\text{sen}\theta)|011100\rangle + \\ &+ i(\text{sen}\theta)|010110\rangle + i(\text{sen}\theta)|011010\rangle + i(\text{sen}\theta)|011110\rangle + i(\text{sen}\theta)|011111\rangle \end{aligned} \right). \quad (4.63)$$

A variação de $\gamma_6(|\Phi(\theta)\rangle)$ versus θ , pode ser visto na Figura 4.1, enquanto os entrelaçamentos bipartes, \mathcal{N}_{AB}^2 e \mathcal{N}_{DE}^2 podem ser visto na Figura 4.2.

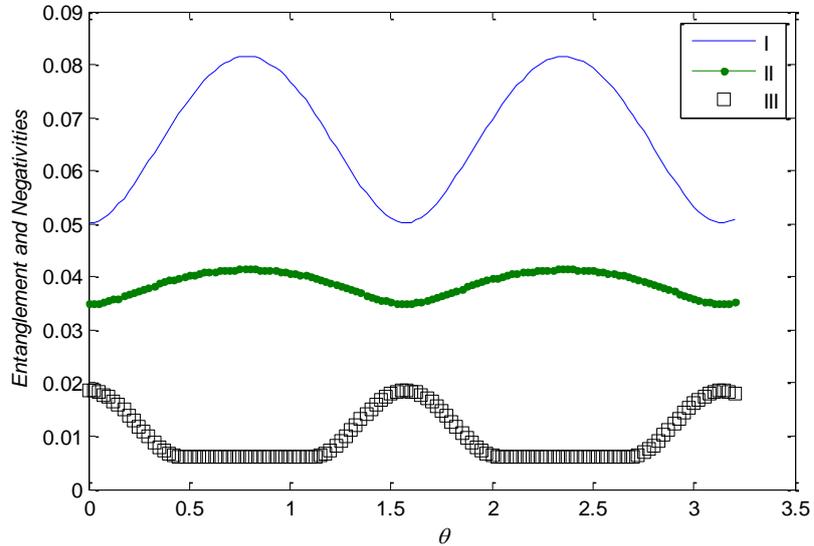


Figura 4.1. Entrelaçamento e negatividades do estado (4.62), medido por $\gamma_6/10$ (I), $\mathcal{N}_{A(BC)}^2$ (II) e $\mathcal{N}_{AD}^2 + \mathcal{N}_{AE}^2 + \mathcal{N}_{AF}^2$ (III) versus θ .

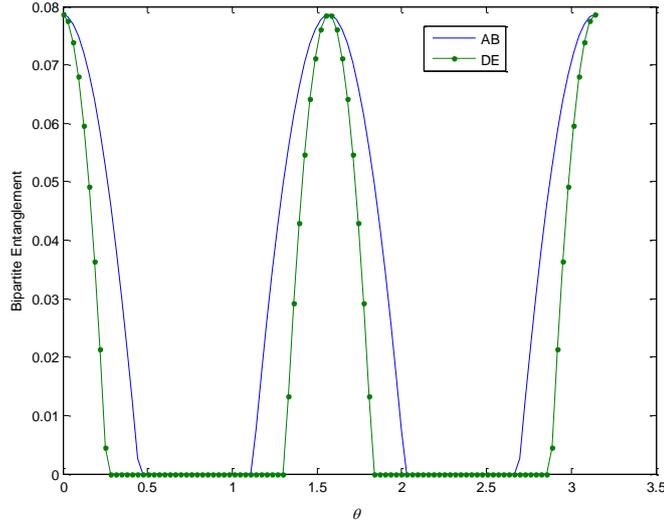


Figura 4.2. Entrelaçamentos Bipartites \mathcal{N}_{AB}^2 e \mathcal{N}_{DE}^2 do estado (4.62) versus θ .

O comportamento suave de γ_6 visto na Figura 4.1 contrasta com a morte súbita de \mathcal{N}_{AB}^2 e \mathcal{N}_{DE}^2 mostrada na Figura 4.2. O valor máximo de γ_6 ocorre quando $\theta = \frac{\pi}{4}$, neste caso

$$\gamma_6 \left(\left| \Phi \left(\frac{\pi}{4} \right) \right\rangle \right) > \gamma_6 (|W_6\rangle).$$

Como segundo exemplo, considere os seguintes estados de seis qubits:

$$|G_1\rangle = U_{12}U_{16}U_{23}U_{34}U_{45}U_{56} (\cos(\theta)|0\rangle + \text{sen}(\theta)|1\rangle)^{\otimes 6}, \quad (4.64)$$

$$|G_2\rangle = U_{12}U_{13}U_{16}U_{23}U_{25}U_{34}U_{45}U_{46}U_{56} (\cos(\theta)|0\rangle + \text{sen}(\theta)|1\rangle)^{\otimes 6}, \quad (4.65)$$

$$U_{ij} = |0\rangle\langle 0|_i \otimes I_j + |1\rangle\langle 1|_i \otimes Z_j. \quad (4.66)$$

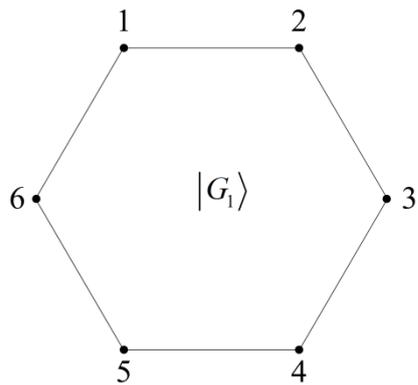


Figura 4.3. Grafo correspondente ao estado grafo $|G_1\rangle$.

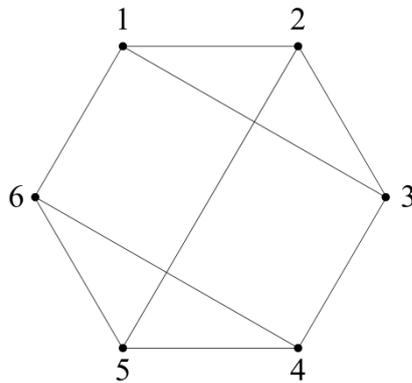


Figura 4.4. Grafo correspondente ao estado grafo $|G_2\rangle$.

Em (4.66), U_{ij} é a porta de fase controlada aplicada aos qubits i e j . Os entrelaçamentos do estado $|G_1\rangle$ versus θ podem ser vistos na Figura 4.5, enquanto os entrelaçamentos do estado $|G_2\rangle$ são mostrados na Figura 4.6.

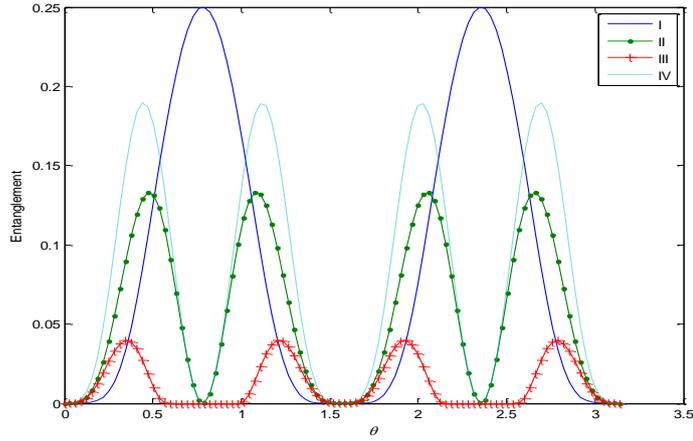


Figura 4.5. Entrelaçamentos de $|G_1\rangle$ versus θ : I) $\frac{\gamma_6}{4}$; II) $\mathcal{N}_{A(BC)}^2 = \mathcal{N}_{C(AB)}^2 = \mathcal{N}_{D(EF)}^2 = \mathcal{N}_{F(ED)}^2$; III)

$$\mathcal{N}_{AB}^2 = \mathcal{N}_{AF}^2 = \mathcal{N}_{BC}^2 = \mathcal{N}_{CD}^2 = \mathcal{N}_{DE}^2 = \mathcal{N}_{EF}^2; \text{IV) } \mathcal{N}_{B(AC)}^2 = \mathcal{N}_{E(DF)}^2.$$

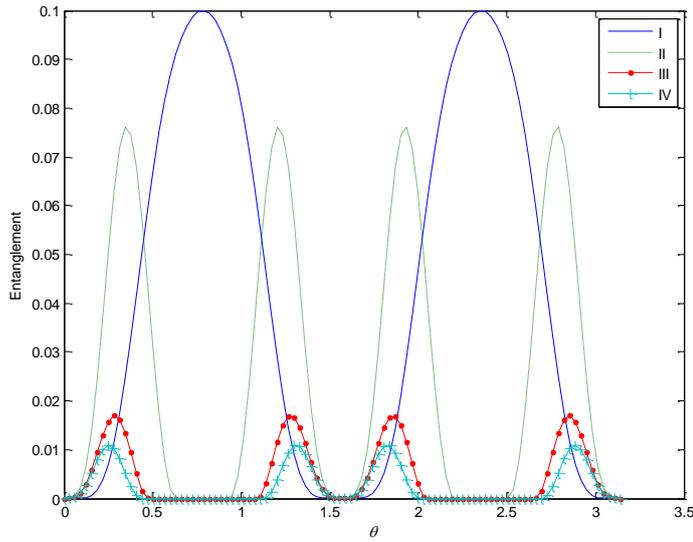


Figura 4.6. Entrelaçamentos de $|G_2\rangle$ versus θ :

$$\text{I) } \frac{\gamma_6}{10}; \text{II) } \mathcal{N}_{A(BC)}^2 = \mathcal{N}_{B(AC)}^2 = \mathcal{N}_{C(AB)}^2 = \mathcal{N}_{D(EF)}^2 = \mathcal{N}_{E(DF)}^2 = \mathcal{N}_{F(ED)}^2; \text{III)}$$

$$\mathcal{N}_{AB}^2 = \mathcal{N}_{AC}^2 = \mathcal{N}_{BC}^2 = \mathcal{N}_{DE}^2 = \mathcal{N}_{DF}^2 = \mathcal{N}_{EF}^2; \text{IV) } \mathcal{N}_{AF}^2 = \mathcal{N}_{BE}^2 = \mathcal{N}_{CD}^2.$$

Como esperado, para os estados $|G_1\rangle$ e $|G_2\rangle$, o entrelaçamento em seis vias é máximo ($\gamma_6 = 1$) para $\theta = \frac{\pi}{4}$ e $\theta = \frac{3\pi}{4}$, visto que, nesses casos, $|G_1\rangle$ e $|G_2\rangle$ são estados grafos de seis qubits representando completamente os grafos conectados. Uma diferença clara entre $|G_1\rangle$ e

$|G_2\rangle$ aparece nos entrelaçamentos biparte (não nulos). Para $|G_1\rangle$, os entrelaçamentos $X(YZ)$ podem ser divididos em dois conjuntos, as curvas II e IV na Figura 4.5, enquanto os entrelaçamentos bipartes XY pertencem a um conjunto simples, a curva III na Figura 4.5. Para o estado $|G_2\rangle$, acontece o oposto, os entrelaçamentos bipartes XY , podem ser divididos em dois conjuntos, as curvas III e IV, na Figura 4.6, enquanto os entrelaçamentos $X(YZ)$ pertencem a um conjunto simples, a curva II na Figura 4.6. Esta diferença entre os entrelaçamentos biparte de $|G_1\rangle$ e $|G_2\rangle$ é esperada, visto que $|G_1\rangle$ e $|G_2\rangle$ não são equivalentes mediante transformações LU e isomorfismos de grafos.

4.3. Conclusão

Neste capítulo foi introduzida uma medida de entrelaçamento, γ_6 , para estados puros de seis qubits: o entrelaçamento residual baseado na negatividade. Ao contrário de π_4 e π_5 , o quadrado da negatividade entre um qubit simples e dois qubits tem que ser considerado. Existem duas vantagens importantes, quando se considera o γ_6 como uma medida de entrelaçamento: ela é fácil de ser calculada, visto que não é necessário proceder a nenhuma minimização, e mede exclusivamente o entrelaçamento em seis vias. Assim γ_6 pode ser realmente usada para estudar a dinâmica do entrelaçamento em sistemas de seis qubits, como mostram os exemplos apresentados na Seção 4.2.

CAPÍTULO 5

UM ALGORITMO PARA ACHAR O MÍNIMO DE UMA FUNÇÃO REALIZANDO APENAS UMA MEDIÇÃO

Resumo

Vários problemas matemáticos podem ser modelados como um processo de busca em um banco de dados. Um exemplo é o problema de achar o mínimo de uma função. Algoritmos quânticos para resolver este problema foram propostos e todos eles usam um algoritmo de busca quântica como uma sub-rotina e várias medições intermediárias são realizadas. Neste trabalho é proposto um novo algoritmo quântico utilizando amplificação de amplitude para achar o mínimo de uma função em uma busca quântica, no qual tal busca não é usada como uma sub-rotina e apenas uma medição é requerida. Como exemplo, é proposto um algoritmo quântico para encontrar o período de uma função periódica.

