

Universidade Federal do Ceará
Centro de Tecnologia
Departamento de Engenharia de Teleinformática

**Cálculo numérico da medida de entrelaçamento de qutrits
multipartes**

Werther Xisto da Silva Cardoso

Fortaleza, CE
19 de julho de 2011

Werther Xisto da Silva Cardoso

**Cálculo numérico da medida de entrelaçamento de qutrits
multipartes**

Universidade Federal do Ceará

Centro de Tecnologia

Departamento de Engenharia de Teleinformática

Dissertação submetida a Coordenação do Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos pré-requisitos para a obtenção do grau de mestre em Engenharia de Teleinformática.

Orientador: José Cláudio do Nascimento

Fortaleza, CE
19 de julho de 2011

Werther Xisto da Silva Cardoso

Cálculo numérico da medida de entrelaçamento de qutrits multipartes

Dissertação submetida a Coordenação do Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos pré-requisitos para a obtenção do grau de mestre em Engenharia de Teleinformática.

Aprovada em 19 de julho de 2011.

Banca Examinadora:

Prof. Dr. José Cláudio do Nascimento - UFC/Campus Sobral

Prof. Dr. Rubens Viana Ramos - UFC

Prof. Dr. João Batista Rosa Silva - UFC

Prof. Dr. Gerardo Valdísio Rodrigues Viana - UECE

Prof. Dr. Carlile Campos Lavor - UNICAMP

Fortaleza, CE
2011

A minha esposa Vera e filhos, Bryan e Livia.

Agradecimentos

A Deus por provar a sua graça e ser misericordioso para comigo.

Ao meu orientador, Prof. José Cláudio do Nascimento, pelo esforço em me orientar neste tema.

Pelos momentos de trabalho juntos, eu faço meus agradecimentos aos meus colegas de pós-graduação: Rubens Viana Ramos, Paulo Vinícios, Fátima Regina, Daniel Barbosa, Daniela, Fernando, Fábio Alencar e Glaucionor. .

A minha família, pelo apoio durante esta jornada.

Ao CNPQ, pelo apoio financeiro.

Jesus respondeu, e disse-lhe: Na verdade, na verdade te digo que aquele que não nascer de novo, não pode ver o Reino de Deus... E, como Moisés levantou a serpente no deserto, assim importa que o Filho do Homem seja levantado: Para que todo aquele que nele crê não pereça, mas tenha a vida eterna. Porque Deus amor o mundo de tal maneira que deu o seu Filho unigênito, para que todo aquele que nele crê não pereça, mas tenha a eterna. Porque Deus enviou o seu Filho ao mundo, não para que condenasse o mundo, mas que o mundo fosse salvo por ele. Quem crê nele não é condenado, mas quem não crê já está condenado; porquanto não crê no nome do Unigênito Filho de Deus.

Evangelho de João 3:3, 14-18.

Resumo

Este trabalho discute o cálculo numérico da medida de entrelaçamento através da minimização da entropia de Shannon. Este é um problema de otimização e que se torna árduo quando o número de níveis do sistema quântico e o número de partes aumentam. Um algoritmo genético é apresentado para o cálculo da medida de entrelaçamento de qutrits.

Abstract

This work discusses the numerical calculation of the measure of entanglement by minimizing the Shannon entropy. This is an optimization problem and it becomes hard when the number of quantum levels of the system and the number of parts increase. A genetic algorithm is presented for calculating the measure of entanglement of qutrits.

Sumário

Lista de Figuras	vi
Lista de Tabelas	vii
1 Noções sobre entrelaçamento	4
1.1 Introdução	4
1.2 Correlação e entrelaçamento	4
1.3 Estados quânticos classicamente correlacionados e LOCC	5
1.3.1 Estados quânticos classicamente correlacionados	6
1.3.2 Separabilidade e entrelaçamento	8
1.3.3 O problema da separabilidade	9
1.4 Estados puros entrelaçados	10
1.4.1 A decomposição de Schmidt	10
1.4.2 O número de Schmidt e o entrelaçamento	13
1.4.3 Entropia dos subsistemas que constituem uma medida de entrelaçamento	15
2 Medidas de entrelaçamento para estados puros multipartes e seu cálculo numérico	17
2.1 Mínima Entropia de Shannon sobre medição de estados ortogonais	17
2.1.1 Propriedades necessárias para medidas de entrelaçamento	18
2.2 Cálculo de E_{Hmin} para qutrits com algoritmo genético	19
2.2.1 Método para obtenção da transformação unitária local para um qutrit	21
2.2.2 Algoritmo Genético	23
2.3 Resultados numéricos	25
A Introdução à teoria da informação quântica	31
A.1 estados quânticos e transformações unitárias	31

B	Demonstração de que a medida de entrelaçamento $E_{H \min}$ satisfaz as condições exigidas para uma medida de entrelaçamento	34
B.0.1	Propriedades complementares	36
B.1	Propriedades numéricas	38
B.1.1	E_{sh} é consideravelmente uma medida de entrelaçamento multipartite .	39

Lista de Figuras

2.1	Cálculo do grau de entrelaçamento para um estado completamente desentrelaçado.	25
2.2	Cálculo do grau de entrelaçamento para um estado maximamente entrelaçado. .	26
2.3	Entrelaçamento de qutrits com apenas dois termos de superposição.	27
2.4	Entrelaçamento de qutrits com três termos de superposição.	29

Lista de Tabelas

A.1	Resultados das operações X , Z e H aplicada aos qubits de entrada $ 0\rangle$ e $ 1\rangle$ da base B_0 , e aos qubits $ +\rangle$ e $ -\rangle$ da base B_1	33
-----	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----

Introdução

A área de computação e informação quântica possui temas de vanguarda para a área de segurança da informação. A distribuição quântica de chaves é um método de distribuição de chaves secretas para a criptografia simétrica que pode implementar criptografia perfeitamente segura [1–3]. Muitos grupos de pesquisa no Brasil têm realizado esforços em direção à criação de uma rede de comunicação segura, baseada em criptografia quântica, a exemplo dos Estados Unidos, da Áustria, da Alemanha e da Suíça. Portanto, os investimentos em informação quântica têm um caráter estratégico para os ramos das telecomunicações e segurança da informação no país.

No campo da computação, o algoritmo de Shor é capaz de fatorar números primos em tempo polinomial [4]. Quando o computador quântico se tornar factível, este fato tornará frágil qualquer sistema com base em criptografia assimétrica, baseada na dificuldade computacional de fatorar números inteiros, atual tecnologia de criptografia popularmente usada na internet.

Diante disso, aponta-se que o tema alvo desta dissertação refere-se às medidas de entrelaçamento de estados quânticos multipartes e multiníveis. Matematicamente, compreende-se que dois estados quânticos estão entrelaçados quando não se pode separar esses dois estados em um produto tensorial, isto é, seja $|\psi\rangle$ um estado quântico que representa dois sistemas, então não é possível escrever a equação $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, em que os estados $|\psi_1\rangle$ e $|\psi_2\rangle$ representam um sistema cada um. Fisicamente, um estado quântico tem um entrelaçamento entre dois sistemas se os resultados das medições forem aleatórios, mas correlacionados entre si. Por exemplo, considere um estado quântico escrito da forma

$$\frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}.$$

Quando uma medição é feita no sistema A e posteriormente outra medição é realizada no sistema B , com probabilidade $1/2$, é observado o valor 0 no sistema A e 0 no sistema B , ou, com probabilidade $1/2$, é observado o valor 1 no sistema A e 1 no sistema B . Assim, exemplifica-se que embora os resultados das medições se constituam num evento aleatório, os resultados das

medições nos dois sistemas sempre estarão correlacionados.

O entrelaçamento de estados quânticos multipartes possui um papel importante em toda a ciência quântica. O entrelaçamento é necessário para outros protocolos quânticos: teleportação quântica, correção de erro quântico etc. Além disso, a teoria do entrelaçamento quântico deve auxiliar na compreensão dos sistemas de multipartículas da física quântica. Vale destacar também que o entrelaçamento dos estados puros bipartes já é completamente descrito, contudo não há uma completa teoria de entrelaçamento quântico multiparte. No entanto, alguns resultados importantes já são conhecidos. Uma completa classificação de estado puro de três qubits em termos de SLOCC (operações locais estocásticas e comunicação clássica) é dada em [5]. Uma descrição do entrelaçamento quântico com polinômios nilpotentes é construída em [6]. Algumas medidas de entrelaçamento de estados puros e mistos podem ser encontradas, por exemplo, em [7–12]. Logo, a teoria das medidas de entrelaçamento quântico é estudada em [13, 14].

Muitas pesquisas sobre qubits já foram realizadas, porém muitas perguntas sobre qudits ainda continuam sem respostas (sistemas quânticos com d níveis). Para uma ilustração, os níveis de energia de um átomo é um exemplo simples de qudites. Por exemplo, ao se considerar o efeito Zenão quântico observado em laboratório por Itano et al [15]. Este experimento descreve a probabilidade de encontrar um átomo num dado estado de energia. Um campo externo de radiofrequência introduz uma probabilidade de transição do autoestado $|1\rangle$ para o autoestado $|2\rangle$ de encontrar um íon de berílio preso em uma armadilha óptica e resfriado a 0,3K. A observação da energia do átomo, neste caso, consistiu na emissão de um pulso de laser sintonizado de tal forma que se o sistema estiver no autoestado $|1\rangle$, ele absorve um fóton e sofre uma transição para o autoestado $|3\rangle$. Neste experimento, não se pode tratar o autoestado $|3\rangle$ como uma composição de dois qubits $|11\rangle$, mas como um único estado de energia que numa representação matemática é ortogonal a $|1\rangle$ e $|2\rangle$. Assim, consideram-se qudits sistemas quânticos que podem ser descritos por espaço de Hilbert d -dimensional, $d = 2, 3, 4, \dots$. Assim, a superposição de um qutrit (estado quântico de três níveis) é escrita por:

$$e^{-i\alpha_i} \cos(\theta_i) |1\rangle - \text{sen}(\theta_i) \cos\left(\frac{\phi_i}{2}\right) e^{-i(\varphi_i + \alpha_i)} |2\rangle + \text{sen}(\theta_i) \text{sen}\left(\frac{\phi_i}{2}\right) e^{-i(\alpha_i + \varphi_i + \vartheta_i)} |3\rangle. \quad (1)$$

Observa-se, pois, no estado quântico acima que são necessários cinco parâmetros para representar uma superposição arbitrária de qutrits. Portanto, o natural é pensar que uma transformação unitária local para qutrits também seja construída com cinco parâmetros. No entanto, na melhor proposta de parametrização de matrizes unitárias por ângulos de Euler [16, 17], são necessários oito parâmetros para a construção dessas matrizes. A ideia consiste em usar as oito matrizes que compõem o grupo $SU(3)$ para construir uma parametrização da matriz unitária

local.

Desse modo, apresenta-se como exemplo de grande importância deste tema para a área da ciência da computação quântica a descoberta publicada numa edição da revista *Science*, ano de 2009 [18]. Nesse estudo, os autores realizaram operações de computação em um átomo artificial com até cinco níveis de energia. Neste caso, um qudit de cinco níveis. Resultado excelente e promissor para a construção do computador quântico. No entanto, simular sistemas quânticos que ocorrem na natureza é uma aplicação óbvia para computadores quânticos, contudo não simples em computadores clássicos. A razão pela qual eles não conseguem simular sistemas quânticos é a mesma pela qual não conseguem simular computadores quânticos.

A quantidade de números complexos necessários para descrever sistemas quânticos cresce exponencialmente com a dimensão do sistema, e não linearmente, como ocorre em sistema clássicos. Em geral, armazenar o estado quântico de n componentes ocupa cerca de c^n bits de memória de um computador clássico, em que c é uma constante que depende dos detalhes do sistema e da precisão almejada para a simulação. Quando os programadores tentam contornar o problema de memória por não haver hardware para tais cálculos, então eles, conseqüentemente, esperam um tempo que aumenta exponencialmente quando o número de sistemas quânticos se elevam. Já um computador quântico executa essa tarefa usando kn qubits, em que k é uma constante que depende dos detalhes do sistema simulado. No entanto, computadores quânticos ainda não são factíveis para investigação de sistemas quânticos. Portanto, propriedades de sistemas quânticos devem por enquanto ser investigadas, usando os computadores clássicos de última geração com suas impotentes propriedades.

Capítulo 1

Noções sobre entrelaçamento

1.1 Introdução

A história da mecânica quântica é marcada pela crise vivida pela física no início do século XX, a qual foi superada com conceitos estranhos como superposição e entrelaçamento de estados quânticos. O entrelaçamento quântico tem um importante papel em toda ciência quântica e é necessário para o entendimento eficaz dos protocolos quânticos: teleportação quântica, correção de erros quânticos etc.

A não localidade intrínseca no entrelaçamento é um fenômeno que intriga a física contemporânea. Este fenômeno mostra que dois estados quânticos colapsam simultaneamente no ato de medição de um dos estados, independentemente da separação espacial entre os dois estados. Essa “estranha ação à distância” é o conteúdo do Teorema de Bell e do paradoxo EPR.

Neste capítulo encontram-se alguns tópicos importantes para o entendimento do conceito matemático do entrelaçamento quântico, avaliando apenas a separabilidade algébrica de dois estados quânticos em um produto tensorial. Ademais, se estabelece a diferença entre estados quanticamente correlacionados e estados quânticos classicamente correlacionados. Apresenta-se a relação da decomposição de Schmidt, usando estados puros com o entrelaçamento de sistemas bipartes. Por último, mostra-se o cálculo da entropia do entrelaçamento como uma medida de entrelaçamento entre dois estados quânticos puros.

