Emaranhamento em sistemas de dois qubits

Bárbara Lopes Amaral

Fevereiro de 2010

Emaranhamento em sistemas de dois qubits

Bárbara Lopes Amaral

Orientador:
Dr. Marcelo Terra Cunha

Dissertação apresentada à UNIVERSIDADE FEDERAL DE MINAS GERAIS, como requisito parcial para a obtenção do grau de MESTRE EM MATEMÁTICA.

Belo Horizonte, Brasil
Fevereiro de 2010

A meus queridos pais, Ângela e Geraldo,
por nunca me deixarem caminhar sozinha.

Conteúdo

Introdução

Nesse trabalho demonstramos uma série de resultados para sistemas quânticos de dimensão finita. O tema central são os qubits, sistema que se tornou muito importante com o surgimento da computação quântica.

O principal objetivo é estudar dois quantificadores de emaranhamento para o sistema de dois qubits, chamados Negatividade e Concorrência. O emaranhamento é uma propriedade muito interessante de sistemas quânticos compostos, que não aparece em mecânica clássica. Ele está por trás de vários resultados surpreendentes como a teleportação de estados quânticos e o algoritmo de Shor, capaz de fatorar números inteiros em tempo polinomial, entre vários outros. Ainda não se sabe precisamente, mas acredita-se que os sitemas quânticos permitem realizar computação de maneira mais eficiente que os sistemas clássicos e a presença de emaranhamento pode ser um recurso valioso.

A motivação inicial para esse trabalho foi o artigo [1], que faz uma comparação entre a Negatividade e a Concorrência. Essa comparação é o último resultado apresentado na dissertação, no fim do capítulo 4. A demonstração é simples, uma vez conhecidas algumas propriedades desses quantificadores e dos estados de dois qubits.

Por esse motivo, dedicamos o capítulo 3 a um estudo detalhado dos sistemas de um e dois qubits. Em especial, estudamos o efeito das chamadas operações SLOCC (Stochastic Local Operations and Classical Comunication) sobre os estados de dois qubits. Como uma consequência desse resultado obtemos a propriedade necessária para comparar negatividade e concorrência: a transposta parcial de uma matriz densidade de dois qubits possui no máximo um autovalor negativo. Esse é um resultado bem conhecido e utilizado.

Antes de comparar negatividade e concorrência devemos entender porque eles são de fato bons quantificadores de emaranhamento. Apresentamos no capítulo 4 em detalhe as demonstrações, que são baseadas nos trabalhos [2, 3]. Citamos também alguns outros quantificadores importantes, como o Emaranhamento de Formação, que está intimamente relacionado à Concorrência, o Emaranhamento Destilável, Robustez, entre outros.

No capítulo 2, enunciamos os postulados da mecânica quântica. Eles nos dizem que objetos matemáticos representam o espaço de estados de um sistema quântico e as grandezas físicas relacionadas. Veremos que os espaços de Hilbert e os operadores agindo neles serão nossa ferramenta principal. Veremos também como se dá a evolução de um estado, o que nos leva à definição de mapas completamente positivos. Por último, estudamos como encontrar o espaço de estados de um sistema composto a partir dos espaços de estados dos subsistemas. Essa construção faz uso do produto tensorial de espaços vetoriais e é dessa estrutura tensorial que surge o conceito de emaranhamento.

Por trás dos resultados que apresentamos nesse trabalho, está uma matemática rica e bem diversificada. O Capítulo 1 é destinado a introduzir os conceitos e resultados de que

precisaremos adiante.

CAPÍTULO 1

Preliminares

Nesse capítulo vamos apresentar os principais resultados que usaremos ao longo do texto. A intenção aqui é apenas enunciar os resultados e fixar a notação. A primeira seção trata de espaços vetoriais, que são os objetos principais para a mecânica quântica [4, 5, 6, 7, 8]. O objetivo maior dessa seção é apresentar a notação de Dirac, muito usada pelos físicos, mas pouco conhecida pelos matemáticos. A segunda seção trata dos grupos de Lie [9, 10], e os resultados mais importantes são o homomorfismo entre $SL(2,\mathbb{C})$ e o grupo de Lorentz e o isomorfismo entre $SL(2,\mathbb{C}) \otimes SL(2,\mathbb{C})$ e $SO(4,\mathbb{C})$, que serão utilizados para estudarmos a ação de alguns mapas quânticos sobre estados de dois qubits e obter resultados importantes. Por último, estudamos os conjuntos convexos e distribuições de probabilidade discretas [11]. O principal resultado é o teorema HLP, que depois será apresentado em sua versão quântica e que é usado para obtermos condições de convertibilidade de estados por operações locais e comunicação clássica.

1.1 Espaços vetoriais

Nessa seção veremos alguns conceitos básicos sobre espaços vetoriais. Os resultados que apresentaremos e muitos outros podem ser encontrados em [7, 8, 12, 13], sendo que a última referência utiliza também a notação de Dirac.

Um espaço vetorial sobre um corpo $\mathbb{K}$ é um conjunto $\mathcal{V}$ no qual estão definidas a soma entre dois elementos de $\mathcal{V}$ e o produto por elementos de $\mathbb{K}$. Um elemento de $\mathcal{V}$ será denotado por um *ket*:

$$|u\rangle \in \mathcal{V}.$$

As seguintes propriedades devem ser satisfeitas

1. (Associatividade da soma) $(|u\rangle + |v\rangle) + |w\rangle = |u\rangle + (|v\rangle + |w\rangle)$ para $|u\rangle, |v\rangle$ e $|w\rangle$ elementos de $\mathcal{V}$;

2. (Elemento neutro para a soma) Há um elemento $0 \in \mathcal{V}$, tal que, para cada $|v\rangle \in \mathcal{V}$, $|v\rangle + 0 = 0 + |v\rangle = |v\rangle$;

3. (Elemento oposto) Para cada $|v\rangle \in \mathcal{V}$, existe $|u\rangle \in \mathcal{V}$ tal que $|v\rangle + |u\rangle = 0$;

4. (Comutatividade da soma) Para cada $|v\rangle\,,\ |u\rangle \in \mathcal{V},\ |u\rangle + |v\rangle = |v\rangle + |u\rangle$;
5. (Associatividade do produto) Para cada $a,\ b \in \mathbb{K}$ e cada $|v\rangle \in \mathcal{V},\ a.(b.|v\rangle) = (a.b).|v\rangle$;
6. (Elemento neutro para o produto) Se 1 é a unidade de $\mathbb{K}$, então, para cada $|v\rangle \in \mathcal{V},\ 1.|v\rangle = |v\rangle$;
7. (Distributividade) Para cada $a \in \mathbb{K}$ e cada $|v\rangle\,, |u\rangle \in \mathcal{V},\ a.(|v\rangle + |u\rangle) = a.|v\rangle + a.|u\rangle$;
8. (Distributividade) Para cada $a, b \in \mathbb{K}$ e cada $|v\rangle \in \mathcal{V},\ (a+b).|v\rangle = a.|v\rangle + b.|v\rangle$.

Nos preocuparemos apenas com os casos $\mathbb{K} = \mathbb{R}$ e $\mathbb{K} = \mathbb{C}$.

Definição 1. *Um conjunto de vetores $\{|v_1\rangle\,, \ldots |v_n\rangle\}$ é dito linearmente dependente se algum dos $|v_i\rangle$ pode ser escrito como combinação linear dos demais, isto é, existem coeficientes c_j, $j \neq i$, tais que:*

$$|v_i\rangle = c_1\,|v_1\rangle + \ldots + c_{i-1}\,|v_{i-1}\rangle + c_{i+1}\,|v_{i+1}\rangle + \ldots + |v_n\rangle\,.$$

Caso contrários, os vetores são chamados linearmente independentes. Uma base para o espaço vetorial $\mathcal{V}$ é um conjunto linearmente independente $\{|v_1\rangle\,, \ldots, |v_n\rangle\}$que gera o espaço todo, isto é, tal que todo vetor de $\mathcal{V}$ possa ser escrito como combinação linear dos $|v_i\rangle$. Toda base tem o mesmo número de vetores, que é chamado de dimensão de $\mathcal{V}$.

Consideraremos aqui apenas espaços vetoriais de dimensão finita.

Definição 2. *Um funcional linear em $\mathcal{V}$ é uma aplicação linear de $\mathcal{V}$ em $\mathbb{K}$. Os funcionais lineares serão denotados por um* bra*:*

$$\langle\chi| : \mathcal{V} \longrightarrow \mathbb{K}.$$

O conjunto de todos os funcionais lineares em $\mathcal{V}$ também forma um espaço vetorial sobre $\mathbb{K}$, que é chamado espaço dual de $\mathcal{V}$ e é denotado por $\mathcal{V}^*$.

Dados dois espaços vetoriais sobre o mesmo corpo, $\mathcal{V}$ e $\mathcal{U}$, o conjunto de todas as transformações lineares $T : \mathcal{V} \to \mathcal{U}$ será denotado por $\mathcal{L}(\mathcal{V},\mathcal{U})$. Em especial, chamamos as transformações lineares $O : \mathcal{V} \to \mathcal{V}$ de operadores e denotamos $\mathcal{L}(\mathcal{V}) = \mathcal{L}(\mathcal{V},\mathcal{V})$. O conjunto $\mathcal{L}(\mathcal{V},\mathcal{U})$ também é um espaço vetorial sobre $\mathbb{K}$ e $\mathcal{L}(\mathcal{V},\mathbb{K}) = \mathcal{V}^*$.

Suponhamos que $\mathcal{V}$ tenha dimensão finita e que $\dim \mathcal{V} = n$. Fixada uma base, todo operador linear em $\mathcal{L}(\mathcal{V})$ pode ser representado por uma matriz $n \times n$. O conjunto de todas essas matrizes será denotado por $M(\mathcal{V})$.

Definição 3. *Dizemos que um vetor $|v\rangle \neq 0$ é um autovetor de um operador $O \in \mathcal{L}(\mathcal{V})$ com autovalor λ se*

$$O\,|v\rangle = \lambda\,|v\rangle\,.$$

Definição 4. *Um produto interno em $\mathcal{V}$ é uma função $(\cdot,\cdot) : \mathcal{V} \times \mathcal{V} \longrightarrow \mathbb{K}$ que satisfaz*

1. $(|u\rangle\,, |v\rangle) = (|v\rangle\,, |u\rangle)^*$*, em que $*$ denota conjugação complexa;*
2. $(|u\rangle + |v\rangle\,, |w\rangle) = (|u\rangle\,, |w\rangle) + (|v\rangle\,, |w\rangle)$*;*

3. $(|u\rangle, a\,|v\rangle) = a(|u\rangle, |v\rangle),\ a \in \mathbb{K}$;

4. *Para todo* $|u\rangle \neq 0$ *vale* $(|u\rangle, |u\rangle) \in \mathbb{R}$ *e* $(|u\rangle, |u\rangle) > 0$.

Fixado um vetor $|v\rangle$ a função

$$\phi_v : \mathcal{V} \longrightarrow \mathbb{K}$$
$$|u\rangle \longmapsto (|v\rangle, |u\rangle)$$

é um funcional linear, que denotaremos por $\langle v|$. Assim usaremos a notação

$$(|v\rangle, |u\rangle) = \langle v \mid u\rangle .$$

Vale a propriedade $\phi_{v+u} = \langle v| + \langle u|$.

Um vetor é chamado unitário se $\langle v \mid v\rangle = 1$. A projeção de um vetor $|u\rangle$ na direção de um vetor unitário $|v\rangle$ é o vetor $\langle u \mid v\rangle\,|v\rangle$. Dois vetores são chamados ortogonais se o produto interno entre eles é igual a zero. Um conjunto de vetores é chamado ortonormal se os vetores são unitários e ortogonais entre si.

Dados dois vetores $|u\rangle, |v\rangle \in \mathcal{V}$ podemos definir um operador $O : \mathcal{V} \to \mathcal{V}$ da seguinte forma:

$$O\,|w\rangle = |u\rangle\,\langle v \mid w\rangle .$$

Esse operador será denotado por $|u\rangle\,\langle v|$. Em particular, dado um vetor unitário $|v\rangle$, o operador $|v\rangle\,\langle v|$ leva cada vetor $|u\rangle$ em sua projeção na direção de $|v\rangle$ e por isso é chamado de projetor na direção de $|v\rangle$.

Dado um operador $O : \mathcal{V} \to \mathcal{V}$ definimos o operador conjugado hermitiano de O como sendo o operador $O^\dagger : \mathcal{V} \to \mathcal{V}$ tal que

$$(|v\rangle, O\,|u\rangle) = (O^\dagger\,|v\rangle, |u\rangle).$$

Dizemos que um operador é hermitiano ou autoadjunto se $O = O^\dagger$. Os autovalores de um operador hermitiano são todos reais, e autovetores com autovalores distintos são ortogonais.

Se um operador O é hermitiano, então $(|v\rangle, O\,|u\rangle) = (O\,|v\rangle, |u\rangle)$. Nos aproveitamos desse fato para usar a notação

$$(|v\rangle, O\,|u\rangle) = \langle v|\,O\,|v\rangle .$$

Fixada uma base ortonormal, se o operador O é representado pela matriz M, então $O^\dagger$ é representado pela matriz $M^\dagger = (M^T)^*$, em que $*$ representa conjugação complexa e T representa a transposição. Uma matriz é dita hermitiana se $M^\dagger = M$.

Um resultado importante para operadores hermitianos é o teorema espectral.

Teorema 1 (Teorema Espectral)**.** *Seja $O : \mathcal{V} \to \mathcal{V}$ um operador hermitiano sobre um espaço vetorial $\mathcal{V}$ real ou complexo de dimensão finita. Então existe uma base ortonormal para $\mathcal{V}$ formada por autovetores de O.*

Teorema 2 (Decomposição Espectral)**.** *Seja M uma matriz hermitiana e $\{|v_i\rangle\}$ uma base formada por autovetores de M, com autovalores reais correspondentes λ_i. Então*

$$M = \sum_i \lambda_i\,|v_i\rangle\,\langle v_i| .$$

Outro resultado importante é a decomposição em valor singular

Teorema 3. *Dada uma matriz M, existem matrizes unitárias U e V e uma matriz diagonal Σ com entradas não-negativas tais que*

$$UMV = \Sigma.$$

Os elementos da diagonal de Σ são chamados valores singulares de M.

Um operador O é chamado positivo definido se

$$\langle v| O |v\rangle > 0 \quad \forall \quad |v\rangle \neq 0 \in \mathcal{V}$$

e positivo semi-definido se

$$\langle v| O |v\rangle \geq 0 \quad \forall \quad |v\rangle \neq 0 \in \mathcal{V}.$$

Todo operador positivo definido é um operador hermitiano tal que todos os autovalores são positivos e um operador positivo semi-definido é um operador hermitiano tal que todos os autovalores são não-negativos.

Definição 5. *Uma norma em $\mathcal{V}$ é uma função $\|\cdot\| : \mathcal{V} \to \mathbb{R}$ que satisfaz*

1. $\||u\rangle\| = 0 \Leftrightarrow |u\rangle = 0$;
2. $\|\lambda |u\rangle\| = |\lambda| \, \||u\rangle\|, \lambda \in \mathbb{K}$;
3. *(Desigualdade triangular)* $\||u\rangle + |v\rangle\| \leq \||u\rangle\| + \||v\rangle\|$.

Quando podemos definir uma norma em $\mathcal{V}$ dizemos que $\mathcal{V}$ é um espaço vetorial normado.

Dado um produto interno, a função $|v\rangle \mapsto \langle v \mid v\rangle^{1/2}$ é uma norma em $|v\rangle$. Esse fato é uma consequência da desigualdade de Cauchy-Schwartz:

$$\| \langle u \mid v\rangle \|^2 \leq \langle u \mid u\rangle \langle v \mid v\rangle .$$

Logo todo espaço com produto interno é também um espaço normado.

Toda norma, por sua vez, gera uma distância em $\mathcal{V}$.

Definição 6. *Uma distância em $\mathcal{V}$ é uma função $D : \mathcal{V} \times \mathcal{V} \to \mathbb{R}$ que obedece às seguintes condições:*

1. $D(|u\rangle, |v\rangle) \geq 0$ *e* $D(|u\rangle, |v\rangle) = 0 \Leftrightarrow |u\rangle = |v\rangle$;
2. $D(|u\rangle, |v\rangle) = D(|v\rangle, |u\rangle)$;
3. *(Desigualdade triangular)* $D(|v\rangle, |u\rangle) \leq D(|u\rangle, |w\rangle) + D(|w\rangle, |v\rangle)$.

Quando podemos definir uma distância em $\mathcal{V}$ dizemos que $\mathcal{V}$ é um espaço métrico.

Dada uma norma $\|\cdot\|$, a função $|u\rangle, |v\rangle \mapsto \||u\rangle - |v\rangle\|$ define uma distância em $\mathcal{V}$. Logo todo espaço normado é também um espaço métrico.

Dada uma distância D em $\mathcal{V}$, dizemos que a sequência $(|u_n\rangle)$ é convergente, e que converge para o valor $|v\rangle \in \mathcal{V}$, se $\lim_{n\to\infty} |u_n\rangle = |v\rangle$. Isso quer dizer que:

$$\forall \quad \epsilon > 0 \quad \exists \quad n_0 \in \mathbb{N} \ : \ n > n_0 \Rightarrow D(|u_n\rangle, |v\rangle) < \epsilon.$$

Uma sequência em $\mathcal{V}$ é chamada de *sequência de Cauchy* se

$$\forall \quad \epsilon > 0 \quad \exists \quad n_0 \in \mathbb{N} \ : \ m, n > n_0 \Rightarrow D(|u_m\rangle, |u_n\rangle) < \epsilon.$$

Não é difícil mostrar que toda sequência convergente em $\mathcal{V}$ é uma sequência de Cauchy. No entanto, nem sempre uma sequência de Cauchy é convergente. Se toda seqüência de Cauchy em $\mathcal{V}$ é uma sequência convergente, dizemos que $\mathcal{V}$ é um *espaço métrico completo.*

Definição 7. *Dizemos que um espaço vetorial $\mathcal{V}$ é um espaço de Hilbert se é um espaço vetorial com produto interno, completo com a norma gerada por ele.*

Espaços de Hilbert serão denotados por $\mathcal{H}$. Podemos caracterizar os espaços duais de espaços de Hilbert usando o

Teorema 4 (Representação de Riez)**.** *Seja $\mathcal{H}$ um espaço de Hilbert. Dado $\langle\chi| \in \mathcal{H}^*$ existe um único $|v\rangle \in \mathcal{H}$ tal que*

$$\langle\chi| = \langle v|,$$

ou seja, todo funcional linear é dado por produto interno com um vetor fixo.

Podemos caracterizar os autovalores máximo e mínimo de um operador hermitiano em espaços de Hilbert de dimensão finita[1] utilizando o produto interno.

Teorema 5. *Seja $\mathcal{H}$ um espaço de Hilbert e O um operador hermitiano em $\mathcal{H}$. Sejam λ_O e Λ_O o menor e o maior autovalor de O. Então temos*

$$\lambda_O = \inf_{\langle v|v\rangle=1} \langle v| O |v\rangle, \qquad \Lambda_O = \sup_{\langle v|v\rangle=1} \langle v| O |v\rangle.$$

Corolário 1. *Se $M = M_1 + M_2$ então*

$$\lambda_M \geq \lambda_{M_1} + \lambda_{M_2}, \quad \Lambda_M \leq \Lambda_{M_1} + \Lambda_{M_2}.$$

Para demonstração dos resultados a respeito de espaços de Hilbert, veja [4].

Nossa preocupação é com espaços de Hilbert de dimensão finita. Se $\dim \mathcal{H} = N$, denotaremos por

$$\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$$

uma base ortonormal para $\mathcal{H}$, isto é, uma base tal que

$$\langle i \mid j\rangle = \delta_{ij}, \quad i, j = 0, 1, \ldots, N-1.$$

[1] O resultado é válido também para os chamados operadores compactos em espaço de dimensão infinita.

1.1.1 Produto tensorial

Dados dois espaços vetoriais $\mathcal{V}_A$ e $\mathcal{V}_B$ de dimensões n_A e n_B respectivamente, podemos construir um espaço vetorial de dimensão $n_A n_B$ através do produto tensorial [8, 14, 13]. Para construirmos[2] esse novo espaço, que denotaremos por $\mathcal{V}_A \otimes \mathcal{V}_B$, tomamos bases $|i_A\rangle$ para $\mathcal{V}_A$ e $|j_B\rangle$ para $\mathcal{V}_B$ e declaramos que os $n_A n_B$ elementos da forma

$$|i_A\rangle \otimes |j_B\rangle\,, \quad i_A = 0, 1, \ldots, n_A,\ j_B = 0, 1, \ldots, n_B$$

formam uma base para $\mathcal{V}_A \otimes \mathcal{V}_B$. As seguintes condições são impostas

1. Para um escalar arbitrário $a \in \mathbb{K}$ e elementos $|v_A\rangle$ de $\mathcal{V}_A$ e $|v_B\rangle$ de $\mathcal{V}_B$,

$$a(|v_A\rangle \otimes |v_B\rangle) = (a\,|v_A\rangle) \otimes |v_B\rangle = |v_A\rangle \otimes (a\,|v_B\rangle);$$

2. Para $|v_A\rangle$ e $|u_A\rangle$ arbitrários em $\mathcal{V}_A$ e $|v_B\rangle$ em $\mathcal{V}_B$,

$$(|v_A\rangle + |u_A\rangle) \otimes |v_B\rangle = |v_A\rangle \otimes |v_B\rangle + |u_A\rangle \otimes |v_B\rangle\,;$$

3. Para $|v_A\rangle$ arbitrário em $\mathcal{V}$ e $|u_B\rangle$ e $|v_B\rangle$ em $\mathcal{V}_B$,

$$|v_A\rangle \otimes (|u_B\rangle + |v_B\rangle) = |v_A\rangle \otimes |u_B\rangle + |v_A\rangle \otimes |v_B\rangle\,.$$

A construção é independente das escolhas de base para $\mathcal{V}_A$ e $\mathcal{V}_B$.

Definição 8. *Dizemos que um vetor $|v\rangle \in \mathcal{V}_A \otimes \mathcal{V}_B$ é decomponível se é da forma $|v_A\rangle \otimes |v_B\rangle$.*

É comum usarmos a notação $|v_A\rangle \otimes |v_B\rangle = |v_A v_B\rangle$.

Se $\mathcal{V}_A$ e $\mathcal{V}_B$ são espaços vetoriais com produto interno, podemos definir um produto interno em $\mathcal{V}_A \otimes \mathcal{V}_B$ da seguinte maneira: para vetores decomponíveis fazemos

$$\langle v_A v_B \mid u_A u_B\rangle = \langle v_A \mid u_A\rangle \langle v_B \mid u_B\rangle\,,$$

e em seguida estendemos aos outros vetores:

$$(\langle v_A v_B| + \langle w_A w_B|)\,|u_A u_B\rangle = \langle v_A v_B \mid u_A u_B\rangle + \langle w_A w_B \mid u_A u_B\rangle$$

$$\langle v_A v_B|\,(|w_A w_B\rangle + |u_A u_B\rangle) = \langle v_A v_B \mid w_A w_B\rangle + \langle v_A v_B \mid u_A u_B\rangle\,.$$

Teorema 6. *Se $\mathcal{V}_A$ e $\mathcal{V}_B$ são espaços de Hilbert, $\mathcal{V}_A \otimes \mathcal{V}_B$ também é.*

Os conjuntos $M(\mathcal{V}_A)$ e $M(\mathcal{V}_B)$ são também espaços vetorias sobre $\mathbb{K}$ e por isso também podemos definir o produto tensorial $M(\mathcal{V}_A) \otimes M(\mathcal{V}_B)$. Podemos então definir uma ação de $M(\mathcal{V}_A) \otimes M(\mathcal{V}_B)$ em $\mathcal{V}_A \otimes \mathcal{V}_B$ da seguinte forma: para vetores decomponíveis fazemos

$$M_A \otimes M_B(|v_A\rangle \otimes |v_B\rangle) = M_A\,|v_A\rangle \otimes M_B\,|v_B\rangle\,,$$

e em seguida estendemos por linearidade aos outros vetores. Essa ação define um mapa de $M(\mathcal{V}_A) \otimes M(\mathcal{V}_B)$ em $M(\mathcal{V}_A \otimes \mathcal{V}_B)$, que é um isomorfismo de espaços vetoriais.

[2] Para uma definição mais precisa, veja [8, 14].

Definição 9. *Definimos o traço parcial em relação a $\mathcal{V}_A$ de uma matriz $M_A \otimes M_B$ em $M(\mathcal{V}_A) \otimes M(\mathcal{V}_B)$ por*

$$Tr_A(M_A \otimes M_B) = Tr(M_A)M_B,$$

e estendemos por linearidade às matrizes não decomponíveis. De maneira análoga definimos o traço parcial em relação a $\mathcal{V}_B$.

Definição 10. *Definimos a transposta parcial em relação a $\mathcal{V}_A$ de uma matriz $M_A \otimes M_B$ em $M(\mathcal{V}_A) \otimes M(\mathcal{V}_B)$ por*

$$(M_A \otimes M_B)^{T_A} = (M_A)^T \otimes M_B,$$

e estendemos por linearidade às matrizes não decomponíveis. De maneira análoga definimos a transposta parcial em relação a $\mathcal{V}_B$.