5.1. Introdução

O algoritmo de busca quântica de Grover é um importante resultado em computação quântica que prova que uma superposição quântica pode acelerar a tarefa de achar um valor específico em um banco de dados não ordenado. A busca quântica usa em média $O(\sqrt{N})$ operações do oráculo (em comparação com as $O(N)$ operações do melhor dos algoritmos clássicos), indicando ganho de velocidade quadrático [56-58]. Vários problemas matemáticos podem ser modelados como uma busca, por exemplo, o problema de achar o mínimo (ou o máximo) de uma função. Assim, alguns algoritmos para achar o mínimo ou máximo usando busca quântica têm sido propostos [59,60], nos quais a generalização da busca quântica proposta em [61] é usada como uma sub-rotina que é requerida várias vezes. Nestes

algoritmos, a cada momento que a busca quântica é chamada, no fim uma medição é realizada. O número de medições propostas em [59] é $O(\log^2 N)$, sendo N o número de elementos no banco de dados. Objetivando reduzir o número de medições, Kowada et al [62] propuseram um novo algoritmo quântico para achar o mínimo de uma função que realiza $O(\log N)$ medições. Aqui, o objetivo é ir mais longe, propondo um algoritmo quântico para achar o mínimo, efetuando apenas uma medição no final do algoritmo. Ele é chamado de busca quântica assintótica. O algoritmo é descrito e um exemplo de sua utilização é demonstrado.

A seguir será feita uma revisão sobre amplificação de amplitude.

5.2. Revisão de Amplificação de Amplitude

Uma vez que o algoritmo de busca assintótica proposto é baseado na amplificação de amplitude, uma breve revisão desta é apresentada seguindo o tratamento do tema descrito em [10]. Seja A um algoritmo quântico capaz de produzir a resposta procurada codificada em um estado quântico. Por exemplo, o algoritmo de Grover usa um conjunto de portas Hadamard como A . Neste caso todas as possibilidades (respostas corretas e erradas) são geradas e todas possuem a mesma amplitude. Um algoritmo A mais geral produz também uma superposição com todos os possíveis resultados, mas com amplitudes diferentes para diferentes resultados. Ou seja,

$$|\psi\rangle = A|000\dots 0\rangle = \sum_x c_x |x\rangle |j(x)\rangle = \sum_{x \in X_{good}} c_x |x\rangle |j(x)\rangle + \sum_{x \in X_{bad}} c_x |x\rangle |j(x)\rangle, \quad (5.1)$$

$$p_{good} = \sum_{x \in X_{good}} |c_x|^2. \quad (5.2)$$

Em (5.1) a solução procurada ($|x\rangle$) é codificada em um número de qubits menor que o número de qubits do estado total. Os demais qubits ($|j(x)\rangle$) são irrelevantes e chamados de lixo. X_{good} e X_{bad} são, respectivamente, os conjuntos das soluções que resolvem (*good*) e não resolvem (*bad*) o problema. Por fim, p_{good} é a probabilidade de uma solução correta ser obtida

em uma medição do estado $|\psi\rangle = A|000\dots 0\rangle$. Dois novos estados podem ser escritos a partir de (5.1):

$$|\psi_{good}\rangle = \sum_{x \in X_{good}} \frac{c_x}{\sqrt{p_{good}}} |x\rangle |j(x)\rangle, \quad (5.3)$$

$$|\psi_{bad}\rangle = \sum_{x \in X_{bad}} \frac{c_x}{\sqrt{p_{bad}}} |x\rangle |j(x)\rangle. \quad (5.4)$$

Portanto, o estado total pode ser reescrito como

$$|\psi\rangle = \sqrt{p_{good}} |\psi_{good}\rangle + \sqrt{p_{bad}} |\psi_{bad}\rangle = \sin(\theta) |\psi_{good}\rangle + \cos(\theta) |\psi_{bad}\rangle. \quad (5.5)$$

Agora, é possível definir o operador $Q = AU_0^\perp A^{-1}U_f = U_\psi^\perp U_f$, para o qual $U_0^\perp |x\rangle = -|x\rangle$, se $x \neq 0$, e $U_0^\perp |0\rangle = |0\rangle$. Portanto, $U_\psi^\perp |\psi\rangle = |\psi\rangle$ e $U_\psi^\perp |\phi\rangle = -|\phi\rangle$ para qualquer $|\phi\rangle$ ortogonal a $|\psi\rangle$, $\langle \phi | \psi \rangle = 0$. Por fim, U_f é o operador oráculo que faz $U_f |x\rangle |b\rangle = |x\rangle |b \oplus f(x)\rangle$ e $f(x) = 1$, se x é a solução buscada, e $f(x) = 0$, se não é. Pode ser mostrado que

$$Q^k |\psi\rangle = \cos((2k+1)\theta) |\psi_{bad}\rangle + \sin((2k+1)\theta) |\psi_{good}\rangle. \quad (5.6)$$

Portanto, o menor valor de k que dá uma alta probabilidade de obter uma solução correta em uma medição é obtido fazendo-se $(2k+1)\theta = \frac{\pi}{2}$.

A seguir será apresentado um algoritmo para achar o mínimo de uma função, usando recursos da mecânica quântica.

5.3. Algoritmo Quântico para Achar o Mínimo de uma Função

Seja $f(x)$ uma função em que x é uma string binária de N bits. A meta é determinar o x que minimiza f . O algoritmo quântico capaz de resolver este problema é mostrado na Fig. 5.1. Nesta figura U_f é a porta quântica que implementa a função f , $U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$, a porta

$QBSC$ é um comparador quântico de strings [63], $QBSC|x\rangle|y\rangle|0\rangle = |x\rangle|y\rangle|b\rangle$, sendo $b = 0$, se $x > y$, e $b = 1$, se $x \leq y$.

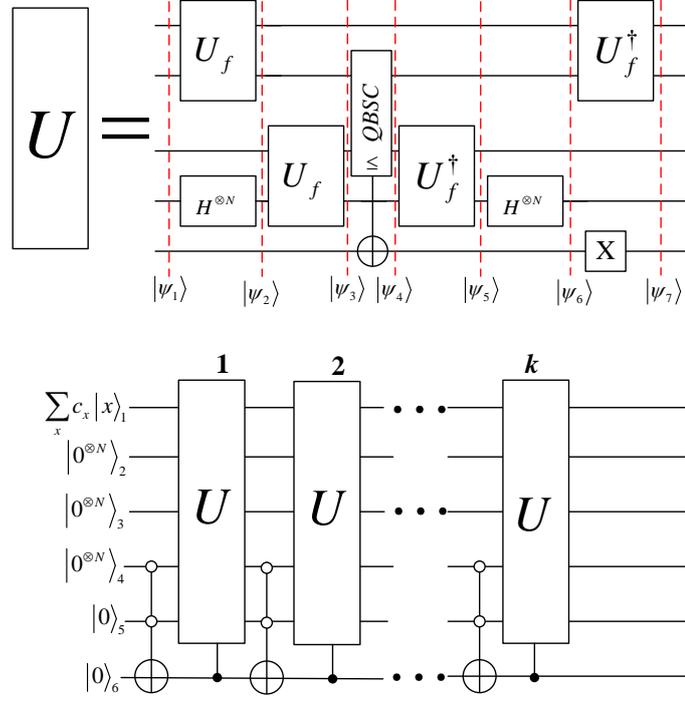


Figura. 5.1. Circuito quântico para busca assintótica.

A operação do circuito quântico U pode ser entendida seguindo os estados nas posições marcadas, $|\psi_1\rangle, \dots, |\psi_7\rangle$.

$$|\psi_1\rangle = \left(\sum_x c_x |x\rangle_1 |0^{\otimes N}\rangle_2 \right) |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 |0\rangle_5, \quad (5.7)$$

$$\begin{aligned} |\psi_2\rangle &= \left(\sum_x c_x U_f |x\rangle_1 |0^{\otimes N}\rangle_2 \right) \left(H^{\otimes N} |0^{\otimes N}\rangle_4 \right) |0^{\otimes N}\rangle_3 |0\rangle_5 \\ &= \left(\sum_x c_x |x\rangle_1 |f(x)\rangle_2 \right) \left(\sum_y \frac{1}{\sqrt{2^N}} |y\rangle_4 \right) |0^{\otimes N}\rangle_3 |0\rangle_5, \end{aligned} \quad (5.8)$$

$$\begin{aligned} |\psi_3\rangle &= \left(\sum_x c_x |x\rangle_1 |f(x)\rangle_2 \right) \left(\sum_y \frac{1}{\sqrt{2^N}} U_f |y\rangle_4 |0^{\otimes N}\rangle_3 \right) |0\rangle_5 \\ &= \left(\sum_x c_x |x\rangle_1 |f(x)\rangle_2 \right) \left(\sum_y \frac{1}{\sqrt{2^N}} |y\rangle_4 |f(y)\rangle_3 \right) |0\rangle_5, \end{aligned} \quad (5.9)$$

$$|\psi_4\rangle = \sum_{\substack{x,y \\ f(x)\leq f(y)}} \frac{c_x}{\sqrt{2^N}} |x\rangle_1 |f(x)\rangle_2 |y\rangle_4 |f(y)\rangle_3 |1\rangle_5 + \sum_{\substack{x,y \\ f(x)>f(y)}} \frac{c_x}{\sqrt{2^N}} |x\rangle_1 |f(x)\rangle_2 |y\rangle_4 |f(y)\rangle_3 |0\rangle_5 \quad (5.10)$$

ou seja,

$$|\psi_4\rangle = \left[\sum_x c_x |x\rangle_1 |f(x)\rangle_2 \sum_{j=1}^{n(x)} \frac{1}{\sqrt{2^N}} |y_j\rangle_4 |f(y_j)\rangle_3 \right] |1\rangle_5 + \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_x |x\rangle_1 |f(x)\rangle_2 \sum_{j=1}^{2^N-n(x)} \frac{1}{\sqrt{2^N}} |y_j\rangle_4 |f(y_j)\rangle_3 \right] |0\rangle_5. \quad (5.11)$$

Em (5.7) - (5.11), N é o número de qubits, portanto, existem 2^N elementos na base de dados. Em (5.11), $1 \leq n(x) \leq 2^N$ é o número de elementos que obedecem $f(x) \leq f(y)$ para um dado valor de x e todos os y 's. Assim, quanto melhor a solução, maior é o valor de $n(x)$. No primeiro termo de (5.11), os y_j são ordenados de forma que $f(y_j) \leq f(y_{j+1})$ e $f(x) = f(y_1)$. No segundo termo de (5.11), os y_j são ordenados de forma que $f(y_j) > f(y_{j+1})$ e $f(x) > f(y_1)$. Continuando, tem-se que

$$|\psi_5\rangle = \left[\sum_x c_x |x\rangle_1 |f(x)\rangle_2 \left(\sum_{j=1}^{n(x)} \frac{1}{\sqrt{2^N}} |y_j\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |1\rangle_5 + \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_x |x\rangle_1 |f(x)\rangle_2 \left(\sum_{j=1}^{2^N-n(x)} \frac{1}{\sqrt{2^N}} |y_j\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |0\rangle_5, \quad (5.12)$$

$$|\psi_6\rangle = \left[c_{x_{\min}} |x_{\min}\rangle_1 |f(x_{\min})\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 + \sum_{\substack{x \\ x \neq x_{\min}}} c_x |x\rangle_1 |f(x)\rangle_2 \left(\sum_{j=1}^{n(x)} \frac{1}{\sqrt{2^N}} H^{\otimes N} |y_j\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |1\rangle_5 + \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_{x_{\min}} |x\rangle_1 |f(x)\rangle_2 \left(\sum_{l=1}^{2^N-n(x)} \frac{1}{\sqrt{2^N}} H^{\otimes N} |y_l\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |0\rangle_5, \quad (5.13)$$

ou seja,

$$\begin{aligned}
 |\psi_6\rangle = & \left[c_{x_{\min}} |x_{\min}\rangle_1 |f(x_{\min})\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 + \right. \\
 & \left. \sum_{\substack{x \\ x \neq x_{\min}}} c_x n(x) 2^{-N} |x\rangle_1 |f(x)\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 \right] |1\rangle_5 + \\
 & + \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_x |x\rangle_1 |f(x)\rangle_2 \left(\sum_{\substack{j=1 \\ H^{\otimes N}|y_j\rangle \neq |0^{\otimes N}\rangle}}^{n(x)} \frac{1}{\sqrt{2^N}} H^{\otimes N} |y_j\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |1\rangle_5 + \quad (5.14) \\
 & + \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_x |x\rangle_1 |f(x)\rangle_2 \left(\sum_{l=1}^{2^N - n(x)} \frac{1}{\sqrt{2^N}} H^{\otimes N} |y_l\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |0\rangle_5.
 \end{aligned}$$

A expressão $H^{\otimes N}|y_j\rangle \neq |0^{\otimes N}\rangle$ significa que o termo $|0^{\otimes N}\rangle$ no resultado de $H^{\otimes N}|y_j\rangle$ já foi levado em conta no primeiro termo de (5.14). Por fim, o último estado marcado na Fig. 5.1, é

$$\begin{aligned}
 |\psi_7\rangle = & U \left[\left(\sum_x c_x |x\rangle_1 |0^{\otimes N}\rangle_2 \right) |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 |0\rangle_5 \right] = \\
 & = \left[\sum_x c_x n(x) 2^{-N} |x\rangle_1 |0^{\otimes N}\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 \right] |0\rangle_5 + \\
 & + \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_x |x\rangle_1 |0^{\otimes N}\rangle_2 \left(\sum_{\substack{j=1 \\ H^{\otimes N}|y_j\rangle \neq |0^{\otimes N}\rangle}}^{n(x)} \frac{1}{\sqrt{2^N}} H^{\otimes N} |y_j\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |0\rangle_5 + \quad (5.15) \\
 & + \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_x |x\rangle_1 |0^{\otimes N}\rangle_2 \left(\sum_{l=1}^{2^N - n(x)} \frac{1}{\sqrt{2^N}} H^{\otimes N} |y_l\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |1\rangle_5.
 \end{aligned}$$

Quanto pior for a solução, ou seja, quanto maior for a solução, menor é o valor de $n(x)$ e mais rápido é o decaimento da amplitude. Agora, usando k vezes a porta U junto com portas CNOTs multicontroladas, como mostra a parte de baixo da Fig. 5.1, o estado quântico final é

$$\begin{aligned}
 & \left[\sum_x c_x [n(x) 2^{-N}]^k |x\rangle_1 |0^{\otimes N}\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 \right] |0\rangle_5 + \\
 & + \sum_{r=1}^k \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_x [n(x) 2^{-N}]^{r-1} |x\rangle_1 |0^{\otimes N}\rangle_2 \left(\sum_{\substack{j=1 \\ H^{\otimes N}|y_j\rangle \neq |0^{\otimes N}\rangle}}^{n(x)} \frac{1}{\sqrt{2^N}} H^{\otimes N} |y_j\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |0\rangle_5 + \quad (5.16) \\
 & + \sum_{r=1}^k \left[\sum_{\substack{x \\ x \neq x_{\min}}} c_x [n(x) 2^{-N}]^{r-1} |x\rangle_1 |0^{\otimes N}\rangle_2 \left(\sum_{l=1}^{2^N - n(x)} \frac{1}{\sqrt{2^N}} H^{\otimes N} |y_l\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |1\rangle_5.
 \end{aligned}$$

Olhando mais atentamente o primeiro termo de (5.16), pode-se observar que a amplitude da resposta procurada é $c_{x_{\min}}$, uma vez que $n(x) = 2^N$ para $x = x_{\min}$. O segundo termo com maior amplitude tem $n(x) = 2^N - 1$, portanto, após a k -ésima aplicação de U sua amplitude será $c_x (1 - 2^{-N})^k$. Assim, se k é grande o suficiente, somente o termo correspondente à resposta procurada terá uma amplitude considerável.