1.2 Correlação e entrelaçamento

Para melhor entendimento de correlação e entrelaçamento, toma-se um exemplo: a composição de um sistema com dois subsistemas que pode ser representado no produto dos estados $|0^A, 0^B\rangle$ ou $|1^A, 1^B\rangle$. O estado quântico $\alpha|0^A, 0^B\rangle + \beta|1^A, 1^B\rangle$ é formado por dois subsistemas

representados pelos subscritos A e B . Para $\alpha \neq 0, \beta \neq 0$, interpreta-se que a observação desses dois subsistemas mostra o estado $|0^A, 0^B\rangle$ com probabilidade $|\alpha|^2$ ou o resultado $|1^A, 1^B\rangle$ com probabilidade $|\beta|^2$. Neste caso, este evento probabilístico apresenta uma correlação entre os sistemas A e B , denominado entrelaçamento. No processo de informação quântica, o estado entrelaçado é fundamental para se entender vários processos computacionais.

Sistemas compostos e entrelaçamento andam juntos, ou seja, somente é possível fazer menção ao entrelaçamento mediante dois ou mais sistemas quântico. Por exemplo, se o observável σ_z é usado para medir cada um dos subsistemas do estado $\alpha|0^A, 0^B\rangle + \beta|1^A, 1^B\rangle$, então encontra-se como resultado os valores $(-1, -1)$ ou $(+1, +1)$. No entanto, nem sempre é simples avaliar se subsistemas estão entrelaçados ou não. Agora, apresenta-se um método que consiste em avaliar a correlação entre estados quânticos.

1.3 Estados quânticos classicamente correlacionados e LOCC

Fundamenta-se, inicialmente, a distinção entre estado quântico correlacionado e não correlacionado. Considere um sistema composto S^{AB} , formado pelos subsistemas S^A e S^B . Uma forma de expressar esse sistema é em forma de matriz densidade ρ^{AB} . Quando um estado pode ser escrito em forma de produto tensorial, $\rho^{AB} = \rho^A \otimes \rho^B$, os subsistemas estão completamente independentes um do outro. Neste caso, eles estão descorrelacionados, porque não há nenhuma correlação entre eles. Mas, quando o estado quântico composto não pode ser escrito como um produto, $\rho^{AB} \neq \rho^A \otimes \rho^B$, então os subsistemas S^A e S^B estão correlacionados.

Uma caracterização matemática do entrelaçamento pode ser realizada por uma sentença operacional sobre valores medidos que em princípio podem ser verificados por medições em subsistemas. Um estado ρ^{AB} possui entrelaçamento se somente se existem observáveis C^A e D^B para os quais o valor esperado de $C^A \otimes D^B$ não é dado pelo produto do valor esperado dos operadores densidade reduzidos:

$$\text{Tr} [(C^A \otimes D^B) \rho^{AB}] \neq \text{Tr} [C^A \rho^A] \cdot \text{Tr} [D^B \rho^B].$$

Os operadores reduzidos são calculados pelos traços parciais, $\rho^A = \text{Tr}_B[\rho^{AB}]$ e $\rho^B = \text{Tr}_A[\rho^{AB}]$. Isto está de acordo com a interpretação física intuitiva das medições dos subsistemas. Se duas observações são feitas separadamente, primeiro uma observação no subsistema S^A com o observável C^A e depois uma observação no subsistema S^B com o observável D^B e isto resulta em valores tais que o produto entre eles é igual ao valor esperado da observação conjunta de todo o sistema S^{AB} com o observável $C^A \otimes D^B$, então esses dois sistemas são independentes, pois as medições separadas de cada subsistema não se diferencia da medição de todo o sistema

composto. Afirmado assim que estes subsistemas são independentes quando a igualdade é constatada. Já não podemos afirmar isso quando essa igualdade é violada.

1.3.1 Estados quânticos classicamente correlacionados

Dentre os sistemas quânticos correlacionados, existem sistemas que possuem correlações nas suas medições semelhantes as correlações que são observadas em sistemas clássicos. Além disso, existem correlações que não podem ser reproduzidas por sistemas clássicos. Assim, faz-se necessária descrição detalhada dos sistemas quânticos classicamente correlacionados, e num segundo passo, caracterizar os estados, cujas correlações têm efeitos não clássicos. Isto é importante para o entendimento do conceito entrelaçamento.

O sistema composto S^{AB} é suposto ser preparado por Alice ou Bob, podendo ser modificado por operações locais (LO), abreviação de "local operations", nos subsistemas S^A e S^B . Entre tais operações, têm-se: transformações unitárias locais; medições e toda manipulação local. Além disso, Alice e Bob podem trocar informação por meio de comunicação clássica (CC), tais como mensagens por telefone, e-mail, etc; a fim de coordenar as operações locais entre eles. Logo, optou-se por abreviar este processo denominado “operações locais e comunicação clássica” por LOCC.

Nessa apresentação de sistema composto por meio de LOCC, Alice prepara o sistema S^A no estado ρ_r^A e informa a Bob, via canais de comunicação clássica. Por outro lado, Bob prepara o sistema S^B no estado ρ_r^B que em geral é diferente do que foi preparado por Alice. Essa sequência de ações é repetida várias vezes para diferentes estados de forma aleatória, mantendo o controle das frequências relativas p_r . O estado composto assim preparado, ρ^{AB} , é então por construção uma combinação convexa ou mistura estatística de estados puros:

$$\rho^{AB} = \sum_{r=1}^m p_r \rho_r^A \otimes \rho_r^B, p_r > 0, \sum_r p_r = 1. \quad (1.1)$$

Tal procedimento pode ser reproduzido de forma similar com estados clássicos. O resultado do estado ρ^{AB} está correlacionado, se a soma não pode ser reduzida num produto tensorial de termos simples. Dado que as correlações são produzidas por LOCC puramente clássica com probabilidade p_r , um estado quântico ρ^{AB} que pode ser escrito como uma mistura ($m \neq 1$) de estados puros será um estado classicamente correlacionado. Também evidencia-se que se os estados ρ_r^A e ρ_r^B forem estados mistos, então o estado pode ser reescrito com um novo conjunto

estatísticos da forma:

$$\rho^{AB} = \sum_j \pi_j |a_j^A\rangle\langle a_j^A| \otimes |b_j^B\rangle\langle b_j^B|. \quad (1.2)$$

Em que $0 < \pi_j \leq 1$ e $\sum_j \pi_j = 1$. Os estados da mistura não precisam ser obrigatoriamente ortogonal.

Um estado quântico ρ^{AB} é denominado classicamente correlacionado sempre que produzido pelo processo de preparação descrito acima. Basta que seja possível simular em todos os aspectos um estado preparado desta maneira, isto é, suas propriedades estatísticas podem ser produzidas por um mecanismo de operações locais e comunicação clássica. Matematicamente, isso significa que ρ^{AB} pode ser escrito na forma 1.2.

O termo classicamente correlacionado não deveria originar equívocos, mas a analogia a estados clássicos correlacionados não é perfeita. Assim, será construída uma situação de LOCC em uma situação simples. Considere que Alice e Bob contêm N bolas em que N_a são bolas azuis e N_v são bolas vermelhas. Por conseguinte tem-se que numa escolha aleatória de uma bola entre as N a probabilidade de a bola ser azul é $p_a = N_a/N$ e a probabilidade de a bola ser vermelha é $p_v = N_v/N$. Agora, considera-se o seguinte protocolo:

- Alice escolhe uma bola aleatoriamente, guarda-a numa caixa e informa a cor ao Bob;
- Bob busca uma bola da mesma cor informada por Alice e guarda-a em uma outra caixa.

Este procedimento é realizado N vezes para formar pares de caixas com bolas da mesma cor. Neste exemplo de LOCC, a completude é satisfeita, ou seja, $p_a + p_v = 1$. Quando as caixas são abertas, observa-se a correlação das cores. Pode-se fazer uma analogia disto com a correlação observada na medição da orientação da polarização do campo eletromagnético de um fóton. De uma forma geral, o estado que representa este experimento será expresso por:

$$\begin{aligned} \rho^{AB} &= p_a |a^A, a^B\rangle\langle a^A, a^B| + p_v |v^A, v^B\rangle\langle v^A, v^B| \\ &= p_a |a^A\rangle\langle a^A| \otimes |a^B\rangle\langle a^B| + p_v |v^A\rangle\langle v^A| \otimes |v^B\rangle\langle v^B|. \end{aligned} \quad (1.3)$$

Os estados $|a\rangle$ e $|v\rangle$ correspondem às cores azul e vermelha, respectivamente. Por meio da analogia aos estados quânticos, quando se realiza a medição na base computacional no sistema S^A com probabilidade p_a , encontra-se o estado $|a^A\rangle$. Depois, o estado no sistema S^B é medido e o resultado mostra o estado $|a^B\rangle$, o qual está relacionado com o estado $|a^A\rangle$.

A diferença entre correlação em sistemas clássicos e correlação clássica em sistemas quânticos é que em sistemas quânticos a escolha correta da base de observação é que vai mostrar a

correlação entre os dois sistemas. No experimento anterior, a correlação somente é observada quando nos dois subsistemas as medições são observadas na base $\{|a\rangle, |v\rangle\}$. Agora, considere o caso em que o estado ρ^{AB} da equação 1.3 tem as probabilidades $p_a = p_v = 1/2$. Sem perda de generalidade, considera-se que as medições feita no subsistemas S^A serão observadas na base:

$$\left\{ |+\!^A\rangle = \frac{|a^A\rangle + |v^A\rangle}{\sqrt{2}}, |-\!^A\rangle = \frac{|a^A\rangle - |v^A\rangle}{\sqrt{2}} \right\}.$$

Enquanto que o sistema S^B mantém a base $\{|a^B\rangle, |v^B\rangle\}$ para observação. Assim, tem-se que

$$\rho^{AB} \rightarrow \frac{1}{2} |+\!^A\rangle\langle +\!^A| \otimes \frac{1}{2} I^B + \frac{1}{2} |-\!^A\rangle\langle -\!^A| \otimes \frac{1}{2} I^B$$

O estado de S^B é um estado maximamente misto e neste sentido é um estado completamente indeterminado a partir dos subsistema S^A . O resultado das medições do estado gerado por LOCC não se apresentam correlacionados neste caso.

1.3.2 Separabilidade e entrelaçamento

Até aqui tem-se conhecimento suficiente para lançar uma definição precisa de entrelaçamento. Já foi discutido anteriormente que um estado quântico composto é separável quando seus subsistemas são independentes. Quando os sistemas não são independentes entre as partes, existem correlações de estados quânticos que podem ser simulados por sistemas clássicos. De posse disto, as duas próximas definições formalizam o conceito de entrelaçamento de estados quânticos bipartes.

Definição 1. *Seja o estado quântico ρ^{AB} da composição do sistema S^{AB} . Este sistema é dito ter **subsistemas independentes**, se somente se $\rho^{AB} = \rho^A \otimes \rho^B$, caso contrário, $\rho^{AB} \neq \rho^A \otimes \rho^B$, ele é dito ter **subsistemas correlacionados**.*

Definição 2. *Seja o estado quântico correlacionado ρ^{AB} da composição do sistema S^{AB} . Então este sistema é dito:*

- **separável**, se somente se este estado pode ser escrito por

$$\rho^{AB} = \sum_{r=1}^{m \neq 1} p_r \rho_r^A \otimes \rho_r^B;$$

- **entrelaçado** ou **quanticamente correlacionado** se somente se

$$\rho^{AB} \neq \sum_{r=1}^{m \neq 1} p_r \rho_r^A \otimes \rho_r^B.$$

Destas duas definições, conclui-se que todo sistema composto que possui subsistemas independentes pode ser escrito como um estado separável, mas a recíproca não é verdadeira. Nota-se que estados classicamente correlacionados são separáveis, mas não podem ser decompostos em subsistemas independentes.

O estado ρ^{AB} da composição do sistema S^{AB} é separável, quando escrito na forma da combinação convexa do produto dos estados. Um estado quântico puro ou misto que não é separável é chamado entrelaçado. O procedimento de preparação de um estado por LOCC é que constrói um estado separável. Estados entrelaçados não podem ser produzidos via LOCC.

1.3.3 O problema da separabilidade

Dado que correlações quânticas desempenham um importante papel como ferramenta de protocolos quânticos, uma meta importante é desenvolver critérios que possam dizer se um dado sistema quântico composto tem ou não entrelaçamento. Para estados puros de sistemas bipartes, isso é simples de decidir. O estado puro $|\psi^{AB}\rangle$ é separável se somente se ele pode ser escrito na forma $|\psi^{AB}\rangle = |\varphi^A\rangle \otimes |\chi^B\rangle$, isto é, cada um dos operadores densidade reduzidos é um estado puro.

Estados quânticos como os que estão nos experimentos são quase sempre uma mistura. Em sistemas quânticos, sempre há sistemas adicionais que perturbam o sistema que está sendo construído no experimento. A verdade é que o sistema quântico não pode ser perfeitamente separado do seu ambiente. Adicionar um subsistema a uma composição de sistemas, resulta em uma situação complexa. Assim, uma situação muito complexa surge, a qual se entenderia melhor com um exemplo para captar a intuição sobre o problema do entrelaçamento de misturas. O estados de Bell são estados puros com máximo entrelaçamento. Então, consideram-se os seguintes dois estados de Bell:

$$|\Phi_+^{AB}\rangle = \frac{|0^A, 0^B\rangle + |1^A, 1^B\rangle}{\sqrt{2}};$$

$$|\Phi_-^{AB}\rangle = \frac{|0^A, 0^B\rangle - |1^A, 1^B\rangle}{\sqrt{2}}.$$

Através das misturas com os estados entrelaçados $|\Phi_+^{AB}\rangle$ e $|\Phi_-^{AB}\rangle$ com iguais probabilidade,

$\frac{1}{2}$, obtêm-se os estados:

$$\rho^{AB} = \frac{1}{2} (|\Phi_+^{AB}\rangle\langle\Phi_+^{AB}| + |\Phi_-^{AB}\rangle\langle\Phi_-^{AB}|). \quad (1.4)$$

A partir da inserção da definição do estado de Bell em 1.4, encontra-se

$$\begin{aligned} \rho^{AB} &= \frac{1}{2} (|0^A, 0^B\rangle\langle 0^A, 0^B| + |1^A, 1^B\rangle\langle 1^A, 1^B|) \\ &= \frac{1}{2} (|0^A\rangle\langle 0^A| \otimes |0^B\rangle\langle 0^B| + |1^A\rangle\langle 1^A| \otimes |1^B\rangle\langle 1^B|). \end{aligned} \quad (1.5)$$

Consequentemente, o estado ρ^{AB} está classicamente correlacionado, portanto, não é entrelaçado. É possível prepará-lo apenas por LOCC. Na formação inicial do estado ρ^{AB} , o estado é $|\Phi_+^{AB}\rangle$ ou $|\Phi_-^{AB}\rangle$. Esta simples alternância dos diferentes estados entrelaçados o torna impossível de ser usado em protocolos em que o entrelaçamento é essencial, por exemplo a teleportação. Provavelmente, não há permanência da correlação quântica suficiente no estado depois do processo de mistura.