Proposição 1. *Se uma matriz M é positiva, então $Tr_A(M)$ e $Tr_B(M)$ também o são.*

Demonstração. Suponhamos que $M = \sum_i M_A^i \otimes M_B^i$. Seja $\{|j\rangle\}, j = 1, \ldots, \dim \mathcal{V}_B$ uma base ortonormal para $\mathcal{V}_B$. Então

$$Tr_B(M) = \sum_{i,j} M_A^i \langle j| M_B^i |j\rangle$$

$$\langle v| Tr_B(M) |v\rangle = \sum_{i,j} \langle v| M_A^i |v\rangle \langle j| M_B^i |j\rangle = \sum_{i,j} \langle v| \langle j| M_A^i \otimes M_B^i |j\rangle |v\rangle =$$

$$\sum_j \langle v| \langle j| \sum_i M_A^i \otimes M_B^i |j\rangle |v\rangle = \sum_j \langle v| \langle j| M |j\rangle |v\rangle \geq 0$$

sendo que a última desiguladade é válida pelo fato de que M é positiva e portanto cada termo na última soma é positivo. Segue então que $Tr_B(M)$ também é uma matriz positiva.

De maneira análoga provamos que $Tr_A(M)$ é positiva. □

Um resultado extremamente útil é a decomposição de Schmidt para espaços vetorias com estrutura de produto tensorial.

Proposição 2 (Decomposição de Schmidt)**.** *Dado um vetor $|\Psi\rangle \in \mathcal{V}_A \otimes \mathcal{V}_B$, é possível encontrar bases ortonormais $\{|\psi_A^n\rangle\}$ para $\mathcal{V}_A$ e $\{|\phi_B^m\rangle\}$ para $\mathcal{V}_B$ tais que*

$$|\Psi\rangle = \sum_{i=1}^{d} \alpha_i |\psi_A^i\rangle |\phi_B^i\rangle,$$

em que $d = \min(\dim \mathcal{V}_A, \dim \mathcal{V}_B)$, e $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_d$. Os coeficientes α_i são chamados coeficientes de Schmidt.

Demonstração. Suponhamos $d = \dim \mathcal{V}_A$. Seja $\rho_A = Tr_B(|\Psi\rangle \langle\Psi|)$. A matriz $|\Psi\rangle \langle\Psi|$ é o projetor na direção de $|\Psi\rangle$ e portanto é uma matriz positiva. Assim, ρ_A também é uma matriz positiva, e portanto seus autovetores $|\psi_A^n\rangle$ formam uma base para $\mathcal{V}_A$. Desse modo, dada uma base ortonormal qualquer $|m_B\rangle$ para $\mathcal{V}_B$, podemos escrever

$$|\Psi\rangle = \sum_{n,m} c_{nm} |\psi_A^n\rangle |m_B\rangle,$$

uma vez que o conjunto $\{|\psi_A^n\rangle |m_B\rangle\}$ forma uma base para $\mathcal{V}_A \otimes \mathcal{V}_B$. Seja α_n^2 o autovalor de ρ_A associado ao autovetor $|\psi_A^n\rangle$. Definimos então

$$|\phi_B^n\rangle = \sum_m \frac{c_{nm}}{\alpha_n} |m_B\rangle ,$$

de modo que

$$|\Psi\rangle = \sum_{i=1}^{d} \alpha_i \left|\psi_A^i\right\rangle \left|\phi_B^i\right\rangle ,$$

Resta mostrar que o conjunto $\{|\phi_B^m\rangle\}$ pode ser estendido a uma base ortonormal. Para isso, devemos verificar que esse é um conjunto ortonormal. De fato

$$\langle \phi_B^n \mid \phi_B^m \rangle = \sum k, l \frac{c_{nk}^* c_{ml}}{\alpha_n \alpha_m} \langle k_B \mid l_B \rangle$$

$$= \sum_k \frac{c_{nk}^* c_{mk}}{\alpha_n \alpha_m} = \frac{1}{\alpha_n \alpha_m} \sum_k \langle \Psi| \, |\psi_A^n\rangle \, |k_B\rangle \, \langle \psi_A^m| \, \langle k_B| \, |\Psi\rangle$$

$$= \frac{1}{\alpha_n \alpha_m} \sum_k \langle \psi_A^m| \, \rho_A \, |\psi_A^n\rangle = \frac{\alpha_n \alpha_m \delta_{nm}}{\alpha_n \alpha_m} = \delta_{nm}.$$

O ordenamento não-crescente dos coeficientes pode ser feito reordenando os vetores da base. □

Os coeficientes de Schmidt são os autovalores das matrizes densidade reduzidas $\rho_A = Tr_B(|\Psi\rangle \langle\Psi|)$ e $\rho_B = Tr_A(|\Psi\rangle \langle\Psi|)$. Por esse motivo o número de coeficientes não nulos (chamado número de Schmidt) e também os seus valores são os mesmos para toda decomposição. Além disso, se

$$|\Psi\rangle = \sum_i a_i \, |i\rangle_A \, |i\rangle_B ,$$

$$|\Psi\rangle = \sum_i a_i \left|i'\right\rangle_A \left|i'\right\rangle_B$$

são duas decomposições distintas, as aplicações lineares U_A e U_B definidas nas bases por

$$|i\rangle_A \mapsto \left|i'\right\rangle_A , \qquad |i\rangle_B \mapsto \left|i'\right\rangle_B$$

são aplicações unitárias tais que

$$U_A \otimes U_B(|\Psi\rangle) = |\Psi\rangle .$$

Desse modo, duas decomposições de Schmidt distintas estão relacionadas por unitárias locais que fixam $|\Psi\rangle$.

Para mais detalhes sobre a decomposição de Schmidt ver [13, 15].

1.2 Grupos de Lie

Nessa seção veremos os grupos de Lie e alguns resultados relevantes que utilizaremos no capítulo 3. Como referências sugerimos [9, 10]. Vamos utilizar aqui alguns resultados bem conhecidos, mas não triviais de topologia [16].

Definição 11. *Um grupo de Lie sobre um corpo $\mathbb{K} = \mathbb{R}, \mathbb{C}$ é um grupo G munido de uma estrutura de variedade diferenciável sobre $\mathbb{K}$ tal que o mapa*

$$\begin{aligned} \mu : G \times G &\longrightarrow G \\ (x, y) &\longmapsto xy \end{aligned}$$

é diferenciável.

Teorema 7. *Dado $p \in G$, o mapa*

$$\begin{aligned} \mu_p : G &\longrightarrow G \\ x &\longmapsto px \end{aligned}$$

é um difeomorfismo de variedades de G em G.

Proposição 3. *O mapa*

$$\begin{aligned} \nu : G &\longrightarrow G \\ x &\longmapsto x^{-1} \end{aligned}$$

é um difeomorfismo de variedades de G em G.

Demonstração. Dado $x \in G$, o inverso $\nu(x) = x^{-1}$ é definido pela equação

$$\mu(x, \nu(x)) = e.$$

A derivada parcial de μ em relação à segunda variável é a derivada de μ_x, que é um isomorfismo, já que μ_x é um difeomorfismo. Desse modo, podemos utilizar o teorema da aplicação implícita para concluir que ν é uma função diferenciável. Como sua inversa é ela própria, ν é um difeomorfismo. □

Exemplos:

1. O grupo aditivo $\mathbb{K}$.
2. O grupo multiplicativo $\mathbb{K}^*$.
3. O grupo $GL(n, \mathbb{K})$ de matrizes invertíveis $n \times n$. Identificando $M(n)$, o conjunto das matrizes $n \times n$ com entradas em $\mathbb{K}$, a $\mathbb{K}^{n^2}$, fica claro que a multiplicação de matrizes é diferenciável, uma vez que as entradas do produto AB são funções polinomiais das entradas de A e B. $GL(n, \mathbb{K})$ é uma variedade porque é o subconjunto de $M(n)$ definido pela equação $det(A) \neq 0$. Como o determinante é uma equação polinomial nas entradas de A, o conjunto das matrizes que satisfazem essa equação formam um aberto de $\mathbb{K}^{n^2}$, e portanto é uma subvariedade de $\mathbb{K}^{n^2}$.

4. O grupo $SL(n, \mathbb{K})$, formado pelas matrizes $n \times n$ de determinante igual a um. Pelo teorema da aplicação implícita, $SL(n, \mathbb{K})$ é uma variedade de $\mathbb{K}^{n^2}$, e portanto um grupo de Lie.

5. O grupo $O(n, \mathbb{K})$ das matrizes ortogonais $n \times n$. Esse conjunto é definido pela equação $AA^T = I$, que é um sistema de equações polinomiais nas entradas de A. Podemos usar o teorema da aplicação implícita para mostrar que o conjunto formado pelas matrizes que satisfazem essa equação também é uma variedade de $\mathbb{K}^{n^2}$. Também é uma variedade o grupo $SO(n, \mathbb{K}) = O(n, \mathbb{K}) \cap SL(n, \mathbb{K})$.

6. De maneira semelhante mostramos que $U(n)$, o conjunto das matrizes complexas unitárias $n \times n$, definidas pela equação $UU^\dagger = I$, é um grupo de Lie. Também é um grupo de Lie $SU(n) = SL(n, \mathbb{C}) \cap U(n)$, o conjunto das matrizes unitárias especiais.

7. O grupo de Lorentz, formado pelas matrizes 4×4 que satisfazem a equação

$$AMA^T = M \qquad M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

   Para ver que esse grupo é uma variedade em $\mathbb{K}^{n^2}$, podemos usar mais uma vez o teorema da aplicação implícita, já que a equação acima é polinomial nas entradas de A. Um subgrupo importante do grupo de Lorentz consiste das transformações de Lorentz próprias e ortócronas, que é chamado de grupo de Lorentz restrito e que será denotado por L. Uma transformação de Lorentz é dita *própria* se possuir determinante igual a um e *ortócrona* se possuir a entrada 11 maior que zero.

Definição 12. *Um subgrupo H do grupo G é dito um subgrupo de Lie de G se H é uma subvariedade de G.*

Exemplos:

1. $SL(n)$, $O(n)$, $SO(n)$, $U(n)$ e $SU(n)$ são subgrupos de Lie de $GL(n)$.

2. O grupo das transformações de Lorentz próprias e ortócronas é um subgrupo de Lie do grupo de Lorentz.

Como um subgrupo de Lie H é uma subvariedade, é aberto em seu fecho $\overline{H}$, que também é um subgrupo, já que a multiplicação em G é uma aplicação contínua. Como μ_p é um difeomorfismo para todo $p \in G$, cada classe lateral de H em $\overline{H}$ também é um aberto em $\overline{H}$. Como H é o complementar da união de suas classes laterais, exceto o próprio H, segue que H é fechado em $\overline{H}$ e por consequência também é fechado em G. Logo todo subgrupo de Lie aberto é união de componentes conexas de G.

Corolário 2. *Todo subgrupo de Lie aberto contém a componente conexa da identidade G^0.*

Proposição 4. *A componente conexa G^0 de G que contém a identidade é um subgrupo de Lie normal de G. As componentes conexas restantes são as classes laterais de G^0.*

Demonstração. Primeiro vamos mostrar que G^0 é um grupo. Sejam $h_1, h_2 \in G^0$. Devemos mostrar que $h_1 h_2$ e $h_1^{-1} \in G^0$. Sabemos que $\mu_{h_1} : G \to G$ é um difeomorfismo e por isso deve levar G_0 em alguma componente conexa de G. Como $e \in G^0$, essa componente conexa deve ser G^0, uma vez que $h_1 \in G^0$. Desse modo, μ_{h_1} é uma bijeção entre G^0 e ele mesmo e $h_1 h_2 \in G^0$.

Como o mapa ν que leva cada elemento em seu inverso é um difeomorfismo, também deve levar G^0 em alguma componente conexa. Como $\nu(e) = e$, essa componente deve ser o próprio G^0 de modo que $h_1^{-1} \in G^0$.

Agora devemos mostrar que G^0 é normal, ou seja, que as classes laterias à direita e à esquerda são iguais. Como a multiplicação à esquerda e à direita são difeomorfismos, pG^0 e $G^0 p$ são componentes conexas de G. Como $e \in G^0$, $p \in pG^0$ e $p \in G^0 p$, o que implica que $pG^0 = G^0 p$ para todo $p \in G$.

Resta mostrar que as outras componentes conexas são classes laterais de G^0. Seja H uma componente conexa de G e $h \in H$. Então $hG^0 = H$ pois hG^0 é uma componente conexa de g e $he = h$. □

Corolário 3. *O subgrupo gerado por qualquer vizinhança da identidade é G^0.*

Demonstração. Seja V uma vizinhança da identidade e $h \in V$. Como a multiplicação à esquerda é um difeomorfismo, hV é um aberto que contém h, uma vez que $e \in V$, e que está contido no subgrupo gerado por V. Logo esse subgrupo é aberto e portanto é um subgrupo de Lie, de modo que deve conter G^0. Como G^0 é um subgrupo que contém V, o subgrupo gerado por V é igual a G^0. □

1.2.1 Álgebra de Lie

Definição 13. *A álgebra de Lie $\mathfrak{g}$ de um grupo de Lie G é o espaço tangente de G na identidade do grupo e.*

Muitas informações sobre G podem ser obtidas a partir de $\mathfrak{g}$. Veremos na seção seguinte como $\mathfrak{g}$ pode ser útil para provar resultados a respeito de G.

O espaço tangente de uma variedade pode ser mapeado na variedade através de uma aplicação, chamada aplicação exponencial. Restrita à vizinhanças adequadas, chamadas vizinhanças normais, a exponencial é um difeomorfismo entre o espaço tangente e a variedade. No caso dos grupos de Lie matriciais, a aplicação exponencial que leva a álgebra de Lie ao grupo coincide com a exponencial matricial, dada pela expressão

$$e^A \equiv I + A + \frac{A^2}{2} + \frac{A^3}{3!} + \ldots + \frac{A^n}{n!} + \ldots$$

Em uma vizinhança normal da identidade esse mapa é um difeomorfismo, e o difeomorfismo inverso é chamado de logaritmo.

Teorema 8. *Se a álgebra de Lie de um grupo matricial G é gerada pelos elementos g_i e a álgebra de Lie de um grupo matricial H é gerada por elementos h_j então a álgebra de Lie de $G \otimes H$ é gerada pelos elemento $g_i \otimes I$ e $I \otimes h_j$.*

1.2.2 Alguns homomorfismos importantes

Alguns dos grupos dos quais falamos na seção anterior estão relacionadas através de dois homomorfismos que serão muito úteis para aplicações que mostraremos no capítulo 3. O primeiro deles relaciona $SL(2,\mathbb{C})$ e L e o segundo relaciona o produto tensorial $SL(2,\mathbb{C}) \otimes SL(2,\mathbb{C})$ e $SO(4,\mathbb{C})$. As demonstrações são baseadas nas demonstrações apresentadas em [2].

Vamos precisar de algumas propriedades desses grupos de Lie.

Lema 1. *$SL(2,\mathbb{C})$ é um grupo de Lie conexo, cuja álgebra de Lie é o conjunto das matrizes complexas 2×2 de traço nulo.*

Lema 2. *$SO(4,\mathbb{C})$ é um grupo de Lie conexo, cuja álgebra de Lie é o conjunto das matrizes complexas 4×4 antissimétricas.*

Lema 3. *O grupo de Lorentz restrito é um grupo conexo, cuja álgebra de Lie tem dimensão 6.*

Proposição 5. *Seja* $B = 1/2 \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & i & i & 0 \\ 0 & -1 & 1 & 0 \\ i & 0 & 0 & -i \end{bmatrix}$ *e*

$$\begin{aligned} \Phi : SL(2,\mathbb{C}) \otimes SL(2,\mathbb{C}) &\longrightarrow SO(4,\mathbb{C}) \\ A_1 \otimes A_2 &\longmapsto B(A_1 \otimes A_2)B^\dagger. \end{aligned}$$

Então Φ é um isomorfismo de grupos de Lie.

Demonstração. Não é difícil mostrar que se $A_1, A_2 \in SL(2,\mathbb{C})$ então $B(A_1 \otimes A_2)B^\dagger \in SO(4,\mathbb{C})$. De fato,

$$\begin{aligned} (B(A_1 \otimes A_2)B^\dagger)(B(A_1 \otimes A_2)B^\dagger)^T &= B(A_1 \otimes A_2)B^\dagger B^*(A_1^T \otimes A_2^T)B^T \\ = B(A_1 \otimes A_2)(\sigma_2 \otimes \sigma_2)(A_1^T \otimes A_2^T)B^T &= det(A_1)det(A_2)B(\sigma_2 \otimes \sigma_2)B^T = I. \end{aligned}$$

em que

$$\sigma_2 = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}.$$

Além disso, Φ é injetiva pois B é uma matriz invertível.

Resta mostrar a sobrejetividade. A álgebra de Lie $\mathfrak{sl}(2)$ é gerada pelas matrizes:

$$h = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad f = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Por esse motivo, a álgebra de Lie de $SL(2) \otimes SL(2)$, que denotaremos por $\mathfrak{al}(SL(2,\mathbb{C}) \otimes SL(2,\mathbb{C}))$, é gerada pelas matrizes $A_1 = I \otimes h,\ A_2 = I \otimes e,\ A_3 = I \otimes f,\ A_4 = h \otimes I,\ A_5 = e \otimes I,\ A_6 = f \otimes I$.

Calculando $BA_iB^\dagger$, obtemos seis matrizes antissimétricas e linearmente independentes, uma vez que B é invertível. Como a dimensão do espaço das matrizes antissimétricas 4×4 é

6, essas matrizes geram esse espaço, que é justamente a álgebra de Lie de $SO(4,\mathbb{C})$. Logo o mapa

$$\begin{aligned} \phi : \mathfrak{al}(SL(2,\mathbb{C})\otimes SL(2,\mathbb{C})) &\longrightarrow \mathfrak{so}(4,\mathbb{C}) \\ A &\longmapsto BAB^\dagger \end{aligned}$$

é um isomorfismo de álgebras de Lie. Como $\exp(BAB^\dagger) = B\exp(A)B^\dagger$, uma vez que $B^\dagger B = I$, temos que $\exp\circ\,\phi\circ\log = \Phi$. Seja V uma vizinhança normal da identidade em $SL(2,\mathbb{C})\otimes SL(2,\mathbb{C})$ cuja imagem seja também uma vizinhança normal. Então, restrita a essas vizinhanças, Φ é um difeomorfismo. Logo existe uma vizinhança da identidade em $SO(4,\mathbb{C})$ em que todas as matrizes podem ser escritas na forma $BA_1\otimes A_2B^\dagger$, $A_i \in SL(2,\mathbb{C})$. Como $B^\dagger B = I$, toda matriz no subgrupo gerado por essa vizinhança pode ser escrita nessa forma. Mas o subgrupo gerado por qualquer vizinhança da identidade em $SO(4,\mathbb{C})$ é o grupo todo, pois $SO(4,\mathbb{C})$ é conexo. Assim mostramos que Φ é sobrejetivo. □

Proposição 6. *Seja* $T = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & i & -i & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$ *e*

$$\begin{aligned} \Phi : SL(2,\mathbb{C}) &\longrightarrow L \\ A &\longmapsto T(A\otimes A^*)T^\dagger. \end{aligned}$$

Então Φ *é uma aplicação sobrejetiva e* $\Phi(A) = \Phi(B) \Leftrightarrow B = \pm A$.

Demonstração. Definimos um mapa induzido por Φ nas álgebras de Lie da seguinte forma:

$$\begin{aligned} \phi : \mathfrak{sl}(2,\mathbb{C}) &\longrightarrow \mathfrak{L} \\ X &\longmapsto T(X\otimes I + I\otimes X^*)T^\dagger. \end{aligned}$$

Restringindo-nos a vizinhanças da identidade adequadas, de modo que o logaritmo esteja bem definido, temos que, como $\Phi(A) = T(A\otimes A^*)T^\dagger$:

$$\log(\Phi(\exp(X))) = \log(T(\exp(X)\otimes\exp(X)^*)T^\dagger) =$$

$$T(\log(\exp(X)\otimes\exp(X)^*))T^\dagger = T(\log((\exp(X)\otimes I)(I\otimes\exp(X)^*)))T^\dagger =$$

$$T(\log(\exp(X)\otimes I) + \log(I\otimes\exp(X)^*))T^\dagger = T(X\otimes I + I\otimes X^*)T^\dagger.$$

Desse modo, $\phi(X) = \log(\Phi(\exp(X)))$, e $\Phi = \exp\circ\phi\circ\log$.

Considerando $\mathfrak{sl}(2,\mathbb{C})$ uma álgebra de Lie sobre $\mathbb{R}$, seus geradores são h, e, f, ih, ie, if. As imagens dessas matrizes por ϕ são matrizes linearmente independentes, e por isso o mapa ϕ é um isomorfismo entre as álgebras de Lie. Desse modo, obtemos um difeomorfismo entre vizinhanças da identidade. Pelo fato de L ser conexo, essa vizinhança gera o grupo inteiro. Como produto de elementos da imagem pertence à imagem, uma vez que $T^\dagger T = I$, o mapa Φ é sobrejetivo.

Como T é uma matriz invertível, $\phi(A) = \phi(B) \Leftrightarrow A\otimes A^* = B\otimes B^*$, o que acontece se e somente se $A = \pm B$. De fato, se

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad B = \begin{bmatrix} x & y \\ w & z, \end{bmatrix}$$

então

$$\begin{bmatrix} aa^* & ab^* & ba^* & bb^* \\ ac^* & ad^* & bc^* & bd^* \\ ca^* & cb^* & da^* & db^* \\ cc^* & cd^* & dc^* & dd^* \end{bmatrix} = \begin{bmatrix} xx^* & xy^* & yx^* & yy^* \\ xw^* & xz^* & yw^* & yz^* \\ wx^* & wy^* & zx^* & zy^* \\ ww^* & wz^* & zw^* & zz^* \end{bmatrix}$$

e então temos:

$$|a|^2 = |x|^2, \quad |b|^2 = |y|^2, \quad |c|^2 = |w|^2, \quad |d|^2 = |z|^2$$
$$ac^* = xw^*, \quad ab^* = xy^*, \quad bd^* = yz^*, \quad cd^* = wz^*$$

Escrevendo

$$a = r_1 e^{i\alpha_1}, \quad b = r_2 e^{i\alpha_2}, \quad c = r_3 e^{i\alpha_3}, \quad d = r_4 e^{i\alpha_4}$$
$$x = r'_1 e^{i\alpha'_1}, \quad y = r'_2 e^{i\alpha'_2}, \quad w = r'_3 e^{i\alpha'_3}, \quad z = r'_4 e^{i\alpha'_4},$$

obtemos as seguintes relações:

$$r_i = r'_i \ \ \forall \ \ i, \quad \alpha_i - \alpha'_i = \beta \ \ \forall \ \ i,$$

o que implica que $B = e^{i\beta}A$. Como $det(A) = det(B) = 1$ então $e^{i\beta} = \pm 1$, como queríamos mostrar. □

1.3 Convexidade

Convexidade é uma restrição importante para que um conjunto possa servir como o conjunto de estados possíveis de um sistema físico. Essa restrição vem do fato de que queremos formar "misturas"de dois estados, que geometricamente seriam representadas por pontos no segmento de reta que liga os estados que queremos misturar. Nessa seção vamos estudar apresentar as principais propriedades de conjuntos convexos e vetores de probabilidade [11].

Definição 14. *Um conjunto C em um espaço vetorial $\mathcal{V}$ é chamado convexo se dados dois vetores $v, u \in C$ os pontos da forma*

$$\lambda v + (1-\lambda)u \ , \quad \lambda \in [0,1],$$

também pertencem a C.

Alguns conjuntos convexos possuem pontos especiais que não podem ser escritos como soma convexa de outros pontos, chamados pontos extremais. Por exemplo, os vértices são pontos extremais do quadrado, do cubo e do triângulo, e os pontos na esfera de raio um são os pontos extremais da bola de raio um. O quadrante em $\mathbb{R}^n$ formado por todos os pontos cujas coordenadas são positivas é um exemplo de um conjunto convexo sem pontos extremais.

Definição 15. *O fecho convexo de um conjunto A em $\mathcal{V}$ é o menor conjunto convexo que contém A.*

O fecho convexo de um conjunto de $p+1$ pontos, tais que eles não pertençam todos a um subespaço afim de dimensão $p-1$, é chamado de p-simplexo.

Um importante resultado para conjuntos convexos em espaços vetoriais normados é o teorema de Hahn-Banach [4].

Teorema 9 (Hahn-Banach versão geométrica)**.** *Seja $\mathcal{V}$ um espaço vetorial normado e sejam $A, B \subset \mathcal{V}$ conjuntos convexos, não-vazios, disjuntos, A fechado e B compacto. Então existe um funcional linear $f : \mathcal{V} \to \mathbb{K}$ e uma constante c tais que*

$$f(a) > c \ \ \forall \ \ a \in A, \quad f(b) < c \ \ \forall \ \ b \in B.$$

1.3.1 Probabilidades

Queremos agora estudar um conjunto convexo especial em $\mathbb{R}^N$: o conjunto de todas as distribuições de probabilidade para uma variável aleatória X.

Uma variável aleatória pode ser considerada como o resultado numérico de fazer uma experiência não determinística para gerar resultados aleatórios, como por exemplo jogar uma moeda, um dado, ou realizar a medição de uma grandeza física. Vamos considerar o caso em que o conjunto dos possíveis resultados, ou seja, o espaço amostral, possua N elementos. Representaremos resultados possíveis por x_i e a probabilidade de cada resultado ser obtido por $P(X = x_i) = p_i$. Como representam as probabilidades de uma variável aleatória, cada $p_i \geq 0$ e $\sum_i p_i = 1$.