Considerando k grande o bastante para que $(1 - 2^{-N})^k$ seja suficientemente próximo de zero para ser desconsiderado, a equação (5.16) pode ser reescrita na forma dada em (5.1)

$$\sum_{z \in Z_{\text{good}}} d_z |z\rangle_{45} |j(z)\rangle_{123} + \sum_{z \in Z_{\text{bad}}} d_z |z\rangle_{45} |j(z)\rangle_{123} \approx c_{x_{\min}} |0^{\otimes N}\rangle_4 |0\rangle_5 |x_{\min}\rangle_1 |0^{\otimes N}\rangle_2 |0^{\otimes N}\rangle_3 + \sum_{\substack{z \neq 0 \\ z \in Z_{\text{bad}}}}^{2^{(N+1)}} d_z |z\rangle_{45} |j(z)\rangle_{123}. \quad (5.17)$$

Uma vez que o estado (5.17) está escrito na forma (5.1), uma amplificação de amplitude é suficiente para encontrar o valor de x_{\min} . Neste caso, a resposta procurada pelo algoritmo de amplificação de amplitude é uma sequência de $N+1$ zeros nos registradores 4 e 5, ou seja, $|0^{\otimes N}\rangle_4 |0\rangle_5$. Ao final desta busca o estado quântico obtido será

$$\approx |0^{\otimes N}\rangle_4 |0\rangle_5 |x_{\min}\rangle_1 |0^{\otimes N}\rangle_2 |0^{\otimes N}\rangle_3 \quad (5.18)$$

e, portanto, uma medição no primeiro registrado revelará, por fim, o valor do mínimo procurado. Está é a única medição a ser realizada.

Por exemplo, escolhendo $c_x = 1/\sqrt{2^N}$ para todo x , a maior amplitude após usar a porta U (na Fig. 5.1) k vezes (antes da amplificação da amplitude) é $c_{x_{\min}} = 1/\sqrt{2^N}$, enquanto a segunda maior amplitude será $c_x = c_{x_{\min}} (1 - 2^{-N})^k$. O oráculo na amplificação de amplitude é aplicado $\frac{\pi}{4\theta}$ vezes, sendo [10]:

$$\text{sen}\theta = \sqrt{p_{\text{good}}} = 2^{-\frac{N}{2}}. \quad (5.19)$$

A fim de fazer a análise da complexidade do algoritmo proposto, é necessário contar quantas aplicações de U (Figura 5.1.) são necessárias para deixar a segunda maior amplitude dentro do primeiro termo de (5.16) muito próxima de zero, considerando que o estado inicial é uma superposição igualmente pesada, $c_x = 1/\sqrt{2^N}$, para todo x . Para um número $\varepsilon \ll 1$ muito pequeno, tem-se que

$$(1 - 2^{-N})^k < \varepsilon \Leftrightarrow k \geq 2^N \log\left(\frac{1}{\varepsilon}\right). \quad (5.20)$$

Assim, o número de vezes que U é usada é da mesma ordem do tamanho do banco de dados. Uma vez que a última aplicação de U foi realizada, a amplificação da amplitude é executada e a resposta correta pode ser obtida, numa medição simples, com probabilidade próxima de 1, após $O(\sqrt{N})$ vezes. Como os termos que não são soluções do problema de busca tendem a zero assintoticamente, o circuito da Fig. 5.1 é chamado de busca quântica assintótica (BQA). Uma comparação da busca quântica assintótica com os algoritmos quânticos LM e DH propostos em [62] e [59], respectivamente, podem ser vistos na Tabela 5.1.

	N_1	N_2	N_3	Probabilidade de sucesso
BQA	$2^N \log(1/\varepsilon)$	$O(2^{N/2})$	1	$1 - O(2^{-N})$
LM [7]	0	$O(2^{N/2})$	$O(\log(2^N))$	pelo menos $1/2$
DH [4]	0	$O(2^{N/2})$	$O(\log^2(2^N))$	pelo menos $1/2$

Tabela 5.1 – Comparação entre os algoritmos quânticos BQA, LM [62] e DH [59].

Na Tabela 5.1, N_1 é o número de operações realizadas antes da aplicação da amplificação de amplitude (ou do algoritmo de Grover), N_2 é o número de consultas ao oráculo durante a amplificação de amplitude, e N_3 é o número de medições executadas. Observando a Tabela 5.1, pode-se ver que o custo a ser pago a fim de se ter uma grande probabilidade de sucesso em apenas uma medição é o número de operações realizadas antes da amplificação da amplitude.

5.4. Algoritmo Quântico para Encontrar o Período de uma Função Periódica usando a Busca Quântica Assintótica

A transformada quântica de Fourier (TQF) está no coração de algoritmos quânticos importantes, como o algoritmo de fatorização de Shor [64] e algoritmo quântico de contagem [10]. A tarefa mais básica da TQF é encontrar o período de estados periódicos. Sejam o estado quântico periódico $|\psi\rangle$ e sua TQF dados por

$$|\psi\rangle = U_r |0^{\otimes N}\rangle = \sqrt{r/M} \sum_{j=0}^{M/r-1} |jr\rangle, \quad (5.21)$$

$$U_{QFT} |\psi\rangle = r^{-1/2} \sum_{j=0}^{r-1} |jM/r\rangle, \quad (5.22)$$

sendo U_{QFT} o operador unitário que implementa a TQF, $M = 2^N$ (N é o número de qubits) e r é o período, um número inteiro que divide M . Medindo s cópias of (5.22), a probabilidade de obter M/r como o máximo divisor comum do conjunto composto pelos resultados das medições é, pelo menos, $1 - r/2^s$ [65]. Aqui, o cálculo do período r é transformado na busca de um mínimo, e então o algoritmo de busca quântica assintótica é utilizado para encontrar r realizando apenas uma medição. Para isso, pode-se observar que o mínimo de $f(x) = (x-1) \bmod M$, $x \in [0, r-1]$, é $M/r - 1$. Portanto, usando (5.22) como estado de

entrada, $\sum_x c_x |x\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |jM/r\rangle$, $f(x) = (x-1) \bmod M$ e a porta U mostrada na Fig.

5.1, a busca assintótica pode ser usada para encontrar o período r . O circuito quântico é mostrado na Fig. 5.2, na qual $A = U_{QFT} U_r$.

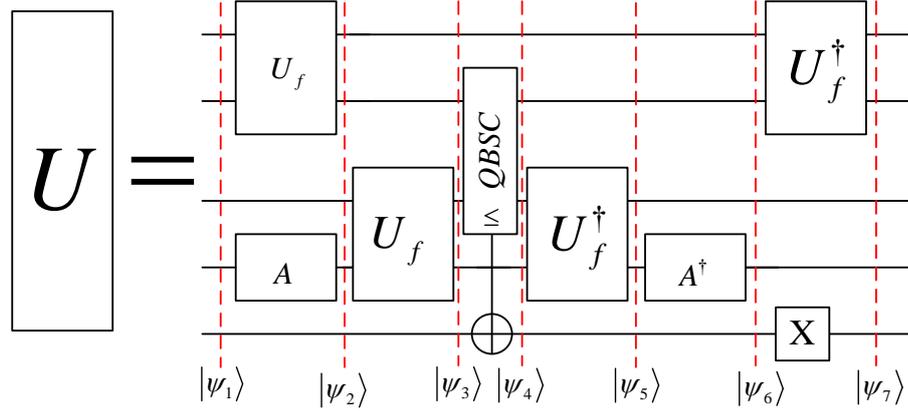


Figura 5.2. Circuito quântico para encontrar o período de uma função periódica, usando a busca quântica assintótica.

Seguindo os estados quânticos nos pontos marcados, como feito anteriormente, chega-se a

$$\begin{aligned}
 |\psi_7\rangle = & \left[\frac{1}{\sqrt{r}} \left| \frac{M}{r} \right\rangle_1 |0^{\otimes N}\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 + \sum_{j \neq 1} \frac{1}{\sqrt{r}} \frac{n(j)}{r} \left| \frac{jM}{r} \right\rangle_1 |0^{\otimes N}\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 \right] |0\rangle_5 + \\
 & + \left[\sum_{j \neq 1} \frac{1}{\sqrt{r}} \left| \frac{jM}{r} \right\rangle_1 |0^{\otimes N}\rangle_2 \left(\sum_{\substack{t=1 \\ A^{\otimes N}|y_t\rangle \neq |0^{\otimes N}\rangle}}^{n(j)} \frac{1}{\sqrt{r}} A^{\otimes N} |y_t\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |0\rangle_5 + \\
 & + \left[\sum_{j \neq 1} \frac{1}{\sqrt{r}} \left| \frac{jM}{r} \right\rangle_1 |0^{\otimes N}\rangle_2 \left(\sum_{l=1}^{r-n(j)} \frac{1}{\sqrt{r}} A^{\otimes N} |y_l\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |1\rangle_5.
 \end{aligned} \tag{5.23}$$

Em (5.23) tem-se que $1 \leq n(j) \leq r$, em particular $n(1) = r$. Após k aplicações de U , o estado final antes da amplificação de amplitude é

$$\begin{aligned}
 & \left[\frac{1}{\sqrt{r}} \left| \frac{M}{r} \right\rangle_1 |0^{\otimes N}\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 + \sum_{j \neq 1} \frac{1}{\sqrt{r}} \left[\frac{n(j)}{r} \right]^k \left| \frac{jM}{r} \right\rangle_1 |0^{\otimes N}\rangle_2 |0^{\otimes N}\rangle_4 |0^{\otimes N}\rangle_3 \right] |0\rangle_5 + \\
 & + \sum_{p=1}^k \left[\sum_{j \neq 1} \frac{1}{\sqrt{r}} \left[\frac{n(j)}{r} \right]^{p-1} \left| \frac{jM}{r} \right\rangle_1 |0^{\otimes N}\rangle_2 \left(\sum_{\substack{t=1 \\ A^{\otimes N}|y_t\rangle \neq |0^{\otimes N}\rangle}}^{n(j)} \frac{1}{\sqrt{r}} A^{\otimes N} |y_t\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |0\rangle_5 + \\
 & + \sum_{p=1}^k \left[\sum_{j \neq 1} \frac{1}{\sqrt{r}} \left[\frac{n(j)}{r} \right]^{p-1} \left| \frac{jM}{r} \right\rangle_1 |0^{\otimes N}\rangle_2 \left(\sum_{l=1}^{r-n(j)} \frac{1}{\sqrt{r}} A^{\otimes N} |y_l\rangle_4 \right) |0^{\otimes N}\rangle_3 \right] |1\rangle_5.
 \end{aligned} \tag{5.24}$$

Observando (5.24), pode-se notar que após a amplificação de amplitude uma medição no primeiro registrador fornecerá o resultado $\left| \frac{M}{r} \right\rangle$ com probabilidade próxima de 1.

5.5. Conclusão

Foi proposto um novo algoritmo quântico para achar o mínimo de uma função que exige apenas uma medição. Isto é importante, uma vez que medições de qubits não estão livres de ruídos. Este algoritmo é uma busca quântica assintótica. Suas vantagens são a alta probabilidade de obter o resultado correto e o fato de que a busca quântica e as medições são realizadas apenas uma vez. A desvantagem é o número de operações a serem realizadas antes da amplificação de amplitude. Como exemplo de sua aplicação, construiu-se um algoritmo quântico, para encontrar o período de uma função periódica.

CAPÍTULO 6

CONCLUSÕES E TRABALHOS FUTUROS

Os três focos principais desta tese são:

- i) O cálculo da negatividade de estados quânticos via menores principais;
- ii) A proposição de uma medida para o cálculo do entrelaçamento de seis qubits.
- iii) A proposição de um algoritmo quântico que permite encontrar o mínimo de uma função com apenas uma medição.