O operador densidade de uma dada mistura tem muitas formas de decomposições de ensembles. Se para um sistema biparte, pelo menos uma destas tem a forma de correlação separável, então o estado é separável. Caso contrário, o estado está entrelaçado. Para um sistema com muitos subsistemas e um espaço de Hilbert de alta dimensão, a separabilidade deve fazer uma declaração sobre todos os conjuntos da decomposição, isso não tem sido formulada de uma forma satisfatória até agora.

1.4 Estados puros entrelaçados

1.4.1 A decomposição de Schmidt

A decomposição de Schmidt têm-se revelado útil para uma discussão sobre o entrelaçamento de estados puros $|\psi^{AB}\rangle$ dos sistemas bipartes. Este procedimento também é chamado de decomposição biortogonal ou decomposição polar (expansão biortogonal ou polar) do vetor $|\psi^{AB}\rangle$. Abaixo está a demonstração do teorema apresentada em [19].

Teorema 1. *Seja $|\psi^{AB}\rangle$ um estado puro normalizado do sistema composto S^{AB} no produto dos espaços de Hilbert, $\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$, com $\dim \mathcal{H}^A = a$ e $\dim \mathcal{H}^B = b$. Sendo $\rho^{AB} = |\psi^{AB}\rangle\langle\psi^{AB}|$ têm-se que $\rho^A = \text{Tr}_B[\rho^{AB}]$ e $\rho^B = \text{Tr}_A[\rho^{AB}]$ são os operadores densidades reduzidos dos subsistemas S^A e S^B , então temos os seguintes resultados:*

1. O vetor $|\psi^{AB}\rangle$ pode ser escrito na forma de decomposição de Schmidt.

$$|\psi^{AB}\rangle = \sum_{n=1}^k \sqrt{p_n} |u_n^A, w_n^B\rangle, \text{ com } p_n > 0 \quad (1.6)$$

Com $k \leq \min(a, b)$, em que $\{|u_n^A\rangle\}$ e $\{|w_n^B\rangle\}$ são autovetores normalizados de ρ^A em \mathcal{H}^A (ou ρ^B em \mathcal{H}^B) com fase devidamente escolhida. Para um par de matrizes diferindo os autovalores p_n (isto é, nenhuma degenerescência), os vetores $|u_n^A\rangle$ e $|w_n^B\rangle$ são unicamente determinados. Daqui resulta que:

2. Os estados ρ^A e ρ^B têm os mesmos autovalores positivos $p_1 \cdots p_k$ (por g vezes degenerescência, ou seja o correspondente autovalor repete-se g vezes). O número k é chamado de constante de Schmidt do estado $|\psi^{AB}\rangle$.

Para provar o resultado (1), expande-se $|\psi^{AB}\rangle$ numa base ortonormal $\{|n^A\rangle, 1 \leq n \leq a\}$ de \mathcal{H}^A e $\{|i^B\rangle, 1 \leq i \leq b\}$ de \mathcal{H}^B com $a \leq b$, tem-se:

$$|\psi^{AB}\rangle = \sum_{n,i=1}^{a,b} a_{ni} |n^A, i^B\rangle. \quad (1.7)$$

Introduz-se novamente o estado relativo

$$|\tilde{w}_n^B\rangle := \sum_{i=1}^b a_{ni} |i^B\rangle. \quad (1.8)$$

Este resultado pode ser direcionado para:

$$|\psi^{AB}\rangle = \sum_{n=1}^a |n^A, \tilde{w}_n^B\rangle. \quad (1.9)$$

Os estados relativos $|\tilde{w}_n^B\rangle$, em geral, não são ortogonais e nem normalizados. Observa-se como a ortogonalidade na expressão (1.6) pode ser obtida. Para isso, escolhe-se como base ortonormal na equação (1.7) os autovetores particulares ortogonais $\{|u_n^A\rangle\}$ de ρ^A e expande-se ρ^A ,

$$\rho^A = \sum_{n=1}^a p_n |u_n^A\rangle \langle u_n^A| \text{ com } p_n \geq 0, \sum_{n=1}^a p_n = 1. \quad (1.10)$$

Sendo $p_n > 0$ para $1 \leq n \leq k$ e $p_n = 0$ para $k+1 \leq n \leq a$, os autovalores p_n podem ser degenerados. O vetor $|u_n^A\rangle$ é determinado apenas até uma fase de autovalores não degenerados

¹. Por outro lado, com os estados relativos associados com $|u_n^A\rangle, |\tilde{w}_n^B\rangle$, segue-se a fórmula:

$$\begin{aligned}
\rho^A &= \text{Tr}_B (|\psi^{AB}\rangle\langle\psi^{AB}|) \\
&= \text{Tr}_B \left(\sum_{l,n}^a |u_l^A, \tilde{w}_l^B\rangle\langle u_n^A, \tilde{w}_n^B| \right) \\
&= \text{Tr}_B \left(\sum_{l,n}^a |u_l^A\rangle\langle u_n^A| \otimes |\tilde{w}_l^B\rangle\langle \tilde{w}_n^B| \right) \\
&= \sum_{l,n}^a |u_l^A\rangle\langle u_n^A| \text{Tr}_B [|\tilde{w}_l^B\rangle\langle \tilde{w}_n^B|] \\
&= \sum_{l,n}^a \langle \tilde{w}_n^B | \tilde{w}_l^B \rangle |u_l^A\rangle\langle u_n^A|
\end{aligned} \tag{1.11}$$

Em que o último passo é o seguinte o cálculo:

$$\begin{aligned}
\text{Tr}_B (|\tilde{w}_l^B\rangle\langle \tilde{w}_n^B|) &= \sum_{i=1}^b \langle i^B | \tilde{w}_l^B \rangle \langle \tilde{w}_n^B | i^B \rangle \\
&= \sum_{i=1}^b \langle \tilde{w}_l^B | i^B \rangle \langle i^B | \tilde{w}_n^B \rangle = \langle \tilde{w}_n^B | \tilde{w}_l^B \rangle.
\end{aligned} \tag{1.12}$$

Ao comparar as equações (1.10) e (1.11), conclui-se da ortogonalidade entre os estados que:

$$\langle \tilde{w}_n^B | \tilde{w}_l^B \rangle = p_n \delta_{nl}. \tag{1.13}$$

Para $n \leq k = 1$, os estados $|\tilde{w}_l^B\rangle$ são vetores não nulos. Levando-se em conta o fato de que foi escolhido $\{|u_n^A\rangle\}$, como base ortonormal, ao invés de $\{|n^A\rangle\}$, encontra-se como um resultado da equação (1.13) com a equação (1.9) a proposição (1). Alegando que (2) é um resultado direto.

Da equação (1.6), o operador densidade reduzido de S^A é encontrado:

$$\rho^A = \sum_{i=1}^k p_n |u_n^A\rangle\langle u_n^A|. \tag{1.14}$$

Os valores p_n são chamados coeficientes de Schmidt. Salienta-se o fato de que o operador

¹Autovalores degenerados são autovalores que possuem dois ou mais autovetores linearmente independente associado a ele, o seja, o seu autoespaço possui dimensão maior ou igual a dois.

densidade ρ^B tem os mesmos valores p_n como autovalores.

$$\rho^B = \sum_{i=1}^k p_n |w_n^A\rangle\langle w_n^A|. \quad (1.15)$$

Isto tem como consequência imediata: o fato de que todas as funções de um operador densidade que depende apenas de seus autovalores tem o mesmo valor para ambos os operadores densidades reduzidos.

A decomposição Schmidt sempre se refere a um determinado estado puro de um sistema composto. Diferentes estados têm diferentes decomposições de Schmidt. Em geral, a decomposição Schmidt não pode ser estendida para sistemas com mais de dois subsistemas. Esta é a razão pela qual ela é usada apenas para o estudo do entrelaçamento biparte.

1.4.2 O número de Schmidt e o entrelaçamento

As decomposições ortonormais $\{|u_n^A\rangle\}$ e $\{|w_n^B\rangle\}$, com $n = 1, \dots, k$, são chamados de bases de Schmidt dos espaços \mathcal{H}^A ou \mathcal{H}^B . Nelas, os dois operadores densidades reduzidos são diagonalizáveis. A decomposição de Schmidt é uma superposição de estados separáveis. Toda a informação sobre o entrelaçamento de $|\psi^{AB}\rangle$ está contida nos coeficientes de Schmidt. O número de Schmidt k é o número de coeficientes de Schmidt não nulos. Neste caso, o estado $|\psi^{AB}\rangle$ é um estado produto e, portanto, não entrelaçado, se e somente o número de Schmidt é igual a um. Os estados quânticos ρ^A e ρ^B são ditos ter rank 1 neste caso. Esta é uma equivalência para $\text{Tr}[(\rho^A)^2] = \text{Tr}[(\rho^B)^2] = 1$.

Assim, infere-se que um estado quântico puro $|\psi^{AB}\rangle$ pode ser lido a partir de qualquer um de seus subsistemas quando ele não está entrelaçado. O número de Schmidt pode servir como uma medida de entrelaçamento dos estados puros. Esta é a razão do seu significado. Além disso, pode-se ler diretamente que se um dos operadores densidade reduzido descreve um estado puro, então o outro também é. Quando o sistema global S^{AB} é um estado puro $|\psi^{AB}\rangle$, então é impossível que um sistema, sendo um estado puro implique que o outro seja uma mistura. Similarmente, encontra-se que: quando um estado está entrelaçado com um sistema com m estados linearmente independentes, então a decomposição de Schmidt contém somente dois termos. Para efeito de cálculo, às vezes é conveniente introduzir a base de Schmidt. Em geral, o enunciado vale: se um subsistema tem a dimensão d , então ele não pode estar entrelaçado com mais do que d estados ortogonais de outros sistemas.

Se o estado ρ^A e o estado ρ^B têm como seus autovalores apenas autovalores degenerados e mais um nulo, então a decomposição de Schmidt é unicamente determinada por ρ^A e ρ^B , na

qual pode-se encontrar os correspondentes autovalores de ρ^A e ρ^B e formar o produto de estados pertencentes ao mesmo autovalor como na equação (1.6). Para $\dim\mathcal{H}^A \leq \dim\mathcal{H}^B$, o espectro de ρ^B consiste em coeficientes de Schmidt e $\dim\mathcal{H}^B - \dim\mathcal{H}^A$ na quantidade de autovalores que são nulos.

Agora será exemplificado que a degenerência na decomposição de Schmidt ocorre. Seja o estado de Bell

$$|\psi_{-}^{AB}\rangle = \frac{1}{\sqrt{2}} (|0^A, 1^B\rangle - |1^A, 0^B\rangle) \quad (1.16)$$

As bases associadas de \mathcal{H}^A e \mathcal{H}^B são em geral $\{|0^A, 1^B\rangle\}$ e $\{|1_r^A\rangle, |0_r^B\rangle\}$. O estado $|\psi_{-}^{AB}\rangle$ apresenta simetria esférica, uma vez que se pode facilmente verificar que

$$|\psi_{-}^{AB}\rangle = \frac{1}{\sqrt{2}} (|0_r^A, 1_r^B\rangle - |1_r^A, 0_r^B\rangle) \quad (1.17)$$

Em que os estados

$$|0_r\rangle = \begin{pmatrix} e^{-i\frac{\phi}{2}} \cos(\theta/2) \\ e^{i\frac{\phi}{2}} \sin(\theta/2) \end{pmatrix} \text{ e } |1_r\rangle = \begin{pmatrix} -e^{-i\frac{\phi}{2}} \sin(\theta/2) \\ e^{i\frac{\phi}{2}} \cos(\theta/2) \end{pmatrix} \quad (1.18)$$

são autovetores do operador

$$r\sigma = \begin{pmatrix} \cos\theta & e^{-i\phi/2} \sin\theta \\ e^{i\phi/2} \sin\theta & -\cos\theta \end{pmatrix} \quad (1.19)$$

escritos como vetores arbitrários da esfera de Bloch. Isto revela que, neste caso, a decomposição de Schmidt para o estado de Bell não é exclusiva. Se os valores p_n na equação (1.6) são os mesmos, os vetores correspondentes $|u_n^A, w_n^B\rangle$ podem ser substituídos por combinações lineares, correspondendo ao fato de que para o $|\psi_{-}^{AB}\rangle$ os autovetores dos operadores densidades reduzidos não são determinados, ou seja,

$$\rho^A = \rho^B = \frac{1}{2}I. \quad (1.20)$$

É possível para todo sistema quântico misto inserir um segundo sistema quântico, em que o sistema composto como um todo é um estado puro. O procedimento matemático que evidencia isto denomina-se purificação e será dado a seguir como um teorema.