O conjunto de todas as distribuições de probabilidades possíveis para X é o conjunto de todos os vetores em $\mathbb{R}^N$ com coordenadas não-negativas e que somam um. Esse conjunto é um (N-1)-simplexo em $\mathbb{R}^N$, fecho convexo de seus pontos extremais que são as distribuições tais que um dos p_i é igual a um e os outros são zero, e será denotado por Δ.
Vamos agora definir um conceito que, de certa forma, torna mais precisa a noção de que um vetor de probabilidade pode ser mais "uniforme"que outro.

Definição 16. *Consideremos dois vetores $x, y \in \Delta$. Sejam $x^\downarrow$ e $y^\downarrow$ os vetores obtidos de x e y colocando suas coordenadas em ordem não-crescente. Dizemos que x é majorado por y, ou que y majora x se para todo $k = 1, \ldots, N$ vale*

$$\sum_{i=1}^{k} x^\downarrow \leq \sum_{i=1}^{k} y^\downarrow.$$

Se y majora x, denotamos $x \prec y$ ou $y \succ x$.

É claro que vale a reflexividade, ou seja, $x \prec x$ e também a transitividade, ou seja, se $x \prec y$ e $y \prec z$ então, $x \prec z$. No entanto $x \prec y$ e $y \prec x$ não implica $x = y$ pois as coordenadas de y podem ser uma permutação das coordenadas de x. No entanto, se considerarmos o conjunto das classes de equivalência tais que dois vetores estão relacionados se as coordenadas de um são permutação das coordenadas do outro, então $x \prec y$ e $y \prec x$ implica $x = y$. Desse modo, a majoração impõe uma ordem parcial em Δ, com a relação de equivalência explicada. A ordem é apenas parcial pois existem vetores tais que nenhum deles majora o outro. Existem um menor e um maior elemento para essa ordem parcial:

$$x_N \equiv \left[\ \tfrac{1}{N} \quad \tfrac{1}{N} \quad \ldots \quad \tfrac{1}{N} \ \right] \prec x \prec \left[\ 1 \quad 0 \quad \ldots \quad 0 \ \right] \equiv x_1.$$

Se x é majorado por y, de maneira intuitiva x está mais "próximo"da distribuição uniforme x_N que y.

Definição 17. *Uma matriz estocástica B agindo em Δ é uma matriz com N colunas tal que*

$$B_{ij} \geq 0, \quad \sum_{i=1}^{N} B_{ij} = 1.$$

Uma matriz biestocástica é uma matriz estocástica quadrada que também satisfaz

$$\sum_{j=1}^{N} B_{ij} = 1.$$

Uma matriz estocástica é uma matriz que leva uma distribuição de probabilidade em outra, não necessariamente com o mesmo número de coordenadas. Uma matriz biestocática é uma matriz que leva uma distribuição de probabilidade em outra com o mesmo número de coordenadas e além disso preserva o menor elemento x_N. Um resultado importante é o seguinte

Teorema 10 (Hardy, Littlewood e Pólya (HLP))**.** *Dados dois vetores $x, y \in \Delta$, $x \prec y$ se, e somente se, existe uma matriz biestocástica tal que $x = By$.*

Esse resultado nos permite interpretar a ação de uma matriz biestocástica em Δ como uma contração do simplexo em direção ao seu centro x_N, uma vez que essa ação torna as distribuições mais próximas da distribuição uniforme.

Teorema 11. *Se y majora x, então x pertence ao fecho convexo do conjunto de vetores formados por todas as permutações das coordenadas de y.*

Definição 18. *Dizemos que uma função $f : S \to \mathbb{R}$ é convexa de Schur se*

$$y \succ x \Longrightarrow f(y) \geq f(x).$$

Dizemos que f é côncava de Schur se

$$y \succ x \Longrightarrow f(y) \leq f(x).$$

Motivado pela melhoria na transmissão de informação através de canais como cabos telefônicos, Shannon desenvolveu a primeira teoria de informação bem sucedida, dando uma definição matemática para o conceito de informação.

Definição 19. *Dada uma variável aleatória X com resultados possíveis x_i que ocorrem com probabilidade p_i, a informação do evento $X = x_i$ é dada por*

$$I(X = x_i) = -\log(p_i).$$

A função $\log$ é escolhida pelo fato de ser a única que satisfaz três propriedades desejáveis para uma função que represente *informação*: depender apenas da probabilidade p_i, ser contínua e ser aditiva, isto é, se temos duas variáveis aleatórias independentes X e Y, então

$$I(X = x_i, Y = y_i) = I(X = x_i) + I(Y = y_i).$$

Definição 20. *A entropia de Shannon de X é a esperança de I em X*

$$S(X) = \sum_i p_i I(X = x_i) = -\sum_i p_i \log(p_i).$$

Usamos a convenção $0 \log 0 = 0$.

A entropia de Shannon quantifica a "incerteza"da variável aleatória X. Se não há incerteza nenhuma, ou seja, se $p_i = 1$ para algum i, $S(X) = 0$. Se a incerteza é "máxima", ou seja, se a distribuição de probabilidade de X é uniforme, então $S(X)$ assume seu valor máximo.

Teorema 12. *A entropia de Shannon é uma função côncava de Schur.*

Uma maneira de generalizarmos as distribuições de probabilidade em Δ é através das matrizes positivas de traço um, que chamaremos matrizes densidade. Elas representam uma versão quântica dos vetores de probabilidade clássicos. O vetor formado pelos autovalores de uma matriz densidade é um vetor em Δ.

Assim como Δ, o conjunto de todas as matrizes densidade de uma dada dimensão é um conjunto convexo e muitas das definições e resultados válidos para vetores em Δ podem ser generalizado para matrizes densidade, como por exemplo o conceito de majoração e o lema HLP, que veremos no capítulo 4. Podemos também definir o análogo da entropia de Shannon, a entropia de von Neumann.

Definição 21. *A entropia de von Neumann de uma matriz densidade ρ é definida como*

$$S(\rho) = -Tr(\rho \log \rho), \tag{1.1}$$

e é igual à entropia de Shannon do vetor formado pelos autovalores de ρ.

Voltaremos a falar da entropia de Von Neumann no capítulo 4, onde ela será utilizada para quantificar emaranhamento de estados puros de sistemas bipartites. Para mais detalhes sobre teoria de informação e entropia de Shannon veja [11, 15, 17].

CAPÍTULO 2

Sistemas quânticos

Nesse capítulo, apresentamos os conceitos matemáticos básicos da mecânica quântica. Eles serão apresentados em forma de postulados, e não será dada ênfase às motivações para tais postulados e sim aos resultados que podemos obter como consequência deles.

Na primeira seção, estudamos o conjunto de todos os estados possíveis de um sistema quântico, o chamado espaço de estados do sistema. Definições precisas de sistema e estado são difíceis de serem dadas. O leitor possivelmente possui uma noção intuitiva do que sejam ambos e ela será suficiente para nossos propósitos. É importante somente que o leitor esteja familiarizado com a seção .

Na segunda seção, veremos como obter informações sobre o sistema a partir de seu estado, através das medições. O passo seguinte é estudar os canais quânticos, que estão relacionados à evolução temporal de um sistema físico. A caracterização desses canais nos leva à definição dos mapas completamente positivos.

Na última seção, chegamos à definição que é o assunto central dessa dissertação: o emaranhamento, que surge como uma consequência da estrutura tensorial do espaço de estados de sistemas quânticos compostos.

2.1 Estados quânticos

A mecânica quântica é a teoria física adequada para descrever o comportamento de vários sitemas físicos microscópicos como átomos e fótons. Ela impõe quais são os objetos que descrevem os estados do sistema e as grandezas físicas associadas, e as regras que eles devem obedecer. É difícil encontrar uma definição precisa para o que é um sistema quântico, e aqui simplesmente adotaremos a visão apresentada no livro de Asher Peres [18]:

A quantum system is whatever admits a closed dynamical descripition within quantum mechanics.

Em relação aos objetos que representam os *estados* do sistema, a mecânica quântica diz o seguinte:

Postulado 22 (Estados do sistema)**.** *A cada sistema quântico está associado um espaço de Hilbert sobre $\mathbb{C}$, que denotaremos por $\mathcal{H}$. Os estados do sistema são representados por operadores positivos de traço um em $\mathcal{H}$, que chamaremos de matrizes densidade.*

Aqui nos preocuparemos apenas com os casos de dimensão finita. O conjunto de todas as matrizes densidade será denotado por $D(\mathcal{H})$. Esse é um conjunto convexo, cujos pontos extremais representam um papel especial em mecânica quântica, como veremos mais adiante.

Definição 23. *Os pontos extremais do conjunto $D(\mathcal{H})$ são chamados estados puros do sistema quântico.*

Vejamos quem são esses pontos. Toda matriz ρ positiva de traço um pode ser escrita em decomposição espectral

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad p_i \geq 0, \quad \sum_i p_i = 1,$$

em que cada $|\psi_i\rangle$ é um vetor de norma um. Desse modo, toda matriz densidade pode ser escrita como soma convexa de projetores. Por outro lado, um projetor nunca pode ser escrito como soma convexa de outros. Logo os pontos extremais de $D(\mathcal{H})$ são os projetores $|\psi\rangle\langle\psi|$. Os estados que não são puros são chamados *mistos* e sempre podem ser escritos como soma convexa de estados puros. Essa decomposição, no entanto, não é única, e existem muitas maneiras diferentes de escrever um estado misto como soma convexa de estados puros.

A cada projetor está associada de maneira única uma direção em $\mathcal{H}$. Desse modo, podemos identificar os estados puros de um sistema quântico com classes de equivalência de vetores unitários em $\mathcal{H}$ pela relação

$$|\psi\rangle \sim e^{i\phi}|\psi\rangle.$$

O número ϕ é chamado de *fase global*. Assim, um estado do sistema é caracterizado por uma reta complexa passando pela origem em $\mathcal{H}$. O conjunto dessas retas é o espaço de Hilbert projetivo $\mathcal{PH}$. É comum representarmos os estados puros do sistema usando simplesmente vetores unitários em $\mathcal{H}$, mas devemos ter em mente que eles são apenas representantes da classe de equivalência associada a um estado, ou seja, vários vetores unitários distintos representam o mesmo estado puro.

2.2 Operações Quânticas

2.2.1 Medições e Observáveis

A próxima preocupação é entendermos que objetos estão associados às grandezas físicas relacionadas ao sistema em questão. De acordo com a mecânica quântica temos

Postulado 24 (Medições)**.** *Uma medição está associada a um conjunto de operadores M_i relacionados aos possíveis resultados i que satisfazem a relação de completude*

$$\sum_i M_i^\dagger M_i = I.$$

A probabilidade do resultado i ser obtido quando a medição é realizada em um sistema no estado ρ é

$$p_i = Tr(M_i^\dagger M_i \rho),$$

e o estado do sistema após a medição, se o resultado i for obtido é

$$\rho_i = \frac{M_i \rho M_i^\dagger}{Tr(M_i^\dagger M_i \rho)}.$$

Aqui aparece mais uma novidade da mecânica quântica: as medições são sempre probabilísticas. Em física clássica, a cada estado puro correspondem valores definidos para cada grandeza física, sendo que as medições apenas revelam quais são esses valores. Qualquer indeterminação é fruto do fato de possuirmos apenas informação incompleta sobre o sistema. Em física quântica, a cada estado puro estão associadas probabilidades para os resultados possíveis da medição, e a medição do mesmo observável em duas cópias do sistema no mesmo estado pode gerar resultados diferentes. Outra mudança é que o estado do sistema, mesmo no caso de o estado inicialmente ser puro, é modificado pela medição.

Um caso importante é quando temos $M_i = |\psi_i\rangle\langle\psi_i|$ para cada i. Para que a relação de completude seja satisfeita, os vetores $|\psi_i\rangle$ devem formar uma base ortonormal para $\mathcal{H}$. Esse tipo de medição é chamado de *medição projetiva.*

Proposição 7. *Para todo estado puro $|\psi\rangle$ existe uma medição projetiva para a qual $p_1 = 1$ e $p_i = 0$ para todo $i \neq 1$.*

Demonstração. Basta tomar $M_1 = |\psi\rangle\langle\psi|$. □

Já se temos um estado misto

$$\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|,$$

nenhuma medição projetiva pode ter resultado definido. De fato, suponhamos que $M_j = |\phi_j\rangle\langle\phi_j|$. Se algum $p_j = 0$ então todos os estados que aparecem na soma convexa são ortogonais a $|\phi_j\rangle$. Se $p_j = 0$ para todo $j \neq 1$, então todos os estados que aparecem na soma convexa devem ser múltiplos de $|\phi_1\rangle$, de modo que ρ representaria um estado puro.

Uma medição projetiva também pode ser usada para realizarmos *preparações* de estados puros. Desejamos um exemplar de um sistema físico em um determinado estado puro. Para obter esse exemplar podemos realizar uma medição projetiva em uma cópia do sistema em um outro estado, de maneira que um dos projetores da medição seja o projetor na direção do estado que desejamos preparar. Com esse procedimento, há uma probabilidade não nula de obtermos o estado desejado como estado final depois da medição, desde que o estado inicial do sistema não seja ortogonal a ele.

Postulado 25 (Grandezas Físicas)**.** *As grandezas físicas, ou observáveis, são representadas por operadores hermitianos O em $\mathcal{H}$.*

Cada operador hermitiano pode ser escrito em decomposição espectral

$$O = \sum_i o_i |\psi_i\rangle\langle\psi_i|.$$

A medição do observável O corresponde à medição projetiva com $M_i = |\psi_i\rangle\langle\psi_i|$. Os resultados possíveis são os autovalores o_i. Desse modo, quando medimos um observável O em um estado ρ obtemos o_i com probabilidade $p_i = Tr(|\psi_i\rangle\langle\psi_i|\rho)$.

A *esperança* ou *valor esperado* de O em um estado ρ é

$$\langle O \rangle = \sum_i p_i o_i = Tr(\rho O).$$

2.2.2 Evolução

Agora vamos considerar a dinâmica do sistema [11]. Vamos ver o que acontece com a matriz densidade quando aplicamos *mapas quânticos*, que são mapas que levam o espaço de estados do sistema nele próprio, de uma maneira que faça sentido do ponto de vista físico, o que explicaremos melhor mais a frente. Para que o mapa leve o espaço de estados nele mesmo, queremos que ele leve uma matriz densidade em outra, ou seja

$$\begin{aligned} \Phi : D(\mathcal{H}) &\longrightarrow M(\mathcal{H}) \\ \rho &\longmapsto \rho', \end{aligned}$$

tal que $\Phi\left(D(\mathcal{H})\right) \subset D(\mathcal{H})$.

A primeira condição que exigimos de um mapa desse tipo é que ele seja linear. A justificativa para tal restrição é que não queremos que o resultado da operação dependa de como escrevemos uma matriz densidade como soma convexa de outras. Desse modo temos:

$$\Phi(p_1\rho_1 + p_2\rho_2) = p_1\Phi(\rho_1) + p_2\Phi(\rho_2).$$

O mapa Φ pode ser representado por uma matriz que age em um espaço vetorial de dimensão N^2, ou seja, uma matriz $N^2 \times N^2$. Usaremos dois índices para indicar as componentes de uma matriz densidade $(N \times N)$ e quatro índices para indicar as componentes de um mapa agindo no espaço de matrizes densidade $(N^2 \times N^2)$. Assim temos:[1]

$$\rho'_{m\mu} = \Phi_{\substack{m\mu \\ n\nu}} \rho_{n\nu}.$$

O mapa Φ deve levar matrizes densidade em matrizes densidade, ou seja, ρ' deve ser uma matriz positiva de traço um. Isso implica que

1. $\Phi(\rho)$ deve ser autoadjunta:

$$\rho' = (\rho')^\dagger : \rho'_{m\mu} = (\rho'_{\mu m})^* \Rightarrow$$

$$\Phi_{\substack{m\mu \\ n\nu}} \rho_{n\nu} = \Phi^*_{\substack{\mu m \\ \nu n}} \rho^*_{\nu n} = \Phi^*_{\substack{\mu m \\ \nu n}} \rho_{n\nu} \Rightarrow \Phi_{\substack{m\mu \\ n\nu}} = \Phi^*_{\substack{\mu m \\ \nu n}} .$$

A última implicação é óbvia quando consideramos Φ como um mapa do espaço $M(\mathcal{H})$ em $M(\mathcal{H})$. No entanto, se consideramos Φ como um mapa de $D(\mathcal{H})$ em $D(\mathcal{H})$, ela

[1] Na notação que vamos usar em seguida, chamada, convencionamos que quando um índice aparece repetido em uma expressão, o somatório sobre esse índice está implícito, o que é chamado de convenção de Einstein. Em alguns momentos explicitamos o somatório, para evidenciar alguma observação feita.

continua válida. Para vermos isso, basta usarmos matrizes com apenas um elemento não nulo, igual a um, na diagonal, e matrizes com apenas um bloco 2×2 não nulo na diagonal, dos tipos

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \quad , \quad \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}.$$

2. $Tr(\rho') = 1$:

$$\rho'_{mm} = \Phi_{\substack{mm \\ n\nu}} \rho_{n\nu} = 1.$$

Como essa equação deve valer para todo ρ, podemos usar $\rho = |i\rangle\langle i|$, caso em que $\rho_{n\nu} = \delta_{n\nu}\delta_{ni}$, para concluir que $\Phi_{\substack{mm \\ n\nu}} = 1$, se $n = \nu$. Para concluir que $\Phi_{\substack{mm \\ n\nu}} = 0$, se $n \neq \nu$, utilizamos novamente as matrizes com os blocos mostrados acima.

3. A matriz ρ' deve ser positiva, ou seja, Φ deve levar matrizes positivas em matrizes positivas.

Definição 26. *Um mapa $\Phi : M(\mathcal{H}) \longrightarrow M(\mathcal{H})$ é chamado positivo se $\Phi(\rho)$ é positiva para toda matriz positiva ρ.*

Para estudarmos melhor que restrições essas propriedades impõem ao mapa Φ, vamos definir a *matriz dinâmica* associada a Φ:

$$D_{\substack{mn \\ \mu\nu}} = \Phi_{\substack{m\mu \\ n\nu}}.$$

Em termos da matriz dinâmica as condições acima podem ser dadas por:

1. $\rho' = (\rho')^\dagger \Leftrightarrow D = D^\dagger$.
2. $Tr(\rho') = 1 \Leftrightarrow D_{\substack{mn \\ m\nu}} = \delta_{n\nu}$.

Resta estudar qual é a condição imposta a D pela positividade de Φ. Vejamos inicialmente o que acontece para estados puros $\rho = |z\rangle\langle z|$, $\rho_{n\nu} = z_n z_\nu^*$. Se Φ for positivo então ρ' é positiva, o que implica que:

$$0 \leq \langle x|\rho'|x\rangle = x_m^* \rho'_{m\mu} x_\mu = x_m^* z_n D_{\substack{mn \\ \mu\nu}} x_\mu z_\nu^* = \langle z^*|\langle x|D|x\rangle|z^*\rangle.$$

Logo, se Φ é um mapa positivo, D deve satisfazer a condição $\langle z^*|\langle x|D|x\rangle|z^*\rangle \geq 0$ para todos $|z\rangle, |x\rangle \in \mathcal{H}$. Essa propriedade é chamada *positividade por blocos*.

Para ver que essa condição além de necessária é também suficiente, devemos mostrar que ela implica que ρ' é positiva também quando ρ é um estado misto, o que segue por convexidade. Tomamos $\rho = \sum_i p_i |z_i\rangle\langle z_i|$, $\rho_{n\nu} = \sum_i p_i (z_i)_n (z_i)_\nu^*$. Nesse caso,

$$\langle x|\rho'|x\rangle = x_m^* \rho'_{m\mu} x_\mu = x_m^* D_{\substack{mn \\ \mu\nu}} \left(\sum_i p_i (z_i)_n (z_i)_\nu^* \right) x_\mu$$

$$= \sum_i p_i \left(x_m^* (z_i)_n D_{\substack{mn \\ \mu\nu}} (z_i)_\nu^* x_\mu \right) \geq 0.$$

Isso prova o seguinte teorema:

Teorema 13 (Jamiołkowski)**.** *Um mapa linear $\Phi : M(\mathcal{H}) \longrightarrow M(\mathcal{H})$ é positivo se e somente se a matriz dinâmica é positiva por blocos.*

No entanto, a positividade do mapa Φ não é suficiente para que ele represente uma operação fisicamente permitida. Suponhamos que nosso sistema seja apenas um subsistema de um sistema maior. Como veremos na próxima seção, podemos representar um sistema composto em um espaço de Hilbert com estrutura de produto tensorial $\mathcal{H} \otimes \mathcal{H}'$, em que $\mathcal{H}$ é o espaço de Hilbert associado ao nosso sistema de interesse e $\mathcal{H}'$ é o espaço de Hilbert do sistema adicional. Gostaríamos que um mapa fisicamente permitido não só levasse a matriz densidade do nosso sistema em uma matriz densidade, mas que também o fizesse se considerarmos a operação agindo em $\mathcal{H} \otimes \mathcal{H}'$. Isso quer dizer que não só Φ deve ser um mapa positivo, mas também deve ser positiva toda extensão da forma $\Phi \otimes I$, em que I é o operador identidade em $M(\mathcal{H}')$.

Definição 27. *Se o mapa $\Phi \otimes I$ agindo em $M(\mathcal{H} \otimes \mathcal{H}')$ é positivo, em que $\mathcal{H}'$ é um espaço vetorial de dimensão k, dizemos que Φ é um mapa k-positivo. Se Φ é um mapa k-positivo para todo $k \in \mathbb{N}$ então Φ é chamado um mapa completamente positivo.*

A exigência que impomos agora em Φ é que ele seja um mapa completamente positivo. Vejamos que implicação essa propriedade tem sobre a matriz dinâmica correspondente. Como ela é uma matriz $N^2 \times N^2$, podemos vizualizá-la como uma matriz agindo em um espaço vetorial de dimensão N^2, que pode ser identificado com $\mathcal{H} \otimes \mathcal{H}$. Como ela é hermitiana, podemos escrevê-la em decomposição espectral:[2]

$$D = \sum_i d_i |\chi^i\rangle\langle\chi^i|, \quad D_{\substack{mn \\ \mu\nu}} = \sum_i d_i \chi^i_{mn} (\chi^i_{\mu\nu})^*.$$

Tomamos um estado puro em um espaço de Hilbert estendido,

$$\rho \in M(\mathcal{H} \otimes \mathcal{H}'), \quad \rho_{mm',\mu\mu'} = z_{mm'} z^*_{\mu\mu'}.$$

e aplicamos o mapa estendido $\Phi \otimes I$ a ρ

$$\begin{aligned}
\rho'_{mm',\mu\mu'} &= (\Phi \otimes I)_{\substack{mm' \\ nn' \\ ,\nu\nu'}}^{\substack{,\mu\mu' \\ }} \rho_{nn',\nu\nu'} \\
&= \Phi_{\substack{m\mu \\ n\nu}} I_{\substack{m'\mu' \\ n'\nu'}} \rho_{nn',\nu\nu'} \\
&= \Phi_{\substack{m\mu \\ n\nu}} \delta_{m'n'} \delta_{\mu'\nu'} z_{nn'} z^*_{\nu\nu'} \\
&= \Phi_{\substack{m\mu \\ n\nu}} z_{nm'} z^*_{\nu\mu'} = \sum_i d_i \chi^i_{mn} z_{nm'} (\chi^i_{\mu\nu})^* z^*_{\nu\mu'}.
\end{aligned}$$

Agora tomamos um outro vetor $|x\rangle$ em $\mathcal{H}' \otimes \mathcal{H}$ e testamos se $\langle x|\rho'|x\rangle \geq 0$:

$$\langle x|\rho'|x\rangle = x_{mm'} \rho'_{mm',\mu\mu'} x^*_{\mu\mu'} = \sum_i d_i (\chi^i_{mn} z_{nm'} x_{mm'})(\chi^i_{\mu\nu} z_{\nu\mu'} x_{\mu\mu'})^*.$$

[2] Escrevemos $|\chi^i\rangle$ com dois índices pois estamos usando a estrutura tensorial de $\mathcal{H} \otimes \mathcal{H}$.

Explicitando um pouco mais os somatórios envolvidos na expressão acima temos:

$$\langle x|\rho'|x\rangle = \sum_i d_i \left(\sum_{mm'n} \chi^i_{mn} z_{nm'} x_{mm'}\right)\left(\sum_{\mu\mu'\nu} \chi^i_{\mu\nu} z_{\nu\mu'} x_{\mu\mu'}\right)^* =$$

$$\sum d_i \left|\sum_{mm'n} \chi^i_{mn} z_{nm'} x_{mm'}\right|^2 .$$

Essa quantidade deve ser não-negativa para todo $|z\rangle$ e todo $|x\rangle$ que escolhermos. Isso só acontece se cada um dos d_i for um número não-negativo, ou seja, se D for uma matriz positiva semidefinida.

Por outro lado, se D é uma matriz positiva e $\rho = \sum_j p_j |z^j\rangle\langle z^j|$, então vale:

$$x_{mm'}\rho'_{mm',\mu\mu'}x^*_{\mu\mu'} = \sum_i \sum_j d_i p_j \left(\sum_{mm'n} \chi^i_{mn} z^j_{nm'} x_{mm'}\right)\left(\sum_{\mu\mu'\nu} \chi^i_{\mu\nu} z^j_{\nu\mu'} x_{\mu\mu'}\right)^*$$

$$= \sum_i \sum_j d_i p_j \left|\sum_{mm'n} \chi^i_{mn} z^j_{nm'} x_{mm'}\right|^2 \geq 0.$$

Com isso, acabamos de provar o seguinte teorema:

Teorema 14 (Choi)**.** *Um mapa linear Φ é completamente positivo se e somente se a matriz dinâmica correspondente é positiva semidefinida.*

Uma forma muito útil de caracterizar os mapas completamente positivos é através da representação de Kraus [19].