Neste sentido, as contribuições desta tese foram:

1. A determinação de uma relação entre a negatividade e os menores principais da transposta parcial da matriz densidade de um estado quântico de dois qubits, que permite que os problemas onde a negatividade é usada, possam ser abordados pelos menores principais, em particular, as medidas de entrelaçamento (Capítulo 2).
2. Para estados puros tripartes de qubits, mostrou-se que o quadrado da negatividade do estado $X(YZ)$ é igual à soma dos menores principais de ordem 3 da transposta parcial da matriz densidade do estado. Para estados quadripartes de qubits, tem-se também que o quadrado da negatividade do estado $W(XYZ)$ é igual à soma dos menores principais de ordem 3 da transposta parcial da matriz densidade do estado. Em ambos os casos, a soma de todos os menores principais de ordem 3, é a característica relevante. Assim, é suficiente determinar o polinômio característico e tomar o termo S_3 (Capítulo 3).
3. A principal contribuição desta tese é a proposta de uma medida de entrelaçamento para estados puros de seis qubits: o entrelaçamento residual baseado na negatividade, γ_6 . Esta medida se apresenta com duas vantagens importantes: ela é fácil de ser calculada, visto que não é necessário proceder a uma minimização, e mede exclusivamente o entrelaçamento em seis vias (Capítulo 4).

4. Foi proposto um novo algoritmo quântico, que é uma busca assintótica, para achar o mínimo de uma função que exige apenas uma medição, com uma alta probabilidade de obter o resultado correto. Este algoritmo tem uma desvantagem: o número de operações a serem realizadas antes da amplificação de amplitude que é da ordem do tamanho da base de dados (Capítulo 5). Como exemplo foi descrito um algoritmo para encontrar o período de uma função periódica.

As perspectivas de continuidade deste trabalho são:

1. A generalização das relações entre negatividade e menores principais para estados de n qubits;
2. Obter uma medida de entrelaçamento para estados de 5 qubits;
3. Obter medidas de entrelaçamento baseadas em negatividades para estados com mais de seis qubits;
4. Fazer uma análise de complexidade do algoritmo de busca proposto.

APÊNDICES

Resumo

Nos Apêndices a seguir serão apresentados alguns tópicos de Álgebra Linear, junto com a notação usada em Mecânica Quântica (Apêndice 1), alguns Fundamentos de Informação Quântica (Apêndice 2), Algoritmo de Grover, Amplificação de Amplitude e a Transformada Quântica de Fourier (Apêndice 3). A inserção desses Apêndices no referido trabalho tem como objetivo facilitar a leitura do mesmo, fornecendo uma fonte de consulta auxiliar aos que vierem a se interessar pelo tema.

APÊNDICE 1

ÁLGEBRA LINEAR

I.1. Números Complexos

O conjunto $\mathbb{C} = \{\alpha; \alpha = x + iy, x, y \in \mathbb{R}, i^2 = -1\}$ é denominado conjunto dos números complexos. O módulo de $\alpha = x + iy$, $|\alpha|$, é definido por $|\alpha| = \sqrt{x^2 + y^2}$. Se $\varphi \in [0, 2\pi)$, então $\alpha \in \mathbb{C}$ pode ser escrito na forma $\alpha = |\alpha|e^{i\varphi} = |\alpha|(\cos \varphi + \text{sen} \varphi)$. O número complexo α^* , chamado conjugado de $\alpha \in \mathbb{C}$, é definido por $\alpha^* = x - iy = e^{-i\varphi}$. Observe que:

- (i) $|\alpha|^2 = \alpha\alpha^*, \forall \alpha \in \mathbb{C}$;
- (ii) $|\alpha + \beta| \leq |\alpha| + |\beta|, \forall \alpha, \beta \in \mathbb{C}$.

I.2. Espaços de Hilbert de Dimensão Finita (Sistemas Quânticos)

O conceito de espaço de Hilbert é extremamente importante em Computação Quântica e Informação quântica. Isto deve-se ao fato de que o estado de um sistema quântico é descrito por um vetor ou um operador densidade em um espaço de Hilbert. Um *espaço de Hilbert* N -dimensional é um espaço vetorial \mathcal{H} , complexo de dimensão N , com produto interno. Um vetor $|\psi\rangle \in \mathcal{H}$ é chamado vetor de estado, e \mathcal{H} , o espaço de estado. Para representar um vetor de estado, $|\psi\rangle \in \mathcal{H}$, a notação padrão utilizada em mecânica quântica, é a notação de Dirac: um vetor linha é denotado por $\langle\psi|$ (bra de ψ), e um vetor coluna, por $|\psi\rangle$ (ket de ψ). Sendo \mathcal{B} uma base de \mathcal{H} , um estado quântico, que é uma superposição de todos os estados dessa base, é representado por um vetor de norma 1, em \mathcal{H} . De acordo com a definição de espaço de Hilbert, $\mathcal{H} = \mathbb{C}^N$, com $N = 2^n$ e $n \in \mathbb{N}$. Se $\mathcal{B} = \{|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle\}$, então,

$$|\psi\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle, \quad (\text{I.1})$$

onde $|i\rangle \in \mathcal{B}$, $\alpha_i \in \mathbb{C}$ e $\sum_{i=0}^{N-1} |\alpha_i|^2 = 1$. Dado um vetor coluna $|\psi\rangle$, o vetor linha correspondente de $|\psi\rangle$, é o vetor $\langle\psi|$, dado por $\langle\psi| = (|\psi\rangle)^\dagger$. Assim,

$$\langle\psi| = \sum_{i=0}^{N-1} \alpha_i^* \langle i|, \quad (\text{I.2})$$

onde α_i^* é o conjugado complexo de α_i e $\langle i| = (|i\rangle)^\dagger$.

I.2.1. Produto Interno

O *produto interno* em \mathbb{C}^N ,

$$\begin{aligned} \langle \bullet | \bullet \rangle : \mathbb{C}^N \times \mathbb{C}^N &\rightarrow \mathbb{C} \\ (|\psi_1\rangle, |\psi_2\rangle) &\mapsto \langle\psi_1|\psi_2\rangle, \end{aligned} \quad (\text{I.3})$$

é uma aplicação de $\mathbb{C}^N \times \mathbb{C}^N$ em \mathbb{C} , que transforma o par de vetores $(|\psi_1\rangle, |\psi_2\rangle) \in \mathbb{C}^N \times \mathbb{C}^N$ (dois vetores de dimensão N) em um número complexo $\langle\psi_1|\psi_2\rangle$, chamado *produto interno* de $|\psi_1\rangle$ e $|\psi_2\rangle$. É este produto interno que torna \mathbb{C}^N um espaço de Hilbert de dimensão N . Se

$|\psi_1\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle$ e $|\psi_2\rangle = \sum_{i=0}^{N-1} \beta_i |i\rangle$ são vetores em \mathbb{C}^N , então, o *produto interno* de $|\psi_1\rangle$ e $|\psi_2\rangle$

é obtido assim

$$\langle\psi_1|\psi_2\rangle = \sum_{i=0}^{N-1} \alpha_i^* \beta_i = \langle\psi_2|\psi_1\rangle^*. \quad (\text{I.4})$$

Voltando às equações (I.1) e (I.2), os vetores $|\psi\rangle$ e $\langle\psi|$ podem ser escritos na base $\mathcal{B} = \{|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle\}$, podem ainda ser escritos, respectivamente, como

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} \text{ e } (|\psi\rangle)^\dagger = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix}^\dagger = (\alpha_0^* \quad \alpha_1^* \quad \cdots \quad \alpha_{N-1}^*) = \langle\psi|, \quad (\text{I.5})$$

onde $\alpha_i = \langle i|\psi\rangle$, $i = 0, 1, 2, \dots, N-1$.

Cada um dos vetores na base $\mathcal{B} = \{|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle\}$ pode ser escrito como uma seqüência binária de $n = \log_2(N)$ bits, assim: $\underbrace{|000\dots 0\rangle}_n, |000\dots 1\rangle, |000\dots 10\rangle, \dots, |111\dots 1\rangle$.

Então, os vetores acima correspondem aos vetores colunas:

$$\underbrace{|000\dots 0\rangle}_n = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}; \underbrace{|000\dots 1\rangle}_n = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}; \dots; \underbrace{|111\dots 1\rangle}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \quad (\text{I.6})$$

A norma de um vetor $|\psi\rangle \in \mathbb{C}^N$ é definida por $\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$. Se o vetor de estado é unitário, então $\| |\psi\rangle \| = 1$ (condição de normalização). Para os vetores $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^N$, vale a desigualdade triangular $\| \alpha|\psi_1\rangle + \beta|\psi_2\rangle \| \leq \| \alpha|\psi_1\rangle \| + \| \beta|\psi_2\rangle \|$, $\alpha, \beta \in \mathbb{C}$.

I.2.2. Produto Externo

O *produto externo* em \mathbb{C}^N ,

$$\begin{aligned} |\cdot\rangle\langle\cdot|: \mathbb{C}^N \times \mathbb{C}^N &\rightarrow \mathbb{C}^{N \times N} \\ (|\psi_1\rangle, |\psi_2\rangle) &\mapsto |\psi_1\rangle\langle\psi_2|, \end{aligned} \quad (\text{I.7})$$

é uma aplicação que transforma um par de vetores de \mathbb{C}^N (dimensão N) em uma matriz $N \times N$, denotada por $|\psi_1\rangle\langle\psi_2|$ (produto externo de $|\psi_1\rangle$ e $|\psi_2\rangle$). Usando-se

$\mathcal{B} = \{|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle\}$ como uma base de \mathbb{C}^N , o produto externo $|\psi_1\rangle\langle\psi_2|$ é obtido da seguinte maneira $|\psi_1\rangle\langle\psi_2| = \left(\sum_{i=0}^{N-1} \alpha_i |i\rangle \right) \left(\sum_{j=0}^{N-1} \beta_j^* \langle j| \right)$, ou seja,

$$|\psi_1\rangle\langle\psi_2| = \sum_{i,j=0}^{N-1} \alpha_i \beta_j^* |i\rangle\langle j|, \quad (\text{I.8})$$

onde $\alpha_i, \beta_j \in \mathbb{C}$, $|i\rangle\langle j|$ é uma matriz $N \times N$, com os elementos da i -ésima linha e j -ésima coluna iguais 1, e os demais elementos iguais a 0.

Se $|\psi\rangle, |\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^N$, então, o produto externo tem as seguintes propriedades:

- (i) $\langle\psi|\psi_1\rangle \neq |\psi\rangle\langle\psi_1|$;
- (ii) $|\psi\rangle(\langle\psi_1| + \langle\psi_2|) = |\psi\rangle\langle\psi_1| + |\psi\rangle\langle\psi_2|$;
- (iii) $(|\psi\rangle\langle\psi_1|)(|\psi_1\rangle\langle\psi|) = |\psi\rangle\langle\psi|$, pois, $\langle\psi_1|\psi_1\rangle = 1$.

I.3. Medidas

Dados os estados $|\psi\rangle, |\phi\rangle \in \mathbb{C}^N$, de acordo com a mecânica quântica, a probabilidade de se obter o resultado “ $|\psi\rangle$ ” quando o estado observado é “ $|\phi\rangle$ ”, é dada por

$$p_{|\psi\rangle,|\phi\rangle} = |\langle\psi|\phi\rangle|^2 = \langle\psi|\phi\rangle\langle\phi|\psi\rangle^*. \quad (\text{I.9})$$

Verifica-se que:

- (i) $0 \leq |\langle\psi|\phi\rangle|^2 \leq 1$;
- (ii) Se $\langle\psi|\phi\rangle = 0$, então $|\psi\rangle$ e $|\phi\rangle$ são ortogonais;
- (iii) Se $\langle\psi|\phi\rangle = 1$, então $|\psi\rangle$ e $|\phi\rangle$ são idênticos a menos de um fator de fase geral.

Embora, matematicamente presente, tal diferença de fase nunca pode ser observada na realidade, e assim, ele não tem relevância física.

I.4. Construção do Produto Tensorial

Dados dois espaços de Hilbert, usando a operação “ \otimes ”, que será chamada de *produto tensorial*, é possível construir um terceiro espaço de Hilbert, que é o produto tensorial entre os mesmos. Isto significa que, se os espaços considerados são \mathbb{C}^N e \mathbb{C}^M , então eles podem ser combinados para formar um novo espaço, representado por $\mathbb{C}^{NM} = \mathbb{C}^N \otimes \mathbb{C}^M$, e chamado produto tensorial dos espaços \mathbb{C}^N e \mathbb{C}^M . Sejam $\mathcal{B}_1 = \{|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle\}$ e $\mathcal{B}_2 = \{|0\rangle, |1\rangle, |2\rangle, \dots, |M-1\rangle\}$ bases de \mathbb{C}^N e \mathbb{C}^M , respectivamente. Assim, o conjunto $\mathcal{B}_1 \otimes \mathcal{B}_2 = \{|i\rangle \otimes |j\rangle; 0 \leq i \leq N-1 \text{ e } 0 \leq j \leq M-1\}$ é uma base de $\mathbb{C}^{NM} = \mathbb{C}^N \otimes \mathbb{C}^M$.