Teorema 2. (Purificação) *Para cada sistema com operador densidade ρ^A em \mathcal{H}^A , existe um*

estado puro $|\varphi^{AB}\rangle$ em $\mathcal{H}^A \otimes \mathcal{H}^B$ de tal forma que ρ^A está associado ao operador densidade

$$\rho^A = \text{Tr}_B [|\varphi^{AB}\rangle\langle\varphi^{AB}|]. \quad (1.21)$$

Para a prova, considera-se a base ortonormal $\{|u_n^A\rangle\}$ a qual ρ^A é diagonalizável:

$$\rho^A = \sum_{n=1}^a p_n |u_n^A\rangle\langle u_n^A|$$

De acordo com a decomposição de Schmidt, então

$$|\varphi^{AB}\rangle = \sum_{n=1}^a p_n |u_n^A, w_n^B\rangle$$

Qualquer base ortonormal $\{|w_n^B\rangle\}$ é uma purificação possível. Outras purificações podem ser obtidas pela transformação unitária desta base. Isto torna mais uma vez claro que não há uma única inversa para a operação de traço parcial. Em vista disso, conclui-se que há um número infinito de sistemas compostos S^{AB} que têm o mesmo estado de S^A como subsistema.

1.4.3 Entropia dos subsistemas que constituem uma medida de entrelaçamento

Para estados puros de um sistema bipartes S^{AB} que estejam em um estado produto, somente existem duas conclusões possíveis: ou os subsistemas não estão correlacionados ou estão entrelaçados. Correlações neste caso apenas podem ser não clássicas. Denota-se a entropia do sistema composto por $S(AB)$ e as entropias dos subsistemas, obtidas através dos operadores densidades reduzidos, por $\rho^A = \text{Tr}_B [\rho^{AB}]$ e $\rho^B = \text{Tr}_A [\rho^{AB}]$. Uma vez que se avaliam apenas os estados puros, tem-se sempre a máxima certeza sobre o estado composto

$$S(AB) = 0. \quad (1.22)$$

O estado produto também oferece máxima certeza sobre os estados dos subsistemas, pois

$$S(A) = S(B) = 0. \quad (1.23)$$

Em contraste, tem-se o operador densidade do estado de Bell. Para ele, tem-se que

$$\rho^A = \rho^B = \frac{1}{2}I. \quad (1.24)$$

Os subsistemas deste caso são maximamente misturados e maximamente indeterminados:

$$S(A) = S(B) = 1. \quad (1.25)$$

A entropia (indeterminação do estado) dos subsistemas é uma medida do desaparecimento da informação que compara o estado puro com o sistema composto. No caso acima, considerando apenas os subsistemas, se perderá todas as informações sobre o estado composto. A informação sobre o sistema composto está contida na correlação entre os subestados. Quanto maior a entropia dos sistemas, mais forte é a correlação entre os subsistemas do estado puro composto. Deste modo, define-se a medida de entrelaçamento $E(\psi)$ do estado biparte $|\psi^{AB}\rangle$ a partir da entropia dos seus subsistemas

$$0 \leq E(\psi) := S(A) = S(B) \leq 1. \quad (1.26)$$

A medida $E(\psi)$ é também chamada de entropia de entrelaçamento. Com a equação (1.26) obtém-se que a medida entrelaçamento é dada por:

$$E(\psi) = - \sum_{n=1}^k p_n \log_2 p_n. \quad (1.27)$$

A entropia de entrelaçamento é função dos coeficiente de Schmidt p_n . Esta medida quantitativa do entrelaçamento é aplicável apenas para os estados puros bipartes. Para estados mistos, há uma série de medidas sugeridas que têm a entropia de entrelaçamento $E(\psi)$ como um especial de estados puros de sistemas bipartes.

A entropia de entrelaçamento depende apenas dos coeficientes de Schmidt, independe da base e não muda quando aplicadas transformações unitárias locais. Para $|\psi'^{AB}\rangle = U^A \otimes U^B |\psi^{AB}\rangle$, tem-se $E(\psi') = E(\psi)$. Estados em $\mathcal{H}_d \otimes \mathcal{H}_d$, para os quais $E(\psi) = \log_2^d$ com $d = \dim \mathcal{H}_d$ são chamados maximamente entrelaçados.

Capítulo 2

Medidas de entrelaçamento para estados puros multipartes e seu cálculo numérico

Neste capítulo apresenta-se um estudo de medida de entrelaçamento para estados puros multipartites (o mínimo da entropia da entropia de Shannon para a medição de estados ortogonais). Esta medida é aditiva, monótona sob LOCC, e coincide com a entropia do entrelaçamento para os estados puros bipartites. O cálculo da medida de entrelaçamento apresentado é um problema de otimização, [20].

Este capítulo está organizado com a seguinte estrutura: na primeira seção é apresentado o mínimo da entropia de Shannon para a medição de estados ortogonais como uma medida de entrelaçamento. Em seguida é apresentado um modelo de algoritmo genético para o cálculo dessa medida de entrelaçamento junto de um resultado numérico teste.

2.1 Mínima Entropia de Shannon sobre medição de estados ortogonais

Neste texto é necessário que se tenha em mente duas definições de entropia [21]: a entropia de Shannon, denotada por H_{sh} e a entropia de Von Neumann, denotada por H_{vN} . Considere um estado quântico puro de n qudits escrito por:

$$|\psi\rangle = \sum_{i_1, \dots, i_n=1}^d a_{i_1, \dots, i_n} |i_1, \dots, i_n\rangle . \quad (2.1)$$

Uma medição deste estado na base computacional apresenta o estado $|i_1, \dots, i_n\rangle$ com probabilidade $|a_{i_1, \dots, i_n}|^2$. Então, pode-se considerar este processo de medição como um gerador de

sinal aleatório que envia o estado $|i_1, \dots, i_n\rangle$ com probabilidade $|a_{i_1, \dots, i_n}|^2$. Assim, a entropia de Shannon deste gerador é a medição da incerteza anterior a medida do estado $|\psi\rangle$

$$H_{medida}(|\psi\rangle) = H_{sh}(Diag(|\psi\rangle\langle\psi|)) = \sum_{i_1, \dots, i_n=1}^d |a_{i_1, \dots, i_n}|^2 \log_2 |a_{i_1, \dots, i_n}|^2.$$

E essa característica de um estado quântico é variante sob mudanças locais da base de medição. O teorema de Shannon da codificação na fonte mostra que, no limite, o comprimento médio da representação mais curta possível para codificar as mensagens em um dado alfabeto é a entropia deles, dividida pelo logaritmo do número de símbolos do alfabeto. No caso do estado quântico de n qudits, na base computacional, são possíveis d^n símbolos.

O caminho natural para construir uma medida invariante com a base de medição é a minimização do $H_{medida}(|\psi\rangle)$, sob todas as possibilidades de mudança locais da base de medição:

$$E_{H \min}(|\psi\rangle) = \min_{U_1, \dots, U_n} H_{medida}(U_1 \otimes \dots \otimes U_n |\psi\rangle). \quad (2.2)$$

Para ilustração da minimização, considere a entropia do estado $|\psi\rangle$ quando todos os n sistemas quânticos estão desentrelaçados. Nota-se que a entropia para esse sistema pode assumir um valor maior que zero. No entanto, existem n transformações unitárias que transformam estes qudits em n qudits da base computacional, ou seja, $U_1 \otimes \dots \otimes U_n |\psi\rangle = |0_1 0_2 \dots 0_n\rangle$. Nota-se que qualquer estado quântico desentrelaçado pode ser transformado em um estado quântico da base computacional, em que não há superposição. Se não existe superposição, então a entropia é nula. Assim, a entropia de qualquer estado desentrelaçado sempre pode ser levada ao valor zero com as apropriadas transformações unitárias. No entanto, nota-se que um estado entrelaçado nunca terá entropia nula na sua medição. Pois, operações locais não transformam estados entrelaçados em estados que não possuem superposição. Logo, percebe-se que $E_{H \min}$ é uma medida de entrelaçamento do estado puro $|\psi\rangle$. É preciso somente avaliar se essa medida de entrelaçamento proposta satisfaz algumas condições para ser reconhecida como uma medida de entrelaçamento.

2.1.1 Propriedades necessárias para medidas de entrelaçamento

Medidas de entrelaçamento de estado quântico puro devem satisfazer as seguintes condições:

1. deve ser igual a zero para o estado desentrelaçado por completo;
2. deve ser invariante com aplicações de operações unitárias locais;
3. deve ser invariante a adição ou subtração de ancillas desentrelaçadas.

4. Não pode aumentar com LOCC.

Agora a tarefa a ser desenvolvida é provar que $E_{H \min}$ satisfaz as propriedades de (1) até (4). Os detalhes da prova de que $E_{H \min}$ é uma medida de entrelaçamento que satisfaz as quatro propriedades apresentadas (Apêndice B).

2.2 Cálculo de $E_{H \min}$ para qutrits com algoritmo genético

Para resolver o problema de otimização, é necessário parametrizar as matrizes unitárias U_i . Quando $d = 2$ esta parametrização é bem conhecida:

$$U_i(\beta_i, \delta_i, \gamma_i) = \begin{pmatrix} e^{i(-\beta_i - \delta_i)} \cos \gamma_i & -e^{i(-\beta_i + \delta_i)} \sin \gamma_i \\ e^{i(\beta_i - \delta_i)} \sin \gamma_i & e^{i(\beta_i + \delta_i)} \cos \gamma_i \end{pmatrix},$$

em que β_i , δ_i e γ_i são números reais. Parametrizações de matrizes unitárias de $d > 2$ é ainda uma questão em aberto. A mais conhecida parametrização está proposta em [16, 17], na qual tem um espaço de busca muito grande o que aumenta significativamente o tempo de execução na solução do problema. Ela é calculada a partir de um conjunto de oito matrizes 3×3 que formam o grupo de Lie $SU(3)$. Assim, foi necessária realizar uma escolha de uma outra parametrização que parametriza a matriz unitária U_i em função de 5 parâmetros independentes: $\alpha_i, \phi_i, \theta_i, \varphi_i$ e ϑ_i . Para facilitar a visualização de que U_i apresenta uma transformação unitária, escreve-se $U_i = T_A^i T_B^i$, e que T_A^i e T_B^i são matrizes unitárias escritas por:

$$T_A^i = \begin{pmatrix} \cos\left(\frac{\theta_i}{2}\right) & -\sin\left(\frac{\theta_i}{2}\right) e^{-i\frac{\varphi_i}{2}} & 0 \\ \sin\left(\frac{\phi_i}{2}\right) \cos\left(\frac{\phi_i}{2}\right) e^{i\frac{\varphi_i}{2}} & \cos\left(\frac{\theta_i}{2}\right) \cos\left(\frac{\phi_i}{2}\right) & -\sin\left(\frac{\phi_i}{2}\right) e^{-i\frac{\varphi_i}{2}} \\ \sin\left(\frac{\theta_i}{2}\right) \sin\left(\frac{\phi_i}{2}\right) e^{i\frac{(\varphi_i + \vartheta_i)}{2}} & \cos\left(\frac{\theta_i}{2}\right) \sin\left(\frac{\phi_i}{2}\right) e^{i\frac{\vartheta_i}{2}} & \cos\left(\frac{\phi_i}{2}\right) \end{pmatrix} e^{-i\frac{\alpha_i}{2}}$$

$$T_B^i = \begin{pmatrix} \cos\left(\frac{\theta_i}{2}\right) & -\sin\left(\frac{\theta_i}{2}\right) \cos\left(\frac{\phi_i}{2}\right) e^{-i\frac{\varphi_i}{2}} & \sin\left(\frac{\theta_i}{2}\right) \sin\left(\frac{\phi_i}{2}\right) e^{-i\frac{(\varphi_i + \vartheta_i)}{2}} \\ \sin\left(\frac{\phi_i}{2}\right) e^{i\frac{\varphi_i}{2}} & \cos\left(\frac{\theta_i}{2}\right) \cos\left(\frac{\phi_i}{2}\right) & -\sin\left(\frac{\phi_i}{2}\right) \cos\left(\frac{\theta_i}{2}\right) e^{-i\frac{\vartheta_i}{2}} \\ 0 & \sin\left(\frac{\phi_i}{2}\right) e^{i\frac{\vartheta_i}{2}} & \cos\left(\frac{\phi_i}{2}\right) \end{pmatrix}$$

No lugar de escrever a matriz unitária U_i , serão escritos os vetores coluna dessa matriz que são os estados quânticos de três níveis:

$$\begin{aligned}
|\psi_i^1\rangle &= e^{-i\frac{\alpha_i}{2}} \begin{pmatrix} \cos(\theta_i) \\ -\text{sen}(\theta_i) \cos\left(\frac{\phi_i}{2}\right) e^{-i\frac{\varphi_i}{2}} \\ \text{sen}(\theta_i) \text{sen}\left(\frac{\phi_i}{2}\right) e^{-i\frac{(\varphi_i+\vartheta_i)}{2}} \end{pmatrix} \\
|\psi_i^2\rangle &= e^{-i\frac{\alpha_i}{2}} \begin{pmatrix} \text{sen}(\theta_i) \cos\left(\frac{\phi_i}{2}\right) e^{i\frac{\varphi_i}{2}} \\ \cos^2\left(\frac{\phi_i}{2}\right) \cos(\theta_i) - \text{sen}^2\left(\frac{\phi_i}{2}\right) \\ -\frac{\text{sen}(\phi_i)}{2} (\cos(\theta_i) + 1) e^{-i\frac{\vartheta_i}{2}} \end{pmatrix} \\
|\psi_i^3\rangle &= e^{-i\frac{\alpha_i}{2}} \begin{pmatrix} \text{sen}(\theta_i) \text{sen}\left(\frac{\phi_i}{2}\right) e^{i\frac{(\varphi_i+\vartheta_i)}{2}} \\ \frac{\text{sen}(\phi_i)}{2} (\cos(\theta_i) + 1) e^{i\frac{\vartheta_i}{2}} \\ \cos^2\left(\frac{\phi_i}{2}\right) - \text{sen}^2\left(\frac{\phi_i}{2}\right) \cos(\theta_i) \end{pmatrix} \tag{2.3}
\end{aligned}$$

Portanto, tem-se a transformação unitária local para sistemas de três níveis escrita por:

$$U_i = e^{-i\frac{\alpha_i}{2}} \left(|\psi_i^1\rangle \quad |\psi_i^2\rangle \quad |\psi_i^3\rangle \right) \rightarrow U_i^\dagger = e^{i\frac{\alpha_i}{2}} \begin{pmatrix} \langle\psi_i^1| \\ \langle\psi_i^2| \\ \langle\psi_i^3| \end{pmatrix}.$$

Verifica-se que a seguinte igualdade é verdadeira:

$$U_i^\dagger U_i = \begin{pmatrix} \langle\psi_i^1|\psi_i^1\rangle & \langle\psi_i^1|\psi_i^2\rangle & \langle\psi_i^1|\psi_i^3\rangle \\ \langle\psi_i^2|\psi_i^1\rangle & \langle\psi_i^2|\psi_i^2\rangle & \langle\psi_i^2|\psi_i^3\rangle \\ \langle\psi_i^3|\psi_i^1\rangle & \langle\psi_i^3|\psi_i^2\rangle & \langle\psi_i^3|\psi_i^3\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Pode-se observar que o vetor coluna da matriz U_i é o estado quântico escrito na equação (1). Esse vetor pode representar com esses 5 parâmetros toda superposição possível de um qutrit. Além disso, todos os vetores coluna são unitários e ortogonais entre si. O segundo e o terceiro vetor coluna têm os mesmos parâmetros do primeiro vetor coluna. Nota-se em cálculos que o primeiro vetor coluna é ortogonal ao segundo e ao terceiro. Também, o segundo vetor coluna é ortogonal ao terceiro.