Teorema 15 (Representação de Kraus)**.** *Um mapa linear Φ é completamente positivo se, e somente se, é da forma*

$$\rho \longmapsto \rho' = \sum_i A_i \rho A_i^\dagger,$$

em que cada A_i é uma matriz quadrada da mesma dimensão de ρ. Além disso, Φ preserva o traço se, e somente se, as matrizes A_i satisfazem

$$\sum_i A_i^\dagger A_i = I.$$

Demonstração. Suponhamos que Φ seja completamente positivo e seja D a matriz dinâmica associada. Como D é positiva, pode ser escrita em decomposição espectral

$$D = \sum_i d_i |\chi^i\rangle\langle\chi^i| \ , \quad d_i > 0.$$

Definindo $|A^i\rangle = \sqrt{d_i}|\chi^i\rangle$, temos que

$$D = \sum |A^i\rangle\langle A^i|, \quad D_{\substack{mn \\ \mu\nu}} = \sum_i A^i_{mn}(A^i_{\mu\nu})^*.$$

Cada vetor $|A^i\rangle \in \mathcal{H} \otimes \mathcal{H}$ possui n^2 coordenadas que indexamos usando dois índices para deixar evidente a estrutura de produto tensorial. Assim podemos identificar cada $|A^i\rangle$ com um operador A_i agindo em $\mathcal{H}$ da forma $(A_i)_{mn} = A^i_{mn}$. Daí temos:

$$\rho'_{m\mu} = \Phi_{\substack{m\mu \\ n\nu}} \rho_{n\nu} = D_{\substack{mn \\ \mu\nu}} \rho_{n\nu} =$$
$$\sum_i A^i_{mn}(A^i_{\mu\nu})^* \rho_{n\nu} = \sum_i (A_i)_{mn}\rho_{n\nu}(A_i)^\dagger_{\nu\mu} = \sum_i (A_i\rho(A_i)^\dagger)_{m\mu}$$
$$\Rightarrow \rho' = \sum_i A_i\rho(A_i)^\dagger.$$

Se Φ preservar o traço, temos também:

$$\delta_{n\nu} = \sum_m D_{\substack{mn \\ m\nu}} = \sum_i \sum_m (A_i)_{mn}(A_i)^*_{m\nu} = \sum_i \sum_m (A_i)^\dagger_{\nu m}(A_i)_{mn} = \sum_i ((A_i)^\dagger A_i)_{\nu n},$$
$$\Rightarrow \sum_i (A_i)^\dagger A_i = I.$$

Por outro lado, se $\Phi(\rho) = \sum_i A_i\rho A_i^\dagger$, então $\Phi \otimes I(\sigma) = \sum_i A_i \otimes I(\sigma) A_i^\dagger \otimes I$, que é claramente um mapa positivo. □

Na demonstração acima, usamos o fato de que $\mathcal{L}(E, F) \equiv E^* \otimes F$, em que E^* denota o espaço dual de E. Como estamos trabalhando em dimensão finita, vale $E^* \equiv E$ de modo que temos $\mathcal{L}(E, F) \equiv E \otimes F$. Desse modo temos $\mathcal{L}(\mathcal{H}) \equiv \mathcal{H} \otimes \mathcal{H}$ e podemos identificar cada vetor $|A^i\rangle$ com um operador A_i.

2.2.3 Mapas positivos gerais

Os mapas que consideramos na seção anterior correspondem às possíveis evoluções de um dado sistema quântico. Podemos também considerar canais tais que o sistema de saída do canal não seja o mesmo que o de entrada. Queremos considerar agora mapas entre dois espaços de estados de dimensões distintas $\Lambda : M(\mathcal{H}_A) \to M(\mathcal{H}_B)$ [20, 21]. As definições de mapa *positivo*, *k-positivo* e *completamente positivo* se generalizam para esses casos

Definição 28. *Um mapa $\Phi : M(\mathcal{H}_A) \longrightarrow M(\mathcal{H}_B)$ é chamado positivo se $\Phi(\rho)$ é positiva para toda matriz positiva $\rho \in M(\mathcal{H}_A)$. Se o mapa $\Phi \otimes I : M(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}') \to M(\mathcal{H}_\mathcal{B} \otimes \mathcal{H}')$ é positivo, em que $\mathcal{H}'$ é um espaço vetorial de dimensão k, dizemos que Φ é um mapa k-positivo. Um mapa é chamado completamente positivo se é k-positivo pra todo k.*

Nesse caso mais geral também é possível associar uma matriz dinâmica ao mapa Φ

$$D_{\substack{mn \\ \mu\nu}} = \Phi_{\substack{m\mu \\ n\nu}}.$$

A matriz associada ao mapa Φ não é uma matriz quadrada. Se $\dim(\mathcal{H}_A) = N$ e $\dim(\mathcal{H}_B) = K$, então a matriz de Φ é $K^2 \times N^2$. No entanto a matriz dinâmica é uma matriz quadrada $NK \times NK$. Os resultados apresentados nos teoremas de Jamiołkowski e Choi podem ser facilmente generalizados para esse caso

Teorema 16. *Um mapa $\Phi : M(\mathcal{H}_A) \longrightarrow M(\mathcal{H}_B)$ é positivo se e somente se matriz dinâmica associada é positiva por blocos.*

Teorema 17. *Um mapa $\Phi : M(\mathcal{H}_A) \longrightarrow M(\mathcal{H}_B)$ é completamente positivo se e somente se a matriz dinâmica associada é positiva.*

A matriz dinâmica pode ser escrita em termos da ação do mapa $\Lambda \otimes I : M(\mathcal{H}_A \otimes \mathcal{H}_A) \rightarrow M(\mathcal{H}_B \otimes \mathcal{H}_A)$ em $P_+ = |\Phi_+\rangle\langle\Phi_+| \in M(\mathcal{H}_A \otimes \mathcal{H}_A)$ sendo

$$|\Phi_+\rangle = \sum_i |ii\rangle.$$

Teorema 18 (Isomorfismo de Jamiołkowski)**.** *Dado um mapa $\Lambda : M(\mathcal{H}_A) \rightarrow M(\mathcal{H}_B)$, temos*

$$\Lambda \otimes I(|\Phi_+\rangle\langle\Phi_+|) = D_\Lambda.$$

Demonstração.

$$(\Lambda \otimes I(P_+))_{\substack{m m' \\ \mu \mu'}} = (\Lambda \otimes I)_{\substack{m m' \\ n n'}, \substack{\mu \mu' \\ \nu \nu'}} (P_+)_{\substack{n n' \\ \nu \nu'}} =$$

$$\sum_{ij=1}^{dim(\mathcal{H}_A)} \Lambda_{\substack{m \mu \\ n \nu}} I_{\substack{m' \mu' \\ n' \nu'}} \delta_{in}\delta_{j\nu}\delta_{in'}\delta_{j\nu'} = \sum_{ij} \Lambda_{\substack{m \mu \\ n \nu}} \delta_{m'i}\delta_{\mu' j}\delta_{in}\delta_{j\nu}$$

$$= \Lambda_{\substack{m \mu \\ m' \mu'}} = (D_\Lambda)_{\substack{m m' \\ \mu \mu'}}.$$

□

2.3 Sistemas compostos e Emaranhamento

Sabendo como representar os estados de dois sistemas A e B, a mecânica quântica fornece uma receita para encontrarmos os objetos que representam os estados do sistema composto AB.

Postulado 29 (Sistemas compostos)**.** O espaço de Hilbert associado ao sistema composto AB é o produto tensorial dos espaços de Hilbert associados aos sistemas simples A e B.

Por esse motivo, as matrizes densidade do sistema AB pertencem ao conjunto[3] $M(\mathcal{H}_A \otimes \mathcal{H}_B) \equiv M(\mathcal{H}_A) \otimes M(\mathcal{H}_B)$ .Nesse conjunto distinguimos três tipos de matrizes densidade, as *fatoráveis* ou *decomponíveis*, as *separáveis* e as *emaranhadas*.

Definição 30. *Dizemos que uma matriz densidade $\rho \in M(\mathcal{H}_{AB})$ é decomponível se $\rho = \rho_A \otimes \rho_B$, com $\rho_A \in M(\mathcal{H}_A)$ e $\rho_B \in M(\mathcal{H}_B)$. Dizemos que ρ é separável se pode ser escrita como soma convexa de matrizes densidade decomponíveis:*

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i, \quad p_i \geq 0, \quad \sum_i p_i = 1,$$

com $\rho_A^i \in M(\mathcal{H}_A)$ e $\rho_b^i \in M(\mathcal{H}_B)$. Caso ρ não possa ser escrita dessa forma dizemos que ρ representa um estado emaranhado. O conjunto das matrizes densidade separáveis em $\mathcal{H}_{AB}$ será denotado por $S(\mathcal{H}_{AB})$.

[3] O isomorfismo que tomamos aqui é positivo e preserva o traço. Por essa razão, as matrizes densidade do sistema AB podem ser vistas como matrizes positivas de traço um em $M(\mathcal{H}_A) \otimes M(\mathcal{H}_B)$.

Segue que um estado puro de AB é emaranhado se não é um estado decomponível em $\mathcal{H}_A \otimes \mathcal{H}_B$.

Devemos também ter uma receita para fazer o caminho inverso. Dado o estado do sistema composto, seria possível associar um estado, e portanto uma matriz densidade, a cada sistema simples?

Postulado 31 (Matrizes densidade reduzidas)**.** Dada a matriz densidade ρ que descreve um sistema quântico composto AB, a matriz densidade ρ_A que descreve o sistema A é dada por

$$\rho_A = Tr_B(\rho),$$

e a matriz que ρ_B que descreve o sistema B é dada por

$$\rho_B = Tr_A(\rho).$$

A matriz ρ_A é chamada matriz densidade reduzida do sistema A e ρ_B é chamada matriz densidade reduzida do sistema B.

Muitos protocolos de computação e informação quântica dependem da presença de emaranhamento. Por essa razão, o emaranhamento passou a ser visto como um recurso valioso e começou-se a buscar critérios para identificar se um estado é ou não emaranhado.

2.3.1 Critérios de separabilidade

Um critério de separabilidade é um procedimento que aplicamos a uma matriz densidade que nos permite dizer se ela é separável ou emaranhada. Um bom critério seria aquele que fornecesse uma condição necessária e suficiente para separabilidade e que além disso fosse fácil de testar. Essas exigência são muito fortes para o caso geral.

2.3.2 Estados puros

Se estamos considerando apenas estados puros é fácil verificar separabilidade.

Teorema 19. *Um estado puro é separável se e somente se as matrizes densidade reduzidas ρ_A e ρ_B correspondem a estados puros.*

Demonstração. Basta utilizarmos a decomposição de Schmidt

$$|\psi\rangle = \sum_i a_i |ii\rangle.$$

Se $|\psi\rangle$ é fatorável então apenas um coeficiente de Schmidt a_j pode ser não nulo de modo que $\rho_A = |j\rangle\langle j|$ e $\rho_B = |j\rangle\langle j|$ são estados puros. Por outro lado, se dois ou mais coeficientes de Schmidt são não nulos então temos que

$$\rho_A = \sum_i a_i^2 |i\rangle\langle i|$$

é um estado misto. □

Testemunhas de Emaranhamento

O critério baseado em testemunhas de emaranhamento [20, 22] tem a propriedade adicional de possuir interpretação física e possivelmente implementação prática. Ele está relacionado com observáveis do sistema, e por isso pode ser verificado no laboratório.

Definição 32. *Um operador hermitiano $W \in \mathcal{L}(\mathcal{H})$ é chamado de testemunha de emaranhamento para um estado $\rho \in D(\mathcal{H})$ se*

$$Tr(W\rho) < 0, \quad Tr(W\sigma) \geq 0 \ \forall \ \sigma \ \in \ S(\mathcal{H}).$$

Toda testemunha de emaranhamento é uma matriz positiva por blocos. De fato, dados $|\psi_A\rangle \in \mathcal{H}_A$ e $|\psi_B\rangle \in \mathcal{H}_B$ temos

$$\langle\psi_B|\langle\psi_A|W|\psi_A\rangle|\psi_B\rangle = Tr(W|\psi_A\rangle|\psi_B\rangle\langle\psi_B|\langle\psi_A|) \geq 0.$$

Por outro lado, toda matriz W positiva por blocos mas não semidefinida positiva é uma testemunha de emaranhamento. Como W é positiva por blocos temos que $Tr(W\sigma) \geq 0$ para toda matriz densidade separável σ. Se W não é positiva então ela possui um autovalor negativo. Para o autovetor $|\psi\rangle$ associado temos

$$\langle\psi|W|\psi\rangle = Tr(W|\psi\rangle\langle\psi|) < 0.$$

Esse autovetor deve ser um estado emaranhado porque W é positiva por blocos. Logo W é uma testemunha de emaranhamento para $|\psi\rangle$.

Então toda testemunha é a matriz dinâmica de um mapa positivo mas não completamente positivo $\Lambda : M(\mathcal{H}_A) \to M(\mathcal{H}_B)$ e todo mapa positivo da mesma forma possui uma matriz dinâmica que é uma testemunha de emaranhamento.

Teorema 20. *Para todo estado emaranhado ρ existe uma testemunha de emaranhamento.*

Demonstração. Basta aplicarmos o Teorema de Hahn-Banach aos conjuntos convexos $S(\mathcal{H})$ e $\{\rho\}$ no espaço vetorial real formado pelas matrizes hermitianas cuja norma vem do produto interno definido por $(A, B) = Tr(AB)$. Assim, garantimos que existe um funcional linear f definido nesse espaço vetorial e uma constante c tais que $f(\sigma) \geq c \ \forall \ \sigma \in S(\mathcal{H})$ e $f(\rho) < c$. Como a norma vem de um produto interno, existe um elemento M tal que $f(A) = (A, M) \ \forall \ A$, de modo que

$$Tr(\sigma M) \geq c \ \forall \ \sigma \in S(\mathcal{H}), \quad Tr(\rho M) < c,$$

o que garante que $W = M - cI$ é uma testemunha de emaranhamento para ρ. □

Uma testemunha define um hiperplano em $D(\mathcal{H})$ dado pela equação $Tr(W\sigma) = 0$. Esse hiperplano separa ρ do conjunto $S(\mathcal{H})$. Uma testemunha é dita *ótima* se esse hiperplano toca a borda de $S(\mathcal{H})$. A interpretação física desse critério está no fato de que $Tr(W\sigma)$ é o valor médio do observável W no estado σ, o que permite encontrar maneiras experimentais de decidir se um estado é ou não emaranhado.

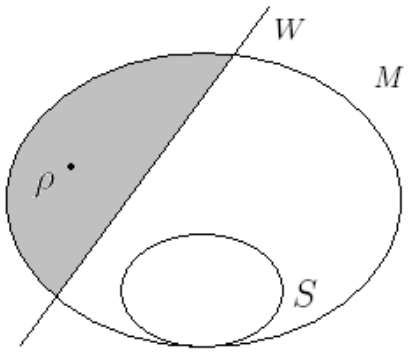


Figura 2.1: Testemuna de emaranhamento W para um estado emaranhado ρ

Critério de mapas positivos

Uma outra maneira de caracterizar estados emaranhados é através da ação de mapas positivos [20].

Teorema 21. *Um estado ρ é separável em $D(\mathcal{H}_{AB})$, se para todo mapa positivo $\Lambda : M(\mathcal{H}_A) \rightarrow M(\mathcal{H}_B)$, a imagem de ρ por $\Lambda \otimes I : M(\mathcal{H}_{AB}) \rightarrow M(\mathcal{H}_B \otimes \mathcal{H}_B)$ é uma matriz positiva.*

Demonstração. Se ρ é separável, então

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i,$$

$$\Lambda \otimes I(\rho) = \sum_i p_i \Lambda(\rho_A^i) \otimes \rho_B^i.$$

Como Λ é um mapa positivo, $\Lambda(\rho_A^i)$ é uma matriz positiva, de modo que $\Lambda \otimes I(\rho)$ é uma matriz positiva.

Suponhamos agora que $\Lambda \otimes I(\rho)$ seja uma matriz positiva para todo mapa positivo $\Lambda : M(\mathcal{H}_A) \rightarrow M(\mathcal{H}_B)$. Então $Tr(P\rho') \geq 0$ para todo projetor $P \in M(\mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{B})$. Tomamos então $P_+ = |\Phi_+\rangle\langle\Phi_+|$. Daí segue que

$$0 \leq Tr(P_+ \Lambda \otimes I(\rho)) = \langle P_+, \Lambda \otimes I(\rho)\rangle =$$

$$\langle (\Lambda \otimes I)^\dagger P_+, \rho\rangle.$$

O mapa $\Lambda^\dagger : M(\mathcal{H}_B) \rightarrow M(\mathcal{H}_A)$ também é um mapa positivo. De fato, $\Lambda^\dagger$ satisfaz a propriedade de levar matrizes hermitianas em matrizes hermitianas

$$\underset{n\nu}{\overset{m\mu}{\Lambda^\dagger}} = \underset{m\mu}{\overset{n\nu}{\Lambda^*}} = \underset{\mu m}{\overset{\nu n}{\Lambda^*}} = \underset{\nu n}{\overset{\mu m}{\Lambda^\dagger}} .$$

Além disso, sua matriz dinâmica também é positiva por blocos. De fato dados $|x\rangle \in \mathcal{H}_A$ e $|z\rangle \in \mathcal{H}_B$ temos

$$\langle z^*| \langle x| D_{\Lambda^\dagger} |x\rangle |z^*\rangle = x^*_m z_n (D_{\Lambda^\dagger})^{mn}_{\mu\nu} x_\mu z^*_\nu = z^*_\nu x_\mu (D_\Lambda)^{\nu\mu}_{nm} z_n x^*_m = \langle z| \langle x^*| D_\Lambda |z\rangle |x^*\rangle \geq 0,$$

em que usamos o fato de que $(D_{\Lambda^\dagger})^{mn}_{\mu\nu} = (D_\Lambda)^{\nu\mu}_{nm}$ e o fato de que D_Λ é positiva por blocos na última desigualdade. Daí temos então

$$0 \leq Tr(P_+ \Lambda \otimes I(\rho)) = \langle (\Lambda \otimes I)^\dagger P_+, \rho\rangle = \langle D_{\Lambda^\dagger}, \rho\rangle,$$

em que $D_{\Lambda^\dagger}$ é a matriz dinâmica de $\Lambda^\dagger$, que é positiva por blocos, e portanto uma testemunha de emaranhamento. Como para cada matriz hermitiana positiva por blocos W está associado um mapa positivo do qual W é a matriz dinâmica, segue que $Tr(W\rho) \geq 0$ pra toda testemunha W. Logo pelo critério de testemunhas temos que ρ é separável. □

Critério de Peres-Horodecki

Em [23], Asher Peres encontrou uma condição necessária para separabilidade. Ela se baseia no mapa transposição, dada uma escolha prévia de bases

$$T : M(\mathcal{H}_A) \to M(\mathcal{H}_A)$$
$$\rho \longmapsto \rho^T.$$

A extensão para o sistema composto AB, $T \otimes I$ é chamada de *transposição parcial*.

Proposição 8. *O mapa T é positivo mas não completamente positivo.*

Demonstração. Os autovalores de ρ^T são os mesmos de ρ o que implica a positividade de T. No entanto, já no caso de um sistema[4] 2×2 , ou seja, um sistema composto de dois subsistemas com espaço de estados de dimensão dois, temos

$$T \otimes I\left(|\Phi_+\rangle\langle\Phi_+|\right) = T \otimes I \left(\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

que não é uma matriz positiva. □

Teorema 22. *Se uma matriz densidade $\rho \in M(\mathcal{H}_A \otimes \mathcal{H}_B)$ é separável então $T \otimes I(\rho)$ é uma matriz densidade.*

Demonstração. Seja

$$\rho = \sum_i p_i \rho^i_A \otimes \rho^i_B,$$

de modo que

$$T \otimes I(\rho) = \sum_i p_i (\rho^i_A)^T \otimes \rho^i_B.$$

Como T é um mapa positivo e preserva o traço, $(\rho^i_A)^T$ é uma matriz densidade, de modo que $T \otimes I(\rho)$ também o é. □

[4] Chamaremos de sistema $m \times n$ um sistema composto de um subsistema de dimensão m e de um subsistema de dimensão n.

Os estados que possuem transposta parcial positiva são chamados estados PPT, da sigla em inglês para *Positive Partial Transpose.*

Esse é um critério bastante útil pois a transposta parcial de uma matriz densidade pode ser facilmente calculada. Além disso, para dimensões baixas, o critério é necessário e suficiente.

Teorema 23. *Uma matriz densidade ρ em um sistema 2×2 ou 2×3 é separável se, e somente se, sua transposta parcial também é uma matriz densidade, ou seja, para dimensões até 6, todo estado PPT é separável.*

A condição se torna suficiente nessas dimensões porque nesses casos todo mapa positivo mas não completamente positivo $\Lambda : M(\mathcal{H}_A) \to M(\mathcal{H}_B)$ pode ser decomposto na forma

$$\Lambda = \Lambda_1 + \Lambda_2 \circ T,$$

em que $\Lambda_i : M(\mathcal{H}_A) \to M(\mathcal{H}_B)$ são mapas completamente positivos. Desse modo se $\Lambda \otimes I$ leva uma matriz positiva em uma matriz não positiva, ele o faz porque a transposição parcial o faz, de modo que o critério de mapas positivos implica a suficiência do critério de Peres-Horodecki para essas dimensões [20].

Em dimensões maiores entretanto, existem estados emaranhados que são também PPT. Um exemplo pode ser encontrado em [21].

Finalizamos aqui nossa discussão sobre sistemas quânticos. Apresentamos apenas os príncipios básicos da mecânica quântica e para discussões mais aprofundadas sobre os postulados e suas motivações, recomendamos [24, 18]. Nossa atenção se voltou apenas para sistemas com espaços de estados de dimensão finita, que são normalmente utilizados em informação e computação quânticas. Muitos sistemas físicos possuem espaço de estados com dimensão infinita, como partículas presas em poços de potencial entre vários outros. Os primeiros exemplos herdados de análogos clássicos já apresentam essa característica. Referências sobre sistemas quânticos de dimensão infinita podem ser encontrados em [5, 6]. Informações sobre emaranhamento em sistemas de dimensão infinita podem ser encontradas em [25, 26]

Vimos aqui vários critérios de separabilidade para matrizes densidade. A principal motivação para estudarmos esses critério é a utilização do emaranhamento como um poderoso recurso em protocolos e algoritmos. Essa é a mesma motivação para tentarmos definir o que é um quantificador de emaranhamento, o que veremos no capítulo 4. No próximo capítulo estudaremos os sistemas quânticos de um e dois qubits, de grande importância para informação e computação quânticas e para os quais muitos resultados já foram encontrados.

CAPÍTULO 3

Os qubits

Nesse capítulo vamos estudar o sistema quântico mais simples e melhor entendido: o qubit. Ele também é o sistema quântico mais importante para as áreas de computação e informação quânticas, pois ele é o portador da informação, o análogo quântico do *bit*.

O qubit é a representação matemática de vários sistema físicos, às vezes depois de uma drástica simplificação. Exemplos são os graus de liberdade de polarização de um fóton e de spin de uma partícula de spin $1/2$. Um átomo ou uma mólecula também podem ser modelados através de um qubit, desde que apenas dois níveis de energia estejam acessíveis ao sistema.

Veremos também o sistema de dois qubits, o sistema mais simples que pode apresentar emaranhamento. Queremos estudar o efeito das chamadas operações de filtragem sobre os estados desse sistema e para isso os resultados sobre grupos de Lie serão utilizados. Como uma consequência, vamos demonstrar um resultado muito útil: a transposta parcial de uma matriz densidade de dois qubits tem no máximo um autovalor negativo. Apesar de simples, esse é um resultado não trivial. Não há nada que nos garanta a princípio que os casos com dois ou três autovalores negativos não sejam possíveis, mas veremos que de fato não são.

3.1 Os qubits e a Fibração de Hopf

Um *qubit* é um sistema quântico ao qual está associado um espaço de Hilbert de dimensão dois, comumente chamado de sistema quântico de *dois níveis*. O nome vem da analogia com o *sistema clássico de dois níveis*, que em computação clássica é chamado de bit. A mesma analogia justifica a notação utilizada para os vetores de uma base ortonormal do espaço de Hilbert do sistema: $|0\rangle$ e $|1\rangle$. Um vetor qualquer em $\mathcal{H}$ pode ser escrito na forma

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}.$$

Se considerarmos α e β como dois vetores em $\mathbb{R}^2$, os estados puros de um qubit podem ser vistos como pontos em $\mathbb{R}^4$. Como esses vetores possuem norma um, eles pertencem à esfera $S^3 \subset \mathbb{R}^4$. No entanto, muitos vetores diferentes em S^3 representam o mesmo estado físico, uma vez que cada estado é representado por uma classe de equivalência de vetores unitários.

Para eliminar essa redundância, desejamos encontar um conjunto em que cada ponto corresponda a um estado físico do sistema e em que cada estado do sistema corresponda a

um único ponto do conjunto. Para isso, vamos cobrir S^3 com círculos S^1, que são os loci dos pontos da forma $e^{i\phi}|\psi\rangle$, com $|\psi\rangle$ fixo. Para fazer essa cobertura, podemos usar a fibração de Hopf.