I.4.1. Produto Tensorial

O estado produto tensorial,

$$\begin{aligned} \otimes: \mathbb{C}^N \times \mathbb{C}^M &\rightarrow \mathbb{C}^N \otimes \mathbb{C}^M \\ (|\psi_1\rangle, |\psi_2\rangle) &\mapsto |\psi_1\rangle \otimes |\psi_2\rangle, \end{aligned} \quad (\text{I.10})$$

dos estados $|\psi_1\rangle \in \mathbb{C}^N$ e $|\psi_2\rangle \in \mathbb{C}^M$, é uma aplicação de $\mathbb{C}^N \times \mathbb{C}^M$ em $\mathbb{C}^N \otimes \mathbb{C}^M$, que transforma $(|\psi_1\rangle, |\psi_2\rangle) \in \mathbb{C}^N \times \mathbb{C}^M$ em $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathbb{C}^N \otimes \mathbb{C}^M$ (produto tensorial). Se $|\psi_1\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle$ e $|\psi_2\rangle = \sum_{j=0}^{M-1} \beta_j |j\rangle$, então $|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1, \psi_2\rangle = \left(\sum_{i=0}^{N-1} \alpha_i |i\rangle \right) \left(\sum_{j=0}^{M-1} \beta_j |j\rangle \right)$, ou seja,

$$|\psi_1\rangle \otimes |\psi_2\rangle = \sum_{i \in \mathcal{B}_1, j \in \mathcal{B}_2} \alpha_i \beta_j |i, j\rangle \in \mathbb{C}^{NM} = \mathbb{C}^N \otimes \mathbb{C}^M. \quad (\text{I.11})$$

I.4.1.1. Conjugado Transposto do Produto Tensorial

O conjugado transposto do produto tensorial $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathbb{C}^N \otimes \mathbb{C}^M$ é obtido da seguinte maneira:

$$(|\psi_1\rangle \otimes |\psi_2\rangle)^\dagger = \langle \psi_2 | \otimes \langle \psi_1 |. \quad (\text{I.12})$$

Se $\mathcal{B}_1 = \{|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle\}$ e $\mathcal{B}_2 = \{|0\rangle, |1\rangle, |2\rangle, \dots, |M-1\rangle\}$, então o produto tensorial, na notação de vetor, é dado por:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{M-1} \end{pmatrix} = \begin{pmatrix} \alpha_0 \beta_0 \\ \alpha_0 \beta_1 \\ \vdots \\ \alpha_0 \beta_{M-1} \\ \alpha_1 \beta_0 \\ \vdots \\ \alpha_{N-1} \beta_{M-1} \end{pmatrix}. \quad (\text{I.13})$$

Se $\| |\psi_1\rangle \| = \| |\psi_2\rangle \| = 1$, então $\| |\psi_1\rangle \otimes |\psi_2\rangle \| = 1$.

O produto tensorial tem as seguintes propriedades:

- (i) $|\psi_1\rangle \otimes |\psi_2\rangle \neq |\psi_2\rangle \otimes |\psi_1\rangle$ ($|\psi_1, \psi_2\rangle \in \mathbb{C}^{NM}$ e $|\psi_2, \psi_1\rangle \in \mathbb{C}^{MN}$);
- (ii) $|\psi_1\rangle \otimes (|\psi_2\rangle \otimes |\psi_3\rangle) = (|\psi_1\rangle \otimes |\psi_2\rangle) \otimes |\psi_3\rangle$, $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle \in \mathbb{C}^N$;
- (iii) $|\psi_1\rangle \otimes (\alpha |\psi_2\rangle + \beta |\psi_3\rangle) = |\psi_1\rangle \otimes \alpha |\psi_2\rangle + |\psi_1\rangle \otimes \beta |\psi_3\rangle = \alpha |\psi_1, \psi_2\rangle + \beta |\psi_1, \psi_3\rangle$, para $|\psi_1\rangle \in \mathbb{C}^N$, $|\psi_2\rangle, |\psi_3\rangle \in \mathbb{C}^M$ e $\alpha, \beta \in \mathbb{C}$.

I.4.2. Produto Tensorial entre Matrizes

O produto tensorial definido acima pode ser estendido para matrizes. Para isto, considere as matrizes $A \in \mathbb{C}^{m \times n}$ e $B \in \mathbb{C}^{p \times q}$, de ordens $m \times n$ e $p \times q$, respectivamente (m, n, p e q são potências de 2). O produto tensorial entre as matrizes A e B é a matriz $A \otimes B \in \mathbb{C}^{(m \times n)(p \times q)}$, definida por

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{pmatrix}, \quad (\text{I.14})$$

onde A_{ij} é o elemento da i -ésima linha e j -ésima coluna de A . Os elementos da matriz $A \otimes B$ são dados por

$$(A \otimes B)_{rs} = A_{ij} B_{kl}, \quad (\text{I.15})$$

onde $r = (i-1)p + k$ e $s = (j-1)q + l$, com $1 \leq i \leq m$, $1 \leq j \leq n$, $1 \leq k \leq p$ e $1 \leq l \leq q$ [55].

I.5. Matrizes Unitárias

Considere $\mathcal{U}(n) = \{U \in \mathbb{C}^{n \times n}; UU^\dagger = I\}$. Este conjunto de operadores lineares preservando norma em \mathbb{C}^n é um grupo de matrizes $U \in \mathbb{C}^{n \times n}$ complexas, chamadas *matrizes unitárias*. O conjugado Hermitiano ou transposto conjugado de U , indicado por U^\dagger , é definido por

$$U_{ij}^\dagger = U_{ji}^*, \quad (\text{I.16})$$

$1 \leq i, j \leq n$ e I é a matriz identidade de ordem n .

Seja $|\psi\rangle \in \mathbb{C}^n$, $|\psi\rangle = \sum_{i=0}^{n-1} \alpha_i |i\rangle$, $|i\rangle \in \{|0\rangle, |1\rangle, \dots, |n-1\rangle\}$. Como $U \in \mathbb{C}^{n \times n}$ é um operador

linear, tem-se

$$U|\psi\rangle = U\left(\sum_{i=0}^{n-1} \alpha_i |i\rangle\right) = \sum_{i=0}^{n-1} \alpha_i U|i\rangle. \quad (\text{I.17})$$

Assim, se são conhecidos os valores de U nos estados da base $|i\rangle \in \{|0\rangle, |1\rangle, \dots, |n-1\rangle\}$, então os valores de U sobre todos os estados quânticos em \mathbb{C}^n são também conhecidos.

Toda matriz $U \in \mathcal{U}(n)$ pode ser escrita como uma soma de produtos externos.

De fato, sendo $|\psi\rangle = \sum_{i=0}^{n-1} \alpha_i |i\rangle$, com $|i\rangle \in \{|0\rangle, |1\rangle, \dots, |n-1\rangle\}$ e $\langle i|\psi\rangle = \alpha_i$, tem-se,

$$\left(\sum_{i=0}^{n-1} |i\rangle\langle i| \right) |\psi\rangle = \sum_{i=0}^{n-1} |i\rangle\langle i|\psi\rangle = \sum_{i=0}^{n-1} \alpha_i |i\rangle = |\psi\rangle, \text{ ou seja,}$$

$$\sum_{i=0}^{n-1} |i\rangle\langle i| = I. \quad (\text{I.18})$$

Agora, como $U = I_U U I_U$, tem-se que

$$U = \sum_{i,j=0}^{n-1} U_{ij} |i\rangle\langle j|, \quad (\text{I.19})$$

onde $U_{ij} = \langle i|U|j\rangle$.

Da linearidade de U , segue que:

$$U|\psi\rangle = \left(\sum_{i,j=0}^{n-1} U_{ij} |i\rangle\langle j| \right) \left(\sum_{l=0}^{n-1} \alpha_l |l\rangle \right) = \sum_{l,x=0}^{n-1} \alpha_l U_{xy} |x\rangle. \quad (\text{I.20})$$

As matrizes unitárias preservam produto interno (portanto, preserva norma). De fato, definindo $|\psi_1\rangle = U|\psi\rangle$ e $|\phi_1\rangle = U|\phi\rangle$, com $|\psi\rangle, |\phi\rangle \in \mathbb{C}^n$ e $U \in \mathbb{C}^{n \times n}$, tem-se

$$\langle \psi_1 | \phi_1 \rangle = \langle \psi_1 | U^\dagger U | \phi_1 \rangle = \langle \psi | I | \phi \rangle = \langle \psi | \phi \rangle. \quad (\text{I.21})$$

Isto significa que U é unitária se, e somente se, os vetores linhas de U formarem uma base ortonormal de \mathbb{C}^n (de modo análogo para as colunas de U). De fato, a entrada na i -ésima linha e j -ésima coluna de UU^* é o produto escalar do i -ésimo vetor linha de U com o j -ésimo vetor coluna de U^* . No entanto, a menos da notação, o j -ésimo vetor coluna de U^* é o j -ésimo vetor linha de U . Assim, se $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ são vetores linhas de U , então o produto UU^* pode ser expresso por

$$UU^* = \begin{pmatrix} \langle \psi_1 | \psi_1 \rangle & \langle \psi_1 | \psi_2 \rangle & \cdots & \langle \psi_1 | \psi_n \rangle \\ \langle \psi_2 | \psi_1 \rangle & \langle \psi_2 | \psi_2 \rangle & \cdots & \langle \psi_2 | \psi_n \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \psi_n | \psi_1 \rangle & \langle \psi_n | \psi_2 \rangle & \cdots & \langle \psi_n | \psi_n \rangle \end{pmatrix}. \quad (\text{I.22})$$

Portanto,

$$UU^* = I \Leftrightarrow \begin{cases} \langle \psi_i | \psi_j \rangle = 1, & \text{se } i = j \\ \langle \psi_i | \psi_j \rangle = 0, & \text{se } i \neq j \end{cases}, \quad (\text{I.23})$$

ou seja, $UU^* = I$, se e somente se, $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ é uma base ortonormal \mathbb{C}^n .

O conjunto das matrizes unitárias de ordem $n \times n$ é um subconjunto do conjunto das matrizes quadradas de mesma ordem $n \times n$. Devido à importância destas para a mecânica quântica, o produto tensorial de matrizes unitárias é, em particular, destacado aqui.

Especificamente, sejam $U \in \mathcal{U}(n)$ e $W \in \mathcal{U}(m)$ matrizes definidas por $U = \sum_{i,j=0}^{n-1} U_{ij} |i\rangle\langle j|$ e

$$W = \sum_{k,l=0}^{m-1} W_{kl} |k\rangle\langle l|, \text{ com } |i\rangle, |j\rangle \in \{|0\rangle, |1\rangle, \dots, |n-1\rangle\} \text{ e } |k\rangle, |l\rangle \in \{|0\rangle, |1\rangle, \dots, |m-1\rangle\}.$$

Então, para o produto tensorial

$$\begin{aligned} \otimes: \mathbb{C}^{n \times n} \times \mathbb{C}^{m \times m} &\rightarrow \mathbb{C}^{nm \times nm} = \mathbb{C}^{n \times n} \otimes \mathbb{C}^{m \times m} \\ (U, W) &\mapsto U \otimes W \end{aligned}, \quad (\text{I.24})$$

tem-se

$$U \otimes W = \sum_{i,j=0}^{n-1} \sum_{k,l=0}^{m-1} U_{ij} W_{kl} |i,k\rangle\langle j,l| \in \mathbb{C}^{nm \times nm}. \quad (\text{I.25})$$

Esta matriz, como foi visto acima, atua no espaço $\mathbb{C}^{nm \times nm} = \mathbb{C}^{n \times n} \otimes \mathbb{C}^{m \times m}$ gerado pelos estados da base $\{|0\rangle, |1\rangle, \dots, |n-1\rangle\} \otimes \{|0\rangle, |1\rangle, \dots, |m-1\rangle\}$. Para os estados $|\psi\rangle \in \mathbb{C}^n$ e $|\phi\rangle \in \mathbb{C}^m$, tem-se

$$(U \otimes W)(|\psi\rangle, |\phi\rangle) = U|\psi\rangle \otimes W|\phi\rangle \in \mathbb{C}^{nm}. \quad (\text{I.26})$$

Supondo $\mathcal{A} = \{|1\rangle, |2\rangle, \dots, |n\rangle\}$ e $\mathcal{B} = \{|1\rangle, |2\rangle, \dots, |m\rangle\}$, o produto tensorial de duas matrizes unitárias é descrito por

$$U \otimes W = \begin{pmatrix} U_{11}W & U_{12}W & \dots & U_{1n}W \\ U_{21}W & \ddots & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ U_{n1}W & \dots & \dots & U_{nn}W \end{pmatrix} = \begin{pmatrix} U_{11}W_{11} & U_{11}W_{12} & \dots & U_{1n}W_{1m} \\ U_{21}W_{21} & \ddots & \dots & U_{1n}W_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ U_{n1}W_{m1} & \dots & \dots & U_{nn}W_{mm} \end{pmatrix}. \quad (\text{I.27})$$

Observe que:

- (i) $U \otimes W \neq W \otimes U$, $U, W \in \mathcal{U}(n)$;
- (ii) $U_1 \otimes (U_2 \otimes U_3) = (U_1 \otimes U_2) \otimes U_3$, $U_1, U_2, U_3 \in \mathcal{U}(n)$;
- (iii) $U_1, U_2 \in \mathcal{U}(n)$ e $W_1, W_2 \in \mathcal{U}(n) \Rightarrow (U_1 \otimes W_1)(U_2 \otimes W_2) = U_1 U_2 \otimes W_1 W_2$;
- (iv) $UU^\dagger = I$ e $WW^\dagger = I \Rightarrow U \otimes W$ é unitária e $(U \otimes W)^\dagger = U^\dagger \otimes W^\dagger$.

De fato, por (iii), $(U \otimes W)(U \otimes W)^\dagger = (U \otimes W)(U^\dagger \otimes W^\dagger) = UU^\dagger \otimes WW^\dagger = I \otimes I = I_{U \otimes W}$.