Para os cálculos, tem-se que α_i é o ângulo da fase global e pode ser desconsiderado. O cálculo de E_{Hmin} para qutrits multipates é uma tarefa de otimização $4n$ parâmetros reais. Para calcular $E_{Hmin}(|\psi\rangle)$, deve-se minimizar a função,

$$f^\psi(\phi_1, \theta_1, \varphi_1, \vartheta_1, \dots, \phi_n, \theta_n, \varphi_n, \vartheta_n) = H_{medida} \left(\bigotimes_{i=1}^n U(\phi_i, \theta_i, \varphi_i, \vartheta_i) |\psi\rangle \right).$$

Em que $U_i = U(\phi_i, \theta_i, \varphi_i, \vartheta_i)$.

Num caso geral, a função f^ψ pode ser multimodal (tendo muitos mínimos locais), devido a este fato não se sugere o uso do método de otimização baseado em gradiente. O algoritmo genético é uma escolha eficaz, pois efetiva uma distinção do melhor valor que otimiza a função.

2.2.1 Método para obtenção da transformação unitária local para um qutrit

Apresenta-se os cálculos para a obtenção de transformação unitária local para qutrits. No algoritmo genético apresentado neste trabalho, várias dessas matrizes sofrem variações nos seus parâmetros para a obtenção do menor valor da entropia de Shannon sobre os elementos da diagonal da matriz densidade de estados puros. A quantidade de operações locais e o número de parâmetros a serem variados em cada matriz determina o espaço de busca do algoritmo genético. Por isso, foi necessária otimizar a representação dessas matrizes dentro do algoritmo genético utilizado. Neste texto, mostra-se o procedimento para o cálculo destas matrizes.

Duas matrizes elementares foram usadas para compor a transformação unitária local para um qutrit. Essas matrizes elementares são:

$$M_1 = \begin{pmatrix} \cos(a) & -e^{-ix}\text{sen}(a) & 0 \\ e^{ix}\text{sen}(a) & \cos(a) & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (2.4)$$

$$M_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(b) & -e^{-iy}\text{sen}(b) \\ 0 & e^{iy}\text{sen}(b) & \cos(b) \end{pmatrix} \quad (2.5)$$

As matrizes M_1 e M_2 são unitárias, constroem apenas superposição de dois níveis e a fase global é negligenciada. Fazendo o produto M_2M_1 e M_1M_2 obtém-se as seguintes matrizes unitárias:

$$M_2M_1 = \begin{pmatrix} \cos(a) & -e^{-ix}\text{sen}(a) & 0 \\ e^{ix}\cos(b)\text{sen}(a) & \cos(a)\cos(b) & -e^{-iy}\text{sen}(b) \\ e^{ix+iy}\text{sen}(a)\text{sen}(b) & e^{iy}\cos(a)\text{sen}(b) & \cos(b) \end{pmatrix} \quad (2.6)$$

$$M_1M_2 = \begin{pmatrix} \cos(a) & -e^{-ix}\cos(b)\text{sen}(a) & e^{-ix-iy}\text{sen}(a)\text{sen}(b) \\ e^{ix}\text{sen}(a) & \cos(a)\cos(b) & -e^{-iy}\cos(a)\text{sen}(b) \\ 0 & e^{iy}\text{sen}(b) & \cos(b) \end{pmatrix} \quad (2.7)$$

Na matriz M_2M_1 , verifica-se que o primeiro e o segundo vetores coluna podem representar qualquer superposição de três níveis. No entanto, um de seus vetores ortogonais (vetor da terceira coluna) não pode representar qualquer superposição de três níveis por conter apenas duas variáveis como parâmetro de construção do estado. De forma análoga, na matriz M_1M_2 os vetores da segunda e terceira coluna podem ser usados para representar quaisquer estados com superposições de três níveis. Note que eles serão sempre ortogonais entre si. No entanto, o primeiro vetor coluna possui apenas duas variáveis e não pode ser usado para representar qualquer superposição de três níveis. Para ser mais preciso, só existe nesse vetor superposição de dois níveis.

O produto $M_2M_1M_1M_2$ foi usado para construir uma transformação unitária local para 3 quidits.

$$\begin{pmatrix} \cos(2a) & -2e^{-ix}\cos(a)\cos(b)\sin(a) & e^{-ix-iy}\text{sen}(2a)\text{sen}(b) \\ e^{ix}\cos(b)\text{sen}(2a) & \cos(2a)\cos(b)^2 - \text{sen}(b)^2 & -e^{-iy}\cos(a)^2\text{sen}(2b) \\ e^{ix+iy}\text{sen}(2a)\text{sen}(b) & e^{iy}\cos(a)^2\text{sen}(2b) & \cos(b)^2 - \cos(2a)\text{sen}(b)^2 \end{pmatrix} \quad (2.8)$$

Multiplicando a matriz acima pelo estado quântico $|1\rangle = (1, 0, 0)^T$ resulta no primeiro vetor coluna da matriz, ou seja, o estado

$$\begin{pmatrix} \cos(2a) \\ e^{ix}\cos(b)\text{sen}(2a) \\ e^{ix+iy}\text{sen}(2a)\text{sen}(b) \end{pmatrix}. \quad (2.9)$$

De forma análoga, a transformação unitária aplicada aos estados $|2\rangle = (0, 1, 0)^T$ e $|3\rangle = (0, 0, 1)^T$, respectivamente, resultam nos estados quânticos abaixo:

$$\begin{pmatrix} -2e^{-ix}\cos(a)\cos(b)\sin(a) \\ \cos(a)^2\cos(b)^2 - \cos(b)^2\text{sen}(a)^2 - \text{sen}(b)^2 \\ e^{iy}\cos(a)^2\text{sen}(2b) \end{pmatrix}; \quad (2.10)$$

$$\begin{pmatrix} e^{-ix-iy}\text{sen}(2a)\text{sen}(b) \\ -e^{-iy}\cos(a)^2\text{sen}(2b) \\ \cos(b)^2 - \cos(2a)\text{sen}(b)^2 \end{pmatrix}. \quad (2.11)$$

O segundo vetor coluna, equação 2.10, está simplificado na equação 2.8.

A matriz da equação (2.8) é a matriz unitária para realizar as transformações unitárias locais nos qutrits que são o objeto de estudo deste trabalho. Todos os vetores possuem superposição de três níveis e são expressos por quatro variáveis livres. Uma quinta variável, a que representa

a fase global, foi negligenciada, porque a sua variação é irrelevante para o estudo do entrelaçamento.

2.2.2 Algoritmo Genético

Um algoritmo genético (GA) é um método de otimização que busca por melhor resultado da função objetivo. Este método é popularmente aplicado em problema de otimização e inspirado na Teoria da Evolução de Darwin. Um algoritmo genético já foi usado para cálculo de entrelaçamento quântico (calcular a entropia relativa de entrelaçamento dos estados bipartite misto) em [22].

Agora, descreve-se o GA que foi usado para calcular E_{Hmin} . Primeiro uma população inicial de matrizes unitárias é gerada:

$$\begin{aligned} \mathcal{U}_1 &= \{U(\phi_{11}, \theta_{11}, \varphi_{11}, \vartheta_{11}), \dots, U(\phi_{1k}, \theta_{1k}, \varphi_{1k}, \vartheta_{1k})\}, \\ &\vdots \\ \mathcal{U}_n &= \{U(\phi_{n1}, \theta_{n1}, \varphi_{n1}, \vartheta_{n1}), \dots, U(\phi_{nk}, \theta_{nk}, \varphi_{nk}, \vartheta_{nk})\}. \end{aligned} \quad (2.12)$$

Em que \mathcal{U}_i é uma coleção de matrizes para serem usadas no i -ésimo sistema de um estado quântico de n partes. O tamanho da população é k , assim são geradas k matrizes para o i -ésimo sistema ($i = 1, 2, 3, \dots, n$). Os parâmetros $\phi_{ij}, \theta_{ij}, \varphi_{ij}, \vartheta_{ij}$ pertencem todos ao intervalo $[0, 2\pi]$ e seus valores são todos escolhidos aleatoriamente ($j = 1, 2, \dots, k$ representa um indivíduo da população).

A seleção é procedida através da função f^ψ para a escolha da melhor matriz

$$U_j = \bigotimes_{i=1}^n U(\phi_{ij}, \theta_{ij}, \varphi_{ij}, \vartheta_{ij}).$$

A matriz que produz o menor valor de f^ψ será escolhida como a melhor, pois deve-se encontrar o menor valor de H_{medida} .

Após a seleção da melhor matriz, um cruzamento dessa matriz é realizado com as demais matrizes da população. Assim, as matrizes herdarão características de semelhança com aquela que ofereceu o melhor resultado. Para ilustrar como o crossover é executado, considere dois filhos de tamanho 10, dados respectivamente pelas strings 0101010101 e 1111000011. Execute-se o crossover de dois pontos nestes dois cromossomos e sorteia-se os pontos de corte 4 e 8. O primeiro filho será dado, então, pela parte do primeiro pai até o ponto de corte 4(0101), a parte do segundo pai entre o ponto de corte 4 e o ponto de corte 8(0000) e a parte do primeiro pai

localizada após o ponto do corte 8(01). No final, o valor deste filho será 0101000001.

Embora algoritmos genéticos sejam simples de serem implementados, a análise de convergência desses algoritmos não é simples de ser feita. Pois sabe-se que em geral ele converge para a solução ótima, mas não se sabe como isso acontece ao longo das gerações. Em princípio, um fato é fácil de ser constatado. A complexidade de tempo desses algoritmos deve ser função principalmente do tamanho do cromossomo.

O tamanho do cromossomo diz o tamanho do espaço de busca real da solução, enquanto que o tamanho da população a cada geração representa apenas uma parte de todo o espaço de busca. Por exemplo, se o tamanho da população $N = 2^{|\text{cromossomo}|}$, acontecerá que o GA se transformará em um algoritmo de busca, pois todas as soluções possíveis estão na população inicial. Logo, na primeira seleção pode-se ter a certeza de que o melhor resultado já foi encontrado. Em geral, é natural a escolha do tamanho da população bem menor que o tamanho do espaço de busca. Embora não se saiba como a convergência do GA acontece, pode-se intuir que $O(f(2^{|\text{cromossomo}|}))$, em que a função $f(\cdot)$ é desconhecida.

O vantagem deste trabalho está exatamente no fato de que o tamanho do cromossomo foi reduzido pela metade. Pois, numa parametrização, usando um parâmetro para cada uma das matrizes do grupo $SU(3)$ são necessários 8 parâmetros reais, enquanto que nesta parametrização são necessárias apenas 4 para obter o mesmo resultado. Assim, a complexidade desse GA passou para $O\left(f\left(2^{\frac{|\text{cromossomo}|}{2}}\right)\right)$. Se $f(\cdot)$ não for uma função logaritma no tamanho do cromossomo, então a redução no tempo de espera se torna significativo. Acredita-se que é exatamente esse o caso, pois percebe-se um acréscimo significativo no tempo de execução do GA quando o cromossomo é aumentado.

Neste trabalho o cálculo da medida de entrelaçamento é um problema de otimização e não de dedução, isto é, nem sempre a resposta encontrada será a melhor solução para o problema. Para diminuir esse problema no algoritmo genético proposto, foi usada uma técnica conhecida como pressão de seleção. Um procedimento para a verificação da homogeneidade da população ou, alternativamente, da perda de diversidade é executado. Então quando verificada a perda de diversidade da população, dois indivíduos mais aptos são guardados e uma nova população é escolhida aleatoriamente. Ainda, para aumentar a diversidade da população, eleva-se a taxa de mutação e evita-se cromossomos duplicados na população quando ela é gerada. Neste trabalho, as taxas de crossover e mutação são independentes do processo de pressão de seleção.

2.3 Resultados numéricos

Agora serão apresentados alguns resultados numéricos que serviram para testar a eficiência do algoritmo proposto. Para estes testes, foram usados qutrits bipartes, uma vez que o entrelaçamento desses estados podem ser facilmente calculados a partir dos coeficientes de Schmidt.