3.1.1 Fibrados

Uma *fibração* é definida por um mapa h que leva um espaço E em um espaço B, chamado *espaço base*. Um conjunto $F \subset E$ é chamado *fibra* se corresponde a $h^{-1}(p)$ para algum $p \in B$.

Um exemplo trivial é a projeção

$$h : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$$

$$h \left[\begin{array}{ccc} a & b & c \end{array} \right] = \left[\begin{array}{cc} a & b \end{array} \right].$$

As fibras são retas paralelas ao eixo z.

No caso da fibração de Hopf, $E = S^3$, $B = S^2$ e $F = S^1$. O mapa h é a composição de dois mapas h_1 e h_2 definidos da seguinte forma

$$h_1 : S^3 \longrightarrow \mathbb{R}^2 + \{\infty\}$$

$$\left[\begin{array}{cc} \alpha & \beta \end{array} \right] \longmapsto C = \alpha\bar{\beta}^{-1},$$

$$h_2 : \mathbb{C} \cup \{\infty\} \longrightarrow S^2$$

$$C \longmapsto \Pi_E^{-1}(C),$$

em que $\Pi_E : S^2 \to \mathbb{C} \cup \{\infty\}$ denota a projeção estereográfica

$$\Pi_E \left[\begin{array}{ccc} a & b & c \end{array} \right] = \left[\begin{array}{cc} \frac{a}{1-c} & \frac{b}{1-c} \end{array} \right].$$

Geometricamente, a projeção estereográfica tem um significado bem interessante. Tomamos um ponto na esfera S^2 $q = \left[\begin{array}{ccc} a & b & c \end{array} \right]$ e construímos a reta que liga esse ponto ao polo norte $p = \left[\begin{array}{ccc} 0 & 0 & 1 \end{array} \right]$

$$\left[\begin{array}{ccc} ta & tb & t(c-1)+1 \end{array} \right], \quad t \in \mathbb{R}.$$

A projeção estereográfica leva q na interseção dessa reta com o plano $z = 0$. O polo norte é levado ao ponto no infinito.

Temos então

$$h_2 \left[\begin{array}{cc} x & y \end{array} \right] = \left[\begin{array}{ccc} \frac{2x}{x^2+y^2+1} & \frac{2y}{x^2+y^2+1} & \frac{x^2+y^2-1}{x^2+y^2+1} \end{array} \right].$$

Escrevendo $\alpha = r_1 e^{i\phi_1}$ e $\beta = r_2 e^{i\phi_2}$, temos

$$C = h_1 \left[\begin{array}{cc} \alpha & \beta \end{array} \right] = \frac{r_1}{r_2} \left[\begin{array}{cc} cos(\phi_2 - \phi_1) & sen(\phi_2 - \phi_1) \end{array} \right].$$

Assim

$$h(|\psi\rangle) = h_2(C) = \left[\begin{array}{ccc} \frac{2r_1 r_2 cos(\phi_2-\phi_1)}{r_1^2+r_2^2} & \frac{2r_1 r_2 sen(\phi_2-\phi_1)}{r_1^2+r_2^2} & \frac{r_1^2+r_2^2}{r_1^2+r_2^2} \end{array} \right]$$

$$= \left[\begin{array}{ccc} 2\mathrm{Re}\left(\alpha\bar{\beta}\right) & 2\mathrm{Im}\left(\alpha\bar{\beta}\right) & |\alpha|^2 - |\beta|^2 \end{array} \right] = \left[\begin{array}{ccc} \langle\sigma_1\rangle & \langle\sigma_2\rangle & \langle\sigma_3\rangle \end{array} \right],$$

em que

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

são chamados operadores de Pauli.

As fibras do mapa h são as fibras do mapa h_1 pois h_2 é bijetivo. Essas fibras são as classes de equivalência $\{e^{i\phi}|\psi\rangle\}$ e aplicando o mapa de Hopf h a redundância na fase global é eliminada, como desejávamos. Assim podemos tomar a esfera S^2, que chamamos de *esfera de Bloch*, como sendo o conjunto de estados puros do sistema quântico de um qubit.

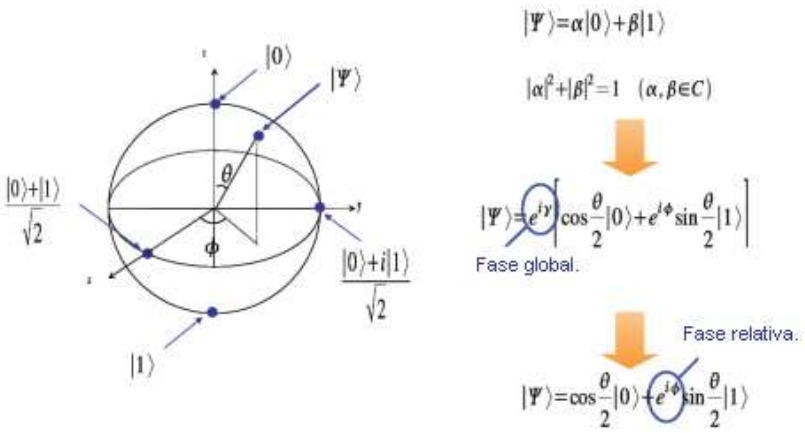


Figura 3.1: Esfera de Bloch e representação de um estado de um qubit.

A fibração de Hopf e a esfera de Bloch estão relacionadas à representação de estados puros através de espaços projetivos. Toda a mecânica quântica pode ser formulada nessa versão projetiva como pode ser visto em [27]. Para mais detalhes sobre a fibração de Hopf e a esfera de Bloch, veja [11, 28, 29, 30].

3.1.2 Estados mistos de um qubit

Um estado geral de um qubit é representado por uma matriz densidade 2×2. O conjunto das matrizes hermitianas é um espaço vetorial real e uma base para esse espaço é formado pelas matrizes de Pauli juntamente com a matriz identidade I. Desse modo, uma matriz densidade de um qubit pode ser sempre escrita na forma

$$\rho = \frac{1}{2}\left(I + a\sigma_1 + b\sigma_2 + c\sigma_3\right).$$

O coeficiente de I deve ser $1/2$ porque ela é a única matriz da base que tem traço não nulo, igual a dois, e $Tr(\rho) = 1$. Agora devemos impor condições ao vetor $\begin{bmatrix} a & b & c \end{bmatrix}$ para

que a matriz seja positiva. Em forma matricial temos

$$\rho = \frac{1}{2}\begin{bmatrix} 1+c & a-ib \\ a+ib & 1-c \end{bmatrix}.$$

Para que ρ seja uma matriz positiva é necessário e suficiente que $det(\rho) \geq 0$, uma vez que $Tr(\rho) \geq 0$. Essa condição é equivalente a

$$a^2 + b^2 + c^2 \leq 1.$$

Logo podemos fazer uma associação bijetiva entre matrizes densidade de um qubit e pontos na bola de raio um em $\mathbb{R}^3$. Os pontos na esfera S^2 correspondem às matrizes que possuem determinante igual a zero, que nesse caso são exatamente os estados puros. Essa associação coincide com a que fizemos na seção anterior utilizando a fibração de Hopf.

3.1.3 Dois qubits

O sistema de dois qubits é o sistema mais simples que apresenta emaranhamento. O espaço de estados do sistema é $\mathbb{C}^2 \otimes \mathbb{C}^2$ e as matrizes densidade são matrizes positivas de traço um que pertencem a $M(\mathbb{C}^2) \otimes M(\mathbb{C}^2)$. Como as matrizes de Pauli formam uma base para o espaço vetorial formado pelas matrizes hermitianas 2×2, uma base para o espaço vetorial formado pelas matrizes hermitianas 4×4 é o conjunto formado pelas matrizes[1] $I, I \otimes \sigma_i, \sigma_i \otimes I, \sigma_i \otimes \sigma_j$, de modo que uma matriz densidade de dois qubits pode ser escrita na forma

$$\rho = \frac{1}{4}\left(I + \sum_i R_{0i} I \otimes \sigma_i + \sum_i R_{i0}\sigma_i \otimes I + \sum_{ij} R_{ij}\sigma_i \otimes \sigma_j\right)$$

$$R_{ij} = Tr(\sigma_i \otimes \sigma_j \rho).$$

Assim, podemos representar uma matriz densidade de dois qubits também através da matriz R cujas entradas são os coeficientes R_{ij} que aparecem na igualdade anterior, com $R_{00} = 1/4$.

Realizando o traço parcial em relação ao primeiro subsistema, vemos que o vetor

$$\begin{bmatrix} R_{01} & R_{02} & R_{03} \end{bmatrix}$$

é o vetor de Bloch da matriz densidade reduzida do segundo subsistema. Já se fizermos o traço parcial em relação ao segundo subsistema, veremos que o vetor

$$\begin{bmatrix} R_{10} & R_{20} & R_{30} \end{bmatrix}$$

é o vetor de Bloch da matriz densidade reduzida do primeiro subsistema.

Infelizmente, as condições que devemos impor aos outros coeficientes para que a matriz seja positiva não são tão facilmente encontradas, a não ser se estudarmos casos especiais como por exemplo o conjunto dos chamados estados T [31].

[1] Estamos usando o símbolo I para representar tanto a matriz identidade 2×2 assim como a matriz identidade 4×4.

Seja D o conjunto das matrizes

$$\frac{1}{4}\left(I+\sum_i R_{0i}I\otimes\sigma_i+\sum_i R_{i0}\sigma_i\otimes I+\sum_{ij}R_{ij}\sigma_i\otimes\sigma_j\right)$$

tais que a matriz R_{ij}, $i,j=1,\dots 3$ seja diagonal.

Proposição 9. *Se $M\in D$ então $M^\dagger=M$ e $Tr(M)=1$. Se além disso ela é uma matriz densidade de dois qubits, então o vetor $r=\left[\begin{array}{ccc} R_{11} & R_{22} & R_{33}\end{array}\right]$ pertence ao tetraedo T cujos vértices são os pontos*

$$\left[\begin{array}{ccc} -1 & -1 & -1\end{array}\right],\quad \left[\begin{array}{ccc} -1 & 1 & 1\end{array}\right],\quad \left[\begin{array}{ccc} 1 & -1 & 1\end{array}\right],\quad \left[\begin{array}{ccc} 1 & 1 & -1\end{array}\right].$$

Demonstração. Se a matriz é positiva, então $Tr(MP)\geq 0$ para todo projetor P. Tomando os projetores na direção dos quatro vetores chamados estados de Bell

$$|\Phi_\pm\rangle = \frac{|00\rangle\pm|11\rangle}{\sqrt{2}}, \tag{3.1}$$

$$|\Psi_\pm\rangle = \frac{|01\rangle\pm|10\rangle}{\sqrt{2}}, \tag{3.2}$$

obtemos as quatro equações

$$\begin{aligned} 1-R_{11}-R_{22}-R_{33}&\geq 0,\\ 1-R_{11}+R_{22}+R_{33}&\geq 0,\\ 1+R_{11}-R_{22}+R_{33}&\geq 0,\\ 1+R_{11}+R_{22}-R_{33}&\geq 0,\end{aligned}$$

que definem justamente o tetraedro T. □

Se além das restrições já impostas também exigirmos que os vetores

$$v_1=\left[\begin{array}{ccc} R_{10} & R_{20} & R_{30}\end{array}\right],\quad v_2=\left[\begin{array}{ccc} R_{01} & R_{02} & R_{03}\end{array}\right]$$

sejam nulos, ou seja, que ambas as matrizes densidade reduzidas sejam a identidade, então a condição acima além de necessária é suficiente. Estados com essa propriedade são chamados *estados T*.

Proposição 10. *Uma matriz M em D com v_1 e v_2 nulos é uma matriz densidade de dois qubits se, e somente se, o vetor r pertence ao tetraedro T.*

Demonstração. Já sabemos que a condição é necessária. Para vermos que é suficiente, basta notarmos que toda matriz dessa forma é uma combinação convexa das quatro matrizes com v_1 e v_2 nulos e cujos vetores r são os vértices do tetraedro. Essas quatro matrizes são exatamente as matrizes densidade dos estados de Bell, de modo que M é combinação convexa de matrizes densidade e portanto também é uma matriz densidade. □

Como ilustração do critério de Peres-Horodecki, vamos tentar encontrar o conjunto dos estados T separáveis.

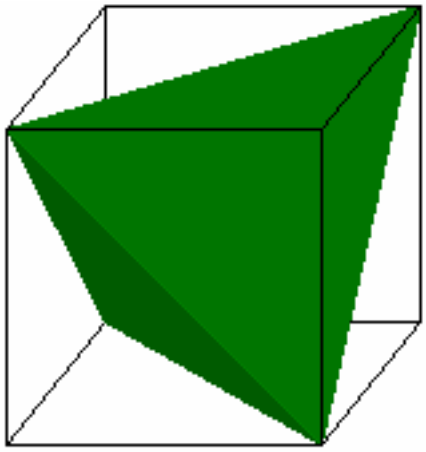


Figura 3.2: Tetraedro T.

Proposição 11. *Se uma matriz M em D é uma matriz densidade separável, então o vetor r deve pertencer ao octaedro O cujos vértices são os pontos*

$$\begin{bmatrix} \pm 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & \pm 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & \pm 1 \end{bmatrix}.$$

Demonstração. O efeito da transposição parcial da matriz densidade sobre o vetor r é trocar o sinal da coordenada R_{22}. Desse modo, o vetor r da transposta parcial deve pertencer ao tetraedro T' cujos vértices são

$$\begin{bmatrix} -1 & 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & -1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & -1 & -1 \end{bmatrix}.$$

Para que a transposta parcial seja positiva, esse vetor deve pertencer a T também. Logo, se M é separável, seu vetor r pertence a $T \cap T'$, que é justamente o octaedro O (vide fig. 3.1.3). □

Como consequência da proposição anterior, vale o seguinte resultado para estados T:

Proposição 12. *Um estado T é separável se, e somente se, seu vetor r pertence ao octaedro O.*

Daqui em diante, nossa atenção se voltará principalmente para o sistema de dois qubits.

3.2 Operações de filtragem em sistemas de dois qubits

Nessa seção, vamos estudar as chamadas *operações de filtragem* ou *operações locais estocásticas com comunicação clássica*, SLOCC [2]. Nosso intuito é encontrar um conjunto pequeno de *formas normais* para a matriz densidade utilizando essas operações, ou seja, queremos encontrar formas simples de matrizes densidades tais que qualquer matriz densidade pode ser levada a uma delas através de operações SLOCC [2, 32].

[2] Do termo em inglês *Stochastic Local Operations and Classical Comunication*

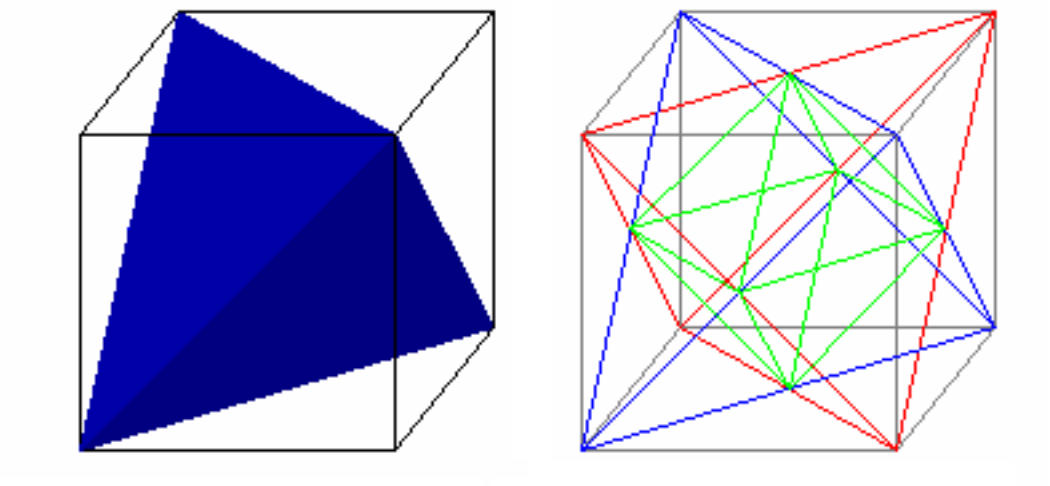
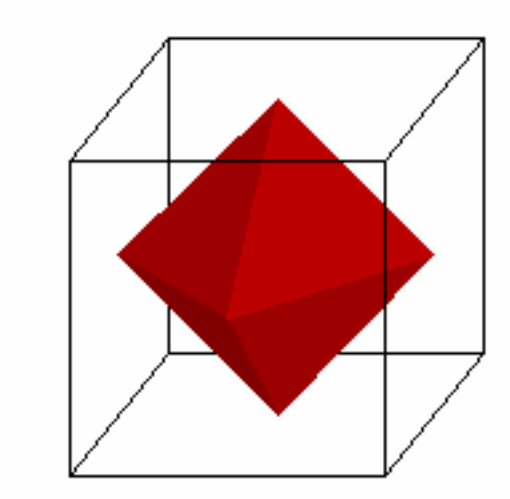


Figura 3.3: À esquerda: o tetraedro T'. À direita: a interseção dos tetraedros T e T', que resulta no octaedro O.



Definição 33. *As operações SLOCC são operações da forma:*

$$\rho' = \frac{(A \otimes B)\rho(A \otimes B)^\dagger}{Tr[(A \otimes B)\rho(A \otimes B)^\dagger]} \tag{3.3}$$

em que A e B satisfazem as seguintes condições [3]*:*

- $A^\dagger A \leq I$ *e* $B^\dagger B \leq I$;
- $detA \neq 0$ *e* $detB \neq 0$.

[3] Usaremos a notação $A \leq B$ para indicar que $B - A$ é uma matriz positiva semi-definida.

A primeira exigência está relacionada ao fato de que queremos enxergar essas operações como um resultado possível de um POVM. Por isso o termo *stochastic*, pois a operação não é feita deterministicamente, mas sim com alguma probabilidade dada por $Tr[(A\otimes B)\rho(A\otimes B)^\dagger]$. Não vamos nos preocupar aqui com as probabilidades, mas apenas com o efeito da operação sobre a matriz densidade. Por isso, essa restrição é menos importante uma vez que estamos dividindo pelo termo $Tr[(A\otimes B)\rho(A\otimes B)^\dagger]$ e não vamos nos preocupar muito com ela. A segunda restrição é apenas uma questão de conveniência. Para nossos propósitos é interessante e também suficiente considerarmos apenas matrizes com determinante não nulo.

Nossa primeira preocupação é entender qual transformação sofre a matriz R quando aplicamos uma operação do tipo 3.3 à matriz ρ.

Teorema 24. *A matriz $R=(R_{ij})$ se transforma sob a ação de transformações do tipo 3.3 da seguinte maneira, a menos de normalização:*

$$R' = L_A R L_B^T$$

em que

$$\begin{aligned} L_A &= \frac{T(A\otimes A^*)T^\dagger}{|detA|}, \\ L_B &= \frac{T(B\otimes B^*)T^\dagger}{|detB|}, \\ T &= \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & i & -i & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}. \end{aligned}$$

Além disso, L_A e L_B são tansformações de Lorentz próprias ortócronas.

Demonstração. A demonstração pode ser dividida em quatro partes.

- **1° passo:** Mostrar que $R = 4T\tilde{\rho}T^T$, em que $\tilde{\rho}$ é obtida escrevendo-se os índices de ρ, que podemos pensar como variando de 0 a 3, em base binária e definindo-se $\tilde{\rho}_{kl,k'l'} = \rho_{kk',ll'}$.

  Desse modo temos:

$$\rho = \begin{bmatrix} \rho_{00} & \rho_{01} & \rho_{02} & \rho_{03} \\ \rho_{10} & \rho_{11} & \rho_{12} & \rho_{13} \\ \rho_{20} & \rho_{21} & \rho_{22} & \rho_{23} \\ \rho_{30} & \rho_{31} & \rho_{32} & \rho_{33} \end{bmatrix} = \begin{bmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{00,10} & \rho_{00,11} \\ \rho_{01,00} & \rho_{01,01} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{10,10} & \rho_{10,11} \\ \rho_{11,00} & \rho_{11,01} & \rho_{11,10} & \rho_{11,11} \end{bmatrix}.$$

  E, portanto,

$$\tilde{\rho} = \begin{bmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{01,00} & \rho_{01,01} \\ \rho_{00,10} & \rho_{00,11} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{11,00} & \rho_{11,01} \\ \rho_{10,10} & \rho_{10,11} & \rho_{11,10} & \rho_{11,11} \end{bmatrix} = \begin{bmatrix} \rho_{00} & \rho_{01} & \rho_{10} & \rho_{11} \\ \rho_{02} & \rho_{03} & \rho_{12} & \rho_{13} \\ \rho_{20} & \rho_{21} & \rho_{30} & \rho_{31} \\ \rho_{22} & \rho_{23} & \rho_{32} & \rho_{33} \end{bmatrix}.$$

  O cálculo de $T\tilde{\rho}T^T$ fornece:

$$\begin{bmatrix} \rho_{00}+\rho_{11}+\rho_{22}+\rho_{33} & \rho_{01}+\rho_{23}+\rho_{10}+\rho_{32} & i(\rho_{01}+\rho_{23}-\rho_{10}-\rho_{32}) & \rho_{00}-\rho_{11}+\rho_{22}-\rho_{33} \\ \rho_{02}+\rho_{20}+\rho_{13}+\rho_{31} & \rho_{03}+\rho_{21}+\rho_{12}+\rho_{30} & i(\rho_{03}+\rho_{21}-\rho_{12}-\rho_{30}) & \rho_{02}+\rho_{20}-\rho_{13}-\rho_{31} \\ i(\rho_{02}+\rho_{13}-\rho_{20}-\rho_{31}) & i(\rho_{03}-\rho_{21}+\rho_{12}-\rho_{30}) & -\rho_{03}+\rho_{21}+\rho_{12}-\rho_{30} & i(\rho_{02}-\rho_{20}-\rho_{13}+\rho_{31}) \\ \rho_{00}+\rho_{11}-\rho_{22}-\rho_{33} & \rho_{01}-\rho_{23}+\rho_{10}-\rho_{32} & i(\rho_{01}-\rho_{23}-\rho_{10}+\rho_{32}) & \rho_{00}-\rho_{11}-\rho_{22}+\rho_{33} \end{bmatrix}.$$

O elemento ij dessa matriz é justamente $R_{ij} = Tr[\sigma_i \otimes \sigma_j \rho]$, como queríamos mostrar.

- **2° passo:** Mostrar que $\tilde{\rho}$ se transforma da seguinte forma:

$$\tilde{\rho}' = (A \otimes A^*)\tilde{\rho}(B \otimes B^*)^T.$$

De fato,

$$\begin{aligned}
\tilde{\rho}'_{kl,k'l'} = \rho'_{kk',ll'} &= \sum_{ii'} (A \otimes B)_{kk',ii'} \cdot (\rho(A \otimes B)^\dagger)_{ii',ll'} \\
&= \sum_{ii'jj'} (A \otimes B)_{kk',ii'} \cdot \rho_{ii',jj'} \cdot (A \otimes B)^\dagger_{jj',ll'} \\
&= \sum_{ii'jj'} (A \otimes B)_{kk',ii'} \cdot \rho_{ii',jj'} \cdot (A \otimes B)^*_{ll',jj'} \\
&= \sum_{ii'jj'} A_{ki} B_{k'i'} \cdot \rho_{ii',jj'} \cdot A^*_{lj} B^*_{l'j'} \\
&= \sum_{ii'jj'} A_{ki} A^*_{lj} \cdot \tilde{\rho}_{ij,i'j'} \cdot B_{k'i'} B^*_{l'j'} \\
&= \sum_{ii'jj'} (A \otimes A^*)_{kl,ij} \cdot \tilde{\rho}_{ij,i'j'} \cdot (B \otimes B^*)_{k'l',i'j'} \\
&= \sum_{ii'jj'} (A \otimes A^*)_{kl,ij} \cdot \tilde{\rho}_{ij,i'j'} \cdot (B \otimes B^*)^T_{i'j',k'l'} \\
&= (A \otimes A^*)\tilde{\rho}(B \otimes B^*)^T_{kl,k'l'}.
\end{aligned}$$

No cálculo acima utilizamos

$$(M \otimes N)_{ii',jj'} = M_{i,j} N_{i',j'}.$$

Essa notação é conveniente pois se aproveita do fato de que se M e N são matrizes $n \times n$ então $M \otimes N$ é $n^2 \times n^2$ e o número de dígitos dos índices de $M \otimes N$ escritos na base 2 é duas vezes o número de dígitos dos índices de M e N.

- **3° passo:** Mostrar que

$$R' = |det(A)||det(B)| L_A R L_B^T.$$

Como provado no 1° passo, temos:

$$R' = 4T\tilde{\rho}'T^T.$$

Pelo 2° passo temos:

$$R' = 4T(A \otimes A^*)\tilde{\rho}(B \otimes B^*)^T T^T$$

Como $\tilde{\rho} = \frac{1}{4} T^\dagger R (T^\dagger)^T$, vale:

$$\begin{aligned}
R' &= T(A \otimes A^*)T^\dagger R (T^\dagger)^T (B \otimes B^*)^T T^T \\
&= \left(\frac{T(A \otimes A^*)T^\dagger}{|detA|}\right) R \left(\frac{T(B \otimes B^*)T^\dagger}{|detB|}\right)^T |detA||detB| \\
&= |det(A)||det(B)| L_A R L_B^T.
\end{aligned}$$

- **4° passo:** Mostrar que L_A e L_B são transformações de Lorentz próprias ortócronas.