I.6. Decomposição Autovalor/Autovetor

Seja $U \in \mathcal{U}(n)$, em que $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle$ e $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{C}$ são, respectivamente, os seus autovetores e autovalores. Então, o operador U pode ser expresso da seguinte forma

$$U = \sum_{i=0}^{n-1} \lambda_i |\psi_i\rangle \langle \psi_i|, \quad (\text{I.28})$$

em que $|\lambda_i| = 1$ e $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ é uma base ortonormal de \mathbb{C}^n . Em particular, para a matriz identidade I tem-se que $\lambda_i = 1$.

O conjugado transposto de U é dado por:

$$U^\dagger = \sum_{i=0}^{n-1} \lambda_i^* |\psi_i\rangle \langle \psi_i|, \quad (\text{I.29})$$

em que $|\lambda_i^*| = 1$ e $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ é uma base ortonormal de \mathbb{C}^n .

Quando U tem a forma (I.28) e $W \in \mathcal{U}(n)$ tem decomposição em autovetores dada por $W = \sum_{j=0}^{m-1} \mu_j |\phi_j\rangle\langle\phi_j|$, então para o produto tensorial de U e W , tem-se

$$U \otimes W = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \lambda_i \mu_j |\psi_i, \phi_j\rangle\langle\psi_i, \phi_j|. \quad (\text{I.30})$$

Observe que se $\{|1\rangle, |2\rangle, \dots, |d\rangle\}$ é uma base ortonormal de \mathcal{H} e se $\{|1\rangle, |2\rangle, \dots, |k\rangle\}$ é uma base ortonormal de um subespaço \mathcal{W} de \mathcal{H} , então um projetor P sobre \mathcal{W} é definido por

$$P = \sum_{i=1}^k |i\rangle\langle i|. \quad (\text{I.31})$$

Um projetor P em \mathcal{H} é um operador que satisfaz $P^2 = P$.

Um projetor P em \mathcal{H} é um projetor ortogonal que satisfaz $P^\dagger = P$, isto é, P é Hermitiano.

APÊNDICE 2

FUNDAMENTOS DE INFORMAÇÃO QUÂNTICA

II.1. Fundamentos Básicos: Bits Quânticos

Em computação clássica, o conceito fundamental é o bit, ou seja, o bit é a menor porção de informação disponível, assumindo apenas dois valores, 0 e 1, por exemplo [1]. A versão quântica do bit clássico é o bit quântico, chamado de qubit. Sendo assim, o bit é substituído pelo qubit e, os valores 0 e 1 de um bit, são substituídos, respectivamente, pelos vetores $|0\rangle$ e $|1\rangle$: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Um qubit genérico $|\psi\rangle$ é uma combinação linear dos vetores $|0\rangle$ e $|1\rangle$, ou seja,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (\text{II.1})$$

com $\alpha, \beta \in \mathbb{C}$. Usando a notação de vetores, tem-se:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \quad (\text{II.2})$$

No Apêndice I foi visto que os vetores $|0\rangle$ e $|1\rangle$ formam uma base ortonormal do espaço vetorial complexo \mathbb{C}^2 , chamada base computacional. Neste caso, o vetor (estado) $|\psi\rangle$ é denominado superposição dos vetores $|0\rangle$ e $|1\rangle$, com amplitudes α e β . O sentido físico do qubit é que ele está simultaneamente nos estados $|0\rangle$ e $|1\rangle$, e isso faz com que a quantidade de informação armazenada no estado $|\psi\rangle$ seja infinita, informação esta que se encontra no nível quântico. Para ter acesso a essa informação no nível clássico, é preciso fazer uma medição. E, assim, feita a medição, define-se de forma irreversível o valor do qubit, obtendo-

se $|0\rangle$ com probabilidade $|\alpha|^2$ e $|1\rangle$, com probabilidade $|\beta|^2$. Como só existem duas possibilidades, $|0\rangle$ ou $|1\rangle$, tem-se $|\alpha|^2 + |\beta|^2 = 1$, ou seja, $\|\psi\rangle\| = 1$, e isto significa que, matematicamente, um qubit é um vetor de norma 1, em \mathbb{C}^2 . Fisicamente, o sistema se comporta como se estivesse em sobreposição até que uma observação seja efetuada. Nesta situação, a informação colapsa definitivamente para um dos dois estados, $|0\rangle$ ou $|1\rangle$, de forma que não é possível descobrir para um qubit arbitrário, os valores de α ou β . Isto significa, que apesar desse comportamento, usando medições só é possível extrair do qubit apenas um dos estados da superposição.

Como foi visto acima, a unidade de informação quântica, se comporta matematicamente como um vetor unitário. Os valores α e β são as projeções da representação desse vetor sobre os eixos ortogonais, e definem as amplitudes para $|0\rangle$ e $|1\rangle$, respectivamente (Figura 7.1). Veja, por exemplo, o estado $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, uma superposição particularmente interessante, em que $\alpha = \beta = \frac{1}{\sqrt{2}}$ (Figura 7.1).

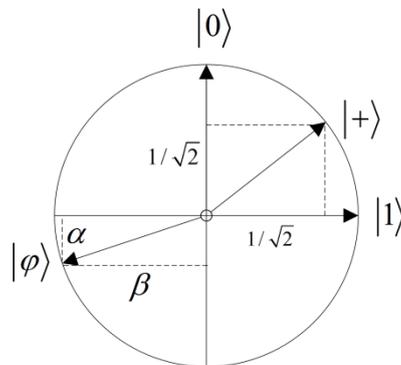


Figura 7.1. Representação geométrica de um qubit.

Em \mathbb{R}^3 , a Esfera de Bloch (esfera unitária), é a representação geométrica de 1 qubit. Na Figura 7.2, a projeção da representação do vetor $|\psi\rangle$ forma um ângulo θ , $0 \leq \theta \leq \pi$, com o eixo z , e a sua projeção sobre o plano xy forma um ângulo φ , $0 \leq \varphi \leq 2\pi$, com o eixo x . Passando a unidade de informação quântica $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, de coordenadas cartesianas para coordenadas polares e considerando-se $\alpha = a + ib$ e $\beta = c + id$, tem-se $\alpha = |\alpha|e^{i\gamma}$ e

$\beta = |\beta|e^{i(\gamma+\varphi)}$, com $0 \leq |\alpha| \leq 1$ e $0 \leq |\beta| \leq 1$. Tomando $|\alpha| = 2\arccos(\theta)$ e $|\beta| = 2\arcsen(\theta)$, obtém-se $\cos\left(\frac{\theta}{2}\right) = |\alpha|$ e $\sen\left(\frac{\theta}{2}\right) = |\beta|$. Se $\varphi = \arg(\beta) - \arg(\alpha)$, com $\gamma = \arg(\alpha)$, então:

$$|\psi\rangle = e^{i\gamma} \left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sen\left(\frac{\theta}{2}\right)|1\rangle \right). \quad (\text{II.3})$$

Como $|e^{i\gamma}| = 1$, $|\psi\rangle$ pode ser escrito na forma

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sen\left(\frac{\theta}{2}\right)|1\rangle. \quad (\text{II.4})$$

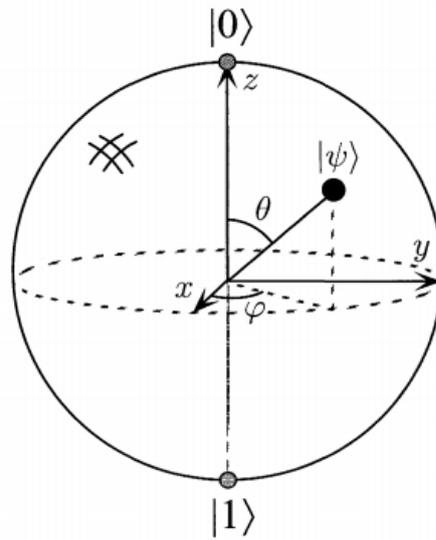
Assim, a representação polar de $|\psi\rangle$, em \mathbb{R}^3 , é dada por:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \cos(\varphi)\sen(\theta) \\ \sen(\varphi)\sen(\theta) \\ \cos(\theta) \end{pmatrix}, \quad (\text{II.5})$$

onde $0 \leq \theta \leq \pi$ e $0 \leq \varphi \leq 2\pi$. E, portanto, os vetores da base computacional de \mathbb{C}^2 , na Esfera de Bloch, são escritos como

$$|0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \text{ e } |1\rangle = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}, \quad (\text{II.6})$$

em que $|0\rangle$ é o pólo Norte da Esfera de Bloch, e $|1\rangle$, o pólo Sul.


 Figura 7.2. Esfera de Bloch do qubit $|\psi\rangle$.

O conceito de informação quântica pode ser ampliado para vários qubits, gerando assim uma superposição de estados com mais de 1 qubit. As operações são feitas através do produto tensorial entre os qubits envolvidos no cálculo. Assim, para 2 estados $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ e $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, da Seção 6.4 segue que

$$|\phi\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle. \quad (\text{II.7})$$

Note-se que os valores das componentes de $|\phi\rangle$ dão as amplitudes para todos os estados possíveis de 2 qubits, de forma que $|00\rangle$ pode ser obtido com probabilidade $|\alpha_1\alpha_2|^2$, $|01\rangle$ com probabilidade $|\alpha_1\beta_2|^2$, $|10\rangle$ com probabilidade $|\beta_1\alpha_2|^2$, e $|11\rangle$ com probabilidade $|\beta_1\beta_2|^2$.

Agora, generalizando esse conceito para um estado $|\phi\rangle$ de n qubits, tem-se:

$$|\phi\rangle = \alpha_0|0\dots 00\rangle + \alpha_1|0\dots 01\rangle + \dots + \alpha_{2^n-1}|1\dots 11\rangle, \quad (\text{II.8})$$

onde $\sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1$. Ou seja, para cada j , $0 \leq j \leq 2^n - 1$, $|\alpha_j|^2$ é a probabilidade de se encontrar cada um dos estados da superposição $|\phi\rangle$, no estado $|j\rangle$.

Independente da notação, o que é importante é deixar clara a idéia do paralelismo intrínseco definido pela superposição dos estados quânticos. Isso implica que, sob o ponto de vista de implementação, um registrador quântico de tamanho n permite armazenar um total de 2^n diferentes estados. É neste ponto que reside a diferença, quando comparado com o modelo clássico. Entretanto, após uma medição, todo o estado colapsa de maneira irreversível para apenas um determinado valor, passando a operar classicamente. Isto reforça a idéia de que operações destrutivas como esta devem ser feitas somente em certos momentos nos algoritmos, a fim de permitir que somente certos estados possam ser encontrados com a maior probabilidade possível.

II.2. Portas Quânticas

Uma porta lógica quântica é representada por uma matriz unitária. As portas quânticas mais comuns operam sobre 1 ou 2 qubits. Sendo assim, podem ser representadas por matrizes 2×2 e 4×4 , respectivamente. Uma porta que atua em n qubits é representada por uma matriz unitária $2^n \times 2^n$. O número de qubits na entrada da porta é igual ao número de qubits na saída. A ação de uma porta é determinada multiplicando-se a matriz que representa essa porta pelo vetor que representa o estado.

Os qubits podem ser manipulados através das portas quânticas, ou seja, a evolução no tempo de um sistema quântico isolado é feita por portas quânticas. Estas, assim como as suas análogas clássicas, constituem as unidades fundamentais para a construção de circuitos. Ao contrário de algumas portas clássicas, as portas quânticas, além de unitárias, são reversíveis. Isto significa que, se U é uma porta quântica, então

$$U^\dagger U = U U^\dagger = I, \quad (\text{II.9})$$

onde $U^\dagger = (U^*)^T$ (ver Seção I.5).

Assim, uma vez que as portas definem a evolução do sistema, todo o processamento executado pode ser desfeito. Por exemplo, sejam U uma porta unitária e $|\psi\rangle$ um estado, ambos com dimensões compatíveis. Aplicando a porta U em $|\psi\rangle$, obtém-se o estado $|\psi_1\rangle = U|\psi\rangle$. Agora, para obter o estado $|\psi\rangle$, a partir de $|\psi_1\rangle$, aplica-se a porta quântica U^\dagger , pois,

$$U^\dagger |\psi_1\rangle = U^\dagger U |\psi\rangle = I |\psi\rangle = |\psi\rangle. \quad (\text{II.10})$$

Isto significa que, sem operações de medição, a aplicação da porta U não causa perda de informação. Fisicamente, isto significa que o sistema perde menos energia, se aquece menos ou, em outras palavras, pode ficar mais econômico.

Dentre as portas elementares de 1 qubit, podem ser citadas:

1. Porta Identidade (I ou σ_0)

É uma porta que atua nos estados $|0\rangle$ e $|1\rangle$: $I|0\rangle = |0\rangle$ e $I|1\rangle = |1\rangle$. Assim,

$$I(a|0\rangle + b|1\rangle) = a|0\rangle + b|1\rangle, \quad (\text{II.11})$$

com $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2. Porta inversora de bit (X ou σ_1) ou Porta NOT Quântica

Esta porta é dada por um operador X que satisfaz $X|0\rangle = |1\rangle$ e $X|1\rangle = |0\rangle$. Assim,

$$X(a|0\rangle + b|1\rangle) = b|0\rangle + a|1\rangle \quad (\text{II.12})$$

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

3. Porta Y ou σ_2

A matriz associada à porta Y é dada por $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, e

$$Y(a|0\rangle + b|1\rangle) = i(a|0\rangle - b|1\rangle). \quad (\text{II.13})$$

4. Porta inversora de fase (Z ou σ_3)

A matriz associada à porta Z é dada por $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, e

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle. \quad (\text{II.14})$$

As portas I , X , Y e Z são também conhecidas como “matrizes de Pauli”. As portas X , Y e Z definem as rotações de 1 qubit na Esfera de Bloch, respectivamente, nos eixos x , y e z . Além disso, as quatro portas acima formam uma base para o conjunto das matrizes de dimensão 2×2 , já que toda matriz U pode ser descrita como

$$U = \sum_{k=0}^3 c_k \sigma_k, \quad (\text{II.15})$$

onde $k = 0, 1, 2, 3$.