O estado quântico $|00\rangle$ é desentrelaçado. Neste caso $E(|00\rangle) = 0$. Com esse estado, nós calculamos o entrelaçamento até 30 gerações para verificarmos a convergência do algoritmo genético para o valor 0. O resultado está na figura abaixo:

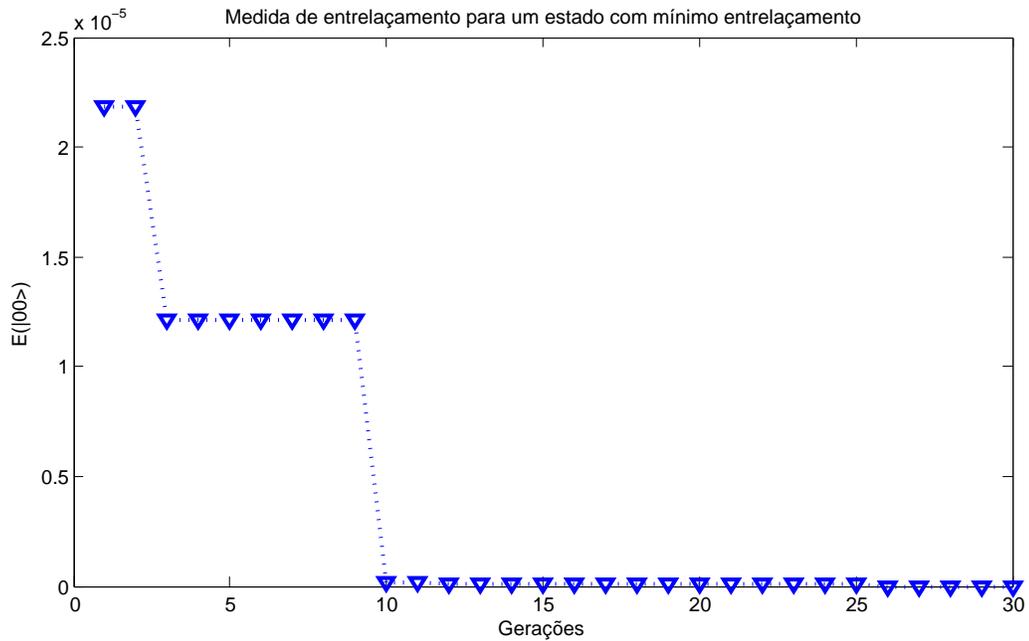


Figura 2.1: Cálculo do grau de entrelaçamento para um estado completamente desentrelaçado.

O estado quântico $|EPR\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ é maximamente entrelaçado. Neste caso o entrelaçamento é $E((|00\rangle + |11\rangle)/\sqrt{2}) = 1$. Com esse estado, nós calculamos o entrelaçamento até 30 gerações para verificarmos a convergência do algoritmo genético para o valor 1. O resultado está na figura abaixo:

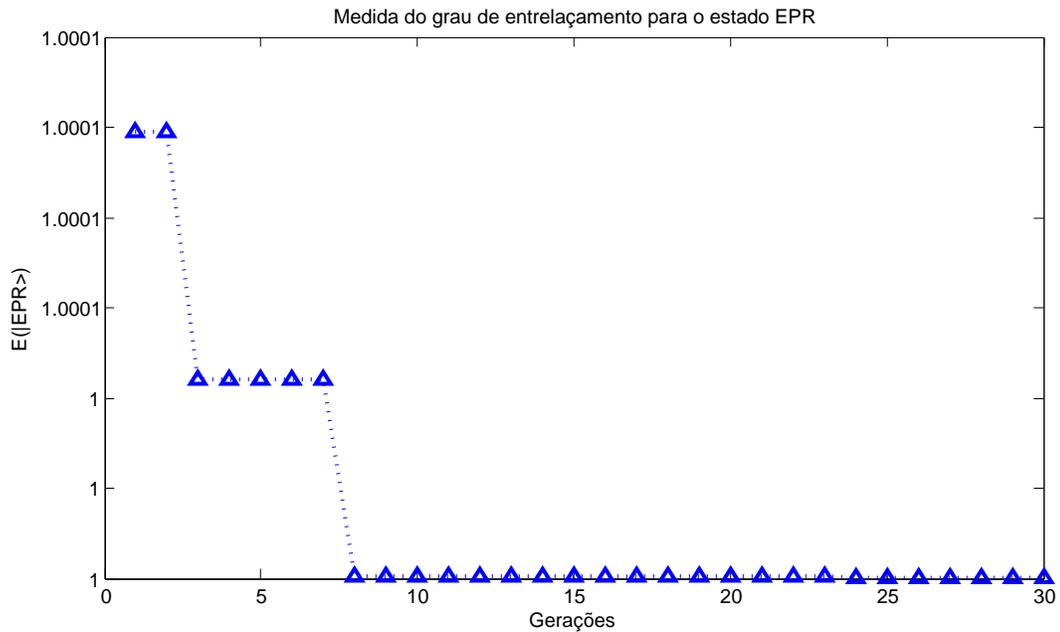


Figura 2.2: Cálculo do grau de entrelaçamento para um estado maximamente entrelaçado.

Notamos que os valores do entrelaçamento nas primeiras gerações já são bem próximos dos valores esperados. Notamos na Figura 2.2 que inicialmente o valor é 1.0001. Acima do que se espera do valor do entrelaçamento para este estado. Nesse caso acreditamos que se trata de um erro de arredondamento que desaparece nas gerações seguintes.

Ao longo das próximas simulações calcularemos o entrelaçamento para cada estado com 2.000 gerações e taxa de mutação de 0.008. Esse número grande de gerações nos faz acreditar que vão haver cruzamentos suficientes para chegar num valor correto de entrelaçamento. Havendo maior chance de ocorrer mutações nessas gerações. O primeiro estado que será visto o entrelaçamento é:

$$|\psi\rangle = \sqrt{p}|00\rangle + \sqrt{1-p}|12\rangle. \quad (2.13)$$

Na figura abaixo obtemos o resultado:

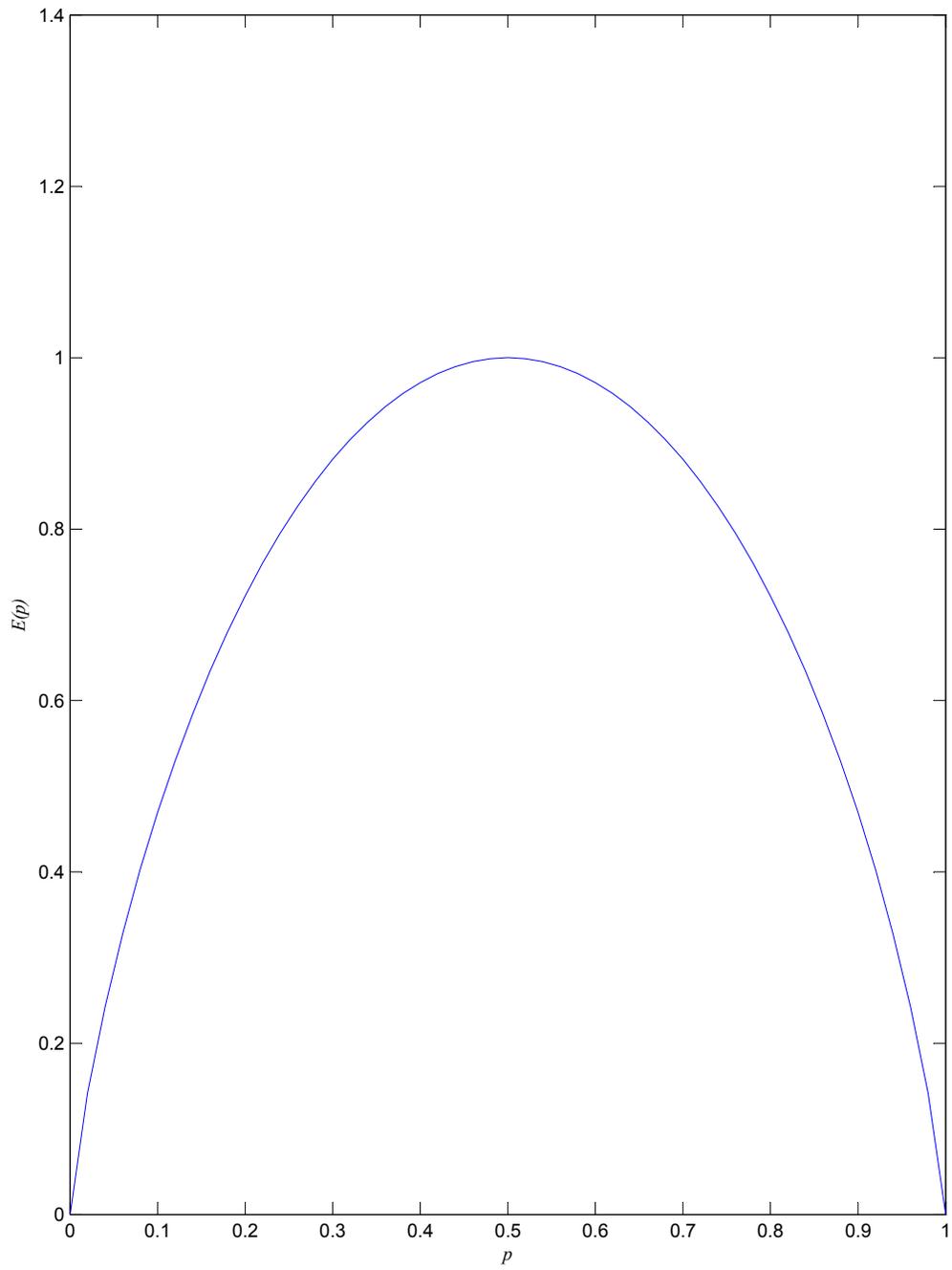


Figura 2.3: Entrelaçamento de qutrits com apenas dois termos de superposição.

Observa-se neste caso exatamente a curva da função da entropia $H(p) = p \log_2^p + (1 - p) \log_2^{1-p}$. O resultado alcançado usando o algoritmo genético é idêntico ao resultado esperado. Mostrando que a parametrização proposta para diminuir o espaço de busca não alterou os resultados da medida de entrelaçamento. Esse é um resultado a favor do uso da parametrização proposta para verificar o grau de entrelaçamento de outros qutrits, embora não seja uma prova de que funcionará para outros estados.

Agora consideremos o estado que possui três estados na superposição escrito por:

$$|\psi\rangle = \sqrt{q}|00\rangle + \sqrt{(1-q)p}|11\rangle + \sqrt{(1-q)(1-p)}|22\rangle. \quad (2.14)$$

A expressão acima representa um conjunto maior de estados entrelaçados. Os valores encontrados do $E(|\psi\rangle)$ usando o algoritmo genético estão dados na matriz abaixo. Foram calculados um total de 25 pontos em que p e q estão variando num intervalo de 0 a 1 com um passo de 0.25.

$$\begin{pmatrix} 0 & 0.8113 & 1.0000 & 0.8113 & 0 \\ 0.8113 & 1.4197 & 1.5613 & 1.4197 & 0.8113 \\ 1.0000 & 1.4056 & 1.5000 & 1.4056 & 1.0000 \\ 0.8113 & 1.0141 & 1.0613 & 1.0141 & 0.8113 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (2.15)$$

Uma verificação satisfatória do algoritmo genético para este estado traz mais confiabilidade quanto ao uso das matrizes unitárias propostas neste trabalho. Sabe-se de antemão de que a medida do entrelaçamento do estado acima é dado por: $E(|\psi\rangle) = q \log_2^q + (1-q)p \log_2^{(1-q)p} + (1-q)(1-p) \log_2^{(1-q)(1-p)}$.

A figura abaixo apresenta o resultado de $E(|\psi\rangle)$ para o estado da equação 2.14 usando o algoritmo genético.