  Primeiramente observamos que $T^\dagger M T^* = -\sigma_2 \otimes \sigma_2$ e que $A\sigma_2 A^T = det(A)\sigma_2$. Desse modo,

$$\begin{aligned} L_A M L_A^T &= \frac{T(A\otimes A^*)T^\dagger M T^* (A\otimes A^*)^T T^T}{|det(A)|^2} \\ &= \frac{-T(A\otimes A^*)\sigma_2\otimes\sigma_2 (A\otimes A^*)^T T^T}{|det(A)|^2} \\ &= -T\sigma_2\otimes\sigma_2 T^T \left(\frac{det(A)det(A^*)}{|det(A)|^2}\right) = -T\sigma_2\otimes\sigma_2 T^T = M. \end{aligned}$$

  Claramente $det(L_A) = det(L_B) = 1$ uma vez que $det(T) = 1$. O elemento 00 de L_A é $|A_{0,0}|^2 + |A_{0,1}|^2 + |A_{1,0}|^2 + |A_{1,1}|^2$, que é sempre positivo, o mesmo valendo para L_B. Logo L_A e L_B são transformações de Lorentz próprias ortócronas.

□

O próximo passo é mostrar que toda matriz de Lorentz é da forma L_A para alguma matriz A de determinante diferente de zero. Para isso, basta considerar $A \in SL(2,\mathbb{C})$ e utilizar o teorema 6.

Em vista do teorema anterior, uma pergunta natural é se podemos encontrar uma decomposição para a matriz R na forma

$$R = L_1 \Sigma L_2^T,$$

em que L_1 e L_2 são transformações de Lorentz próprias ortócronas e Σ é uma matriz da forma mais "simples"possível. Por exemplo, seria ótimo se pudéssemos obter Σ diagonal. Não conseguimos obter uma simplificação tão grande, mas veremos que é possível chegar bem perto disso.

Lema 4. *Seja A uma matriz $n\times n$ positiva semidefinida. Então existe uma matriz $O \in O(n,\mathbb{C})$ e uma matriz da forma $J(A) = \Lambda \oplus \Gamma$ em que*

$$\Lambda = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{n-2r} \end{bmatrix}$$

$$\Gamma = \begin{bmatrix} Q & 0 & \cdots & 0 \\ 0 & Q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Q \end{bmatrix},$$

com $Q = \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}$ *e* $r = posto(A) - posto(AA^*)$ *tais que:*

$$A = OJ(A)O^\dagger.$$

Para uma demonstração desse resultado, veja [33]. Podemos agora provar o seguinte resultado:

Teorema 25. *A matriz R cujos elementos são $R_{ij} = Tr(\rho \cdot \sigma_i \otimes \sigma_j)$ pode ser escrita na forma*

$$R = L_1 \Sigma L_2^T,$$

em que L_1 e L_2 são transformações de Lorentz próprias e ortócronas e Σ é uma matriz de uma das seguintes formas:

$$\begin{bmatrix} \lambda_0+\lambda_1+\lambda_2+\lambda_3 & 0 & 0 & 0 \\ 0 & \lambda_0-\lambda_3+\lambda_1-\lambda_2 & 0 & 0 \\ 0 & 0 & -\lambda_0+\lambda_3+\lambda_2-\lambda_1 & 0 \\ 0 & 0 & 0 & \lambda_0+\lambda_3-\lambda_1-\lambda_2 \end{bmatrix} \tag{3.4}$$

$$\begin{bmatrix} \lambda_0+\lambda_1+2 & 0 & 0 & -2 \\ 0 & \lambda_0-\lambda_1 & 0 & 0 \\ 0 & 0 & -\lambda_0+\lambda_1 & 0 \\ 2 & 0 & 0 & \lambda_0+\lambda_1-2 \end{bmatrix}, \tag{3.5}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3.6}$$

$$\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{3.7}$$

Demonstração. Definimos $\tilde{\rho} = B\rho B^\dagger$, em que

$$B = 1/2 \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & i & i & 0 \\ 0 & -1 & 1 & 0 \\ i & 0 & 0 & -i \end{bmatrix}.$$

Pela lei de inércia de Sylvester, $\tilde{\rho}$ é uma matriz positiva definida. Pelo lema 1, existe uma matriz ortogonal O tal que $O\tilde{\rho}O^\dagger$ possui uma das seguintes formas:

$$\begin{bmatrix} \lambda_0 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 \\ 0 & 0 & 0 & \lambda_3 \end{bmatrix}, \quad \begin{bmatrix} \lambda_0 & 0 & 0 & 0 \\ 0 & 1 & -i & 0 \\ 0 & i & 1 & 0 \\ 0 & 0 & 0 & \lambda_1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & -i \\ 0 & 1 & -i & 0 \\ 0 & i & 1 & 0 \\ i & 0 & 0 & 1 \end{bmatrix}. \tag{3.8}$$

Para garantir que $O \in SO(4, \mathbb{C})$ devemos ainda adicionar a forma[4]:

$$\begin{bmatrix} 1 & 0 & 0 & i \\ 0 & 1 & -i & 0 \\ 0 & i & 1 & 0 \\ -i & 0 & 0 & 1 \end{bmatrix}. \tag{3.9}$$

[4]Se O possui determinante negativo, basta multiplicarmos O pela matriz P que troca o sinal da primeira coordenada para obtermos uma matriz de determinante positivo. $OP\tilde{\rho}P^\dagger O^\dagger$ é igual a $O\tilde{\rho}O^\dagger$ depois que trocamos o sinal da primeira linha e em seguida o sinal da primeira coluna.

Quando submetemos $\tilde{\rho}$ a uma transformação ortogonal, ρ será modificada:

$$\rho' = B^\dagger \tilde{\rho}' B = B^\dagger O \tilde{\rho} O^\dagger B = B^\dagger O B \rho B^\dagger O^\dagger B.$$

Dada uma transformação $O \in SO(4,\mathbb{C})$, sabemos pelo Lema 5 que existe uma transformação $A_1 \otimes A_2 \in SL(2,\mathbb{C}) \otimes SL(2,\mathbb{C})$ tal que $A_1 \otimes A_2 = B^\dagger O B$. Logo, a transformação sofrida pela matriz densidade será da forma:

$$\rho' = (A_1 \otimes A_2)\rho(A_1 \otimes A_2)^\dagger$$

que é uma operação de filtragem. Logo a transformação correspondente em R é

$$R = L_{A_1} \Sigma L_{A_2}^T,$$

em que L_{A_1} e L_{A_2} são como no teorema 1 e portanto são transformações de Lorentz próprias e ortócronas. As matrizes densidade correspondentes às matrizes em (3.8) e (3.9) são, respectivamente:

$$\begin{bmatrix} 1/2(\lambda_0+\lambda_3) & 0 & 0 & 1/2(\lambda_0-\lambda_3) \\ 0 & 1/2(\lambda_1+\lambda_2) & 1/2(\lambda_1-\lambda_2) & 0 \\ 0 & 1/2(\lambda_1-\lambda_2) & 1/2(\lambda_1+\lambda_2) & 0 \\ 1/2(\lambda_0-\lambda_3) & 0 & 0 & 1/2(\lambda_0+\lambda_3) \end{bmatrix}, \tag{3.10}$$

$$\begin{bmatrix} 1/2(\lambda_0+\lambda_1) & 0 & 0 & 1/2(\lambda_0-\lambda_1) \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2(\lambda_0-\lambda_1) & 0 & 0 & 1/2(\lambda_0+\lambda_1) \end{bmatrix}, \tag{3.11}$$

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3.12}$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}. \tag{3.13}$$

Calculando as matrizes R correspondentes, obtemos, respectivamente, as matrizes (3.4)-(3.7), como queríamos mostrar. □

Corolário 4. *A transposta parcial de qualquer matriz densidade de um sistema de dois qubits possui no máximo um autovalor negativo.*

Demonstração. Quando aplicamos uma operação SLOCC à matriz densidade, a transposta parcial sofrerá a seguinte transformação:

$$\rho'^{t_1} = (A^* \otimes B)\rho^{t_1}(A^* \otimes B)^\dagger.$$

De fato, temos:

$$\begin{aligned}
\rho'^{t_1}_{kl,k'l'} = \rho'_{k'l,Kl'} &= ((A\otimes B)\rho(A\otimes B)^\dagger)_{k'l,kl'} \\
&= \sum_{ii'jj'} (A\otimes B)_{k'l,ii'}\cdot\rho_{ii',jj'}\cdot(A\otimes B)^\dagger_{jj',kl'} \\
&= \sum_{ii'jj'} (A\otimes B)_{k'l,ii'}\cdot\rho_{ii',jj'}\cdot(A\otimes B)^*_{kl',jj'} \\
&= \sum_{ii'jj'} A_{k'i}B_{li'}\cdot\rho^{t_1}_{ji',ij'}\cdot A^*_{kj}B^*_{l'j'} \\
&= \sum_{ii'jj'} A^*_{kj}B_{li'}\cdot\rho^{t_1}_{ji',ij'}\cdot A_{k'i}B^*_{l'j'} \\
&= \sum_{ii'jj'} (A^*\otimes B)_{kl,ji'}\cdot\rho^{t_1}_{ji',ij'}\cdot(A^*\otimes B)^\dagger_{k'l',ij'} \\
&= (A^*\otimes B)\rho^{t_1}(A^*\otimes B)^\dagger_{kl,k'l'}.
\end{aligned}$$

Como toda matriz densidade pode ser levada a uma das formas (3.10) - (3.13) e a transposta parcial de cada uma delas possui apenas um autovalor negativo, temos pela lei de inércia de Sylvester que a transposta parcial de qualquer matriz densidade possui apenas um autovalor negativo. □

Com esse importante resultado encerramos nosso estudo do espaço de estados de um e dois qubits. Como vimos, apesar de serem sistemas simples, os espaços de estados já apresentam uma geometria rica, mesmo em casos especiais como os estados puros de um qubit ou os estados T. É possível encontrar uma parametrização bem interessante para os estados puros de dois qubits, que envolve a fibração de Hopf de S^7 com base S^4, mas infelizmente não vamos apresentá-la aqui [30]. Mais detalhes sobre geometria de estados quânticos podem ser encontrados nas referências já citadas, em especial em [11].

CAPÍTULO 4

Quantificadores de Emaranhamento bipartite

Se o emaranhamento pode ser usado como um recurso para várias tarefas [34, 35, 36, 37], então é importante sabermos quanto dele possuímos. Como quantificar o emaranhamento?

Essa não é uma pergunta fácil de ser respondida. Mesmo para o caso de dois qubits, o sistema mais simples possível em que há emaranhamento, existem vários quantificadores diferentes.

Existem muitas maneiras de tentarmos definir um quantificador de emaranhamento. Alguns deles são baseados em uma distância no espaço de estados, outros em propriedades geométricas do espaço de estados, outros em critérios operacionais e interpretações físicas. Veremos nesse capítulo os principais quantificadores de emaranhamento bipartite, em especial a *concorrência* e a *negatividade*, para o sistema de dois qubits.

4.1 Estados puros

Decidir se um estado puro $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ é decomponível ou não é uma tarefa fácil: basta encontrarmos a matriz densidade reduzida de um dos subsistemas e verificar se ela corresponde a um estado puro ou não. Com a utilização do emaranhamento em protocolos de computação e informação quântica, ficou claro que nem todos os estados são igualmente úteis. Assim, surgiu a questão de quantificar o emaranhamento presente em um dado estado do sistema.

Quantificar o emaranhamento é uma questão bem mais complicada. Como o emaranhamento está relacionado de alguma forma às correlações quânticas entre os dois subsistemas, a propriedade mais importante que uma função $E : \mathcal{H}_1 \otimes \mathcal{H}_2 \to \mathbb{R}_+$ deve satisfazer para ser considerada um bom quantificador é não aumentar quando aplicamos as chamadas operações LOCC.

Definição 34. *Suponhamos que um sistema físico consista de dois subsistemas. Uma operação LOCC (*Local Operations and Classical Comunication*) nesse sistema é uma operação em que cada parte age apenas em seu subsistema e em que há apenas troca de informação clássica.*

Em geral, uma operação LOCC pode ser descrita por diversos passos, sendo que cada qual consiste de uma medição em uma das partes e da aplicação de um mapa completamente positivo na outra parte, que depende do resultado da medição realizada.

Se E representa um quantificador de emaranhamento, então

Propriedade 1. *E não deve aumentar por LOCC, ou seja, se Λ é uma operação LOCC então*

$$E(\Lambda(|\psi\rangle)) \leq E(|\psi\rangle).$$

Se E obedece esse critério, dizemos que E é um monótono de emaranhamento. Se E é um monótono de emaranhamento, então E é invariante por unitárias locais, ou seja

$$E(U_A \otimes U_B|\psi\rangle) = E(|\psi\rangle).$$

Essa é uma Propriedade que decorre da Propriedade 1. De fato, uma operação unitária local é uma operação LOCC de modo que

$$E(U_A \otimes U_B|\psi\rangle) \leq E(|\psi\rangle).$$

Por outro lado, a inversa de uma unitária local também é uma unitária local e

$$E(|\psi\rangle) = E((U_A^\dagger \otimes U_B^\dagger)(U_A \otimes U_B)|\psi\rangle) \leq E(U_A \otimes U_B|\psi\rangle).$$

Outra propriedade desejável é

Propriedade 2. *$E(|\psi\rangle) = 0$ se, e somente se, $|\psi\rangle$ é um estado decomponível.*

Como todos os estados decomponíveis são equivalentes por unitárias locais, todo monótono de emaranhamento é constante no conjunto de estados decomponíveis. Como todo estado decomponível pode ser obtido de um estado arbitrário por LOCC, essa constante é o mínimo de E, que podemos ajustar para ser igual a zero. No entanto, a Propriedade 3 exige um pouco mais: que E seja diferente de zero para todos os estados emaranhados. A *negatividade*, que veremos mais adiante, é um exemplo de quantificador que para dimensões maiores que seis não satisfaz essa propriedade.

Vamos mostrar agora que a Propriedade 1 implica que o emaranhamento de um estado puro bipartite depende apenas de seus coeficientes de Schmidt.

Vimos no capítulo 1 que a relação de majoração introduz uma ordem parcial no simplexo de probabilidade. Podemos também definir uma ordem parcial no conjunto de matrizes densidade de um sistema [11].

Definição 35. *Dizemos que uma matriz densidade ρ* majora *uma matriz densidade σ se o vetor formado pelos autovalores de ρ majora o vetor formado pelos autovalores de σ. Nesse caso denotamos $\rho \succ \sigma$.*

Essa ordem está relacionada com a convertibilidade entre os estados por um tipo especial de mapa completamente positivo, chamado mapa *biestocástico*.

Definição 36. *Dizemos que um mapa completamente positivo que preserva o traço Φ, representado por operadores de Kraus A_i, é biestocástico se*

$$\sum_i A_i A_i^\dagger = I.$$

Um mapa biestocástico satisfaz a propriedade $\Phi(I) = I$.

Lema 5 (HLP quântico)**.** *Dadas duas matrizes densidade ρ e σ, existe um mapa biestocástico Φ tal que $\Phi(\rho) = \sigma$ se, e somente se, $\rho \succ \sigma$.*

Demonstração. Primeiro vamos mostrar que se Φ existe então ρ majora σ. Sejam U e V unitárias que diagonalizam ρ e σ respectivamente. Então vale

$$U\rho U^\dagger = diag(\lambda_\rho), \quad V\sigma V^\dagger = diag(\lambda_\sigma),$$

em que λ_A representa o vetor cujas entradas são os autovalores de A. Definimos um novo mapa biestocástico

$$\Psi(A) = U[\Phi(V^\dagger A V)]U^\dagger.$$

Por construção,

$$\Psi(diag(\lambda_\rho)) = diag(\lambda_\sigma).$$

Sejam P_i os projetores nos subespaços gerados pelos vetores da base. Definimos

$$B_{ij} = Tr(P_i \Psi(P_j)).$$

Uma conta simples mostra que B_{ij} é uma matriz biestocástica. Além disso temos

$$\lambda_{\sigma_i} = Tr(P_i diag(\lambda_\sigma)) = Tr(P_i \Psi(\sum_j \lambda_{\rho_j} P_j)) = \sum_j B_{ij}\lambda_{\rho_j}.$$

Desse modo existe uma matriz biestocástica que leva λ_ρ em λ_σ. Pelo HLP clássico 10, temos que $\lambda_\rho \succ \lambda_\sigma$, ou seja, $\rho \succ \sigma$.

Agora devemos mostrar que se $\rho \succ \sigma$ então existe um mapa biestocástico Φ tal que $\Phi(\rho) = \sigma$.

Vamos trabalhar na base em que σ é diagonal. Sejam U_i matrizes unitárias tais que as matrizes $U_i \rho U_i^\dagger$ sejam diagonais e que percorram todas as permutações possíveis dos elementos da diagonal. Precisamos de no máximo $N!$ dessas matrizes, em que N é a dimensão do espaço vetorial em questão. Com as matrizes todas diagonalizadas, voltamos ao caso clássico dado pela proposição 11: λ_σ pertence ao fecho convexo do conjunto formado pelos vetores $\lambda_{U_i\rho U_i^\dagger}$, ou seja

$$\sigma = \sum_i p_i U_i \rho U_i^\dagger, \quad \sum_i p_i = 1,$$

que é a imagem de ρ por um mapa biestocástico. □

Teorema 26 (Majoração de Nielsen)**.** *Dados dois estados $|\psi\rangle$ e $|\phi\rangle$, sejam v_ψ e v_ϕ os vetores de probabilidade formados com os quadrados dos coeficientes de Schmidt de $|\psi\rangle$ e $|\phi\rangle$, respectivamente. Então $|\psi\rangle$ pode ser convertido em $|\phi\rangle$ através de operações LOCC se, e somente se, os v_ψ e v_ϕ satisfazem a relação de majoração $v_\psi \prec v_\phi$. Equivalentemente, $|\psi\rangle$ pode ser convertido em $|\phi\rangle$ por LOCC se, e somente se, as matrizes densidade reduzidas satisfazem a relação $Tr_B(|\psi\rangle\langle\psi|) \prec Tr_B(|\phi\rangle\langle\phi|)$.*

Demonstração. Suponhamos que exista uma operação LOCC que leve $|\psi\rangle$ em $|\phi\rangle$. Suponhamos que a parte A realize uma operação local dada por uma medição cujos operadores de Kraus sejam A_i. O resultado é comunicado à parte B, que realiza uma operação local Φ_i, condicionada ao resultado i da medição na parte A. Estamos supondo que

$$\sum_i [I \otimes \Phi_i](A_i \otimes I|\psi\rangle\langle\psi|A_i^\dagger \otimes I) = |\phi\rangle\langle\phi|.$$

Como o estado resultante é puro, cada termo na soma convexa acima deve ser proporcional a $|\phi\rangle\langle\phi|$. Realizando o traço parcial em relação ao segundo subsistema temos

$$A_i \rho_\psi A_i^\dagger = p_i \rho_\phi \quad \forall \ \ i,$$

em que $\sum_i p_i = 1$, $\rho_\psi = Tr_B(|\psi\rangle\langle\psi|)$ e $\rho_\phi = Tr_B(|\phi\rangle\langle\phi|)$.

Seja $\sqrt{A_i \rho_\psi A_i^\dagger}$ a raiz positiva de $A_i \rho_\psi A_i^\dagger$. Temos que

$$A_i \sqrt{\rho_\psi} = \sqrt{A_i \rho_\psi A_i^\dagger} U_i.$$

De fato, seja $W_i (A_i \sqrt{\rho_\psi}) V_i = \Sigma$ a decomposição em valor singular de $A_i \sqrt{\rho_\psi}$. Como

$$A_i \rho_\psi A_i^\dagger = (A_i \sqrt{\rho_\psi})(A_i \sqrt{\rho_\psi})^\dagger,$$

vale $W_i A_i \rho_\psi A_i^\dagger W_i^\dagger = \Sigma^2$, de modo que W_i deve diagonalizar $A_i \rho_\psi A_i^\dagger$. Como $\sqrt{A_i \rho_\psi A_i^\dagger}$ é diagonal em uma base em que $A_i \rho_\psi A_i^\dagger$ o seja e possui autovalores iguais a raiz dos autovalores de $A_i \rho_\psi A_i^\dagger$ temos

$$W_i \sqrt{A_i \rho_\psi A_i^\dagger} W_i^\dagger = \Sigma = W_i A_i \sqrt{\rho_\psi} V_i,$$

o que implica que $A_i \sqrt{\rho_\psi} = \sqrt{A_i \rho_\psi A_i^\dagger} U_i$, em que $U_i = V_i W_i$, como queríamos.

Usando a relação de completude $\sum_i A_i^\dagger A_i = I$ podemos escrever

$$\rho_\psi = \sqrt{\rho_\psi} I \sqrt{\rho_\psi} = \sum_i \sqrt{\rho_\psi} A_i^\dagger A_i \sqrt{\rho_\psi} = \sum p_i U_i^\dagger \rho_\phi U_i.$$

Logo existe uma operação biestocástica que leva ρ_ϕ em ρ_ψ. Pelo lema HLP quântico, segue que

$$\lambda_{\rho_\psi} \prec \lambda_{\rho_\phi},$$

ou seja, $v_\psi \prec v_\phi$.

Se vale $v_\psi \prec v_\phi$, operações LOCC de conversão podem ser encontrados explicitamente, como em [38, 39] . □

Dado um estado $|\psi\rangle$, esse resultado divide o conjunto de estados puros do sistema em três partes: o conjunto dos estados que podem ser levados a $|\psi\rangle$ através de LOCC, o conjunto dos estados aos quais podemos chegar a partir de $|\psi\rangle$ e o conjunto dos estados aos quais não podemos chegar a partir de $|\psi\rangle$ e que não podem ser levados a $|\psi\rangle$ por LOCC. Como o emaranhamento não pode aumentar por LOCC, o primeiro conjunto contém os estados "menos"emaranhados que $|\psi\rangle$ e o segundo os estados que são "mais"emaranhados que $|\psi\rangle$.

A existência do último conjunto sugere a existência de "diferentes" tipos de emaranhamento, pois dois estados podem não ser comparáveis. A interseção dos dois primeiros representaria o conjunto dos estados que são "tão emaranhados quanto" $|\psi\rangle$.

Para o sistema de dois qubits, como o vetor de Schmidt possui apenas duas coordenadas, a ordenação imposta pela relação de majoração é total, de modo que dados dois estados sempre podemos levar um deles no outro através de LOCC.

O critério de majoração de Nielsen garante que qualquer função côncava de Schur é um monótono de emaranhamento em $\mathcal{H}_1 \otimes \mathcal{H}_2$. Uma das mais utilizadas é a *Entropia de Emaranhamento*:

$$E(|\psi\rangle) = S(\rho_1), \tag{4.1}$$

em que S é a entropia de von Neuman, dada pela equação (1.1) e $\rho_1 = Tr_2(|\psi\rangle\langle\psi|)$ é a matriz densidade reduzida do sistema 1.

A entropia de Von Neumann é o análogo em teoria de informação quântica para a entropia de Shannon em teoria de informação clássica. As distribuiçoes de probabilidade clássicas são substituídas pelas matrizes densidade [11, 15].

4.2 Emaranhamento para estados mistos

Para estados mistos, mesmo o problema de identificar se um estado é separável ou não já é um problema complicado. Como vimos, existem diversos critérios mas nenhum deles é necessário e suficiente no caso geral e ao mesmo tempo prático. O problema é simples apenas no caso de sistemas 2×2 e 2×3, para os quais o critério de Peres-Horodecki é também suficiente. Por esse motivo, esperamos que não deva ser uma tarefa fácil encontrar um bom quantificador de emaranhamento para estados mistos, como de fato é o caso.

Novamente, a propriedade desejável mais importante para um quantificador de emaranhamento é

Propriedade 1. *E não deve aumentar por LOCC, ou seja, se Λ é uma operação LOCC então*

$$E(\Lambda(\rho)) \leq E(\rho).$$

Dela também decorre o fato de que E é invariante por unitárias locais:

$$E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger) = E(\rho).$$

Podemos também impor a

Propriedade 2. *$E(\rho) = 0$ se, e somente se, ρ é um estado separável.*

Para estados mistos, é mais difícil encontrar um quantificador que satisfaça essa propriedade.

Para estados puros, a entropia de emaranhameto é um bom quantificador. Podemos então exigir que um quantificador para estados mistos satisfaça

Propriedade 3. *$E(|\psi\rangle\langle\psi|)$ coincide com a entropia de emaranhamento de $|\psi\rangle$.*

Existem vários quantificadores para estados mistos bipartites. Vejamos alguns exemplos.

4.3 Emaranhamento Destilável e Custo de Emaranhamento

O estado $|\Psi_-\rangle$, dado pela equação 3.2, que é um estado maximamente emaranhado de dois qubits. Utilizando esse estado como recurso, é possível implementar vários protocolos de computação e informação quântica [36, 34]. Acredita-se que tais protocolos não possam ser realizados utilizando apenas sistemas clássicos e por isso a capacidade de realizarmos essas tarefas deve estar relacionada à presença do emaranhamento no estado $|\Psi_-\rangle$ utilizado como recurso. Se usarmos um estado que não possua emaranhamento máximo, não é possível realizar a o protocolo com fidelidade 1.

No entanto, se possuirmos muitas cópias de um sistema em um dado estado $|\phi\rangle$ não maximamente emaranhado, podemos "concentrar"o emaranhamento, obtendo um número menor de cópias no estado $|\Psi_-\rangle$. Desse modo, podemos realizar os protocolos.