A seguir, outras portas de 1 qubit de grande importância em Computação Quântica.

5. Porta Hadamard ou Porta H

Esta porta definida pelo operador $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, gera igual superposição entre os qubits, ou seja,

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \end{aligned} \quad (\text{II.16})$$

6. Porta Fase ou Porta S

É uma porta definida pelo operador $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, sendo

$$S(a|0\rangle + b|1\rangle) = a|0\rangle + ib|1\rangle. \quad (\text{II.17})$$

7. Porta $\pi/8$ ou Porta T

É uma porta definida pelo operador $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$, de modo que

$$T(a|0\rangle + b|1\rangle) = a|0\rangle + e^{i\pi/4}b|1\rangle. \quad (\text{II.18})$$

Outras portas podem ser obtidas a partir destas portas. Por exemplo, $H = (X + Z)/\sqrt{2}$, $S = T^2$ e $XYX = -Y$, de maneira que a quantidade de portas necessárias à computação de circuitos universais pode ser reduzida.

Portas de mais de 1 qubit podem ser arbitrariamente criadas, desde que respeitem a hermiticidade e a reversibilidade. Contudo, enquanto a simples utilização do produto tensorial de portas de 1 qubit possa gerar circuitos de dimensões superiores, o que é normalmente interessante é a utilização de portas não decomponíveis. Essas portas possuem uma importância fundamental porque são responsáveis por gerar entrelaçamento entre os estados quânticos, propriedade fundamental aos algoritmos quânticos. Em particular, um conjunto universal mínimo utiliza a chamada porta CNOT ou de inversão controlada

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (\text{II.19})$$

que pode ser obtida da seguinte maneira

$$CNOT |i, j\rangle = |i, i \oplus j\rangle, \quad (\text{II.20})$$

onde \oplus é a adição módulo 2.

A representação clássica desta porta envolve dois qubits: um controle e um alvo. Estes dois qubits trabalham da seguinte forma: a operação NOT é realizada sobre o segundo qubit (alvo), isto é, o qubit alvo é invertido quando o valor do primeiro qubit (controle) for $|1\rangle$, caso contrário, ele permanece inalterado. Esquemáticamente, tem-se:

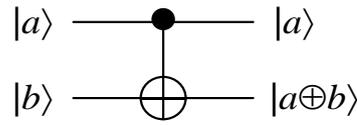


Figura 7.3. Circuito para a porta CNOT Quântica

De maneira geral, as portas controladas atuam sobre 2 ou mais qubits, onde um ou mais qubits atuam como um controle para a mesma operação. Se U é uma porta que atua sobre um qubit, $U = \begin{pmatrix} \alpha_{00} & \alpha_{01} \\ \alpha_{10} & \alpha_{11} \end{pmatrix}$, então a porta controlada $C(U)$ é uma porta que atua sobre dois qubits de modo que o qubit de controle é o primeiro. Ela mapeia os estados da base da seguinte maneira: $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |1\rangle U|0\rangle = |1\rangle(\alpha_{00}|0\rangle + \alpha_{10}|1\rangle)$ e $|11\rangle \mapsto |1\rangle U|1\rangle = |1\rangle(\alpha_{01}|0\rangle + \alpha_{11}|1\rangle)$. A porta controlada $C(U)$ é representada pela matriz

$$C(U) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha_{00} & \alpha_{01} \\ 0 & 0 & \alpha_{10} & \alpha_{11} \end{pmatrix}. \quad (\text{II.21})$$

É graças a esta propriedade condicional, dependendo do valor do qubit de controle, que se cria uma porta lógica capaz de gerar estados não decomponíveis em produtos tensoriais. O exemplo clássico para a criação de um estado de Bell é indicado na Figura 7.4:

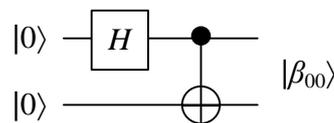


Figura 7.4. Circuito para geração do estado de Bell

Note-se que a aplicação da porta H faz com que em 50% dos casos, a CNOT atue. Assim, a saída é representada pelo estado $|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ que possui como característica o fato de não poder ser escrito como produto tensorial.

Além disso, a porta CNOT é fundamental para a construção de muitas outras portas, tais como a de permutação de qubits (SWAP) e, em particular a Toffoli (T), que pode ser usada para simular circuitos clássicos.

A porta SWAP é definida por $SWAP |i, j\rangle = |j, i\rangle$, sendo sua representação matricial dada por

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (\text{II.22})$$

Basicamente, a porta T corresponde a uma inversora duplamente controlada: ela inverte um qubit alvo se os dois qubits de controle estiverem ativados. Assim,

$$T|i, j, k\rangle = |i, j, k \oplus ij\rangle, \quad (\text{II.23})$$

onde $i, j, k \in \{0, 1\}$ e \oplus é a adição módulo 2. Uma forma de construir a porta T é a partir de portas universais de 1 qubit e CNOT's quânticas.

Vale à pena mencionar que portas controladas podem efetuar qualquer operação (e não apenas a inversão de qubits). Uma generalização para portas multicontroladas foi proposta por Deutsch e consiste na seguinte porta

$$|a, b, c\rangle \mapsto D(\theta) = \begin{cases} i \cos(\theta) |a, b, c\rangle + \sin(\theta) |a, b, 1-c\rangle, & a = b = 1 \\ |a, b, c\rangle, & a \neq 1 \text{ ou } b \neq 1 \end{cases}. \quad (\text{II.24})$$

Quando $\theta = \frac{\pi}{2}$, a porta de Deutsch reduz-se à porta Toffoli clássica, mostrando que todas as operações lógicas podem ser realizadas sobre um computador quântico universal.

APÊNDICE 3

ALGORITMO DE GROVER E TRANSFORMADA QUÂNTICA DE FOURIER

Nesta seção, será apresentada uma aplicação da amplificação de amplitude, mostrando que, no caso em que a lista apresenta apenas uma entrada no estado $|\psi_{good}\rangle$, a amplificação de amplitude reduz-se ao algoritmo de busca de Grover.

III.1. Algoritmo de Grover

Considere uma lista desordenada com N elementos, $N = 2^n$, para algum $n \in \mathbb{N}$, e uma função oráculo f , que pode reconhecer as entradas no estado $|\psi_{good}\rangle$, durante a busca. Se a busca é feita em uma lista $0, 1, 2, \dots, N-1$ e se existem G entradas na lista, inicializadas no estado $|000\dots 0\rangle$, então elas podem ser achadas alterando-se esse estado para formar uma superposição uniforme $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ de todos os elementos da lista. Assim, a probabilidade de se encontrar os estados $|\psi_{good}\rangle$ é igual à frequência das entradas $|\psi_{good}\rangle$ na lista, isto é, $\alpha^2 = \frac{G}{N}$. Portanto, se $\alpha \ll 1$, o número aproximado de iterações necessárias é:

$$k = \left\lceil \frac{\pi}{4\theta} \right\rceil = \left\lceil \frac{1}{4\arcsen(\alpha)} \right\rceil \approx \left\lceil \frac{1}{4\alpha} \right\rceil = \left\lceil \frac{1}{4} \sqrt{\frac{N}{G}} \right\rceil = O(\sqrt{N}). \quad (\text{III.1})$$

Realizando uma medida no estado $\mathcal{Q}^k(|\psi\rangle)$, a probabilidade de a entrada ser o estado $|\psi_{good}\rangle$ será muito alta. Desde que cada iteração necessite de uma simples consulta ao oráculo, é possível encontrar a entrada no estado $|\psi_{good}\rangle$, com $O(\sqrt{N})$ consultas ao oráculo, aproximadamente, obtendo assim, um ganho de velocidade quadrático em relação ao melhor algoritmo clássico.

Observe que, se $G = 1$, então a amplificação de amplitude reduz-se ao algoritmo de Grover.

III.2. Transformada Quântica de Fourier

A revisão feita a seguir sobre Transformada Quântica de Fourier (TQF) segue o tratamento da mesma, descrito em “Notes for the graduate course “Quantum Computation and Quantum Information” (290A), Spring 2005. v1.”

Seja \mathbb{Z}_N o conjunto de todos os inteiros módulo N , denotando o espaço de estados. Neste caso, os estados da base são os inteiros módulo N . Outras notações para \mathbb{Z}_N : $\mathbb{Z}/N\mathbb{Z}$ ou $\mathbb{Z}/(N)$ ou \mathbb{Z}/N .

A Transformada Quântica de Fourier (TQF) sobre \mathbb{Z}_N é uma *transformação unitária* definida por

$$TQF(|x\rangle) = \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}_N} \exp\left(\frac{2\pi i xy}{N}\right) |y\rangle, \quad (\text{III.2})$$

para todo $x \in \mathbb{Z}_N$. Pondo $\xi = \exp\left(\frac{2\pi i}{N}\right)$, tem-se que

$$\sum_{x \in \mathbb{Z}_N} \xi^{dx} = \begin{cases} N, & d = 0 \\ 0, & d \neq 0 \end{cases}. \quad (\text{III.3})$$

Assim, a matriz da Transformada Quântica de Fourier, é:

$$U_{TQF} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \xi & \xi^2 & \dots & \xi^{N-1} \\ 1 & \xi^2 & \xi^4 & \dots & \xi^{2N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{N-1} & \xi^{2N-2} & \dots & \xi^{(N-1)(N-1)} \end{pmatrix}, \quad (\text{III.4})$$

ou

$$U_{TQF} = \frac{1}{\sqrt{N}} \sum_{x,y \in \mathbb{Z}_N} \xi^{xy} |y\rangle \langle x|. \quad (\text{III.5})$$

O conjugado Hermitiano de $U_{TQF} \in \mathbb{C}^{N \times N}$, é

$$U_{TQF}^\dagger = \frac{1}{\sqrt{N}} \sum_{x',y' \in \mathbb{Z}_N} \xi^{-x'y'} |y'\rangle \langle x'|. \quad (\text{III.6})$$

Como $\langle y' | y \rangle = \begin{cases} 1, & y' = y \\ 0, & y' \neq y \end{cases}$, tem-se que $U_{TQF} U_{TQF}^\dagger = I$, isto é, U_{TQF} é unitária.

III.2.1. Implementação Eficiente de U_{TQF}

Para programar U_{TQF} eficientemente, é necessário mostrar que ela pode ser implementada (aproximadamente) como um circuito quântico de tamanho $O(\text{poly}(\log N))$.

Para $N = 2^n$, U_{TQF} pode ser implementada como segue.

Cada número $x \in \mathbb{Z}_N$ é representado por n bits x_0, x_1, \dots, x_{n-1} tais que, por exemplo, $y = \sum_{j=0}^{n-1} y_j 2^j$. A Transformada de Fourier de $x \in \mathbb{Z}_N$ pode então ser escrita como o produto tensorial de n qubits. Ou seja,

$$U_{TQF} (|x\rangle) = \bigotimes_{j=0}^{n-1} |z\rangle_j, \quad (\text{III.7})$$

onde o índice em $|z\rangle_j$ indica a posição do j -ésimo qubit. Agora, como $\exp(2\pi i \cdot x_k 2^s) = 1$ para todos os inteiros $s \geq 0$, veja que o qubit z_j na j -ésima saída, é de fato:

$$|z\rangle_j = \frac{1}{\sqrt{2}} \left[|0\rangle_j + \exp\left(2\pi i (x_0 2^{j-n} + x_1 2^{j+1-n} + \dots + x_{n-1-j} 2^{-1})\right) |1\rangle_j \right], \quad (\text{III.8})$$

e assim, depende somente dos $n - j$ bits $x_0, x_1, \dots, x_{n-1-j}$ de entrada.

Para descrever o circuito quântico que implementa a Transformada Quântica de Fourier, define-se as seguintes rotações de fase de um qubit simples,

$$R_r = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i/2^r) \end{pmatrix}, \quad (\text{III.9})$$

e a rotação de dois qubits, R_r controlada, com $C(R_r)|a,b\rangle \mapsto \exp(2\pi iab/2^r)|a,b\rangle$, para $a,b \in \{0,1\}$, tal que

$$C(R_r) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp(2\pi i/2^r) \end{pmatrix}. \quad (\text{III.10})$$

O circuito a seguir (de tamanho $O(n^2)$) usa essas portas combinadas com n portas Hadamard para implementar a Transformada Quântica de Fourier sobre \mathbb{Z}_{2^n} .

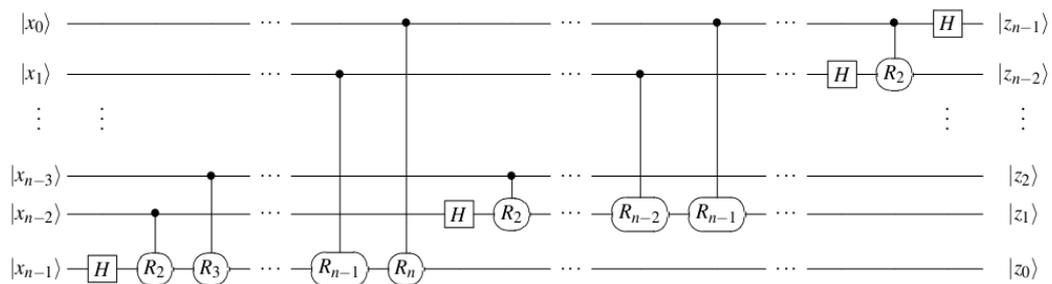


Figura 7.5. Circuito para Transformada Quântica de Fourier.