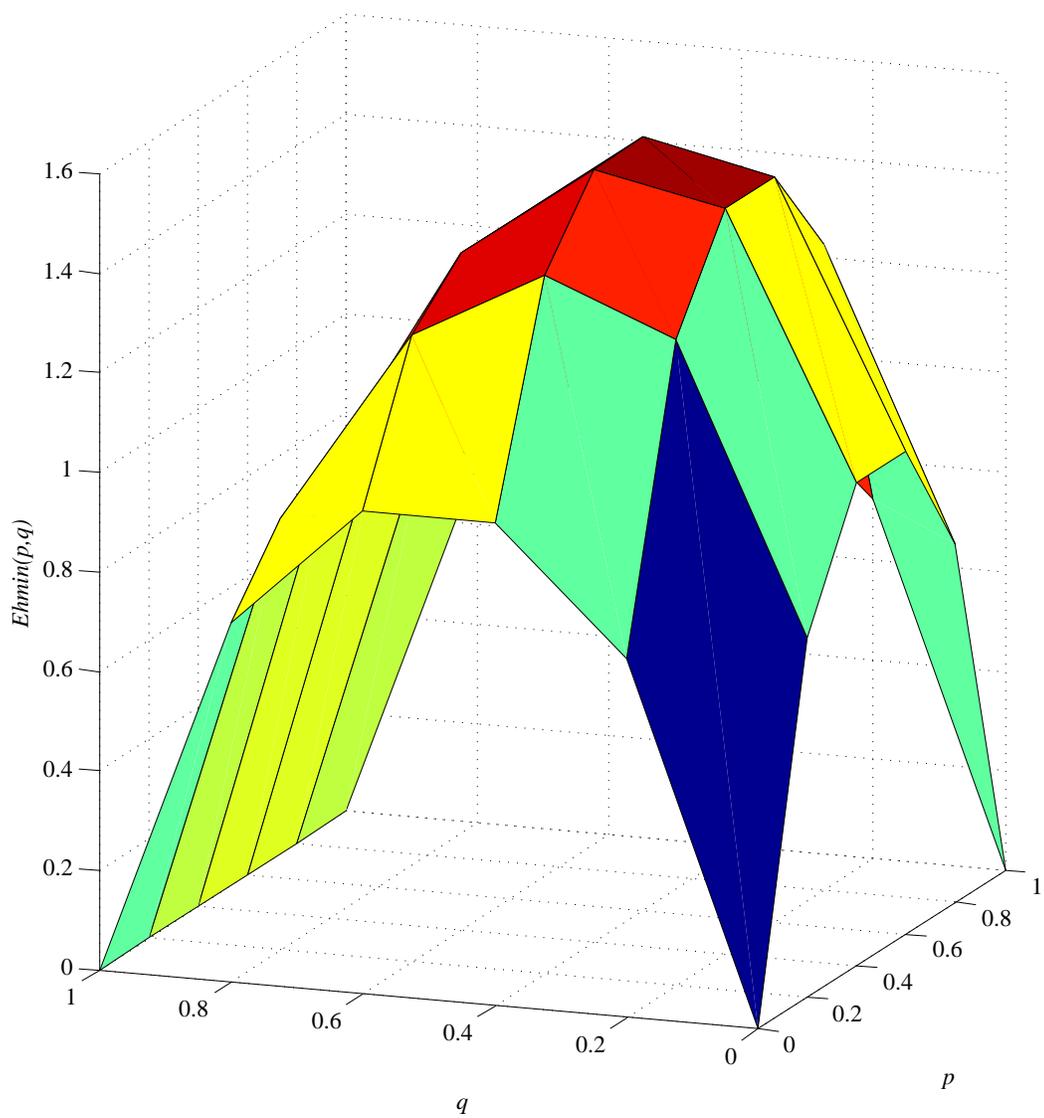


Figura 2.4: Entrelaçamento de qutrits com três termos de superposição.

Conclusões e Perspectivas

Neste trabalho, apresenta-se um algoritmo genético para o cálculo do grau de entrelaçamento de qutrits. A medida de entrelaçamento utilizada neste texto satisfaz todas as condições exigidas para o estudo de entrelaçamento de qutrits multipartes. Por isso, o seu estudo é de grande importância para investigação de outras propriedades de entrelaçamento.

O maior problema no algoritmo apresentado neste texto é o tamanho do espaço de busca que aumenta significativamente o tempo de execução dos cálculos. A parametrização de matrizes unitárias locais para qutrits com apenas cinco parâmetros reduz o espaço de busca e, consequentemente, reduz o tempo de espera pelo fim dos cálculos. A quantidade de parâmetros usada neste trabalho é um valor menor do que a usada em parametrizações já conhecidas que usam oito parâmetros [16, 17]. Porém, não foi provado que esta parametrização é útil para representar qualquer transformação unitária de qutrits, mas ela se aplicou muito bem em resultados já conhecidos, mostrando assim, que a alternativa apresentada pode ser útil para o cálculo da medida de entrelaçamento de qutrits.

As perspectivas futuras são:

- investigar se a parametrização apresentada é útil para representar qualquer transformação unitária local;
- testar o algoritmo genético proposto no cálculo de medida do grau de entrelaçamento de estados quânticos cujas identificação dos seus entrelaçamentos não sejam triviais;
- realizar medições do grau de entrelaçamento usando outras funções fitness, ou seja, usar outras medidas de entrelaçamento.

Apêndice A

Introdução à teoria da informação quântica

A.1 estados quânticos e transformações unitárias

A informação quântica está construída sobre o conceito de bit quântico ou qubit. Da mesma forma que um bit clássico pode assumir os estados 0 ou 1, o qubit pode assumir os estados $|0\rangle$ ou $|1\rangle$. Porém, a diferença entre bit e qubit é que os qubits podem estar em estados diferentes de $|0\rangle$ e $|1\rangle$. O fato é que para eles, também são possíveis combinações lineares dos estados $|0\rangle$ e $|1\rangle$, chamadas de superposição:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \quad (\text{A.1})$$

Os números α e β são números complexos que obedecem à relação $|\alpha| + |\beta| = 1$. O que mostra que na sua forma geral um qubit é um vetor unitário em um espaço vetorial complexo de duas dimensões. Os estados $|0\rangle$ e $|1\rangle$ é a base canônica a qual chamaremos de base retangular, e denotaremos por $B_0 = \{|0\rangle, |1\rangle\}$. A representação vetorial destes qubits é feita pelos seguintes vetores coluna:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad (\text{A.2})$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (\text{A.3})$$

Fisicamente, quando medimos o qubit em (A.1), encontramos o estado $|0\rangle$ com probabilidade $|\alpha|^2$ e o estado $|1\rangle$ com probabilidade $|\beta|^2$. Note que os estados $|0\rangle$ e $|1\rangle$ representam apenas

uma dentre muitas escolhas possíveis para a base de estados de um qubit. Outra escolha possível é a base $B_1 = \{|+\rangle, |-\rangle\}$, denominada base diagonal. Os estados quânticos $|+\rangle$ e $|-\rangle$ são superposições (ou combinações lineares) dos estados quânticos $|0\rangle$ e $|1\rangle$:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ e } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (\text{A.4})$$

Se expressarmos o estado de (A.1) na base diagonal, teremos:

$$|\psi\rangle = \frac{\alpha + \beta}{\sqrt{2}}|+\rangle + \frac{\alpha - \beta}{\sqrt{2}}|-\rangle. \quad (\text{A.5})$$

Naturalmente, uma medição de $|\psi\rangle$ na base diagonal resultará em $|+\rangle$ com probabilidade $|\alpha + \beta|^2/2$ e resultará em $|-\rangle$ com probabilidade $|\alpha - \beta|^2/2$.

Nos computadores clássicos existem portas lógicas que processam a informação alterando ou não os estados dos bits. Na computação quântica também existem portas que atuam sobre o qubit de forma a alterar o estado do mesmo. Vimos que um qubit é um vetor unitário num espaço vetorial duas dimensões sobre o conjunto dos números complexos. Portanto, portas quânticas de um qubit podem ser descritas por matrizes 2×2 . Porém, existem restrições para as matrizes que são usadas para representar uma porta quântica. Um qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ tem uma condição de normalização: $|\beta|^2 + |\alpha|^2 = 1$. Isso também deve ser verdade para o estado $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$, após a atuação da porta. A condição para uma matriz representar uma porta em computação quântica é que a mesma seja uma matriz unitária, $U^\dagger U = U U^\dagger = I$, sendo U^\dagger a matriz adjunta de U (transposta conjugada de U) e I é a matriz identidade.

Nos computadores clássicos, a porta NOT inverte o valor do bit de entrada, NOT(0)=1 e NOT(1)=0. Na computação quântica existem operações unitárias que realizam operações análogas. Para a base retangular a operação unitária que realiza a inversão de qubit é definida por:

$$\begin{aligned} X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ X(\alpha|0\rangle + \beta|1\rangle) &= \alpha X|0\rangle + \beta X|1\rangle \\ &= \alpha \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \alpha \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \beta \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \alpha|1\rangle + \beta|0\rangle. \end{aligned}$$

Para a base diagonal, também existe uma transformação unitária que realiza a troca do qubit $|+\rangle$ para o qubit $|-\rangle$ e vice-versa. Esta transformação unitária é definida por:

Operações unitárias	B_0		B_1	
	Entrada $ 0\rangle$	Entrada $ 1\rangle$	Entrada $ +\rangle$	Entrada $ -\rangle$
X	$ 1\rangle$	$ 0\rangle$	$ +\rangle$	$- -\rangle$
Z	$ 0\rangle$	$- 1\rangle$	$ -\rangle$	$ +\rangle$
H	$ +\rangle$	$ -\rangle$	$ 0\rangle$	$ 1\rangle$

Tabela A.1: Resultados das operações X , Z e H aplicada aos qubits de entrada $|0\rangle$ e $|1\rangle$ da base B_0 , e aos qubits $|+\rangle$ e $|-\rangle$ da base B_1 .

$$\begin{aligned}
Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \\
Z(\alpha|+\rangle + \beta|-\rangle) &= \alpha Z|+\rangle + \beta Z|-\rangle \\
&= \alpha \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \beta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \\
&= \alpha \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} + \beta \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \alpha|-\rangle + \beta|+\rangle
\end{aligned}$$

Por fim, existe uma transformação unitária que realiza a transformação de estados da base B_0 para estados da base B_1 e vice-versa. Esta transformação, chamada de porta Hadamard, é definida por:

$$\begin{aligned}
H &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \\
H|0\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+\rangle \\
H|-\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle
\end{aligned}$$

A Tabela A.1 mostra as operações realizadas pelas portas X , Z e H sobre os qubits de entradas $|0\rangle$, $|1\rangle$, $|+\rangle$ e $|-\rangle$.

Apêndice B

Demonstração de que a medida de entrelaçamento $E_{H \min}$ satisfaz as condições exigidas para uma medida de entrelaçamento

A demonstração apresentada neste texto estão em [20] onde a medida de entrelaçamento usada neste trabalho foi proposta. Para provar as quatro condições requeridas para uma medida de entrelaçamento apresentada no capítulo 2, deve-se considerar uma outra propriedade importante: a aditividade do $E_{H \min}$. Sejam $|\psi_1\rangle$ e $|\psi_2\rangle$ estados puros multipartes (podem estar entrelaçado ou não), então:

$$E_{H \min} (|\psi_1\rangle \otimes |\psi_2\rangle) = E_{H \min} (|\psi_1\rangle) + E_{H \min} (|\psi_2\rangle)$$

A prova é diretamente da definição de $E_{H \min}$ e da aditividade da entropia de Shannon. As propriedades (1) e (2) são triviais e (3) é uma consequência da aditividade de $E_{H \min}$. Para provar (4), dados que (2) e (3) são verdadeiras, precisamos provar somente que $E_{H \min}$ não aumenta sob medições ortogonais. Para mostrar a monotocidade segundo a forma de medições ortogonais média, necessitamos de alguns lemas.

Lema 1. *Seja ρ_{AB} uma matriz densidade em um estado puro bipartite, então*

$$\begin{aligned} H_{sh} (Diag (\rho_A)) &\leq H_{sh} (Diag (\rho_{AB})) \\ &\leq H_{sh} (Diag (\rho_A)) + H_{sh} (Diag (\rho_B)) \end{aligned}$$

Em que ρ_A e ρ_B estão reduzidos a matriz densidade.

Prova. A igualdade deixa seguir do grupo generalizado de entropia de Shannon:

$$\begin{aligned} & H_{sh}(p_1, \dots, p_{\sigma_1}, p_{\sigma_1+1}, \dots, p_{\sigma_2}, \dots, p_{\sigma_{n-1}+1}, \dots, p_{\sigma_n}) \\ &= H_{sh}(p_1 + \dots + p_{\sigma_1}, p_{\sigma_1+1} + \dots + p_{\sigma_2}, \dots, p_{\sigma_{n-1}+1} + \dots + p_{\sigma_n}) \\ &+ \sum (p_{\sigma_{i-1}+1} + \dots + p_{\sigma_i}) H_{sh}\left(p_{\sigma_{i-1}+1} / \sum_{j=\sigma_{i-1}+1}^{\sigma_i} p_j, \dots, p_{\sigma_i} / \sum_{j=\sigma_{i-1}+1}^{\sigma_i} p_j\right) \end{aligned}$$

A parte direita segue a sub-aditividade da entropia:

$$\begin{aligned} & H_{sh}(\nu_{11}, \dots, \nu_{1m}, \nu_{21}, \dots, \nu_{2m}, \dots, \nu_{n1}, \dots, \nu_{nm}) \\ & \leq H_{sh}(\sum_{i=1}^n \nu_{i1}, \dots, \sum_{i=1}^n \nu_{im}) + H_{sh}(\sum_{j=1}^m \nu_{j1}, \dots, \sum_{j=1}^m \nu_{nj}) \end{aligned}$$

Lema 2. Seja $|\psi\rangle = \sum_{i_1, \dots, i_n=1}^d a_{i_1, \dots, i_n} |i_1, \dots, i_n\rangle$ um estado puro de n qudits. Se os estados $|j\rangle \otimes |\psi_j\rangle$ são resultados das medições de $|\psi\rangle$ na base computacional com probabilidade p_j , então

$$H_{medida}(U_1 |\psi\rangle) \geq \sum_{j=1}^d p_j H_{medida}(|j\rangle \otimes |\psi_j\rangle). \quad (\text{B.1})$$

Em que U_1 é uma transformação unitária arbitraria do primeiro qudit.