A pergunta que precisamos responder é quantos estados maximamente emaranhados $|\Psi_-\rangle$ podemos obter a partir de n cópias de $|\phi\rangle$:

$$|\phi\rangle^{\otimes n} \overset{LOCC}{\rightarrow} |\Psi_-\rangle^{\otimes m_n},$$

$$r = lim_{n\rightarrow\infty}\frac{m_n}{n}.$$

Esse procedimento motivou a definição de um quantificador de emaranhamento chamado *Emaranhamento Destilável* [40, 41, 42].

Definição 37. *O Emaranhamento Destilável de um estado de dois qubits dado pela matriz densidade ρ é*

$$E_D(\rho) = sup\{r; lim_{n\rightarrow\infty}\left(inf_\Lambda \left\|\Lambda(\rho^{\otimes n}) - |\Psi_-\rangle^{\otimes rn}\right\|_1 = 0\right)\},$$

em que Λ representa uma operação LOCC.

A intepretação física para a definição acima é a seguinte: as duas partes compartilham inicialmente n cópias do sistema todas no estado ρ. Em seguida eles aplicam uma dada operação LOCC Λ, obtendo como estado final $\Lambda(\rho^{\otimes n})$. Queremos que quando n aumente o estado final se aproxime cada vez mais de $|\Psi_-\rangle^{\otimes rn}$. Se tal operação não existe, dizemos que $E_D = 0$. Caso contrário, chamamos toda operação LOCC Λ satisfazendo essa propriedade de *protocolo de destilação de emaranhamento.*

Teorema 27. *Se um estado ρ é PPT, então $E_D(\rho) = 0$.*

Uma demonstração para esse resultado pode ser encontrada em [43].

Podemos considerar também o problema inverso do considerado acima. As duas partes começam com m cópias de um sistema no estado $|\Psi_-\rangle$ e em seguida aplicam uma operação LOCC Λ obtendo como estado final $\Lambda(\rho)$. Queremos que esse estado se aproxime de $\rho^{\otimes n}$ quando m cresce [41].

Definição 38. *O Custo de Emaranhamento de um estado de dois qubits ρ é*

$$E_C(\rho) = inf\{r; lim_{n\rightarrow\infty}\left(inf_\Lambda \left\|\rho^{\otimes n} - \Lambda(|\Psi_-\rangle^{\otimes rn})\right\|_1 = 0\right)\},$$

em que Λ representa uma operação LOCC qualquer.

Para estados puros, temos $E_C = E_D$. Em geral não vale a igualdade, sendo que existem estados que "consomem" emaranhamento para serem gerados, mas dos quais é possível destilar uma quantidade menor de emaranhamento:

$$E_C(\rho) \geq E_D(\rho).$$

No caso extremo, nenhum emaranhamento pode ser destilado, apesar do estado ser emaranhado, com $E_C \neq 0$. Dessa observação surgiu a noção de estados com emaranhamento preso: estados emaranhados com $E_D = 0$. Para mais detalhes sobre essas observações, veja [11, 21].

4.4 Quantificadores baseados em distância

Podemos construir quantificadores de emaranhameto utilizando uma distância d definida no conjunto de matrizes densidade do sistema [11, 21]:

$$E_d(\rho) = d(\rho, S) = inf_{\sigma \in S} d(\rho, \sigma),$$

em que S denota o conjunto dos estados separáveis.

Para que essa função seja um monótono de emaranhamento a distância d deve satisfazer:

$$d(\rho, \sigma) \geq d(\Lambda(\rho), \Lambda(\sigma)),$$

para toda operação LOCC Λ.

Existem várias distâncias entre as quais podemos escolher. Alguns exemplos são:

1. **Distância de Hilbert-Schmidt:** Vem de um produto interno definido no espaço vetorial de matrizes
$$\langle A, B \rangle_{HS} = Tr(AB^\dagger),$$
que gera a norma
$$\|A\|^2_{HS} = Tr(AA^\dagger),$$
que por sua vez gera a distância de Hilbert-Schmidt
$$d_{HS}(A, B) = \|A - B\|_{HS}.$$

2. **Distância do traço:**
$$d_{tr}(A, B) = \frac{1}{2} Tr(|A - B|).$$

3. **Distância de Bures:**
$$d^2_B(\rho_1, \rho_2) = Tr(\rho_1) + Tr(\rho_2) - 2\sqrt{F}(\rho_1, \rho_2),$$
em que
$$\sqrt{F}(\rho_1, \rho_2) = max_{A_1, A_2}\{|Tr(A_1 A_2^\dagger)|; \quad \rho_1 = A_1 A_1^\dagger, \quad \rho_2 = A_2 A_2^\dagger\}$$
é chamada fidelidade raiz.

Podemos usar um outro quantificador de distinguibilidade no lugar da distância. Por exemplo podemos usar a entropia relativa

$$S(\rho|\sigma) = Tr[\rho(log\rho - log\sigma)].$$

Nesse caso obtemos um quantificador de emaranhamento chamado *Entropia Relativa de Emaranhamento* [44]

$$E_R = inf_{\sigma\in S} S(\rho|\sigma).$$

Outros dois quantificadores importantes são a *Robustez* e a *Robustez Randômica* [45]. Eles estão relacionados com quanto de "ruído"deve ser adicionado ao estado ρ para que ele deixe de ser emaranhado.
Suponhamos que ρ seja um estado emaranhado. Então o caminho

$$I : [0,1] \longrightarrow D(\mathcal{H}_{AB})$$
$$t \mapsto t\rho + (1-t)\frac{I}{d},$$

em que d é a dimensão de $\mathcal{H}_{AB}$, deve cruzar a fronteira do conjunto dos estados separáveis em algum valor $t_0 \in (0,1)$, uma vez que o estado $\frac{I}{d}$ é um estado separável que pertence ao interior do conjunto $S(\mathcal{H}_{AB})$.

Definição 39. *A Robustez Randômica $R_r(\rho)$ de um estado ρ é dada por*

$$R_r\rho = \frac{1-t_0}{t_0},$$

em que t_0 é o menor valor de t tal que $t\rho + (1-t)\frac{I}{d}$ é um estado separável.

Podemos agora fazer a mesma construção com um outro estado separável qualquer σ no lugar de $\frac{I}{d}$. Tomamos o caminho

$$I^\sigma : [0,1] \longrightarrow D(\mathcal{H}_{AB})$$
$$t^\sigma \mapsto t\rho + (1-t)\sigma,$$

Esse caminho deve cruzar a fronteira do conjunto dos estados separáveis em algum valor $t_0^\sigma \in (0,1]$, uma vez que o estado σ é separável. Como permitimos que σ esteja na fronteira do conjunto $S(\mathcal{H}_{AB})$, pode ser que $t_0^\sigma = 1$.

Definição 40. *A Robustez $R(\rho)$ de um estado ρ é dada por*

$$R(\rho) = \sup_{\sigma\in S(\mathcal{H}_{AB})} t_0^\sigma,$$

em que t_0^σ é o menor valor de t tal que o estado $t\rho + (1-t)\sigma$ é separável.

Generalizando mais ainda:

Definição 41. *A Robustez Generalizada $R_g(\rho)$ de um estado ρ é dada por*

$$R_g(\rho) = \sup_{\sigma\in D(\mathcal{H}_{AB})} t_0^\sigma,$$

em que t_0^σ é o menor valor de t tal que o estado $t\rho + (1-t)\sigma$ é separável.

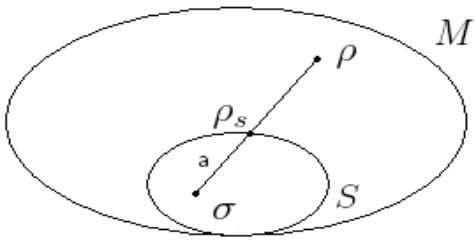


Figura 4.1: Robustez: $R = \frac{1-a}{a}$.

4.5 Fecho convexo e Emaranhamento de Formação

Suponhamos que temos definido um quantificador de emaranhamento para estados puros que denotaremos E_p. A partir dele podemos construir um quantificador de emaranhamento E para estados mistos a partir de E_p, que coincide com E_p para os estados puros:

$$E(\rho) = inf \left\{ \sum_i p_i E_p(|\psi_i\rangle) \right\},$$

em que o ínfimo é tomado sobre todas as decomposições de ρ como soma convexa de estados puros

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

Em geral, quantificadores desse tipo não são muito práticos porque o processo de minimização envolvido pode ser difícil de realizar. Quando o quantificador para estados puros escolhido é a Entropia de Emaranhamento, dada pela equação (4.1), o quantificador de emaranhamento obtido é chamado de emaranhamento de formação. [41].

Definição 42. *O emaranhamento de formação E_F de um estado qualquer ρ de um sistema bipartite é dado por*

$$E(\rho) = inf \left\{ \sum_i p_i E(|\psi_i\rangle) \right\},$$

em que o ínfimo é tomado sobre todas as decomposições de ρ como soma convexa de estados puros

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|,$$

e em que $E(|\psi_i\rangle)$ é a entropia de emaranhamento de $|\psi_i\rangle$.

4.6 Concorrência

Apesar de quantificadores de emaranhamento construidos através do fecho convexo não serem práticos em geral, podemos encontrar uma fórmula que permite calcular o emaranhamento de formação para o sistema de dois qubits sem que precisemos realizar o processo de

minimização envolvido em sua definição. Para isso vamos introduzir a *concorrência* que pode também ser vista como um quantificador de emaranhamento [2, 46].

4.6.1 Concorrência para estados puros

Para definir a concorrência para estados puros, primeiramente definimos a operação de *spin flip* para um qubit:

$$|\tilde{\psi}\rangle = \epsilon|\psi^*\rangle,$$

em que $|\psi^*\rangle$ é o vetor formado a partir de $|\psi\rangle$ conjugando seus coeficientes em alguma base fixada e ϵ é a matriz que, escrita nessa mesma base, tem a forma:

$$\epsilon = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Para n qubits, definimos a operação como sendo conjugação em relação a uma base decomponível seguida da aplicação da matriz ϵ em cada um dos qubits.

Podemos expressar o emaranhamento de um sistema de dois qubits usando a operação de spin flip.

Definição 43. *A* concorrência *de um estado puro $|\psi\rangle$ é*

$$C(|\psi\rangle) = |\langle\psi|\tilde{\psi}\rangle|.$$

A concorrência de um vetor qualquer $|x\rangle$ é dada por

$$C(|x\rangle) = \frac{|\langle x|\tilde{x}\rangle|}{|\langle x|x\rangle|}.$$

Lema 6. *A concorrência é invariante por unitárias locais.*

Demonstração. Seja $U = U_A \otimes U_B$.

Começamos com um estado da forma

$$|\psi\rangle = a|00\rangle + b|11\rangle,$$

com a e b reais e não-negativos. Qualquer estado pode ser levado a um estado desse tipo através de uma unitária local. A concorrência desse estado é $|\langle\psi|\tilde{\psi}\rangle| = 2ab$. Aplicando a unitária U temos:

$$|\psi'\rangle = U|\psi\rangle = a(U_A|0\rangle)(U_B|0\rangle) + b(U_A|1\rangle)(U_B|1\rangle),$$

$$|\psi'^*\rangle = a(U_A^*|0\rangle)(U_B^*|0\rangle) + b(U_A^*|1\rangle)(U_B^*|1\rangle),$$

$$|\tilde{\psi}'\rangle = a(\epsilon U_A^*|0\rangle)(\epsilon U_B^*|0\rangle) + b(\epsilon U_A^*|1\rangle)(\epsilon U_B^*|1\rangle).$$

Calculando o produto interno com $|\psi'\rangle$ temos:

$$\langle\psi'|\tilde{\psi}'\rangle = a^2\langle 0|U_A^\dagger\epsilon U_A^*|0\rangle\langle 0|U_B^\dagger\epsilon U_B^*|0\rangle + ab\langle 0|U_A^\dagger\epsilon U_A^*|1\rangle\langle 0|U_B^\dagger\epsilon U_B^*|1\rangle +$$

$$ab\langle 1|U_A^\dagger \epsilon U_A^*|0\rangle\langle 1|U_B^\dagger \epsilon U_B^*|0\rangle + b^2\langle 1|U_A^\dagger \epsilon U_A^*|1\rangle\langle 1|U_B^\dagger \epsilon U_B^*|1\rangle.$$

Como $U_A^\dagger \epsilon U_A^* = \epsilon$ e $U_B^\dagger \epsilon U_B^* = \epsilon$, temos $\langle\psi'|\tilde{\psi'}\rangle = 2ab$ e a concorrência é invariante por U. □

Usando a concorrência, podemos expressar o emaranhamento de um estado puro de dois qubits.

Lema 7. *A entropia de emaranhamento de um estado puro de dois qubits é dada por*

$$E(|\psi\rangle) = \mathcal{E}\left(\frac{1+\sqrt{1-C^2(|\psi\rangle)}}{2}\right),$$

em que $\mathcal{E}(x) = -xlogx - (1-x)log(1-x)$.

Demonstração. Começamos com o estado em decomposição de Schmidt e fazemos a operação de spin flip em relação à essa base.

$$|\psi\rangle = a|00\rangle + b|11\rangle,$$

com a e b reais. Temos então $C^2 = 4a^2b^2$. Como supomos o estado normalizado, temos $|a|^2 + |b|^2 = 1$, de modo que:

$$1 - C^2 = (|a|^2 + |b|^2)^2 - 4a^2b^2 = (a^2 - b^2)^2.$$

Desse modo temos:

$$\frac{1+\sqrt{1-C^2}}{2} = \frac{1-|a^2-b^2|}{2} = max(a^2, b^2),$$

que é um autovalor da matriz densidade reduzida

$$\rho_A = \begin{bmatrix} a^2 & 0 \\ 0 & b^2 \end{bmatrix}.$$

Como $\epsilon(a^2) = \epsilon(b^2) = S(\rho_A)$, segue o resultado. □

4.6.2 Concorrência para estados mistos

Antes da definição geral de concorrência, enunciaremos dois resultados que serão usados para provar propriedades úteis da concorrência.

Proposição 13. *Seja* $\rho = \sum_i |v_i\rangle\langle v_i|$ *a decomposição para uma matriz densidade* ρ *em termos de autovetores* $|v_i\rangle$ *em que cada* $|v_i\rangle$ *satisfaz* $\langle v_i|v_i\rangle = \eta_i$*, com* η_i *o autovalor de* ρ *associado a* $|v_i\rangle$*. Então para qualquer outra decomposição* $\rho = \sum_i |x_i\rangle\langle x_i|$ *temos:*

$$|x_i\rangle = \sum_i U_{ij}|v_j\rangle.$$

em que U_{ij} *é uma matriz unitária.*

Uma demonstração para esse resultado pode ser encontrada em [13].

Proposição 14. *Se A é uma matriz complexa simétrica, então existe uma matriz unitária U tal que UAU^T é diagonal, sendo que os elementos da diagonal são os valores singulares de A.*

Uma demonstração para esse resultado pode ser encontrada em [47]

Definição 44. *A concorrência de uma matriz densidade ρ é definida como*

$$C(\rho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\},$$

em que λ_i são os valores singulares da matriz $X^T\epsilon \otimes \epsilon X$, em ordem não-crescente, sendo X a raiz positiva de ρ.

Lema 8. *A concorrência como definida acima é invariante por unitárias locais.*

Demonstração. Seja

$$\tilde{\rho} = (\epsilon \otimes \epsilon)\rho^*(\epsilon \otimes \epsilon).$$

Como $X^T\epsilon \otimes \epsilon X$ é simétrica, existe uma unitária V tal que $V^T X^T \epsilon \otimes \epsilon X V = \Sigma$, com Σ diagonal e com elementos da diagonal iguais aos valores singulares de $X^T\epsilon \otimes \epsilon X$. Como Σ é uma matriz real, temos que

$$\Sigma^2 = (V^T X^T \epsilon \otimes \epsilon X V)^\dagger (V^T X^T \epsilon \otimes \epsilon X V) =$$

$$V^\dagger X^\dagger \epsilon \otimes \epsilon X^* V^* V^T X^T \epsilon \otimes \epsilon X V =$$

$$V^\dagger X^\dagger \epsilon \otimes \epsilon \rho^* \epsilon \otimes \epsilon X V = V^\dagger X \tilde{\rho} X V,$$

de modo que V diagonaliza a matriz $X\tilde{\rho}X$ no sentido usual. Logo os valores singulares de $X^T\epsilon\otimes\epsilon X$ são as raízes dos autovalores de $X\tilde{\rho}X$. Como essa matriz tem os mesmos autovalores de $\rho\tilde{\rho}$, basta mostrar que os autovalores dessa última matriz não variam quando aplicamos uma unitária local.

De fato, seja $\rho' = (U_A \otimes U_B)\rho(U_A \otimes U_B)^\dagger$. Devemos mostrar que os autovalores de $\rho'\tilde{\rho'}$ são os mesmos de $\rho\tilde{\rho}$. Mas

$$\rho'\tilde{\rho'} = (U_A \otimes U_B)\rho(U_A^\dagger \otimes U_B^\dagger)\epsilon \otimes \epsilon(U_A^* \otimes U_B^*)\rho^*(U_A^T \otimes U_B^T)\epsilon \otimes \epsilon =$$

$$(U_A \otimes U_B)\rho(\epsilon \otimes \epsilon)\rho^*(\epsilon \otimes \epsilon)(U_A^\dagger \otimes U_B^\dagger) = (U_A \otimes U_B)\rho\tilde{\rho}(U_A \otimes U_B)^\dagger,$$

em que usamos o fato de que

$$U_A^\dagger \otimes U_B^\dagger \epsilon \otimes \epsilon U_A^* \otimes U_B^* = det(A)^* det(B)^* \epsilon \otimes \epsilon,$$

$$U_A^T \otimes U_B^T \epsilon \otimes \epsilon U_A \otimes U_B = det(A) det(B) \epsilon \otimes \epsilon.$$

Como os autovalores de uma matriz não mudam quando aplicamos uma transformação unitária, segue que a concorrência não muda quando aplicamos unitárias locais. □

Proposição 15. *A concorrência da definição 44 para estados puros coincide com a definição 43.*

Demonstração. Como já mostramos que ambas são invariantes por unitárias locais, basta cosiderarmos novamente um estado do tipo

$$|\psi\rangle = a|00\rangle + b|11\rangle.$$

Para esse estado temos

$$\rho\tilde{\rho} = \begin{bmatrix} 2a^2b^2 & 0 & 0 & 2a^3b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2b^3a & 0 & 0 & 2a^2b^2 \end{bmatrix},$$

cujo único autovalor possivelmente não-nulo é $4a^2b^2$, de modo que a concorrência calculada dessa forma coincide com a definição 43. □

Teorema 28. *O emaranhamento de formação de um estado qualquer de dois qubits é dado por:*

$$E(\rho) = \mathcal{E}\left(\frac{1+\sqrt{1-C^2(\rho)}}{2}\right).$$

Além disso, a decomposição que minimiza o emaranhamento médio pode ser tomada com todos os vetores com mesma concorrência.

Vamos dividir a demonstração desse teorema em duas proposições. A primeira vai mostrar que o valor mínimo da concorrência média sobre todas as decomposições possíveis é igual à concorrência de ρ e que, além disso, é possível encontrar uma decomposição minimizante na qual todos os estados puros envolvidos tenham mesma concorrência. A segunda vai mostrar que essa decomposição minimiza o emaranhamento médio, o que mostra o resultado desejado.

Proposição 16. *Dada uma matriz densidade ρ é possível encontrar uma decomposição*

$$\rho = \sum_i |x_i\rangle\langle x_i|,$$

que minimiza a concorrência média $\sum_i \langle x_i|x_i\rangle C(|x_i\rangle)$ e na qual $C(|x_i\rangle) = C(\rho) \ \ \forall \ \ i$.

Demonstração. Seja X a raiz de ρ. Se

$$\rho = \sum_i |w_i\rangle\langle w_i|$$

é uma outra decomposição para ρ então existe uma matriz unitária U tal que os vetores $|w_i\rangle$ são as colunas de XU. De fato, existe uma unitária U tal que

$$|w_i\rangle = \sum_j U_{ij}|v_j\rangle,$$

em que $|v_j\rangle$ são os autovetores de ρ. Na base em que ρ é diagonal temos:

$$(XU)_{ij} = \sum_k X_{ik}U_{kj} = \sum_k \eta_i\delta_{ik}U_{kj} = \eta_i U_{ij} = |w_j\rangle_i.$$

Queremos encontrar uma decomposição que minimize a concorrência média. A concorrência de cada $|w_j\rangle$ é:

$$C(|w_i\rangle) = \frac{|(XU)_i \cdot \epsilon \otimes \epsilon \cdot (XU)_i|}{\langle w_i|w_i\rangle} = \frac{|(XU)^T \epsilon \otimes \epsilon (XU)|_{ii}}{\langle w_i|w_i\rangle}.$$

Como o peso p_j em que cada $|w_j\rangle$ aparece na decomposição é $\langle w_j|w_j\rangle$, temos que a concorrência média é:

$$\langle C\rangle = \sum_i p_i C(|w_i\rangle) = \sum_i |(XU)^T \epsilon \otimes \epsilon (XU)|_{ii}.$$

A matriz $X^T\epsilon \otimes \epsilon X$ é complexa simétrica. Logo existe uma unitária V tal que $V^T(X^T\epsilon \otimes \epsilon X)V = \Sigma$, em que Σ é diagonal. Absorvendo V em U, temos que a concorrência média de uma outra decomposição é dada por:

$$\langle C\rangle = Tr\left(|U^T \Sigma U|\right),$$

em que U é unitária e $|U^T\Sigma U|$ denota a matriz formada tomando o módulo elemento a elemento de $U^T\Sigma U$.

Nosso objetivo é encontar uma decomposição que possua concorrência média mínima. Devemos então encontrar uma matriz U que minimize a expressão acima. Podemos obter uma cota inferior. Escrevendo $U_{ij} = \sqrt{p_{ij}} e^{i\frac{\phi_{ij}}{2}}$ temos:

$$\sum_i |U^T\Sigma U|_{ii} = \sum_i |\sum_{kj} U_{ji}\Sigma_{jk}U_{ki}| = \sum_i |\sum_j \sqrt{p_{ji}} e^{i\frac{\phi_{ji}}{2}} \sigma_j \sqrt{p_{ji}} e^{i\frac{\phi_{ji}}{2}}| =$$

$$\sum_i |p_{1i}\sigma_1 + \sum_{j=2}^{4} p_{ij}\sigma_j e^{i(\phi_{ji}-\phi_{1i})}|$$

$$\geq \sum_i \left(|p_{1i}\sigma_1| - |\sum_j p_{ij} e^{i(\phi_{ji}-\phi_{1i})}\sigma_j| \right)$$

$$\geq \sum_i \left(|p_{1i}\sigma_1| - \sum_j |p_{ij} e^{i(\phi_{ji}-\phi_{1i})}\sigma_j| \right) = \sigma_1 - \sigma_2 - \sigma_3 - \sigma_4 = C(\rho),$$

em que usamos o fato de que $\sum_i p_{ij} = 1$, o que segue do fato de U ser unitária. Desse modo a concorrência média é sempre maior que $C(\rho)$. Devemos agora encontrar uma unitária que sature essa desigualdade. Vamos considerar primeiro o bloco

$$\begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix}.$$

Seja $\phi = arctg\left(\sqrt{\frac{\sigma_2}{\sigma_1}}\right)$. Então a unitária

$$U = \begin{pmatrix} cos(\phi) & -sen(\phi) \\ isen(\phi) & icos(\phi) \end{pmatrix}$$

é tal que

$$U^T \begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix} U = \begin{pmatrix} \sigma_1 - \sigma_2 & -\sqrt{\sigma_1\sigma_2} \\ -\sqrt{\sigma_1\sigma_2} & 0 \end{pmatrix}.$$

Repetindo o mesmo processo[1] , para o bloco $\begin{pmatrix} \sigma_1 - \sigma_2 & 0 \\ 0 & \sigma_3 \end{pmatrix}$ e em seguida para o bloco $\begin{pmatrix} \sigma_1 - \sigma_2 - \sigma_3 & 0 \\ 0 & \sigma_4 \end{pmatrix}$ obtemos uma matriz tal que o primeiro elemento na diagonal é $C(\rho)$ e os outros termos da diagonal são nulos. Desse modo obtemos uma unitária U que satura a desigualdade, de modo que a concorrência média mínima é $C(\rho)$.