Em resumo, tem-se um eficiente (tamanho $O(n^2)$) esquema de implementação da Transformada Quântica de Fourier sobre o grupo \mathbb{Z}_{2^n} . Note que a ordem dos n qubits de saída z_0, z_1, \dots, z_{n-1} é reversível em comparação com a ordem dos bits de entrada x_0, x_1, \dots, x_{n-1} .

ARTIGOS

1. *The minimal principals of Hermitian matrices and the negativity of bipartite qubits states.*
Oliveira, J. L. and Ramos, R. V.
Anais II WECIQ - Escola de Computação e Informação Quântica, p. 147-150, 2007.
2. *Quantum Algorithm for Finding the Period of a Periodic Function Using Asymptotic Quantum Search.*
Oliveira, J. L. and Ramos, R. V.
Fernando Ferreira, Hélia Guerra, Elvira Mayordomo, and João Rasga (editors), Programs, Proofs, Processes, 6th Conference on Computability in Europe, CiE 2010, Ponta Delgada, Azores, Portugal, June/July 2010, CMATI (Centre for Applied Mathematics and Information Technology), University of Azores, 303 - 310, 2010.
3. *Entanglement of pure 4-qubit and 6-qubit States via Negativity.*
Oliveira, J. L. Oliveira, D. S., and Ramos, R. V.
Anais III WECIQ - Escola de Computação e Informação Quântica, p. 4-13, 2010.
4. *Entanglement Measure for Pure 6-qubit Quantum States.*
Oliveira, J. L. Oliveira, D. S., and Ramos, R. V.
Quantum Information Processing, vol. 11, Number 1, p. 255-267, 2012.

REFERÊNCIAS

1. M. A. Nielsen e I. L. Chuang, “*Computação Quântica e Informação Quântica*”, 1ª Edição, Bookman (2005).
2. A. Peres, *Separability Criterion for Density Matrices*, Phys. Rev. Lett. 8, 77 (1996).
3. M. Horodecki, P. Horodecki, and R. Horodecki, *Separability of mixed states: necessary and sufficient conditions*, Physics Letters A 223, 1-8 (1996).
4. S. L. Woronowicz, *Positive maps of low dimensional matrix algebras*, Rep. Math. Phys. 10, 2, 165 - 183 (1976).
5. D. C. Santos, “*Em Busca de um Entendimento Completo a Cerca do Emaranhamento*”, Dissertação de Mestrado, Departamento de Física, UFMG (2006).
6. L. P. Hughston, and W. K. Wootters, *A complete classification of quantum ensembles having a given density matrix*, Physics Letters A 183, 14 - 18 (1993).
7. P. Horodecki, *Separability criterion and inseparable mixed states with positive partial transposition*, Physics Letters A 232, 333-339 (1997).
8. G. G. Rigolin, “*Estados Quânticos Emaranhados*”, Tese de Doutorado, Instituto de Física Gleb Wataghin, UNICAMP (2005).
9. J. Audretsch, “*Entangled Systems – New Directions in Quantum Physics*”, Wiley-VCH, Weinheim (2007).
10. P. Kaye, R. Laflamme, and M. Mosca, “*An introduction to Quantum Computing*”, Oxford University Press, 1st Ed (2007).
11. F. Verstraete, K. Audenaert, and D. De Moor, *Maximally entangled mixed states of two qubits*, Physical Review A 64, 012316 (2001).
12. A. O. Pittenger, and M. H. Rubin, *Convexity and the separability problem of quantum mechanical density matrices*, Linear Algebra and its Applications, 346, 47-71 (2002).
13. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, *Mixed-state entanglement and quantum error correction*, Physical Review A 54, 3824 (1996).
14. M. Horodecki, P. Horodecki, and R. Horodecki, *Limits for Entanglement Measures*, Phys. Rev. Letters, 84, 2014 (2000).
15. M. Horodecki, *Entanglement Measures*, Quantum Information Processing, 1, 1, 3 - 16, (2001).

16. S. Hill, and W. K. Wootters, Entanglement of a Pair of Quantum Bits, *Phys. Rev. Letters*, 78, 26 (1997).
17. W. K. Wootters, *Entanglement of Formation of an Arbitrary State of Two Qubits*, *Phys. Rev. Letters*, 80, 2245 (1998).
18. V. Vedral, M. B. Plenio, M. A. Ripping, and P. L. Knight, *Quantifying Entanglement*, *Phys. Rev. Letters*. 78, 2275 (1997).
19. V. Vedral and M. B. Plenio, *Entanglement measures and purifications procedures*, *Physical Review A* 57, 1619 (1998).
20. G. Vidal and R. F. Werner, *A computable measure of entanglement*, *Physical Review A* 65, 032314/1-11 (2002).
21. J. Eisert, and M. B. Plenio, *A Comparison of Entanglement Measures*, arxiv:quant-ph/9807034v2 (1999).
22. W. K. Wootters, *Entanglement of Formation and Concurrence*, *Quantum Information and Computation*, 1, 27-44 (2001).
23. W. Dür, J. I. Cirac, and R. Tarrach, *Separability and Distillability of Multiparticle Quantum Systems*, *Physical Review Letters*, 83, 3562 (1999).
24. C.-S. Yu, and H.-S. Song, *Measurable entanglement for tripartite quantum pure states of qubits*, *Phys. Rev. A* 76, 022324 (2007).
25. C.-S. Yu, and H.-S. Song, *Free entanglement measure of multiparticle quantum states*, *Physics Letters A* 330, 377-383 (2004).
26. C.-S. Yu, and H.-S. Song, *Multipartite entanglement measure*, *Phys. Rev. A* 71, 042331 (2005).
27. M. H. Partovi, *Universal Measure of Entanglement*, *Physical Review Letters*, 92, 077904 (2004).
28. T. J. Osborne, and F. Verstraete, *General Monogamy Inequality for Bipartite Qubit Entanglement*, *Physical Review Letters*, 96, 220503 (2006).
29. K. Chen, S. Albeverio, and S. - M. Fei, *Concurrence of Arbitrary Dimensional Bipartite Quantum States*, *Physical Review Letters*, 95, 040504 (2005).
30. C. -T. Chen, *“Linear systems theory and design”*, 3rd edition, Oxford University Press (1999).
31. V. Coffman, J. Kundu, and W. K. Wootters, *Distributed entanglement*, *Phys. Rev. A* 61, 052306 (2000).
32. B. M. Terral, *Is entanglement monogamous?* arxiv:quantum-ph/0307120 (2003).

33. A. Wong and N. Christensen, *Potencial multipartite entanglement measure*, Physical Review A 63, 044301 (2001).
34. A. Alcín, A. Adrianov, L. Costa, E. Jané, J. I. Latorre and R. Tarrach, *Generalized Schmidt Decomposition and classification of Three-Quantum-Bit States*, Phys. Rev. Lett. 85, 1560.
35. Y. -C. Ou and H. Fan, *Monogamy inequality in terms of negativity for three-qubit states*, Phys. Rev. A 75, 062308, 1-5 (2007).
36. D. S. Oliveira, and R. V. Ramos, *Entanglement and applications of pure fourpartite of qubit states*, Quantum Information Processing, Vol. 9, N^o. 4, 497 - 508 (2010).
37. D. S. Oliveira, “*Cálculo do Entrelaçamento de Estados Puros com Quatro a Seis Qubits*”, Tese de Doutorado, Departamento de Engenharia de Teleinformática - DETI, UFC (2012).
38. A. Higuchi, and A. Sudbery, *How entangled can two couples get?* Phys. Lett. A 273, 213-217 (2000).
39. M. Horodecki, *Simplifying monotonicity condition for entanglement measures*, Open Sys. & Inf. Dyn., 12, 3, 231-237 (2005).
40. R. D. Dobrzanski, A. Buchleitner, M. Kus, and F. Mintert, *Evaluable multipartite entanglement measures: Multipartite concurrences as entanglement monotones*, Phys. Rev. A 74, 052303 (2006).
41. P. -X. Chen, S. -Y. Zhu, and G. -C. Guo, *General form of genuine multipartite entanglement quantum channels for teleportation*, Phys. Rev. A 74, 032324 (2006).
42. G. Rigolin, T. R. Oliveira, and M. C. Oliveira, *Operational classification and quantification of multipartite entangled states*, Phys. Rev. A 74, 022314 (2006).
43. C. -Y. Lu, X. -Q. Zhou, O. Gühne, W. -B. Gao, J. Zhang, Z. -S. Yuan, A. Goebel, T. Yang, and J. -W. Pan, *Experimental entanglement of six photons in graph states*, Nature Physics, 3, 2, 91-95 (2007).
44. M. Radmark, M. Żukowski, and M. Bourennane, *Experimental high fidelity six-photon entangled state for telecloning protocols*, New J. Phys., 11, 103016 (2009).
45. S. Choudhury, S. Muralidharan, and P. K. Panigrahi, *Quantum teleportation and state sharing using a genuinely entangled six-qubit state*, J. Phys. A: Math. Theor. 42 115303 (2009).
46. Z. -X. Man, Y. -J. Xia, and N. B. An, *Entanglement dynamics for a six-qubit model in cavity QED*, J. Phys. B: At. Mol. Opt. Phys., 41, 155501 (2008).

47. Y.-K. Bai, M. -Y. Ye, and Z. D. Wang, *Entanglement in a class of multiqubit mixed states without multipartite tangles*, Phys. Rev. A, 78, 062325 (2008).
48. J. A. Smolin, *Four-party unlockable bound entangled state*, Phys. Rev. A 63, 032306 (2001).
49. Y.-K. Bai, D. Yang, and Z. D. Wang, *Multipartite quantum correlation and entanglement in four-qubit pure states*, Phys. Rev. A 76, 022336 (2007).
50. A. Chamoli, and C. M. Bhandari, *Groverian entanglement measure and evolution of entanglement in search algorithm for n ($=3,5$)-qubit systems with real coefficients*, Quant. Inf. Process., Vol. 6, N^o. 4, 255-271 (2007).
51. C. H. Bennett, S. Popescu, D. Rohrlich, J. Smolin, and A. Thapliyal, *Exact and asymptotic measures of multipartite pure-state entanglement*, Phys. Rev. A 63, 012307 (2001).
52. F. Pan, D. Liu, G. Lu, and J. P. Draayer, *Extremal entanglement for triqubit pure states*, Phys. Lett. A 336, 384 (2005).
53. J. -M. Cai, Z. -W. Zhou, X. -X. Zhou, and G. -C. Guo, *Information-theoretic measure of genuine multiqubit entanglement*, Phys. Rev. A 74, 042338 (2006).
54. A. Y. Chernyavskiy, *Entanglement measure for multipartite pure states and its numerical calculation*, arxiv:quant-ph/0905.0201 (2009).
55. R. Portugal, C. C. Lavor, L. M. Carvalho e N. Maculan, “*Uma Introdução à Computação Quântica*”, Sociedade Brasileira de Matemática Aplicada e Computacional, São Paulo (2004).
56. L. V. Grover, *A fast quantum mechanical algorithm for database search*, in Proc., 28th Annual ACM Symposium on the Theory of Computing, New York, pp. 212 (1996).
57. L. V. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Phys. Rev. Lett., 79, pp. 325 (1997).
58. M. A. Nielsen, and I. L. Chuang, “*Quantum Computation and Quantum Information*”, Cambridge Univ. Press, Cambridge, ch. 4 and 6 (2000).
59. C. Dürr, and P. Høyer, *A quantum algorithm for finding the minimum*, arxiv:quant-ph/9607014 (1999).
60. A. Ahuja, and S. Kapoor, *A quantum algorithm for finding the maximum*, arxiv:quant-ph/9911082 (1999).
61. M. Boyer, G. Brassard, P. Høyer, and A. Tapp, *Tight bounds on quantum searching*, arxiv:quant-ph/9605034 (1996).

62. L. A. B. Kowada, C. Lavor, R. Portugal, and C. M. H. Figueiredo, *A new quantum algorithm to solve the minimum searching problem*, International Journal of Quantum Information, Vol. 6, N^o. 3, 427 – 436 (2008).
63. D. S. Oliveira, and R. V. Ramos, *Quantum Bit String Comparator: Circuits and Applications*, *Quantum Computers and Computing*, vol. 7, N^o. 1, 17-26 (2008).
64. P. Shor, *Algorithm for quantum computation: Discrete logarithms and factoring*, *proceedings*, 35th Annual Symposium on Foundations of Computer Science, 124-134 (1994).
65. S. Dasgupta, C. Papadimitriou, C., and U. Vazirani, “*Algorithms*”, McGraw Hill (2009).
66. T. D. Kieu, *Quantum algorithms for Hilbert’s tenth problem*, xxx.lanl.gov - quant-ph/0110136 (2003).
67. C. Calude, *Theories of Computational Complexity*, North-Holland, Amsterdam (1998).
68. G. Chaitin, *Meta Math!: the quest for omega*, Pantheon Books (2005).
69. G. Chaitin, *Irreducible Complexity in Pure Mathematics*, Preprint at <http://www.arxiv.org/math.HO/0411091> (2004).
70. G. Chaitin, *Information-theoretic computational complexity*, IEEE Trans. on Inf. Theory, IT-20, 10 (1974).
71. C. Calude, *Information and Randomness*, Springer-Verlag, Berlin (1994).
72. G. Chaitin, “*Algorithmic Information Theory*”, Cambridge University Press, 1st Ed (1987).
73. G. Markowsky, *Introduction to algorithmic information theory*, J. of Universal Comp. Science, 2, N^o. 5, 245 (1996).