Prova. Se $|j\rangle \otimes |\psi_j\rangle$ são resultados da medição de $|\psi\rangle$ na base computacional com probabilidade p_j , então $|\psi\rangle$ pode ser representado por $|\psi\rangle = \sum_{j=1}^d c_j |j\rangle \otimes |\psi_j\rangle$, em que $|c_j|^2 = p_j$. Seja ψ_j^k , para $k = 1, \dots, d^{n-1}$, a amplitude de $|\psi_j\rangle$, então

$$\begin{aligned} & H_{medida}(|\psi\rangle) = H_{medida}\left(\sum_{j=1}^d c_j |j\rangle \otimes |\psi_j\rangle\right) \\ &= H_{sh}\left(|c_1|^2 |\psi_1^1|^2, \dots, |c_1|^2 |\psi_1^{d^{n-1}}|^2, \dots, |c_d|^2 |\psi_d^1|^2, \dots, |c_d|^2 |\psi_d^{d^{n-1}}|^2\right) \\ &\rightarrow \{\text{pela aditividade forte da entropia de Shannon}\} \\ &= H_{sh}(p_1, \dots, p_d) + \sum_{j=1}^d p_j H_{sh}\left(|\psi_j^1|^2, \dots, |\psi_j^{d^{n-1}}|^2\right) \\ &= \sum_{j=1}^d p_j H_{medida}(|j\rangle \otimes |\psi_j\rangle) + H_{sh}(p) \end{aligned}$$

Usando isto, podemos reescrever (3) na forma equivalente

$$H_{medida}(|\psi\rangle) \leq H_{medida}(U_1 |\psi\rangle) + H_{sh}(p) \quad (\text{B.2})$$

Seja $\rho = |\psi\rangle \langle \psi|$ a matriz densidade de estado $|\psi\rangle$, $\rho_1 = T_{\Gamma_{2,3,\dots,d}}(\rho)$, $\rho_2 = T_{\Gamma_1}(\rho)$. Então para o Lema 1 aplicado a ρ , obtemos

$$H_{sh}(\text{Diag}(\rho)) \leq H_{sh}(\text{Diag}(\rho_2)) + H_{sh}(\text{Diag}(\rho_1))$$

ou equivalentemente

$$H_{medida}(\text{Diag}(|\psi\rangle)) \leq H_{sh}(\text{Diag}(\rho_2)) + H_{sh}(\text{Diag}(\rho)) \quad (\text{B.3})$$

Seja $\rho_{U_1} = U_1 |\psi\rangle \langle \psi| U_1^*$ a matriz densidade do estado $U_1 |\psi\rangle$, $\rho_2^{U_1} = T_{\Gamma_1}(\rho_{v_1})$. Desde que U_1 afete somente o primeiro qudit, $\rho_2^{U_1} = \rho_{v_2}$. Pelo Lema 1

$$H_{sh}(\text{Diag}(\rho_2)) = H_{sh}(\text{Diag}(\rho_2^{U_1})) \leq H_{sh}(\text{Diag}(\rho_{v_1})) \quad (\text{B.4})$$

Por (5) e (6) segue que (4) é correto, consequentemente (3) também é.

Teorema 3. (A monotonicidade de $E_{H_{\min}}$ abaixo da medida ortogonal). *Seja $|\psi\rangle$ um estado de n qudits. O estado $|\psi_j\rangle$ é resultado de alguma medição ortogonal com probabilidades ρ_j . Então*

$$E_{H_{\min}}(|\psi\rangle) \geq \sum_j \rho_j E_{H_{\min}}(|\psi_j\rangle).$$

Prova. Assumiremos sem perder de generalidade que mediremos primeiro o qudit em uma base $\{\psi_i^1\}$ (a medição de mais de um qudit pode ser trocada por uma medição de uma sequência de qudits). Então $|\psi_j\rangle = |\psi_i^1\rangle \otimes |\psi_j^2\rangle$. Seja $|\psi_{\min}\rangle$ um estado que tenha uma entropia de medição mínima sobre a órbita unitária local $|\psi\rangle$, e $|\psi_{\min}\rangle = U_1 \otimes U_2 \otimes \dots \otimes U_n |\psi\rangle$, então

$$\begin{aligned} \sum_j \rho_j E_{H_{\min}}(|\psi_j\rangle) &= \sum_j \rho_j E_{H_{\min}}(|\psi_i^1\rangle \otimes |\psi_j^2\rangle) \leq \sum_j \rho_j H_{medida}(|j\rangle \otimes (U_1 \otimes U_2 \otimes \dots \otimes U_n |\psi_j\rangle)) \\ &\leq \{\text{para o Lema 2}\} \leq H_{medida}(\psi) \end{aligned}$$

Assim, do Teorema 1 chegamos a propriedade 4.

B.0.1 Propriedades complementares

Lema 3. (Lema de Klein) *Seja ρ uma matriz densidade, então*

$$H_{sh}(\text{Diag}(\rho)) \geq H_{vN}(\rho).$$

Teorema 4. $E_{H_{\min}}$ coincide com a entropia de Von Neumann reduzida para o estado bipartites, isto é, seja $|\psi\rangle$ um estado puro bipartite; $\rho = |\psi\rangle \langle \psi|$ é uma matriz densidade, $\rho_A =$

$Tr_B(\rho)$ e $\rho_B = Tr_A(\rho)$ são matrizes densidade reduzidas de subsistemas. Então $E_{H_{\min}}(|\psi\rangle) = H_{vN}(\rho_A) = H_{vN}(\rho_B)$.

Prova. Considere a decomposição de Schmidt de $|\psi\rangle$:

$$|\psi\rangle = \sum \sqrt{\lambda_i} |i_A\rangle \otimes |i_B\rangle.$$

Então

$$E_{H_{\min}}(|\psi\rangle) = \min_{U_A, U_B} H_{medida}(U_A \otimes U_B |\psi\rangle) \leq H_{sh}(\lambda_i) = H_{vN}(\rho_A) = H_{vN}(\rho_B)$$

Pelo Lema 2 tem-se:

$$H_{medida}(|\psi\rangle) = H_{sh}(Diag(\rho)) = H_{sh}(Diag(\rho_A))$$

Pelo lema de Klein tem-se que:

$$H_{sh}(Diag(\rho_A)) \geq H_{vN}(\rho_A) = H_{vN}(\rho_B)$$

Assim, $E_{H_{\min}}(|\psi\rangle) = H_{vN}(\rho_A) = H_{vN}(\rho_B)$.

Propriedade 1. ($E_{H_{\min}}$ da generalização do estado GHZ) Considere a generalização do estado GHZ:

$$|GHZ\rangle = \sum_{i=1}^d a_i |i\rangle_1 \otimes |i\rangle_2 \otimes \dots \otimes |i\rangle_n,$$

em que $a_i \in \mathfrak{R}$, $\sum_{i=1}^d |a_i|^2 = 1$. Então

$$H_{medida}(|GHZ\rangle) = \min_{U_1, \dots, U_n} H_{medida}(U_1, \dots, U_n |GHZ\rangle).$$

Prova. Podemos considerar o espaço do estado GHZ um espaço de estados bipartites do primeiro qudit com os qudits remanescente. Então

$$H_{medida}(|GHZ\rangle) = \sum_{i=1}^d a_i |i\rangle_1 \otimes |i\rangle_2$$

Do Teorema e e da Observação 1 temos que a decomposição de Schmidt tem uma entropia de medição mínima. Disso tem-se,

$$H_{medida}(|GHZ\rangle) = \sum_{i=1}^d a_i |i\rangle_1 \otimes |\tilde{i}\rangle \leq H_{medida}(U_1 \otimes \tilde{U} |GHZ\rangle)$$

Em que U_1 é uma transformação unitária do primeiro qudit e \tilde{U} é uma transformação unitária arbitrária de $1, 2, \dots, n$ qudits. Podemos tomar $U_1 \otimes U_2, \dots, U_n$ como \tilde{U} , então

$$H_{medida}(|GHZ\rangle) \leq H_{medida}(U_1 \otimes U_2, \dots, U_n |GHZ\rangle).$$

Assim, termina a prova. Então temos $E_{H \min}(|GHZ\rangle) = - \sum_{i=1}^d |a_i|^2 \ln |a_i|^2$.

B.1 Propriedades numéricas

As seguintes propriedades foram obtida numericamente por algoritmo genético. Deve-se lembrar que verificação numérica não serve como prova de um resultado ou propriedade, pois o algoritmo calcula apenas resultados particulares que não servem de prova geral. No entanto, serve como evidência para investigações.

Resultado numérico 1. ($E_{H \min}$ do estado W generalizado) Considere o estado W generalizado

$$|W\rangle = a_1 |0 \dots 01\rangle + \dots + a_n |0 \dots 01\rangle,$$

em que $\sum_{i=1}^n |a_i|^2 = 1$. Então,

$$E_{H \min}(W) = H_{medida}(W) = \sum_{i=1}^n |a_i|^2 \ln |a_i|^2.$$

Resultado numérico 2. Sejam

$$\begin{aligned} U^1 &= |\psi\rangle = \sum_{i_1, \dots, i_n=1}^d a_{i_1, \dots, i_n} |i_1, \dots, i_n=1\rangle, \\ &|\phi\rangle = \sum_{i_1, \dots, i_n=1}^d b_{i_1, \dots, i_n} |i_1, \dots, i_n=1\rangle, \end{aligned}$$

e $H_{medida}(|\psi\rangle) = H_{medida}(|\phi\rangle) = E_{H \min}(|\psi\rangle) = E_{H \min}(|\phi\rangle)$ (em outras palavras $|\psi\rangle$ e $|\phi\rangle$ têm a mesma $E_{H \min}$ e eles têm a mesma representação de entropia mínima), então,

$$|a_{i_1, \dots, i_n}|^2 = |b_{i_1, \dots, i_n}|^2$$

dentro de permutações locais dos vetores da base, isto é, o quadrado do módulo de uma representação de entropia mínima é única.

B.1.1 E_{sh} é consideravelmente uma medida de entrelaçamento multipartite

Computações numéricas usando algoritmo genético mostram que os dois estados quânticos bipartites de três qubits como $|\phi\rangle$ e $|\psi\rangle$ podem ter diferente E_{Hmin} . Isso significa que E_{Hmin} é consideravelmente multipartite uma medida de entrelaçamento de estados multipartites. A equivalência com o entrelaçamento bipartite mostra que

$$\begin{aligned} &\exists U_1^1, U_{23}^1, U_1^2, U_{13}^2, U_3^3, U_{12}^3 \text{ tal que} \\ &|\phi\rangle = U_1^1 \otimes U_{23}^1 |\psi\rangle, \\ &|\phi\rangle = U_2^2 \otimes U_{23}^2 |\psi\rangle, \\ &|\phi\rangle = U_3^3 \otimes U_{12}^3 |\psi\rangle, \end{aligned}$$

em que U_i^k é evolução unitária do i -ésimo qubit, e U_{ij}^k é evolução unitária (pode ser entrelaçado) dos i -ésimo e j -ésimo qubits. De $E_{Hmin}(|\psi\rangle) \neq E_{Hmin}(|\phi\rangle)$, temos que $|\phi\rangle$ e $|\psi\rangle$ não são equivalentes sob transformações locais unitárias, isto é,

$$\nexists U_1, U_2, U_3 : |\psi\rangle = U_1 \otimes U_2 \otimes U_3 |\phi\rangle$$

Esta propriedade de E_{Hmin} fornece uma resposta para o problema de equivalência de bipartites com multipartites. O entrelaçamento bipartite e multipartite não são equivalentes. Isso também significa que as medidas de entrelaçamento baseado somente nos coeficientes de Schmidt de diferentes decomposições de um estado não são boas para quantificar o entrelaçamento multipartite.

Referências Bibliográficas

- [1] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, May 1992.
- [2] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. *Advances in Cryptology: Proceedings of Crypto 84*, pages 475 – 480, August 1984.
- [3] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, Mar 2002.
- [4] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.
- [5] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(6):062314, Nov 2000.
- [6] Aikaterini Mandilara, Vladimir M. Akulin, Andrei V. Smilga, and Lorenza Viola. Quantum entanglement via nilpotent polynomials. *Phys. Rev. A*, 74(2):022331, Aug 2006.
- [7] M. B. Plenio. Logarithmic Negativity: A Full Entanglement Monotone That is not Convex. *Physical Review Letters*, 95(9):090503–+, August 2005.
- [8] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65(3):032314, Feb 2002.
- [9] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865–942, Jun 2009.
- [10] Alexander Wong and Nelson Christensen. Potential multiparticle entanglement measure. *Phys. Rev. A*, 63(4):044301, Mar 2001.

- [11] G. K. Brennen. An observable measure of entanglement for pure states of multi-qubit systems. *ArXiv Quantum Physics e-prints*, May 2003.
- [12] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57(3):1619–1633, Mar 1998.
- [13] M. B. Plenio and S. Virmani. An introduction to entanglement measures. *ArXiv Quantum Physics e-prints*, April 2005.
- [14] D. Bouwmeester and A. Zeilinger. The physics of quantum information: basic concepts. *The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation*, pages 1–14, 2000.
- [15] Wayne M. Itano, D. J. Heinzen, J. J. Bollinger, and D. J. Wineland. Quantum zeno effect. *Phys. Rev. A*, 41(5):2295–2300, Mar 1990.
- [16] Mark Byrd. Differential geometry on $su(3)$ with applications to three state systems. *Journal of Mathematical Physics*, 39:6125–6136, 1998.
- [17] T. Tilma and E. C. G. Sudarshan. Generalized Euler angle parametrization for $SU(N)$. *Journal of Physics A Mathematical General*, 35:10467–10501, December 2002.
- [18] Matthew Neeley, Markus Ansmann, Radoslaw C. Bialczak, Max Hofheinz, Erik Lucero, Aaron D. O’Connell, Daniel Sank, Haohua Wang, James Wenner, Andrew N. Cleland, Michael R. Geller, and John M. Martinis. Emulation of a Quantum Spin with a Superconducting Phase Qudit. *Science*, 325(5941):722–725, 2009.
- [19] Jurgen Audretsch. *Entangled Systems: New Directions in Quantum Physics*. WILEY-VCH, 2007.
- [20] A. Y. Chernyavskiy. Entanglement measure for multipartite pure states and its numerical calculation. *ArXiv e-prints*, May 2009.
- [21] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.
- [22] Rubens Viana Ramos and Rui Fragassi Souza. Calculation of the quantum entanglement measure of bipartite states, based on relative entropy, using genetic algorithms. *J. Comput. Phys.*, 175(2):576–583, 2002.

Trabalhos Publicados Pelo Autor

1. José Cláudio do Nascimento, Werther Xisto da Silva Cardoso. “Cálculo numérico da medida de entrelaçamento para estados puros multipartes de três níveis”. *III Workshop-Escola de Computação e Informação Quântica (WECIQ 2010)*, Laboratório Nacional de Computação Científica - Petrópolis, Rio de Janeiro, Brasil, Outubro de 2010.