Devemos agora mostrar que os estados $|w_i\rangle$ podem ser escolhidos com mesma concorrência. Para isso vamos utilizar matrizes unitárias reais O, uma vez que elas não alteram a concorrência média:

$$Tr(O^T U \Sigma U O) = Tr(U^T \Sigma U).$$

Nossa tarefa agora é escolher O de modo que todos os estados na decomposição possuam a mesma concorrência. Isso quer dizer que o elemento ii da matriz $O^T U^T \Sigma U O$ deve ser $p_i C(\rho)$, em que p_i é o peso com que $|w_i\rangle$ aparece na decomposição. Como cada $|w_i\rangle$ é a i-ésima coluna da matriz $XVUO$, temos que $p_i = \langle w_i|w_i\rangle = [(XVUO)^\dagger (XVUO)]_{ii}$ e então a condição para que todos os estados tenham a mesma concorrência $C(\rho)$ é equivalente a

$$[O^T (U^T \Sigma U - C(\rho) U^\dagger V^\dagger X^\dagger XVU) O]_{ii} = 0 \ \ \forall \ \ i.$$

Seja $Q = U^T \Sigma U - C(\rho) U^\dagger V^\dagger X^\dagger XVU$. Como a concorrência média é $C(\rho)$, $Tr(Q) = 0$. Se existir algum elemento não nulo na diagonal, então deve haver um positivo e um negativo. Seja

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

um bloco da diagonal de Q com $a < 0$ e $d > 0$. Suponhamos sem perda de generalidade que esse bloco seja o primeiro bloco na diagonal. Consideremos as rotações da forma

$$R_t = \begin{pmatrix} cos(t) & -sen(t) \\ sen(t) & cos(t) \end{pmatrix} \oplus I.$$

$R_0 = I$ e $R_{\pi/2}$ troca a e d. Por continuidade deve haver algum t tal que a primeira entrada desse bloco de $R_t Q R_t^T$ seja igual a zero. Como $Tr(R_t Q R_t^T) = 0$, podemos proceder de maneira análoga para outro bloco em que o primeiro elemento da diagonal seja positivo e o segundo negativo. Isso não altera o elemento da diagonal que já zeramos. Repetimos o procedimento até zerarmos todos os elementos da diagonal. Assim obtemos uma decomposição com concorrência mínima na qual todos os vetores possuem a mesma concorrência. □

Proposição 17. *A decomposição encontrada na proposição acima também minimiza o emaranhamento médio*

$$\sum_i \langle x_i|x_i\rangle E(|x_i\rangle).$$

[1]Esse procedimento altera os elementos fora da diagonal, mas deixa os outros elementos da diagonal além de $\sigma_1 - \sigma_2$ e σ_3 inalterados.

Demonstração. Seja $f(x) = \frac{1+\sqrt{1-x^2}}{2}$. A função $g = \mathcal{E} \circ f$ é uma função convexa. Desse modo temos que, dada uma decomposição $\rho = \sum_i |y_i\rangle\langle y_i|$

$$\langle E\rangle = \sum_i p_i E(|y_i\rangle\langle y_i|) = \sum_i p_i g(C(|y_i\rangle)) \geq g(\sum_i p_i C(|y_i\rangle)) = g(\langle C\rangle).$$

Como g é uma função crescente, e $C(\rho)$ é a concorrência média mínima , temos

$$g(\langle C\rangle) \geq g(C(\rho)) \Longrightarrow \langle E\rangle \geq g(C(\rho)).$$

Para a decomposição encontrada na proposição anterior, temos que todos os estados puros $|x_i\rangle$ envolvidos possuem mesma concorrência $C(\rho)$ e portanto mesmo emaranhamento $g(C(\rho))$, de modo que o emaranhamento médio pra essa decomposição é $g(C(\rho))$. Logo, essa é uma decomposição que minimiza o emaranhamento médio e portanto

$$E(\rho) = g(C(\rho)).$$

□

4.7 Negatividade

Um dos resultados mais poderosos na teoria do emaranhamento é o critério de Peres-Horodecki, que garante condições necessárias para que um estado de um sistema seja separável.

A *negatividade* [3] é um quantificador de emaranhamento criado a partir do critério de Peres-Horodecki, e pode ser vista como uma versão quantitativa deste. De certa forma, ela mede "quanto"a transposta parcial de uma matriz densidade "deixa"de ser positiva.

Definição 45. *A negatividade $\mathcal{N}$ de uma matriz densidade ρ é:*

$$\mathcal{N}(\rho) = \frac{\left\|\rho^{T_1}\right\|_1 - 1}{2},$$

em que $\|A\|_1 = (Tr(A^\dagger A))^{1/2}$ é a norma traço.

No caso de matrizes hermitianas, que é o que estamos considerando, a norma traço é simplesmente a soma dos valores absolutos dos autovalores da matriz. Como o traço da transposta parcial de uma matriz densidade é um, a soma dos autovalores dessa matriz é um. Desse modo a quantidade $\left\|\rho^{T_1}\right\|_1 - 1$ é justamente o dobro dos valores absolutos dos autovalores negativos de ρ^{T_1} e a negatividade é a soma dos valores absolutos dos autovalores negativos de ρ^{T_1}.

Agora devemos verificar se a negatividade é realmente um bom quantificador de emaranhamento. A condição de se anular em estados separáveis é claramente satisfeita, uma vez que a transposta parcial de uma matriz separável não possui autovalores negativos. A outra condição essencial, de não aumentar em média por LOCC, também é satisfeita, como mostraremos em seguida.

A negatividade não aumenta quando fazemos misturas:

Proposição 18. *A negatividade $\mathcal{N}$ é uma função convexa, isto é,*

$$\mathcal{N}\left(\sum p_i\rho_i\right) \leq \sum p_i\mathcal{N}\left(\rho_i\right), \tag{4.2}$$

em que as matrizes ρ_i são hermitianas, $p_i > 0$ e $\sum p_i = 1$.

Demonstração. Segue do fato de que $\|\cdot\|_1$ é uma norma e por isso satisfaz à desigualdade triangular:

$$\begin{aligned}\mathcal{N}\left(\sum p_i\rho_i\right) = \frac{\left\|\sum p_i\rho_i^{T_1}\right\|_1 - 1}{2} &\leq \frac{\sum p_i\left\|\rho_i^{T_1}\right\|_1 - 1}{2} \\ &= \sum p_i\frac{\left\|\rho_i^{T_1}\right\|_1 - 1}{2} = \sum p_i\mathcal{N}\left(\rho_i\right).\end{aligned}$$

□

Definida em termos dos autovalores, a negatividade pode ser facilmente calculada. No entanto, para provar os resultados sobre monotonicidade por LOCC é mais conveniente escrevermos a negatividade em termos de uma expressão variacional. Dada uma matriz hermitiana A, sempre podemos escrevê-la na forma:

$$A = a_+\rho_+ - a_-\rho_-, \tag{4.3}$$

em que ρ_+ e ρ_- são matrizes densidade[2] e $a_+, a_- \geq 0$. Desse modo temos $tr(A) = a_+ - a_-$.

Proposição 19. *Dada uma matriz hermitiana A, existe uma decomposição da forma (4.3) tal que $a_+ + a_-$ é mínimo. Para essa decomposição, temos $\|A\|_1 = a_+ + a_-$ e a_- é a soma dos valores absolutos dos autovalores negativos de A.*

Demonstração. Sabemos que $A + a_-\rho_-$ é uma matriz positiva semidefinida. Seja P_- o projetor sobre o subespaço gerado pelos autovetores cujos autovalores são negativos. Então temos:

$$Tr(P_-(A + a_-\rho_-)) \geq 0.$$

Sejam $\lambda_1, \ldots, \lambda_n$ os autovalores não-negativos de A e $\mu_1, \ldots, \mu_m$ os autovalores negativos de A. Então em uma base de autovetores adequada, A pode ser escrita na forma:

$$A = \begin{bmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_n & & & & \\ & & & \mu_1 & & & \\ & & & & \ddots & & \\ & & & & & \mu_m & \end{bmatrix}.$$

[2]Para ver que isso é sempre possível, basta diagonalizarmos A.

Nessa base, temos

$$P_- = \begin{bmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}, \quad P_-A = \begin{bmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & \mu_1 & & \\ & & & & \ddots & \\ & & & & & \mu_m \end{bmatrix},$$

de modo que $Tr(AP_-) = -\mathcal{N}(A)$. Logo temos

$$Tr(P_-(A + a_-\rho_-)) = -\mathcal{N}(A) + a_-Tr(P_-\rho_-) \geq 0.$$

Como $Tr(P_-\rho_-) \leq 1$, *vale*

$$-\mathcal{N}(A) + a_- \geq 0,$$

ou seja, $a_- \geq \mathcal{N}(A)$. Seja

$$a_-^0\rho_-^0 = \begin{bmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & -\mu_1 & & \\ & & & & \ddots & \\ & & & & & -\mu_m \end{bmatrix},$$

$a_-^0 = -(\mu_1 + \ldots + \mu_m)$. Então,

$$(A + a_-^0\rho_-^0)P_- = \begin{bmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_n & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix} P_- = 0.$$

Nesse caso, temos $a_-^0 = \mathcal{N}(A)$, que é o menor valor possível de a_-. Como $a_+ - a_- = Tr(A)$, temos que se a_- é mínimo, a_+ também deve ser, de modo que $a_+^0 + a_-^0$ é o mínimo de $a_+ + a_-$, em que $a_+^0 = 1 - a_-^0 = \lambda_1 + \ldots + \lambda_n$. Desse modo temos que o mínimo de $a_+ + a_-$ é $\lambda_1 + \ldots + \lambda_n - \mu_1 - \ldots - \mu_m = \|A\|_1$. □

Corolário 5. *A negatividade* $\mathcal{N}$ *de uma matriz densidade* ρ *pode ser definida alternativamente como:*

$$\mathcal{N}(\rho) = min\{a_- |\ \rho^{T_1} = a_+\rho_+ - a_-\rho_-\}, \tag{4.4}$$

em que o mínimo é tomado sobre todas as possíveis decomposições em que ρ_+, ρ_- *são matrizes densidade e em que* $a_+, a_- \geq 0$.

Quando a negatividade é caracterizada dessa maneira, é fácil mostrar que ela é um monótono de emaranhamento. Para mostrar esse fato, devemos verificar que após uma operação LOCC em que os possíveis estados finais são ρ_i, com probabilidade p_i, temos

$$\mathcal{N}(\rho) \geq \sum p_i \mathcal{N}(\rho_i). \tag{4.5}$$

Cada passo de uma operação LOCC pode ser caracterizado por um conjunto de mapas completamente positivos $\mathcal{M}_i$, tais que

$$\begin{aligned} \rho_i &= \frac{\mathcal{M}_i(\rho)}{p_i}. \\ p_i &= Tr(\mathcal{M}_i(\rho)). \end{aligned}$$

Se necessário, podemos ainda decompor cada $\mathcal{M}_i$ na forma:

$$\mathcal{M}_i = \sum_j \mathcal{M}_i^j,$$

de maneira que cada mapa leve estados puros em estados puros, caso em que o mapa é chamado mapa puro. Pelo fato de $\mathcal{N}$ ser convexa, temos:

$$\mathcal{N}(\mathcal{M}_i(\rho)) \leq \sum_j \mathcal{N}(\mathcal{M}_i^j(\rho)),$$

e podemos então considerar apenas mapas $\mathcal{M}_i$ puros. Além disso, podemos considerar que apenas uma das partes realiza a operação, pois uma operação em que as duas partes participam é a composição de uma operação em que somente uma participa com uma operação em que só a outra participa. Vamos supor então que a operação é realizada apenas no segundo subsistema. Desse modo cada $\mathcal{M}_i$ pode ser escrito na forma:

$$\mathcal{M}_i(\rho) = (I \otimes M_i)\rho(I \otimes M_i)^\dagger, \tag{4.6}$$

em que $\sum M_i^\dagger M_i \leq I$.

Lema 9. *Com as definições dadas acima, temos:*

$$(\mathcal{M}_i(\rho))^{T_1} = \mathcal{M}_i(\rho^{T_1}).$$

Demonstração. Escrevendo $\rho = \sum A_j \otimes B_j$, em que A_j, B_j não são necessariamente matrizes densidade, temos:

$$\begin{aligned} (\mathcal{M}_i(\rho))^{T_1} &= \left((I \otimes M_i)\,\rho\,(I \otimes M_i)^\dagger\right)^{T_1} = \\ \left((I \otimes M_i)\left(\sum A_j \otimes B_j\right)(I \otimes M_i)^\dagger\right)^{T_1} &= \left(\sum A_j \otimes M_i B_j M_i^\dagger\right)^{T_1} = \\ \sum A_j^T \otimes M_i B_j M_i^\dagger &= (I \otimes M_i)\left(\sum A_j^T \otimes B_j\right)(I \otimes M_i)^\dagger = \\ (I \otimes M_i)\left(\sum A_j \otimes B_j\right)^{T_1}(I \otimes M_i)^\dagger &= \mathcal{M}_i\left(\rho^{T_1}\right). \end{aligned}$$

□

Proposição 20. *A negatividade é um monótono de emaranhamento.*

Demonstração. Como dissemos, basta considerarmos um passo de LOCC em que apenas o segundo subsistema realiza uma operação "pura", descrita pela equação (4.6). Seja então

$$\rho^{T_1} = (1-N)\rho_+ - N\rho_-$$

a decomposição ótima de ρ^{T_1} dada pela Proposição 19, em que $N = \mathcal{N}(\rho)$. Aplicando $\mathcal{M}_i$ a ambos os lados da equação acima, temos:

$$p_i\rho_i^{T_1} = \mathcal{M}_i(\rho)^{T_1} = \mathcal{M}_i(\rho^{T_1}) = (1-N)\rho_+^i - N\rho_-^i,$$

em que $\rho_+^i = \mathcal{M}_i(\rho_+)$ e $\rho_-^i = \mathcal{M}_i(\rho_-)$. Dividindo por p_i obtemos:

$$\rho_i = \frac{(1-N)}{p_i}\rho_+^i - \frac{N}{p_i}\rho_-^i,$$

que é justamente uma das decomposições que aparecem na Definição 5, com $a_- = \frac{N}{p_i}Tr(\mathcal{M}_i(\rho_-^i)) \leq \frac{N}{p_i}$. Desse modo, pela proposição 19, temos $\mathcal{N}(\rho_i) \leq \frac{N}{p_i}$, de modo que

$$\sum p_i\mathcal{N}(\rho_i) \leq \sum p_i\frac{N}{p_i} = N = \mathcal{N}(\rho),$$

o que prova que a negatividade é um monótono de emaranhamento. □

4.7.1 Comparação entre negatividade e concorrência

Lema 10. *Para estados puros de dois qubits, negatividade e concorrência coincidem.*

Demonstração. Seja $|\Psi\rangle$ um estado puro. Escrevendo $|\Psi\rangle$ em decomposição de Schmidt

$$a\,|00\rangle + b\,|11\rangle$$

sabemos que $C(|\Psi\rangle) = 2ab$. A negatividade de $|\Psi\rangle$ é o valor absoluto do autovalor negativo da matriz

$$\rho^{T_1} = \begin{bmatrix} a^2 & 0 & 0 & 0 \\ 0 & 0 & ab & 0 \\ 0 & ab & 0 & 0 \\ 0 & 0 & 0 & b^2 \end{bmatrix},$$

que é igual a $2ab$. □

Proposição 21. *A negatividade de uma matriz densidade de dois qubits nunca pode exceder sua concorrência.*

Demonstração. Sabemos pela proposição 16 que toda matriz densidade ρ pode ser escrita como soma convexa de matrizes densidade de estados puros, todas com a mesma concorrência $C(\rho)$. Pela linearidade da transposição parcial, ρ^{T_1} é escrita como soma convexa das transpostas parciais dessas matrizes densidade de estados puros.

Como para estados puros, negatividade e concorrência coincidem, cada estado puro que aparece na decomposição possui um autovalor negativo igual a $C(\rho)$, uma vez que provamos no corolário 4 que cada matriz densidade de dois qubits possui no máximo um autovalor negativo.

Sabemos pelo corolário 1 que o autovalor mínimo de uma soma de matrizes é maior que a soma dos autovalores mínimos dessas matrizes. Desse modo, a negatividade de ρ é menor que a negatividade das matrizes que fazem parte da soma convexa, que é igual à concorrência de ρ. Isso prova o resultado.

□

Os estados que maximizam a negatividade dada a concorrência C são os estados puros. Os estados que minimizam a negatividade dada a concorrência são os estados da forma

$$\begin{bmatrix} C/2 & 0 & 0 & C/2 \\ 0 & 1-C & 0 & 0 \\ 0 & 0 & 0 & 0 \\ C/2 & 0 & 0 & C/2 \end{bmatrix}$$

para os quais a negatividade e a concorrência estão relacionados através da equação

$$N^2 + 2N(1-C) - C^2 = 0.$$

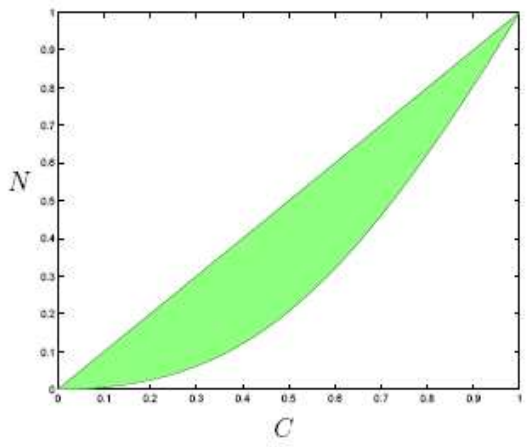


Figura 4.2: Negatividade × Concorrência

Detalhes sobre esses resultados podem ser encontrados em [1].

Comparações como essas podem ser feitas entre vários quantificadores de emaranhamento. Em [11] podemos encontrar algumas delas e referências para os resultados.

O que apresentamos aqui vale para sistemas bipartites, e alguns resultados, como os relativos à negatividade e à concorrência, apenas para o sistema de dois qubits. O próximo passo seria considerarmos sistemas de dimensões maiores e com um número maior de subsistemas.

No entanto, quando aumentamos a dimensão do espaço de estados fica cada vez mais difícil quantificar o emaranhamento de maneira satisfatória. Mesmo decidir se um estado é ou não emaranhado já se torna um problema difícil, uma vez que o critério de Peres-Horodecki não é mais suficiente e os critérios necessários e suficientes não são nada práticos. Surge também uma propriedade que não aparece no sistema de dois qubits: pode haver "diferentes" tipos de

emaranhamento. Quando aumentamos o número de subsistemas a dificuldade é ainda maior. Para começar, devemos especificar que tipo de correlações vamos chamar de emaranhamento. Por exemplo, os subsistemas 1 e 2 podem estar emaranhados, mas o sistema 3 pode estar fatorado do sistema 1-2, ou pode haver o que é chamado de emaranhamento genuíno.

Por todas essas razões, ainda há muito trabalho pela frente no estudo do emaranhamento. Para o leitor interessado em maiores detalhes sobre os quantificadores apresentados e quantificadores para sistemas com dimensões maiores sugerimos as referências [11, 21], onde outras referências também podem ser encontradas.

Considerações finais

O artigo [1], que motivou essa dissertação, foi publicado em 2001. O artigo que apresenta a Negatividade como monótono de emaranhamento [3] foi escrito no mesmo ano e o artigo relacionando Concorrência e Emaranhamento de Formação [46] foi publicado em 1998. Mesmo sendo resultados já conhecidos há algum tempo pela comunidade, suas demonstrações sempre nos pareceram confusas e por isso decidimos estudá-las nessa dissertação de mestrado. Acreditamos que agora essas demonstrações estão mais claras e vão ser mais facilmente entendidas por outros alunos que se interessem pelo assunto.

Desde lá, cerca de 10 anos se passaram e muitos outros quantificadores foram criados e vários novos resultados foram obtidos, além de vários outros que já eram conhecidos na época e que não abordamos nesse trabalho. Por essa razão, o que apresentamos aqui é apenas uma mínima fatia da vasta área de Informação e Computação quânticas. Para uma compilação de vários resultados e referências sugerimos [11, 21]. Essas referências apresentam um resumo dos resultados conhecidos e dos problemas em aberto em vários ramos diferentes da área. Lá também podem ser encontradas referências para as realizações experimentais de vários resultados.

Bibliografia

[1] F. Verstraete, K. Audenaert, J. Dehaene, and B. D. Moor, "*A comparison of the entanglement measures negativity and concurrence*," *J. Phys. A*, vol. 34, p. 10327.

[2] F. Verstraete, A Study of Entanglement in Quantum Information Theory . PhD thesis, Katholieke Universiteit Leuven, 2002.

[3] G. Vidal and R. . Werner, "*Computable Measure of Entanglement*," *Phys. Rev. Lett.*, vol. 65, p. 32314.

[4] R. J. Biezuner, Análise Funcional. Notas de Aula.

[5] C. Cohen-Tannoudji, B. Diu, and F. Laloë, Quantum Mechanics. Wiley, 1977.

[6] D. J. Griffiths, Introduction to Quantum Mechanics. Pearson Prentice Hall, 2005.

[7] K. M. Hoffman and R. Kunze, Linear Algebra. Prentice-Hall, 1961.

[8] I. Vainsencher, Álgebra Linear. Notas de Aula.

[9] S. Helgason, Differential Geometry and Symmetric Spaces. AMS Chelsea Publishing, 1962.

[10] A. L. Onishchik, Lie Groups and Lie Algebras I. Springer-Verlag, 1988.

[11] I. Bengtsson and K. Zyczkowski, Geometry of Quantum States, an Introduction to Quantum Entanglement. Cambridge University Press, 2006.

[12] S. Lang, Linear Algebra. Springer, 1987.

[13] M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information. Cambridge University Press, 2000.

[14] S. Lang, Algebra. Springer, 2002.

[15] V. Vedral, Introduction to Quantum Information Science. Oxford University Press, 2006.

[16] J. R. Munkres, Topology. Prentice Hall, 2000.

[17] C. E. Shannon and W. Weaver, The Mathematical Theory of Comunication. University of Illinois Press, 1949.

[18] A. Peres, Quantum Theory: Concepts and Methods. Kluwer Academic Publishers, 1995.

[19] K. Kraus, States, Effects and Operators: Fundamental Notions of Quantum Theory. Springer-Verlag, 1983.

[20] M. Horodecki, P. Horodecki, and R. Horodecki, "*Separability of Mixed States: Necessary and Sufficient Conditions*," *Phys. Rev. A*, vol. 223, p. 1.

[21] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "*Quantum entanglement*," *Rev. Mod. Phys.*, vol. 81, p. 865.

[22] B. M. Terhal, "*Detecting Quantum Entanglement*," *Phys. Rev. A*, vol. 271, p. 319.

[23] A. Peres, "*Separability Criterion for Density Matrices*," *Phys. Rev. Lett.*, vol. 77, p. 1413.

[24] R. P. Feynman, R. B. Leighton, and M. L. Sands, The Feynman Lectures on Physics. Addison-Wesley, 1965.

[25] J. Eisert, C. Simon, and M. B. Plenio, "*On the quantification of entanglement in infinite-dimensional quantum systems*," *J. Phys. A: Math. Gen*, vol. 35, pp. 3911–3923.

[26] J. Eisert and M. B. Plenio, "*Introduction to the basics of entanglement theory in continuous-variable systems*," *International Journal of Quantum Information*, vol. 1, no. 4, pp. 479–506.

[27] D. C. Brody and L. P. Hughstone, "*Geometric quantum mechanics*," *J.Geom. Phys.*, vol. 38, p. 19.

[28] D. H. Lyons, "*An Elementary Introduction to the Hopf Fibration*," *Mathematics Magazine*, vol. 76, no. 2, 2003.

[29] R. Mosseri, "*Two and Three Qubits and Hopf Fibrations*," *arxiv:quant-ph*, vol. 0310053v1., 2003.

[30] R. Mosseri and P. Milman, "*Topological Phase for Entangled Two-Qubit States*," *Phys. Rev. Lett.*, vol. 90, p. 230403, 2003.

[31] R. H. e M. Horodecki, "*Information-theoretic aspects of insepara- bility of mixed states* ," *Phys. Rev. A*, vol. 54, p. 1838.

[32] F.Verstraete, J. Dehaene, and B. DeMoor, "*Local filtering operations on two qubits*," *Phys. Rev. A*, vol. 64, p. 010101.

[33] Y. Hong, "*A Canonical Form for Hermitian Matrices Under Complex Orthogonal Congruence*," *SIAM J. Matrix Anal. Appl.*, vol. 10, no. 2.

[34] C. H. Bennett, G. Brassard, C. Crépeau, R.Jozsa, A. Peres, and W. K. Wooters, "*Teleporting an Unknown quantum State via Dual Classical and EPR Channels*," *Phys. Rev. Lett.*, vol. 70, p. 1895.

[35] C. H. Bennett and S. J. Wiesner, "*Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*," *Phys. Rev. Lett.*, vol. 69, p. 28821.

[36] P. Shor, "*Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*," *SIAM Review*, vol. 41, no. 2.

[37] R. Jozsa, "*Entanglement and quantum computation*," *arxiv:quant-ph*, vol. 9707034., 1997.

[38] M. J. Donald, M. Horodecki, and O. Rudolph, "*The uniqueness theorem for entanglement measures*," *J. Math. Phys.*, vol. 43, p. 4252.

[39] L. Hardy, "*Method of areas for manipulating the entanglement properties of one copy of a two-particle pure entangled state*," *Phys. Rev. A*, vol. 60, p. 19112.

[40] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, "*Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*," *Phys. Rev. Lett.*, vol. 78, p. 2031.

[41] C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, "*Mixed-state entanglement and quantum error corrections*," *Phys. Rev. A*, vol. 54, p. 3824.

[42] M. B. Plenio and S. Virmani, "*An introduction to entanglement measures*," *Quantum Inf. Comp.*, vol. 7, p. 1.

[43] M. Horodecki, P. Horodecki, and R. Horodecki, "*Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?*," *Phys. Rev. Lett.*, vol. 80, p. 5239.

[44] V. Vedral and M. B. Plenio, "*Entanglement Measures and Purification Procedures*," *Phys. Rev. A*, vol. 57, p. 1619.

[45] G. Vidal and R. Tarrach, "*Robustness of entanglement*," *Phys. Rev. A*, vol. 59, p. 141.

[46] W. K. Wooters, "*Entanglement of Formation so an Arbitrary State of Two Qubits*," *Phys. Rev. Lett.*, vol. 80, p. 2245.

[47] R. A. Horn and C. R. Johnson, Matrix Analysis. Cambridge University Press, 1985.